A procedure for deciding symbolic equivalence between sets of constraint systems[☆]

Vincent Cheval[a], Hubert Comon-Lundh[b], Stéphanie Delaune[c]

[a] *LORIA, CNRS, France*
[b] *LSV, ENS Cachan & Université Paris Saclay, France*
[c] *CNRS & IRISA, France*

Abstract

We consider security properties of cryptographic protocols that can be modeled using the notion of trace equivalence. The notion of equivalence is crucial when specifying privacy-type properties, like anonymity, vote-privacy, and unlinkability.

Infinite sets of possible traces are symbolically represented using deducibility constraints. We describe an algorithm that decides trace equivalence for protocols that use standard primitives (*e.g.,* signatures, symmetric and asymmetric encryptions) and that can be represented using such constraints. More precisely, we consider symbolic equivalence between *sets* of constraint systems, and we also consider disequations. Considering sets and disequations is actually crucial to decide trace equivalence for a general class of processes that may involve else branches and/or private channels (for a bounded number of sessions). Our algorithm for deciding symbolic equivalence between sets of constraint systems is implemented and performs well in practice. Unfortunately, it does not scale up well for deciding trace equivalence between processes. This is however the first implemented algorithm deciding trace equivalence on such a large class of processes.

Keywords: formal methods, verification, security protocols, privacy-type properties, symbolic model.

1. Introduction

The present work is motivated by the decision of security properties of cryptographic protocols. Such protocols are proliferating, because of the expansion of digital communications and the increasing concern on security issues. Finding attacks/proving the security of such protocols is challenging and has a strong societal impact.

In our work, we assume perfect cryptographic primitives: we consider a formal, symbolic, model of execution. Such an assumption may prevent from finding some attacks; the relevance of symbolic models is studied in other research papers (see *e.g.,* [1, 2]), but it is beyond the scope of the present work.

[☆]The research leading to these results has received funding from the ANR project Sequoia.

In this context, the protocols are described in some process algebra, using function symbols to represent the cryptographic primitives and symbolic terms to represent messages. We use the applied pi-calculus [3] in this paper. Many attacks on several protocols have been found during the last 20 years. For example, a flaw has been discovered (see [4]) in the Single-Sign-On protocol used *e.g.,* by Google Apps. These attacks on formal models of protocols can of course be reproduced on the concrete versions of the protocols. Several techniques and tools have been designed for the formal verification of cryptographic protocols. For instance CSP/FDR [5], PROVERIF [6], SCYTHER [7], AVISPA [8] and others.

Most results and tools only consider security properties that can be expressed as the (un)reachability of some bad state. For instance, the (weak) secrecy of s is the non-reachability of a state, in which s is known by the attacker. Authentication is also expressed as the impossibility to reach a state, in which two honest parties hold different values for a variable on which they are supposed to agree. In our work, we are interested in more general properties, typically strong secrecy, anonymity, or more generally any privacy-type property that cannot be expressed as the (non) reachability of a given state, but rather requires the *indistinguishability* of two processes. For instance, the strong secrecy of s is specified as the indistinguishability of $P(s)$ from $P(s')$, where s' is a new name. It expresses that the attacker cannot learn any piece of the secret s. Formally, these properties, as well as many other interesting security properties, can be expressed using *trace equivalence*: roughly, two processes P and Q are trace equivalent if any sequence of attacker's actions yields indistinguishable outputs of P and Q.

Some related work. The automated verification of equivalence properties for security protocols was first considered in [9] (within the spi-calculus). PROVERIF also checks some equivalence properties (so-called diff-equivalence) [10], which is a stronger equivalence, often too strong, as we will see below with a simple example. More recently, the approach behind the TAMARIN verification tool [11] has been extended to check equivalence-based properties [12]. Actually, the equivalence notion is quite similar to the notion of diff-equivalence used in ProVerif, and therefore suffers from the same drawbacks. A few other procedures have been published:

- In [13, 14] a decision procedure for the trace equivalence of bounded deterministic processes is proposed. Their procedure relies on an other procedure for deciding the equivalence of constraint systems such as the one developed by [15] or [16]. In particular, the processes are restricted to be determinate and do not contain (non trivial) conditional branching. Furthermore, the procedure seems to be not well-suited for an implementation. Regarding primitives, these works allow any primitives that are defined using a subterm convergent rewriting system.

- [17] gives a decision procedure for open-bisimulation for bounded processes in the spi-calculus. This procedure has been implemented. The scope is however limited: open-bisimulation is a stronger equivalence notion, and the procedure assumes a fixed set of primitives (in particular no asymmetric encryption) and no conditional branching.

- [18] designs a procedure based on Horn clauses for the class of optimally reducing theories, which encompasses subterm convergent theories. The procedure is sound

and complete but its termination is not guaranteed. It applies to determinate processes without replication nor else branches. Moreover, when processes are not determinate, the procedure can be used for both under- and over-approximations of trace equivalence.

Our contribution. Our aim was to design a procedure, which is general enough and efficient enough, so as to automatically verify the security of some simple protocols, such as the private authentication protocol (see Example 1) or the e-passport protocol analysed *e.g.,* in [19]. Both protocols are beyond the scope of any above mentioned results. An extension of ProVerif has been developed allowing one to analyse the private authentication protocol [20]. However, ProVerif is still unable for instance to deal with the e-passport protocol.

Example 1. *We consider the protocol given in [21] designed for transmitting a secret, while not disclosing the identity of the sender. In this protocol, a is willing to engage in a communication with b. However, a does not want to disclose her identity (nor the identity of b) to the outside world. Consider for instance the following protocol:*

$$\begin{array}{lcl} A \to B & : & \mathsf{aenc}(\langle n_a, \mathsf{pub}(ska)\rangle, \mathsf{pub}(skb)) \\ B \to A & : & \mathsf{aenc}(\langle n_a, \langle n_b, \mathsf{pub}(skb)\rangle\rangle, \mathsf{pub}(ska)) \end{array}$$

In words, the agent a (playing the role A) generates a new name n_a and sends it, together with her identity (here public key), encrypted with the public key of b. The agent b (playing the role B) replies by generating a new name n_b, sending it, together with n_a and his identity $\mathsf{pub}(skb)$*, encrypted with the public key of a. More formally, using pattern-matching, and assuming that each agent a holds a private key ska and a public key* $\mathsf{pub}(ska)$*, which is publicly available, the protocol could be written as follows:*

$$\mathit{PrivAuth1} \quad \left\{ \begin{array}{ll} A(ska, pkb): & \nu\, n_a.\, \mathsf{out}(\mathsf{aenc}(\langle n_a, \mathsf{pub}(ska)\rangle, pkb)) \\ B(skb, pka): & \mathsf{in}(\mathsf{aenc}(\langle x, pka\rangle, \mathsf{pub}(skb))).\\ & \quad \nu\, n_b.\, \mathsf{out}(\mathsf{aenc}(\langle x, \langle n_b, \mathsf{pub}(skb)\rangle\rangle, pka)) \end{array} \right.$$

We will later write $A(a, b)$ for $A(ska, \mathsf{pub}(skb))$,$B(b, a)$ for $B(skb, \mathsf{pub}(ska))$, and $B(b, c)$ for $B(skb, \mathsf{pub}(skc))$.

This is fine, as long as only mutual authentication is concerned. Now, if we want to ensure in addition privacy, an attacker should not get any information on who is trying to set up the agreement: $B(b, a)$ and $B(b, c)$ must be indistinguishable. This is not the case in the above protocol. Indeed, an attacker can forge e.g., *the message* $\mathsf{aenc}(\langle \mathsf{pub}(ska), \mathsf{pub}(ska)\rangle, \mathsf{pub}(skb))$ *and find out whether $c = a$ or not by observing whether b replies or not.*

The solution proposed in [21] consists in modifying the process B in such a way that a "decoy" message: $\mathsf{aenc}(\langle n_b, n_b\rangle, \mathsf{pub}(ska))$ *is sent when the received message is not as expected. This message should look like B's other message from the point of view of an outsider. More formally, this can be modelled using the following process:*

$$\mathit{PrivAuth2} \quad \left\{ \begin{array}{ll} A(ska, pkb): & \nu\, n_a.\, \mathsf{out}(\mathsf{aenc}(\langle n_a, \mathsf{pub}(ska)\rangle, pkb)) \\ B'(skb, pka): & \mathsf{in}(x).\, \nu\, n_b.\\ & \quad \mathsf{if}\ \mathsf{proj}_2(\mathsf{adec}(x, skb)) = pka \\ & \quad\quad \mathsf{then}\ \mathsf{out}(\mathsf{aenc}(\langle \mathsf{proj}_1(\mathsf{adec}(x, skb)), \langle n_b, \mathsf{pub}(skb)\rangle\rangle, pka)) \\ & \quad\quad \mathsf{else}\ \mathsf{out}(\mathsf{aenc}(\langle n_b, n_b\rangle, pka)) \end{array} \right.$$

Again, we will later write $B'(b, a)$ for $B'(skb, \mathsf{pub}(ska))$.

Still, this solution is not yet fully satisfactory since, for instance, an attacker could distinguish $B'(b, a)$ from $B'(b, c)$ by sending a message $\mathsf{aenc}(\langle H, \mathsf{pub}(ska)\rangle, \mathsf{pub}(skb))$, where H is a huge message, and observing the size of the output. This can be fixed, considering a process B'' that, additionally, checks the length of its input and sends the decoy message if the length does not match its expectation. In this paper, we will assume perfect cryptography, including length hiding. As shown in [22], the properties of our algorithm allow to extend the procedure to protocols that include length tests.

With length tests, the above protocol is secure in our model. It is actually also computationally secure, for an IND-CCA1 encryption scheme, which satisfies key-privacy (see [23] for instance). When the encryption scheme does not satisfy key-privacy, deciding the computational security would require to give explicitly to the attacker the capability of comparing the encryption keys. We do not include this test in our model. It is likely that it could be added without any significant modification of our decision procedure (extend the rule Eq-frame-frame*).*

This example shows that the conditional branching in the process B' is necessary. However, such a conditional branching is, in general, beyond the scope of any method that we mentioned so far (though, the extension [20] of ProVerif can handle the above example).

Another example is the e-passport protocol, that was analysed in [19], for which, also, conditional branchings are essential for privacy purposes. Another limitation of the existing works is the determinacy condition: for each attacker's message, there is at most one possible move of the protocol. This condition forces each message to contain the recipient's name, which is a natural restriction, but it also prevents from using private channels (which occur in some natural formalisations).

The results presented in the current paper yield a decision procedure for bounded processes, with conditional branching and non-determinism. It has been implemented and the above examples were automatically analysed.

Some difficulties. One of the main difficulties in the automated analysis of cryptographic protocols is the unbounded possible actions of an attacker: the transition system defined by a protocol is infinitely branching (and also infinite in depth when the protocols under study contain replications - which is not the case here). One of the solutions consists in symbolically representing this infinite set of possible transitions, using *symbolic constraint systems*. More precisely, *deducibility constraints* [24, 25, 26] allow one to split the possible attacker's actions in finitely many sets of actions yielding the same output of the protocol. Each of these sets is represented by a set of deducibility constraints. In this framework, attackers inputs are represented by variables, that must be deducible from the messages available at the time the input is generated and satisfying the conditions that trigger a new message output.

Example 2. *Consider the protocol PrivAuth1 and PrivAuth2given in Example 1. Assume a has sent her message. The message $\mathsf{aenc}(\langle n_a, \langle n_b, \mathsf{pub}(skb)\rangle\rangle, \mathsf{pub}(ska))$ is output only if the attacker's input x can be computed from the messages available and the attacker's initial knowledge $\{\mathsf{pub}(ska), \mathsf{pub}(skb)\}$ and satisfies the test. Formally, x is a solution of*

the constraint system:

$$\begin{cases} \mathsf{pub}(ska),\ \mathsf{pub}(skb),\ \mathsf{aenc}(\langle n_a, \mathsf{pub}(ska)\rangle, \mathsf{pub}(skb))) \vdash^? x \\ \mathsf{proj}_2(\mathsf{adec}(x, skb)) =^? \mathsf{pub}(ska) \end{cases}$$

The symbol $\vdash^?$ is interpreted as the attacker's computing capability. In our case (perfect cryptography), the attacker may only apply function symbols to known messages. This is followed by a normalisation step, in which, for instance, the second projection of a pair gives back the second component, according to the rule $\mathsf{proj}_2(\langle x, y\rangle) \to y$. Similarly, in the protocol PrivAuth2, the message $\mathsf{aenc}(\langle n_b, n_b\rangle, \mathsf{pub}(ska))$ is output if x is a solution of the constraint system:

$$\begin{cases} \mathsf{pub}(ska),\ \mathsf{pub}(skb),\ \mathsf{aenc}(\langle n_a, \mathsf{pub}(ska)\rangle, \mathsf{pub}(skb))) \vdash^? x \\ \mathsf{proj}_2(\mathsf{adec}(x, skb)) \neq^? \mathsf{pub}(ska) \end{cases}$$

Hence, though the variable x may take infinitely many values, only two relevant sets of messages have to be considered, that are respectively the solutions of the first and the second constraint systems.

Now, let us consider the trace equivalence problem. Given two processes P and Q, we have to decide whether or not, for every attacker's sequences of actions, the sequences of outputs of P and Q respectively are indistinguishable. Again, since there are infinitely many possible attacker's actions, we split them into sets that are symbolically represented using constraint systems, in such a way that the operations that are performed by, say, the process P are the same for any two solutions of the same constraint system $\mathcal{C}_P$. Assume first that there is a constraint system $\mathcal{C}_Q$ that represents the same set of attacker's actions and for which Q performs the same operations. Then P and Q are trace equivalent if and only if (at each output step) $\mathcal{C}_P$ and $\mathcal{C}_Q$ are *equivalent constraint systems*: $\mathcal{C}_P$ and $\mathcal{C}_Q$ have the same solutions and, for each solution of $\mathcal{C}_P$ the output messages of P are indistinguishable from the output messages of Q. This indistinguishability property on sequences of messages is formalised using *static equivalence*.

Example 3. *Let us come back to the private authentication protocol presented in Example 1. As explained in [21], the privacy property can be formally expressed as the (trace) equivalence of the two processes $B(b, a)$ and $B(b, c)$ that formalise the role B, in which, respectively, b is willing to talk to a and b is willing to talk to c (assuming a, b, and c are honest and their public keys are known by the attacker).*

In the protocol PrivAuth1, the traces of $B(b, a)$ are represented, as explained in Example 2, by the constraint system $\mathcal{C}_P$:

$$\mathcal{C}_P = \begin{cases} \mathsf{pub}(ska),\ \mathsf{pub}(skb),\ \mathsf{pub}(skc),\ \mathsf{aenc}(\langle n_a, \mathsf{pub}(ska)\rangle, \mathsf{pub}(skb))) \vdash^? x \\ \mathsf{proj}_2(\mathsf{adec}(x, skb)) =^? \mathsf{pub}(ska) \end{cases}$$

For any solution of the constraint, the trace consists of one message

$$\Phi_P = \mathsf{aenc}(\langle \mathsf{proj}_1(\mathsf{adec}(x, skb)), \langle n_b, \mathsf{pub}(skb)\rangle\rangle, \mathsf{pub}(ska)).$$

Otherwise, the trace is empty. The traces of $B(b, c)$ are represented in a similar way by the constraint $\mathcal{C}_Q$:

$$\mathcal{C}_Q = \begin{cases} \mathsf{pub}(ska),\ \mathsf{pub}(skb),\ \mathsf{pub}(skc),\ \mathsf{aenc}(\langle n_a, \mathsf{pub}(ska)\rangle, \mathsf{pub}(skb))) \vdash^? x \\ \mathsf{proj}_2(\mathsf{adec}(x, skb)) =^? \mathsf{pub}(skc) \end{cases}$$

For any solution of the constraint, the trace consists of one message

$$\Phi_Q = \mathsf{aenc}(\langle \mathsf{proj}_1(\mathsf{adec}(x, skb)), \langle n_b, \mathsf{pub}(skb)\rangle\rangle, \mathsf{pub}(skc)).$$

Otherwise, the trace is empty. In this particular case, $B(b, a)$ and $B(b, c)$ are trace equivalent if and only if:

1. *the sets of solutions of the two constraint systems are identical (otherwise, there is an attacker input, for which one of the traces is empty and the other is not empty)*
2. *for any solution of either constraint systems, the two output messages are indistinguishable (formally, they are statically equivalent).*

This is what is formalized (in a general setting) by the equivalence of constraint systems.

In this very example, $x = \mathsf{aenc}(\langle \mathsf{pub}(ska), \mathsf{pub}(ska)\rangle, \mathsf{pub}(skb))$ is a solution of $\mathcal{C}_P$ and not of $\mathcal{C}_Q$, thus the sets of solutions do not coincide.

In general, the situation is however more complex since, for two attacker's actions yielding two solutions of $\mathcal{C}_P$, the process Q may move in different ways. This depends in general on additional properties of the attacker's input: the actions of the attacker are split into the solutions of $\mathcal{C}_Q^1, \mathcal{C}_Q^2$.... Now, we need to consider not only the equivalence of constraint systems, but also the equivalence of *sets* of constraint systems.

Example 4. *Consider now the protocol PrivAuth2: the privacy is expressed as the trace equivalence of $B'(b, a)$ and $B'(b, c)$. The traces of $B'(b, a)$ consist in a single message:*

1. *the message $\mathsf{aenc}(\langle \mathsf{proj}_1(\mathsf{adec}(x, skb)), \langle n_b, \mathsf{pub}(skb)\rangle\rangle, \mathsf{pub}(ska))$ if x is a solution of the constraint $\mathcal{C}_1(ska)$ where:*

$$\mathcal{C}_1(\alpha) \stackrel{\mathsf{def}}{=} \begin{cases} \mathsf{pub}(ska),\ \mathsf{pub}(skb),\ \mathsf{pub}(skc),\ \mathsf{aenc}(\langle n_a, \mathsf{pub}(ska)\rangle, \mathsf{pub}(skb))) \vdash^? x \\ \mathsf{proj}_2(\mathsf{adec}(x, skb)) =^? \mathsf{pub}(\alpha) \end{cases}$$

2. *the message $\mathsf{aenc}(\langle n_b, n_b\rangle, \mathsf{pub}(ska)))$ if x is a solution of the constraint $\mathcal{C}_2(ska)$ where:*

$$\mathcal{C}_2(\alpha) \stackrel{\mathsf{def}}{=} \begin{cases} \mathsf{pub}(ska),\ \mathsf{pub}(skb),\ \mathsf{pub}(skc),\ \mathsf{aenc}(\langle n_a, \mathsf{pub}(ska)\rangle, \mathsf{pub}(skb))) \vdash^? x \\ \mathsf{proj}_2(\mathsf{adec}(x, skb)) \neq^? \mathsf{pub}(\alpha) \end{cases}$$

Now, $B'(b, a)$ and $B'(b, c)$ are trace equivalent if, for every x,

1. *$\mathcal{C}_1(ska) \vee \mathcal{C}_2(ska)$ and $\mathcal{C}_1(skc) \vee \mathcal{C}_2(skc)$ have the same solutions (when there is an output on one side, there is also an output on the other side).*
2. *For any solution of either sets of constraint systems, the output messages are statically equivalent.*

In this very example, the equivalence boils down to the static equivalence of the two following (sequences of) messages:

- $\mathsf{aenc}(\langle \mathsf{proj}_1(\mathsf{adec}(x, skb)), \langle n_b, \mathsf{pub}(skb)\rangle\rangle, \mathsf{pub}(ska))$ *(when x is a solution of $\mathcal{C}_1(ska)$),*
- $\mathsf{aenc}(\langle n_b, n_b\rangle, \mathsf{pub}(ska)))$.

This example shows already the use of sets of constraints. Let us also emphasize another important feature of our (sets of) constraint systems. In the context of equivalence problems, the relevant notion of solutions of constraint systems are not the assignments to the free variables (as it is the case in [24, 25, 26] for instance), but the *recipes* used to get such assignments, as illustrated by the following example.

Example 5. *Consider the following two processes:*

$$P = \mathsf{out}(\langle t_1, t_2\rangle).\mathsf{in}(x).\mathsf{if}\ x = t_1\ \mathsf{then}\ \mathsf{out}(s_1)\ \mathsf{else\ if}\ x = t_2\ \mathsf{then}\ \mathsf{out}(s_2)$$
$$Q = \mathsf{out}(\langle t_2, t_1\rangle).\mathsf{in}(x).\mathsf{if}\ x = t_1\ \mathsf{then}\ \mathsf{out}(s_1)\ \mathsf{else\ if}\ x = t_2\ \mathsf{then}\ \mathsf{out}(s_2)$$

where t_1, t_2 are any distinct messages that are statically equivalent, e.g., *two random numbers freshly generated.*

Let $\mathcal{C}_P^1, \mathcal{C}_P^2$ (resp. $\mathcal{C}_Q^1, \mathcal{C}_Q^2$) be the constraint systems associated with the two branches of P (resp. Q). The same assignments to x satisfy respectively $\mathcal{C}_P^1 \vee \mathcal{C}_P^2$ and $\mathcal{C}_Q^1 \vee \mathcal{C}_Q^2$. And for any such assignment, the output messages are identical. Yet, the processes are trace equivalent only if s_1, s_2 are statically equivalent. Indeed, the attacker may either forward (as x) the first or the second projection of the first output message. If he forwards the first projection, he will get s_1 in the first experiment and s_2 in the second experiment. This example shows that the relevant notion of solution *of a constraint system is not the assignment of x, but rather the way x is constructed, which we will call a* recipe.

In summary, each constraint system comes with a *frame*, recording the output messages. For instance, in Example 3, the constraint system $\mathcal{C}_P$ comes with the frame

$$\mathsf{pub}(ska);\ \mathsf{pub}(skb);\ \mathsf{pub}(skc);\ \mathsf{aenc}(\langle n_a, \mathsf{pub}(ska)\rangle, \mathsf{pub}(skb)); \Phi_P$$

and the constraint system $\mathcal{C}_Q$ comes with a frame

$$\mathsf{pub}(ska);\ \mathsf{pub}(skb);\ \mathsf{pub}(skc);\ \mathsf{aenc}(\langle n_a, \mathsf{pub}(ska)\rangle, \mathsf{pub}(skb)); \Phi_Q.$$

Later, we will define formally a more general notion of frame.

Two sets of constraint systems $\mathcal{S}$ and $\mathcal{S}'$ are equivalent if (and only if) for any solution of a constraint $\mathcal{C} \in \mathcal{S}$ and any possible way θ (recipe) to construct this solution, there is a constraint $\mathcal{C}' \in \mathcal{S}'$ such that θ also yields a solution of $\mathcal{C}'$ and the corresponding instance of the frame associated with $\mathcal{C}$ is statically equivalent to the corresponding instance of the frame associated with $\mathcal{C}'$.

In a companion paper [14], we show how the trace equivalence of processes without replication, but that may contain non trivial conditional branching and non deterministic choices, can be effectively reduced to the equivalence of sets of constraint systems. The focus of this paper is on the decision of the equivalence of such sets of constraint systems. Though, we will illustrate our techniques using examples coming from process equivalence problems. In addition, as explained in [27, 28], we will consider constraint systems that do not contain destructors (no projection nor decryption for instance). For the cryptographic primitives that we consider, this is not a restriction, since, using a narrowing technique [29], it is always possible to get rid of them, possibly at the price of introducing new variables.

Example 6. *Consider the constraint $\mathcal{C}_1(\alpha)$ in Example 4. The equality constraint* $\mathsf{proj}_2(\mathsf{adec}(x, skb)) =^? \mathsf{pub}(\alpha)$ *contains destructors. It can however be narrowed to eliminate the destructors, replacing the equation with*

$$x =^? \mathsf{aenc}(\langle x_1, x_2\rangle, \mathsf{pub}(skb)) \ \wedge \ x_2 =^? \mathsf{pub}(\alpha).$$

Overview of our procedure. The general idea of our decision algorithm for the equivalence of (sets of) constraint systems is borrowed from earlier work on deducibility constraints: we simplify the constraints until we get a simple form, on which the equivalence problem should be easy. Since we are interested in equivalence properties, there are two main differences. First, we need to consider pairs of (sets of) constraint systems. The simplification rules should be applied on both (sets of) systems at the same time; when this corresponds to guessing an attacker action, it should be the same rule, which is applied on both (sets of) systems. The second main difference concerns the equivalence checking: we have to keep track of an extended frame, recording some of the deductions of the attacker, and check the static equivalence of all instances, when the constraints are in solved form.

In comparison to previous constraint solving algorithms, there are many additional difficulties, which we will emphasize along the paper. One of the problems is that, when applying the rules in a naive way, the two (sets of) constraint systems do not necessarily reach a solved form at the same time. So, we may need to apply further rules, even when one of the systems is in solved form, which causes termination issues.

Finally, along the algorithm, we guess for instance whether or not a key is deducible. This introduces negative deducibility constraints, which might be hard to solve. We turn around the difficulty, keeping track of previous choices (*e.g.,* whether a key was deducible or not). This yields matrices of constraint systems: the different columns correspond to constraint systems that share the same structure, but may yield different outputs of the protocol, whereas the different rows correspond to different guesses of deducibility along the constraint simplification. This complication in the syntax allows some simplifications in the algorithm, since we may take advantage of the bookkeeping of different rows.

Outline. In this paper, we decide to focus on the algorithm itself, and we only give some hints about the soundness, completeness and termination of our algorithm. The interested reader will find detailed proofs of these results in appendix.

In Section 2, we introduce most of the definitions together with a few examples. The algorithm is explained in Section 3. We start with single constraint systems, before extending the rules to pairs of (sets of) constraint systems, and later matrices of constraint systems. Section 4 is probably the most technical one; it is devoted to the description of the strategy that is used to ensure soundness, completeness, and termination of our transformation rules. We describe our strategy and we illustrate the main difficulties we encountered using several examples. The procedure has been implemented in a tool called APTE, and we provide with a short summary of the experiments in Section 5.

This paper can be seen as an extended and enriched version of a part of [27]. In [27], it was shown that trace equivalence is decidable for a large class of processes. The core of [27] is the design of an algorithm for equivalence of sets of constraint systems. However, due to space limitations, the algorithm is only briefly presented. In this paper, a detailed description is given with many examples for illustration purposes. The strategy described

in this paper is not exactly the same as the one presented in [27, 28]. Actually, we manage to simplify the last steps of the strategy.

2. Messages, constraint systems, and symbolic equivalence

In this section, we introduce most of the definitions together with a few examples. In particular, we define formally the problem we are interested in, *i.e.,* symbolic equivalence between sets of constraint systems.

2.1. Messages

To model messages, we consider an infinite set of *names* $\mathcal{N} = \{a, b, \ldots, sk, k, n, m, \ldots\}$, which are used to model atomic data. We consider $\mathcal{X}^1 = \{x, y, \ldots\}$ an infinite set of *first-order variables*, as well as a *signature* $\mathcal{F}$, *i.e.,* a set of *function symbols*. More precisely, we consider $\mathcal{F} = \mathcal{F}_c \uplus \mathcal{F}_d$ where:

$$\mathcal{F}_c = \{\mathsf{senc}/2,\ \mathsf{aenc}/2,\ \mathsf{pub}/1,\ \mathsf{sign}/2,\ \mathsf{vk}/1,\ \langle\,\rangle/2,\ \mathsf{h}/1\}$$
$$\mathcal{F}_d = \{\mathsf{sdec}/2,\ \mathsf{adec}/2,\ \mathsf{check}/2,\ \mathsf{proj}_1/1,\ \mathsf{proj}_2/1\}.$$

These function symbols model signature, pairing, hash function, symmetric and asymmetric encryptions. Symbols in $\mathcal{F}_c$ are *constructors* and those in $\mathcal{F}_d$ are *destructors*.

Terms are defined as names, variables, and function symbols applied to other terms. For any $\mathsf{F} \subseteq \mathcal{F}$, $\mathsf{N} \subseteq \mathcal{N}$ and $\mathsf{V} \subseteq \mathcal{X}^1$, the set of terms built from N and V by applying function symbols in F is denoted by $\mathcal{T}(\mathsf{F}, \mathsf{N} \cup \mathsf{V})$. We denote by $vars^1(u)$ the set of (first-order) variables occurring in a term u. A term u is *ground* if $vars^1(u) = \emptyset$. We denote by $st(u)$ the set of subterms of u. A *constructor term*, resp. *ground constructor term*, is a term belonging to $\mathcal{T}(\mathcal{F}_c, \mathcal{N} \cup \mathcal{X}^1)$, resp. to $\mathcal{T}(\mathcal{F}_c, \mathcal{N})$. A ground constructor term is also called a *message*.

Example 7. *Going back to Example 1,* $m = \mathsf{aenc}(\langle n_a, \mathsf{pub}(ska)\rangle, \mathsf{pub}(skb))$ *is a message and* $t = \mathsf{aenc}(\langle \mathsf{proj}_1(\mathsf{adec}(x, skb)), \langle n_b, \mathsf{pub}(skb)\rangle\rangle, \mathsf{pub}(ska))$ *is a non ground term.*

In order to take into account the properties of our cryptographic primitives, we consider the following term rewriting system.

$$\begin{array}{rcl} \mathsf{sdec}(\mathsf{senc}(x, y), y) & \to & x \\ \mathsf{adec}(\mathsf{aenc}(x, \mathsf{pub}(y)), y) & \to & x \end{array} \qquad \begin{array}{rcl} \mathsf{proj}_1(\langle x, y\rangle) & \to & x \\ \mathsf{proj}_2(\langle x, y\rangle) & \to & y \end{array} \qquad \mathsf{check}(\mathsf{sign}(x, y), \mathsf{vk}(y)) \to x$$

The rules are standard, for instance, the first column states that the decryption of a ciphertext with the appropriate decryption key gives back the plaintext. Symmetric and asymmetric encryptions are respectively considered in each of the two rules. These rules define a convergent term rewriting system [30], and $t{\downarrow}$ denotes the normal form of t.

Example 8. *Continuing Example 7, and considering an honest execution (the one where the attacker does not interfere) of the protocol described in Example 1, the variable* x *will be instantiated with the message* $m = \mathsf{aenc}(\langle n_a, \mathsf{pub}(ska)\rangle, \mathsf{pub}(skb))$*, and* $t\{x \mapsto m\}{\downarrow} = \mathsf{aenc}(\langle n_a, \langle n_b, \mathsf{pub}(skb)\rangle\rangle, \mathsf{pub}(ska))$*, which is a message.*

We now consider a set $\mathcal{X}^2 = \{X, Y, \ldots\}$ of *recipe variables* and we write $vars^2(\cdot)$ the function that returns the set of recipe variables occurring in its argument. A *recipe* is a term built on $\mathcal{F}_c, \mathcal{F}_d$, a set of *parameters* $\mathcal{AX} = \{ax_1, \ldots, ax_n, ...\}$, that can be seen as pointers to the hypotheses (or known messages), and variables in $\mathcal{X}^2$. As in the applied pi-calculus, all the function symbols are public, *i.e.,* available to the attacker. Moreover, names are excluded from recipes: names that are known to the attacker must be given explicitly as hypotheses. We denote by Π the set of recipes, *i.e.,* $\Pi = \mathcal{T}(\mathcal{F}, \mathcal{AX} \cup \mathcal{X}^2)$. A *ground recipe* ζ is a recipe that does not contain variables ($vars^2(\zeta) = \emptyset$). We denote by $param(\zeta)$ the set of parameters that occur in ζ. Intuitively, a ground *recipe* records the attacker's computation. It is used as a witness of how a deduction has been performed.

Example 9. *As seen in Example 3, to mount an attack against the simplified version of the private authentication protocol, the attacker can build the message:*

$$\mathsf{aenc}(\langle \mathsf{pub}(ska), \mathsf{pub}(ska) \rangle, \mathsf{pub}(skb)).$$

This is indeed possible using the ground recipe $\mathsf{aenc}(\langle ax_1, ax_1 \rangle, ax_2)$ *(assuming that* ax_1 *and* ax_2 *are pointers to* $\mathsf{pub}(ska)$ *and* $\mathsf{pub}(skb)$*).*

2.2. Frames

In [3] (and subsequent papers) a *frame* is used to record the sequence of messages (or terms in a symbolic execution) that have been sent by the participants of the protocol. It can be written, using the formalism that we introduce below, as a sequence

$$\{ax_1, 1 \rhd u_1; \ldots; ax_n, n \rhd u_n\}$$

where ax_i are parameters, $1, ..., n$ are the numbering of successive outcomes (the stages of the execution) and $u_1, \ldots, u_n$ are the corresponding output messages. We extend this notion to record some additional information on attacker's deductions. Typically $(\mathsf{sdec}(X, \zeta), i \rhd u)$ records that, using a decryption with the recipe ζ, on top of a recipe X, allows one to get u (at stage i). After recording this information in the frame, we may rely on this bookkeeping, and no longer consider a decryption on top of X.

With such an extension, members of the frame may look like $\zeta, i \rhd v$ and the same stage may appear several times. However, if $\zeta = ax_j$, then we still have $i = j$. The recipes ζ that are added to the frame will always different from the previous ones, which allows to define a substitution associated with a frame, as we explain below.

Definition 1 (frame)**.** *A* frame Φ *(resp. a* closed frame*) is a sequence of the form* $\{\zeta_1, i_1 \rhd u_1; \ldots; \zeta_n, i_n \rhd u_n\}$ *where:*

- $u_1, \ldots, u_n$ *are constructor terms (resp. ground constructor terms),*
- $i_1, \ldots, i_n$ *are integers, and*
- $\zeta_1, \ldots, \zeta_n$ *are distinct general recipes (resp. ground recipes).*

The domain *of the frame* Φ *is* $\mathrm{dom}(\Phi) = \mathcal{AX} \cap \{\zeta_1, \ldots, \zeta_n\}$*. It must be equal to* $\{ax_1, \ldots, ax_m\}$ *for some* m*, and* m *is called the* size *of* Φ*. Moreover, we assume that for all* $(\zeta, i \rhd u) \in \Phi$*,* $i \leq m$ *and if* $\zeta = ax_j$ *then* $i = j$*.*

The indices $i_1, \ldots, i_n$ represent the stages at which a message is known. An attacker could indeed distinguish two processes, simply because some message can be computed earlier in one of the processes than in the other: the stage at which messages are available is a relevant information.

A frame Φ of size m defines a substitution on $\mathrm{dom}(\Phi)$: if $\mathrm{dom}(\Phi) = \{ax_1, \ldots, ax_m\}$ and, for $i = 1, \ldots, m$, we have that $(ax_i, i \rhd v_i) \in \Phi$, then we write again Φ the substitution $\{ax_1 \mapsto v_1, \ldots, ax_m \mapsto v_m\}$. We denote by $\mathsf{Init}(\Phi)$ the frame Φ restricted to its domain $\mathrm{dom}(\Phi)$. A closed frame Φ is *consistent* if, for every $(\zeta, i \rhd u) \in \Phi$, we have that $(\zeta\Phi)\!\downarrow = u$. Lastly, an *initial frame* is a frame of the form $\{ax_1, 1 \rhd u_1; \ldots; ax_m, m \rhd u_m\}$ where $ax_1, \ldots, ax_m \in \mathcal{AX}$, *i.e.* a frame such that $\Phi = \mathsf{Init}(\Phi)$.

Example 10. *Consider the following initial frame:*

$$\Phi = \{ax_1, 1 \rhd \mathsf{aenc}(\langle n_a, \mathsf{pub}(ska)\rangle, \mathsf{pub}(skb)));\ ax_2, 2 \rhd \mathsf{aenc}(n_b, \mathsf{pub}(skb))\}$$

Let $\Phi' = \Phi \uplus \{ax_3, 3 \rhd skb;\ \mathsf{adec}(ax_1, ax_3), 3 \rhd \langle n_a, \mathsf{pub}(ska)\rangle\}$. Φ' *is a closed frame. The intermediate component* $\mathsf{adec}(ax_1, ax_3), 3 \rhd \langle n_a, \mathsf{pub}(ska)\rangle$ *records the deduction of* $\langle n_a, \mathsf{pub}(ska)\rangle$ *using the recipe* $\mathsf{adec}(ax_1, ax_3)$ *at stage* 3.

Actually, we do not need to consider recipes that make unnecessary detours, or yield always junk messages. We introduce therefore a restricted set of recipes Π_r:

$$\Pi_r = \{\xi \in \Pi \mid \forall \mathsf{f} \in \mathcal{F}_d, \forall \xi_1, \ldots, \xi_n \in \Pi, \mathsf{f}(\xi_1, \ldots, \xi_n) \in st(\xi) \Rightarrow \mathsf{root}(\xi_1) \notin \mathcal{F}_c\}.$$

where $\mathsf{root}(u)$ is the root symbol of u.

Example 11. *The recipe* $\mathsf{sdec}(\mathsf{senc}(ax_1, ax_2), ax_2)$ *is not in normal form, and thus not in* Π_r*, whereas* $\mathsf{sdec}(\mathsf{senc}(ax_1, ax_1), ax_2)$*, though in normal form, is not in* Π_r*. Intuitively, this recipe, when applied to a frame, will either not yield a message or yield the message pointed by* ax_1*. In the latter case, there is a simpler recipe consisting in* ax_1 *alone.*

We define below the static equivalence in a way similar to [3]. We make explicit the success (or the failure) of decrypting or checking a signature.

Definition 2 (static equivalence)**.** *Two closed frames* Φ *and* Φ' *are* statically equivalent*, written* $\Phi \sim \Phi'$*, if they have the same size* m *and*

1. *for any ground recipe* $\zeta \in \Pi_r$ *such that* $param(\zeta) \subseteq \{ax_1, \ldots, ax_m\}$,
$$\zeta\Phi\!\downarrow \in \mathcal{T}(\mathcal{F}_c, \mathcal{N}) \text{ if, and only if, } \zeta\Phi'\!\downarrow \in \mathcal{T}(\mathcal{F}_c, \mathcal{N})$$
2. *for any ground recipes* $\zeta, \zeta' \in \Pi_r$ *such that* $param(\{\zeta, \zeta'\}) \subseteq \{ax_1, \ldots, ax_m\}$*, and the terms* $\zeta\Phi\!\downarrow$, $\zeta'\Phi\!\downarrow$ *are in* $\mathcal{T}(\mathcal{F}_c, \mathcal{N})$,
$$\zeta\Phi\!\downarrow = \zeta'\Phi\!\downarrow \text{ if, and only, if } \zeta\Phi'\!\downarrow = \zeta'\Phi'\!\downarrow.$$

We could have stated the definition with arbitrary recipes in Π. The definition would have been equivalent (see Lemma 6.7 in [28]). We chose, without loss of generality, to consider recipes in Π_r only, because it simplifies the following.

Example 12. *From Example 1, we consider the two closed frames:*

- $\Phi_1 = \Phi_0 \uplus \{ax_3, 3 \rhd m;\ ax_4, 4 \rhd \mathsf{aenc}(\langle n_a, \langle n_b, \mathsf{pub}(skb)\rangle\rangle, \mathsf{pub}(ska))\}$*, and*

- $\Phi_2 = \Phi_0 \uplus \{ax_3, 3 \rhd m;\ ax_4, 4 \rhd \mathsf{aenc}(n_b, \mathsf{pub}(ska))\}$

with $\Phi_0 = \{ax_1, 1 \rhd \mathsf{pub}(ska);\ ax_2, 2 \rhd \mathsf{pub}(skb)\}$ *and* $m = \mathsf{aenc}(\langle n_a, \mathsf{pub}(ska)\rangle, \mathsf{pub}(skb))$. *They are statically equivalent. Indeed, for any recipe* $\zeta \in \Pi_r$, *there is no redex in either* $\zeta\Phi_1$ *or* $\zeta\Phi_2$. *Moreover, it is not possible to build any ciphertext present in the frame from its components (since each ciphertext involves at least one fresh nonce which is not available to the attacker).*

Example 13. *Assume* b, c *are names. Consider the two following frames:*

$$\Phi_1 = \{ax_1, 1 \rhd a;\ ax_2, 2 \rhd \mathsf{senc}(b, a)\} \qquad \Phi_2 = \{ax_1, 1 \rhd a;\ ax_2, 2 \rhd \mathsf{senc}(c, a)\}$$

They are statically equivalent. Though the recipe $\zeta = \mathsf{sdec}(ax_1, ax_2)$ *yields a non trivial reduction when applied to* Φ_1 *(resp.* Φ_2*), the results* b *and* c *are indistinguishable. Actually, only trivial equalities can be derived on both sides. Now, if we disclose explicitly* b *(or* c*, or both), as in the frames*

$$\Phi'_1 = \Phi_1 \uplus \{ax_3, 3 \rhd b\} \qquad \Phi'_2 = \Phi_2 \uplus \{ax_3, 3 \rhd b\}$$

then the frames are not statically equivalent. Choosing the recipes $\zeta = \mathsf{sdec}(ax_1, ax_2)$ *and* $\zeta' = ax_3$, *we have that* $\zeta\Phi'_1{\downarrow} = \zeta'\Phi'_1{\downarrow}(= b)$, *while* $\zeta\Phi'_2{\downarrow} \neq \zeta'\Phi'_2{\downarrow}$. *The attacker may observe an equality on the first frame, which does not hold on the second frame.*

The first condition in the definition of static equivalence is also important: the attacker may observe the success of some operation on one of the frames, while it fails on the other.

Example 14. *Consider the two following frames:*

$$\Phi_1 = \{ax_1, 1 \rhd \mathsf{sign}(a, b); ax_2, 2 \rhd \mathsf{vk}(b)\},\ \textit{and}\ \Phi_2 = \{ax_1, 1 \rhd \mathsf{sign}(a, b); ax_2, 2 \rhd \mathsf{vk}(c)\}.$$

The attacker can only observe trivial equalities on both frames. However, if we let $\zeta = \mathsf{check}(ax_1, ax_2)$, *then* $\zeta\Phi_1{\downarrow} \in \mathcal{T}(\mathcal{F}_c, \mathcal{N})$ *and* $\zeta\Phi_2{\downarrow} \notin \mathcal{T}(\mathcal{F}_c, \mathcal{N})$. *The attacker observes the success of checking the signature in one case and its failure in the other case.*

2.3. Constraint systems

As explained in the introduction, our decision algorithm will rely on deducibility constraints, as a means to represent symbolically sets of traces of a protocol. The following definitions are consistent with [25]. In particular, the so-called monotonicity and origination properties are expressed through item 3 in the next definition. Since we are interested here in equivalence properties, we do not only need to represent sets of traces, but also to record some information on the attacker's actions that led to these traces. That is why we also include equations between recipes and a set NoUse of obsolete elements in the frame; roughly, a component of the frame is obsolete when the attacker used another recipe to get the message, at an earlier stage. Finally, we also consider negative constraints, in order to enable splitting the set of traces into disjoint sets.

Definition 3. *A* constraint system *is either* $\bot$ *or a tuple* $(S_1; S_2; \Phi; D; E; E_\Pi; ND; \mathsf{NoUse})$ *where:*

1. S_1 *(resp.* S_2*) is a set of variables in* $\mathcal{X}^1$ *(resp.* $\mathcal{X}^2$*);*
2. Φ *is a frame, whose size is some* m *and* NoUse *is a subset of* Φ*;*

3. D *is a sequence* $X_1, i_1 \vdash^? t_1;\ \ldots;\ X_n, i_n \vdash^? t_n$ *where*
   - $X_1, \ldots, X_n$ *are distinct variables in* $\mathcal{X}^2$
   - $t_1, \ldots, t_n$ *are constructor terms*
   - $1 \leq i_1 \leq \ldots \leq i_n \leq m$.
   - *for every* $(\xi, i \rhd t) \in \Phi$, $vars^1(t) \subseteq \bigcup_{i_j < i} vars^1(t_j)$;
   - *for every* $(\xi, i \rhd t) \in \Phi$, $param(\xi) \subseteq \{ax_1, \ldots, ax_i\}$ *and* $vars^2(\xi) \subseteq \{X_k \mid i_k \leq i\}$.
4. $E = \bigwedge_k u_k =^? v_k \wedge \bigwedge_i \forall \tilde{x_i} \cdot [\bigvee_j u_{i,j} \neq^? v_{i,j}]$ *where* $u_k, v_k, u_{i,j}$ *and* $v_{i,j}$ *are constructor terms.*
5. $E_\Pi = \bigwedge_i \zeta_i =^? \zeta'_i \wedge \bigwedge_j \xi_j \neq^? \xi'_j \wedge \bigwedge_k \mathsf{root}(\beta_k) \neq^? \mathsf{f}_k$ *where* ζ_i, ζ'_i, ξ_j, ξ'_j, β_k *are recipes in* Π_r *and* f_k *are constructor symbols.*
6. $ND = \bigwedge_i \forall \tilde{x_i}.[u_i \neq^? v_i \vee \bigvee_j k_{i,j} \not\vdash^? w_{i,j}]$ *where* $u_i, v_i, w_{i,j}$ *are constructor terms and* $k_{i,j} \in \mathbb{N}$.

We say that a constraint system is initial *if* $\mathsf{NoUse} = \emptyset$, $ND = \emptyset$, $E_\Pi = \emptyset$, $vars^2(D) = S_2$ *and* Φ *is an initial frame.*

Intuitively, S_1 is the set of free variables in $\mathcal{X}^1$; we may have to introduce auxiliary variables, that will be (implicitly) existentially quantified, as well as (explicitly) universally quantified variables. Similarly, S_2 is a set of main recipe variables (in $\mathcal{X}^2$) of the constraint. For readability, we will sometimes omit some of the components of the constraint system, because they are either straightforward from the context or empty. We also write $\Phi_\mathcal{C}$ for the frame part of a constraint system $\mathcal{C}$. We will later call the component D the *deducibility part* of the constraint system.

Example 15. *The constraints, as displayed in Example 2, follow another (simpler) syntax. However, as already explained, we need not only to reason about the attacker's inputs, but also on* how *he computed these values. Furthermore, as we explained in the introduction, the terms are assumed to be narrowed, so as to eliminate the destructors; in the Example 2, the variable* x *has been narrowed to* $\mathsf{aenc}(\langle x, y\rangle, \mathsf{pub}(skb))$*: for each occurrence* $d(s_1, \ldots, s_n)$ *of a destructor* d*, we unify* $d(s_1, \ldots, s_n)$ *with a left hand side of a rewrite rule* $d(v_1, \ldots, v_n) \to w$*, then replace* $d(s_1, \ldots, s_n)$ *with* w *and add the equations* $s_i =^? v_i$.

According to the syntax of the above definition, the first constraint system of that example should be written:

$$\begin{array}{ll} \Phi = & \{ax_1, 1 \rhd \mathsf{pub}(ska);\ ax_2, 2 \rhd \mathsf{pub}(skb);\ ax_3, 3 \rhd \mathsf{aenc}(\langle n_a, \mathsf{pub}(ska)\rangle, \mathsf{pub}(skb)))\} \\ D = & \{X, 3 \vdash^? \mathsf{aenc}(\langle x, y\rangle, \mathsf{pub}(skb))\} \\ E = & \{y =^? \mathsf{pub}(ska)\} \end{array}$$

Implicitly $S_1 = \{x, y\}$, $S_2 = \{X\}$, *and the set* E_Π, NoUse *and* ND *are empty. This is an initial constraint system.*

More examples will be given later. From now, $vars^1(\mathcal{C})$ will denote the set of free first-order variables of $\mathcal{C}$ (while it was, according to the Section 2.1 the set of all variables occurring in $\mathcal{C}$).

Before defining the semantics of such extended constraint systems, we need first to consider the components ND, E, and E_Π, and also to introduce the notion of *path* (see Definition 5). The semantics of ND, E and E_Π is obtained from the interpretation of atomic formulas, using the usual interpretation of logical connectives. Hence we focus on the semantics of atomic formulas in the next definition.

Definition 4 (solution of side constraints)**.** *Let θ be a substitution mapping $vars^2(\mathcal{C})$ to ground recipes, and σ be a substitution mapping $vars^1(\mathcal{C})$ to ground constructor terms.*

1. $\sigma \vDash (i \not\vdash^? u)$ *if, and only if, there is no ground recipe* $\xi \in \Pi_r$*, with* $param(\xi) \subseteq \{ax_1, \ldots, ax_i\}$*, such that* $\xi(\Phi\sigma)\downarrow = u\sigma\downarrow$*.*
2. $\sigma \vDash u \neq^? v$ *if, and only if,* $u\sigma \neq v\sigma$*.*
3. $\theta \vDash \xi_1 =^? \xi_2$ *(resp.* $\theta \vDash \xi_1 \neq^? \xi_2$*) if, and only if,* $\xi_1\theta = \xi_2\theta$ *(resp.* $\xi_1\theta \neq \xi_2\theta$*).*
4. $\theta \vDash \mathsf{root}(\xi) \neq^? \mathsf{f}$ *if, and only if,* $\mathsf{root}(\xi\theta) \neq \mathsf{f}$*.*

Note that, in items 2 and 3, we only check that the equalities and disequalities hold syntactically. Actually, some additional information about systems obtained along our procedure allow us to ensure that resulting terms are in normal form (and thus rewriting is not needed here).

Example 16. *Let* $\Phi = \{ax_1, 1 \rhd \mathsf{senc}(a, x);\ ax_2, 2 \rhd b\}$ *and* $\sigma = \{x \mapsto b\}$*. We have that* $\sigma \models (1 \not\vdash^? a)$ *whereas* $\sigma \not\models (2 \not\vdash^? a)$ *since* $\mathsf{sdec}(ax_1, ax_2)(\Phi\sigma)\downarrow = a$*.*

There are possibly several ways to compute the same message, given a frame. All possible ways of computing a given message are the observable equalities that are used in the static equivalence. Checking static equivalence will be part of the procedure for the decision of symbolic trace equivalence. Therefore, we may consider only one way (a "canonical" recipe) to get a message from a frame. We choose our recipe according to its *path*, which is the sequence of destructors applied on its leftmost argument. This sequence determines the result, regardless of other arguments. Let us make this point more precise.

Definition 5 (path)**.** *Let* $\xi \in \Pi_r$ *be such that* $\mathsf{root}(\xi) \notin \mathcal{F}_c$*. The* path of ξ*, denoted* $\mathsf{path}(\xi)$*, is a word in the language defined by the regular expression* $\mathcal{F}_d^* \cdot (\mathcal{A}\mathcal{X} + \mathcal{X}^2)$ *over an infinite alphabet. In other words, it is recursively defined as follows:*

$$\mathsf{path}(\xi) = \xi \text{ when } \xi \in \mathcal{A}\mathcal{X} \cup \mathcal{X}^2, \text{ and } \mathsf{path}(\mathsf{f}(\xi_1, \ldots, \xi_n)) = \mathsf{f} \cdot \mathsf{path}(\xi_1) \text{ otherwise.}$$

Note that, if $\mathsf{f}(\xi_1, \ldots, \xi_n) \in \Pi_r$ and $\mathsf{f} \notin \mathcal{F}_c$, then $\mathsf{root}(\xi_1)$ is a destructor, by definition of Π_r. Hence, if $\mathsf{root}(\xi) \notin \mathcal{F}_c$, $\mathsf{path}(\xi)$ is a sequence of destructors, followed by an element of $\mathcal{A}\mathcal{X} + \mathcal{X}^2$.

Example 17. *Let* $\xi = \mathsf{sdec}(\mathsf{sdec}(ax_2, ax_1), \mathsf{sdec}(ax_1, ax_2))$*. We have that* $\mathsf{path}(\xi) = \mathsf{sdec}{\cdot}\mathsf{sdec}{\cdot}ax_2$*. Assuming that the computation will lead to a message, this path determines the result of the computation.*

NoUse is a subset of the frame whose use is forbidden, because we changed the canonical recipe. This happens only in the course of our algorithm when we discover that a message can actually be computed at an earlier stage. The following defines the restrictions on the recipes that we consider.

Definition 6 (ξ conforms to Φ)**.** *Let Φ be a closed frame,* NoUse *be a subset of Φ, and ξ be a ground recipe in Π_r. We say that ξ* conforms to *the frame Φ w.r.t.* NoUse *if :*

- $\forall \zeta \in st(\xi), \forall (\zeta', i \rhd u) \in \Phi, \mathsf{path}(\zeta) = \mathsf{path}(\zeta') \Rightarrow \zeta = \zeta'$.
- $\forall (\zeta, i \rhd u) \in \mathsf{NoUse}$, $\zeta \notin st(\xi)$

Example 18. *Consider the following frame Φ:*

$$\{ax_1, 1 \rhd \langle a, b\rangle;\ ax_2, 2 \rhd \mathsf{senc}(a, b);\ ax_3, 3 \rhd b;\ ax_4, 4 \rhd a;\ ax_5, 5 \rhd \mathsf{senc}(c, a)\}$$

At some point (stage 2), we may choose a canonical way of computing a, for instance decrypting the second message with the second component of the first one. Then we record this choice in the frame $\Phi^+ = \Phi \cup \{\mathsf{sdec}(ax_2, \mathsf{proj}_2(ax_1)), 2 \rhd a\}$ as well as this commitment to the recipe used to get a: $\mathsf{NoUse} = \{ax_4, 4 \rhd a\}$.

The recipe $\mathsf{sdec}(ax_2, ax_3)$, which yields a, does not conform to Φ^+ w.r.t. NoUse *because of the first condition in the Definition 6. The recipe $\mathsf{sdec}(ax_5, ax_4)$ (that yields c) does not conform to Φ^+ w.r.t.* NoUse *because of the second condition. However, the recipes $\mathsf{sdec}(ax_2, \mathsf{proj}_2(ax_1))$, $\mathsf{proj}_1(ax_1)$, and $\mathsf{sdec}(ax_5, \mathsf{sdec}(ax_2, \mathsf{proj}_2(ax_1)))$ are conform to Φ^+ w.r.t.* NoUse.

Definition 7 (solution)**.** *A* solution *of $\mathcal{C} = (S_1; S_2; \Phi; D; E; E_\Pi; ND; \mathsf{NoUse})$ consists of a substitution σ mapping $vars^1(\mathcal{C})$ to ground constructor terms and a substitution θ mapping $vars^2(\mathcal{C})$ to ground recipes in Π_r, such that:*

1. *for every $X \in vars^2(\mathcal{C})$, $X\theta$ conforms to $\Phi\theta\sigma$ w.r.t.* $\mathsf{NoUse}\theta$*;*
2. *for every $X, j \vdash^? u$ in D, $X\theta(\Phi\sigma)\downarrow = u\sigma\downarrow$ and $param(X\theta) \subseteq \{ax_1, \ldots, ax_j\}$;*
3. *$\sigma \vDash ND \wedge E$ and $\theta \vDash E_\Pi$.*

We denote by $\mathsf{Sol}(\mathcal{C})$ the set of solutions of $\mathcal{C}$. By convention, $\mathsf{Sol}(\bot) = \emptyset$. A pair (σ, θ) that only satisfies the two first items is a pre-solution of $\mathcal{C}$.

Example 19. *Consider the constraint of Example 15. $\sigma = \{x \mapsto n_a, y \mapsto \mathsf{pub}(ska)\}$, $\theta = \{X \mapsto ax_3\}$ is the obvious solution of the constraint. Another solution is the pair (σ', θ') with $\sigma' = \{x \mapsto \mathsf{pub}(ska), y \mapsto \mathsf{pub}(ska)\}$ and $\theta' = \{X \mapsto \mathsf{aenc}(\langle ax_1, ax_1\rangle, ax_2)\}$.*

Example 20. *Consider the frame Φ^+ of Example 18, together with*

$$X, 5 \vdash^? \mathsf{senc}(x, a);\ \ x \neq^? a \wedge x \neq^? b \wedge \forall y_1, y_2.(x \neq^? \langle y_1, y_2\rangle \wedge x \neq^? \mathsf{senc}(y_1, y_2)).$$

One possible solution is $\sigma = \{x \mapsto c\}$ with $\theta = \{X \mapsto ax_5\}$.

2.4. Sets of constraint systems

Before moving to the equivalence of constraint systems, we need to consider sets of constraint systems, as explained in the introduction. We do not have however to consider arbitrary sets of constraint systems, but only constraint systems that have the same *structure*. Roughly, two systems have the same structure if they correspond to the same attacker's actions, but do not necessarily correspond to the same frame nor the same side constraints. As shown in Example 4, we needed to move from constraint systems to sets of constraint systems, because of non-deterministic choices and non-trivial conditional branchings: for the same attacker's recipes, several outcomes are possible. In such a case, the different constraint systems share the same structure, as defined below.

Definition 8 (structure)**.** *Let $\mathcal{C} = (S_1; S_2; \Phi; D; E; E_\Pi; ND; \mathsf{NoUse})$ be a constraint system. The* structure *of $\mathcal{C}$ is given by the following sets:*

$$S_2,\ E_\Pi,\ \{(X,i) \mid X, i \vdash^? u \in D\},\ \{(\xi,i) \mid \xi, i \rhd u \in \Phi\} \text{ and } \{(\xi,i) \mid \xi, i \rhd u \in \mathsf{NoUse}\}.$$

Two constraint systems $\mathcal{C}$ and $\mathcal{C}'$ have the same structure *if their underlying structures are identical. By convention, the constraint system $\bot$ has the same structure as any other constraint system.*

Definition 9. Sets of constraint systems *are sequences of constraint systems sharing the same structure.*

Example 21. *Back to Example 4, the initial set of constraint systems is given by the pair $[\mathcal{C}_1(ska), \mathcal{C}_2(ska)]$:*

$$\mathcal{C}_1(\alpha) = \begin{cases} \Phi_1 = & \Phi_0 \uplus \{ax_4, 4 \rhd m;\ ax_5, 5 \rhd \mathsf{aenc}(\langle x, \langle n_b, \mathsf{pub}(skb)\rangle\rangle, \mathsf{pub}(ska))\} \\ D_1 = & \{X, 4 \vdash^? \mathsf{aenc}(\langle x, y\rangle, \mathsf{pub}(skb))\} \\ E_1 = & \{y =^? \mathsf{pub}(\alpha)\} \end{cases}$$

$$\mathcal{C}_2(\alpha) = \begin{cases} \Phi_2 = & \Phi_0 \uplus \{ax_4, 4 \rhd m;\ ax_5, 5 \rhd \mathsf{aenc}(n_b, \mathsf{pub}(skb))\} \\ D_2 = & \{X, 4 \vdash^? \mathsf{aenc}(\langle x, y\rangle, \mathsf{pub}(skb))\} \\ E_2 = & \{y \neq^? \mathsf{pub}(\alpha)\} \end{cases}$$

where $\Phi_0 = \{ax_1, 1 \rhd \mathsf{pub}(ska);\ ax_2, 2 \rhd \mathsf{pub}(skb);\ ax_3, 3 \rhd \mathsf{pub}(skc)\}$, and $m = \mathsf{aenc}(\langle n_a, \mathsf{pub}(ska)\rangle, \mathsf{pub}(skb))$. Both constraint systems are initial constraint systems and they have the same structure.

2.5. Symbolic equivalence

We come finally to the symbolic equivalence, the property that we want to decide.

Definition 10 (symbolic equivalence $\approx_s$)**.** *Let $\mathcal{S}$ and $\mathcal{S}'$ be two sets of constraint systems. $\mathcal{S} \subseteq_s \mathcal{S}'$ if, for every $\mathcal{C} \in \mathcal{S}$, for every $(\sigma, \theta) \in \mathsf{Sol}(\mathcal{C})$, there exists $\mathcal{C}' \in \mathcal{S}'$ and a substitution σ' such that $(\sigma', \theta) \in \mathsf{Sol}(\mathcal{C}')$ and $\Phi_{\mathcal{C}}\sigma \sim \Phi_{\mathcal{C}'}\sigma'$.*

If $\mathcal{S} \subseteq_s \mathcal{S}'$ and $\mathcal{S}' \subseteq_s \mathcal{S}$, then we say that $\mathcal{S}$ and $\mathcal{S}'$ are in symbolic equivalence*, which we write $\mathcal{S} \approx_s \mathcal{S}'$.*

Example 22. *Using the notations of Example 21, the two sets of constraint systems $[\mathcal{C}_1(ska), \mathcal{C}_2(ska)]$ and $[\mathcal{C}_1(skc), \mathcal{C}_2(skc)]$ are symbolically equivalent (this is a non-trivial equivalence).*

The decision of symbolic equivalence between sets of constraint systems (the problem that is solved in this paper) is exactly the crucial piece for the decision of privacy-type security properties:

Theorem 1 ([14, 28])**.** *If symbolic equivalence between sets of constraint systems is decidable, then trace equivalence between processes with non determinism and conditional branching (but without replication) is decidable.*

3. Our algorithm

As explained in the introduction, our algorithm which decides symbolic equivalence between sets of constraint systems is based on transformations of such systems until a solved formed is reached. We start by defining and explaining these rules on a single constraint system and then explain how it is extended to pairs of sets (and actually even matrices) of constraint systems.

3.1. The transformation rules

The transformation rules are split in two parts. They are displayed in Figure 1 and Figure 2 respectively, and we start by explaining the rules on a single constraint system. For sake of readability, we only write the components of the constraint system that are modified by an application of an instance of a rule. Moreover, in all the following examples, we apply eagerly some simplifications (such simplifications are formalised and explained in Section 3.2).

The rules of Figure 1 aim at simplifying the deducibility constraints, until they only involve variables. In some respect, this amounts to enumerate (relevant) recipes. The only subtle point is that such recipes are constructed both from bottom (Dest) and from top (Cons, Axiom). Therefore, they may either yield instantiations of the recipe variables (construction from the top) or new elements in the frame (postpone the instantiation). These rules are necessary, but not sufficient, for the decision of equivalence properties, because of possible observable identities that hold on a constraint system and not on the other. The obvious case is an equality between two members of the frame, but there are more subtle examples. The complementary rules are described in Figure 2 and will be commented further.

Transformation rules for satisfiability (Figure 1). A simple idea would be to guess the top function symbol of a recipe and replace the recipe variable with the corresponding instance. When the head symbol of a recipe is a constructor and the corresponding term is not a variable, we can simplify the constraint, breaking it into pieces. This is the purpose of the rule Cons. Cons(X, f) rule simply makes a case distinction on whether the top symbol of the recipe variable X is a constructor f. Either it is, and then we can decompose the constraint, or it is not and we add a disequation of the form $\mathsf{root}(X) \neq^? \mathsf{f}$ forbidding X to start with f.

Example 23. *Consider the constraint $\mathcal{C}_1(ska)$ of Example 21:*

$$X, 4 \vdash^? \mathsf{aenc}(\langle x, \mathsf{pub}(ska)\rangle, \mathsf{pub}(skb))$$

Cons(X, aenc) *can be applied to the constraint, guessing whether or not the attacker computed the term $t = \mathsf{aenc}(\langle x, \mathsf{pub}(ska)\rangle, \mathsf{pub}(skb))$ by applying an asymmetric encryption on two previously computed messages. This yields the two constraint systems:*

$$\mathcal{C}_{11} := \left\{ \begin{array}{l} X_1, 4 \vdash^? x_1;\ X_2, 4 \vdash^? x_2 \\ t =^? \mathsf{aenc}(x_1, x_2) \ \wedge\ y =^? \mathsf{pub}(ska) \\ X =^? \mathsf{aenc}(X_1, X_2) \end{array} \right. \qquad \mathcal{C}_{12} := \left\{ \begin{array}{l} X, 4 \vdash^? t \\ y =^? \mathsf{pub}(ska) \\ \mathsf{root}(X) \neq^? \mathsf{aenc} \end{array} \right.$$

The first constraint system can be simplified, solving equations and performing replacements, which yields:

$$X_1, 4 \vdash^? \langle x, \mathsf{pub}(ska)\rangle;\ X_2, 4 \vdash^? \mathsf{pub}(skb); \quad y =^? \mathsf{pub}(ska); \quad X =^? \mathsf{aenc}(X_1, X_2)$$

$$\underline{\textsc{Cons}(X,\mathsf{f})}: \quad S_2; X, i\vdash^? t; E; E_\Pi \;\Rightarrow\; \begin{array}{l} S_2'; \; X_1, i\vdash^? x_1; \cdots; X_n, i\vdash^? x_n; \\ E\wedge t =^? \mathsf{f}(x_1,\ldots,x_n); \\ E_\Pi \wedge X =^? \mathsf{f}(X_1,\ldots,X_n) \end{array} \quad \text{or} \quad X, i\vdash^? t \;;\; E;\; E_\Pi \wedge \mathsf{root}(X) \neq^? \mathsf{f}$$

where: • $x_1,\ldots,x_n,X_1,\ldots X_n$ are fresh variables, and
• $S_2' = S_2 \cup \{X_1,\ldots,X_n\}$ if $X \in S_2$ and $S_2' = S_2$ otherwise.

$$\underline{\textsc{Axiom}(X,\mathsf{p})}: \quad \Phi;\; X, i\vdash^? u;\; E;\; E_\Pi \;\Rightarrow\; \Phi;\; E\wedge u =^? v;\; E_\Pi \wedge X =^? \xi \quad \text{or} \quad \Phi;\; X, i\vdash^? u;\; E;\; E_\Pi \wedge X \neq^? \xi$$

If Φ contains $\xi, j \rhd v$ with $i \geq j$, $\mathsf{path}(\xi) = \mathsf{p}$ and $(\xi, j \rhd v) \notin \mathsf{NoUse}$.

$$\underline{\textsc{Dest}(\xi, l\to r, i)}: \quad \Phi; E; ND \;\Rightarrow\; \begin{array}{l} \Phi,\, \mathsf{f}(\xi, X_2,\ldots,X_n), i \rhd w;\; E\wedge v =^? u_1 \\ X_2, i\vdash^? u_2;\; \ldots X_n, i\vdash^? u_n; ND \end{array} \quad \text{or} \quad \begin{array}{l} \Phi;\; E; \\ ND \wedge \forall \tilde{x}\cdot [v \neq u_1 \vee i \not\vdash^? u_2 \vee \ldots \vee i \not\vdash^? u_n] \end{array}$$

If Φ contains $\xi, j \rhd v$ with $j \leq i$ and $(\xi, j \rhd v) \notin \mathsf{NoUse}$. We denote by $\tilde{x}$ the set of variables that occur in $\mathsf{f}(u_1,\ldots,u_n) \to w$, a fresh renaming of $l \to r$. $X_2,\ldots,X_n$ are fresh variables.

Figure 1: Transformation rules for satisfiability

The rule Axiom also makes a case distinction on whether a trivial recipe (a left member of the frame, typically an axiom ax_i) can be applied. If so, the constraint can simply be removed. Otherwise, we also add a disequation between recipes forbidding it.

Example 24. *Continuing with the two constraints (respectively named $\mathcal{C}_{11}$ and $\mathcal{C}_{12}$), obtained in the previous example, $\mathcal{C}_{11}$ yields, by application of* $\textsc{Axiom}(X_2, ax_2)$*,*

$$\mathcal{C}_{111} := \left\{ \begin{array}{l} X_1, 4\vdash^? \langle x, \mathsf{pub}(ska)\rangle \\ \mathsf{pub}(skb) =^? \mathsf{pub}(skb) \\ X =^? \mathsf{aenc}(X_1, X_2) \wedge X_2 =^? ax_2 \end{array} \right. \qquad \mathcal{C}_{112} := \left\{ \begin{array}{l} X_1, 4\vdash^? \langle x, \mathsf{pub}(ska)\rangle \\ X_2, 4\vdash^? \mathsf{pub}(skb) \\ X =^? \mathsf{aenc}(X_1, X_2) \wedge X_2 \neq^? ax_2 \end{array} \right.$$

Again, $\mathcal{C}_{111}$ can be simplified as follows:

$$X_1, 4\vdash^? \langle x, \mathsf{pub}(ska)\rangle; \quad X =^? \mathsf{aenc}(X_1, ax_2) \;\wedge\; X_2 =^? ax_2$$

Trying to apply Axiom *to other deducibility constraints of $\mathcal{C}_{11}$ or using other members of the frame yields a failure of unification (we get $X_1 \neq^? ax_1, X_2 \neq^? ax_1, \ldots$). When applied to the constraint $\mathcal{C}_{12}$, the only case where the two branches are non-trivial is the*

application of $\text{AXIOM}(X, ax_4)$*:*

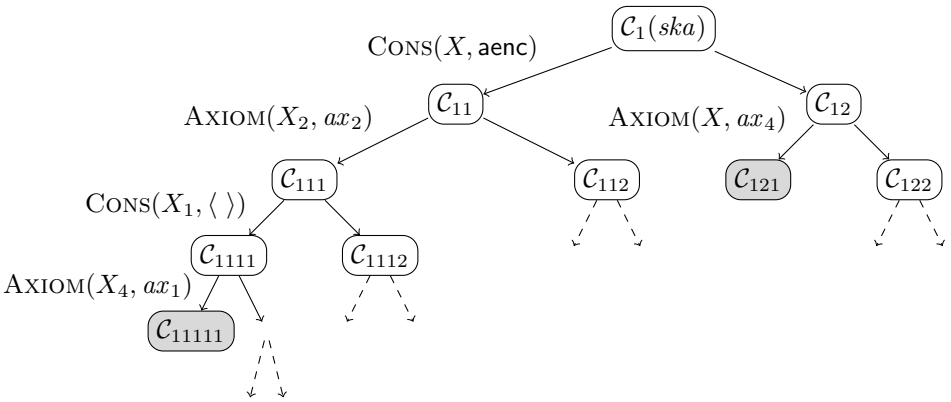
$$\mathcal{C}_{121} := \left\{ \begin{array}{l} \mathsf{aenc}(\langle x, \mathsf{pub}(ska)\rangle, \mathsf{pub}(skb)) =^? \mathsf{aenc}(\langle n_a, \mathsf{pub}(ska)\rangle, \mathsf{pub}(skb)) \\ X =^? ax_4 \wedge \mathsf{root}(X) \neq^? \mathsf{aenc} \end{array} \right.$$

$$\mathcal{C}_{122} := \left\{ \begin{array}{l} X, 4 \vdash^? \mathsf{aenc}(\langle x, \mathsf{pub}(ska)\rangle, \mathsf{pub}(skb)) \\ X \neq^? ax_4 \ \wedge \ \mathsf{root}(X) \neq^? \mathsf{aenc} \end{array} \right.$$

This can be simplified as follows:

$$\mathcal{C}_{121} = \left\{ \begin{array}{l} x =^? n_a \wedge y =^? \mathsf{pub}(ska) \\ X =^? ax_4 \end{array} \right. \qquad \mathcal{C}_{122} = \left\{ \begin{array}{l} X, 4 \vdash^? \mathsf{aenc}(\langle x, \mathsf{pub}(ska)\rangle, \mathsf{pub}(skb)) \\ X \neq^? ax_4 \ \wedge \ \mathsf{root}(X) \neq^? \mathsf{aenc} \end{array} \right.$$

An overview of our procedure applied to the constraint system $\mathcal{C}_1(ska)$ is given below:



The constraint systems $\mathcal{C}_{11}$ and $\mathcal{C}_{12}$ are those described in Example 23 whereas the constraint systems $\mathcal{C}_{111}$, $\mathcal{C}_{112}$, $\mathcal{C}_{121}$ and $\mathcal{C}_{122}$ are given in Example 24. The system $\mathcal{C}_{121}$ is actually in solved form (no more rule can be applied) and it admits a solution:

$$\sigma = \{x \mapsto n_a, y \mapsto \mathsf{pub}(ska)\} \text{ with } \theta = \{X \mapsto ax_4\}.$$

The dashed arrows indicate that even if some rules can still be applied, they would lead to constraint systems with no solution (*i.e.,* $\bot$). The constraint system $\mathcal{C}_{112}$ is not yet in solved form but $\mathcal{C}_{112}$ can not be satisfied because the only way to deduce $\mathsf{pub}(skb)$ is to use ax_2 which is forbidden by $X \neq^? ax_2$. Regarding the constraint system $\mathcal{C}_{122}$ the two possible ways to deduce a term of the form $\mathsf{aenc}(\langle x, \mathsf{pub}(ska)\rangle, \mathsf{pub}(skb))$ is to build it using aenc (but this is forbidden by the constraint $\mathsf{root}(X) \neq^? \mathsf{aenc}$) or to use ax_4 (also forbidden due to $X \neq^? ax_4$).

Regarding the left branch of the tree, we can apply the rule $\text{CONS}(X_1, \langle\,\rangle)$ on $\mathcal{C}_{111}$ to obtain the constraint systems $\mathcal{C}_{1111}$ and $\mathcal{C}_{1112}$ (which has actually no solution):

$$\mathcal{C}_{1111} := \left\{ \begin{array}{l} X_3, 4 \vdash^? x; \ X_4, 4 \vdash^? \mathsf{pub}(ska); \\ X =^? \mathsf{aenc}(\langle X_3, X_4\rangle, ax_2) \\ X_2 =^? ax_2 \wedge X_1 =^? \langle X_3, X_4\rangle \end{array} \right. \qquad \mathcal{C}_{1112} := \left\{ \begin{array}{l} X_1, 4 \vdash^? \langle x, \mathsf{pub}(ska)\rangle; \\ X =^? \mathsf{aenc}(X_1, ax_2) \\ X_2 =^? ax_2 \wedge \mathsf{root}(X_1) \neq^? \langle\,\rangle \end{array} \right.$$

Lastly, we may apply the rule $\textsc{Axiom}(X_4, ax_1)$ on $\mathcal{C}_{1111}$ and obtain on the left branch the (solved) constraint system $\mathcal{C}_{11111}$:

$$X_3, 4 \vdash^? x; \quad X =^? \mathsf{aenc}(\langle X_3, ax_1\rangle, ax_2) \wedge X_2 =^? ax_2 \wedge X_1 =^? \langle X_3, ax_1\rangle \wedge X_4 =^? ax_1$$

This system has several solutions among which $\sigma = \{x \mapsto \mathsf{pub}(ska),\ y \mapsto \mathsf{pub}(ska)\}$ obtained by mapping X_3 to ax_1. This means that the recipe $X = \mathsf{aenc}(\langle ax_1, ax_1\rangle, ax_2)$ can be used to build a message that will satisfy all the requirements: the message $\mathsf{aenc}(\langle \mathsf{pub}(ska), \mathsf{pub}(ska)\rangle, \mathsf{pub}(skb))$ is indeed of the expected form, *i.e.,* of the form $\mathsf{aenc}(\langle x, \mathsf{pub}(ska)\rangle, \mathsf{pub}(skb))$.

Now, when the top symbol of a recipe is a destructor, we can not apply the same transformation since the resulting constraint systems will become more complex, introducing new terms, which yields non-termination. Thus, our strategy is different. We switch from the top position of the recipe to the *redex position* using the rule Dest. If v is term of the frame, that can be unified with a non variable subterm of a left-hand side of a rewrite rule (for instance v is a ciphertext), we guess whether the rule can be applied to v. This corresponds to the equation $v =^? u_1$ occurring in the Dest rule, that yields an instance of w, the right member of the rewrite rule, provided that the other left members are also deducible. Typically, in case of symmetric encryption, if a ciphertext is in the frame, we will give a direct access to the plaintext by adding a new element in the frame. For this, we have to ensure that the decryption key is deducible. The index i corresponds to the stage at which we try to deduce the key. Note that a key that is not deducible at stage i may become deducible later on, *i.e.,* at stage $j > i$. Thus, we may need to apply this rule several times on the same frame element (at different stages).

Example 25. *Consider the constraint system, that includes the frame*

$$\Phi = \{ax_1, 1 \rhd \mathsf{senc}(\langle a, b\rangle, c);\ ax_2, 2 \rhd c;\ ax_3, 3 \rhd \mathsf{senc}(c, a)\}$$

and the constraint $X, 3 \vdash^? b$. *Applying* $\textsc{Dest}(ax_1, \mathsf{sdec}(\mathsf{senc}(x, y), y) \to x, 2)$, *we get:*

$$\begin{cases} \Phi,\ \mathsf{sdec}(ax_1, X_2), 2 \rhd x \\ X_2, 2 \vdash^? y;\ X, 3 \vdash^? b \\ \mathsf{senc}(x, y) =^? \mathsf{senc}(\langle a, b\rangle, c) \end{cases} \qquad \begin{cases} \Phi \\ X, 3 \vdash^? b \\ \forall x, y.(\mathsf{senc}(x, y) \neq \mathsf{senc}(\langle a, b\rangle, c) \vee 2 \not\vdash^? y) \end{cases}$$

Basically, we guess here whether the key c can be deduced at stage 2.

The second constraint is unsatisfiable, while the first one can be simplified to:

$$\Phi,\ \mathsf{sdec}(ax_1, X_2), 2 \rhd \langle a, b\rangle \qquad X_2, 2 \vdash^? c;\ X, 3 \vdash^? b$$

These transformation rules are rather schemes of rules: the side conditions both may impose some restrictions on the parameters of the rule and on the constraint, on which it is applied. They also specify the resulting constraint. In other words, we can see the side conditions as a way to schematize a (possibly infinite, yet recursive) set of rules.

Of course, these transformation rules will not be applied without restriction, otherwise we would roughly enumerate all possible attackers recipes and, though this would be complete, this would certainly not terminate. For instance, we will avoid to apply $\textsc{Cons}(X, \mathsf{f})$ to $X, i \vdash^? t$ when t is a variable, or $\textsc{Dest}(\xi, l \to r, i)$ to $\xi, j \rhd v$ when v is a variable. These restrictions will be explained at the beginning of Section 4.

Transformation rules for static equivalence (Figure 2). For equivalence properties, it is necessary to ensure that the observable identities are the same on both systems. Let us illustrate this point on an example.

Example 26. *Consider the frames:*

- $\Phi_1 = \{ax_1, 1 \rhd a;\ ax_2, 2 \rhd k_1;\ ax_3, 3 \rhd \mathsf{senc}(x, k);\ ax_4, 4 \rhd \mathsf{senc}(\mathsf{senc}(a, k_1), k)\}$
- $\Phi_2 = \{ax_1, 1 \rhd a;\ ax_2, 2 \rhd k_1;\ ax_3, 3 \rhd \mathsf{senc}(x, k);\ ax_4, 4 \rhd \mathsf{senc}(b, k)\}$.

If $x = \mathsf{senc}(a, k_1)$, then the two frames are not statically equivalent since $ax_3 = ax_4$ is an equality satisfied on the first frame and not on the second. If $x \neq \mathsf{senc}(a, k_1)$ on the first frame, and $x \neq b$ on the second one, then the two frames are statically equivalent. If, for instance, the deducibilityy constraint associated with both frames is $X, 2 \vdash^? x$, then the rules of Figure 1 will not help in finding the witness of non-equivalence.

Another set of rules, the *equality rules* described in Figure 2, will be used in such a situation. The purpose of these equality rules is to distinguish between cases, in which some equalities hold and cases, in which they do not hold. The relevant equalities that we have to consider concern the right-hand sides of deducibility constraints and/or members of the frame. These rules do not correspond to attacker's actions and they are not necessary if we are only interested in reachability properties.

The first set of rules allowed roughly to reduce any deducibility constraint to a conjunction of constraints $X, i \vdash^? x$ where X, x are variables. It allows further to assume that any relevant application of destructors to the frame has been recorded in the frame. We still miss immediately observable equalities between members of the frame: such equalities must hold (or not) simultaneously on two equivalent contraint systems. This is the purpose of the rule Eq-frame-frame, that makes a case distinction, depending on equalities between members of the frame.

This rule has to be complemented with a rule that computes other deducible subterms, that are not obtained from the frame by applications of destructors (see Example 30 and the rule Ded-st).

There are still a few ways to distinguish between two constraint systems:

- if a constraint imposes that two recipes yield the same result, then it must also be the case in the other constraint (see Example 29). Similarly if a constraint allows (for some instance of the variables) that two recipes yield the same result, this must be true on the other constraint (see Example 29 again). This is the purpose of the rule Eq-ded-ded, which investigates possible equalities relating the members of deducibility constraints.

- if some instance of a variable can be computed at an earlier stage than what is imposed by the deducibility constraint, it has to be an an earlier stage also in the other constraint system. The rule Eq-frame-ded therefore investigates whether or not some member of a deducibility constraint can be obtained at an earlier stage.

As we prove later, this finally covers all the possible situations.

$$\underline{\text{Eq-frame-frame}(\xi_1,\xi_2)}: \ E \ \begin{cases} \nearrow \ E \wedge u_1 =^? u_2 \\ \searrow \ E \wedge u_1 \neq^? u_2 \end{cases}$$

where $\xi_1, i_1 \rhd u_1,\ \xi_2, i_2 \rhd u_2 \in \Phi$ for some ξ_1, ξ_2, i_1, i_2

$$\underline{\text{Eq-frame-ded}(\xi_1,X_2)}: \ E, \mathsf{NoUse} \ \begin{cases} \nearrow \ E \wedge u_1 =^? u_2, \mathsf{NoUse} \cup (\xi_1, i_1 \rhd u_1) \\ \searrow \ E \wedge u_1 \neq^? u_2, \mathsf{NoUse} \end{cases}$$

where $\xi_1, i_1 \rhd u_1 \in \Phi$ and $X_2, i_2 \vdash^? u_2 \in D$, with $i_2 < i_1$ and $X_2 \in S_2$ for some ξ_1, ξ_2, u_1, u_2

$$\underline{\text{Eq-ded-ded}(X,\xi)}: \ X, i \vdash^? u;\ E;\ E_\Pi \ \begin{cases} \nearrow \ E \wedge u =^? v;\ E_\Pi \wedge X =^? \xi \\ \searrow \ X, i \vdash^? u;\ E \wedge u \neq^? v;\ E_\Pi \end{cases}$$

where $\xi \in \mathcal{T}(\mathcal{F}_c, \mathrm{dom}(\alpha))$, $v = \xi\alpha$ with $\alpha = \{Y \mapsto w \mid (Y, j \vdash^? w) \in D \wedge j \leq i \wedge Y \in S_2\}$. Moreover, we assume that:

- if $\mathsf{root}(\xi) = \mathsf{f}$ then $E_\Pi \not\models \mathsf{root}(X) \neq^? \mathsf{f}$
- if $\xi = Y$ then for all $\mathsf{f} \in \mathcal{F}_c$, $E_\Pi \models \mathsf{root}(X) \neq^? \mathsf{f}$ is equivalent to $E_\Pi \models \mathsf{root}(Y) \neq^? \mathsf{f}$.

$$\underline{\text{Ded-st}(\xi,\mathsf{f})}: \Phi; E; ND \ \begin{cases} \nearrow \ \Phi;\ X_1, \mathsf{s}_{max} \vdash^? x_1;\ \cdots;\ X_n, \mathsf{s}_{max} \vdash^? x_n \\ \quad E \wedge u =^? \mathsf{f}(x_1,\ldots,x_n);\ ND \\ \searrow \ \Phi;\ E;\ ND \\ \quad \forall \tilde{x} \cdot [u \neq^? \mathsf{f}(x_1,\ldots,x_n) \vee \mathsf{s}_{max} \not\vdash^? x_1 \vee \ldots \vee \mathsf{s}_{max} \not\vdash^? x_n] \end{cases}$$

If Φ contains $\xi, i \rhd u$ and $(\xi, i \rhd u) \notin \mathsf{NoUse}$. The sequences $\tilde{x} = x_1, \ldots, x_n$, and $X_1, \ldots, X_n$ are sequences of fresh variables and s_{max} represents the maximal index that occurs in $\mathcal{C}$.

Figure 2: Additional transformation rules for static equivalence

Example 27. *Let us come back to Example 26. Applying* Eq-frame-frame(ax_3, ax_4) *to the first constraint system, we get:*

$$\left\{\begin{array}{l} \Phi_1, \quad X, 2 \vdash^? x \\ \mathsf{senc}(x,k) =^? \mathsf{senc}(\mathsf{senc}(a,k_1),k) \end{array}\right. \qquad \left\{\begin{array}{l} \Phi_1, \quad X, 2 \vdash^? x \\ \mathsf{senc}(x,k) \neq^? \mathsf{senc}(\mathsf{senc}(a,k_1),k) \end{array}\right.$$

The case $x = \mathsf{senc}(a,k_1)$ is now distinguished from the case $x \neq \mathsf{senc}(a,k_1)$.

Here, we could additionally put the frame element $ax_4 \rhd \mathsf{senc}(\mathsf{senc}(a,k_1),k)$ of the first constraint system in the set NoUse (thus forbidding the use of this element). However, as illustrated by the following example (Example 28), this is not always possible,

and thus this feature is not present in the rule Eq-frame-frame contrary to what is done in the rule Eq-frame-ded.

Example 28. *Let* $\Phi = \{ax_1, 1 \rhd \langle k, \mathsf{senc}(k,k)\rangle\}$. *After applying some transformation rules, assume that we reach the frame:*

$$\Phi^+ = \{ax_1, 1 \rhd \langle k, \mathsf{senc}(k,k)\rangle;\ \mathsf{proj}_1(ax_1), 1 \rhd k;\ \mathsf{proj}_2(ax_1), 1 \rhd \mathsf{senc}(k,k);\ \mathsf{sdec}(\mathsf{proj}_2(ax_1), \mathsf{proj}_1(ax_1)), 1 \rhd k\}.$$

Applying Eq-frame-frame(ξ_1, ξ_2) *with* $\xi_1 = \mathsf{proj}_1(ax_1)$ *and* $\xi_2 = \mathsf{sdec}(\mathsf{proj}_2(ax_1), \mathsf{proj}_1(ax_1))$, *we will be tempted to put* $\mathsf{proj}_1(ax_1) \rhd k$ *in* NoUse. *If so, in order to deduce* k, *we now need to use the recipe* $\xi_2 = \mathsf{sdec}(\mathsf{proj}_2(ax_1), \mathsf{proj}_1(ax_1))$ *which is not conform to* Φ^+ *since* $\mathsf{proj}_1(ax_1) \in st(\xi_2)$ *(see Definition 6). When we put a frame element in the set* NoUse, *we have to be sure that it has not been already used to build another frame element.*

Example 29. *Consider the two constraint systems:*

$$\Phi_1 = \{ax_1, 1 \rhd a;\ ax_2, 2 \rhd b;\ ax_3, 3 \rhd x_1\},\quad D_1 = \{X, 1 \vdash^? x_1;\ Y, 2 \vdash^? x_1;\ Z, 3 \vdash^? y_1\}$$
$$\Phi_2 = \{ax_1, 1 \rhd a;\ ax_2, 2 \rhd b;\ ax_3, 3 \rhd x_2\},\quad D_2 = \{X, 1 \vdash^? x_2;\ Y, 2 \vdash^? y_2;\ Z, 3 \vdash^? y_2\}$$

There are redundant constraints in each individual system. However, we need $x_1 = y_1$ *and* $x_2 = y_2$ *in order to get equivalent systems, since the recipes* X, Y *must yield the same value, according to the first system (hence* $x_2 = y_2$*) and the recipes* Y, Z *yield the same value, according to the second system (hence* $x_1 = y_1$*). The rule* Eq-ded-ded *takes care of such situations: we guess whether different recipe variables yield the same value and record the result of the guess in the constraint.*

Actually, we sometimes need to apply Eq-ded-ded *with a recipe* ξ *which is not reduced to a variable. In particular, this is the case when we have to handle disequations between terms. Consider the two constraint systems:*

$$D_3 := \{Z, 1 \vdash^? z;\ Y, 2 \vdash^? y;\ X, 3 \vdash^? x\},\ \textit{with}\ E_3 := x \neq^? \langle y, z\rangle$$
$$D_4 := \{Z, 1 \vdash^? z;\ Y, 2 \vdash^? y;\ X, 3 \vdash^? x\}$$

The deducibility constraints are identical in both systems but the disequations in E_3 *should be satisfied by both constraint systems in order to be equivalent. By applying the rule* Eq-ded-ded *with* X *and* $\xi = \langle Y, Z\rangle$, *we split the solutions of both constraint systems into two disjoint sets: those that satisfy the equation* $x =^? \langle y, z\rangle$, *and those that do not satisfy this equation.*

As it is displayed, the rule Eq-ded-ded has infinitely many instances, as the recipe ξ is an arbitrary constructor recipe. Our strategy will later restrict the situations, in which the rule has to be applied, so that only specific instances are needed.

Finally, the last transformation rule of Figure 2 investigates the possible deducible subterms of the frame. This is a necessary step to capture static equivalence in presence of non-invertible primitives such as hash function and asymmetric encryption.

Example 30. *Consider the two constraint systems:*

- $\Phi_1 = \{ax_1, 1 \rhd \mathsf{pub}(ska);\ ax_2, 2 \rhd \mathsf{aenc}(x, \mathsf{pub}(ska))\}$ *and* $D_1 = \{X, 1 \vdash^? x\}$*;*
- $\Phi_2 = \{ax_1, 1 \rhd \mathsf{pub}(ska);\ ax_2, 2 \rhd \mathsf{aenc}(b, \mathsf{pub}(ska))\}$ *and* $D_2 = \{X, 1 \vdash^? x\}$.

Intuitively, the transformation rules we have seen so far do not help in simplifying any of the two constraint systems. The only relevant possibility would be to try decrypting $\mathsf{aenc}(x, \mathsf{pub}(sk_a))$*, but the private key ska is not deducible. Nevertheless, the two constraint systems are not equivalent since the attacker can construct* $\mathsf{aenc}(x, \mathsf{pub}(sk_a))$ *(using the recipe* $\mathsf{aenc}(X, ax_1)$*) and therefore observe the identity* $\mathsf{aenc}(X, ax_1) = ax_2$ *on* Φ_1*, which is not possible on* Φ_2*. This is the reason of the rule* Ded-st*, that guesses the subterms of the frame that can be constructed by the attacker. In the above example, the first constraint system would become:*

$$\Phi_1, \quad \{X, 1 \vdash^? x;\ X_1, 2 \vdash^? x;\ X_2, 2 \vdash^? \mathsf{pub}(ska)\}$$

(the other branch is unsatisfiable), while on the second constraint system, we get:

$$\Phi_2, \quad \{X, 1 \vdash^? x;\ X_1, 2 \vdash^? b;\ X_2, 2 \vdash^? \mathsf{pub}(ska)\}$$

Eventually, this last constraint will be proven unsatisfiable, witnessing the non-equivalence of the constraint systems.

Our rule Ded-st only considers a one-step intruder deduction, in order to incrementally check equalities and disequalities, avoiding unnecessary blow ups.

Now, before explaining how to apply the rules on pairs of sets of constraint systems, we formalise what we used implicitly in all our examples, *i.e.,* normalisation of constraint systems after the application of a transformation rule.

3.2. Normalisation

The normalisation consists mainly in simplifying the equations and disequations and performing the replacements when relevant. The *normalisation rules* are displayed in Figure 3. As usual, substitutions are confused with solved conjunctions of equations. We also switch sometimes the order of the components of a constraint system in order to ease the display, and omit irrelevant parts of the constraint system.

Here, mgu is a function that maps any conjunction of equations to their most general unifier. Such a unifier is confused with a solved system of equations, which is either $\bot$ or a conjunction $x_1 =^? t_1 \wedge \ldots \wedge x_n =^? t_n$, where $x_1, \ldots, x_n$ are variables that appear only once. Furthermore, the variables of $\mathsf{mgu}(e)$ are contained in the variables of e and $\mathsf{mgu}(\mathsf{mgu}(e)) = \mathsf{mgu}(e)$.

The first four rules simplify equations between terms/recipes. The last four rules simplify the disequations on recipes, removing them when they are trivially satisfied, or replacing the whole system with $\bot$ when they are trivially inconsistent. The remaining rules simplify disequations between (first-order) terms taking care of variables that are universally quantified. The soundness of the rules follows from complete axiomatisations of the free term algebra (see *e.g.,* [31]); let us recall that these formulas are interpreted in the free constructor algebra, according to Definition 4. If the simplification rules are applied only when they modify a constraint, then the set of rules is strongly terminating, i.e., any rewriting strategy is terminating.

We further apply two normalisation rules, that are displayed in Figure 4. Before explaining these rules, we say that the application of the rule $\textsc{Cons}(X, \mathsf{f})$, $\textsc{Axiom}(X, \mathsf{path})$, or $\textsc{Dest}(\xi, l \to r, i)$ is *useless on a constraint system* $\mathcal{C}$ if such a rule is not applicable or if a similar instance has already been applied along the same branch. In case of the rule Cons and Axiom, by similar, we mean that exactly the same instance has already been

$$\Phi; D; E_\Pi; ND; \mathsf{NoUse}; E \wedge \bigwedge_{i=1}^n u_i =^? v_i \quad \rightsquigarrow \quad \Phi\sigma; D\sigma; E_\Pi; ND\sigma; \mathsf{NoUse}\sigma; E\sigma \wedge \sigma \quad \text{if } \sigma = \mathsf{mgu}(\bigwedge_{i=1}^n u_i =^? v_i)$$

$$\Phi; D; E_\Pi; ND; \mathsf{NoUse}; E \wedge \bigwedge_{i=1}^n u_i =^? v_i \quad \rightsquigarrow \quad \bot \quad \text{if } \mathsf{mgu}(\bigwedge_{i=1}^n u_i =^? v_i) = \bot$$

$$\Phi; D; E; ND; \mathsf{NoUse}; E_\Pi \wedge \bigwedge_{i=1}^n \zeta_i =^? \xi_i \quad \rightsquigarrow \quad \Phi\theta; D; E; ND; \mathsf{NoUse}\theta; E_\Pi\theta \wedge \theta \quad \text{if } \theta = \mathsf{mgu}(\bigwedge_{i=1}^n \zeta_i =^? \xi_i)$$

$$\Phi; D; E; ND; \mathsf{NoUse}; E_\Pi \wedge \bigwedge_{i=1}^n \zeta_i =^? \xi_i \quad \rightsquigarrow \quad \bot \quad \text{if } \mathsf{mgu}(\bigwedge_{i=1}^n \zeta_i =^? \xi_i) = \bot$$

$$E \wedge \forall\tilde{x}.[\bigvee_{i=1}^n u_i \neq^? v_i] \quad \rightsquigarrow \quad E \quad \text{if } \mathsf{mgu}(\bigwedge_{i=1}^n u_i =^? v_i) = \bot$$

$$E \wedge \forall\tilde{x}.[E' \vee u \neq^? u] \quad \rightsquigarrow \quad E \wedge \forall\tilde{x}.E'$$

$$E \wedge \forall\tilde{x}.[E' \vee x \neq^? u] \quad \rightsquigarrow \quad E \wedge \forall\tilde{x} \setminus \{x\}.E'\sigma \text{if } x \in \tilde{x} \setminus vars^1(u) \text{ and } \sigma = \{x \to u\}$$

$$E \wedge \forall\tilde{x}.\forall x.E' \quad \rightsquigarrow \quad E \wedge \forall\tilde{x}.E \quad \text{if } x \notin vars^1(E)$$

$$E \wedge \forall\tilde{x}.[E' \vee \mathsf{f}(u_1, \ldots, u_n) \neq^? \mathsf{f}(v_1, \ldots v_n)] \quad \rightsquigarrow \quad E \wedge \forall\tilde{x}.[E' \vee \bigvee_{i=1}^n u_i \neq^? v_i]$$

$$E \wedge u \neq^? v \wedge \forall\tilde{x}.[E' \vee u \neq^? v] \quad \rightsquigarrow \quad E \wedge u \neq^? v$$

$$E_\Pi \wedge \zeta \neq^? \xi \quad \rightsquigarrow \quad E_\Pi \quad \text{if } \mathsf{mgu}(\zeta, \xi) = \bot$$

$$E_\Pi \wedge \zeta \neq^? \zeta \quad \rightsquigarrow \quad \bot$$

$$E_\Pi \wedge \mathsf{root}(\mathsf{f}(\xi_1, \ldots, \xi_n)) \neq \mathsf{f} \quad \rightsquigarrow \quad \bot$$

$$E_\Pi \wedge \mathsf{root}(\mathsf{f}(\xi_1, \ldots, \xi_n)) \neq \mathsf{g} \quad \rightsquigarrow \quad E_\Pi \quad \text{if } \mathsf{f} \neq \mathsf{g}$$

Figure 3: Normalisation rules for side constraints

$E \wedge \forall\tilde{x}.[E' \vee x \neq^? a] \quad \rightsquigarrow E$
if $a \in \mathcal{N}$, $(X, i \vdash^? x) \in D$, $\textsc{Axiom}(X, \mathsf{path})$ is useless for any path and
$\textsc{Dest}(\xi, l \to r, i)$ is useless for any $\xi, l \to r$, and
for all $(\zeta, j \rhd v) \in \Phi$, $j \leq i$ and $v \in \mathcal{X}^1$ implies $(\zeta, j \rhd v) \in \mathsf{NoUse}$

$D \wedge X, i \vdash^? u \quad \rightsquigarrow \quad \bot$
if $\textsc{Cons}(X, \mathsf{f})$ is useless for all $\mathsf{f} \in \mathcal{F}_c$; and $\textsc{Axiom}(X, \mathsf{path})$ is useless for any path; and
$\textsc{Dest}(\xi, l \to r, i)$ is useless for all $\xi, l \to r$; and
for all $(\zeta, j \rhd v) \in \Phi$, $j \leq i$ and $v \in \mathcal{X}^1$ implies $(\zeta, j \rhd v) \in \mathsf{NoUse}$

Figure 4: Two additional normalisation rules

applied. In case of the rule Dest, additional instances are actually useless. Indeed, there is no need to apply *e.g.,* $\textsc{Dest}(\xi, l \to r, 3)$ on the branch where a "successful" application

of $\textsc{Dest}(\xi, l \to r, 2)$ has been considered. We illustrate this concept through an example.

Example 31. *Continuing with the constraint systems named $\mathcal{C}_1^{\textsc{Dest}}$ and $\mathcal{C}_2^{\textsc{Dest}}$, obtained in Example 25, we have that:*

- $\textsc{Dest}(ax_1, l \to r, 2)$ *and* $\textsc{Dest}(ax_1, l \to r, 3)$ *are useless on* $\mathcal{C}_1^{\textsc{Dest}}$ *since an element of the form* $\mathsf{sdec}(ax_1, \_), 2 \rhd \_$ *is already present in the frame;*
- $\textsc{Dest}(ax_1, l \to r, 2)$ *is useless on* $\mathcal{C}_2^{\textsc{Dest}}$ *since the associated non-deducibility constraint already occurs in the constraint system;*
- $\textsc{Dest}(ax_3, l \to r, 1)$ *and* $\textsc{Dest}(ax_3, l \to r, 2)$ *are useless on both* $\mathcal{C}_1^{\textsc{Dest}}$ *and* $\mathcal{C}_2^{\textsc{Dest}}$ *since they do not contain any frame element of the form* $ax_3, j \rhd \_$ *with* $j \leq 2$*;*

where $(l, r) = (\mathsf{sdec}(\mathsf{senc}(x, y), y), x)$.

Now, we can explain rules displayed in Figure 4. Intuitively, the first rule states that x cannot be the name a, if it has to be deducible and cannot be obtained by Axiom or Dest. The second rule states that, in order to deduce a message, the attacker has either to construct it from deducible messages, or retrieve it from the frame and deducible messages. In other words, any attacker's ground recipe is built using $\mathcal{F}_c$, $\mathcal{F}_d$ and the ax_i.

Definition 11 (normalisation)**.** *If $\mathcal{C}$ is a constraint system, we let $\mathcal{C}\!\downarrow$ be an irreducible form of $\mathcal{C}$, w.r.t. the rules of Figures 3 and 4.*

In what follows we assume that every constraint system is eagerly normalised.

3.3. From constraint systems to pairs of sets of constraint systems

Given two constraint systems, we cannot only simplify them independently and then check for their equivalence, because actions and tests must be performed by the attacker in the same way in both experiments.

Example 32. *Consider the two following frames:*

$$\Phi_1 = \{ax_1, 1 \rhd a;\ ax_2, 2 \rhd a;\ ax_3, 3 \rhd b\}, \text{ and } \Phi_2 = \{ax_1, 1 \rhd a; ax_2, 2 \rhd b; ax_3, 3 \rhd a\}.$$

For sake of simplicity, assume there are no deducibility constraints. These two frames are not statically equivalent. Indeed, choosing $\zeta_1 = ax_1$ and $\zeta_2 = ax_2$, we have that $\zeta_1\Phi_1\!\downarrow = \zeta_2\Phi_1\!\downarrow$, while $\zeta_1\Phi_2\!\downarrow \neq \zeta_2\Phi_2\!\downarrow$.

On the other hand, we may only apply the Eq-frame-frame *rule, whose (in each case) one of the branches yields $\bot$ and on the other branch the constraint system is unchanged. Hence the rules do not help witnessing the non-equivalence, unless we apply the same instance of* Eq-frame-frame *simultaneously on both frames. For instance* $\textsc{Eq-frame-frame}(ax_1, ax_2)$ *applied to Φ_1 and Φ_2 simultaneously yields Φ_1 and $\bot$ on one branch, and $\bot$ and Φ_2 on the other.*

Intuitively, each transformation rule of Figure 1 corresponds to an action of the attacker and each rule of Figure 2 corresponds to a test of the attacker. Two constraints systems are therefore symbolically equivalent if, and only if, applying the *same rule* on both systems yields (on each branch) symbolically equivalent constraint systems.

In the introduction we motivate the need of considering sets of constraint systems, and more precisely pairs of sets of constraint systems. We explain now how our transformation rules will be applied in such a setting. Remember that sets of constraint systems are sequences of constraint systems sharing the same structure (see Definition 9). The basic idea is to apply the same transformation rule (with the same parameters) on each constraint system of each set. Note that, the parameters of a transformation rule only depend on the structure of the underlying constraint system. Thanks to this, the simultaneous application of a transformation rule can be defined in a natural way.

Given $\mathcal{S} = [\mathcal{C}_1, \ldots, \mathcal{C}_n]$ and $\mathcal{S}' = [\mathcal{C}'_1, \ldots, \mathcal{C}'_{n'}]$ two sets of size n (resp. n') of constraint systems having the same structure, and $\textsc{Rule}(\tilde{p})$ an instance of a transformation rule. The application of $\textsc{Rule}(\tilde{p})$ on the pair $(\mathcal{S}, \mathcal{S}')$ yields two pairs of sets of constraint systems $(\mathcal{S}_1, \mathcal{S}'_1)$ and $(\mathcal{S}_2, \mathcal{S}'_2)$ such that:

$$\begin{array}{ccc} & (\mathcal{S}, \mathcal{S}') & \\ \swarrow & & \searrow \\ ([\mathcal{C}_{1,1}, ..., \mathcal{C}_{1,n}], [\mathcal{C}'_{1,1}, ..., \mathcal{C}'_{1,n'}]) =: (\mathcal{S}_1, \mathcal{S}'_1) & & (\mathcal{S}_2, \mathcal{S}'_2) := ([\mathcal{C}_{2,1}, ..., \mathcal{C}_{2,n}], [\mathcal{C}'_{2,1}, ..., \mathcal{C}'_{2,n'}]) \end{array}$$

where:

- for all $i \in \{1 \ldots n\}$, the constraint systems $\mathcal{C}_{1,i}$ and $\mathcal{C}_{2,i}$ are those obtained by application of $\textsc{Rule}(\tilde{p})$ on $\mathcal{C}_i$; and
- for all $i \in \{1 \ldots n'\}$, the constraint systems $\mathcal{C}'_{1,i}$ and $\mathcal{C}'_{2,i}$ are those obtained by application of $\textsc{Rule}(\tilde{p})$ on $\mathcal{C}'_i$.

3.4. Matrices of constraint systems

The transformation of pairs of sets of constraint systems make successive case distinctions. If we only work with pairs of sets of constraint systems, we loose the relationships between the two complementary cases. This is harmless when the case distinction roughly corresponds to attacker's actions (later called *external applications*). There are however situations, in which we wish to remember that two constraints originate from the same one, and hence are complementary. We give some examples below, as well as in Section 4.

Keeping track of complementary constraints is achieved through *matrices* of constraint systems: each row corresponds to a set (now a sequence) of constraint systems, while the columns correspond to complementary choices. The matrices can be seen as a merge of some branches of the case distinction tree of the previous section.

The non-deducibility constraints introduced by the rules Dest and Ded-st allow us to properly divide the solutions of a constraint system. However, no transformation rule solves these non-deducibility constraints. When a non-deducibility constraint is introduced, the idea is to take advantage of informations that are collected, while solving the constraint in the other branch. This requires however gathering together in the same structure the constraint systems that result from the application of a rule introducing non-deducibility constraints.

Example 33. *Let $\mathcal{C}$ be a constraint system with the deducibility constraint $X, 2 \vdash^? \mathsf{senc}(a,a)$, and the frame $\Phi = \{ax_1, 1 \rhd a;\ ax_2, 2 \rhd \mathsf{senc}(b,a)\}$.* $\textsc{Dest}(ax_2, \mathsf{sdec}(\mathsf{senc}(x,y),y) \to x, 2)$ *applied on $\mathcal{C}$ gives us:*

$$\mathcal{C}_1 = \left\{ \begin{array}{l} \Phi,\ \mathsf{sdec}(ax_2, Y), 2 \rhd b \\ X, 2 \vdash^? \mathsf{senc}(a,a);\ Y, 2 \vdash^? a \end{array} \right. \quad \mathcal{C}_2 = \left\{ \begin{array}{l} \Phi;\ \ X, 2 \vdash^? \mathsf{senc}(a,a) \\ \forall x_1, x_2.[\mathsf{senc}(x_1,x_2) \neq^? \mathsf{senc}(b,a) \vee 2 \not\vdash^? x_2] \end{array} \right.$$

To solve the non-deducibility constraint in $\mathcal{C}_2$, we will use the information we get from the transformation rules applied on $\mathcal{C}_1$. Applying $\textsc{Axiom}(Y, ax_1)$ *on $\mathcal{C}_1$, we get:*

$$\mathcal{C}_3 = \left\{ \begin{array}{l} \Phi,\ \mathsf{sdec}(ax_2, ax_1), 2 \rhd b \\ X, 2 \vdash^? \mathsf{senc}(a,a) \\ Y =^? ax_1 \end{array} \right. \qquad \mathcal{C}_4 = \left\{ \begin{array}{l} \Phi,\ \mathsf{sdec}(ax_2, Y), 2 \rhd b \\ X, 2 \vdash^? \mathsf{senc}(a,a);\ Y, 2 \vdash^? a \\ Y \neq^? ax_1 \end{array} \right.$$

Using successive applications of $\textsc{Cons}(Y, \mathsf{f})$ *and* $\textsc{Axiom}(Y, \mathsf{path})$ *for any* f *and* path*, $\mathcal{C}_4$ is eventually reduced to $\bot$. Now, the formula $\forall x_1, x_2.[\mathsf{senc}(x_1,x_2) \neq^? \mathsf{senc}(b,a) \vee 2 \not\vdash^? x_2]$ has no free variable and its negation is a consequence of $\mathcal{C}_1$ (since the rule splits the set of solutions). The satisfiability of $\mathcal{C}_3$ therefore implies the unsatisfiability of $\mathcal{C}_2$.*

If we wish to perform such an inference, we need to keep in the same structure the constraints $\mathcal{C}_2$ and $\mathcal{C}_3$ (instead of solving them independently).

As illustrated in Example 33 above, solving the non-deducibility constraints will rely on the information obtained from the application of the rules on other constraint systems. That is why we gather together sets of constraint systems, and organise them into matrices, each row being a set of constraint systems.

Infering the unsatisfiability of $\mathcal{C}_2$ in Example 33 requires some properties of $\mathcal{C}_3$, typically that $\mathcal{C}_3$ is in pre-solved form. In more general situations, in which $\mathcal{C}_2$ contains (free first-order) variables that appear also in $\mathcal{C}_1$, we will also be able to apply such an inference, thanks to an invariant: if $\mathcal{C}, \mathcal{C}'$ are two constraint systems in the same column such that the frame of $\mathcal{C}$ is (roughly) a strict superset of the frame of $\mathcal{C}'$, then, for any assignment σ of the free first-order variables of $\mathcal{C}$, the solutions of $\mathcal{C}\sigma$ and $\mathcal{C}'\sigma$ are disjoint.

This relationship between constraints in the same column is eventually exploited in the step e of Section 4.

Example 34. *Applying* $\textsc{Dest}(ax_2, \mathsf{sdec}(\mathsf{senc}(x,y),y) \to x, 2)$ *on (the set)* $[\mathcal{C}]$ *given in Example 33, a priori yields two sets $[\mathcal{C}_1]$ and $[\mathcal{C}_2]$ where $\mathcal{C}_1, \mathcal{C}_2$ are the constraint systems of Example 33. We group however the resulting systems in the following matrix:*

$$\left[\begin{array}{l} \mathcal{C}_1 \\ \mathcal{C}_2 \end{array} \right]$$

Applying $\textsc{Axiom}(Y, ax_1)$*, we get now the following matrix of constraint systems:*

$$\left[\begin{array}{l} \mathcal{C}_3 \\ \mathcal{C}_4 \\ \mathcal{C}_2 \end{array} \right]$$

In order to check the non-deducibility constraint in $\mathcal{C}_2$, we only need the information provided by the constraint systems in the same column as $\mathcal{C}_2$. We will see later on how to exploit this information (see Section 4 - Phase 1 / Step e).

Note that in Example 34, the constraint systems $\mathcal{C}_1$, $\mathcal{C}_2$, $\mathcal{C}_3$, and $\mathcal{C}_4$ have the same set S_1 (resp. S_2) of first-order (resp. recipe) variables. Moreover, they have the same shape according to the following definition.

Definition 12 (shape)**.** *Let* $\mathcal{C} = (S_1; S_2; \Phi; D; E; E_\Pi; ND; \mathsf{NoUse})$ *be a constraint system. The* shape *of* $\mathcal{C}$ *is given by* S_2*, and* $\{(X, i) \mid X, i \vdash^? u \in D \text{ and } X \in S_2\}$.

Intuitively, the shape of a constraint system only takes into account the free recipe variables, *i.e.,* those that represent the actions of the attacker. By convention, we assume that the constraint system $\bot$ has the same shape as any other constraint system.

We extend the notion of *same structure* to matrices of constraint systems as follows: $\mathcal{M}$ (n rows, m columns) and $\mathcal{M}'$ (n' rows, m' columns) have the *same structure* if:

- all the constraint systems stored in $\mathcal{M}$ and $\mathcal{M}'$ have the same shape;
- $n = n'$, *i.e.,* $\mathcal{M}$ and $\mathcal{M}'$ have the same number of rows; and
- for all $i \in \{1 \dots n\}$, the constraint systems stored in the i^{th} row of the matrices $\mathcal{M}$ and $\mathcal{M}'$ have the same structure.

In fact, introducing matrices of constraint systems serves a greater purpose than just solving the non-deducibility constraints. Indeed, deciding the symbolic equivalence of sets of constraint systems contains two main issues:

- matching an existing solution from one set to the other;
- and deciding whether the two resulting frames are statically equivalent or not.

The idea behind matrices with several rows is to keep all the guesses on static equivalence into a single matrix. Intuitively, when we guess the form of the solutions, we split the matrix into two matrices. However, when we guess an equality between terms or a property on static equivalence, we gather the information in a single matrix. We thus consider two kinds of application: *internal* and *external*.

The transformation rules Ded-st, Eq-frame-frame, Eq-frame-ded and Dest will be applied internally whereas $\textsc{Cons}(X, \mathsf{f})$, $\textsc{Axiom}(X, \mathsf{path})$ and $\textsc{Eq-ded-ded}(X, \xi)$ will be applied externally when $X \in S_2$ and internally otherwise (*i.e.,* $X \notin S_2$).

Internal/external application of a transformation rule. Let $(\mathcal{M}, \mathcal{M}')$ be a pair of matrices of constraint systems having the same structure. In particular, $\mathcal{M}$ and $\mathcal{M}'$ have the same number of rows, say n. Let $\mathcal{M} = [\mathcal{S}_1, \dots, \mathcal{S}_n]$ and $\mathcal{M}' = [\mathcal{S}'_1, \dots, \mathcal{S}'_n]$. Let $\textsc{Rule}(\tilde{p})$ be an instance of a transformation rule and i be an index representing a row, *i.e.,* $1 \leq i \leq n$.

An *internal application* of $\textsc{Rule}(\tilde{p})$ to the i^{th} row of the pair $(\mathcal{M}, \mathcal{M}')$ yields a pair of matrices $(\tilde{\mathcal{M}}, \tilde{\mathcal{M}}')$ such that:

$$\tilde{\mathcal{M}} = [\mathcal{S}_1, \dots, \mathcal{S}_{i-1}, \mathcal{T}_{1,i}, \mathcal{T}_{2,i}, \mathcal{S}_{i+1}, \mathcal{S}_n] \quad \tilde{\mathcal{M}}' = [\mathcal{S}'_1, \dots, \mathcal{S}'_{i-1}, \mathcal{T}'_{1,i}, \mathcal{T}'_{2,i}, \mathcal{S}'_{i+1}, \mathcal{S}'_n]$$

where $(\mathcal{T}_{1,i}, \mathcal{T}'_{1,i})$ and $(\mathcal{T}_{2,i}, \mathcal{T}'_{2,i})$ are the pair of row matrices obtained by applying $\textsc{Rule}(\tilde{p})$ on $(\mathcal{S}_i, \mathcal{S}'_i)$. Note that, since the two matrices $\mathcal{M}$ and $\mathcal{M}'$ have the same structure, the

two sets $\mathcal{S}_i$ and $\mathcal{S}'_i$ have the same structure too and we have already seen how to apply a transformation rule in such a situation. We actually obtain two matrices with $n+1$ rows. We say that an instance $\textsc{Rule}(\tilde{p})$ of a rule is *internally applicable* on $(\mathcal{M}, \mathcal{M}')$ on row i if $\textsc{Rule}(\tilde{p})$ is applicable on $(\mathcal{S}_i, \mathcal{S}'_i)$.

An *external application* of $\textsc{Rule}(\tilde{p})$ on $(\mathcal{M}, \mathcal{M}')$ yields two pairs of matrices $(\tilde{\mathcal{M}}_1, \tilde{\mathcal{M}}'_1)$ and $(\tilde{\mathcal{M}}_2, \tilde{\mathcal{M}}'_2)$ such that:

$$\tilde{\mathcal{M}}_1 = [\mathcal{T}_{1,1}, \ldots, \mathcal{T}_{1,n}] \qquad \tilde{\mathcal{M}}'_1 = [\mathcal{T}'_{1,1}, \ldots, \mathcal{T}'_{1,n}]$$
$$\tilde{\mathcal{M}}_2 = [\mathcal{T}_{2,1}, \ldots, \mathcal{T}_{2,n}] \qquad \tilde{\mathcal{M}}'_2 = [\mathcal{T}'_{2,1}, \ldots, \mathcal{T}'_{2,n}]$$

where $(\mathcal{T}_{1,i}, \mathcal{T}'_{1,i})$ and $(\mathcal{T}_{2,i}, \mathcal{T}'_{2,i})$ are the pairs of sets obtained by applying $\textsc{Rule}(\tilde{p})$ on $(\mathcal{S}_i, \mathcal{S}'_i)$ for each $i \in \{1, \ldots, n\}$. Each resulting pair of matrices has exactly the same numbers of rows and columns as the original one $(\mathcal{M}, \mathcal{M}')$.

Remark. Unfortunately, all the constraint systems in $\mathcal{M}$ and $\mathcal{M}'$ do not necessarily have the same structure, but only the same shape. When the external application involved is an instance of a rule Cons, it is easy to see that having the same shape will ensure that the rule can be applied on each set, *i.e.,* on each row of the matrix. Regarding an external application of the rule $\textsc{Axiom}(X, \mathsf{path})$, we have to be careful. Since the constraint systems have the same shape and we know that $X \in S_2$, we can ensure that X occurs in each constraint system. However, it could happen that some rows do not contain the required frame element. By convention, in such a pair $(\mathcal{S}_i, \mathcal{S}'_i)$ of row matrices, the resulting pairs of row matrices are $(\mathcal{T}_{1,i}, \mathcal{T}'_{1,i}) \stackrel{\mathsf{def}}{=} (\bot, \bot)$ and $(\mathcal{T}_{2,i}, \mathcal{T}'_{2,i}) \stackrel{\mathsf{def}}{=} (\mathcal{S}_i, \mathcal{S}'_i)$.

Example 35. *All the rules applied in Example 34 are internal rules.*

Since our algorithm manipulates matrices of constraint systems, we extend the notion of symbolic equivalence accordingly. Given a matrix $\mathcal{M}$ having n rows and m columns, we denote by $\mathcal{M}_{i,j}$ the constraint system stored in the i^{th} row and j^{th} column, and we denote by $\Phi_{i,j}$ its associated frame.

Definition 13 (symbolic equivalence $\approx_s$)**.** *Let $\mathcal{M}$ and $\mathcal{M}'$ be two matrices of constraint systems having the same structure and of size $(n \times m)$ and $(n \times m')$ respectively. We have that $\mathcal{M} \subseteq_s \mathcal{M}'$ if for all $1 \leq i \leq n$, for all $1 \leq j \leq m$, for all $(\sigma, \theta) \in \mathsf{Sol}(\mathcal{M}_{i,j})$, there exists $1 \leq k \leq m'$ and a substitution σ' such that $(\sigma', \theta) \in \mathsf{Sol}(\mathcal{M}'_{i,k})$ and $\Phi_{i,j}\sigma \sim \Phi'_{i,k}\sigma'$.*

If $\mathcal{M} \subseteq_s \mathcal{M}'$ and $\mathcal{M}' \subseteq_s \mathcal{M}$, then we say that $\mathcal{M}$ and $\mathcal{M}'$ are in symbolic equivalence*, denoted by $\mathcal{M} \approx_s \mathcal{M}'$.*

In the following section, we will describe a quite complex strategy $\mathcal{S}$ that always terminates on sets of initial constraint systems. Before describing it, we state some soundness and completeness results, and we explain the test that is performed on the leaves to decide symbolic equivalence.

Our transformation rules yield a finite tree labeled with pairs of matrices of constraint systems. Actually, if we follow the strategy $\mathcal{S}$, we can show that our notion of equivalence is preserved through application of our transformation rules: for any transformation rule, we have that symbolic equivalence holds for the father if, and only if, symbolic equivalence holds for the children. Formally, we distinguish the case of an application of an internal rule from the one of an external rule.

Theorem 2. *[soundness and completeness for internal rules] Let $\mathcal{M}_1$, $\mathcal{M}'_1$ be two matrices of constraint systems obtained from a pair of sets of initial constraint systems by following the strategy $\mathcal{S}$. Let* $\text{RULE}(\tilde{p})$ *be an internal transformation rule applicable on $(\mathcal{M}_1, \mathcal{M}'_1)$ on the i^{th} row. Let $(\mathcal{M}_2, \mathcal{M}'_2)$ be the resulting pair of matrices of constraint systems obtained by the application of* $\text{RULE}(\tilde{p})$*. We have that:*

$$\mathcal{M}_2 \approx_s \mathcal{M}'_2 \text{ is equivalent to } \mathcal{M}_1 \approx_s \mathcal{M}'_1$$

Theorem 3. *[soundness and completeness for external rules] Let $\mathcal{M}$, $\mathcal{M}'$ be two matrices of constraint systems obtained from a pair of sets of initial constraint systems by following the strategy $\mathcal{S}$. Let* $\text{RULE}(\tilde{p})$ *be an external transformation rule applicable on $(\mathcal{M}, \mathcal{M}')$. Let $(\mathcal{M}_1, \mathcal{M}'_1)$ and $(\mathcal{M}_2, \mathcal{M}'_2)$ be the two resulting pairs of matrices of constraint systems obtained by the application of* $\text{RULE}(\tilde{p})$*. We have that:*

$$\mathcal{M}_1 \approx_s \mathcal{M}'_1 \text{ and } \mathcal{M}_2 \approx_s \mathcal{M}'_2 \text{ is equivalent to } \mathcal{M} \approx_s \mathcal{M}'$$

The proof of the soundness and completeness theorems stated above are done by a case analysis on the transformation rules. Basically, we assume the existence of a solution for a given constraint system (satisfying some properties due to our strategy $\mathcal{S}$), and we show how to transform this solution to obtain a solution for a slightly different constraint system (typically we consider a solution of a given constraint system and we have to show that, after application of a transformation rule, this solution still exists in one of its sons). In most cases, the transformation consists in replacing a recipe by another one that allows one to deduce the same message. The main issue of this replacement is to guarantee that the new recipe also satisfies all the needed properties (*e.g.,* the recipe has to be in Π_r, conformity of the recipe w.r.t. the frame, ...).

Example 36. *Consider the following constraint system $\mathcal{C}$.*

$$\mathcal{C} = \left\{ \begin{array}{l} ax_1, 1 \rhd a;\ ax_2, 2 \rhd \mathsf{senc}(a, a);\ ax_3, 3 \rhd a \\ X, 1 \vdash^? \mathsf{senc}(a, a);\ \ Y, 3 \vdash^? a \end{array} \right.$$

A solution of such a constraint system is $\theta = \{X \mapsto \mathsf{senc}(ax_1, ax_1); Y \mapsto \mathsf{sdec}(ax_2, ax_3)\}$. Note that the recipes are in Π_r and conform to the frame.

Applying the rule $\text{EQ-FRAME-DED}(ax_2, X)$*, the frame element $ax_2, 2 \rhd \mathsf{senc}(a, a)$ is added to the set* NoUse*, and thus now we have to replace ax_2 by $X\theta$ (note that both deduce the same term $\mathsf{senc}(a, a)$).*

In such a situation, $Y\theta$ will become $\mathsf{sdec}(\mathsf{senc}(ax_1, ax_1), ax_3)$ which is not a recipe in Π_r anymore. To cope with this problem, we have to replace ax_2 by $\mathsf{senc}(ax_1, ax_1)$, but also $Y\theta$ by ax_1. Thus, we get $\theta' = \{X \mapsto \mathsf{senc}(ax_1, ax_1);\ Y \mapsto ax_1\}$.

3.5. Test on leaves

By applying the rules on a pair of sets of initial constraint systems, we obtain a tree whose nodes (including the leaves) are labeled by a pair of matrices. The idea behind our transformation rules (given in Figure 1 and Figure 2) is to transform constraint systems into simpler ones, so that deciding symbolic equivalence will become trivial. Typically, as it is done in [32], we want to consider systems in which right-hand sides of deducibility constraints are distinct variables. However, in presence of disequations, putting the systems in such a form does not guarantee anymore that the two resulting systems will be in symbolic equivalence. Let us illustrate this using a simple example.

Example 37. *Consider the pair $(\mathcal{C}, \mathcal{C}')$ of sets of initial constraint systems given below (each set is reduced to a singleton):*

$$\mathcal{C} = \left\{ \ \Phi = \{ax_1, 1 \rhd a\};\ \ X, 1 \vdash^? x \right. \qquad \mathcal{C}' = \left\{ \begin{array}{l} \Phi = \{ax_1, 1 \rhd a\};\ \ X, 1 \vdash^? x \\ x \neq^? \langle a, a \rangle \end{array} \right.$$

Although these two systems have the expected form, they are not in symbolic equivalence. To see this, consider for instance the substitution $\theta = \{X \mapsto \langle ax_1, ax_1 \rangle\}$. We have that $\theta \in \mathsf{Sol}(\mathcal{C})$ but $\theta \notin \mathsf{Sol}(\mathcal{C}')$ due to the presence of the disequation.

Thus, once the system is put in this kind of "pre-solved form", the basic idea will be to continue to apply our transformation rules to "match" disequations of each constraint system. For this, we need to transform the disequations in which some names or universally quantified variables occur until obtaining disequations that only contain free variables and public function symbols. This will guarantee that there exists a recipe associated to this term and this gives us the way to match it in another constraint system. Once the system is transformed into such a new kind of "solved form" (*i.e.,* distinct variables on the right-hand side of deducibility constraints as well as matched disequations), we can now easily conclude. Indeed, since we also take care of static equivalence on the resulting frames, disequations that correspond to public disequality tests are easily transferable from one constraint system to another without any additional checks.

Example 38. *Continuing Example 37 and assuming that the pairing operator is the only constructor symbol, we will go on, applying* $\textsc{Cons}(X, \langle\ \rangle)$. *The resulting pair on the left branch will be the pair $(\mathcal{C}_1, \mathcal{C}'_1)$ where:*

$$\mathcal{C}_1 = \left\{ \begin{array}{l} \Phi;\ \ X = \langle X_1, X_2 \rangle \\ X_1, 1 \vdash^? x_1;\ X_2, 1 \vdash^? x_2 \end{array} \right. \qquad \mathcal{C}'_1 = \left\{ \begin{array}{l} \Phi;\ \ X = \langle X_1, X_2 \rangle \\ X_1, 1 \vdash^? x_1;\ X_2, 1 \vdash^? x_2 \\ x_1 \neq^? a \vee x_2 \neq^? a \end{array} \right.$$

Now, by applying the Axiom *rule twice, the resulting pair on the left branch will be the pair $(\mathcal{C}_{11}, \mathcal{C}'_{11})$ where:*

$$\mathcal{C}_{11} = \{\Phi;\ \ X = \langle ax_1, ax_1 \rangle \qquad \mathcal{C}'_{11} = \Big\{\Phi;\ \ X = \langle ax_1, ax_1 \rangle;\ \ a \neq^? a \vee a \neq^? a$$

The disequations occurring in $\mathcal{C}'_{11}$ are trivially not satisfied, thus we have that $\mathcal{C}'_{11}{\downarrow} = \bot$. These two constraint systems are trivially not in symbolic equivalence.

As illustrated above, our goal is to reach pairs of (sets) of constraint systems in *solved form*. Each constraint system is either $\bot$ or satisfies the following conditions:

1. for all $X, i \vdash^? u \in D$, we have $X \in S_2$ and u is a variable distinct from the right-hand side of any other deducibility constraint;
2. the set E does not contain any variable that is universally quantified, and for all $u \neq^? v$ in E, we have that u, v do not contain any names. Moreover, the disequations are "the same" on each constraint system occurring in the pair.

The first phase of our strategy consists in applying transformation rules to fulfil the first condition (without taking care of the disequations) and obtain a system in *pre-solved* form, whereas the second phase of our strategy will reduce the constraint systems into *solved* form. The next section is dedicated to the description of the strategy $\mathcal{S}$ that has been designed with a lot of care to ensure the termination of our procedure.

Once solved forms are reached, the test performed on each leaf labeled $(\mathcal{M}, \mathcal{M}')$ consists of checking that for each row of the matrices, either both matrices contain a constraint system different form $\bot$, or both matrices contain only $\bot$ on the whole row. More formally, we have that:

Definition 14 (test $\mathsf{LeafTest}$)**.** *Let $(\mathcal{M}, \mathcal{M}')$ be a pair of matrices of constraint systems with n rows and m (resp. m') columns.* $\mathsf{LeafTest}(\mathcal{M}, \mathcal{M}') = \mathsf{true}$ *if and only if for each row $i \in \{1 \dots n\}$, we have that:*

$\exists j \in \{1, \dots, m\}$ *with* $\mathcal{M}_{i,j} \neq \bot$ *if, and only if,* $\exists j' \in \{1, \dots, m'\}$ *with* $\mathcal{M}'_{i,j'} \neq \bot$.

Theorem 4. *Let $(\mathcal{M}_0, \mathcal{M}'_0)$ be a pair of sets of initial constraint systems and $(\mathcal{M}, \mathcal{M}')$ be a leaf of the tree whose root is labeled with $(\mathcal{M}_0, \mathcal{M}'_0)$ and which is obtained following the strategy $\mathcal{S}$. We have that $\mathcal{M} \approx_s \mathcal{M}'$ if, and only if,* $\mathsf{LeafTest}(\mathcal{M}, \mathcal{M}') = \mathsf{true}$.

The proof of this theorem is done relying on the two following properties that are satisfied by each leaf $(\mathcal{M}, \mathcal{M}')$ of the tree.

1. Any constraint system $\mathcal{C}$ occurring in $\mathcal{M}$ (resp. $\mathcal{M}'$) different from $\bot$ admits a solution, *i.e.,* $\mathsf{Sol}(\mathcal{C}) \neq \emptyset$.

2. For any constraint systems $\mathcal{C}$, $\mathcal{C}'$ that occur in the same row (possibly of the same matrice) and that are different from $\bot$, we have that $\mathcal{C} \approx_s \mathcal{C}'$.

Corollary 1 (main result)**.** *Let $\mathcal{S}$ and $\mathcal{S}'$ be two sets of initial constraint systems. We have that $\mathcal{S} \approx_s \mathcal{S}'$ if, and only if,* $\mathsf{LeafTest}(\mathcal{M}, \mathcal{M}') = \mathsf{true}$ *for any leaf of the tree whose root is labeled with $(\mathcal{S}, \mathcal{S}')$ and which is obtained following the strategy $\mathcal{S}$.*

4. Strategy

Our goal is to reduce (matrices of) constraint systems to solved forms. We proceed in two steps: first reduce the (matrices of) constraint systems to pre-solved forms, i.e., taking care on deducibility constraints only and then reduce them to solved form, considering the disequality constraints. Let us consider the first step. We may restrict the rules applications, as long as there is always at least a rule that can be applied when (some) constraint system is not in pre-solved form. That is how we design our strategy; we restrict the rules applications, while ensuring that an unsolved contraint system can be reduced by at least one rule. This is what we later call "strong application". Such a strategy is terminating when applied to a single constraint system, and yields a pre-solved form.

We are however working on pairs of (matrices of) constraint systems. In that case, we must focus on one unsolved constraint system. Otherwise, since the same rule is applied on all the constraint systems of the pair, we may go back and forth and never reach a pair in which all the systems are in solved form. We will give an example of such a phenomenon: we could go back and forth forever, simplifying alternatively the left and the right component of a pair. That is why, we need to design a more elaborate strategy on pairs of matrices. It will, roughly, require to focus on one unsolved constraint system, and to ensure that the rule is a strong application for this system. Once this system is in

pre-solved form, other rule applications (applied to put the other systems in pre-solved form) may not, as a side effet, impair this pre-solved form.

We say that a rule is *strongly applicable* on $\mathcal{C} = (S_1; S_2; \Phi; D; E; E_\Pi; ND; \mathsf{NoUse})$ when the following extra conditions are fulfilled:

- Rule Cons(X, f): either the term t is not a variable, or there exists an atomic statement $(\mathsf{root}(X) \neq^? \mathsf{g})$ in E_Π such that $\mathsf{g} \in \mathcal{F}_c$ and $\mathsf{g} \neq \mathsf{f}$;
- Rule Axiom(X, path): the term v is not a variable or there exists $\mathsf{f} \in \mathcal{F}_c$ such that $(\mathsf{root}(X) \neq^? \mathsf{f})$ in E_Π;
- Rule Dest: the term v is not a variable;
- Rule Ded-st: the term u is not a variable;
- Rule Eq-frame-frame: no additional condition;
- Rule Eq-frame-ded: the terms u_1, u_2 are the same variable.
- Rule Eq-ded-ded: $\xi \in vars^2(D)$, and u and v are the same variable.

Since we have to apply simultaneously our transformation rules on several constraint systems, we can not guarantee that each application will be a strong one. As illustrated by Example 39, this yields some termination issues.

Example 39. *Consider the pair $(\mathcal{C}, \mathcal{C}')$ of sets of initial constraint systems given below (each set is actually reduced to a singleton):*

$$\mathcal{C} = \{\ \Phi;\ X, 1 \vdash^? \mathsf{senc}(x_1, x_2);\ Y, 2 \vdash^? x_1 \qquad \mathcal{C}' = \{\ \Phi;\ X, 1 \vdash^? y_1;\ Y, 2 \vdash^? \mathsf{senc}(y_1, y_2)$$

We may apply Cons(X, senc) *on the system $\mathcal{C}$ yielding (on the left branch):*

$$\mathcal{C}_1 = \begin{cases} \Phi;\ X =^? \mathsf{senc}(X_1, X_2) \\ X_1, 1 \vdash^? x_1 \\ X_2, 1 \vdash^? x_2 \\ Y, 2 \vdash^? x_1 \end{cases} \qquad \mathcal{C}'_1 = \begin{cases} \Phi;\ X =^? \mathsf{senc}(X_1, X_2) \\ X_1, 1 \vdash^? z_1; \\ X_2, 1 \vdash^? z_2 \\ Y, 2 \vdash^? \mathsf{senc}(\mathsf{senc}(z_1, z_2), y_2) \end{cases}$$

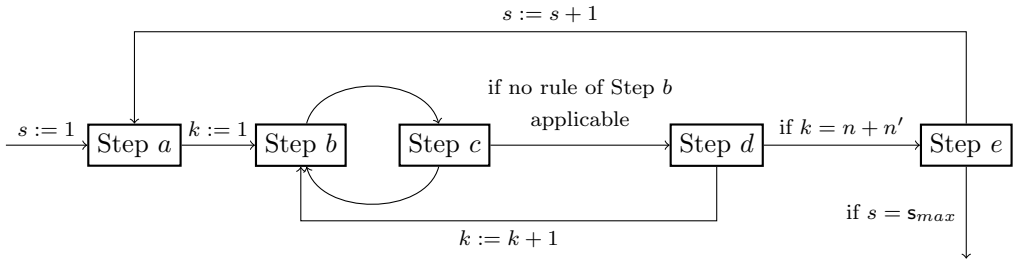
Then, again using a strong application of Cons(Y, senc) *on the system $\mathcal{C}'_1$, we obtain (on the left branch):*

$$\mathcal{C}_{11} = \begin{cases} \Phi;\ X =^? \mathsf{senc}(X_1, X_2) \\ X_1, 1 \vdash^? \mathsf{senc}(x_{11}, x_{12}) \\ X_2, 1 \vdash^? x_2 \\ Y =^? \mathsf{senc}(Y_1, Y_2) \\ Y_1, 2 \vdash^? x_{11} \\ Y_2, 2 \vdash^? x_{12} \end{cases} \qquad \mathcal{C}'_{11} = \begin{cases} \Phi;\ X =^? \mathsf{senc}(X_1, X_2) \\ X_1, 1 \vdash^? z_1 \\ X_2, 1 \vdash^? z_2 \\ Y =^? \mathsf{senc}(Y_1, Y_2) \\ Y_1, 2 \vdash^? \mathsf{senc}(z_1, z_2) \\ Y_2, 2 \vdash^? y_2 \end{cases}$$

Thus, we get back to a subproblem of the original deducibility constraints.

4.1. Taking care of deducibility constraints

The first phase of our strategy consists of applying transformation rules to put constraint systems in "pre-solved" form. As depicted below, this first phase is a cycle of several steps.



The integer s indicates the *support of the rules* that are applied during the cycle. This notion of *support of a rule* is formally defined as follows:

- the support of $\textsc{Cons}(X, \mathsf{f})$ (resp. $\textsc{Axiom}(X, \mathsf{path})$, $\textsc{Eq-ded-ded}(X, \xi)$) is i where $X, i \vdash^? u \in D$;
- the support of $\textsc{Dest}(\xi, \ell \to r, i)$ (resp. $\textsc{Ded-st}(X, \xi)$) is i (resp. s_{max} *i.e.,* the maximal index that occurs in $\mathcal{C}$);
- the support of $\textsc{Eq-frame-frame}(\xi_1, \xi_2)$ is $\max(i_1, i_2)$ where $\xi_1, i_1 \rhd u_1 \in \Phi$ and $\xi_2, i_2 \rhd u_2 \in \Phi$;
- the support of $\textsc{Eq-frame-ded}(\xi_1, X_2)$ is i_1 where $\xi_1, i_1 \rhd u_1 \in \Phi$;

The integer n (resp. n') is the number of columns in matrix $\mathcal{M}$ (resp. $\mathcal{M}'$) and m is the size of the frames that occur in $\mathcal{M}$ and $\mathcal{M}'$. The integer k indicates the column of the matrix on which we are currently working. By convention, when $k > n$, *i.e., k* is strictly greater than the number of columns in the matrix $\mathcal{M}$, this means that we work on the $(k-n)^{\text{th}}$ column of the matrix $\mathcal{M}'$.

We now explain in more detail each of these steps.

Step a: frame analysis. We apply the rules Dest and Eq-frame-ded, with support equal to s, as long as possible with priority on the rule Eq-frame-ded. The application of those rules has to be a strong application for at least one constraint system that occurred in the row of the matrix on which we apply the rule.

The main idea is to work on the frame to learn the deducible subterms (this is the purpose of the rule Dest). However, when we encounter a frame element of the form $\xi, i \rhd x$, we can not apply the Dest rule on it. The purpose of using the rule Eq-frame-ded is to "discard" this frame element by adding it into the set NoUse. To ensure that rule Eq-frame-ded will be applicable each time we are in such a situation, it is important to work by increasing support. Indeed, by definition of constraint system, we know that the variable x will appear in a deducibility constraint of support less than i. Putting deducibility constraints of support less than i in pre-solved form allows us to ensure that there exists $X, j \vdash^? x$ with $j < i$, and thus Eq-frame-ded is applicable.

In order to satisfy some necessary properties, when $\textsc{Dest}(\tilde{p})$ or $\textsc{Eq-frame-ded}(\tilde{p})$ is applied on one row of the matrix, we will apply the same rule with similar parameter on each row of the matrix. More specifically,

- if $\textsc{Dest}(\xi, \ell \to r, s)$ is applied on a row $(\mathcal{S}, \mathcal{S}')$ of $(\mathcal{M}, \mathcal{M}')$ where (ξ, i) (with $i \leq s$) belongs to the structure of the constraint systems in $(\mathcal{S}, \mathcal{S}')$, then for each row $(\mathcal{T}, \mathcal{T}')$ of $(\mathcal{M}, \mathcal{M}')$ where there exists ξ' such that (ξ', i) belongs to the structure of the constraint systems in $(\mathcal{T}, \mathcal{T}')$ and $\mathsf{path}(\xi') = \mathsf{path}(\xi)$, we also apply $\textsc{Dest}(\xi', \ell \to r, s)$ on $(\mathcal{T}, \mathcal{T}')$.
- if $\textsc{Eq-frame-ded}(\xi, X)$ is applied on a row $(\mathcal{S}, \mathcal{S}')$ of $(\mathcal{M}, \mathcal{M}')$ where (ξ, i) belongs to the structure of the constraint systems in $(\mathcal{S}, \mathcal{S}')$, then for each row $(\mathcal{T}, \mathcal{T}')$ of $(\mathcal{M}, \mathcal{M}')$ where there exist ξ' such that (ξ', i) belongs to the structure of the constraint systems in $(\mathcal{T}, \mathcal{T}')$ and $\mathsf{path}(\xi') = \mathsf{path}(\xi)$, we apply $\textsc{Eq-frame-ded}(\xi', X)$ on $(\mathcal{T}, \mathcal{T}')$.

At the end of Step a, the frame of any constraint system is fixed for the support s. The existing frame elements (for support s) could be further instantiated, but no frame element will be added (for this support).

To avoid the non-terminating behaviour mentioned in Example 39, we break the symmetry between the different components. The idea is to focus on one column of the matrix and to reduce the constraint systems until reaching "pre-solved form" (distinct variables on the right-hand sides of the deducibility constraints), and then move to the next column of the matrix.

Example 40. *Going back to Example 39, and assuming that* $\Phi = \{ax_1, 1 \rhd a;\ ax_2, 2 \rhd b\}$*, we can first observe that there is nothing to do regarding Step a. The idea will be to apply* $\textsc{Cons}(X, \mathsf{senc})$ *as in Example 39, but then we will be forced to work on the constraint system* $\mathcal{C}_1$*. We can apply* $\textsc{Eq-ded-ded}(Y, X_1)$ *yielding (on the left branch) the pair* $(\mathcal{C}_{11}, \mathcal{C}'_{11})$ *where:*

$$\mathcal{C}_{11} = \left\{ \begin{array}{c} \Phi;\ X_1, 1 \vdash^? x_1;\ X_2, 2 \vdash^? x_2 \\ X =^? \mathsf{senc}(X_1, X_2) \wedge Y =^? X_1 \end{array} \right.$$

and $\mathcal{C}'_{11} = \bot$*. Indeed, the equality* $z_1 =^? \mathsf{senc}(\mathsf{senc}(z_1, z_2), y_2)$ *can not be satisfied.*

More formally, we have a cycle of three different steps. The parameter of this cycle is the index of the column on which we are currently working. Each of this cycle alternates Step b and Step c, and then ends with Step d.

Steps b and c: dealing with internal deducibility constraints. The purpose of this cycle (Steps b and c) is to deal with internal deducibility constraints (of support s), *i.e.,* the constraints of the form $X, s \vdash^? u$ with $X \notin S_2$. During Step b, the idea is to put internal deducibility constraints in "pre-solved" form, whereas during Step c, the main goal is to remove them. At the end of Step c, all the internal deducibility constraints would have disappeared.

Step b. We apply the internal applications of the rules Eq-ded-ded, Eq-frame-frame, Cons, Axiom, and Ded-st with support less than s, as long as possible. To be applied on *e.g.,* the i^{th} row, the application of the rule has to correspond to a strong application w.r.t. the constraint system located at the i^{th} row and k^{th} column.

Step c. Given a constraint system $\mathcal{C} = (S_1; S_2; \Phi; D; E; E_\Pi; ND; \mathsf{NoUse})$, we consider the set $\mathsf{X}_\mathcal{C}$ defined as follows:

$$\mathsf{X}_\mathcal{C} = \{x \in \mathcal{X}^1 \mid (Y, j \vdash^? x) \in D, \text{ and } Y \notin S_2\}$$

The purpose of this set is to contain all the first-order variables that occur on the right-hand side of an internal deducibility constraint. We apply by order of preference:

1. The internal rule Eq-ded-ded(X, Y) with $X \notin S_2$ when the rule is strongly applicable on one constraint system of the k^{th} column.
2. The external rule Cons(X, f) when a variable in $\mathsf{X}_\mathcal{C}$ occurs in the deducibility constraint $X, i \vdash^? u$. This has again to correspond to a strong application.
3. The external rule Axiom(X, path) on $X, i \vdash^? u$ if this correspond to a strong application and i is minimal.

Intuitively, the purpose of Step c is to discard the internal deducibility constraints using the rule Eq-ded-ded. However, when this is not possible (*e.g.,* because the variable that occurs on the right-hand side of the internal constraint does not appear as a right member of an external deducibility constraint), we will try break the term u that contains such a variable using the rule Cons with the hope to be able to apply Eq-ded-ded once the variable will appear at the root position. Once this is done, and if an application of Eq-ded-ded is still not possible, we will use the rule Axiom to instantiate some variables. Doing this at the end allows us to ensure that the variables that will be introduced during the replacement will be "smaller" (*i.e.,* the deducibility constraints that introduce each of these variables have a support smaller than the variables that are removed thanks to the Axiom rule).

Step d: dealing with external deducibility constraints. Now, we have to put the external deducibility constraints in "pre-solved" form. For this, we apply the external application of the rules Eq-ded-ded, Cons and Axiom as long as they are strongly applicable on the constraint system $\mathcal{M}_{i,k}$ (or $\mathcal{M}_{i,k-n}$ when $k > n$) by increasing order on the index i of the row. For instance, if $\text{Rule}_1(\tilde{p}_1)$ is strongly applicable on $\mathcal{M}_{i_1,k}$, $\text{Rule}_2(\tilde{p}_2)$ is strongly applicable on $\mathcal{M}_{i_2,k}$, and $i_1 \leq i_2$ then we apply the rule $\text{Rule}_1(\tilde{p}_1)$ on $(\mathcal{M}, \mathcal{M}')$.

Step e: solving non-deducibility constraints. This last step consists of solving the non-deducibility constraints that occur in the matrices. This is done by replacing some constraint systems with $\bot$. Intuitively, we only keep the constraint systems that have a frame which is "maximal" (*i.e.,* a frame which contains a maximal number of elements).

Formally, for each constraint system $\mathcal{C}$ in the matrix (with its associated frame Φ), if there exists a constraint system $\mathcal{C}'$ (with its associated frame Φ') in the same column as $\mathcal{C}$, a recipe ξ, such that $(\xi, s \rhd u) \in \Phi'$ for some u, whereas Φ does not have such an element – *i.e.,* for all $(\xi', s \rhd v) \in \Phi$, we have that $\mathsf{path}(\xi) \neq \mathsf{path}(\xi')$ – then we replace the constraint system $\mathcal{C}$ in the matrix by $\bot$.

The fact that $\mathcal{C}$ does not contain a frame element for $\mathsf{path}(\xi)$ means that $\mathcal{C}$ contains some non-deducibility constraints instead. However, since $\mathcal{C}'$ is in pre-solved form, we know that the deducibility constraints introduced by the DEST rule have been solved, and thus the non-deducibility constraints in $\mathcal{C}'$ can not be satisfied. During Step e, each constraint system that is replaced by $\bot$ does not have a solution due to the non-deducibility constraints. The same applies to solve the non-deducibility constraints introduced by the rule DED-ST. We illustrate this through an example.

Example 41. *Consider the constraint system $\mathcal{C}$ presented in Example 33 as well as the constraint system $\mathcal{C}'$ made of the deducibility constraint $X, 2 \vdash^? \mathsf{senc}(a, a)$ and the frame $\Phi' = \{ax_1, 1 \rhd a;\ ax_2, 2 \rhd b\}$. We consider the matrices $\mathcal{M} = [\mathcal{C}]$ and $\mathcal{M}' = [\mathcal{C}']$. In Example 33, we have seen that applying the rule $\text{DEST}(ax_2, \mathsf{sdec}(\mathsf{senc}(x, y), y) \to x, 2)$ on $\mathcal{C}$ yields $\mathcal{C}_1$ and $\mathcal{C}_2$. The application of this rule on $\mathcal{C}'$ yields after normalisation the constraint system $\bot$ and the following constraint system $\mathcal{C}'_2$:*

$$\mathcal{C}'_2 = \left\{ \begin{array}{l} \Phi';\ \ X, 2 \vdash^? \mathsf{senc}(a, a) \\ \forall x_1, x_2.[\mathsf{senc}(x_1, x_2) \neq^? b \vee 2 \not\vdash^? x_2] \end{array} \right.$$

Thus the application of the rule $\text{DEST}(ax_2, \mathsf{sdec}(\mathsf{senc}(x, y), y) \to x, 2)$ on $\mathcal{M}$ and $\mathcal{M}'$ yields the pair of matrices $(\mathcal{M}_1, \mathcal{M}'_1)$:

$$\mathcal{M}_1 = \left[\begin{array}{c} \mathcal{C}_1 \\ \mathcal{C}_2 \end{array} \right] \qquad \mathcal{M}'_1 = \left[\begin{array}{c} \bot \\ \mathcal{C}'_2 \end{array} \right]$$

Then, we may apply the rule $\text{AXIOM}(Y, ax_1)$ internally (on the first row of the matrix), and we obtain:

$$\mathcal{M}_2 = \left[\begin{array}{c} \mathcal{C}_3 \\ \mathcal{C}_4 \\ \mathcal{C}_2 \end{array} \right] \qquad \mathcal{M}'_2 = \left[\begin{array}{c} \bot \\ \bot \\ \mathcal{C}'_2 \end{array} \right]$$

On the constraint system $\mathcal{C}_4$, the successive applications of $\text{CONS}(Y, \mathsf{f})$ and $\text{AXIOM}(Y, \mathsf{path})$ for any f and path will yield after normalisation the constraint system $\bot$. All these rules are internal, and thus we obtain the following pair of matrices:

$$\mathcal{M}_3 = \left[\begin{array}{c} \mathcal{C}_3 \\ \bot \\ \dots \\ \bot \\ \mathcal{C}_2 \end{array} \right] \qquad \mathcal{M}'_3 = \left[\begin{array}{c} \bot \\ \bot \\ \dots \\ \bot \\ \mathcal{C}'_2 \end{array} \right]$$

Then, the successive applications of the rules CONS and AXIOM on $\mathcal{M}_3$ and $\mathcal{M}'_3$ (to solve the remaining deducibility constraints in $\mathcal{C}_3$, $\mathcal{C}_2$, and $\mathcal{C}'_2$) will yield in particular a leaf $(\mathcal{M}_4, \mathcal{M}'_4)$ where:

$$\mathcal{M}_4 = \left[\begin{array}{c} \mathcal{C}_5 \\ \bot \\ \dots \\ \bot \\ \mathcal{C}_6 \end{array} \right] \qquad \mathcal{M}'_4 = \left[\begin{array}{c} \bot \\ \bot \\ \dots \\ \bot \\ \mathcal{C}'_6 \end{array} \right]$$

where the constraint systems $\mathcal{C}_5$, $\mathcal{C}_6$ and $\mathcal{C}'_6$ are as follows:

$$\mathcal{C}_5 = \left\{ \begin{array}{l} \Phi,\ \mathsf{sdec}(ax_2, ax_1), 2 \rhd b \\ X =^? \mathsf{senc}(ax_1, ax_1) \\ Y =^? ax_1 \end{array} \right. \qquad \mathcal{C}_6 = \left\{ \begin{array}{l} \Phi;\ \ X =^? \mathsf{senc}(ax_1, ax_1) \\ \forall x_1, x_2.[\mathsf{senc}(x_1, x_2) \neq^? \mathsf{senc}(b, a) \vee 2 \not\vdash^? x_2] \end{array} \right.$$

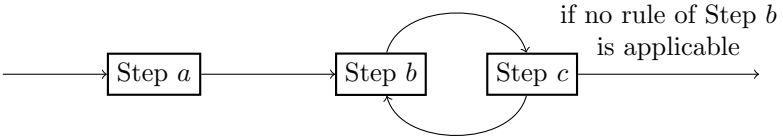
$$\mathcal{C}'_6 = \left\{ \begin{array}{l} \Phi';\ \ X =^? \mathsf{senc}(ax_1, ax_1) \\ \forall x_1, x_2.[\mathsf{senc}(x_1, x_2) \neq^? b \vee 2 \not\vdash^? x_2] \end{array} \right.$$

Now, following the transformation explained above, the system $\mathcal{C}_6$ will be replaced by $\bot$. Indeed, there exists $\mathcal{C}_5$ in the same column as $\mathcal{C}_6$ that contains the frame element $\mathsf{sdec}(ax_2, ax_1), 2 \rhd b$, and for which there is no counterpart in $\mathcal{C}_6$. Instead, in $\mathcal{C}_6$, we have a non-deducibility constraint that is actually unsatisfiable.

Indeed, the existence of a solution for the constraint system $\mathcal{C}_5$ implies that the recipe $\mathsf{sdec}(ax_2, ax_1)$ yields a message, thus ax_2 is a ciphertext whose key is deducible at stage 2, and so the non-deducibility constraint of $\mathcal{C}_6$ can not be satisfied.

4.2. Taking care of disequations

After the first phase of our strategy $\mathcal{S}$, the rules DEST, EQ-FRAME-DED, EQ-FRAME-FRAME and DED-ST will never be applicable anymore for any parameter. Thus, the only rules that can be applied during the second phase are CONS, AXIOM and EQ-DED-DED. Furthermore these rules will always be applied as external rules. As already explained, the purpose of this phase is to take care of the disequations. For this, we need to match them, and ensure that the same disequations occur in each constraint system. As depicted below, this second phase is made up of three steps.



Step a: getting rid of universally quantified variables. In order to be able to match the disequations, we have to get rid of variables that are universally quantified. For this, we apply the rules $\text{CONS}(X, \mathsf{f})$ and $\text{AXIOM}(X, \mathsf{path})$ as long as, for at least one constraint system occurring in the matrix, this corresponds to a strong application of the rule or there exists an atomic statement $u \neq^? w$ in E (where u is such that $X, i \vdash^? u$ – actually at this stage u will be a variable) for which there exists a variable $y \in vars^1(w)$ which is universally quantified. At the end of this Step a, variables that are universally quantified would have been removed.

Example 42. *Let $\Phi^+ = \{ax_1, 1 \rhd a;\ ax_2, 2 \rhd \langle b, a\rangle;\ \mathsf{proj}_1(ax_2), 2 \rhd b;\ \mathsf{proj}_2(ax_2) \rhd a\}$, and consider the following constraint system:*

$$\mathcal{C} = \left\{ \ \Phi^+;\ \ Y, 1 \vdash^? y;\ \ \forall x.\ y \neq^? \langle x, a\rangle \right.$$

For sake of simplicity, we will assume that $\langle\ \rangle$ is the only constructor symbol. In order to get rid of the variable x, the strategy will tell us to apply $\text{CONS}(Y, \langle\ \rangle)$. This gives us:

$$\mathcal{C}_1 = \left\{ \begin{array}{l} \Phi^+;\ Y_1, 1 \vdash^? y_1;\ Y_2, 1 \vdash^? y_2 \\ \forall x.\ y \neq^? \langle x, a\rangle \\ y =^? \langle y_1, y_2\rangle;\ Y =^? \langle Y_1, Y_2\rangle \end{array} \right. \qquad \mathcal{C}_2 = \left\{ \begin{array}{l} \Phi^+;\ Y, 1 \vdash^? y \\ \forall x.\ y \neq^? \langle x, a\rangle \\ \mathsf{root}(Y) \neq^? \langle\ \rangle \end{array} \right.$$

Using our simplification rules, the first system will be simplified as follows:

$$\mathcal{C}_1{\downarrow} = \left\{ \begin{array}{l} \Phi^+;\ Y_1, 1 \vdash^? y_1;\ Y_2, 1 \vdash^? y_2 \\ y_2 \neq^? a \\ y =^? \langle y_1, y_2 \rangle;\ Y =^? \langle Y_1, Y_2 \rangle \end{array} \right.$$

Note that $\mathcal{C}_1{\downarrow}$ does not contain any quantified variable anymore. Considering the constraint system $\mathcal{C}_2$, in order to get rid of the variable x, we can for instance apply the rule Axiom(Y, ax_1). *We obtain (after some simplifications):*

$$\mathcal{C}_{21} = \left\{ \ \Phi^+;\ Y = ax_1;\ y = a \right. \qquad \mathcal{C}_{22} = \left\{ \begin{array}{l} \Phi^+; Y, 1 \vdash^? y;\ \forall x.\ y \neq^? \langle x, a \rangle \\ \mathsf{root}(Y) \neq^? \langle\ \rangle \wedge Y \neq^? ax_1 \end{array} \right.$$

The system $\mathcal{C}_{21}$ does not contain any quantified variable anymore. We can pursue like this using Cons(Y, ax_2) *on $\mathcal{C}_{22}$. We obtain (after some simplifications) $\mathcal{C}_{221} = \bot$ and*

$$\mathcal{C}_{222} = \left\{ \begin{array}{l} \Phi^+; Y, 1 \vdash^? y;\ \forall x.\ y \neq^? \langle x, a \rangle \\ \mathsf{root}(Y) \neq^? \langle\ \rangle \wedge Y \neq^? ax_1 \wedge Y \neq^? ax_2 \end{array} \right.$$

We can continue with Cons$(Y, \mathsf{proj}_1(ax_2))$ *and* Cons$(Y, \mathsf{proj}_2(ax_2))$. *The resulting systems on the left branches will not contain any disequations (they are actually trivially satisfied) whereas on the right branch the constraint system will be turned to $\bot$ following the simplification rule given in Figure 4. Thus, at the end, all the quantified variables have been removed.*

Steps b and c: matching disequations. To ensure that we will reach a solved form in which all the disequations are matched, the rule Eq-ded-ded plays an important role. The rule Eq-ded-ded allows one to "externalise" the disjunctions, splitting disjunctive disequations, each of which will appear in different matrices. However, it may happen that the rule Eq-ded-ded can not be applied to get rid of a particular disequation. In such a situation, we will first use the rules Cons and Axiom to simplify it, and allow eventually the application of the rule Eq-ded-ded. The only rules that can be applied during these two steps (b and c) are Cons, Axiom and Eq-ded-ded. However, as illustrated by Example 43, to ensure termination we can not apply them in any order.

Example 43. *We consider a constraint system in "pre-solved" form such that:*

$$E = [x_1 \neq^? y \vee x_2 \neq^? a] \wedge y \neq^? \langle \langle x_1, x_2 \rangle, b \rangle.$$

For sake of simplicity, we do not described Φ and D. We simply assume that the frame contains the terms a and b. First, we apply Axiom *on x_2 (with a), on one branch we will obtain $x_1 \neq^? y \wedge y \neq^? \langle \langle x_1, a \rangle, b \rangle$. Then applying* Cons *twice, we obtain $x_1 \neq^? \langle \langle y_1, y_2 \rangle, y_3 \rangle \wedge [y_1 \neq^? x_1 \vee y_2 \neq^? a \vee y_3 \neq^? b]$. Lastly, applying* Axiom *on y_3 (with b), we obtain:*

$$x_1 \neq^? \langle \langle y_1, y_2 \rangle, b \rangle \wedge [y_1 \neq^? x_1 \vee y_2 \neq^? a]$$

getting back to the original set of disequations.

To avoid such a situation, the main idea is to postpone the use of the Axiom rule. We apply as long as we can the rules Cons and Eq-ded-ded, and only after that we can move to Step c and apply the Axiom rule.

Example 44. *Going back to Example 43 and following our strategy, we will first apply* Eq-ded-ded *to deal with the disequation* $x_1 \neq^? y$. *On the left branch,* i.e., *assuming the equality* $x_1 = y$ *is satisfied, the disequation* $y \neq^? \langle\langle x_1, x_2\rangle, b\rangle$ *becomes* $y \neq^? \langle\langle y, x_2\rangle, b\rangle$, *and disappears since it is trivially satisfied. Hence, we obtain two constraint systems that respectively contains:*

$$x_2 \neq^? a \qquad\qquad x_1 \neq^? y \wedge y \neq^? \langle\langle x_1, x_2\rangle, b\rangle$$

Then, on the resulting system on the left branch, we have no choice, we have to apply an Axiom *rule. On the right, we pursue using the* Cons *rule on* y *allowing us to simplify (on the left branch) a bit more the disequations – the name* b *is now at the root position:*

$$x_1 \neq^? \langle y_1, y_2\rangle \wedge [y_1 \neq^? \langle x_1, x_2\rangle \vee y_2 \neq^? b]$$

Then, we may apply Eq-ded-ded *to deal with* $y_1 \neq^? \langle x_1, x_2\rangle$. *We get*

$$y_2 \neq^? b \qquad\qquad x_1 \neq^? \langle y_1, y_2\rangle \wedge y_1 \neq^? \langle x_1, x_2\rangle$$

Again, on the left, the disequation $x_1 \neq^? \langle y_1, y_2\rangle$ *has disappeared since after replacing* y_1 *with* $\langle x_1, x_2\rangle$, *it is trivially satisfied. On the right, the disequations now contain free variables and public function symbols and applying* Eq-ded-ded *will be useless. On the left, we now have to apply an instance of the* Axiom *rule. Thus, this strategy avoids the non termination issue mentioned in the previous example.*

Step b. During this step, we apply as long as we can the rules Cons and Eq-ded-ded. However, as illustrated with the following example, due to the fact that we have to apply simultaneously our transformation rules on several constraint systems, we can get some termination troubles.

Example 45. *Consider the pair* $(\mathcal{C}, \mathcal{C}')$ *of sets of initial constraint systems given below (each set is actually reduced to a singleton):*

$$\mathcal{C} = \left\{ \begin{array}{l} ax_1, 1 \rhd a \\ X, 1 \vdash^? x;\ Y, 1 \vdash^? y \\ x \neq^? \mathsf{h}(y) \wedge x \neq^? y \end{array} \right. \qquad \mathcal{C}' = \left\{ \begin{array}{l} ax_1, 1 \rhd a \\ X, 1 \vdash^? x;\ Y, 1 \vdash^? y \end{array} \right.$$

We could apply Cons(X, h) *replacing* x *with* $\mathsf{h}(x')$ *to simplify the disequation* $x \neq^? \mathsf{h}(y)$ *into* $x' \neq^? y$. *However, this operation will transform the other disequation, namely* $x \neq^? y$ *into* $\mathsf{h}(x') \neq^? y$. *More precisely, this gives (on the left branch):*

$$\mathcal{C}_0 = \left\{ \begin{array}{l} ax_1, 1 \rhd a \\ X', 1 \vdash^? x';\ Y, 1 \vdash^? y \\ x' \neq^? y \wedge \mathsf{h}(x') \neq^? y \\ X =^? \mathsf{h}(X') \end{array} \right. \qquad \mathcal{C}'_0 = \left\{ \begin{array}{l} ax_1, 1 \rhd a \\ X', 1 \vdash^? x';\ Y, 1 \vdash^? y \\ X =^? \mathsf{h}(X') \end{array} \right.$$

This pair $(\mathcal{C}_0, \mathcal{C}'_0)$ *is made up of two systems on which the* Cons *rule is again applicable, and we can go on forever with* Cons.

The main idea is to favour the application of Eq-ded-ded. However, given a particular disequation, necessarily of the form $x \neq^? u$ at this stage, it may happen that Eq-ded-ded can not be applied for two main reasons:

1. either a name occurred in the disequation, *i.e.,* u contains a name;

2. or a "faulty" variable occurred in the disequation, *i.e.,* u contains a variable whose support is greater than the support of x.

In both cases, the idea is to apply the Cons rule to bring the name or the "faulty" variable at the root position. Thus, we authorise the application of the rule $\textsc{Cons}(X, \mathsf{f})$ on $X, i_0 \vdash^? t$ during Step b (actually t is a variable at this stage) if there exists a constraint system $\mathcal{C}$ on which the rule $\textsc{Cons}(X, \mathsf{f})$ is not useless, and such that:

1. either $\textsc{Cons}(X, \mathsf{f})$ is strongly applicable on $\mathcal{C}$ (at this stage, since t is a variable, this means that there exists an atomic statement $(\mathsf{root}(X) \neq \mathsf{g})$ in $E_\Pi(\mathcal{C})$ such that $\mathsf{g} \in \mathcal{F}_c$ and $\mathsf{g} \neq \mathsf{f}$);
2. or there is a disequation of the form $t \neq u$ with $\mathsf{root}(u) = \mathsf{f}$, and u contains a name or a "faulty" variable, *i.e.,* $i_0 < \max\{i \mid x \in vars^1(u) \text{ and } (X, i \vdash^? x) \in D(\mathcal{C})\}$.

Example 46. *Going back to Example 45. Applying* $\textsc{Cons}(X, \mathsf{h})$ *is now forbidden. Instead, we may apply* $\textsc{Eq-ded-ded}(X, \mathsf{h}(Y))$. *This leads us to the pairs* $(\bot; \mathcal{C}'_1)$ *and* $(\mathcal{C}; \mathcal{C}'_2)$ *where:*

$$\mathcal{C}'_1 = \left\{ \begin{array}{l} ax_1, 1 \rhd a \\ Y, 1 \vdash^? y \\ x =^? \mathsf{h}(y);\ X =^? \mathsf{h}(Y) \end{array} \right. \qquad \mathcal{C}'_2 = \left\{ \begin{array}{l} ax_1, 1 \rhd a \\ X, 1 \vdash^? x;\ Y, 1 \vdash^? y \\ x \neq^? \mathsf{h}(y) \end{array} \right.$$

From the pair $(\bot; \mathcal{C}'_1)$ *we will conclude that symbolic equivalence does not hold. Regarding the pair* $(\mathcal{C}; \mathcal{C}'_2)$*, we can go on and reach a solved form by applying* $\textsc{Eq-ded-ded}(X, Y)$ *obtaining again two pairs of constraint systems. The first one will be of the form* $(\bot; \mathcal{C}'_3)$ *and the second one will contain two systems in which all the disequations are matched.*

We have shown that applying the rules Cons (under the additional conditions mentioned above) and Eq-ded-ded in any order will terminate (for Step b). However, to ensure termination of the cycle made of Step b and Step c, we have to work on a disequation which is *maximal*, *i.e.* one that involves variables whose supports are maximal. The necessity of this extra condition and its formal definition will be discussed later on (actually after the description of Step c).

Step c. In this last step, we apply the rule $\textsc{Axiom}(X, \mathsf{path})$ as long as possible, *i.e.,* as long as there is at least one constraint system $\mathcal{C}$ in the pair of matrices on which $\textsc{Axiom}(X, \mathsf{path})$ is strongly applicable on it. Note that, at this stage, the term t in the constraint $X, i \vdash^? t$ is necessarily a variable. Thus a strong application means that $(\mathsf{root}(X) \neq \mathsf{f}) \in E_\Pi(\mathcal{C})$ for some f. When no more instance of the Axiom rule can be applied, we go back to Step b. It is quite easy to see that Step c alone will terminate. The number of variables decreases on the left branch, and at some point all the possible instances of the Axiom rule would have been considered.

However, to ensure termination of the cycle made of Step b and Step c, we have to restrict the order on which the rules Cons and Eq-ded-ded are applied during Step b. We prove termination of this cycle under the hypothesis that we always work on the maximal disequation. The measure associated to a disequation $u \neq^? v$ occurring in a constraint system $\mathcal{C}$ is a pair of integers defined by $\mathcal{L}^1_{\mathcal{C}}(u \neq^? v) = (\mathcal{L}^1_{\mathcal{C}}(u); \mathcal{L}^1_{\mathcal{C}}(v))$ where:

$$\mathcal{L}^1_{\mathcal{C}}(u) = max\left(\{\, i \mid (X, i \vdash^? x) \in D(\mathcal{C}) \text{ and } x \in vars(u)\} \cup \{0\}\right).$$

We use a "lexicographic" order to compare those pairs, and to decide on which disequation we will work. We have that $(i_1, i_2) >_{\mathsf{lex}} (j_1, j_2)$ if

- either $max(i_1, i_2) > max(j_1, j_2)$;
- or $max(i_1, i_2) = max(j_1, j_2)$ and $min(i_1, i_2) > min(j_1, j_2)$

Note that, using this order, we have that $\mathcal{L}^1_{\mathcal{C}}(u \neq^? v) = \mathcal{L}^1_{\mathcal{C}}(v \neq^? u)$ for any terms u and v.

Example 47. *Let $(\mathcal{C}, \mathcal{C}')$ be two constraint systems obtained at the end of Phase 2/ Step a that only differ by the content of their frame. For sake of simplicity, we also assume that f is a function symbol of arity 2 and the only one that we consider here. (this symbol could be mimicked in our setting using h and $\langle\ ,\ \rangle$). Moreover, regarding disequations, we assume that they contain:*

$$x \neq \mathsf{f}(y, z) \qquad x \neq z \qquad \mathsf{root}(Y) \neq \mathsf{f}.$$

Note that Cons *and* Eq-ded-ded *can not be applied, but due to the presence of $\mathsf{root}(Y) \neq \mathsf{f}$, the rule* Axiom *is strongly applicable on Y. Consider the left branch during such an application, and assume that such an application will instantiate y with $\mathsf{f}(\mathsf{f}(a, a), w)$ on $\mathcal{C}$, and y with $\mathsf{f}(w, \mathsf{f}(a, a))$ on $\mathcal{C}'$. Let $(\mathcal{C}_1, \mathcal{C}'_1)$ be the resulting pair. Such a scenario is possible since even if $\mathcal{C}$ and $\mathcal{C}'$ have the same structure, they may differ on the content of their frame. The constraint systems $\mathcal{C}_1$ and $\mathcal{C}'_1$ will now have different sets of disequations. In particular, we have that*

$$\mathcal{C}_1 = \left\{ \begin{array}{c} \dots \\ x \neq^? \mathsf{f}(\mathsf{f}(\mathsf{f}(a, a), w), z) \\ x \neq^? z \end{array} \right. \qquad \mathcal{C}_1 = \left\{ \begin{array}{c} \dots \\ x \neq^? \mathsf{f}(\mathsf{f}(w, \mathsf{f}(a, a)), z) \\ x \neq^? z \end{array} \right.$$

Here a is a name whereas w is variable, and we necessarily have that $W, i_w \vdash^? w$ (but also $Y, j_y \vdash^? y$) occurs in both $\mathcal{C}$ and $\mathcal{C}'$, and we have also that $i_w < i_y$. Now, on this branch, we have nothing to do regarding Step c, and we go back to Step b. We have still nothing to do regarding the second disequation of each constraint system, but we can apply the Cons *rule on the first one. Consider the left branch during such an application of* Cons(X, f)*, we get $(\mathcal{C}_{11}, \mathcal{C}'_{11})$ where:*

$$\mathcal{C}_{11} = \left\{ \begin{array}{c} \dots \\ x_1 \neq^? \mathsf{f}(\mathsf{f}(a, a), w) \vee x_2 \neq^? z \\ \mathsf{f}(x_1, x_2) \neq^? z \end{array} \right. \qquad \mathcal{C}'_{11} = \left\{ \begin{array}{c} \dots \\ x_1 \neq^? \mathsf{f}(w, \mathsf{f}(a, a)) \vee x_2 \neq^? z \\ \mathsf{f}(x_1, x_2) \neq^? z \end{array} \right.$$

Now, depending on the values of i_w and i_z, we may have a choice. We can either apply Cons *to simplify $x_1 \neq^? \mathsf{f}(\mathsf{f}(a, a), w)$ (and $x_1 \neq^? \mathsf{f}(w, \mathsf{f}(a, a))$) or apply* Eq-ded-ded *on $x_2 \neq^? z$. We consider here the first option (to respect maximality, this is only possible if $i_w \geq i_z$), and we get (on the left branch) the pair $(\mathcal{C}_{111}, \mathcal{C}'_{111})$ where:*

$$\mathcal{C}_{111} = \left\{ \begin{array}{c} \dots \\ x_{11} \neq^? \mathsf{f}(a, a) \vee x_{12} \neq^? w \vee x_2 \neq^? z \\ \mathsf{f}(\mathsf{f}(x_{11}, x_{12}), x_2) \neq^? z \end{array} \right. \quad \mathcal{C}'_{111} = \left\{ \begin{array}{c} \dots \\ x_{11} \neq^? w \vee x_{12} \neq^? \mathsf{f}(a, a) \vee x_2 \neq^? z \\ \mathsf{f}(\mathsf{f}(x_{11}, x_{12}), x_2) \neq^? z \end{array} \right.$$

Now, we may still have some choice, but it is not possible for instance to consider an application of the Cons *rule on* $x_{11} \neq \mathsf{f}(a,a)$. *Indeed,* $\mathcal{L}^1_{\mathcal{C}_{111}}(x_{11} \neq^? \mathsf{f}(a,a))$ *is not maximal since* $\mathcal{L}^1_{\mathcal{C}}(\mathsf{f}(a,a)) = 0$ *in any constraint system* $\mathcal{C}$. *This remark is important to avoid non termination. Indeed, applying* $\textsc{Cons}(X_{11}, \mathsf{f})$ *would allow us to add* $\mathsf{root}(X_{11}) \neq \mathsf{f}$ *on the constraint systems on the right branch, and then applying* Eq-ded-ded *on* $x_{12} \neq^? w$, *and then on* $x_2 \neq^? z$, *and considering the pair of constraint systems obtained along the right branch, we will eventually obtain a pair of constraint systems that will contain:*

$$\mathcal{C}_{\mathsf{right}} = \left\{ \begin{array}{c} \cdots \\ x_{12} \neq^? w \\ x_2 \neq^? z \\ \mathsf{f}(\mathsf{f}(x_{11}, x_{12}), x_2) \neq^? z \\ \mathsf{root}(X_{12}) \neq \mathsf{f} \end{array} \right. \quad \mathcal{C}'_{\mathsf{right}} = \left\{ \begin{array}{c} \cdots \\ x_{12} \neq^? w \\ x_2 \neq^? z \\ \mathsf{f}(\mathsf{f}(x_{11}, x_{12}), x_2) \neq^? z \\ \mathsf{root}(X_{12}) \neq \mathsf{f} \end{array} \right.$$

Assuming that x, y, *and* z *have the same support,* i.e., $X, i_x \vdash^? x$, $Y, i_y \vdash^? y$ *and* $Z, i_z \vdash^? z$ *are in* $\mathcal{C}$ *and* $\mathcal{C}'$ *with* $i_x = i_y = i_z$, *the situation is quite similar to the pair of constraint systems we consider at the very beginning of this example. We may apply a similar sequence of transformation rules leading to a termination issue. Note however that this sequence does not respect our maximality condition. The application of* $\textsc{Cons}(X_1, \mathsf{f})$ *on* $(\mathcal{C}_{11}, \mathcal{C}'_{11})$ *does not respect our maximality condition. Indeed, by definition of a constraint system, we have that* $i_w < i_y$, *and together with the hypothesis that* $i_x = i_y = i_z$, *this would contradicts the fact that* $i_w \geq i_z$.

Relying on this strategy, we are now able to prove termination of our algorithm.

Theorem 5. *(termination) Applying the transformation rules on a pair of sets of initial constraint systems and following the strategy* $\mathcal{S}$ *always terminates.*

5. Implementation

This decision procedure has been implemented in a tool called APTE. The tool is implemented in Ocaml (around 12 000 lines). APTE is an open source software and is distributed under GNU General Public Licence 3.0. The tool as well as the description of the protocols we have analysed using it are available at:

`http://projects.lsv.ens-cachan.fr/APTE/`.

As expected, APTE checks trace equivalence for processes that use standard primitives (*e.g.,* pairing, signatures, hash functions, symmetric and asymmetric encryptions). We can model in particular conditionals (with non-trivial else branches), private channels, and non-deterministic choices, but we consider processes without replication. In case of failure when establishing trace equivalence, APTE provides a witness of non-equivalence. In terms of protocols, APTE has been used to analyse several protocols among them the private authentication protocol, and some protocols issued from the e-passeport application as described in [33].

Our implementation closely follows the transformation rules that are described along the paper. However, for efficiency reasons, some optimisations have been implemented. In particular, the strategy described in the previous section imposes us to apply the rule

AXIOM on each frame element and the rule CONS for each constructor symbol. Thus, giving the attacker some useless capabilities, *e.g.,* by adding some fresh names in the frame, or considering some additional hash functions, will considerably increase the execution time of our algorithm. To cope with these issues, we adapt the strategy: only the relevant instances of the rule CONS and AXIOM are applied. We manage to obtain a quite efficient algorithm for checking symbolic equivalence between sets of constraint systems. However, the interleaving step, that is required for moving from symbolic equivalence to trace equivalence, is expensive from the computation point of view. Actually, we are faced with the usual interleaving explosion problem. For example, using such an approach, deciding anonymity for one session of the private authentication protocol amounts to solve 15 symbolic equivalences between pairs of sets of constraint systems (each pair containing between 2 and 8 constraint systems). Around 200 symbolic equivalence have to be solved to deal with 2 sessions, and more than 900 when we want to analyse 3 sessions of this protocol. Moreover, it is worth mentioning that the size of the constraint systems but also the number of constraint systems in each set are increasing, and we thus rapidly reach the limit of the tool.

To illustrate this exponential blow up, we report on Table 5 and Table 6 some experiments that we have performed to analyse the private authentication protocol for 1 and 2 sessions respectively. We indicate the number of symbolic traces of each length, and since a given symbolic trace may lead to several constraint systems, we also indicate this number (on the average). For instance, considering symbolic traces of length 6 (*i.e.,* traces made up of 6 input/output actions), there are 4 different symbolic traces of this length. On the average, one such trace leads to 6 constraint systems, and we will have to launch our algorithm 4 times for checking symbolic equivalence between pairs $(\mathcal{S}, \mathcal{S}')$ of sets of constraint systems (each pair containing 6 constraint systems in average). Checking one symbolic equivalence will require the applications of 428 transformations rules (most of the rules are applied internally) and this will be done in less than a few milliseconds.

	# traces	# systems *(in average per trace)*	# rules *(in average per symbolic equivalence)*	int. - ext.	time (s)
1	1	2	6	83% - 17%	0.00
2	1	2	14	86% - 14%	0.00
3	1	2	25	88% - 12%	0.00
4	2	2	41	90% - 10%	0.00
5	2	6	182	93% - 7%	0.00
6	4	6	428	94% - 6%	0.00
7	4	6	1734	95% - 5%	0.01

Figure 5: Results obtained when analysing 1 session of the private authentication protocol.

As indicated in Table 6, analysing two sessions of the private authentication protocol, we reach the limit of our tool. In particular, checking trace equivalence for traces up to length 9 requires us to launch our algorithm for checking symbolic equivalence between pairs of sets of constraint systems more that 90 times. The total time to get an answer is around 1500 seconds but it still remains around one hundred of symbolic equivalences

to check and the underlying sets of constraint systems become very huge, *e.g.,* for traces of length 10, each pair contains 360 constraint systems in average.

	# traces	# systems *(in average per trace)*	# rules *(in average per symbolic equivalence)*	int. - ext.	time (s)
1	1	2	6	83% - 17%	0.00
2	1	2	14	86% - 14%	0.00
3	1	2	25	88% - 12%	0.00
4	2	4	41	90% - 10%	0.00
5	4	12	129	90% - 10%	0.00
6	6	41	793	93% - 7%	0.03
7	12	87	2468	94% - 6%	0.29
8	18	204	13324	96% - 4%	4.67
9	36	280	39292	96% - 4%	40.19
10	54	360	...	...	...
11	54	373	...	...	...

Figure 6: Results obtained when analysing 2 sessions of the private authentication protocol.

The results summarised in Table 5 and 6 correspond to what we obtain when enumerating all the symbolic traces and then applying our procedure for checking symbolic equivalence on each resulting symbolic trace. Since checking trace equivalence requires to consider partial symbolic traces, we managed to optimise the tool by exploiting the result of our algorithm launched on symbolic traces of size n when analysing the symbolic traces of size $n+1$. This avoids us to apply some transformations that have already been applied during the analysis of the traces of size n and push a bit the boundaries of our tool but an analysis of the private authentication protocol for 3 sessions is still out of reach.

6. Conclusion

Trace equivalence is a central notion for expressing privacy-type properties. It has been shown that trace equivalence can be reduced to checking equivalence between sets of constraint systems (see *e.g.,* [14]). This reduction result is very general and holds for arbitrary processes (without replication) and for arbitrary equational theories. In this paper, we present a procedure to automatically check equivalence between sets of constraint systems. Altogether, this gives us an algorithm for checking trace equivalence in the applied pi-calculus. The procedure described in this paper has been implemented and performed well on constraint systems. However, the interleaving step that is required for moving from symbolic equivalence to trace equivalence, is performed in a rather naive way and it appears that this step is expensive from the computation point of view.

To cope with the interleaving problem mentioned above, we would like to propose some optimisations to reduce the number of interleavings that have to be considered, and so the number of equivalence between sets of constraint systems that have to be checked. This problem has already been studied in the context of reachability properties [34]

but seems to be more challenging for trace equivalence (see *e.g.,* for some preliminary results [35]).

Although our procedure is tailored to a fixed set of primitives, it can probably be extended to primitives that are described by subterm convergent rewriting systems. Similarly, adding more tests (such as equal encryption keys or equal lengths) should not be a problem. We would also like to enrich our algorithm to deal with less standard primitives such as blind signatures or trapdoor commitment functions that are crucial in the context of e-voting protocols but do not fall in any existing decidability results. Handling other associative-commutative primitives, such as exclusive-or, or modular exponentiationm, seems to be extremely challenging for the class of protocols that we consider: for the side constraints only (quantified disequalities) there is no quantifier elimination procedure.

Lastly, we would like also to pursue the study of the constraint systems that are generated by our algorithm. The matrices of constraint systems obtained at the end (*i.e.,* on the leaves) enjoy some nice properties (*e.g.,* existence of a "constructor" solution, one-to-one equivalence between constraint systems that occur on the same row, ...). We think that these properties can be further exploited to decide some more fine grained notion of equivalence. Actually, relying on these nice properties, it has already been shown that the notion of *length trace equivalence*, a notion of equivalence that takes into account the length of messages [22], is decidable (relying on the algorithm presented in this paper).

References

[1] V. Cortier, S. Kremer (Eds.), Formal Models and Techniques for Analyzing Security Protocols, Vol. 5 of Cryptology and Information Security Series, IOS Press, 2011.

[2] V. Cortier, S. Kremer, B. Warinschi, A survey of symbolic methods in computational analysis of cryptographic systems, Journal of Automated Reasoning 46 (3-4) (2010) 225–259.

[3] M. Abadi, C. Fournet, Mobile values, new names, and secure communication, in: Proc. 28th Symposium on Principles of Programming Languages (POPL'01), ACM Press, 2001, pp. 104–115.

[4] A. Armando, R. Carbone, L. Compagna, J. Cuéllar, M. L. Tobarra, Formal analysis of SAML 2.0 web browser single sign-on: breaking the SAML-based single sign-on for Google apps, in: Proc. 6th ACM Workshop on Formal Methods in Security Engineering (FMSE'08), ACM, 2008, pp. 1–10.

[5] P. Ryan, S. Schneider, M. Goldsmith, G. Lowe, B. Roscoe, The Modelling and Analysis of Security Protocols, Addison Wesley, 2000.

[6] B. Blanchet, An Efficient Cryptographic Protocol Verifier Based on Prolog Rules, in: Proc. 14th Computer Security Foundations Workshop (CSFW'01), IEEE Comp. Soc. Press, 2001, pp. 82–96.

[7] C. Cremers, The Scyther Tool: Verification, falsification, and analysis of security protocols, in: Proc. 20th International Conference on Computer Aided Verification (CAV'08), Vol. 5123/2008 of LNCS, Springer, 2008, pp. 414–418.

[8] A. Armando, et al., The AVISPA Tool for the automated validation of internet security protocols and applications, in: Proc. 17th International Conference on Computer Aided Verification (CAV'05), Vol. 3576 of LNCS, Springer, 2005, pp. 281–285.

[9] H. Hüttel, Deciding framed bisimulation, in: Proc. 4th International Workshop on Verification of Infinite State Systems INFINITY'02, 2002, pp. 1–20.

[10] B. Blanchet, M. Abadi, C. Fournet, Automated verification of selected equivalences for security protocols, Journal of Logic and Algebraic Programming 75 (1) (2008) 3–51.

[11] S. Meier, B. Schmidt, C. Cremers, D. Basin, The tamarin prover for the symbolic analysis of security protocols, in: Proc. International Conference on Computer Aided Verification (CAV'13), Springer, 2013, pp. 696–701.

[12] D. Basin, J. Dreier, R. Sasse, Automated symbolic proofs of observational equivalence, in: Proc. 22nd Conference on Computer and Communications Security (CCS'15), ACM, 2015, pp. 1144–1155.

[13] V. Cortier, S. Delaune, A method for proving observational equivalence, in: Proc. of 22nd Computer Security Foundations Symposium (CSF'09), IEEE Comp. Soc. Press, 2009, pp. 266–276.

[14] V. Cheval, V. Cortier, S. Delaune, Deciding equivalence-based properties using constraint solving, Theoretical Computer Science 492 (2013) 1–39.
[15] M. Baudet, Deciding security of protocols against off-line guessing attacks, in: Proc. 12th ACM Conference on Computer and Communications Security (CCS'05), ACM Press, 2005.
[16] Y. Chevalier, M. Rusinowitch, Decidability of symbolic equivalence of derivations, Journal of Automated Reasoning.
[17] A. Tiu, J. E. Dawson, Automating open bisimulation checking for the spi calculus, in: Proc. 23rd IEEE Computer Security Foundations Symposium (CSF'10), IEEE Computer Society Press, 2010, pp. 307–321.
[18] R. Chadha, Ş. Ciobâcă, S. Kremer, Automated verification of equivalence properties of cryptographic protocols, in: Proc. 21th European Symposium on Programming (ESOP'12), Vol. 7211 of LNCS, Springer, 2012, pp. 108–127.
[19] M. Arapinis, T. Chothia, E. Ritter, M. Ryan, Analysing unlinkability and anonymity using the applied pi calculus, in: Proc. 23rd IEEE Computer Security Foundations Symposium (CSF'10), IEEE Computer Society Press, 2010, pp. 107–121.
[20] V. Cheval, B. Blanchet, Proving more observational equivalences with Proverif, in: Proc. 2nd International Conference on Principles of Security and Trust (POST'13), LNCS, Springer, 2013, pp. 226–246.
[21] M. Abadi, C. Fournet, Private authentication, Theoretical Computer Science 322 (3) (2004) 427–476.
[22] V. Cheval, V. Cortier, A. Plet, Lengths may break privacy – or how to check for equivalences with length, in: Proc. 25th International Conference on Computer Aided Verification (CAV'13), Vol. 8043 of LNCS, Springer, 2013, pp. 708–723.
[23] G. Bana, H. Comon-Lundh, A computationally complete symbolic attacker for equivalence properties, in: Proc. ACM Conference on Computers and Communications Security, 2014.
[24] J. Millen, V. Shmatikov., Constraint solving for bounded-process cryptographic protocol analysis, in: Proc. of 8th ACM Conference on Computer and Communications Security, 2001.
[25] H. Comon-Lundh, V. Cortier, E. Zalinescu, Deciding security properties of cryptographic protocols. application to key cycles., Transaction on Computational Logic 11 (2).
[26] H. Comon-Lundh, S. Delaune, J. Millen, Constraint solving techniques and enriching the model with equational theories, in: V. Cortier, S. Kremer (Eds.), Formal Models and Techniques for Analyzing Security Protocols, Vol. 5 of Cryptology and Information Security Series, IOS Press, 2011, pp. 35–61.
[27] V. Cheval, H. Comon-Lundh, S. Delaune, Trace equivalence decision: Negative tests and non-determinism, in: Proc. 18th ACM Conference on Computer and Communications Security (CCS'11), ACM Press, 2011, pp. 321–330.
[28] V. Cheval, Automatic verification of cryptographic protocols: privacy-type properties, Thèse de doctorat, Laboratoire Spécification et Vérification, ENS Cachan, France (Dec. 2012).
[29] H. Comon-Lundh, S. Delaune, The finite variant property: How to get rid of some algebraic properties, in: Proc. 16th International Conference on Rewriting Techniques and Applications (RTA'05), Vol. 3467 of LNCS, 2005.
[30] N. Dershowitz, J.-P. Jouannaud, Rewrite systems, in: Handbook of Theoretical Computer Science, Vol. B, Elsevier, 1990, Ch. 6.
[31] H. Comon, P. Lescanne, Equational problems and disunification, Journal of Symbolic Computation 7 (3/4) (1989) 371–425.
[32] V. Cheval, H. Comon-Lundh, S. Delaune, Automating security analysis: symbolic equivalence of constraint systems, in: Proc. 5th International Joint Conference on Automated Reasoning (IJCAR'10), Vol. 6173 of LNAI, Springer-Verlag, 2010, pp. 412–426.
[33] V. Cheval, Apte: an algorithm for proving trace equivalence, in: Proc. 20th International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS'14), LNCS, Springer, 2014.
[34] D. Basin, S. Mödersheim, L. Viganò, Constraint Differentiation: A New Reduction Technique for Constraint-Based Analysis of Security Protocols, in: Proc. 10th ACM Conference on Computer and Communications Security (CCS'03), ACM Press, New York, 2003, pp. 335–344.
[35] D. Baelde, S. Delaune, L. Hirschi, A reduced semantics for deciding trace equivalence using constraint systems, in: Proc. 3rd Conference on Principles of Security and Trust POST'14, LNCS, Springer, 2014.
[36] H. Comon, C. Delor, Equational formulae with membership constraints, Information and Computation 112 (2) (1994) 167–216.

The appendices are dedicated to the proofs of Theorem 5 and Corollary 1. This task is difficult and highly technical task due to several reasons:

- The proofs of the intermediate results are often done relying on a case analysis considering each rule one by one, and this tends to lengthen the proofs. This is even more true for the termination proof since we have to consider the different rules but also the different phases and steps of the strategy.
- The constraint systems are composed of several elements which make them difficult to manipulate in the proofs.
- The technicality of the proofs comes also from the fact that the soundness and termination proofs overlap. A good example is Step e of the first phase of the strategy which is a necessary step for the soundness of our algorithm.

Outline. In Appendix A, we give the different invariants that are satisfied by the pairs (of matrices) of constraint systems obtained during the algorithm. We prove the completeness of our transformation rules in Appendix B. However, the soundness of our transformation rules also depends on the strategy we use. Hence, before proving the soundness of the rules in Appendix D, we show some additional invariants related to the strategy in Appendix C. We conclude the proofs of soundness and completeness by proving Theorems 2 and 3 in Appendix E. We also show the soundness and completeness of our final test on a pair of matrices of constraint systems,*i.e.* the proof of Theorem 4, in Appendix F. In Appendix G, we establish termination.

Notations. Note that given a pair of sets of initial constraint systems, the maximal index that occurs in the constraint systems will be the same along the procedure, and we will denote it s_{max}.

Appendix A. Some invariants

We establish in this section some invariants that are independent from the strategy $\mathcal{S}$. We start by showing that our transformation rules preserve the fact that matrices share the same structure.

Lemma 1. *Let $(\mathcal{M}, \mathcal{M}')$ be a pair of matrices of constraint systems such that $\mathcal{M}$ and $\mathcal{M}'$ have the same structure. Any internal (resp. external) application of a rule in Figure 1 and/or Figure 2 transforms the pair $(\mathcal{M}, \mathcal{M}')$ on a pair $(\mathcal{M}_1, \mathcal{M}'_1)$ (resp. two pairs $(\mathcal{M}_1, \mathcal{M}'_1)$ and $(\mathcal{M}_2, \mathcal{M}'_2)$) of matrices having the same structure.*

Proof. Let $\mathcal{C}$ and $\mathcal{C}'$ be two constraint systems. Recall that the transformations rules Dest, Eq-frame-frame, Eq-frame-ded and Ded-st are applied internally whereas the rules Cons(X, f), Axiom(X, path) and Eq-ded-ded(X, ξ) are applied externally when $X \in S_2$ and internally otherwise (*i.e.* $X \notin S_2$).

Let Rule$(\tilde{p})$ be a rule and let $\mathcal{C}_1, \mathcal{C}_2$ (resp. $\mathcal{C}'_1, \mathcal{C}'_2$) be the two constraint systems obtained by application of R on $\mathcal{C}$ (resp. $\mathcal{C}'$). We assume that the application of Rule$(\tilde{p})$ is done simultaneously on $\mathcal{C}$ and $\mathcal{C}'$ (*i.e.* the possible fresh recipe variables created are the same in both applications). We show that :

1. if $\mathcal{C}$ and $\mathcal{C}'$ have the same structure (resp. shape) then $\mathcal{C}_1, \mathcal{C}'_1$ and $\mathcal{C}_2, \mathcal{C}'_2$ have the same structure (resp. shape);

2. if $\text{RULE}(\tilde{p})$ is applied internally on $\mathcal{C}$, then $\mathcal{C}, \mathcal{C}_1$ and $\mathcal{C}_2$ have the same shape.

With theses properties, the result directly holds. We prove theses properties by case analysis on the rule $\text{RULE}(\tilde{p})$. To simplify the notation, we will use the notation $S_1(\mathcal{C}), S_2(\mathcal{C}), \Phi(\mathcal{C}), \ldots$ while we refer to the different elements of a constraint system $\mathcal{C}$.

Case $\text{RULE}(\tilde{p}) = \text{CONS}(X, \mathsf{f})$: We assume that the application of $\text{RULE}(\tilde{p})$ was done simultaneously, thus if $\mathsf{ar}(\mathsf{f}) = n$, we denote by $X_1, \ldots, X_n$ the fresh recipe variables used in $\mathcal{C}_1$ and $\mathcal{C}'_1$.

Assume first that $\mathcal{C}$ and $\mathcal{C}'$ have the same structure. Thus we have that $S_2(\mathcal{C}) = S_2(\mathcal{C}')$. By definition of $\text{CONS}(X, \mathsf{f})$, we have that $S_2(\mathcal{C}) = S_2(\mathcal{C}_2)$ and $S_2(\mathcal{C}') = S_2(\mathcal{C}'_2)$ which means that $S_2(\mathcal{C}_2) = S_2(\mathcal{C}'_2)$. Furthermore, If $X \in S_2(\mathcal{C}) = S_2(\mathcal{C}')$, then $S_2(\mathcal{C}_1) = S_2(\mathcal{C}) \cup \{X_1, \ldots, X_n\} = S_2(\mathcal{C}') \cup \{X_1, \ldots, X_n\} = S_2(\mathcal{C}'_1)$. Otherwise, we have that $S_2(\mathcal{C}_1) = S_2(\mathcal{C}) = S_2(\mathcal{C}') = S_2(\mathcal{C}'_1)$.

We also have that $E_\Pi(\mathcal{C}) = E_\Pi(\mathcal{C}')$. But by definition of $\text{CONS}(X, \mathsf{f})$, $E_\Pi(\mathcal{C}_1) = E_\Pi(\mathcal{C}) \wedge X =^? \mathsf{f}(X_1, \ldots, X_n)$ and $E_\Pi(\mathcal{C}'_1) = E_\Pi(\mathcal{C}') \wedge X =^? \mathsf{f}(X_1, \ldots, X_n)$. Thus we have that $E_\Pi(\mathcal{C}'_1) = E_\Pi(\mathcal{C}_1)$. Similarly, we have that $E_\Pi(\mathcal{C}_2) = E_\Pi(\mathcal{C}'_2)$.

Since the frame is not modified by the rule $\text{CONS}(X, \mathsf{f})$, then we have $\{(\xi, i) \mid \xi, i \rhd \Phi(\mathcal{C})\} = \{(\xi, i) \mid \xi, i \rhd \Phi(\mathcal{C}')\}$ implies that $\{(\xi, i) \mid \xi, i \rhd \Phi(\mathcal{C}_1)\} = \{(\xi, i) \mid \xi, i \rhd \Phi(\mathcal{C}'_1)\}$. The same holds for $\mathcal{C}_2$ and $\mathcal{C}'_2$.

At last, we have $D(\mathcal{C}_1) = D(\mathcal{C}) \cup \{X_1, i \vdash^? x_1, \ldots, X_n, i \vdash^? x_n\}$ and $D(\mathcal{C}'_1) = D(\mathcal{C}') \cup \{X_1, i \vdash^? x'_1, \ldots, X_n, i \vdash^? x'_n\}$ where $x_1, \ldots, x_n, x'_1, \ldots, x'_n$ are fresh variables. Thus, $\{(X, i) \mid X, i \vdash^? u \in D(\mathcal{C})\} = \{(X, i) \mid X, i \vdash^? u \in D(\mathcal{C}')\}$ implies that $\{(X, i) \mid X, i \vdash^? u \in D(\mathcal{C}_1)\} = \{(X, i) \mid X, i \vdash^? u \in D(\mathcal{C}'_1)\}$. The case for $\mathcal{C}_2$ and $\mathcal{C}'_2$ is trivial since $D(\mathcal{C}_2) = D(\mathcal{C})$ and $D(\mathcal{C}'_2) = D(\mathcal{C}')$.

We can conclude that if $\mathcal{C}$ and $\mathcal{C}'$ have the same structure then $\mathcal{C}_1$ and $\mathcal{C}'_1$ (resp. $\mathcal{C}_2$ and $\mathcal{C}'_2$) also have the same structure. Similarly, we show that if $\mathcal{C}$ and $\mathcal{C}'$ have the same shape then $\mathcal{C}_1$ and $\mathcal{C}'_1$ (resp. $\mathcal{C}_2$ and $\mathcal{C}'_2$) also have the same shape.

At last, if $\text{CONS}(X, \mathsf{f})$ is applied internally (*i.e.* $X \notin S_2(\mathcal{C})$), then we have that $S_2(\mathcal{C}) = S_2(\mathcal{C}_1) = S_2(\mathcal{C}_2)$. Furthermore since $X_1, \ldots, X_n$ are fresh then $X_1, \ldots, X_n \notin S_2(\mathcal{C})$ and so $\mathcal{C}, \mathcal{C}_1$ and $\mathcal{C}_2$ have the same shape.

Case $\text{RULE}(\tilde{p}) = \text{AXIOM}(X, \mathsf{path})$: The rule $\text{AXIOM}(X, \mathsf{path})$ does not modify S_2 and either it does not modify D, in the case of $\mathcal{C}_2$ and $\mathcal{C}'_2$, or it removes this constraint in the case of $\mathcal{C}_1$, and $\mathcal{C}'_1$. Thus, we easily have that if $\mathcal{C}$ and $\mathcal{C}'$ have the same shape, then $\mathcal{C}_1$ and $\mathcal{C}'_1$ (resp. $\mathcal{C}_2$ and $\mathcal{C}'_2$) also have the same shape. Furthermore, in the case of an internal application of $\text{AXIOM}(X, \mathsf{path})$, we have that $X \notin S_2(\mathcal{C})$. If $(X, i \vdash^? u) \in D(\mathcal{C})$, then we have that $(X, i) \notin \{(Y, j) \mid (Y, j \vdash^? v \in D(\mathcal{C}) \wedge Y \in S_2(\mathcal{C})\}$. Thus we can also deduce that $\mathcal{C}, \mathcal{C}_1$ and $\mathcal{C}_2$ have the same shape when the rule $\text{AXIOM}(X, \mathsf{path})$ is applied internally.

At last, assume that $\mathcal{C}$ and $\mathcal{C}'$ have the same structure. Thus, we have that $\{(\xi, i) \mid \xi, i \rhd u \in \Phi(\mathcal{C})\} = \{(\xi, i) \mid \xi, i \rhd u \in \Phi(\mathcal{C}')\}$. But if there exists $(\xi, i \rhd u) \in \Phi(\mathcal{C})$ with $\mathsf{path}(\xi) = \mathsf{path}$ then it implies that there exists u' such that $(\xi, i \rhd u') \in \Phi(\mathcal{C}')$. With this, we can deduce that $E_\Pi(\mathcal{C}_1) = E_\Pi(\mathcal{C}) \wedge X =^? \xi$ and $E_\Pi(\mathcal{C}'_1) = E_\Pi(\mathcal{C}') \wedge X =^? \xi$. Since $E_\Pi(\mathcal{C}) = E_\Pi(\mathcal{C}')$, we can conclude that $E_\Pi(\mathcal{C}_1) = E_\Pi(\mathcal{C}'_1)$ and so $\mathcal{C}_1$ and $\mathcal{C}'_1$ have the

same structure. A similar reasoning allows us to conclude that $\mathcal{C}_2$ and $\mathcal{C}'_2$ have the same structure.

Case $\textsc{Rule}(\tilde{p}) = \textsc{Dest}(\xi, \ell \to r, i)$: The application of this rule on $\mathcal{C}$ (resp $\mathcal{C}'$) only adds a new non deducibility constraint on $\mathcal{C}_2$ (resp. $\mathcal{C}'_2$). Thus, we trivially have that $\mathcal{C}, \mathcal{C}_2$ have the same shape; and $\mathcal{C}, \mathcal{C}'$ have the same structure (resp. shape) implies that $\mathcal{C}_2, \mathcal{C}'_2$ have the same structure (resp. shape).

We consider now the constraint systems $\mathcal{C}_1$ and $\mathcal{C}'_1$. Since $\textsc{Dest}(\xi, \ell \to r, i)$ is applied simultaneously on $\mathcal{C}$ and $\mathcal{C}'$, then there exists $X_2, \ldots, X_n$ fresh recipe variables such that $D(\mathcal{C}_1) = D(\mathcal{C}) \cup \{X_2, i \vdash^? u_2;\ \ldots;\ X_n, i \vdash^? u_n\}$ and $D(\mathcal{C}'_1) = D(\mathcal{C}') \cup \{X_2, i \vdash^? u'_2;\ \ldots;\ X_n, i \vdash^? u'_n\}$ where $f(u_1, \ldots u_n) \to w$ and $f(u'_1, \ldots, u'_n) \to w'$ are fresh renaming of $\ell \to r$. Thus we can deduce that $\{(X, i) \mid X, i \vdash^? u \in D(\mathcal{C})\} = \{(X, i) \mid X, i \vdash^? u \in D(\mathcal{C}')\}$ implies that $\{(X, i) \mid X, i \vdash^? u \in D(\mathcal{C}_1)\} = \{(X, i) \mid X, i \vdash^? u \in D(\mathcal{C}'_1)\}$.

Furthermore, we also have that $\Phi(\mathcal{C}_1) = \Phi(\mathcal{C}) \cup \{\mathsf{f}(\xi, X_2, \ldots, X_n), i \rhd w\}$ and $\Phi(\mathcal{C}'_1) = \Phi(\mathcal{C}') \cup \{\mathsf{f}(\xi, X_2, \ldots, X_n), i \rhd w'\}$. Thus, we deduce that $\{(\xi, i) \mid \xi, i \rhd u \in \Phi(\mathcal{C})\} = \{(\xi, i) \mid \xi, i \rhd u \in \Phi(\mathcal{C}')\}$ implies that $\{(\xi, i) \mid \xi, i \rhd u \in \Phi(\mathcal{C}_1)\} = \{(\xi, i) \mid \xi, i \rhd u \in \Phi(\mathcal{C}'_1)\}$.

Since $S_2(\mathcal{C}) = S_2(\mathcal{C}_1)$ and $S_2(\mathcal{C}') = S_2(\mathcal{C}'_1)$ by definition of $\textsc{Dest}$, we can conclude that if $\mathcal{C}, \mathcal{C}'$ have the same structure then $\mathcal{C}_1, \mathcal{C}'_1$ also have the same structure.

At last, the facts that $S_2(\mathcal{C}) = S_2(\mathcal{C}_1)$ and $X_2, \ldots, X_n$ are fresh variables (*i.e.* $X_2, \ldots, X_n \notin S_2(\mathcal{C})$) also imply that $\{(X, i) \mid X, i \vdash^? u \in D(\mathcal{C}) \wedge X \in S_2(\mathcal{C})\} = \{(X, i) \mid X, i \vdash^? u \in D(\mathcal{C}_1) \wedge X \in S_2(\mathcal{C}_1)\}$. Thus, we can conclude that $\mathcal{C}, \mathcal{C}_1$ have the same shape.

Case $\textsc{Rule}(\tilde{p}) = \textsc{Eq-frame-frame}(\xi_1, \xi_2)$: This rule only modifies $E(\mathcal{C})$ and $E(\mathcal{C}')$ thus the result trivially holds.

Case $\textsc{Rule}(\tilde{p}) = \textsc{Eq-frame-ded}(\xi_1, X_2)$: The application of this rule modifies $E(\mathcal{C})$, $E(\mathcal{C}')$ and adds an frame element on $\mathsf{NoUse}(\mathcal{C})$ and $\mathsf{NoUse}(\mathcal{C}')$. Hence, it is easy to see that the rule does not modify the shape of the constrain systems. Assume now that $\mathcal{C}$ and $\mathcal{C}'$ have the same structure. It implies that $\{\xi, i \mid (\xi, i \rhd u) \in \mathsf{NoUse}(\mathcal{C})\} = \{\xi, i \mid (\xi, i \rhd u) \in \mathsf{NoUse}(\mathcal{C}')\}$ and $\{\xi, i \mid (\xi, i \rhd u) \in \Phi(\mathcal{C})\} = \{\xi, i \mid (\xi, i \rhd u) \in \Phi(\mathcal{C}')\}$. Hence, we have that there exists u, u' such that $(\xi_1, i_1 \rhd u) \in \Phi(\mathcal{C})$ and $(\xi_1, i_1 \rhd u') \in \Phi(\mathcal{C}')$. Thus, by definition of the rule, we have that $\mathsf{NoUse}(\mathcal{C}_1) = \mathsf{NoUse}(\mathcal{C}) \cup \{\xi_1, i_1 \rhd u\}$ and $\mathsf{NoUse}(\mathcal{C}'_1) = \mathsf{NoUse}(\mathcal{C}') \cup \{\xi_1, i_1 \rhd u'\}$. It implies that $\{\xi, i \mid (\xi, i \rhd u) \in \mathsf{NoUse}(\mathcal{C}_1)\} = \{\xi, i \mid (\xi, i \rhd u) \in \mathsf{NoUse}(\mathcal{C}'_1)\}$ and so $\mathcal{C}_1$, $\mathcal{C}'_1$ have the same structure.

Since only $E(\mathcal{C}_2)$, $E(\mathcal{C}'_2)$ are modified from $E(\mathcal{C})$, $E(\mathcal{C}')$, we easily deduce that $\mathcal{C}_2$,$\mathcal{C}_2$ have the same structure.

Case $\textsc{Rule}(\tilde{p}) = \textsc{Eq-ded-ded}(X, \xi)$: By the application of this rule on $\mathcal{C}$ and $\mathcal{C}'$, we have that $E_\Pi(\mathcal{C}_1) = E_\Pi(\mathcal{C}) \wedge X =^? \xi$ and $E_\Pi(\mathcal{C}'_1) = E_\Pi(\mathcal{C}') \wedge X =^? \xi$. Furthermore, the constraint $X, i \vdash^? u \in D(\mathcal{C})$ (resp. $X, i \vdash^? u' \in D(\mathcal{C}')$) is removed in $D(\mathcal{C}_1)$ (resp. $D(\mathcal{C}_2)$). Thus, we can easily see that if $\mathcal{C}, \mathcal{C}'$ have the same structure (resp. shape) then $\mathcal{C}_1, \mathcal{C}'_1$ and $\mathcal{C}_2, \mathcal{C}'_2$ also have the same structure (resp. shape).

In the case were $\textsc{Eq-ded-ded}(X, \xi)$ is applied internally, we have that $X \notin S_2(\mathcal{C})$ which means that $(X, i) \notin \{(Y, j) \mid Y, j \vdash^? v \in D(\mathcal{C}) \wedge Y \in S_2(\mathcal{C})\}$. Thus, we have that $\{(Y, j) \mid Y, j \vdash^? v \in D(\mathcal{C}) \wedge Y \in S_2(\mathcal{C})\} = \{(Y, j) \mid Y, j \vdash^? v \in D(\mathcal{C}_1) \wedge Y \in S_2(\mathcal{C}_1)\}$. This allows us to conclude that $\mathcal{C}$ and $\mathcal{C}_1$ have the same shape when $\textsc{Eq-ded-ded}(X, \xi)$ is applied internally. The result trivially holds for $\mathcal{C}_2$ and $\mathcal{C}'_2$.

Case $\text{RULE}(\tilde{p}) = \text{DED-ST}(\xi, \mathsf{f})$: The application of this rule on $\mathcal{C}$ (resp $\mathcal{C}'$) only adds a new non deducibility constraint on $\mathcal{C}_2$ (resp. $\mathcal{C}'_2$). Thus, we trivially have that $\mathcal{C}, \mathcal{C}_2$ have the same shape; and $\mathcal{C}, \mathcal{C}'$ have the same structure (resp. shape) implies that $\mathcal{C}_2, \mathcal{C}'_2$ have the same structure (resp. shape).

We consider now the constraint systems $\mathcal{C}_1$ and $\mathcal{C}'_1$. Since $\text{DED-ST}(\xi, \mathsf{f})$ is applied simultaneously on $\mathcal{C}$ and $\mathcal{C}'$, then $X_1, \ldots, X_n$ fresh recipe variables such that $D(\mathcal{C}_1) = D(\mathcal{C}) \cup \{X_1, \mathsf{s}_{max} \vdash^? x_1;\ \ldots;\ X_n, \mathsf{s}_{max} \vdash^? x_n\}$ and $D(\mathcal{C}'_1) = D(\mathcal{C}') \cup \{X_1, \mathsf{s}_{max} \vdash^? x_1;\ \ldots;\ X_n, \mathsf{s}_{max} \vdash^? x_n\}$ where $x_1, \ldots, x_n$ are fresh variables. Thus we can deduce that $\{(X, i) \mid X, i \vdash^? u \in D(\mathcal{C})\} = \{(X, i) \mid X, i \vdash^? u \in D(\mathcal{C}')\}$ implies that $\{(X, i) \mid X, i \vdash^? u \in D(\mathcal{C}_1)\} = \{(X, i) \mid X, i \vdash^? u \in D(\mathcal{C}'_1)\}$.

Since $S_2(\mathcal{C}) = S_2(\mathcal{C}_1)$ and $S_2(\mathcal{C}') = S_2(\mathcal{C}'_1)$ by definition of DED-ST, we can conclude that if $\mathcal{C}, \mathcal{C}'$ have the same structure then $\mathcal{C}_1, \mathcal{C}'_1$ also have the same structure.

At last, the facts that $S_2(\mathcal{C}) = S_2(\mathcal{C}_1)$ and $X_2, \ldots, X_n$ were fresh variables (*i.e.* $X_2, \ldots, X_n \notin S_2(\mathcal{C})$) also imply that $\{(X, i) \mid X, i \vdash^? u \in D(\mathcal{C}) \wedge X \in S_2(\mathcal{C})\} = \{(X, i) \mid X, i \vdash^? u \in D(\mathcal{C}_1) \wedge X \in S_2(\mathcal{C}_1)\}$. Thus, we can conclude that $\mathcal{C}, \mathcal{C}_1$ have the same shape. □

Initially, we consider two row matrices of initial constraint systems. By applying our rules, the constraint systems we consider become more and more complex. Nevertheless, we will show that the strategy and the rules ensure several invariants on constraint systems that will be used in the proof of completeness, soundness and termination. A constraint system satisfying all the invariants will be called *well-formed* (see Definition 18 stated later on). Before to state this definition, we introduce the notions of *context w.r.t. a frame*, *direct access mappings* and *maximal parameter of a recipe*.

Intuitively, the context of a recipe w.r.t. a frame represents part of the recipe that are not directly defined by the frame.

Definition 15 (context w.r.t. Φ)**.** *Let Φ be a frame and ξ be a recipe in Π_r. The* context *of ξ w.r.t. Φ, denoted $\mathsf{C}\lfloor\xi\rfloor_\Phi$, is a term in $\mathcal{T}(\mathcal{F}, \mathcal{F}_d^* \cdot \mathcal{A}\mathcal{X} \cup \mathcal{X}^2)$ and is defined recursively as follows:*

- $\mathsf{C}\lfloor\xi\rfloor_\Phi = \mathsf{path}(\xi)$ *if there exists* $(\xi', i \rhd u) \in \Phi$ *such that* $\mathsf{path}(\xi) = \mathsf{path}(\xi')$*;*
- $\mathsf{C}\lfloor\xi\rfloor_\Phi = \xi$ *if* $\xi \in \mathcal{X}^2$*;*
- $\mathsf{C}\lfloor\xi\rfloor_\Phi = \mathsf{f}(\mathsf{C}\lfloor\xi_1\rfloor_\Phi, \ldots, \mathsf{C}\lfloor\xi_n\rfloor_\Phi)$ *if* $\xi = \mathsf{f}(\xi_1, \ldots, \xi_n)$.

For sake of clarity, when Φ is clear from the context, we denote it by $\mathsf{C}\lfloor\xi\rfloor$.

Definition 16 (direct access mappings)**.** *Let $\mathcal{C} = (S_1; S_2; \Phi; D; E; E_\Pi; ND; \mathsf{NoUse})$ be a constraint system. We define the* direct access mapping *of $\mathcal{C}$, denoted $\delta^1(\mathcal{C})$ (resp. $\delta^2(\mathcal{C})$), to be a mapping from $(\mathcal{F}_d^* \cdot \mathcal{A}\mathcal{X}) \cup \mathcal{X}^2$ to constructor terms (resp. recipe in Π_r) where:*

- *for all $(X, i \vdash^? u) \in D$, we have that $X\delta^1(\mathcal{C}) = u$ (resp. $X\delta^2(\mathcal{C}) = X$)*
- *for all $(\xi, i \rhd u) \in \Phi$, we have that $\mathsf{path}(\xi)\delta^1(\mathcal{C}) = u$ (resp. $\mathsf{path}(\xi)\delta^2(\mathcal{C}) = \xi$).*

Example 48. *Let* $\mathcal{C} = (S_1; S_2; \Phi; D; E; E_\Pi; ND; \mathsf{NoUse})$ *be a constraint system where* $\mathsf{NoUse} = \emptyset$, $D = \{X, 1 \vdash^? \langle x, a\rangle \ ; \ Y, 2 \vdash^? b\}$, $\Phi = \{ax_1, 1 \rhd \mathsf{senc}(a, b) \ ; \ ax_2, 2 \rhd b \ ; \ \mathsf{sdec}(ax_1, Y), 2 \rhd a\}$. *Let* ξ_1, ξ_2 *and* ξ_3 *three recipes such that* $\xi_1 = \langle X, Y\rangle$, $\xi_2 = \mathsf{sdec}(ax_1, Y)$ *and* $\xi_3 = \mathsf{senc}(X, \mathsf{sdec}(ax_1, ax_2))$. *We have :*

- $\mathsf{C}\lfloor\xi_1\rfloor = \langle X, Y\rangle$ *and* $\mathsf{C}\lfloor\xi_1\rfloor\delta^1(\mathcal{C}) = \langle\langle x, a\rangle, b\rangle$
- $\mathsf{C}\lfloor\xi_2\rfloor = \mathsf{sdec} \cdot ax_1$ *and* $\mathsf{C}\lfloor\xi_2\rfloor\delta^1(\mathcal{C}) = a$
- $\mathsf{C}\lfloor\xi_3\rfloor = \mathsf{senc}(X, \mathsf{sdec} \cdot ax_1)$ *and* $\mathsf{C}\lfloor\xi_3\rfloor\delta^1(\mathcal{C}) = \mathsf{senc}(\langle x, a\rangle, a)$

Note that for all ground recipe ξ *conforms to a ground frame* Φ, $\mathsf{C}\lfloor\xi\rfloor_\Phi\delta^2(\mathcal{C}) = \xi$. *This illustrates the fact that the context of a recipe represents the canonical way to represent a recipe. Moreover, if* Φ *is consistent then* $\mathsf{C}\lfloor\xi\rfloor_\Phi\delta^1(\mathcal{C})\downarrow = \xi\Phi\downarrow$.

Definition 17 (maximal parameter of a recipe)**.** *Let* $\mathcal{C} = (S_1; S_2; \Phi; D; E; E_\Pi; ND; \mathsf{NoUse})$ *be a constraint system and let* $\xi \in \Pi_r$ *such that* $vars(\xi) \subseteq vars^2(D)$. *We define the maximal parameter of* ξ *in* $\mathcal{C}$, *denoted* $\mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(\xi)$, *such that:*

$$\mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(\xi) = \max\{i \mid ax_i \in st(\xi) \text{ or } (Y, i, \vdash^? v) \in D \text{ with } Y \in st(\xi)\}$$

Most of the invariants stated below in Definition 18 are about structural properties of the frame, and are direct consequences of the application of the rules Dest, Axiom and Cons. For example, the first property states that for any frame element $(\xi, i \rhd u)$, the path of the recipe ξ is defined and closed. For all constraint systems $\mathcal{C}$, we denote by $\mathsf{mgu}(E(\mathcal{C}))$ (resp. $\mathsf{mgu}(E_\Pi(\mathcal{C}))$) the most general unifier of all the equations in $E(\mathcal{C})$ (resp. $\mathsf{mgu}(E_\Pi(\mathcal{C}))$).

Definition 18 (well-formed)**.** *Let* $\mathcal{C} = (S_1; S_2; \Phi; D; E; E_\Pi; ND; \mathsf{NoUse})$ *be a constraint system. We say that* $\mathcal{C}$ *is* well-formed *if it satisfies the following properties:*

Invariants on the frame Φ: *for all* $(\xi, i \rhd u) \in \Phi$,

1. $\mathsf{path}(\xi)$ *exists and is closed. Moreover, for all distinct frame elements* $(\xi_1, i_1 \rhd u_1)$ *and* $(\xi_2, i_2 \rhd u_2)$ *in* Φ, *we have that* $\mathsf{path}(\xi_1) \neq \mathsf{path}(\xi_2)$.
2. *if* $\mathsf{path}(\xi) = \mathsf{f} \cdot w$ *then there exists* $(\xi', j \rhd v) \in \Phi$ *such that* $j \leq i$, $\mathsf{path}(\xi') = w$, $\xi' \in st(\xi)$ *and* $u \in st(v)$.
3. $\mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(\xi) \leq i$
4. *for all* $X \in vars^2(\xi)$, *for all* $x \in vars^1(X\delta^1(\mathcal{C}))$, *there exists* $(\zeta, k \rhd w) \in \Phi$ *such that* $k \leq i$ *and* $x \in vars^1(w)$.
5. *for all ground substitution* λ, *if for all* $X \in vars^2(\xi)$, *we have that* $(X\lambda)\Phi\lambda\downarrow = v\lambda$ *where* $(X, j \vdash^? v) \in D$, *then* $(\xi\lambda)(\Phi\lambda)\downarrow = u\lambda$.

Other invariants: *let* $\theta = \mathsf{mgu}(E_\Pi)$

6. *any inequation in* E_Π *are:*
   - *either of the form* $X \neq \xi$ *and there exists* $i \in \mathbb{N}$ *and a term* u *such that* $(\xi, i \rhd u) \in \Phi$;

- *or of the form* $\mathsf{root}(X) \neq \mathsf{f}$ *with* $\mathsf{f} \in \mathcal{F}_c$.

7. *for all* $X \in vars^2(\mathcal{C})$, $\mathsf{C}\lfloor X\theta \rfloor_\Phi \in \mathcal{T}(\mathcal{F}_c, \mathcal{F}_d^* \cdot \mathcal{AX} \cup \mathcal{X}^2)$ *and for all* $\zeta \in st(X\theta)$, $\mathsf{path}(\zeta) \in \mathcal{F}_d^* \cdot \mathcal{AX}$ *implies that there exists* j *and* v *such that* $(\zeta, j \rhd v) \in \Phi$
8. *For all* $(\zeta, i \rhd u) \in \mathsf{NoUse}$, *there exists* $X \in vars^2(\mathcal{C})$ *such that* $\mathsf{C}\lfloor X\theta \rfloor_\Phi \delta^1(\mathcal{C}) = u$ *and* $\mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(X\theta) < i$
9. *for all* $(\xi, i \rhd u) \in \Phi$, *for all* $\xi' \in st(\xi)$, $\mathsf{C}\lfloor \xi' \rfloor_\Phi \in \mathcal{T}(\mathcal{F}_c, \mathcal{F}_d^* \cdot \mathcal{AX} \cup \mathcal{X}^2)$ *and if* $\mathsf{path}(\xi') \in \mathcal{F}_d^* \cdot \mathcal{AX}$ *then there exists* j *and* v *such that* $(\xi', j \rhd v) \in \Phi$
10. *for all* $(X, i \vdash^? u) \in D$, $X \notin S_2(\mathcal{C})$ *implies that for all* $x \in vars^1(u)$, *there exists* $(Z, j \vdash^? v) \in D$ *such that* $i < j$ *and* $x \in vars^1(v)$.

We will conclude this appendix by showing that our transformation rules transform a well-formed constraint system into a pair of constraint systems that are also well-formed. To be able to prove this result, we first need to show the following two properties (Lemma 2 and Lemma 3).

Lemma 2. *Let* $\xi, \zeta \in \Pi_r$ *and let* $X \in \mathcal{X}^2$. *Let* θ *and* Θ *be two substitutions such that* $\theta = \{X \mapsto \zeta\}$ *and* $\Theta = \{X \mapsto \mathsf{path}(\zeta)\}$. *The following property holds:*

$$\mathsf{path}(\xi\theta) = \mathsf{path}(\xi)\Theta$$

Proof. We prove this result by induction on $|\mathsf{path}(\xi)|$:

Base case $|\mathsf{path}(\xi)| = 1$*:* In such a case, either $\xi \in \mathcal{AX}$ or $\xi \in \mathcal{X}^2$. If $\xi \in \mathcal{AX}$, then $\xi\theta = \xi$, $\mathsf{path}(\xi) = \xi$ and $\xi\Theta = \xi$. Thus, we have $\mathsf{path}(\xi\theta) = \mathsf{path}(\xi)\Theta$. Otherwise $\xi \in \mathcal{X}^2$ and $\mathsf{path}(\xi) = \xi$. We distinguish two cases: $\xi = X$ or $\xi \neq X$. If $\xi = X$ then $\mathsf{path}(X\theta) = \mathsf{path}(\zeta) = X\Theta = \mathsf{path}(X)\Theta$. Else, we have that $\xi\theta = \xi$. But $\mathsf{path}(\xi) = \xi$ and so $\mathsf{path}(\xi)\Theta = \mathsf{path}(\xi)$. Thus we conclude $\mathsf{path}(\xi\theta) = \mathsf{path}(\xi)\Theta$.

Inductive step $|\mathsf{path}(\xi)| > 1$*:* Otherwise, there exist $\xi_1, \ldots, \xi_n \in \Pi_r$ and $\mathsf{f} \in \mathcal{F}$ such that $\xi = \mathsf{f}(\xi_1, \ldots, \xi_n)$ and $\mathsf{path}(\xi) = \mathsf{f} \cdot \mathsf{path}(\xi_1)$. Thus $\xi\theta = \mathsf{f}(\xi_1\theta, \ldots, \xi_n\theta)$ and so $\mathsf{path}(\xi\theta) = \mathsf{f} \cdot \mathsf{path}(\xi_1\theta)$. Using our induction hypothesis on $\mathsf{path}(\xi_1)$, we have that $\mathsf{path}(\xi_1\theta) = \mathsf{path}(\xi_1)\Theta$, and therefore $\mathsf{path}(\xi\theta) = \mathsf{f} \cdot \mathsf{path}(\xi_1)\Theta = \mathsf{path}(\xi)\Theta$. □

Lemma 3. *Let* $\mathcal{C}$ *be a well formed constraint system and* Φ *its associated frame. Let* $\xi \in \Pi_r$ *such that* $\mathsf{C}\lfloor \xi \rfloor_\Phi \in \mathcal{T}(\mathcal{F}_c, \mathcal{F}_d^* \cdot \mathcal{AX} \cup \mathcal{X}^2)$. *Let* θ, Θ *be two substitutions such that* $\theta = \{X \to \xi'\}$, $\Theta = \{X \to \mathsf{C}\lfloor \xi' \rfloor_\Phi\}$ *and* $\mathsf{C}\lfloor \xi' \rfloor_\Phi \in \mathcal{T}(\mathcal{F}_c, \mathcal{F}_d^* \cdot \mathcal{AX} \cup \mathcal{X}^2)$. *The following property holds:*

$$\mathsf{C}\lfloor \xi\theta \rfloor_\Phi = \mathsf{C}\lfloor \xi \rfloor_\Phi\Theta$$

Proof. We prove this result by induction on $|\mathsf{C}\lfloor \xi \rfloor_\Phi|$:

Base case $|\mathsf{C}\lfloor \xi \rfloor_\Phi| = 1$*:* In such a case, either $\mathsf{C}\lfloor \xi \rfloor_\Phi \in (\mathcal{F}_d^* \cdot \mathcal{AX})$ or $\xi \in \mathcal{X}^2$. If $\xi \in \mathcal{X}^2 \setminus \{X\}$, then $\xi\theta = \xi$ and so $\mathsf{C}\lfloor \xi\theta \rfloor_\Phi = \xi = \mathsf{C}\lfloor \xi \rfloor_\Phi\Theta$. Thus the result holds. On the other hand, if $\xi = X$, then $\xi\theta = \xi'$ and $\mathsf{C}\lfloor \xi \rfloor_\Phi = X$ and so $\mathsf{C}\lfloor \xi\theta \rfloor_\Phi = \mathsf{C}\lfloor \xi' \rfloor_\Phi = X\Theta$.

Assume now that $\mathsf{C}\lfloor \xi \rfloor_\Phi \in (\mathcal{F}_d^* \cdot \mathcal{AX})$. In such case, there exists $(\zeta, i \rhd u) \in \Phi$ such that $\mathsf{path}(\zeta) = \mathsf{path}(\xi)$. But since $\mathsf{path}(\xi) \in (\mathcal{F}_d^* \cdot \mathcal{AX})$, we also have that $\mathsf{path}(\xi) = \mathsf{path}(\xi\theta)$, which means that $\mathsf{C}\lfloor \xi\theta \rfloor_\Phi = \mathsf{C}\lfloor \xi \rfloor_\Phi = \mathsf{C}\lfloor \xi \rfloor_\Phi\Theta$.

Inductive step $|\mathsf{C}\lfloor\xi\rfloor_\Phi| > 1$*:* By hypothesis, we know that $\mathsf{C}\lfloor\xi\rfloor_\Phi \in \mathcal{T}(\mathcal{F}_c, \mathcal{F}_d^* \cdot \mathcal{AX} \cup \mathcal{X}^2)$, thus, we have that $\mathsf{root}(\mathsf{C}\lfloor\xi\rfloor_\Phi) \in \mathcal{F}_c$ and so $\mathsf{root}(\xi) \in \mathcal{F}_c$. Assume that $\xi = \mathsf{f}(\xi_1, \ldots, \xi_n)$. By definition of a context, we have: $\mathsf{C}\lfloor\xi\rfloor_\Phi = \mathsf{f}(\mathsf{C}\lfloor\xi_1\rfloor_\Phi, \ldots, \mathsf{C}\lfloor\xi_n\rfloor_\Phi)$. Thus we can applied our inductive hypothesis on ξ_i, for $i \in \{1 \ldots n\}$. This allows us to deduce that $\mathsf{C}\lfloor\xi_i\theta\rfloor_\Phi = \mathsf{C}\lfloor\xi_i\rfloor_\Phi\Theta$. Hence, we have that

$$\begin{array}{rcl} \mathsf{C}\lfloor\xi\theta\rfloor_\Phi & = & \mathsf{C}\lfloor\mathsf{f}(\xi_1, \ldots, \xi_n)\theta\rfloor_\Phi \\ & = & \mathsf{f}(\mathsf{C}\lfloor\xi_1\theta\rfloor_\Phi, \ldots, \mathsf{C}\lfloor\xi_n\theta\rfloor_\Phi) \\ & = & \mathsf{f}(\mathsf{C}\lfloor\xi_1\rfloor_\Phi, \ldots, \mathsf{C}\lfloor\xi_n\rfloor_\Phi)\Theta \\ & = & \mathsf{C}\lfloor\mathsf{f}(\xi_1, \ldots, \xi_n)\rfloor_\Phi\Theta \\ & = & \mathsf{C}\lfloor\xi\rfloor_\Phi\Theta \end{array}$$

This allows us to conclude. □

We can now prove that our rules preserve the well-formedness of contraint systems.

Lemma 4. *Any rule in Figure 1 and Figure 2 transforms a normalised well-formed constraint system into a pair of constraint systems that are also well-formed after normalisation. For the rule* Dest*, we assume that its application is not useless.*

Proof. Let $\mathcal{C} = (S_1; S_2; \Phi; D; E; E_\Pi; ND; \mathsf{NoUse})$ be a normalised well-formed constraint system and let $\textsc{Rule}(\tilde{p})$ be a rule. Let $\mathcal{C}_1$ and $\mathcal{C}_2$ be the two constraint systems obtained by application of $\textsc{Rule}(\tilde{p})$ on $\mathcal{C}$. In the case where the normalisation of $\mathcal{C}_1$ and $\mathcal{C}_2$ is $\bot$, the result trivially holds thus we will assume that $\mathcal{C}_1{\downarrow} \neq \bot$ and $\mathcal{C}_2{\downarrow} \neq \bot$. We show the result by case analysis on the rule $\textsc{Rule}(\tilde{p})$.

Case $\textsc{Rule}(\tilde{p}) = \textsc{Cons}(X, \mathsf{f})$: The rule Cons only adds $\mathsf{root}(X) \neq \mathsf{f}$ on $E_\Pi(\mathcal{C}_2)$. Thus, we have that $\mathcal{C}_2{\downarrow} = \mathcal{C}_2$ and $\mathcal{C}_2$ trivially satisfies all the properties of Definition 18, except for the property 6. But $E_\Pi(\mathcal{C}_2) = E_\Pi(\mathcal{C}) \wedge \mathsf{root}(X) \neq \mathsf{f}$. Since $\mathcal{C}$ is a well-formed constraint system, then $E_\Pi(\mathcal{C})$ satisfies Property 6. Furthermore, since $\mathsf{f} \in \mathcal{F}_c$, then $\mathsf{root}(X) \neq \mathsf{f}$ also satisfies Property 6. We can conclude that $\mathcal{C}_2$ is a well-formed constraint system.

On the other hand, we have that $E_\Pi(\mathcal{C}_1) = E_\Pi(\mathcal{C}) \wedge X =^? \mathsf{f}(X_1, \ldots, X_n)$, $D(\mathcal{C}_1) = D(\mathcal{C}) \backslash \{X, i \vdash^? t\} \cup \{X_1, i \vdash^? x_1;\ \ldots;\ X_n, i \vdash^? x_n\}$, $E(\mathcal{C}_1) = E(\mathcal{C}) \wedge t =^? \mathsf{f}(x_1, \ldots, x_n)$ and $\Phi(\mathcal{C}) = \Phi(\mathcal{C}_1)$. Let $\sigma = \mathsf{mgu}(t =^? \mathsf{f}(x_1, \ldots, x_n))$ and $\theta = \mathsf{mgu}(X =^? \mathsf{f}(X_1, \ldots, X_n))$. By hypothesis, we know that $\mathcal{C}$ is normalised which means that $X \notin \mathrm{dom}(\mathsf{mgu}(E_\Pi(\mathcal{C})))$ and $vars^1(t) \cap \mathrm{dom}(\mathsf{mgu}(E(\mathcal{C}))) = \emptyset$. Since $X_1, \ldots, X_n, x_1, \ldots, x_n$ are fresh variables, we can deduce $\mathsf{mgu}(E_\Pi(\mathcal{C}_1)) = \mathsf{mgu}(E_\Pi(\mathcal{C}))\theta$ and $\mathsf{mgu}(E(\mathcal{C}_1)) = \mathsf{mgu}(E(\mathcal{C}))\sigma$.

Furthermore, $\mathcal{C}$ normalised also implies that $\Phi(\mathcal{C})\mathsf{mgu}(E_\Pi(\mathcal{C}))\mathsf{mgu}(E(\mathcal{C})) = \Phi(\mathcal{C})$ and also that $D(\mathcal{C})\mathsf{mgu}(E(\mathcal{C})) = D(\mathcal{C})$. Thus, we can deduce that $\Phi(\mathcal{C}_1{\downarrow}) = \Phi(\mathcal{C})\theta\sigma$ and $D(\mathcal{C}_1{\downarrow}) = D(\mathcal{C}_1)\sigma$. We now prove the different properties one by one.

Let $(\xi, j \rhd u) \in \Phi(\mathcal{C}_1{\downarrow})$. Since $\Phi(\mathcal{C}_1{\downarrow}) = \Phi(\mathcal{C})\theta\sigma$, we know that there exists $(\xi', j \rhd u') \in \Phi(\mathcal{C})$ such that $\xi = \xi'\theta$ and $u = u'\sigma$.

1. this property is direct from Lemma 2 and $\mathcal{C}$ being a well-formed constraint system.
2. this property is direct from Lemma 2 and $\mathcal{C}$ being a well-formed constraint system.
3. We know that $\xi = \xi'\theta$ where $\theta = \mathsf{mgu}(X =^? \mathsf{f}(X_1, \ldots, X_n))$. But $\mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(X) = i = \mathsf{param}^{\mathcal{C}_1{\downarrow}}_{\mathsf{max}}(X_j)$, we deduce that $\mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(\xi) = \mathsf{param}^{\mathcal{C}_1{\downarrow}}_{\mathsf{max}}(\xi')$. Since $\mathcal{C}$ is well-formed, we have $\mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(\xi) \leq j$ and so $\mathsf{param}^{\mathcal{C}_1{\downarrow}}_{\mathsf{max}}(\xi') \leq j$.

4. Let $Y \in vars^2(\xi)$ and $y \in vars^1(Y\delta^1(\mathcal{C}_1\downarrow))$. If $Y \in \{X_1, \ldots, X_n\}$ then there exists z such that $y \in vars^1(z\sigma)$ and $z \in vars^1(t)$. Thus $z \in vars^1(X\delta^1(\mathcal{C}))$. But $\xi = \xi'\theta$ thus it implies that $X \in vars^2(\xi')$. Since $\mathcal{C}$ is well formed, we deduce that there exists $(\zeta, k \rhd w) \in \Phi(\mathcal{C})$ such that $z \in vars^1(w)$ and $k \leq j$. We already showed that $\Phi(\mathcal{C}_1\downarrow) = \Phi(\mathcal{C})\theta\sigma$ hence $y \in vars^1(w\sigma)$ with $(\zeta\theta, k \vdash^? w\sigma) \in \Phi(\mathcal{C}_1\downarrow)$. The result holds

   If $Y \notin \{X_1, \ldots, X_n\}$, then $Y \in vars^2(\xi')$ and $Y \neq X$. Hence $Y \in vars^2(D(\mathcal{C}))$. Since $D(\mathcal{C}_1\downarrow) = D(\mathcal{C}_1)\sigma$, $\Phi(\mathcal{C}_1\downarrow) = \Phi(\mathcal{C})\theta\sigma$ and $\mathcal{C}$ is well-formed, we deduce the result.

5. Let λ be a ground substitution such that for all $Y \in vars^2(\xi)$, $(Y\lambda)\Phi(\mathcal{C}_1\downarrow)\lambda\downarrow = v\lambda$ where $(Y, k \vdash^? v) \in D(\mathcal{C}_1\downarrow)$. Let λ' the substitution such that $\lambda' = \theta\sigma\lambda$. We show that for all $Z \in vars^2(\xi')$, $(Z\lambda')\Phi(\mathcal{C})\lambda'\downarrow = w\lambda'$ where $(Z, k \vdash^? w) \in D(\mathcal{C})$. Let $Z \in vars^2(\xi')$. Since $\xi = \xi'\theta$, we have to distinguish two cases :

   - Either $Z = X$: In this case, we have that $Z\lambda' = X\theta\sigma\lambda = \mathsf{f}(X_1, \ldots, X_n)\lambda$. But in such a case, we have that $X_1, \ldots, X_n \in vars^2(\xi)$ and so by hypothesis, we have that $(X_k\lambda)\Phi(\mathcal{C}_1\downarrow)\lambda\downarrow = x_k\lambda$, for all $k \in \{1, \ldots, n\}$. Since $\Phi(\mathcal{C}_1\downarrow) = \Phi(\mathcal{C})\theta\sigma$, we can deduce that $(X_k\lambda)\Phi(\mathcal{C})\lambda'\downarrow = x_k\lambda = x_k\lambda'$. Thus $(Z\lambda')(\Phi(\mathcal{C})\lambda')\downarrow = \mathsf{f}(x_1, \ldots, x_n)\lambda' = t\lambda'$.
   - Or $Z \in vars^2(\xi)\backslash\{X_1, \ldots, X_n\}$: In such a case, we have that $Z\theta\sigma = Z$ and so $Z\lambda' = Z\lambda$. Furthermore, we know that $\Phi(\mathcal{C}_1\downarrow) = \Phi(\mathcal{C})\theta\sigma$ and so $\Phi(\mathcal{C}_1\downarrow)\lambda = \Phi(\mathcal{C})\lambda'$. Thus, we have that $(Z\lambda')\Phi(\mathcal{C})\lambda'\downarrow = (Z\lambda)\Phi(\mathcal{C}_1\downarrow)\lambda\downarrow$. By hypothesis, there exists $Z, k \vdash^? v \in D(\mathcal{C}_1\downarrow)$ such that $(Z\lambda)\Phi(\mathcal{C}_1\downarrow)\lambda\downarrow = v\lambda$. But $D(\mathcal{C}_1\downarrow) = D(\mathcal{C}_1)\sigma$ and $D(\mathcal{C}_1) = D(\mathcal{C})\backslash\{X, i \vdash^? t\} \cup \{X_1, i \vdash^? x_1;\ \ldots;\ X_n, i \vdash^? x_n\}$. Thus there exists $Z, k \vdash^? v' \in D(\mathcal{C})$ such that $v = v'\sigma$ and so $v\lambda = v'\lambda'$. We can conclude that $(Z\lambda')\Phi(\mathcal{C})\lambda'\downarrow = v'\lambda'$ with $Z, k \vdash^? v' \in D(\mathcal{C})$.

   By hypothesis, we know that $\mathcal{C}$ is a well-formed constraint system and so we deduce that $(\xi'\lambda')(\Phi(\mathcal{C})\lambda')\downarrow = u'\lambda'$. But $\xi'\lambda' = \xi\lambda$, $u'\lambda' = u\lambda$ and $\Phi(\mathcal{C})\lambda' = \Phi(\mathcal{C}_1\downarrow)\lambda$. Thus we conclude that $(\xi\lambda)\Phi(\mathcal{C}_1\downarrow)\lambda = u\lambda$.

6. Let $(\zeta_1 \neq^? \zeta_2) \in E_\Pi(\mathcal{C}_1\downarrow)$. By the normalisation, we know that there exists $(\zeta_1' \neq^? \zeta_2') \in E_\Pi(\mathcal{C}_1)$ such that $\zeta_1'\theta = \zeta_1$ and $\zeta_2'\theta = \zeta_2$. Moreover, by the rule Cons, the sets of inequations of $E_\Pi(\mathcal{C})$ and $E_\Pi(\mathcal{C}_1)$ are the same thus $(\zeta_1' \neq^? \zeta_2') \in E_\Pi(\mathcal{C})$. Since $\mathcal{C}$ is well formed, we deduce that $\zeta_1' \in \mathcal{X}^2$ and there exists $k \in \mathbb{N}$ and a term u such that $(\zeta_2', k \rhd u) \in \Phi(\mathcal{C})$. Since $\Phi(\mathcal{C}_1\downarrow) = \Phi(\mathcal{C})\theta\sigma$, we deduce that $(\zeta_2, k \rhd u\sigma) \in \Phi(\mathcal{C}_1\downarrow)$.

   But $\mathsf{path}(\zeta_2')$ exists thanks to $\mathcal{C}$ being well-formed (Property 1) thus $\mathsf{root}(\zeta_2') \notin \mathcal{F}_c$. Since $\mathsf{f} \in \mathcal{F}_c$ and $\zeta_1 = \zeta_1'\theta$, we deduce that $\zeta_1' \neq X$ otherwise the inequation would have disappeared by the normalisation rule. Thus $\zeta_1 \in \mathcal{X}^2$ and so the result holds.

   Let $(\mathsf{root}(\zeta) \neq^? \mathsf{g}) \in E_\Pi(\mathcal{C}_1\downarrow)$. Thanks to the normalisation, we know that $\zeta \in \mathcal{X}^2$ otherwise the inequation would have disappeared by the normalisation rules. Hence the result holds.

7. Let $Y \in vars^2(\mathcal{C}_1\downarrow)$. If $Y \in \{X_1, \ldots, X_n\}$, then since $\theta = \{X =^? \mathsf{f}(X_1, \ldots, X_n)\}$ and Y is fresh, we have $Y\mathsf{mgu}(E_\Pi(\mathcal{C}_1\downarrow)) = Y$ and so $\mathsf{C}\lfloor Y\mathsf{mgu}(E_\Pi(\mathcal{C}_1\downarrow))\rfloor_{\Phi(\mathcal{C}_1\downarrow)} = Y \in \mathcal{T}(\mathcal{F}_c, \mathcal{F}_d^* \cdot \mathcal{A}\mathcal{X} \cup \mathcal{X}^2)$. Otherwise, we have that $Y \in vars^2(\mathcal{C})$. Note that $\mathcal{C}$

is well-formed, thus we deduce that $\mathsf{C}\lfloor Y\mathsf{mgu}(E_\Pi(\mathcal{C}))\rfloor_{\Phi(\mathcal{C})} \in \mathcal{T}(\mathcal{F}_c, \mathcal{F}_d^* \cdot \mathcal{AX} \cup \mathcal{X}^2)$. But the path of any recipe in $\Phi(\mathcal{C})$ is closed which means that any context with $\Phi(\mathcal{C}_1\downarrow)$ and $\Phi(\mathcal{C})$ are the same. More specifically, we have $\mathsf{C}\lfloor Y\mathsf{mgu}(E_\Pi(\mathcal{C}))\rfloor_{\Phi(\mathcal{C})} = \mathsf{C}\lfloor Y\mathsf{mgu}(E_\Pi(\mathcal{C}))\rfloor_{\Phi(\mathcal{C}_1\downarrow)}$. Note that $\mathsf{mgu}(E_\Pi(\mathcal{C}_1\downarrow)) = \mathsf{mgu}(E_\Pi(\mathcal{C}))\theta$, $\theta = \{X \mapsto \mathsf{f}(X_1, \ldots, X_n)\}$ and $\mathsf{f} \in \mathcal{F}_c$. Thus by Lemma 3, we have $\mathsf{C}\lfloor Y\mathsf{mgu}(E_\Pi(\mathcal{C}_1\downarrow))\rfloor_{\Phi(\mathcal{C}_1\downarrow)} = \mathsf{C}\lfloor Y\mathsf{mgu}(E_\Pi(\mathcal{C}))\rfloor_{\Phi(\mathcal{C})}\theta \in \mathcal{T}(\mathcal{F}_c, \mathcal{F}_d^* \cdot \mathcal{AX} \cup \mathcal{X}^2)$.

Let $\zeta \in st(Y\mathsf{mgu}(E_\Pi(\mathcal{C}_1\downarrow))$ such that $\mathsf{path}(\zeta) \in \mathcal{F}_d^* \cdot \mathcal{AX}$. Since $\theta = \{X \mapsto \mathsf{f}(X_1, \ldots, X_n)\}$ with $\mathsf{f} \in \mathcal{F}_c$ and $\mathsf{mgu}(E_\Pi(\mathcal{C}_1)) = \mathsf{mgu}(E_\Pi(\mathcal{C}))\theta$, then there exists $\zeta' \in st(Y\mathsf{mgu}(E_\Pi(\mathcal{C})))$ such that $\zeta = \zeta'\theta$. Since $\mathcal{C}$ is well-formed, then there exists k and u such that $(\zeta', k \rhd u) \in \Phi(\mathcal{C})$. But $\Phi(\mathcal{C}_1\downarrow) = \Phi(\mathcal{C})\theta\sigma$. Hence $(\zeta, k \rhd u\sigma) \in \Phi(\mathcal{C}_1\downarrow)$. Hence the result holds.

8. Assume that $(\xi, j \rhd u) \in \mathsf{NoUse}(\mathcal{C}_1\downarrow)$. Since $\mathsf{NoUse}(\mathcal{C}_1\downarrow) = \mathsf{NoUse}(\mathcal{C})\theta\sigma$, we have that $(\xi', j \rhd u') \in \mathsf{NoUse}(\mathcal{C})$. Since $\mathcal{C}$ is a well-formed constraint system, we deduce that there exists $Y \in vars^2(\mathcal{C})$ such that $\mathsf{C}\lfloor Y\mathsf{mgu}(E_\Pi(\mathcal{C}))\rfloor_{\Phi(\mathcal{C})}\delta^1(\mathcal{C}) = u'$ and $\mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(Y\mathsf{mgu}(E_\Pi(\mathcal{C}))) < j$. We have seen that $\mathsf{C}\lfloor Y\mathsf{mgu}(E_\Pi(\mathcal{C}_1\downarrow))\rfloor_{\Phi(\mathcal{C}_1\downarrow)} = \mathsf{C}\lfloor Y\mathsf{mgu}(E_\Pi(\mathcal{C}))\rfloor_{\Phi(\mathcal{C})}\theta$ when proving the previous item. Furthermore, we know that $D(\mathcal{C}_1\downarrow) = D(\mathcal{C}_1)\sigma$ and $D(\mathcal{C}_1) = D(\mathcal{C})\backslash\{X, i \vdash^? t\} \cup \{X_1, i \vdash^? x_1;\ \ldots;\ X_n, i \vdash^? x_n\}$. Thus, we deduce that $\delta^1(\mathcal{C})\sigma = \theta\delta^1(\mathcal{C}_1\downarrow)$. This allows us to conclude that $u = u'\sigma = \mathsf{C}\lfloor Y\mathsf{mgu}(E_\Pi(\mathcal{C}))\rfloor_{\Phi(\mathcal{C})}\theta\delta^1(\mathcal{C}_1\downarrow) = \mathsf{C}\lfloor Y\mathsf{mgu}(E_\Pi(\mathcal{C}_1\downarrow))\rfloor_{\Phi(\mathcal{C}_1\downarrow)}\delta^1(\mathcal{C}_1\downarrow)$.

   At last, we already have that $Y\mathsf{mgu}(E_\Pi(\mathcal{C}_1\downarrow)) = Y\mathsf{mgu}(E_\Pi(\mathcal{C}))\theta$. Thus, since $\mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(X) = \mathsf{param}^{\mathcal{C}_1\downarrow}_{\mathsf{max}}(\mathsf{f}(X_1, \ldots, X_n)) = i$, then $\mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(Y\mathsf{mgu}(E_\Pi(\mathcal{C}))) < j$ implies that $\mathsf{param}^{\mathcal{C}_1\downarrow}_{\mathsf{max}}(Y\mathsf{mgu}(E_\Pi(\mathcal{C}_1\downarrow)) < j$.

9. Similar to Property 7

10. Let $(Z, k \vdash^? u) \in D(\mathcal{C}_1\downarrow)$. Assume that $Z \notin S_2(\mathcal{C}_1)$ and let $x \in vars^1(u)$. If $X \in S_2(\mathcal{C})$ then it implies that there exists $(Z, k \vdash^? u') \in D(\mathcal{C})$ such that $u = u'\sigma$. There exists a variable z such that $x \in vars^1(z\sigma)$ and $z \in vars^1(u')$. Since $\mathcal{C}$ is well-formed, we deduce that there exists $(Y, p \vdash^? w') \in D(\mathcal{C})$ such that $z \in vars^1(w')$ and $p < k$. Thus $x \in vars^1(w'\sigma)$. If $Y \neq X$ then we deduce that $(Y, p \vdash^? w'\sigma) \in D(\mathcal{C}_1\downarrow)$ and so the result holds. If $Y = X$, then $t = w'$ and $p = i$. Since $\sigma = \mathsf{mgu}(t =^? \mathsf{f}(x_1, \ldots, x_n))$, we deduce that there exists $\ell \in \{1 \ldots, n\}$ such that $x \in vars^1(x_\ell\sigma)$. But $(X_\ell, i \vdash^? x_\ell) \in D(\mathcal{C}_1)$ with $k < i$ and so the result holds.

    Assume now that $X \notin S_2(\mathcal{C})$. If $Z \notin \{X_1, \ldots, X_n\}$ then the proof is similar to the case where $X \in S_2(\mathcal{C})$ and so the result holds. If $X \in \{X_1, \ldots, X_n\}$ then there exists $\ell \in \{1, \ldots, n\}$ such that $x \in vars^1(x_\ell\sigma)$. Since $\sigma = \mathsf{mgu}(t =^? \mathsf{f}(x_1, \ldots, x_n))$, we deduce that $x \in vars^1(t\sigma)$. Hence, there exists z such that $x \in vars^1(z\sigma)$ and $z \in vars^1(t)$. Once again, thanks to $\mathcal{C}$ being well-formed, there exists $(Y, p \vdash^? w') \in D(\mathcal{C})$ such that $p < k$ and $z \in vars^1(w')$ and so $x \in vars^1(w'\sigma)$. But $(Y, p \vdash^? w'\sigma) \in D(\mathcal{C}_1\downarrow)$ thus the result holds.

Case $\textsc{Rule}(\tilde{p}) = \textsc{Axiom}(X, \mathsf{path})$: By definition of $\textsc{Axiom}$, we have $X, i \vdash^? u \in D(\mathcal{C})$ and $\xi, j \rhd v$ in $\Phi(\mathcal{C})$ such that $i \geq j$, $\mathsf{path}(\xi) = \mathsf{path}$ and $(\xi, j \rhd v) \notin \mathsf{NoUse}(\mathcal{C})$. The rule $\textsc{Axiom}$ only adds the inequation $X \neq^? \xi$ on $E_\Pi(\mathcal{C}_2)$. Thus, we have that $\mathcal{C}_2\downarrow = \mathcal{C}_2$ and $\mathcal{C}_2$ trivially satisfies all the properties of Definition 18, except for the property 6. But $E_\Pi(\mathcal{C}_2) = E_\Pi(\mathcal{C}) \wedge X \neq^? \xi$. Since $\mathcal{C}$ is a well-formed constraint system, then $E_\Pi(\mathcal{C})$

satisfies Property 6. Furthermore, $X \neq^? \xi$ also satisfies Property 6 by definition. We can conclude that $\mathcal{C}_2$ is a well-formed constraint system.

On the other hand, we have that $E_\Pi(\mathcal{C}_1) = E_\Pi(\mathcal{C}) \wedge X =^? \xi$, $D(\mathcal{C}_1) = D(\mathcal{C}) \backslash \{X, i \vdash^? u\}$, $E(\mathcal{C}_1) = E(\mathcal{C}) \wedge u =^? v$ and $\Phi(\mathcal{C}) = \Phi(\mathcal{C}_1)$. Let $\sigma = \mathsf{mgu}(u =^? v)$ and $\theta = \mathsf{mgu}(X =^? \xi)$. By hypothesis, $\mathcal{C}$ is a normalized constraint system which means that $(\{X\} \cup vars^2(\xi)) \cap \mathrm{dom}(\mathsf{mgu}(E_\Pi(\mathcal{C}))) = \emptyset$ and $vars^1(u, v) \cap \mathrm{dom}(\mathsf{mgu}(E(\mathcal{C}))) = \emptyset$. Thus, we can deduce $\mathsf{mgu}(E_\Pi(\mathcal{C}_1)) = \mathsf{mgu}(E_\Pi(\mathcal{C}))\theta$ and $\mathsf{mgu}(E(\mathcal{C}_1)) = \mathsf{mgu}(E(\mathcal{C}))\sigma$. Since $\mathcal{C}$ is normalized, we have that $\Phi(\mathcal{C})\mathsf{mgu}(E_\Pi(\mathcal{C}))\mathsf{mgu}(E(\mathcal{C})) = \Phi(\mathcal{C})$ and $D(\mathcal{C})\mathsf{mgu}(E(\mathcal{C})) = D(\mathcal{C})$. Thus, we can deduce that $\Phi(\mathcal{C}_1\downarrow) = \Phi(\mathcal{C})\theta\sigma$ and $D(\mathcal{C}_1\downarrow) = D(\mathcal{C})\sigma \backslash \{X, i \vdash^? u\sigma\}$. We now prove the different properties one by one.

Let $(\zeta, k \rhd w) \in \Phi(\mathcal{C}_1\downarrow)$. Since $\Phi(\mathcal{C}_1\downarrow) = \Phi(\mathcal{C})\theta\sigma$, we know that there exists $(\zeta', k \rhd w') \in \Phi(\mathcal{C})$ such that $\zeta = \zeta'\theta$ and $w = w'\sigma$.

1. this property is direct from Lemma 2 and $\mathcal{C}$ being a well-formed constraint system.

2. this property is direct from Lemma 2 and $\mathcal{C}$ being a well-formed constraint system.

3. We know that $\zeta = \zeta'\theta$ where $\theta = \{X \mapsto \xi\}$. But $\mathcal{C}$ is a well-formed constraint system hence we deduce that $\mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(\xi) \leq j$. Since $\mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(X) = i \geq j \geq \mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(\xi)$, we deduce that $\mathsf{param}^{\mathcal{C}_1\downarrow}_{\mathsf{max}}(\zeta) \leq \mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(\zeta') \leq j$. Hence the result holds.

4. Let $Y \in vars^2(\zeta)$ and $y \in vars^1(Y\delta^1(\mathcal{C}_1\downarrow))$. $Y \in vars^2(D(\mathcal{C}_1\downarrow))$ which means that $Y \in vars^2(D(\mathcal{C}))$. Since $D(\mathcal{C}_1\downarrow) = D(\mathcal{C}_1)\sigma$, $\Phi(\mathcal{C}_1\downarrow) = \Phi(\mathcal{C})\theta\sigma$ and $\mathcal{C}$ is well-formed, we deduce the result.

5. Let λ be a substitution such that for all $Y \in vars^2(\zeta)$, $(Y\lambda)\Phi(\mathcal{C}_1\downarrow)\lambda\downarrow = r\lambda$ where $(Y, \ell \vdash^? r) \in D(\mathcal{C}_1\downarrow)$. Let λ' the substitution such that $\lambda' = \theta\sigma\lambda$. We show that for all $Y \in vars^2(\zeta')$, $(Y\lambda')\Phi(\mathcal{C})\lambda'\downarrow = r\lambda'$ where $(Y, \ell \vdash^? r) \in D(\mathcal{C})$. Let $Y \in vars^2(\zeta')$. Since $\zeta = \zeta'\theta$, we have to distinguish two cases :

   - Either $Y = X$: In this case, we have that $\xi \in st(\zeta)$. Thus, by hypothesis, we have that for all $Z \in vars^2(\xi)$, $(Z\lambda)\Phi(\mathcal{C}_1\downarrow)\lambda\downarrow = t\lambda$, where $(Z, m \vdash^? t) \in D(\mathcal{C}_1\downarrow)$. But $(Z, m \vdash^? t) \in D(\mathcal{C}_1\downarrow)$ implies that there exist t' such that $(Z, m \vdash^? t') \in D(\mathcal{C})$ and $t = t'\sigma$. Since $\Phi(\mathcal{C}_1\downarrow) = \Phi(\mathcal{C})\theta\sigma$, we can deduce that $(Z\lambda)\Phi(\mathcal{C})\lambda'\downarrow = t'\sigma\lambda = t'\lambda'$. At last, $\theta = \{X \mapsto \xi\}$ implies that $Z\theta = Z$ and so $Z\lambda = Z\lambda'$. Thus we have that $(Z\lambda')\Phi(\mathcal{C})\lambda'\downarrow = t\lambda'$. Since $\mathcal{C}$ is a well-formed constraint system, we can deduce that $(\xi\lambda')\Phi(\mathcal{C})\lambda'\downarrow = v\lambda'$. Since $X\theta = \xi$ and $\lambda' = \theta\sigma\lambda$, we have that $\xi\lambda' = X\lambda'$. With $u\sigma = v\sigma$, we can conclude that $(X\lambda')\Phi(\mathcal{C})\lambda'\downarrow = u\lambda'$.
   - Or $Y \in vars^2(\zeta)$: In such a case, we have that $Y\theta\sigma = Y$ and so $Y\lambda' = Y\lambda$. Furthermore, we know that $\Phi(\mathcal{C}_1\downarrow) = \Phi(\mathcal{C})\theta\sigma$ and so $\Phi(\mathcal{C}_1\downarrow)\lambda = \Phi(\mathcal{C})\lambda'$. Thus, we have that $(Y\lambda')\Phi(\mathcal{C})\lambda'\downarrow = (Y\lambda)\Phi(\mathcal{C}_1\downarrow)\lambda\downarrow$. By hypothesis, there exists $Y, \ell \vdash^? r \in D(\mathcal{C}_1\downarrow)$ such that $(Y\lambda)\Phi(\mathcal{C}_1\downarrow)\lambda\downarrow = r\lambda$. However, we have that $D(\mathcal{C}_1\downarrow) = D(\mathcal{C})\sigma \backslash \{X, i \vdash^? u\sigma\}$ and $Y \neq X$. Thus there exists $Y, \ell \vdash^? r' \in D(\mathcal{C})$ such that $r = r'\sigma$ and so $r\lambda = r'\lambda'$. We can conclude that $(Y\lambda')\Phi(\mathcal{C})\lambda'\downarrow = r'\lambda'$ with $Y, \ell \vdash^? r' \in D(\mathcal{C})$.

By hypothesis, we know that $\mathcal{C}$ is well-formed and so $(\zeta'\lambda')(\Phi(\mathcal{C})\lambda')\downarrow = w'\lambda'$. We have that $\zeta'\lambda' = \zeta\lambda$, $w'\lambda' = w\lambda$ and $\Phi(\mathcal{C})\lambda' = \Phi(\mathcal{C}_1\downarrow)\lambda$. Thus we conclude that $(\zeta\lambda)\Phi(\mathcal{C}_1\downarrow)\lambda = w\lambda$.

6. Let $(\zeta_1 \neq^? \zeta_2) \in E_\Pi(\mathcal{C}_1\downarrow)$. By the normalisation, we know that there exists $(\zeta_1' \neq^? \zeta_2') \in E_\Pi(\mathcal{C}_1)$ such that $\zeta_1'\theta = \zeta_1$ and $\zeta_2'\theta = \zeta_2$. Moreover, by the rule Axiom, the sets of inequations of $E_\Pi(\mathcal{C})$ and $E_\Pi(\mathcal{C}_1)$ are the same thus $(\zeta_1' \neq^? \zeta_2') \in E_\Pi(\mathcal{C})$. Since $\mathcal{C}$ is well formed, we deduce that $\zeta_1' \in \mathcal{X}^2$ and there exists $k \in \mathbb{N}$ and a term u such that $(\zeta_2', k \rhd u) \in \Phi(\mathcal{C})$. Since $\Phi(\mathcal{C}_1\downarrow) = \Phi(\mathcal{C})\theta\sigma$, we deduce that $(\zeta_2, k \rhd u\sigma) \in \Phi(\mathcal{C}_1\downarrow)$.

   But thanks to $\mathcal{C}$ being well-formed (Property 1), $\mathsf{path}(\zeta_2')$ and $\mathsf{path}(\xi)$ exists, are closed and if $\mathsf{path}(\zeta_2') = \mathsf{path}(\xi')$ then $\zeta_2' = \xi'$. But $\xi = \xi'\theta$, $\zeta_2 = \zeta_2'\theta$ $\mathsf{path}(\zeta_2') = \mathsf{path}(\zeta_2)$ and $\mathsf{path}(\xi) = \mathsf{path}(\xi')$. Thus we deduce that $\zeta_2 = \xi$ implies that $\zeta_1 \neq \xi$ otherwise $\mathcal{C}_1\downarrow = \bot$ by the normalisation rule.

   Moreover, by definition of the path of recipe, $\mathsf{path}(\xi) \neq \mathsf{path}(\zeta_2)$ implies $\xi \neq \zeta_2$. Thus we deduce that $\zeta_1 \neq \xi$ otherwise the inequation would have disappeared by the normalisation rule. Thus $\zeta_1 \in \mathcal{X}^2$ and so the result holds.

7. Let $Y \in vars^2(\mathcal{C}_1\downarrow)$. We have $\mathsf{mgu}(E_\Pi(\mathcal{C}_1\downarrow)) = \mathsf{mgu}(E_\Pi(\mathcal{C}))\theta$ with $\theta = \{X \mapsto \xi\}$. Furthermore, we know that $\mathsf{path}(\xi) \in \mathcal{F}_d^* \cdot \mathcal{AX}$ since $\mathcal{C}$ is well-formed. Let $\Theta = \{X \mapsto \mathsf{path}(\xi)\}$. By Lemma 3, we have that $\mathsf{C}\lfloor Y\mathsf{mgu}(E_\Pi(\mathcal{C}_1\downarrow))\rfloor_{\Phi(\mathcal{C}_1\downarrow)} = \mathsf{C}\lfloor Y\mathsf{mgu}(E_\Pi(\mathcal{C}))\rfloor_{\Phi(\mathcal{C}_1\downarrow)}\Theta$. However, $\mathsf{C}\lfloor Y\mathsf{mgu}(E_\Pi(\mathcal{C}))\rfloor_{\Phi(\mathcal{C}_1\downarrow)} = \mathsf{C}\lfloor Y\mathsf{mgu}(E_\Pi(\mathcal{C}))\rfloor_{\Phi(\mathcal{C})}$ and since $\mathcal{C}$ is well-formed, we also have that $\mathsf{C}\lfloor Y\mathsf{mgu}(E_\Pi(\mathcal{C}))\rfloor_{\Phi(\mathcal{C})} \in \mathcal{T}(\mathcal{F}_c, \mathcal{F}_d^* \cdot \mathcal{AX} \cup \mathcal{X}^2)$. Since $\mathsf{path}(\xi) \in \mathcal{F}_d^* \cdot \mathcal{AX}$, we conclude that $\mathsf{C}\lfloor Y\mathsf{mgu}(E_\Pi(\mathcal{C}_1\downarrow))\rfloor_{\Phi(\mathcal{C}_1\downarrow)} \in \mathcal{T}(\mathcal{F}_c, \mathcal{F}_d^* \cdot \mathcal{AX} \cup \mathcal{X}^2)$.

   Let $\zeta \in st(Y\mathsf{mgu}(E_\Pi(\mathcal{C}_1\downarrow))$ such that $\mathsf{path}(\zeta) \in \mathcal{F}_d^* \cdot \mathcal{AX}$. Since $\theta = \{X \mapsto \xi\}$ and $\mathsf{mgu}(E_\Pi(\mathcal{C}_1)) = \mathsf{mgu}(E_\Pi(\mathcal{C}))\theta$, then (a) either $\zeta \in st(\xi)$ with $(\xi, i \rhd v) \in \Phi(\mathcal{C})$ and $(\xi, i \rhd v\sigma) \in \Phi(\mathcal{C}_1\downarrow)$ or (b) there exists $\zeta' \in st(Y\mathsf{mgu}(E_\Pi(\mathcal{C})))$ such that $\zeta = \zeta'\theta$. In both cases, since $\mathcal{C}$ is well-formed (Property 7), then there exists k and u such that $(\zeta', k \rhd u) \in \Phi(\mathcal{C})$. But $\Phi(\mathcal{C}_1\downarrow) = \Phi(\mathcal{C})\theta\sigma$. Hence $(\zeta, k \rhd u\sigma) \in \Phi(\mathcal{C}_1\downarrow)$. Hence the result holds.

8. Assume that $(\zeta, k \rhd w) \in \mathsf{NoUse}(\mathcal{C}_1\downarrow)$. Since $\mathsf{NoUse}(\mathcal{C}_1\downarrow) = \mathsf{NoUse}(\mathcal{C})\theta\sigma$, we have that $(\zeta', k \rhd w') \in \mathsf{NoUse}(\mathcal{C})$. Since $\mathcal{C}$ is well-formed, we deduce that there exists $Y \in vars^2(\mathcal{C})$ such that $\mathsf{C}\lfloor Y\mathsf{mgu}(E_\Pi(\mathcal{C}))\rfloor_{\Phi(\mathcal{C})}\delta^1(\mathcal{C}) = w'$ and $\mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(Y\mathsf{mgu}(E_\Pi(\mathcal{C}))) < k$. We have seen that $\mathsf{C}\lfloor Y\mathsf{mgu}(E_\Pi(\mathcal{C}_1\downarrow))\rfloor_{\Phi(\mathcal{C}_1\downarrow)} = \mathsf{C}\lfloor Y\mathsf{mgu}(E_\Pi(\mathcal{C}))\rfloor_{\Phi(\mathcal{C})}\Theta$ when proving the previous point. We have that $\mathsf{path}(\xi)\delta^1(\mathcal{C})\sigma = v\sigma = u\sigma = X\delta^1(\mathcal{C})\sigma$. Thus, we deduce that $\Theta\delta^1(\mathcal{C})\sigma = \delta^1(\mathcal{C})\sigma$. Furthermore, we know that $D(\mathcal{C}_1\downarrow) = D(\mathcal{C})\sigma\backslash\{X, i \vdash^? u\sigma\}$ and $\Phi(\mathcal{C}_1\downarrow) = \Phi(\mathcal{C})\theta\sigma$ which means that $\delta^1(\mathcal{C})\sigma = \Theta\delta^1(\mathcal{C}_1\downarrow)$. This allows us to conclude that $w = w'\sigma = \mathsf{C}\lfloor Y\mathsf{mgu}(E_\Pi(\mathcal{C}))\rfloor_{\Phi(\mathcal{C})}\delta^1(\mathcal{C})\sigma = \mathsf{C}\lfloor Y\mathsf{mgu}(E_\Pi(\mathcal{C}_1\downarrow))\rfloor_{\Phi(\mathcal{C}_1\downarrow)}\delta^1(\mathcal{C}_1\downarrow)$.

   Lastly, since $\mathcal{C}$ is a well formed constraint system, we know that for all $Z \in vars^2(\xi)$, $\mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(Z) \leq j \leq i = \mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(X)$. Since $Y\mathsf{mgu}(E_\Pi(\mathcal{C}_1\downarrow)) = Y\mathsf{mgu}(E_\Pi(\mathcal{C}))\theta$, then $\mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(Y\mathsf{mgu}(E_\Pi(\mathcal{C}))) < k$ implies that $\mathsf{param}^{\mathcal{C}_1\downarrow}_{\mathsf{max}}(Y\mathsf{mgu}(E_\Pi(\mathcal{C}_1\downarrow))) < k$.

9. Similar to Property 7

10. Let $(Z, k \vdash^? t) \in D(\mathcal{C}_1\downarrow)$. Assume that $Z \notin S_2(\mathcal{C}_1)$ and let $x \in vars^1(u)$. It implies that there exists $(Z, k \vdash^? t') \in D(\mathcal{C})$ such that $t = t'\sigma$. Hence, there exists a variable

z such that $x \in vars^1(z\sigma)$ and $z \in vars^1(t')$. Since $\mathcal{C}$ is well-formed, we deduce that there exists $(Y, p \vdash^? w') \in D(\mathcal{C})$ such that $z \in vars^1(w')$ and $p < k$. Thus $x \in vars^1(w'\sigma)$. If $Y \neq X$ then we deduce that $(Y, p \vdash^? w'\sigma) \in D(\mathcal{C}_1{\downarrow})$ and so the result holds. If $Y = X$, then $u = w'$ and $p = i$. Since $\sigma = \mathsf{mgu}(u =^? v)$, we deduce that $x \in vars^1(v\sigma)$. But $(\xi, j \vdash^? v\sigma) \in \Phi(\mathcal{C}_1{\downarrow})$ with $j \leq i$. Thus by the origination property of a constraint system, there exists $(Y_2, p_2 \vdash^? w_2) \in D(\mathcal{C}_1{\downarrow})$ such that $p_2 < j$ and $x \in vars^1(w_2)$. Since $p_2 < j \leq i < k$ then the result holds.

Case $\textsc{Rule}(\tilde{p}) = \textsc{Dest}(\xi, \ell \to r, i)$: By definition of $\textsc{Dest}$, we have that $(\xi, j \rhd v) \in \Phi(\mathcal{C})$ such that $j \leq i$, $(\xi, j \rhd v) \notin \mathsf{NoUse}(\mathcal{C})$, $X_2, \ldots, X_n$ fresh variables and $\mathsf{f}(u_1, \ldots, u_n) \to w$ a fresh renaming of $\ell \to r$. The rule $\textsc{Dest}$ only adds a non-deducibility constraint in $\mathcal{C}_2$. Hence, we have that $\mathcal{C}_2{\downarrow} = \mathcal{C}_2$ and since $\mathcal{C}$ is well formed, we easily deduce that $\mathcal{C}_2$ is also well-formed.

On the other hand, we have that $D(\mathcal{C}_1) = D(\mathcal{C}) \backslash \{X_2, i \vdash^? u_2;\ \ldots;\ X_n, i \vdash^? u_n\}$, $E(\mathcal{C}_1) = E(\mathcal{C}) \wedge u_1 =^? v$ and $\Phi(\mathcal{C}_1) = \Phi(\mathcal{C}) \cup \{\mathsf{f}(\xi, X_2, \ldots, X_n), i \rhd w\}$. By hypothesis, we know that $\mathcal{C}$ is normalised which means that $vars^1(v) \cap \mathrm{dom}(\mathsf{mgu}(E(\mathcal{C}))) = \emptyset$. Let $\sigma = \mathsf{mgu}(u_1 =^? v)$. Since $\mathsf{f}(u_1, \ldots, u_n) \to w$ is a fresh renaming of $\ell \to r$ and for all $k \in \{1, \ldots, k\}$, $vars^1(u_k) \subseteq vars^1(u_1)$, we can deduce $\mathsf{mgu}(E(\mathcal{C}_1)) = \mathsf{mgu}(E(\mathcal{C}))\sigma$. Furthermore, $\mathcal{C}$ normalised also implies that $\Phi(\mathcal{C})\mathsf{mgu}(E(\mathcal{C})) = \Phi(\mathcal{C})$ and $D(\mathcal{C})\mathsf{mgu}(E(\mathcal{C})) = D(\mathcal{C})$. Thus, we can deduce that $\Phi(\mathcal{C}_1{\downarrow}) = \Phi(\mathcal{C})\sigma \cup \{\mathsf{f}(\xi, X_2, \ldots, X_n) \rhd w\sigma\}$ and $D(\mathcal{C}_1{\downarrow}) = D(\mathcal{C})\sigma \cup \{X_2, i \vdash^? u_2\sigma;\ \ldots, X_n, i \vdash^? u_n\sigma\}$. We now prove the different properties one by one.

Let $(\zeta, k \rhd u) \in \Phi(\mathcal{C}_1{\downarrow})$. Since $\Phi(\mathcal{C}_1{\downarrow}) = \Phi(\mathcal{C})\sigma \cup \{\mathsf{f}(\xi, X_2, \ldots, X_n) \rhd w\sigma\}$, we know that either there exists u' such that $(\zeta, k \rhd u') \in \Phi(\mathcal{C})$ with $u'\sigma = u$, or $(\zeta, k \rhd u) = (\mathsf{f}(\xi, X_2, \ldots, X_n), i \rhd w\sigma)$

1. If $(\zeta, k \rhd u) = (\mathsf{f}(\xi, X_2, \ldots, X_n), i \rhd w\sigma)$, we have that $\mathsf{path}(\zeta) = \mathsf{f} \cdot \mathsf{path}(\xi)$. Since $\mathcal{C}$ is well-formed, we have that $\mathsf{path}(\xi)$ exists and is closed. Thus $\mathsf{path}(\zeta)$ exists and is closed.

   Furthermore, since the rule $\textsc{Dest}$ is never applied if its application is useless, then we deduce that the frame $\Phi(\mathcal{C})$ does not contain $\mathsf{f}(\xi, \zeta_2, \ldots, \zeta_n), j \rhd w'$ and $j \leq i$ and $\mathsf{root}(\ell) = \mathsf{f}$. Thus, with $\mathcal{C}$ being well formed hence satisfies Property 1, we can conclude that for all distinct frame elements $(\xi_1, i_1 \rhd u_1)$ and $(\xi_2, i_2 \rhd u_2)$ in $\Phi(\mathcal{C}_1{\downarrow})$, $\mathsf{path}(\xi_1) \neq \mathsf{path}(\xi_2)$.

2. If $(\zeta, k \rhd u) = (\mathsf{f}(\xi, X_2, \ldots, X_n), i \rhd w\sigma)$, since we know that $(\xi, j \rhd v\sigma) \in \Phi(\mathcal{C}_1{\downarrow})$, the result trivially holds. Otherwise, we have that $(\zeta, k \rhd u') \in \Phi(\mathcal{C})$ and since $\mathcal{C}$ is well-formed, we easily conclude.

3. If $(\zeta, k \rhd u) = \mathsf{f}(\xi, X_2, \ldots, X_n)$ then $\mathsf{param}^{\mathcal{C}_1{\downarrow}}_{\mathsf{max}}(\zeta) = \max(\mathsf{param}^{\mathcal{C}_1{\downarrow}}_{\mathsf{max}}(\xi), i)$. But $\mathsf{param}^{\mathcal{C}_1{\downarrow}}_{\mathsf{max}}(\xi) = \mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(\xi)$ thus since $\mathcal{C}$ is well-formed, we deduce $\mathsf{param}^{\mathcal{C}_1{\downarrow}}_{\mathsf{max}}(\xi) \leq j$. Since $j \leq i$ by definition, we conclude that $\mathsf{param}^{\mathcal{C}_1{\downarrow}}_{\mathsf{max}}(\zeta) = i$ thus the result holds.

4. Let $Y \in vars^2(\zeta)$ and $y \in vars^1(Y\delta^1(\mathcal{C}_1{\downarrow}))$. If $Y \in \{X_2, \ldots, X_n\}$ then $y \in vars^1(v\sigma)$. Indeed, our rewrite rule satisfies $vars^1(u_2, \ldots, u_n) \subseteq vars^1(u_1)$ thus with $\sigma = \mathsf{mgu}(u_1, v)$ and $y \in vars^1(u_2\sigma, \ldots, u_n\sigma)$ the result holds.

If $Y \notin \{X_2, \ldots, X_n\}$ then $Y \in vars^2(D(\mathcal{C}))$ and so there exists z such that $y \in vars^1(z\sigma)$ and $z \in vars^1(Y\delta^1(\mathcal{C}))$. Since $\mathcal{C}$ is well-formed, we deduce that there exists $(\beta, m \rhd t) \in \Phi(\mathcal{C})$ such that $m \leq k$ and $z \in vars^1(t)$. But $(\beta, m \rhd t\sigma) \in \Phi(\mathcal{C}_1\downarrow)$ hence $y \in vars^1(t\sigma)$. Thus the result holds.

5. Let λ be a substitution such that for all $Y \in vars^2(\zeta)$, we have that $(Y\lambda)\Phi(\mathcal{C}_1\downarrow)\lambda\downarrow = r\lambda$ where $(Y, k \vdash^? r) \in D(\mathcal{C}_1\downarrow)$. Let $\lambda' = \sigma\lambda$. Actually, $Y \in vars^2(\zeta)$ and $(\zeta, k \rhd u') \in \Phi(\mathcal{C})$ implies that there exists r' such that $(Y, k \vdash^? r') \in D(\mathcal{C})$ and $r'\sigma = r$. Since $Y\sigma\lambda = Y\lambda$ and $\Phi(\mathcal{C}_1\downarrow) = \Phi(\mathcal{C})\sigma \cup \{\mathsf{f}(\xi, X_2, \ldots, X_n) \rhd w\sigma\}$, we can deduce that $(Y\lambda')\Phi(\mathcal{C})\sigma\lambda\downarrow = (Y\lambda')\Phi(\mathcal{C})\lambda'\downarrow = r'\lambda'$. Since $\mathcal{C}$ is well-formed, we have that $(\zeta\lambda')(\Phi(\mathcal{C})\lambda')\downarrow = u'\lambda'$. Since $\zeta\sigma\lambda = \zeta\lambda$ and $u'\lambda' = u\lambda$, we can deduce that $(\zeta\lambda)\Phi(\mathcal{C}_1\downarrow)\lambda\downarrow = u\lambda$.

6. $E_\Pi(\mathcal{C}_1\downarrow) = E_\Pi(\mathcal{C})$ thus the result trivially holds.

7. Let $X \in vars^2(\mathcal{C}_1\downarrow)$. We have that $E_\Pi(\mathcal{C}_1\downarrow) = E_\Pi(\mathcal{C})$. Let $\theta = \mathsf{mgu}(E_\Pi(\mathcal{C}))$. We show that $\mathsf{C}\lfloor X\theta \rfloor_{\Phi(\mathcal{C}_1\downarrow)} \in \mathcal{T}(\mathcal{F}_c, \mathcal{F}_d^* \cdot \mathcal{A}\mathcal{X} \cup \mathcal{X}^2)$. If $X \in \{X_2, \ldots, X_n\}$, then the result trivially holds. Otherwise, we have that $X \in vars^2(\mathcal{C})$. Since $\mathcal{C}$ is a well-formed constraint system, we know that $\mathsf{C}\lfloor X\theta \rfloor_{\Phi(\mathcal{C})} \in \mathcal{T}(\mathcal{F}_c, \mathcal{F}_d^* \cdot \mathcal{A}\mathcal{X} \cup \mathcal{X}^2)$. Thus for all $\xi' \in st(\mathsf{C}\lfloor X\theta \rfloor_{\Phi(\mathcal{C})})$, $\mathsf{root}(\xi') \notin \mathcal{F}_d$. Since $\Phi(\mathcal{C}_1\downarrow) = \Phi(\mathcal{C})\sigma \cup \{\mathsf{f}(\xi, X_2, \ldots, X_n) \rhd w\sigma\}$ and $\mathsf{f} \in \mathcal{F}_d$, we conclude that $\mathsf{C}\lfloor X\theta \rfloor_{\Phi(\mathcal{C}_1\downarrow)} = \mathsf{C}\lfloor X\theta \rfloor_{\Phi(\mathcal{C})} \in \mathcal{T}(\mathcal{F}_c, \mathcal{F}_d^* \cdot \mathcal{A}\mathcal{X} \cup \mathcal{X}^2)$.

   Let $\beta \in st(X\mathsf{mgu}(E_\Pi(\mathcal{C}_1\downarrow)))$ and $\mathsf{path}(\beta) \in \mathcal{F}_d^* \cdot \mathcal{A}\mathcal{X}$. Since $\mathsf{mgu}(E_\Pi(\mathcal{C}_1\downarrow)) = \mathsf{mgu}(E_\Pi(\mathcal{C}))$, then $\beta \in st(X\mathsf{mgu}(E_\Pi(\mathcal{C})))$. Thanks to $\mathcal{C}$ being well-formed, we deduce that there exists k, u such that $(\beta, k \rhd u) \in \Phi(\mathcal{C})$ and so $(\beta, k \rhd u\sigma) \in \Phi(\mathcal{C}_1\downarrow)$. Hence the result holds.

8. Assume that $(\zeta, k \rhd u) \in \mathsf{NoUse}(\mathcal{C}_1\downarrow)$. Since $\mathsf{NoUse}(\mathcal{C}_1\downarrow) = \mathsf{NoUse}(\mathcal{C})\sigma$, we know that there exists u' such that $(\zeta, k \rhd u') \in \Phi(\mathcal{C})$ and $u'\sigma = u$. Since $\mathcal{C}$ is a well formed constraint system, we know that there exists $X \in vars^2(\mathcal{C})$ such that $\mathsf{C}\lfloor X\theta \rfloor_{\Phi(\mathcal{C})}\delta^1(\mathcal{C}) = u'$ and $\mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(X\mathsf{mgu}(E_\Pi(\mathcal{C}))) < k$. Since $\mathsf{mgu}(E_\Pi(\mathcal{C})) = \mathsf{mgu}(E_\Pi(\mathcal{C}_1\downarrow))$ and $D(\mathcal{C})\sigma \subseteq D(\mathcal{C}_1\downarrow)$, we deduce that $\mathsf{param}^{\mathcal{C}_1\downarrow}_{\mathsf{max}}(X\mathsf{mgu}(E_\Pi(\mathcal{C}_1\downarrow))) = \mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(X\mathsf{mgu}(E_\Pi(\mathcal{C}))) < k$

   In the previous point, we have shown that $\mathsf{C}\lfloor X\theta \rfloor_{\Phi(\mathcal{C})} = \mathsf{C}\lfloor X\theta \rfloor_{\Phi(\mathcal{C}_1\downarrow)}$. Furthermore, we have $\delta^1(\mathcal{C}_1\downarrow) = \delta^1(\mathcal{C})\sigma \cup \{\mathsf{f} \cdot \mathsf{path}(\xi) \mapsto w\sigma;\ X_2 \mapsto u_2\sigma;\ \ldots;\ X_n \mapsto u_n\sigma\}$. Actually, $\mathsf{C}\lfloor X\theta \rfloor_{\Phi(\mathcal{C})} = \mathsf{C}\lfloor X\theta \rfloor_{\Phi(\mathcal{C}_1\downarrow)}$ implies that $\mathsf{f}\cdot, \mathsf{path}(\xi), X_2, \ldots, X_n \notin st(\mathsf{C}\lfloor X\theta \rfloor_{\Phi(\mathcal{C}_1\downarrow)})$. Hence, we have that $\mathsf{C}\lfloor X\theta \rfloor_{\Phi(\mathcal{C}_1\downarrow)}\delta^1(\mathcal{C}_1\downarrow) = \mathsf{C}\lfloor X\theta \rfloor_{\Phi(\mathcal{C})}\delta^1(\mathcal{C})\sigma = u'\sigma = u$.

9. Similar to Property 7

10. Let $(Z, k \vdash^? u) \in D(\mathcal{C}_1\downarrow)$. Assume that $Z \notin S_2(\mathcal{C}_1)$ and let $x \in vars^1(u)$. If $Z \notin \{X_2, \ldots, X_n\}$ then there exists $(Z, k \vdash^? u') \in D(\mathcal{C})$ such that $u = u'\sigma$. There exists a variable z such that $x \in vars^1(z\sigma)$ and $z \in vars^1(u')$. Since $\mathcal{C}$ is well-formed, we deduce that there exists $(Y, p \vdash^? t') \in D(\mathcal{C})$ such that $z \in vars^1(t')$ and $k < p$. Thus $x \in vars^1(t'\sigma)$. But $(Y, p \vdash^? t'\sigma) \in D(\mathcal{C}_1\downarrow)$ hence the result holds.

    If $Z \in \{X_2, \ldots, X_n\}$ then there exists $\ell \in \{2, \ldots, n\}$ such that $x \in vars^1(x_\ell\sigma)$. Since $\sigma = \mathsf{mgu}(u_1 =^? v)$, $\mathsf{f}(u_1, \ldots, u_n) \to w$ is a renaming of $\ell \to r$ and $vars^1(u_\ell) \subseteq$

$vars^1(u_1)$, we deduce that $x \in vars^1(v\sigma)$. By the origination property of a constraint system, $(\xi, j \rhd v\sigma) \in \Phi(\mathcal{C}_1{\downarrow})$ and $x \in vars^1(v\sigma)$ implies that there exists $(Y, p \vdash^? t) \in D(\mathcal{C}_1{\downarrow})$ such that $p < j$ and $x \in vars^1(t)$. But $j \leq i$ hence $p < i = k$ and so the result holds.

Case $\text{RULE}(\tilde{p}) = \text{EQ-FRAME-FRAME}(\xi_1, \xi_2)$: The rule EQ-FRAME-FRAME only adds the inequation $u_1 \neq^? u_2$ in $\mathcal{C}_2$. Since $\mathcal{C}$ is well-formed, we easily deduce that $\mathcal{C}_2{\downarrow}$ is also well-formed.

On the other hand, we have that $\Phi(\mathcal{C}_1) = \Phi(\mathcal{C})$, $D(\mathcal{C}_1) = D(\mathcal{C})$, $\mathsf{NoUse}(\mathcal{C}_1) = \mathsf{NoUse}(\mathcal{C})$, $E_\Pi(\mathcal{C}) = E_\Pi(\mathcal{C}_1)$ and $E(\mathcal{C}_1) = E(\mathcal{C}) \wedge u_1 =^? u_2$. Since $\mathcal{C}$ is a well formed constraint, we have $vars^1(u_1, u_2) \cap \text{dom}(\mathsf{mgu}(E(\mathcal{C}))) = \emptyset$. Let $\sigma = \mathsf{mgu}(u_1 =^? u_2)$. We have that $\Phi(\mathcal{C}_1{\downarrow}) = \Phi(\mathcal{C})\sigma$, $D(\mathcal{C}_1{\downarrow}) = D(\mathcal{C})\sigma$ and $\mathsf{NoUse}(\mathcal{C}_1{\downarrow}) = \mathsf{NoUse}(\mathcal{C})\sigma$. We have also that $\delta^1(\mathcal{C}_1{\downarrow}) = \delta^1(\mathcal{C})\sigma$. Thus, we easily deduce that $\mathcal{C}_1{\downarrow}$ is a well-formed constraint system.

Case $\text{RULE}(\tilde{p}) = \text{EQ-FRAME-DED}(\xi_1, X_2)$: This case is similar to the rule EQ-FRAME-FRAME. Let $\sigma = \mathsf{mgu}(u_1 =^? u_2)$. We have that $\Phi(\mathcal{C}_1{\downarrow}) = \Phi(\mathcal{C})\sigma$, $D(\mathcal{C}_1{\downarrow}) = D(\mathcal{C})\sigma$ and $\delta^1(\mathcal{C}_1{\downarrow}) = \delta^1(\mathcal{C})\sigma$. On the other hand, we have that $\mathsf{NoUse}(\mathcal{C}_1{\downarrow}) = \mathsf{NoUse}(\mathcal{C})\sigma \cup \{\xi_1, i_1 \rhd u_1\sigma\}$. Thus $\mathcal{C}_1$ easily satisfies all the properties of Definition 18 except the property 8. We know that $u_1\sigma = u_2\sigma$ and $X_2, i_2 \vdash^? u_2\sigma \in D(\mathcal{C}_1{\downarrow})$. Furthermore, since $\mathcal{C}$ is normalised, we have that $X_2\mathsf{mgu}(E_\Pi(\mathcal{C})) = X_2\mathsf{mgu}(E_\Pi(\mathcal{C}_1{\downarrow})) = X_2$ and so $\mathsf{C}\lfloor X_2\mathsf{mgu}(E_\Pi(\mathcal{C}_1{\downarrow}))\rfloor_{\Phi(\mathcal{C}_1{\downarrow})} = X_2$. Lastly, since $X_2\delta^1(\mathcal{C}_1) = u_2\sigma$, we deduce that $\mathsf{C}\lfloor X_2\mathsf{mgu}(E_\Pi(\mathcal{C}_1{\downarrow}))\rfloor_{\Phi(\mathcal{C}_1{\downarrow})}\delta^1(\mathcal{C}_1{\downarrow}) = u_1\sigma$. Moreover, by definition of the rule EQ-FRAME-DED, $i_1 > i_2$ hence we deduce that $\mathsf{param}^{\mathcal{C}_1{\downarrow}}_{\mathsf{max}}(X_2) < i_1$.

For any frame element other than $(\xi_1, i_1 \rhd u_1\sigma)$ the result holds since $\mathcal{C}$ is well-formed, $\Phi(\mathcal{C}_1{\downarrow}) = \Phi(\mathcal{C})\sigma$, $D(\mathcal{C}_1{\downarrow}) = D(\mathcal{C})\sigma$ and $\delta^1(\mathcal{C}_1{\downarrow}) = \delta^1(\mathcal{C})\sigma$.

Case $\text{RULE}(\tilde{p}) = \text{EQ-DED-DED}(X, \xi)$: By definition of the rule EQ-DED-DED, we have that $X, i \vdash^? u \in D(\mathcal{C})$, $\xi \in \mathcal{T}(\mathcal{F}_c, vars^2(D(\mathcal{C}))$, and $\xi\delta^1(\mathcal{C}) = v$. The rule EQ-DED-DED only adds the insequation $u \neq^? v$ in $E(\mathcal{C}_2)$. Thus, we have that $\mathcal{C}_2{\downarrow} = \mathcal{C}_2$. Since $\mathcal{C}$ is well-formed, we also have that $\mathcal{C}_2{\downarrow}$ is a well-formed constraint system.

On the other hand, we have that $E_\Pi(\mathcal{C}_1) = E_\Pi(\mathcal{C}) \wedge X =^? \xi$, $D(\mathcal{C}_1) = D(\mathcal{C}) \setminus \{X, i \vdash^? u\}$, $E(\mathcal{C}_1) = E(\mathcal{C}) \wedge u =^? v$ and $\Phi(\mathcal{C}) = \Phi(\mathcal{C}_1)$. By hypothesis, $\mathcal{C}$ is normalised which means that $(\{X\} \cup vars^2(\xi)) \cap \text{dom}(\mathsf{mgu}(E_\Pi(\mathcal{C}))) = \emptyset$ and $vars^1(u, v) \cap \text{dom}(\mathsf{mgu}(E(\mathcal{C}))) = \emptyset$. Let $\sigma = \mathsf{mgu}(u =^? v)$ and $\theta = \mathsf{mgu}(X =^? \xi)$. We deduce that $\mathsf{mgu}(E_\Pi(\mathcal{C}_1)) = \mathsf{mgu}(E_\Pi(\mathcal{C}))\theta$ and $\mathsf{mgu}(E(\mathcal{C}_1)) = \mathsf{mgu}(E(\mathcal{C}))\sigma$. Furthermore, since $\mathcal{C}$ is normalized, we have that $\Phi(\mathcal{C})\mathsf{mgu}(E_\Pi(\mathcal{C}))\mathsf{mgu}(E(\mathcal{C})) = \Phi(\mathcal{C})$ and $D(\mathcal{C})\mathsf{mgu}(E(\mathcal{C})) = D(\mathcal{C})$. Thus, we can deduce that $\Phi(\mathcal{C}_1{\downarrow}) = \Phi(\mathcal{C})\theta\sigma$ and $D(\mathcal{C}_1{\downarrow}) = D(\mathcal{C})\sigma \setminus \{X, i \vdash^? u\sigma\}$. We now prove the different properties one by one.

Let $(\zeta, k \rhd w) \in \Phi(\mathcal{C}_1{\downarrow})$. Since $\Phi(\mathcal{C}_1{\downarrow}) = \Phi(\mathcal{C})\theta\sigma$, we know that there exists $(\zeta', k \rhd w') \in \Phi(\mathcal{C})$ such that $\zeta = \zeta'\theta$ and $w = w'\sigma$.

1. this property is direct from Lemma 2 and $\mathcal{C}$ being a well-formed constraint system.
2. this property is direct from Lemma 2 and $\mathcal{C}$ being a well-formed constraint system.
3. We know that $\zeta = \zeta'\theta$ where $\theta = \mathsf{mgu}(X =^? \xi)$. By definition of the rule EQ-DED-DED, $\mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(\xi) \leq \mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(X) = i$. Since $\mathcal{C}$ is a well-formed constraint system hence we deduce that $\mathsf{param}^{\mathcal{C}_1{\downarrow}}_{\mathsf{max}}(\zeta'\theta) \leq \mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(\zeta') \leq j$. Hence the result holds.

4. Let $Y \in vars^2(\zeta)$ and $y \in vars^1(Y\delta^1(\mathcal{C}_1\downarrow))$. $Y \in vars^2(D(\mathcal{C}_1\downarrow))$ implies that $Y \in vars^2(D(\mathcal{C}))$. Since $D(\mathcal{C})\sigma \subseteq D(\mathcal{C}_1\downarrow)$, we deduce that there exists $z \in vars^1(Y\delta^1(\mathcal{C}))$ such that $y \in vars^1(z\sigma)$. Since $\mathcal{C}$ is well-formed, we deduce that there exists $(\beta, j \rhd v) \in \Phi(\mathcal{C})$ such that $j \leq k$ and $z \in vars^1(v)$. Hence $(\beta\theta, j \rhd v\sigma) \in \Phi(\mathcal{C}_1\downarrow)$ and $y \in vars^1(v\sigma)$. Thus the result holds.

5. Let λ be a substitution such that for all $Y \in vars^2(\zeta)$, $(Y\lambda)\Phi(\mathcal{C}_1\downarrow)\lambda\downarrow = r\lambda$ where $(Y, \ell \vdash^? r) \in D(\mathcal{C}_1\downarrow)$. Let λ' the substitution such that $\lambda' = \theta\sigma\lambda$. We show that for all $Y \in vars^2(\zeta')$, $(Y\lambda')\Phi(\mathcal{C})\lambda'\downarrow = r\lambda'$ where $(Y, \ell \vdash^? r) \in D(\mathcal{C})$. Let $Y \in vars^2(\zeta')$. Since $\zeta = \zeta'\theta$, we have to distinguish two cases :

   - Either $Y = X$: In this case, we have that $\xi \in st(\zeta)$. Thus, by hypothesis, we have that for all $Z \in vars^2(\xi)$, $(Z\lambda)\Phi(\mathcal{C}_1\downarrow)\lambda\downarrow = t\lambda$, where $(Z, m \vdash^? t) \in D(\mathcal{C}_1\downarrow)$. But $(Z, m \vdash^? t) \in D(\mathcal{C}_1\downarrow)$ implies that there exist t' such that $(Z, m \vdash^? t') \in D(\mathcal{C})$ and $t = t'\sigma$. Since $\Phi(\mathcal{C}_1\downarrow) = \Phi(\mathcal{C})\theta\sigma$, we deduce that $(Z\lambda)\Phi(\mathcal{C})\lambda'\downarrow = t'\sigma\lambda = t'\lambda'$. Moreover, $\theta = \{X \mapsto \xi\}$ implies that $Z\theta = Z$ and so $Z\lambda = Z\lambda'$. Thus we have $(Z\lambda')\Phi(\mathcal{C})\lambda'\downarrow = t'\lambda' = Z\delta^1(\mathcal{C})\lambda'$. Since $\xi \in \mathcal{T}(\mathcal{F}_c, vars^2(D(\mathcal{C})))$, we deduce that $(\xi\lambda')\Phi(\mathcal{C})\lambda'\downarrow = \xi\delta^1(\mathcal{C})\lambda' = v\lambda'$. Since $X\theta = \xi$ and $\lambda' = \theta\sigma\lambda$, we have that $\xi\lambda' = X\lambda'$. With $u\sigma = v\sigma$, we can conclude that $(X\lambda')\Phi(\mathcal{C})\lambda'\downarrow = u\lambda'$.
   - Or $Y \in vars^2(\zeta)$: In such a case, we have that $Y\theta\sigma = Y$ and so $Y\lambda' = Y\lambda$. Furthermore, we know that $\Phi(\mathcal{C}_1\downarrow) = \Phi(\mathcal{C})\theta\sigma$ and so $\Phi(\mathcal{C}_1\downarrow)\lambda = \Phi(\mathcal{C})\lambda'$. Thus, we have that $(Y\lambda')\Phi(\mathcal{C})\lambda'\downarrow = (Y\lambda)\Phi(\mathcal{C}_1\downarrow)\lambda\downarrow$. By hypothesis, there exists $Y, \ell \vdash^? r \in D(\mathcal{C}_1\downarrow)$ such that $(Y\lambda)\Phi(\mathcal{C}_1\downarrow)\lambda\downarrow = r\lambda$. Since $D(\mathcal{C}_1\downarrow) = D(\mathcal{C})\sigma\backslash\{X, i \vdash^? u\sigma\}$ and $Y \neq X$, there exists $Y, \ell \vdash^? r' \in D(\mathcal{C})$ such that $r = r'\sigma$ and so $r\lambda = r'\lambda'$. We can conclude that $(Y\lambda')\Phi(\mathcal{C})\lambda'\downarrow = r'\lambda'$ with $Y, \ell \vdash^? r' \in D(\mathcal{C})$.

   By hypothesis, we know that $\mathcal{C}$ well-formed. Hence, we have that $(\zeta'\lambda')(\Phi(\mathcal{C})\lambda')\downarrow = w'\lambda'$. Since $\zeta'\lambda' = \zeta\lambda$, $w'\lambda' = w\lambda$ and $\Phi(\mathcal{C})\lambda' = \Phi(\mathcal{C}_1\downarrow)\lambda$, we conclude that $(\zeta\lambda)\Phi(\mathcal{C}_1\downarrow)\lambda = w\lambda$.

6. We know that $\xi \in \mathcal{T}(\mathcal{F}_c, \mathcal{A}\mathcal{X})$ hence this case is similar to the proof of Property 6 for the rule Cons.

7. Let $Y \in vars^2(\mathcal{C}_1\downarrow)$. We have $\mathsf{mgu}(E_\Pi(\mathcal{C}_1\downarrow)) = \mathsf{mgu}(E_\Pi(\mathcal{C}))\theta$ with $\theta = \{X \mapsto \xi\}$. Furthermore, we know that $\xi \in \mathcal{T}(\mathcal{F}_c, vars^2(D(\mathcal{C})))$ and so $\mathsf{C}\lfloor\xi\rfloor_{\Phi(\mathcal{C}_1\downarrow)} = \xi \in \mathcal{T}(\mathcal{F}_c, \mathcal{X}^2)$. By Lemma 3, $\mathsf{C}\lfloor Y\mathsf{mgu}(E_\Pi(\mathcal{C}_1\downarrow))\rfloor_{\Phi(\mathcal{C}_1\downarrow)} = \mathsf{C}\lfloor Y\mathsf{mgu}(E_\Pi(\mathcal{C}))\rfloor_{\Phi(\mathcal{C}_1\downarrow)}\theta$. Hence $\mathsf{C}\lfloor Y\mathsf{mgu}(E_\Pi(\mathcal{C}))\rfloor_{\Phi(\mathcal{C}_1\downarrow)} = \mathsf{C}\lfloor Y\mathsf{mgu}(E_\Pi(\mathcal{C}))\rfloor_{\Phi(\mathcal{C})}$ and $\mathsf{C}\lfloor Y\mathsf{mgu}(E_\Pi(\mathcal{C}))\rfloor_{\Phi(\mathcal{C})} \in \mathcal{T}(\mathcal{F}_c, \mathcal{F}_d^*\cdot\mathcal{A}\mathcal{X} \cup \mathcal{X}^2)$ (since $\mathcal{C}$ is well-formed). Since we have $\xi \in \mathcal{T}(\mathcal{F}_c, vars^2(D(\mathcal{C})))$, we conclude that $\mathsf{C}\lfloor Y\mathsf{mgu}(E_\Pi(\mathcal{C}_1\downarrow))\rfloor_{\Phi(\mathcal{C}_1\downarrow)} \in \mathcal{T}(\mathcal{F}_c, \mathcal{F}_d^* \cdot \mathcal{A}\mathcal{X} \cup \mathcal{X}^2)$.

   Let $\zeta \in st(Y\mathsf{mgu}(E_\Pi(\mathcal{C}_1\downarrow)))$ such that $\mathsf{path}(\zeta) \in \mathcal{F}_d^*\cdot\mathcal{A}\mathcal{X}$. We have $\mathsf{mgu}(E_\Pi(\mathcal{C}_1\downarrow)) = \mathsf{mgu}(E_\Pi(\mathcal{C}))\theta$. But $\theta = \mathsf{mgu}(X =^? \xi)$ with $\xi \in \mathcal{T}(\mathcal{F}_c, \mathcal{A}\mathcal{X})$. Hence $\mathsf{path}(\zeta) \in \mathcal{F}_d^*\cdot\mathcal{A}\mathcal{X}$ implies that there exists $\zeta' \in st(Y\mathsf{mgu}(E_\Pi(\mathcal{C})))$ such that $\zeta = \zeta'\theta$. Since $\mathcal{C}$ is well-formed, we deduce that there exists k, w such that $(\zeta', k \rhd w) \in \Phi(\mathcal{C})$. Thus $(\zeta'\theta, k \rhd w\sigma) \in \Phi(\mathcal{C}_1\downarrow)$ and so the result holds.

8. Assume that $(\zeta, k \rhd w) \in \mathsf{NoUse}(\mathcal{C}_1\downarrow)$. Since $\mathsf{NoUse}(\mathcal{C}_1\downarrow) = \mathsf{NoUse}(\mathcal{C})\theta\sigma$, we have that $(\zeta', k \rhd w') \in \mathsf{NoUse}(\mathcal{C})$. Since $\mathcal{C}$ is well-formed, we deduce that there exists

$Y \in vars^2(\mathcal{C})$ such that $\mathsf{C}\lfloor Y\mathsf{mgu}(E_\Pi(\mathcal{C}))\rfloor_{\Phi(\mathcal{C})}\delta^1(\mathcal{C}) = w'$ and $\mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(Y\mathsf{mgu}(E_\Pi(\mathcal{C}))) < k$. As shown in the previous point, we have that $\mathsf{C}\lfloor Y\mathsf{mgu}(E_\Pi(\mathcal{C}_1\downarrow))\rfloor_{\Phi(\mathcal{C}_1\downarrow)} = \mathsf{C}\lfloor Y\mathsf{mgu}(E_\Pi(\mathcal{C}))\rfloor_{\Phi(\mathcal{C})}\theta$. Furthermore, we have $\xi\delta^1(\mathcal{C})\sigma = v\sigma = u\sigma = X\delta^1(\mathcal{C})\sigma$. Thus, we deduce that $\theta\delta^1(\mathcal{C})\sigma = \delta^1(\mathcal{C})\sigma$. Moreover, we know that $D(\mathcal{C}_1\downarrow) = D(\mathcal{C})\sigma\backslash\{X, i \vdash^? u\sigma\}$ and $\Phi(\mathcal{C}_1\downarrow) = \Phi(\mathcal{C})\theta\sigma$ which means that $\delta^1(\mathcal{C})\sigma = \theta\delta^1(\mathcal{C}_1\downarrow)$. We can conclude $\mathsf{C}\lfloor Y\mathsf{mgu}(E_\Pi(\mathcal{C}_1\downarrow))\rfloor_{\Phi(\mathcal{C}_1\downarrow)}\delta^1(\mathcal{C}_1\downarrow) = \mathsf{C}\lfloor Y\mathsf{mgu}(E_\Pi(\mathcal{C}))\rfloor_{\Phi(\mathcal{C})}\delta^1(\mathcal{C})\sigma = w'\sigma = w$. Lastly, for all $Z \in vars^2(\xi)$, $\mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(Z) \leq i = \mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(X)$. Since $Y\mathsf{mgu}(E_\Pi(\mathcal{C}_1\downarrow)) = Y\mathsf{mgu}(E_\Pi(\mathcal{C}))\theta$, we conclude that $\mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(Y\mathsf{mgu}(E_\Pi(\mathcal{C}))) < k$ implies that $\mathsf{param}^{\mathcal{C}_1\downarrow}_{\mathsf{max}}(Y\mathsf{mgu}(E_\Pi(\mathcal{C}_1\downarrow))) < k$.

9. Similar to Property 7

10. Let $(Z, k \vdash^? t) \in D(\mathcal{C}_1\downarrow)$. Assume that $Z \notin S_2(\mathcal{C}_1)$ and let $x \in vars^1(u)$. It implies that there exists $(Z, k \vdash^? t') \in D(\mathcal{C})$ such that $t = t'\sigma$. Hence, there exists a variable z such that $x \in vars^1(z\sigma)$ and $z \in vars^1(t')$. Since $\mathcal{C}$ is well-formed, we deduce that there exists $(Y, p \vdash^? w') \in D(\mathcal{C})$ such that $z \in vars^1(w')$ and $p < k$. Thus $x \in vars^1(w'\sigma)$. If $Y \neq X$ then we deduce that $(Y, p \vdash^? w'\sigma) \in D(\mathcal{C}_1\downarrow)$ and so the result holds. If $Y = X$, then $u = w'$ and $p = i$. Since $\sigma = \mathsf{mgu}(u =^? v)$, we deduce that $x \in vars^1(v\sigma)$. Moreover, by construction of v, it implies that there exists $(Y', p' \vdash^? u') \in D(\mathcal{C}_1\downarrow)$ such that $Y' \in vars^2(\xi)$, $p' \leq i$ and $x \in vars^1(u')$. Since $p' \leq i = p < k$, we deduce that $p' < k$ and so the result holds.

Case $\textsc{Rule}(\tilde{p}) = \textsc{Ded-st}(\xi, \mathsf{f})$: The rule Ded-st only adds a non-deducibility constraint in $\mathcal{C}_2$. Thus, we have that $\mathcal{C}_2\downarrow = \mathcal{C}_2$ and since $\mathcal{C}$ is a well formed constraint system, we easily deduce that $\mathcal{C}_2$ is also well-formed.

On the other hand, we have that $\Phi(\mathcal{C}_1) = \Phi(\mathcal{C})$, $D(\mathcal{C}_1) = D(\mathcal{C}) \cup \{X_1, \mathsf{s}_{max} \vdash^? x_1;\ \ldots;\ X_n, \mathsf{s}_{max} \vdash^? x_n\}$, $\mathsf{NoUse}(\mathcal{C}_1) = \mathsf{NoUse}(\mathcal{C})$, $E_\Pi(\mathcal{C}) = E_\Pi(\mathcal{C}_1)$ and $E(\mathcal{C}_1) = E(\mathcal{C}) \wedge u =^? \mathsf{f}(x_1, \ldots, x_n)$ where $x_1, \ldots, x_n$ are fresh variables. Since $\mathcal{C}$ is well-formed, we deduce that $vars^1(u) \cap \mathrm{dom}(\mathsf{mgu}(E(\mathcal{C}))) = \emptyset$. Let $\sigma = \mathsf{mgu}(u =^? \mathsf{f}(x_1, \ldots, x_n))$. We have that $\Phi(\mathcal{C}_1\downarrow) = \Phi(\mathcal{C})\sigma$ and $D(\mathcal{C}_1\downarrow) = D(\mathcal{C})\sigma \cup \{X_1, \mathsf{s}_{max} \vdash^? x_1\sigma;\ \ldots;\ X_n, \mathsf{s}_{max} \vdash^? x_n\sigma\}$ and $\mathsf{NoUse}(\mathcal{C}_1\downarrow) = \mathsf{NoUse}(\mathcal{C})\sigma$. Since the variables $X_1, \ldots, X_n$ do not appear in the frame, the facts that $\mathcal{C}$ is well-formed and $\sigma = \mathsf{mgu}(u =^? \mathsf{f}(x_1, \ldots, x_n))$ implies that $\mathcal{C}_1\downarrow$ is also a well-formed constraint system. □

Appendix B. Proof of completeness

This section is devoted to completeness whose proof does not rely on our strategy $\mathcal{S}$. As explained in Section 3, our algorithm transforms a pair of matrices of constraint systems into one or two pairs of matrices of constraint systems. The main idea behind the soundness and completeness is to locally prove that our transformation preserves the symbolic equivalence between matrices of constraint systems. Since we have several rules, we will need to prove the local preservation of the symbolic equivalence for each rule.

Let $\mathcal{C} = (S_1; S_2; \Phi; D; E; E_\Pi; ND; \mathsf{NoUse})$ be a constraint system. We denote by $\overline{\mathcal{C}}$ the constraint system $(S_1; S_2; \Phi; D; E; E_\Pi; \emptyset; \mathsf{NoUse})$, *i.e.* the constraint system obtained from $\mathcal{C}$ by removing the non-deducibility constraints. This notation is extended as expected to matrices of constraint systems.

Lemma 5. *Let $\mathcal{C}$ be a normalised and well-formed constraint system and* $\textsc{Rule}(\tilde{p})$ *be a transformation rule applicable on $\mathcal{C}$. Let $\mathcal{C}_1$ and $\mathcal{C}_2$ be the two resulting constraint systems obtained by applying* $\textsc{Rule}(\tilde{p})$ *on $\mathcal{C}$. We denote by Φ, Φ_1 and Φ_2 the respective frames of $\mathcal{C}$, $\mathcal{C}_1$ and $\mathcal{C}_2$ and we denote by S_1 the set of free variable of $\mathcal{C}$.*

For all $i \in \{1,2\}$, for all $(\sigma_i, \theta_i) \in \mathsf{Sol}(\mathcal{C}_i)$, $(\sigma, \theta) \in \mathsf{Sol}(\mathcal{C})$ and $\mathsf{Init}(\Phi)\sigma = \mathsf{Init}(\Phi_i)\sigma_i$ where $\sigma = \sigma_i|_{vars^1(\mathcal{C})}$ and $\theta = \theta_i|_{vars^2(\mathcal{C})}$

Variation: For all $i \in \{1,2\}$, for all $(\sigma_i, \theta_i) \in \mathsf{Sol}(\overline{\mathcal{C}_i})$, $(\sigma, \theta) \in \mathsf{Sol}(\overline{\mathcal{C}})$ and $\mathsf{Init}(\Phi)\sigma = \mathsf{Init}(\Phi_i)\sigma_i$ where $\sigma = \sigma_i|_{vars^1(\overline{\mathcal{C}})}$ and $\theta = \theta_i|_{vars^2(\overline{\mathcal{C}})}$.

Proof. We prove this lemma by case analysis on the transformation rule that is used to transform $\mathcal{C}$ on $\mathcal{C}_1, \mathcal{C}_2$. In each situation where some conditions are added on the resulting constraint system (without modifying the conditions that are already present in $\mathcal{C}$), the result trivially holds. This remark allows one to conclude for the rules Eq-frame-frame, Eq-frame-ded, Ded-st, Dest, and the case $i = 2$ for the rules Cons, Axiom and Eq-ded-ded. Therefore, it remains to prove the result for the remaining cases, *i.e.* rule Cons when $i = 1$, rule Axiom when $i = 1$ and rule Eq-ded-ded when $i = 1$.

Let $\mathcal{C} = (S_1; S_2; \Phi; D; E; E_\Pi; ND; \mathsf{NoUse})$. We consider the remaining cases using the notation introduced in Figure 1.

Rule $\textsc{Cons}(X, \mathsf{f})$, $i = 1$: Assume that $X, k \vdash^? t \in D(\mathcal{C})$ and so $D(\mathcal{C}_1) = \{X_1, k \vdash^? x_1;\ \ldots; X_n, k \vdash^? x_n\} \cup D(\mathcal{C}) \setminus \{X, k \vdash^? t\}$, $E(\mathcal{C}_1) = E(\mathcal{C}) \wedge t =^? \mathsf{f}(x_1, \ldots, x_n)$ and $E_\Pi(\mathcal{C}_1) = E_\Pi(\mathcal{C}) \wedge X =^? \mathsf{f}(X_1, \ldots, X_n)$, $\Phi(\mathcal{C}) = \Phi(\mathcal{C}_1)$ with $x_1, \ldots, x_n$ and $X_1, \ldots, X_n$ fresh variables.

Let $(\sigma_1, \theta_1) \in \mathsf{Sol}(\mathcal{C}_1)$. By definition of a solution of a constraint system, we know that:

1. $(X_j\theta_1)(\Phi(\mathcal{C}_1)\sigma_1)\downarrow = x_j\sigma_1\downarrow$ and $param(X_j\theta_1) \subseteq \{ax_1, \ldots, ax_i\}$ for any $j \in \{1, \ldots, n\}$;
2. $\sigma_1 \models E(\mathcal{C}) \wedge t =^? \mathsf{f}(x_1, \ldots, x_n) \wedge ND(\mathcal{C})$ and so $t\sigma_1\downarrow = \mathsf{f}(x_1\sigma_1, \ldots, x_n\sigma_1)\downarrow$;
3. $\theta_1 \models E_\Pi(\mathcal{C}) \wedge X =^? \mathsf{f}(X_1, \ldots, X_n)$ and so $X\theta_1 = \mathsf{f}(X_1\theta_1, \ldots, X_n\theta_1)$.

Hence, we have that:

$$\begin{array}{rcl}(X\theta_1)(\Phi(\mathcal{C})\sigma_1)\downarrow & = & \mathsf{f}(X_1\theta_1, \ldots, X_n\theta_1)(\Phi(\mathcal{C})\sigma_1)\downarrow \\ & = & \mathsf{f}((X_1\theta_1)\Phi(\mathcal{C})\sigma_1\downarrow, \ldots, (X_n\theta_1)\Phi(\mathcal{C})\sigma_1\downarrow)\downarrow \\ & = & \mathsf{f}(x_1\sigma_1\downarrow, \ldots, x_n\sigma_1\downarrow)\downarrow \\ & = & \mathsf{f}(x_1\sigma_1, \ldots, x_n\sigma_1)\downarrow \\ & = & t\sigma_1\downarrow\end{array}$$

Moreover, thanks to $param(X_j\theta_1) \subseteq \{ax_1, \ldots, ax_i\}$ for $j \in \{1, \ldots, n\}$, we have that $param(X\theta_1) \subseteq \{ax_1, \ldots, ax_i\}$. This allows us to conclude that $(\sigma_1|_{vars^1(\mathcal{C})}, \theta_1|_{vars^2(\mathcal{C})}) \in \mathsf{Sol}(\mathcal{C})$.

Rule $\textsc{Axiom}(X, \mathsf{path})$, $i = 1$. Assume that $(X, k \vdash^? u) \in D(\mathcal{C})$ and $(\xi, j \rhd v) \in \Phi(\mathcal{C})$ with $j \leq k$ and $\mathsf{path}(\xi) = \mathsf{path}$. Thus, we have $E_\Pi(\mathcal{C}_1) = E_\Pi(\mathcal{C}) \wedge X =^? \xi$, $E(\mathcal{C}_1) = E(\mathcal{C}) \wedge u =^? v$, $D(\mathcal{C}_1) = D(\mathcal{C}) \setminus \{(X, k \vdash^? u)\}$ and $\Phi(\mathcal{C}_1) = \Phi(\mathcal{C})$

Let $(\sigma_1, \theta_1) \in \mathsf{Sol}(\mathcal{C}_1)$. By definition of a solution of a constraint system, we know that:

1. $\sigma_1 \models E(\mathcal{C}) \wedge u =^? v \wedge ND(\mathcal{C})$, and so $u\sigma_1 = v\sigma_1$.

2. $\theta_1 \models E_\Pi(\mathcal{C}) \wedge X =^? \xi$, and so $X\theta_1 = \xi\theta_1$.

Hence, we have that $(X\theta_1)(\Phi\sigma_1)\downarrow = (\xi\theta_1)(\Phi\sigma_1)\downarrow$. Moreover, since $\mathcal{C}$ is well-formed (Definition 18, item 3), we deduce that $\mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(\xi) \leq j$ hence for all $Y \in vars^2(\xi)$, there exists $q \leq j$ and w such that $(Y, q \vdash^? w) \in D(\mathcal{C})$. Since X an ξ are unifiable, we also deduce that $X \notin vars^2(\xi)$. Hence $(Y, q \vdash^? w) \in D(\mathcal{C}_1)$. Thanks to $(\sigma_1, \theta_1) \in \mathsf{Sol}(\mathcal{C}_1)$, $Y\theta_1\Phi(\mathcal{C}_1)\sigma_1\downarrow = w\sigma_1$. Hence, thanks to $\mathcal{C}$ being well-formed (Definition 18, item 5) and $\Phi(\mathcal{C}_1) = \Phi(\mathcal{C})$, we deduce that $\xi\theta_1\Phi(\mathcal{C})\sigma_1\downarrow = v\sigma_1 = u\sigma_1$.

At last, since $\mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(\xi) \leq j$ and for all $Y \in vars^2(\xi)$, $(\sigma_1, \theta_1) \in \mathsf{Sol}(\mathcal{C}_1)$ also indicates that $param(Y\theta_1) \subseteq \{ax_1, \ldots, ax_j\}$ and so $param(\xi\theta_1) \subseteq \{ax_1, \ldots, ax_j\}$. At last, with $j \leq k$ and $X\theta_1 = \xi\theta_1$, we conclude that $param(X\theta_1) \subseteq \{ax_1, \ldots, ax_k\}$. This allow us to conclude that $(\sigma_1|_{vars^1(\mathcal{C})}, \theta_1|_{vars^2(\mathcal{C})}) \in \mathsf{Sol}(\mathcal{C})$.

Rule EQ-DED-DED(X, ξ), $i = 1$. Assume that $(X, k \vdash^? u) \in D(\mathcal{C})$ and $\xi \in \mathcal{T}(\mathcal{F}_c, \mathrm{dom}(\alpha))$ with $\alpha = \{Y \to w \mid (Y, j \vdash^? w) \in D(\mathcal{C}) \wedge j \leq i \wedge Y \in S_2\}$. Thus, we have $E_\Pi(\mathcal{C}_1) = E_\Pi(\mathcal{C}) \wedge X =^? \xi$, $E(\mathcal{C}_1) = E(\mathcal{C}) \wedge u =^? v$, $D(\mathcal{C}_1) = D(\mathcal{C}) \setminus \{(X, k \vdash^? u)\}$ and $\Phi(\mathcal{C}_1) = \Phi(\mathcal{C})$.

Let $(\sigma_1, \theta_1) \in \mathsf{Sol}(\mathcal{C}_1)$. By definition of a solution of a constraint system, we know that:

1. $\sigma_1 \models E \wedge u =^? v \wedge ND$, and so $u\sigma_1\downarrow = v\sigma_1\downarrow$.
2. $\theta_1 \models E_\Pi \wedge X =^? \xi$, and so $X\theta_1 = \xi\theta_1$.

Hence, we have that $(X\theta_1)(\Phi(\mathcal{C}_1)\sigma_1)\downarrow = (\xi\theta_1)(\Phi(\mathcal{C}_1)\sigma_1)\downarrow$. Moreover, according to Figure 2, we have that $\xi \in \mathcal{T}(\mathcal{F}_c, \mathrm{dom}(\alpha))$ and $v = \xi\alpha$

Since $(\sigma_1, \theta_1) \in \mathsf{Sol}(\mathcal{C}_1)$, we have that for all $(Y, j \vdash^? w) \in D(\mathcal{C}_1)$, $(Y\theta_1)\Phi(\mathcal{C})\sigma_1\downarrow = w\sigma_1$. Since $\xi \in \mathcal{T}(\mathcal{F}_c, \mathcal{X}^2)$, we can deduce that $(\xi\theta_1)(\Phi(\mathcal{C})\sigma_1)\downarrow = v\sigma_1$. This allows us to deduce that $(X\theta_1)(\Phi(\mathcal{C})\sigma_1)\downarrow = v\sigma_1\downarrow$ and so $(X\theta_1)(\Phi(\mathcal{C})\sigma_1)\downarrow = u\sigma_1\downarrow$. Furthermore, we also know that for all $(Y, j \vdash^? w) \in D$, if $Y \in vars^2(\xi)$, then $j \leq i$ which means that $param(Y\theta_1) \subseteq \{ax_1, \ldots, ax_i\}$. Thus we have:

$$param(X\theta_1) = param(\xi\theta_1) \subseteq \{ax_1, \ldots, ax_i\}.$$

This allows us to conclude that $(\sigma_1|_{vars^1(\mathcal{C})}, \theta_1|_{vars^2(\mathcal{C})}) \in \mathsf{Sol}(\mathcal{C})$. □

Appendix C. Invariants that depends on the strategy

In Appendix A, we described some general invariants, *i.e.* those that does not depend on the strategy. Typically, they are very useful to prove some general properties on constraint systems. However, they are not sufficient to establish soundness of our rules or even the termination. The strategy we described in Section 4 has been essentially designed to ensure termination of our algorithm. However, this strategy also allows us to extract some new invariants that will help us to prove soundness. We start this section by listing these invariants.

Appendix C.1. List of invariants

Among the invariants, some of them are specific to some steps of the strategy. We start by describing the invariants that are satisfied at any step of the strategy.

Invariant 1 (InvGeneral)**.** *Let $\mathcal{M}$ be a matrix of constraint systems. We say that $\mathcal{M}$ satisfies the invariant* InvGeneral*, if and only if:*

For all constraint systems $\mathcal{C}$ in $\mathcal{M}$, if $\mathcal{C} \neq \bot$ then for all $(\sigma, \theta) \in \mathsf{Sol}(\mathcal{C})$, for all $(\xi, i \rhd u) \in \Phi(\mathcal{C})$, we have that:

1. $ax_i \in st(\xi\theta)$.
2. *for all $\xi' \in \Pi_r$ with $\mathsf{root}(\xi') \notin \mathcal{F}_c$, if $\mathsf{path}(\xi') = \mathsf{path}(\xi\theta)$ and $\xi'(\Phi\sigma)\downarrow \in \mathcal{T}(\mathcal{F}_c, \mathcal{N})$, then $param(\xi') \not\subseteq \{ax_1, \ldots, ax_{i-1}\}$.*
3. *for all $X \in vars^2(\mathcal{C})$, if $\mathsf{path}(\xi) \in st(\mathsf{C}\lfloor X\mathsf{mgu}(E_\Pi)\rfloor_\Phi)$ then $(\xi, i \rhd u) \notin \mathsf{NoUse}$.*
4. *if $(\xi, i \rhd u) \notin \mathsf{NoUse}$ then for all $\xi' \in st(\xi)$, if there exists j and v such that $(\xi', j \rhd v) \in \Phi$ then $(\xi', j \rhd v) \notin \mathsf{NoUse}$.*

For all constraint systems $\mathcal{C}$, $\mathcal{C}'$ in a same column of $\mathcal{M}$, if we denote $\theta = \mathsf{mgu}(E_\Pi(\mathcal{C}))$ and $\theta' = \mathsf{mgu}(E_\Pi(\mathcal{C}'))$, then

5. $\forall X \in S_2(\mathcal{C}), \mathsf{C}\lfloor X\theta\rfloor_{\Phi(\mathcal{C})} = \mathsf{C}\lfloor X\theta'\rfloor_{\Phi(\mathcal{C}')}$
6. $\forall X \in S_2(\mathcal{C}), \forall \mathsf{f} \in \mathcal{F}_c$, $E_\Pi(\mathcal{C}) \vDash \mathsf{root}(X) \neq^? \mathsf{f}$ *implies that* $E_\Pi(\mathcal{C}') \vDash \mathsf{root}(X) \neq^? \mathsf{f}$
7. $\forall X \in S_2(\mathcal{C})$, *for all $(\xi, i \rhd u) \in \Phi(\mathcal{C})$, for all $(\xi', i' \rhd u') \in \Phi(\mathcal{C}')$, if $\mathsf{path}(\xi) = \mathsf{path}(\xi')$ then $E_\Pi(\mathcal{C}) \vDash X \neq^? \xi$ is equivalent to $E_\Pi(\mathcal{C}') \vDash X \neq^? \xi'$.*

Typically, items 1 and 2 ensure that we use in the frame the minimal recipes w.r.t. the parameters to deduce the key of a cipher or the verification key of a signature. These two properties are given by the application of the rule Dest (Step a of Phase 1) and more specifically by the fact that the cycle of steps in Phase 1 is applied by increasing support. Items 3 and 4 indicate that during Step a, we always prioritized the application of the rule Eq-frame-ded over Dest. The last three properties established similarities between constraint systems of a same column. We already know that the shape of the constraint systems are the same but the strategy allows us to be even more specific. Indeed, item 5 indicates that the actions of the attacker are the same in each constraint system of a given column (up to the context), and items 6 and 7 also indicate that the inequalities corresponding the attacker's actions are the same. These three properties are in fact due to the application on the external rules on the matrices of constraint system.

The next invariants are more specific to the different steps and phase of the strategy. Thus, they depend on a parameter, *i.e.* the support of the rules.

Invariant 2 (InvVarConstraint(s))**.** *Let $\mathcal{C}$ be a constraint system. We say that $\mathcal{C}$ satisfies* InvVarConstraint(s) *if $\mathcal{C} = \bot$ or*

1. *for all $(X, i \vdash^? u) \in D(\mathcal{C})$, if $i \leq s$ then $u \in \mathcal{X}^1$ and $X \in S_2(\mathcal{C})$; and*
2. *for all $(X, i \vdash^? x), (Y, j \vdash^? y) \in D(\mathcal{C})$, if $i \leq s$, $j \leq s$ and $X \neq Y$ then $x \neq y$.*

Invariant 3 (InvVarFrame(s))**.** *Let $\mathcal{C} = (S_1; S_2; \Phi; D; E; E_\Pi; ND; \mathsf{NoUse})$ be a constraint system. We say that $\mathcal{C}$ satisfies* InvVarFrame(s) *if and only if for all $(\xi, p \rhd v) \in \Phi$, $p \leq s$ implies for all $X \in vars^2(\xi)$, there exists $q < p$ and $u \in \mathcal{T}(\mathcal{F}_c, \mathcal{N} \cup \mathcal{X}^1)$ such that $(X, q \vdash^? u) \in D$.*

Intuitively, $\mathsf{InvVarConstraint}(s)$ corresponds to the purpose of the first phase of the strategy, *i.e.* modifying the constraint systems such that all right hand term of deducible constraints are distinct variables. Thus, all constraint systems during Phase 2 will satisfy this invariant.

Invariant 4 ($\mathsf{InvNoUse}(s)$)**.** *Let $\mathcal{C} = (S_1; S_2; \Phi; D; E; E_\Pi; ND; \mathsf{NoUse})$ be a constraint system. We say that $\mathcal{C}$ satisfies $\mathsf{InvNoUse}(s)$ if and only if for all $(\xi, p \rhd v) \in \Phi$, $p \leq s$ and $v \in \mathcal{X}^1$ implies $(\xi, p \rhd v) \in \mathsf{NoUse}$.*

Invariant 5 ($\mathsf{InvDest}(s)$)**.** *Let $\mathcal{C} = (S_1; S_2; \Phi; D; E; E_\Pi; ND; \mathsf{NoUse})$ be a constraint system. We say that $\mathcal{C}$ satisfies $\mathsf{InvDest}(s)$ if and only if for all $(\xi, p \rhd v) \in \Phi$, for all $\mathsf{f} \in \mathcal{F}_d$, $(\xi, p \rhd v) \notin \mathsf{NoUse}$ and $p \leq s$ implies:*

- *either there exists $p' \in \mathbb{N}$ such that*
  - *$s \geq p' \geq p$; and*
  - *$(\xi', p' \rhd v') \in \Phi$ for some ξ' such that $\mathsf{path}(\xi') = \mathsf{f} \cdot \mathsf{path}(\xi)$; and*
  - *for every $p \leq k < p'$, for all σ, $\sigma \vDash ND$ implies that $\sigma \vDash \forall \tilde{x}, v \neq u_1 \vee k \not\vdash^? u_2 \vee \ldots \vee k \not\vdash^? u_n$ where $\mathsf{f}(u_1, \ldots, u_n) \to w$ is a fresh rewriting rule with $vars^1(u_1, \ldots, u_n, w) = \tilde{x}$.*
- *or else for every $p \leq k \leq s$, we have that*

$$ND \vDash \forall \tilde{x}, v \neq u_1 \vee k \not\vdash^? u_2 \vee \ldots \vee k \not\vdash^? u_n$$

  where $\mathsf{f}(u_1, \ldots, u_n) \to w$ is a fresh rewriting rule with $vars^1(u_1, \ldots, u_n, w) = \tilde{x}$.

Invariant 6 ($\mathsf{InvDedsub}$)**.** *Let $\mathcal{C} = (S_1; S_2; \Phi; D; E; E_\Pi; ND; \mathsf{NoUse})$ be a constraint system. Let $\theta = \mathsf{mgu}(E_\Pi)$. We say that $\mathcal{C}$ satisfies $\mathsf{InvDedsub}$ if and only if, for all $(\xi, p \rhd v) \in \Phi$, for all $\mathsf{f} \in \mathcal{F}_c$, $(\xi, p \rhd v) \notin \mathsf{NoUse}$ implies:*

- *either there exist $X_1, \ldots, X_n \in vars^2(\mathcal{C})$ such that:*

$$\text{for all } i \in \{1, \ldots, n\},\ \mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(X_i\theta) \leq \mathsf{s}_{max} \text{ and } \mathsf{C}\lfloor \mathsf{f}(X_1, \ldots, X_n)\theta \rfloor_\Phi \delta^1(\mathcal{C}) = v$$

- *or else $ND \vDash \forall \tilde{x}, v \neq \mathsf{f}(x_1, \ldots, x_n) \vee \mathsf{s}_{max} \not\vdash^? x_1 \vee \ldots \vee \mathsf{s}_{max} \not\vdash^? x_n$ where $\tilde{x} = x_1 \ldots x_n$ are fresh.*

Typically, $\mathsf{InvDest}(s)$ ensures that no new subterm can be obtained by applying a destructor while $\mathsf{InvDedsub}$ ensures that no new subterm can be obtained by applying a constructor. The invariants $\mathsf{InvDest}(s)$ and $\mathsf{InvNoUse}(s)$ will be satisfied by any constraint system after Step a of Phase 1 with support s.

The next invariant indicates that no rule was applied with support strictly greater than s. Typically, it is satisfied by all constraint systems during Phase 1 with support smaller than s.

Invariant 7 ($\mathsf{InvUntouched}(s)$)**.** *Let $\mathcal{C} = (S_1; S_2; \Phi; D; E; E_\Pi; ND; \mathsf{NoUse})$ be a constraint system. We say that $\mathcal{C}$ satisfies $\mathsf{InvUntouched}(s)$ if and only if*

1. *for all $(\xi, k \rhd u) \in \Phi$, if $s < k$ then $\xi = ax_k$; and*

2. for all $(X, k \vdash^? u) \in D$*, if* $s < k$ *then* $X \in S_2$ *and* $X \notin vars^2(E_\Pi)$*.*

Lastly, we define an invariant that impacts on several constraint systems in the matrices.

Invariant 8 ($\mathsf{InvMatrix}(s)$)**.** *Let* $\mathcal{M}$ *be a matrix of constraint systems. We say that* $\mathcal{M}$ *satisfies* $\mathsf{InvMatrix}(s)$ *if and only if for all* $\mathcal{C}$*,* $\mathcal{C}'$ *two constraint systems in the same column of* $\mathcal{M}$*,*

- $\{\mathsf{path}(\xi), i \mid (\xi, i \rhd u) \in \Phi(\mathcal{C}) \wedge i \leq s\} = \{\mathsf{path}(\xi), i \mid (\xi, i \rhd u) \in \Phi(\mathcal{C}') \wedge i \leq s\}$
- $\{\mathsf{path}(\xi), i \mid (\xi, i \rhd u) \in \mathsf{NoUse}(\mathcal{C}) \wedge i \leq s\} = \{\mathsf{path}(\xi), i \mid (\xi, i \rhd u) \in \mathsf{NoUse}(\mathcal{C}') \wedge i \leq s\}$

The remaining of this appendix will be dedicated to stating and proving which invariants are satisfied at each step and phase of the algorithm

Appendix C.2. Preliminaries

We write $\mathcal{C} \to^* \mathcal{C}'$ when $\mathcal{C}'$ is obtained from $\mathcal{C}$ by applying a sequence of transformation rules.

Lemma 6. *Let* $\mathcal{C}$ *and* $\mathcal{C}'$ *be two normalised well-formed constraint systems such that* $\mathcal{C} \to^* \mathcal{C}'$*. Let* $\theta = \mathsf{mgu}(E_\Pi(\mathcal{C}))$*,* $\theta' = \mathsf{mgu}(E_\Pi(\mathcal{C}'))$ *and* $\sigma' = \mathsf{mgu}(E(\mathcal{C}'))$*. The following property holds: for all* $X \in vars^2(\mathcal{C})$*,* $\mathsf{C}\lfloor X\theta \rfloor_\Phi \delta^1(\mathcal{C})\sigma' = \mathsf{C}\lfloor X\theta' \rfloor_{\Phi'} \delta^1(\mathcal{C}')$ *and* $\mathsf{param}^{\mathcal{C}'}_{\mathsf{max}}(X\theta') \leq \mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(X\theta)$*.*

Proof. We prove this result by induction on the length N of the derivation $\mathcal{C} \to^* \mathcal{C}'$.

Base case $N = 0$*:* In such a case, $\mathcal{C} = \mathcal{C}'$. Thus, we have that $\theta = \theta'$ and $\delta^1(\mathcal{C}) = \delta^1(\mathcal{C}')$. Therefore, we have for all $X \in vars^2(\mathcal{C})$, $\mathsf{C}\lfloor X\theta \rfloor_\Phi \delta^1(\mathcal{C})\sigma' = \mathsf{C}\lfloor X\theta' \rfloor_{\Phi'} \delta^1(\mathcal{C}')\sigma'$. Since $\mathcal{C}$ is normalised, we have that $\mathrm{dom}(\sigma') \cap \mathrm{img}(\delta^1(\mathcal{C}')) = \emptyset$, which means that $\mathsf{C}\lfloor X\theta' \rfloor_{\Phi'} \delta^1(\mathcal{C}')\sigma' = \mathsf{C}\lfloor X\theta' \rfloor_{\Phi'} \delta^1(\mathcal{C}')$ and so $\mathsf{C}\lfloor X\theta \rfloor_\Phi \delta^1(\mathcal{C})\sigma' = \mathsf{C}\lfloor X\theta' \rfloor_{\Phi'} \delta^1(\mathcal{C}')$. Furthermore, since $\theta = \theta'$ and $\mathcal{C} = \mathcal{C}'$, we trivially have that $\mathsf{param}^{\mathcal{C}'}_{\mathsf{max}}(X\theta') \leq \mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(X\theta)$. Hence the result holds.

Inductive case $N > 0$*:* In such a case, we have that $\mathcal{C} \to^* \mathcal{C}'' \to \mathcal{C}'$ for some normalised constraint system $\mathcal{C}''$. By Lemma 4, we know that $\mathcal{C}''$ is also well-formed. Let $\theta'' = \mathsf{mgu}(E_\Pi(\mathcal{C}''))$ and $\sigma'' = \mathsf{mgu}(E(\mathcal{C}''))$. By inductive hypothesis, we know that for all $X \in vars^2(\mathcal{C})$, $\mathsf{C}\lfloor X\theta \rfloor_\Phi \delta^1(\mathcal{C})\sigma'' = \mathsf{C}\lfloor X\theta'' \rfloor_{\Phi''} \delta^1(\mathcal{C}'')$ and $\mathsf{param}^{\mathcal{C}''}_{\mathsf{max}}(X\theta'') \leq \mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(X\theta)$. The application of a rule on $\mathcal{C}''$ produced two constraint systems $\mathcal{C}_1$ and $\mathcal{C}_2$. We show the result by case analysis on the rule applied on $\mathcal{C}''$ and we distinguish two cases depending on whether $\mathcal{C}' = \mathcal{C}_1$ or $\mathcal{C}' = \mathcal{C}_2$.

Case $\mathcal{C}' = \mathcal{C}_2$ for any rule: According to Figure 1 and Figure 2, for any rule, only inequations or non deducibility constraint are added in $\mathcal{C}_2$, or some frame elements are marked as NoUse. Hence, we have that $\theta'' = \theta'$, $\sigma'' = \sigma'$, $,\Phi'' = \Phi'$ and $D'' = D'$. Thus, $\mathsf{C}\lfloor X\theta \rfloor_\Phi \delta^1(\mathcal{C})\sigma'' = \mathsf{C}\lfloor X\theta'' \rfloor_{\Phi''} \delta^1(\mathcal{C}'')$ implies $\mathsf{C}\lfloor X\theta \rfloor_\Phi \delta^1(\mathcal{C})\sigma' = \mathsf{C}\lfloor X\theta' \rfloor_{\Phi'} \delta^1(\mathcal{C}')$. Moreover, we also deduce $\mathsf{param}^{\mathcal{C}'}_{\mathsf{max}}(X\theta') = \mathsf{param}^{\mathcal{C}''}_{\mathsf{max}}(X\theta'')$. Since $\mathsf{param}^{\mathcal{C}''}_{\mathsf{max}}(X\theta'') \leq \mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(X\theta)$, we conclude that $\mathsf{param}^{\mathcal{C}'}_{\mathsf{max}}(X\theta') \leq \mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(X\theta)$ and so the result holds.

We now consider the case where $\mathcal{C}'' = \mathcal{C}_1$, and we consider each rule in turn:

Rule $\textsc{Cons}(X, \mathsf{f})$: Let $Y \in vars^2(\mathcal{C})$. The rule described in Figure 1 tells us that:

- $E' = E'' \wedge t =^? \mathsf{f}(x_1, \ldots, x_n)$.
- $E'_\Pi = E''_\Pi \wedge X =^? \mathsf{f}(X_1, \ldots, X_n)$
- $(X, i \vdash^? t) \in D(\mathcal{C}'')$

Since $\mathcal{C}''$ is normalised, it means that $vars(t) \cap \mathrm{dom}(\sigma'') = \emptyset$. Furthermore, $x_1, \ldots, x_n$ are fresh variables, and so $\{x_1, \ldots, x_n\} \cap \mathrm{dom}(\sigma'') = \emptyset$. Thus, $\mathsf{mgu}(E'' \wedge t =^? \mathsf{f}(x_1, \ldots, x_n)) = \sigma''\mathsf{mgu}(t =^? \mathsf{f}(x_1, \ldots, x_n))$. Let $\Sigma = \mathsf{mgu}(t =^? \mathsf{f}(x_1, \ldots, x_n))$ (it exists otherwise the normalised constraint system $\mathcal{C}'$ would be $\bot$), we have $\sigma' = \sigma''\Sigma$. Since $X_1, \ldots, X_n$ are also fresh variables, thus if we denote $\Theta = \mathsf{mgu}(X =^? \mathsf{f}(X_1, \ldots, X_n))$, then $\theta' = \theta''\Theta$.

According to Figure 1, $(X, i \vdash^? t) \in D(\mathcal{C}'')$ implies $(X_k, i \vdash^? x_k\Sigma) \in D(\mathcal{C}')$ for all $k \in \{1, \ldots, n\}$. Hence, we have that $\mathsf{param}^{\mathcal{C}''}_{\mathsf{max}}(X) = \mathsf{param}^{\mathcal{C}'}_{\mathsf{max}}(X\Theta)$. Since only $X, i \vdash^? t$ was removed from $D(\mathcal{C}'')$, we deduce that $\mathsf{param}^{\mathcal{C}'}_{\mathsf{max}}(Y\theta''\Theta) = \mathsf{param}^{\mathcal{C}''}_{\mathsf{max}}(Y\theta'')$. Hence $\mathsf{param}^{\mathcal{C}'}_{\mathsf{max}}(Y\theta') = \mathsf{param}^{\mathcal{C}''}_{\mathsf{max}}(Y\theta'') \leq \mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(Y\theta)$.

From the first equality, we deduce that $\mathsf{C}\lfloor Y\theta \rfloor_\Phi \delta^1(\mathcal{C})\sigma' = \mathsf{C}\lfloor Y\theta \rfloor_\Phi \delta^1(\mathcal{C})\sigma''\Sigma$. Therefore by our inductive hypothesis, we have $\mathsf{C}\lfloor Y\theta \rfloor_\Phi \delta^1(\mathcal{C})\sigma' = \mathsf{C}\lfloor Y\theta'' \rfloor_{\Phi''} \delta^1(\mathcal{C}'')\Sigma$. But since no frame element was added on Φ', thus we have $\mathsf{C}\lfloor Y\theta'' \rfloor_{\Phi''} = \mathsf{C}\lfloor Y\theta'' \rfloor_{\Phi'}$. Furthermore, since $\mathcal{C}''$ is well-formed, we know that $\mathsf{C}\lfloor Y\theta'' \rfloor_{\Phi''} \in \mathcal{T}(\mathcal{F}_c \cup (\mathcal{F}_d^* \cdot \mathcal{AX}), \mathcal{X}^2)$ and since $\mathsf{C}\lfloor \mathsf{f}(X_1, \ldots, X_n) \rfloor_{\Phi'} \in \mathcal{T}(\mathcal{F}_c \cup (\mathcal{F}_d^* \cdot \mathcal{AX}), \mathcal{X}^2)$, we can deduce by Lemma 3 that $\mathsf{C}\lfloor Y\theta''\Theta \rfloor_{\Phi'} = \mathsf{C}\lfloor Y\theta'' \rfloor_{\Phi'}\{X \to \mathsf{C}\lfloor \mathsf{f}(X_1, \ldots, X_n) \rfloor_{\Phi'}\}$ and so $\mathsf{C}\lfloor Y\theta''\Theta \rfloor_{\Phi'} = \mathsf{C}\lfloor Y\theta'' \rfloor_{\Phi''}\Theta$.

At last, since the constraint with the variable X was removed in D' and since we consider $\mathcal{C}'$ normalised, we have :

- for all $Z \in vars^2(D'') \setminus \{X\}$, $Z\Theta\delta^1(\mathcal{C}') = Z\delta^1(\mathcal{C}') = Z\delta^1(\mathcal{C}'')\Sigma$
- for all $i \in \{1, \ldots, n\}$, $X_i\delta^1(\mathcal{C}') = x_i\Sigma$ and so $X\delta^1(\mathcal{C}'')\Sigma = t\Sigma = \mathsf{f}(x_1, \ldots, x_n)\Sigma = X\Theta\delta^1(\mathcal{C}')$

Thus, we deduce that $\delta^1(\mathcal{C}'')\Sigma = \Theta\delta^1(\mathcal{C}')$, which implies, thanks to $\mathsf{C}\lfloor Y\theta''\Theta \rfloor_{\Phi'} = \mathsf{C}\lfloor Y\theta'' \rfloor_{\Phi''}\Theta$, that : $\mathsf{C}\lfloor Y\theta'' \rfloor_{\Phi''}\delta^1(\mathcal{C}'')\Sigma = \mathsf{C}\lfloor Y\theta' \rfloor_{\Phi'}\delta^1(\mathcal{C}')$ and so we obtain $\mathsf{C}\lfloor Y\theta \rfloor_\Phi \delta^1(\mathcal{C})\sigma' = \mathsf{C}\lfloor Y\theta' \rfloor_{\Phi'}\delta^1(\mathcal{C}')$.

Rule Axiom(X, path): Let $Y \in vars^2(\mathcal{C})$. The rule described in Figure 1 tells us that:

- $E' = E'' \wedge u =^? v$.
- $E'_\Pi = E''_\Pi \wedge X =^? \xi$
- $(X, i \vdash^? u) \in D(\mathcal{C}'')$, $(\xi, j \rhd v) \in \Phi(\mathcal{C}'')$ and $\mathsf{path}(\xi) = \mathsf{path}$

Since $\mathcal{C}''$ is normalised, it means that $(vars(u) \cup vars(v)) \cap \mathrm{dom}(\sigma'') = \emptyset$ which means that $\mathsf{mgu}(E'' \wedge u =^? v) = \sigma''\mathsf{mgu}(u =^? v)$. Let $\Sigma = \mathsf{mgu}(u =^? v)$; we have $\sigma' = \sigma''\Sigma$. For the same reason, if we denoted $\Theta = \mathsf{mgu}(X =^? \xi)$, we have $\theta' = \theta''\Theta$. No element has been added into the frame $\mathcal{C}'$ (from $\mathcal{C}''$), which means that $\mathsf{C}\lfloor Y\theta' \rfloor_{\Phi'} = \mathsf{C}\lfloor Y\theta' \rfloor_{\Phi''} = \mathsf{C}\lfloor Y\theta''\Theta \rfloor_{\Phi''}$. By Lemma 3 and since $\mathcal{C}''$ is well-formed, we deduce that $\mathsf{C}\lfloor Y\theta''\Theta \rfloor_{\Phi''} = \mathsf{C}\lfloor Y\theta'' \rfloor_{\Phi''}\{X \to \mathsf{C}\lfloor \xi \rfloor_{\Phi''}\}$.

Thanks to $\mathcal{C}$ being well formed (Definition 18, item 3), we deduce that $\mathsf{param}^{\mathcal{C}''}_{\mathsf{max}}(\xi) \leq j$. Moreover, since $\Theta = \mathsf{mgu}(X =^? \xi)$, we deduce that $X \notin vars^2(\xi)$ and so $(\xi, j \rhd v\Sigma) \in \Phi(\mathcal{C}')$. The deducible constraint $(X, i \vdash^? u)$ being the only one removed from $D(\mathcal{C}'')$, we deduce that $\mathsf{param}^{\mathcal{C}''}_{\mathsf{max}}(\xi) = \mathsf{param}^{\mathcal{C}'}_{\mathsf{max}}(\xi)$. Hence $\mathsf{param}^{\mathcal{C}'}_{\mathsf{max}}(X) = i \geq j \geq \mathsf{param}^{\mathcal{C}''}_{\mathsf{max}}(\xi)$.

Therefore we deduce $\mathsf{param}^{\mathcal{C}'}_{\mathsf{max}}(Y\theta''\Theta) \leq \mathsf{param}^{\mathcal{C}''}_{\mathsf{max}}(Y\theta'')$. Thus we deduce that $\mathsf{param}^{\mathcal{C}'}_{\mathsf{max}}(Y\theta') = \mathsf{param}^{\mathcal{C}'}_{\mathsf{max}}(Y\theta''\Theta) \leq \mathsf{param}^{\mathcal{C}''}_{\mathsf{max}}(Y\theta'') \leq \mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(Y\theta)$.

At last, since the constraint with the variable X was removed in D' and $\mathcal{C}'$ normalised, we have:

- for all $Z \in vars(D'') \setminus \{X\}$, $Z\{X \to \mathsf{C}\lfloor\xi\rfloor_{\Phi''}\}\delta^1(\mathcal{C}') = Z\delta^1(\mathcal{C}') = Z\delta^1(\mathcal{C}'')\Sigma$
- $X\delta^1(\mathcal{C}'')\Sigma = u\Sigma = v\Sigma = X\{X \to \mathsf{C}\lfloor\xi\rfloor_{\Phi''}\}\delta^1(\mathcal{C}')$

Thus, we deduce that $\delta^1(\mathcal{C}'')\Sigma = \{X \to \mathsf{C}\lfloor\xi\rfloor_{\Phi''}\}\delta^1(\mathcal{C}')$. Hence, thanks to our inductive hypothesis (applied on $\mathcal{C}''$ and Y), we have that $\mathsf{C}\lfloor Y\theta\rfloor_{\Phi}\delta^1(\mathcal{C})\sigma'' = \mathsf{C}\lfloor Y\theta''\rfloor_{\Phi''}\delta^1(\mathcal{C}'')$, and we deduce that $\mathsf{C}\lfloor Y\theta\rfloor_{\Phi}\delta^1(\mathcal{C})\sigma' = \mathsf{C}\lfloor Y\theta\rfloor_{\Phi}\delta^1(\mathcal{C})\sigma''\Sigma = \mathsf{C}\lfloor Y\theta''\rfloor_{\Phi''}\delta^1(\mathcal{C}'')\Sigma = \mathsf{C}\lfloor Y\theta''\rfloor_{\Phi''}\{X \to \mathsf{C}\lfloor\xi\rfloor_{\Phi''}\}\delta^1(\mathcal{C}') = \mathsf{C}\lfloor Y\theta''\Theta\rfloor_{\Phi''}\delta^1(\mathcal{C}') = \mathsf{C}\lfloor Y\theta'\rfloor_{\Phi'}\delta^1(\mathcal{C}')$.

Rule $\textsc{Dest}(\xi, \ell \to r, i)$: Let $Y \in vars^2(\mathcal{C})$. The rule described in Figure 1 tells us that:

- $E' = E'' \wedge u =^? u_1$.
- $E'_\Pi = E''_\Pi$ and so $\theta' = \theta''$.

Since $\mathcal{C}'$ is normalised, it means that $vars(u) \cap \mathrm{dom}(\sigma'') = \emptyset$. Furthermore, we know that all variable in u_1 are fresh variables, which means that $\mathsf{mgu}(E'' \wedge u =^? u_1) = \sigma''\mathsf{mgu}(u =^? u_1)$. Let $\Sigma = \mathsf{mgu}(u =^? u_1)$. We have that $\sigma' = \sigma''\Sigma$.

Since $\theta' = \theta''$ and no deducible constraint is removed from $D(\mathcal{C}'')$ to $D(\mathcal{C}')$, we trivially have that $\mathsf{param}^{\mathcal{C}''}_{\mathsf{max}}(Y\theta'') = \mathsf{param}^{\mathcal{C}'}_{\mathsf{max}}(Y\theta')$ and so $\mathsf{param}^{\mathcal{C}'}_{\mathsf{max}}(Y\theta') \leq \mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(Y\theta)$.

The frame element $(\mathsf{f}(\xi, X_1, \ldots, X_n), i \rhd w)$ with $f \in \mathcal{F}_d$ was added in Φ', but since $\mathcal{C}''$ is well-formed, we know that $\mathsf{C}\lfloor Y\theta''\rfloor_{\Phi''} \in \mathcal{T}(\mathcal{F}_c, (\mathcal{F}_d^* \cdot \mathcal{AX}) \cup \mathcal{X}^2)$, thus we deduce that $\mathsf{C}\lfloor Y\theta''\rfloor_{\Phi''} = \mathsf{C}\lfloor Y\theta''\rfloor_{\Phi'} = \mathsf{C}\lfloor Y\theta'\rfloor_{\Phi'}$.

At last, since only constraints with fresh variable X_k were added in D' and since $\mathcal{C}'$ is normalised, we have that $\delta^1(\mathcal{C}')_{|\,\mathrm{dom}(\delta^1(\mathcal{C}''))} = \delta^1(\mathcal{C}'')\Sigma$. With this last property, we can use the inductive hypothesis (on $\mathcal{C}''$ and Y). We obtain that $\mathsf{C}\lfloor Y\theta\rfloor_{\Phi}\delta^1(\mathcal{C})\sigma'' = \mathsf{C}\lfloor Y\theta''\rfloor_{\Phi''}\delta^1(\mathcal{C}'')$, and so $\mathsf{C}\lfloor Y\theta\rfloor_{\Phi}\delta^1(\mathcal{C})\sigma' = \mathsf{C}\lfloor Y\theta\rfloor_{\Phi}\delta^1(\mathcal{C})\sigma''\Sigma = \mathsf{C}\lfloor Y\theta''\rfloor_{\Phi''}\delta^1(\mathcal{C}'')\Sigma = \mathsf{C}\lfloor Y\theta'\rfloor_{\Phi'}\delta^1(\mathcal{C}'')\Sigma = \mathsf{C}\lfloor Y\theta'\rfloor_{\Phi'}\delta^1(\mathcal{C}')_{|\,\mathrm{dom}(\delta^1(\mathcal{C}''))}$.

Since $\mathsf{C}\lfloor Y\theta''\rfloor_{\Phi''} = \mathsf{C}\lfloor Y\theta'\rfloor_{\Phi'}$, then for all $Z \in vars^2(\mathsf{C}\lfloor Y\theta'\rfloor_{\Phi'})$, $Z \in \mathrm{dom}(\delta^1(\mathcal{C}''))$. Moreover, it also implies that for all $\mathsf{path} \in st(\mathsf{C}\lfloor Y\theta'\rfloor_{\Phi'})$, $\mathsf{path} \in \mathrm{dom}(\delta^1(\mathcal{C}''))$. Hence, we deduce that $\mathsf{C}\lfloor Y\theta'\rfloor_{\Phi'}\delta^1(\mathcal{C}')_{|\,\mathrm{dom}(\delta^1(\mathcal{C}''))} = \mathsf{C}\lfloor Y\theta'\rfloor_{\Phi'}\delta^1(\mathcal{C}')$ and so $\mathsf{C}\lfloor Y\theta\rfloor_{\Phi}\delta^1(\mathcal{C})\sigma' = \mathsf{C}\lfloor Y\theta'\rfloor_{\Phi'}\delta^1(\mathcal{C}')$.

Rules $\textsc{Eq-frame-ded}$ and $\textsc{Eq-frame-frame}$: Let $Y \in vars^2(\mathcal{C})$. The rule described in Figure 1 tells us that $E' = E'' \wedge u_1 =^? u_2$ and $E'_\Pi = E''_\Pi$, hence $\theta'' = \theta'$. Since $\mathcal{C}''$ is normalised, we have that $(vars(u_1) \cup vars(u_2)) \cap \mathrm{dom}(\sigma'') = \emptyset$ which means that $\mathsf{mgu}(E'' \wedge u_1 =^? u_2) = \sigma''\mathsf{mgu}(u_1 =^? u_2)$. Let $\Sigma = \mathsf{mgu}(u_1 =^? u_2)$. We have that $\sigma' = \sigma''\Sigma$.

Neither the frame nor the constraints changed between $\mathcal{C}''$ and $\mathcal{C}'$, which means that $\mathsf{C}\lfloor Y\theta'\rfloor_{\Phi'} = \mathsf{C}\lfloor Y\theta'\rfloor_{\Phi''}$. Since $\mathcal{C}'$ is normalised, we also have $\delta^1(\mathcal{C}') = \delta^1(\mathcal{C}'')\Sigma$. By the inductive hypothesis (applied on $\mathcal{C}''$ and Y), we have that $\mathsf{C}\lfloor Y\theta\rfloor_{\Phi}\delta^1(\mathcal{C})\sigma'' = \mathsf{C}\lfloor Y\theta''\rfloor_{\Phi''}\delta^1(\mathcal{C}'')$ and so $\mathsf{C}\lfloor Y\theta\rfloor_{\Phi}\delta^1(\mathcal{C})\sigma' = \mathsf{C}\lfloor Y\theta\rfloor_{\Phi}\delta^1(\mathcal{C})\sigma''\Sigma = \mathsf{C}\lfloor Y\theta''\rfloor_{\Phi''}\delta^1(\mathcal{C}'')\Sigma = \mathsf{C}\lfloor Y\theta'\rfloor_{\Phi'}\delta^1(\mathcal{C}')$.

Furthermore, since $\theta' = \theta''$ and no deducible constraint is removed from $D(\mathcal{C}'')$ to $D(\mathcal{C}')$, we trivially have that $\mathsf{param}^{\mathcal{C}''}_{\mathsf{max}}(Y\theta'') = \mathsf{param}^{\mathcal{C}'}_{\mathsf{max}}(Y\theta')$ and so $\mathsf{param}^{\mathcal{C}'}_{\mathsf{max}}(Y\theta') \leq \mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(Y\theta)$.

Rule EQ-DED-DED(X, ξ): Let $Y \in vars^2(\mathcal{C})$. The rule described in Figure 1 tells us that:

- $E' = E'' \wedge u =^? v$.
- $E'_\Pi = E''_\Pi \wedge X =^? \xi$
- $(X, i \vdash^? u) \in D(\mathcal{C}'')$

where $\xi \in \mathcal{T}(\mathcal{F}_c, \mathrm{dom}(\alpha))$ and $v = \xi\alpha$ with $\alpha = \{Y \to u \mid (Y, j \vdash^? u) \in D(\mathcal{C}'') \wedge j \leq i \wedge Y \in S_2\}$. But $\delta^1(\mathcal{C}'')_{|\,\mathrm{dom}(\alpha)} = \alpha$. Hence, we have that $v = \xi\delta^1(\mathcal{C}'')$.

Since $\mathcal{C}''$ is normalised, it means that $(vars(u) \cup vars(v)) \cap \mathrm{dom}(\sigma'') = \emptyset$ which means that $\mathsf{mgu}(E'' \wedge u =^? v) = \sigma''\mathsf{mgu}(u =^? v)$. Let $\Sigma = \mathsf{mgu}(u =^? v)$. We have that $\sigma' = \sigma''\Sigma$. For the same reason, we have that $\theta' = \theta''\Theta$ where $\Theta = \{X \to \xi\}$. No element has been added into the frame $\mathcal{C}'$ (w.r.t. $\mathcal{C}''$). Hence, we have that $\mathsf{C}\lfloor Y\theta' \rfloor_{\Phi'} = \mathsf{C}\lfloor Y\theta' \rfloor_{\Phi''} = \mathsf{C}\lfloor Y\theta''\Theta \rfloor_{\Phi''}$. By Lemma 3, $\mathcal{C}''$ well formed and $\xi \in \mathcal{T}(\mathcal{F}_c, \mathcal{X}^2)$, we deduce that $\mathsf{C}\lfloor Y\theta''\Theta \rfloor_{\Phi''} = \mathsf{C}\lfloor Y\theta'' \rfloor_{\Phi''}\Theta$.

Since for all $Z \in vars^2(\xi)$, $\mathsf{param}^{\mathcal{C}''}_{\mathsf{max}}(Z) \leq i = \mathsf{param}^{\mathcal{C}''}_{\mathsf{max}}(X)$ and $\Theta = \{X \to \xi\}$, we deduce that $\mathsf{param}^{\mathcal{C}'}_{\mathsf{max}}(X\Theta) \leq \mathsf{param}^{\mathcal{C}''}_{\mathsf{max}}(X)$. Therefore $\mathsf{param}^{\mathcal{C}'}_{\mathsf{max}}(Y\theta''\Theta) \leq \mathsf{param}^{\mathcal{C}''}_{\mathsf{max}}(Y\theta'')$. Thus we deduce that $\mathsf{param}^{\mathcal{C}'}_{\mathsf{max}}(Y\theta') = \mathsf{param}^{\mathcal{C}'}_{\mathsf{max}}(Y\theta''\Theta) \leq \mathsf{param}^{\mathcal{C}''}_{\mathsf{max}}(Y\theta'') \leq \mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(Y\theta)$.

At last, since the constraint with the variable X was removed in D' and $\mathcal{C}'$ normalised, we have:

- for all $Z \in vars(D'') \setminus \{X\}$, $Z\Theta\delta^1(\mathcal{C}') = Z\delta^1(\mathcal{C}') = Z\delta^1(\mathcal{C}'')\Sigma$
- $X\delta^1(\mathcal{C}'')\Sigma = u\Sigma = v\Sigma = X\Theta\delta^1(\mathcal{C}'')\Sigma = X\Theta\delta^1(\mathcal{C}')$

Thus, we deduce that $\delta^1(\mathcal{C}'')\Sigma = \Theta\delta^1(\mathcal{C}')$. Hence, thanks to our inductive hypothesis (applied on $\mathcal{C}''$ and Y), we have that $\mathsf{C}\lfloor Y\theta \rfloor_\Phi\delta^1(\mathcal{C})\sigma'' = \mathsf{C}\lfloor Y\theta'' \rfloor_{\Phi''}\delta^1(\mathcal{C}'')$. From this, we deduce that $\mathsf{C}\lfloor Y\theta \rfloor_\Phi\delta^1(\mathcal{C})\sigma' = \mathsf{C}\lfloor Y\theta \rfloor_\Phi\delta^1(\mathcal{C})\sigma''\Sigma = \mathsf{C}\lfloor Y\theta'' \rfloor_{\Phi''}\delta^1(\mathcal{C}'')\Sigma = \mathsf{C}\lfloor Y\theta'' \rfloor_{\Phi''}\Theta\delta^1(\mathcal{C}') = \mathsf{C}\lfloor Y\theta''\Theta \rfloor_{\Phi''}\delta^1(\mathcal{C}')$. Hence we conclude that $\mathsf{C}\lfloor Y\theta \rfloor_\Phi\delta^1(\mathcal{C})\sigma' = \mathsf{C}\lfloor Y\theta' \rfloor_{\Phi'}\delta^1(\mathcal{C}')$.

Rule DED-ST: Let $Y \in vars^2(\mathcal{C})$. The rule described in Figure 1 tells us that:

- $E' = E'' \wedge u =^? \mathsf{f}(x_1, \ldots, x_n)$.
- $E'_\Pi = E''_\Pi$ and so $\theta' = \theta''$.

Since $\mathcal{C}''$ is normalised, this means that $vars(u) \cap \mathrm{dom}(\sigma'') = \emptyset$. Furthermore, we know that the variables x_i are fresh variables, which means that $\mathsf{mgu}(E'' \wedge u =^? \mathsf{f}(x_1, \ldots, x_n)) = \sigma''\mathsf{mgu}(u =^? \mathsf{f}(x_1, \ldots, x_n))$. Let $\Sigma = \mathsf{mgu}(u =^? \mathsf{f}(x_1, \ldots, x_n))$. We have that $\sigma' = \sigma''\Sigma$.

Since $\theta' = \theta''$ and no deducible constraint are removed from $D(\mathcal{C}'')$ to $D(\mathcal{C}')$, we trivially have that $\mathsf{param}^{\mathcal{C}''}_{\mathsf{max}}(Y\theta'') = \mathsf{param}^{\mathcal{C}'}_{\mathsf{max}}(Y\theta')$ and so $\mathsf{param}^{\mathcal{C}'}_{\mathsf{max}}(Y\theta') \leq \mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(Y\theta)$.

No element has been added into the frame $\mathcal{C}'$ (w.r.t. $\mathcal{C}''$). Hence, we have that $\mathsf{C}\lfloor Y\theta'' \rfloor_{\Phi''} = \mathsf{C}\lfloor Y\theta'' \rfloor_{\Phi'} = \mathsf{C}\lfloor Y\theta' \rfloor_{\Phi'}$.

At last, since only constraints with fresh variable X_i were added in D' and since $\mathcal{C}'$ normalised, we have that $\delta^1(\mathcal{C}')_{|\,\mathrm{dom}(\delta^1(\mathcal{C}''))} = \delta^1(\mathcal{C}'')\Sigma$. With this last property, we can use the inductive hypothesis (applied on $\mathcal{C}''$ and Y). We obtain that $\mathsf{C}\lfloor Y\theta \rfloor_\Phi\delta^1(\mathcal{C})\sigma'' = \mathsf{C}\lfloor Y\theta'' \rfloor_{\Phi''}\delta^1(\mathcal{C}'')$, and so $\mathsf{C}\lfloor Y\theta \rfloor_\Phi\delta^1(\mathcal{C})\sigma' = \mathsf{C}\lfloor Y\theta \rfloor_\Phi\delta^1(\mathcal{C})\sigma''\Sigma = \mathsf{C}\lfloor Y\theta'' \rfloor_{\Phi''}\delta^1(\mathcal{C}'')\Sigma = \mathsf{C}\lfloor Y\theta' \rfloor_{\Phi'}\delta^1(\mathcal{C}'')\Sigma = \mathsf{C}\lfloor Y\theta' \rfloor_{\Phi'}\delta^1(\mathcal{C}')_{|\,\mathrm{dom}(\delta^1(\mathcal{C}''))}$.

Since $\mathsf{C}\lfloor Y\theta'' \rfloor_{\Phi''} = \mathsf{C}\lfloor Y\theta' \rfloor_{\Phi'}$, then for all $Z \in vars^2(\mathsf{C}\lfloor Y\theta' \rfloor_{\Phi'})$, $Z \in \mathrm{dom}(\delta^1(\mathcal{C}''))$. Moreover, it also implies that for all $\mathsf{path} \in st(\mathsf{C}\lfloor Y\theta' \rfloor_{\Phi'})$, $\mathsf{path} \in \mathrm{dom}(\delta^1(\mathcal{C}''))$. Hence,

we deduce that $\mathsf{C}\lfloor Y\theta' \rfloor_{\Phi'} \delta^1(\mathcal{C}')_{|\,\mathrm{dom}(\delta^1(\mathcal{C}''))} = \mathsf{C}\lfloor Y\theta' \rfloor_{\Phi'} \delta^1(\mathcal{C}')$ and so $\mathsf{C}\lfloor Y\theta \rfloor_{\Phi} \delta^1(\mathcal{C})\sigma' = \mathsf{C}\lfloor Y\theta' \rfloor_{\Phi'} \delta^1(\mathcal{C}')$. □

Lemma 7. *Let $\mathcal{C}$ and $\mathcal{C}'$ be two normalised well-formed constraint systems such that $\mathcal{C} \to^* \mathcal{C}'$. Let $\sigma = \mathsf{mgu}(E(\mathcal{C}'))$, and $(\xi, i \rhd u) \in \Phi$. There exist $(\xi', i \rhd u') \in \Phi'$ such that $\mathsf{path}(\xi) = \mathsf{path}(\xi')$ and $u' = u\sigma$.*

Proof. According to the rules described in Figure 1 and 2 and the fact that $\mathcal{C}$ is well-formed, the path $\mathsf{path}(\xi)$ of a frame element $(\xi, i \rhd u)$ is never modified. The only operation that affects this frame element is the normalisation of a constraint system, *i.e.* the most general unifier of E is applied on u (idem for E_Π). Thus, if $\sigma = \mathsf{mgu}(E(\mathcal{C}'))$, we can conclude that $u' = u\sigma$. □

Lemma 8. *Let $\mathcal{C}$ be a normalised well-formed constraint system. Let $\mathcal{C}_1$ and $\mathcal{C}_2$ be two normalised well formed constraint systems such that $\mathcal{C} \to^* \mathcal{C}_1$ and $\mathcal{C} \to^* \mathcal{C}_2$. Let $ax \in \mathcal{AX}$ such that $\{ax, i \rhd u_1\} \in \Phi_1$ and $\{ax, i \rhd u_2\} \in \Phi_2$. Let $w \in \mathcal{F}_d^*$, $\{\xi_1, i_1 \rhd v_1\} \in \Phi_1$ and $\{\xi_2, i_2 \rhd v_2\} \in \Phi_2$ such that $\mathsf{path}(\xi_1) = \mathsf{path}(\xi_2) = w \cdot ax$, and $u_1\rho = u_2$ for some variable renaming ρ from $\mathcal{X}^1$ to $\mathcal{X}^1$. We have that $v_1\rho = v_2$.*

Proof. We prove the result by induction on $|w|$:

Base case $|w| = 0$: In such a case, we have that $\xi_1 = \xi_2 = ax$. Thus by item 1 of a well-formed constraint system, we know that $u_1 = v_1$ and $u_2 = v_2$ and so the result trivially holds.

Inductive step $|w| > 0$: Assume that $w = \mathsf{f} \cdot w'$ and $u_1\rho = u_2$. By item 2 of a well-formed constraint system, we know that there exists $(\xi_1', i_1' \rhd v_1') \in \Phi_1$ and $(\xi_2', i_2' \rhd v_2') \in \Phi_2$ such that $\mathsf{path}(\xi_1') = \mathsf{path}(\xi_2') = w' \cdot ax$. Thus by our inductive hypothesis, we know that $v_1'\rho = v_2'$. Furthermore, by definition of the rule DEST (the only rule that can add an element into the frame), we know that there exists a position p (actually for our rewriting rules $p = 1$) such that $v_1 = v_1'|_p$ and $v_2 = v_2'|_p$. Hence, we have that $v_1\rho = (v_1'|_p)\rho = (v_1'\rho)|_p = v_2'|_p = v_2$. □

Appendix C.3. Preservation of the invariants along the whole procedure

First, we consider the invariants that are satisfied at any step of the strategy. The other ones are established in the next section.

Lemma 9. *Let $\mathcal{C}$ be a well-formed constraint system satisfying $\mathsf{InvVarConstraint}(s)$. Let $\textsc{Rule}(\tilde{p})$ be an instance of the rule CONS, or AXIOM or EQ-DED-DED with support $s' \leq s$. Let $\mathcal{C}_1, \mathcal{C}_2$ be the two constraint systems obtained by applying $\textsc{Rule}(\tilde{p})$ on $\mathcal{C}$. We have that for all $i \in \{1, 2\}$, $\mathcal{C}_i$ satisfies $\mathsf{InvVarConstraint}(s)$.*

Proof. According to the definitions of the three rules, $\mathcal{C}_2$ only differs from $\mathcal{C}$ by an additional inequality on recipes. Thus, we trivially deduce that $\mathcal{C}_2$ satisfies $\mathsf{InvVarConstraint}(s)$. We prove the result for $\mathcal{C}_1$ by case analysis on the rule applied:

Rule $\textsc{Cons}(X, \mathsf{f})$: Since the support of the rule is s', then there exists $(X, s' \vdash^? u) \in D(\mathcal{C})$. Moreover, $\mathcal{C}$ satisfies $\mathsf{InvVarConstraint}(s)$ hence $u \in \mathcal{X}^1$. But $D(\mathcal{C}_1) = D(\mathcal{C})\sigma \setminus \{X, s' \vdash^? u\sigma\} \cup \{X_1, s' \vdash^? x_1\sigma; \ldots; X_n, s' \vdash^? x_n\sigma\}$ where $\sigma = \mathsf{mgu}(u =^? \mathsf{f}(x_1, \ldots, x_n))$ and

$x_1, \ldots, x_n, X_1, \ldots, X_n$ are fresh variables. Since $s' \leq s$ then $\mathcal{C}$ satisfies $\mathsf{InvVarConstraint}(s)$ also implies that $X \in S_2$. Thus, by definition of the rule CONS, $X_1, \ldots, X_n \in S_2$.

Moreover, since $u \in \mathcal{X}^1$, we deduce that $\sigma = \{u \mapsto \mathsf{f}(x_1, \ldots, x_n)\}$. Hence for all $i \in \{1, \ldots, n\}$, $x_i\sigma = x_i$. Moreover, since $\mathcal{C}$ satisfies $\mathsf{InvVarConstraint}(s)$, we deduce that for all $(Y, j \rhd y) \in D$ such that $Y \neq X$, $y\sigma = y$. Thus, thanks to $x_1, \ldots, x_n$ and $X_1, \ldots, X_n$ being fresh, the result holds.

Rule AXIOM(X, path)*:* Since the support of the rule is s', then there exists $(X, s' \vdash^? u) \in D(\mathcal{C})$ and $(\xi, j \rhd v) \in \Phi(\mathcal{C})$ with $j \leq s'$. Moreover, $\mathcal{C}$ satisfies $\mathsf{InvVarConstraint}(s)$ hence, we deduce $u \in \mathcal{X}^1$. But $D(\mathcal{C}_1) = D(\mathcal{C})\sigma \setminus \{X, s' \vdash^? u\sigma\}$ where $\sigma = \mathsf{mgu}(u =^? v)$. Thus the first property is trivially satisfied.

Moreover, $u \in \mathcal{X}^1$ implies that either (a) $\sigma = \{u \mapsto v\}$ or (b) $v \in \mathcal{X}^1$ and $\sigma = \{v \mapsto u\}$. In case (a), since $\mathcal{C}$ satisfies $\mathsf{InvVarConstraint}(s)$, we deduce that for all $(Z, k \vdash^? z) \in D(\mathcal{C})$ and $k \leq s$, if $Z \neq X$ then $(Z, k \vdash^? z) \in D(\mathcal{C}_1)$ hence the result holds. In case (b), $v \in \mathcal{X}^1$ implies, by the origination property, that there exists $(Y, k \vdash^? v') \in D(\mathcal{C})$ such that $k < j$ and $v \in vars^1(v')$. But $\mathcal{C}$ satisfies $\mathsf{InvVarConstraint}(s)$ thus $v = v'$. Hence for all $(Z_1, \ell_1 \vdash^? z_1) \in D(\mathcal{C}_1)$, if $\ell_1 \leq s$ then either $Z_1 \neq Y$ and so $(Z_1, \ell_1 \vdash^? z_1) \in D(\mathcal{C})$, or $Z_1 = Y$ and $v' = u$. By relying on $\mathcal{C}$ satisfying $\mathsf{InvVarConstraint}(s)$, the result holds.

Rule EQ-DED-DED(X, ξ)*:* Proof similar to the rule AXIOM. □

Lemma 10. *Let $\mathcal{C}$ be a well-formed constraint system satisfying $\mathsf{InvUntouched}(s)$. Let $\text{RULE}(\tilde{p})$ be an instance of a rule with support $s' \leq s$. Let $\mathcal{C}_1, \mathcal{C}_2$ be the two constraint systems obtained by applying $\text{RULE}(\tilde{p})$ on $\mathcal{C}$. We have that for all $i \in \{1, 2\}$, $\mathcal{C}_i$ satisfies $\mathsf{InvUntouched}(s)$.*

Proof. The rule DEST is the only one that adds an element into the frame. But the support of the rule being s', DEST can only introduce frame element of the form $(\zeta, s' \rhd w)$. Thus since $s' \leq s$, we deduce that for all $(\xi, k \rhd u) \in \Phi(\mathcal{C}_1)$ (resp. $\Phi(\mathcal{C}_2)$), if $s < k$ then $\xi = ax_k$. Similarly, the only rules that add elements in $E_\Pi(\mathcal{C})$ are CONS, AXIOM and EQ-DED-DED. In case of CONS and EQ-DED-DED, the result trivially holds by definition of the rules and the fact that $s' \leq s$. In case of application of the rule AXIOM(X, path), by definition, we know that there exists $(X, s' \vdash^? u) \in D(\mathcal{C})$ and $(\xi, k \rhd v) \in \Phi(\mathcal{C})$ with $k \leq s'$. But since $\mathcal{C}$ is well-formed (Definition 18, item 3), we know that $\mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(\xi) \leq k$ which implies that for all $Y \in vars^2(\xi)$, $(Y, \ell \vdash^? w) \in D(\mathcal{C})$ implies that $\ell \leq k$. Hence any new (in)equations in E_Π only contain variables Y such that $\mathsf{param}^{\mathcal{C}_1}_{\mathsf{max}}(Y) \leq s' \leq s$. Hence the result holds. □

Lemma 11. *Let $\mathcal{C}$ be a well-formed constraint system satisfying $\mathsf{InvNoUse}(s)$ (resp. $\mathsf{InvDest}(s)$, $\mathsf{InvVarFrame}(s)$ and $\mathsf{InvDedsub}$). Let $\text{RULE}(\tilde{p})$ be an instance of a rule different from DEST, or the rule DEST with support $s' > s$. Let $\mathcal{C}_1, \mathcal{C}_2$ be the two constraint systems obtained by applying $\text{RULE}(\tilde{p})$ on $\mathcal{C}$. We have that for all $i \in \{1, 2\}$, $\mathcal{C}_i$ satisfies $\mathsf{InvNoUse}(s)$ (resp. $\mathsf{InvDest}(s)$, $\mathsf{InvVarFrame}(s)$ and $\mathsf{InvDedsub}$).*

Proof. We prove the different invariants by case analysis on the rule applied.

Rule CONS(X, f)*:* The rule CONS only adds the inequation $\mathsf{root}(X) \neq \mathsf{f}$ into $E_\Pi(\mathcal{C}_2)$. Thus, $\mathcal{C}_2$ trivially satisfies all the wanted invariants.

On the other hand, we have that $\Phi(\mathcal{C}_1) = \Phi(\mathcal{C})\theta\sigma$, $\mathsf{NoUse}(\mathcal{C}_1) = \mathsf{NoUse}(\mathcal{C})\theta\sigma$, $ND(\mathcal{C}_1) = ND(\mathcal{C})\sigma$ and $D(\mathcal{C}_1) = D(\mathcal{C})\sigma \setminus \{X, i \vdash^? t\sigma\} \cup \{X_1, i \vdash^? x_1\sigma;\ \ldots;\ X_n, i \vdash^? x_n\sigma\}$ where

$\sigma = \mathsf{mgu}(t =^? \mathsf{f}(x_1, \ldots, x_n))$ and $\theta = \mathsf{mgu}(X =^? \mathsf{f}(X_1, \ldots, X_n))$. We now prove the different invariants one by one.

Let $(\xi, p \rhd v) \in \Phi(\mathcal{C}_1)$ such that $p \leq s$. Since $\Phi(\mathcal{C}_1) = \Phi(\mathcal{C})\sigma$, there exists ξ' and v' such that $(\xi', p \rhd v') \in \Phi(\mathcal{C})$, $\xi'\theta = \xi$ and $v'\sigma = v$:

- $\mathsf{InvNoUse}(s)$: Assume that $v \in \mathcal{X}^1$. In such a case, $v'\sigma = v$ implies $v' \in \mathcal{X}^1$. But $\mathcal{C}$ satisfies $\mathsf{InvNoUse}(s)$ hence $(\xi', p \rhd z) \in \mathsf{NoUse}(\mathcal{C})$. With $\mathsf{NoUse}(\mathcal{C}_1) = \mathsf{NoUse}(\mathcal{C})\theta\sigma$, we deduce that $(\xi, p \rhd v) \in \mathsf{NoUse}(\mathcal{C}_1)$ thus the result holds.

- $\mathsf{InvVarFrame}(s)$: Let $Y \in vars^2(\xi)$. In such a case, $\xi'\theta = \xi$ implies that there exists $Y' \in vars^2(\xi')$ such that $Y \in vars^2(Y'\theta)$. But $\mathcal{C}$ satisfies $\mathsf{InvVarFrame}(s)$ implies that there exists $q < p$ and $u \in \mathcal{T}(\mathcal{F}_c, \mathcal{N} \cup \mathcal{X}^1)$ such that $(Y', q \vdash^? u) \in D(\mathcal{C})$. If $Y' \neq X$ then $Y' = Y$ and so $(Y, q \vdash^? u\sigma) \in D(\mathcal{C}_1)$ thus the result holds. If $Y' = X$ then $Y \in \{X_1, \ldots, X_n\}$ and $s' = q$. But for all $k \in \{1, \ldots, n\}$, we have $(X_k, s' \vdash^? x_k\sigma) \in D(\mathcal{C}_1)$. With $s' = q < p$ then the result holds.

- $\mathsf{InvDest}(s)$: The result is direct from $\Phi(\mathcal{C}_1) = \Phi(\mathcal{C})\theta\sigma$, $\mathsf{NoUse}(\mathcal{C}_1) = \mathsf{NoUse}(\mathcal{C})\theta\sigma$, $ND(\mathcal{C}_1) = ND(\mathcal{C})\sigma$ and the fact that $\mathcal{C}$ satisfies the invariant $\mathsf{InvDest}(s)$.

- $\mathsf{InvDedsub}$: Since $\mathcal{C}$ satisfies the invariant, then for all $\mathsf{g} \in \mathcal{F}_c$, $(\xi', p \rhd v') \in \mathsf{NoUse}(\mathcal{C})$ implies that either (a) there exists $Y_1, \ldots, Y_k \in vars^2(\mathcal{C})$ such that for all $i \in \{1, \ldots, k\}$, we have that $\mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(Y_i \mathsf{mgu}(E_\Pi(\mathcal{C}))) \leq \mathsf{s}_{max}$ and $\mathsf{C}\lfloor \mathsf{g}(Y_1, \ldots, Y_m)\, \mathsf{mgu}(E_\Pi(\mathcal{C}))\rfloor \delta^1(\mathcal{C}) = v'$, or else (b)

$$ND(\mathcal{C}) \vDash \forall \tilde{x}. v' \neq^? \mathsf{g}(x_1, \ldots, x_n) \vee \mathsf{s}_{max} \not\vdash^? x_1 \vee \ldots \vee \mathsf{s}_{max} \not\vdash^? x_k$$

  where $x_1, \ldots, x_k$ are fresh variables.

  In case (a), by Lemma 3 and since $\mathsf{mgu}(E_\Pi(\mathcal{C}_1)) = \mathsf{mgu}(E_\Pi(\mathcal{C}))\theta$, $\mathsf{f}(X_1, \ldots, X_n) = \mathsf{C}\lfloor \mathsf{f}(X_1, \ldots, X_n)\rfloor \in \mathcal{T}(\mathcal{F}_c, \mathcal{X}^2)$, we deduce that $\mathsf{C}\lfloor \mathsf{g}(Y_1, \ldots, Y_k)\mathsf{mgu}(E_\Pi(\mathcal{C}_1))\rfloor = \mathsf{C}\lfloor \mathsf{g}(Y_1, \ldots, Y_k)\mathsf{mgu}(E_\Pi(\mathcal{C}))\rfloor\theta$. But for all $Z \in vars^2(\mathcal{C})$, $Z\delta^1(\mathcal{C})\sigma = Z\theta\delta^1(\mathcal{C}_1)$ thus $\mathsf{C}\lfloor \mathsf{g}(Y_1, \ldots, Y_k)\mathsf{mgu}(E_\Pi(\mathcal{C}_1))\rfloor \delta^1(\mathcal{C}_1) = \mathsf{C}\lfloor \mathsf{g}(Y_1, \ldots, Y_k)\mathsf{mgu}(E_\Pi(\mathcal{C}))\rfloor \delta^1(\mathcal{C})\sigma = v'\sigma = v$. Hence the result holds.

  In case (b), since $ND(\mathcal{C}_1) = ND(\mathcal{C})\sigma$ then $ND(\mathcal{C}_1) \vDash \forall \tilde{x}. v \neq^? \mathsf{g}(x_1, \ldots, x_n) \vee \mathsf{s}_{max} \not\vdash^? x_1 \vee \ldots \vee \mathsf{s}_{max} \not\vdash^? x_k$. Hence the result holds.

Rule $\textsc{Dest}(\xi, \ell \to r, s')$ *and* $s' > s$ *:* Since the rule only adds a frame element $(\zeta, s' \rhd w)$ for some ζ, w and applies a substitution on first order term, then the result holds by relying on $\mathcal{C}$ verifying each invariant respectively.

All the other rules: The proofs of all the others rules are similar to the rule Cons. Note that for the rule $\textsc{Ded-st}(\xi, \mathsf{f})$, if $\mathcal{C}$ satisfies the invariant $\mathsf{InvDedsub}$, then it implies that the application of the rule $\textsc{Ded-st}(\xi, \mathsf{f})$ was in fact useless hence according to the strategy, such application could not have happen. Hence the result holds. □

Lemma 12. *Let $\mathcal{M}$ be a well-formed matrix of constraint systems satisfying* $\mathsf{InvMatrix}(s)$. *Let* $\textsc{Rule}(\tilde{p})$ *be an instance of a rule different from* Dest *and* Eq-frame-ded*, or* Dest *with support $s' > s$, or* Eq-frame-ded *with support $s' > s$. Let $\mathcal{M}_1, \mathcal{M}_2$ be the two matrices of constraint systems obtained by applying* $\textsc{Rule}(\tilde{p})$ *on $\mathcal{M}$ (if* $\textsc{Rule}(\tilde{p})$ *is an internal rule, only $\mathcal{M}_1$ exists). We have that for all $i \in \{1, 2\}$, $\mathcal{M}_i$ satisfies* $\mathsf{InvMatrix}(s)$.

Proof. Note that the invariant $\mathsf{InvMatrix}(s)$ mainly focuses on the path of the frames. But thanks to $\mathcal{M}$ being well-formed we have that for all $\mathcal{C} \in \mathcal{T}(\mathcal{F}_c, \mathcal{N})$, $\mathcal{C}$ is well-formed. Hence by Definition 18, item 1, we know that the path of any frame element is closed. Hence relying on Lemma 2, we trivially deduce that the result holds for the rule Cons, Axiom, Eq-ded-ded, Eq-frame-frame and Ded-st. Hence it remains to prove that the result holds for Eq-frame-ded with support $s' > s$ and Dest with support $s' > s$. But in both cases, the only possible modifications on the frames or on the sets NoUse only occurs on frame elements with support stricly bigger than s. Hence the result holds. □

Lemma 13. *Let $\mathcal{C}$ be a well-formed constraint system. Let $s \in \mathbb{N}$, if $\mathcal{C}$ satisfies* $\mathsf{InvDedsub}$ *(resp.* $\mathsf{InvVarFrame}(s)$*,* $\mathsf{InvNoUse}(s)$*,* $\mathsf{InvDest}(s)$ *and* $\mathsf{InvVarConstraint}(s)$*) then for all $s' \leq s$, $\mathcal{C}$ satisfies* $\mathsf{InvDedsub}$ *(resp.* $\mathsf{InvVarFrame}(s')$*,* $\mathsf{InvNoUse}(s')$*,* $\mathsf{InvDest}(s')$ *and* $\mathsf{InvVarConstraint}(s')$*).*

If $\mathcal{C}$ satisfies $\mathsf{InvUntouched}(s)$ *then for all $s' \geq s$, $\mathcal{C}$ satisfies* $\mathsf{InvUntouched}(s')$*.*

Proof. Direct from the definition of the invariants. □

Lemma 14. *Let $\mathcal{M}$ be a well-formed constraint system satisfying* $\mathsf{InvGeneral}$*. Let* Rule$(\tilde{p})$ *be an instance of a rule different from* Dest *and* Eq-frame-ded*. Let $\mathcal{M}_1, \mathcal{M}_2$ be the two matrices of constraint systems obtained by applying* Rule$(\tilde{p})$ *on $\mathcal{M}$ (if* Rule$(\tilde{p})$ *is an internal rule, only $\mathcal{M}_1$ exists). We have that for all $i \in \{1, 2\}$, $\mathcal{M}_i$ satisfies the invariant* $\mathsf{InvGeneral}$*.*

Let Rule$(\tilde{p})$ *be an instance of the rule* Dest *or* Eq-frame-ded*. Let $\mathcal{M}'$ be the matrix of constraint systems obtained by applying* Rule$(\tilde{p})$ *on $\mathcal{M}$. We have that $\mathcal{M}'$ satisfies Properties 5, 6 and 7 of the invariant* $\mathsf{InvGeneral}$*.*

Proof. First of all, let us notice that when the rule Rule$(\tilde{p})$ is an internal rule then we directly obtain from $\mathcal{M}$ satisfying $\mathsf{InvGeneral}$ that $\mathcal{M}_1$ satisfies Properties 5, 6 and 7. Indeed, these invariants focuses on the variable from $S_2(\mathcal{C})$ for $\mathcal{C}$ a constraint system in the matrix. But by definition of the internal rules, none of them involves variables from $S_2(\mathcal{C})$. This allows us to prove the second part of the lemma. Hence, it remains to prove the result for external rules and Properties 1, 2, 3 and 4 of $\mathsf{InvGeneral}$ for internal rules other than Dest and Eq-frame-ded. Note that for rules that can be both external and internal, it is sufficient to prove Properties 1, 2, 3 and 4 of $\mathsf{InvGeneral}$ in the external case. Let us do a case analysis on the rule applied.

Rule Cons(X, f): Let us first start with $\mathcal{M}_2$. In such a case, we only added $\mathsf{root}(X) \neq^? \mathsf{f}$ to all constraint systems of the matrix $\mathcal{M}$ to obtain $\mathcal{M}_2$. Hence, since $\mathcal{M}$ satisfies $\mathsf{InvGeneral}$ then we directly obtain that Properties 5, 6 and 7 of $\mathsf{InvGeneral}$ are satisfied by $\mathcal{M}_2$. Consider $\mathcal{C}_2$ be a constraint system of $\mathcal{M}_2$ and let $\mathcal{C}$ be the constraint system from $\mathcal{M}$ from which $\mathcal{C}_2$ is obtained. Let $(\sigma, \theta) \in \mathsf{Sol}(\mathcal{C}_2)$. Thanks to Lemma 5, we know that $(\sigma_{|vars^1(\mathcal{C})}, \theta_{|vars^2(\mathcal{C})}) \in \mathsf{Sol}(\mathcal{C})$. Moreover, we know by the rule that $\Phi(\mathcal{C}) = \Phi(\mathcal{C}_2)$, $\mathsf{NoUse}(\mathcal{C}) = \mathsf{NoUse}(\mathcal{C}_2)$, $E_\Pi(\mathcal{C}) = E_\Pi(\mathcal{C}_2)$ and $vars^2(\mathcal{C}) = vars^2(\mathcal{C}_2)$. Therefore, we deduce that Properties 1,2,3 and 4 of $\mathsf{InvGeneral}$ are satisfied by $\mathcal{M}_2$ since $\mathsf{InvGeneral}$ is satisfied by $\mathcal{M}$.

Let us now focus on $\mathcal{M}_1$. Consider $\mathcal{C}_1$ a constraint system from $\mathcal{M}_1$ and let $\mathcal{C}$ be the constraint system in $\mathcal{M}$ from which $\mathcal{C}_1$ is obtained. Let $(\sigma, \theta) \in \mathsf{Sol}(\mathcal{C}_1)$. Thanks to Lemma 5, we know that $(\sigma_{|vars^1(\mathcal{C})}, \theta_{|vars^2(\mathcal{C})}) \in \mathsf{Sol}(\mathcal{C})$. Moreover, we have $\Phi(\mathcal{C}_1)\theta'\sigma' =$

$\Phi(\mathcal{C}_1)$, $\mathsf{NoUse}(\mathcal{C})\theta'\sigma'$ and $\mathsf{mgu}(E_\Pi(\mathcal{C}_1)) = \mathsf{mgu}(E_\Pi(\mathcal{C}))\theta'$ where $\theta' = \{X \to \mathsf{f}(X_1, \ldots, X_n)\}$ and $\sigma' = \mathsf{mgu}(t, \mathsf{f}(x_1, \ldots, x_n))$. Note that $\Phi(\mathcal{C}_1)\theta\sigma = \Phi(\mathcal{C}_1)\theta'\sigma'\theta\sigma = \Phi(\mathcal{C})\theta\sigma$.

Let $(\xi, i \rhd u) \in \Phi(\mathcal{C}_1)$. We know that there exists ξ', u' such that $(\xi', i \rhd u') \in \Phi(\mathcal{C})$ and $\xi = \xi'\theta'$, $u = u'\sigma'$, $\xi\theta = \xi'\theta$ and $u\sigma = u'\sigma$. Since $\mathcal{M}$ satisfies $\mathsf{InvGeneral}$, we directly then deduce that Properties 1 and 2 of Invariant $\mathsf{InvGeneral}$. are satisfied by $\mathcal{M}_1$. Let $Y \in vars^2(\mathcal{C}_1)$. We know that either $Y \in \{X_1, \ldots, X_n\}$ or $Y \in vars^2(\mathcal{C})$. In the former case, we have that $Y\mathsf{mgu}(E_\Pi(\mathcal{C}_1)) = Y$ and so Property 3 of Invariant $\mathsf{InvGeneral}$. directly holds. In the latter case, we know that $\mathsf{mgu}(E_\Pi(\mathcal{C}_1)) = \mathsf{mgu}(E_\Pi(\mathcal{C}))\theta'$. Moreover, $\mathsf{C}\lfloor \mathsf{f}(X_1, \ldots, X_n)\rfloor_{\Phi(\mathcal{C}_1)} = \mathsf{f}(X_1, \ldots, X_n)$. Therefore, thanks to $\mathcal{C}$ and $\mathcal{C}_1$ being well formed (Property 1) and thanks to Lemma 3, we know that $\mathsf{C}\lfloor Y\mathsf{mgu}(E_\Pi(\mathcal{C}_1))\rfloor_{\Phi(\mathcal{C}_1)} = \mathsf{C}\lfloor Y\mathsf{mgu}(E_\Pi(\mathcal{C}))\rfloor_{\Phi(\mathcal{C})}\theta'$. Thus, since $\mathsf{path}(\xi) = \mathsf{path}(\xi')$, we have that if $\mathsf{path}(\xi) \in st(\mathsf{C}\lfloor Y\mathsf{mgu}(E_\Pi(\mathcal{C}_1))\rfloor_{\Phi(\mathcal{C}_1)})$, then $\mathsf{path}(\xi') \in st(\mathsf{C}\lfloor Y\mathsf{mgu}(E_\Pi(\mathcal{C}))\rfloor_{\Phi(\mathcal{C})})$ which would lead to $(\xi', i \rhd u') \notin \mathsf{NoUse}(\mathcal{C})$ which would allows us to deduce that $(\xi, i \rhd u) \notin \mathsf{NoUse}(\mathcal{C}_1)$.

Assume now that $(\xi, i \rhd u) \notin \mathsf{NoUse}(\mathcal{C}_1)$. Let $\zeta \in st(\xi)$. We know that $\xi = \xi'\theta'$. Hence either $\zeta \in \{X_1, \ldots, X_n\}$ or there exists $\zeta' \in st(\xi')$ such that $\zeta'\theta' = \zeta$. In the former case, Property 4 directly holds since $\mathsf{path}(\zeta)$ is not closed. In the latter case, if there exists v, j such that $(\zeta, j \rhd v) \in \Phi(\mathcal{C}_1)$ then it implies that $(\zeta', j \rhd v') \in \Phi(\mathcal{C})$ for some v' with $v'\sigma' = v$. But $\mathcal{M}$ satisfies $\mathsf{InvGeneral}$ hence $(\zeta', j \rhd v') \notin \mathsf{NoUse}(\mathcal{C})$ and so $(\zeta, j \rhd v) \notin \mathsf{NoUse}(\mathcal{C}_1)$.

Let us now focus on Properties 5, 6 and 7 of Invariant $\mathsf{InvGeneral}$. Let $\mathcal{C}_1, \mathcal{C}_1'$ be two constraint systems in the same column of $\mathcal{M}_1$. Let $\mathcal{C}, \mathcal{C}'$ the constraint systems in $\mathcal{M}$ from which $\mathcal{C}_1, \mathcal{C}_1'$ are respectively obtained. In such a case, we already shown above that $\mathsf{mgu}(E_\Pi(\mathcal{C}_1)) = \mathsf{mgu}(E_\Pi(\mathcal{C}))\theta'$ and $\mathsf{mgu}(E_\Pi(\mathcal{C}_1')) = \mathsf{mgu}(E_\Pi(\mathcal{C}'))\theta'$ where $\theta' = \{X \to \mathsf{f}(X_1, \ldots, X_n)\}$. Thanks to Lemma 3, we deduce that for all $Y \in S_2(\mathcal{C})$, $\mathsf{C}\lfloor Y\mathsf{mgu}(E_\Pi(\mathcal{C}_1))\rfloor_{\Phi(\mathcal{C}_1)} = \mathsf{C}\lfloor Y\mathsf{mgu}(E_\Pi(\mathcal{C}))\rfloor_{\Phi(\mathcal{C})}\theta'$ and $\mathsf{C}\lfloor Y\mathsf{mgu}(E_\Pi(\mathcal{C}_1'))\rfloor_{\Phi(\mathcal{C}_1')} = \mathsf{C}\lfloor Y\mathsf{mgu}(E_\Pi(\mathcal{C}'))\rfloor_{\Phi(\mathcal{C}')}\theta'$. But since $\mathcal{M}$ satisfies Invariant $\mathsf{InvGeneral}$, by Property 5, we obtain $\mathsf{C}\lfloor Y\mathsf{mgu}(E_\Pi(\mathcal{C}))\rfloor_{\Phi(\mathcal{C})} = \mathsf{C}\lfloor Y\mathsf{mgu}(E_\Pi(\mathcal{C}'))\rfloor_{\Phi(\mathcal{C}')}$ and so $\mathsf{C}\lfloor Y\mathsf{mgu}(E_\Pi(\mathcal{C}_1))\rfloor_{\Phi(\mathcal{C}_1)} = \mathsf{C}\lfloor Y\mathsf{mgu}(E_\Pi(\mathcal{C}_1'))\rfloor_{\Phi(\mathcal{C}_1')}$. Lastly since $S_2(\mathcal{C}_1) = S_2(\mathcal{C}) \cup \{X_1, \ldots, X_n\}$ and for all $i \in \{1, \ldots, n\}$, $\mathsf{C}\lfloor X_i\mathsf{mgu}(E_\Pi(\mathcal{C}_1))\rfloor_{\Phi(\mathcal{C}_1)} = X_i = \mathsf{C}\lfloor X_i\mathsf{mgu}(E_\Pi(\mathcal{C}_1'))\rfloor_{\Phi(\mathcal{C}_1')}$, we deduce that $\mathcal{M}_1$ satisfies Property 5 of Invariant $\mathsf{InvGeneral}$. Properties 6 and 7 directly hold since we do not add any disequalities in $\mathcal{M}_1$ compared to $\mathcal{M}$. We conclude that $\mathcal{M}_1$ satisfies Invariant $\mathsf{InvGeneral}$.

Rule $\textsc{Axiom}(X, \mathsf{path})$: Let us first start with $\mathcal{M}_2$. In such a case, for all $\mathcal{C}_2 \in \mathcal{M}_2$ different from $\bot$, if $\mathcal{C}$ is the constraint systems in $\mathcal{M}$ from which $\mathcal{C}_2$ is obtain then the rule added in $\mathcal{C}_2$ the disequality $X \neq^? \xi$ where $(\xi, i \rhd u) \in \Phi(\mathcal{C})$ and $\mathsf{path}(\xi) = \mathsf{path}$. In other words, for all $\mathcal{C}_2, \mathcal{C}_2'$, for all $(\xi, i \rhd u) \in \Phi(\mathcal{C}_2)$, for all $(\xi', i' \rhd u') \in \Phi(\mathcal{C}_2')$, if $\mathsf{path}(\xi) = \mathsf{path}(\xi') = \mathsf{path}$ then $E_\Pi(\mathcal{C}_2) \vDash X \neq^? \xi$ and $E_\Pi(\mathcal{C}_2') \vDash X \neq^? \xi'$. In combinaison with the fact that $\mathcal{M}$ satisfies $\mathsf{InvGeneral}$, we deduce that $\mathcal{M}_2$ satisfies Property 7 of $\mathsf{InvGeneral}$. Note that we also directly obtain from $\mathcal{M}$ satisfying $\mathsf{InvGeneral}$ that $\mathcal{M}_2$ satisfies Properties 5 and 6. Consider now $\mathcal{C}_2$ a constraint system in $\mathcal{M}_2$ and C a constraint system in $\mathcal{M}$ from which $\mathcal{C}_2$ is obtained. Let $(\sigma, \theta) \in \mathsf{Sol}(\mathcal{C}_2)$. Thanks to Lemma 5, we know that $(\sigma_{|vars^1(\mathcal{C})}, \theta_{|vars^2(\mathcal{C})}) \in \mathsf{Sol}(\mathcal{C})$. Moreover, we know by the rule that $\Phi(\mathcal{C}) = \Phi(\mathcal{C}_2)$, $\mathsf{NoUse}(\mathcal{C}) = \mathsf{NoUse}(\mathcal{C}_2)$, $E_\Pi(\mathcal{C}) = E_\Pi(\mathcal{C}_2)$ and $vars^2(\mathcal{C}) = vars^2(\mathcal{C}_2)$. Therefore, we deduce that Properties 1,2,3 and 4 of $\mathsf{InvGeneral}$ are satisfied by $\mathcal{M}_2$ since $\mathsf{InvGeneral}$ is satisfied by $\mathcal{M}$.

Let us now focus on $\mathcal{M}_1$. Consider $\mathcal{C}_1$ a constraint system from $\mathcal{M}_1$ and let $\mathcal{C}$ be

the constraint system in $\mathcal{M}$ from which $\mathcal{C}_1$ is obtained. Let $(\sigma, \theta) \in \mathsf{Sol}(\mathcal{C}_1)$. Thanks to Lemma 5, we know that $(\sigma_{|vars^1(\mathcal{C})}, \theta_{|vars^2(\mathcal{C})}) \in \mathsf{Sol}(\mathcal{C})$. Moreover, we have $\Phi(\mathcal{C}_1)\theta'\sigma' = \Phi(\mathcal{C}_1)$, $\mathsf{NoUse}(\mathcal{C})\theta'\sigma'$ and $\mathsf{mgu}(E_\Pi(\mathcal{C}_1)) = \mathsf{mgu}(E_\Pi(\mathcal{C}))\theta'$ where $\theta' = \{X \to \xi\}$, $(\xi, j \rhd v) \in \Phi(\mathcal{C})$, $\mathsf{path}(\xi) = \mathsf{path}$, $(X, i \vdash^? u) \in D(\mathcal{C})$ and $\sigma' = \mathsf{mgu}(u, v)$. Note that $X \notin vars^2(\xi)$ and $\Phi(\mathcal{C}_1)\theta\sigma = \Phi(\mathcal{C}_1)\theta'\sigma'\theta\sigma = \Phi(\mathcal{C})\theta\sigma$.

Let $(\zeta, k \rhd t) \in \Phi(\mathcal{C}_1)$. We know that there exists ζ', t' such that $(\zeta', k \rhd t') \in \Phi(\mathcal{C})$ and $\zeta = \zeta'\theta'$, $t = t'\sigma'$, $\zeta\theta = \zeta'\theta$ and $t\sigma = t'\sigma$. Since $\mathcal{M}$ satisfies $\mathsf{InvGeneral}$, we directly then deduce that Properties 1 and 2 of Invariant $\mathsf{InvGeneral}$. are satisfied by $\mathcal{M}_1$. Let $Y \in vars^2(\mathcal{C}_1)$. We know that $Y \in vars^2(\mathcal{C})$ and $\mathsf{mgu}(E_\Pi(\mathcal{C}_1)) = \mathsf{mgu}(E_\Pi(\mathcal{C}))\theta'$. Moreover, $\mathsf{C}\lfloor\xi\rfloor_{\Phi(\mathcal{C}_1)} = \mathsf{path}$. Therefore, thanks to $\mathcal{C}$ and $\mathcal{C}_1$ being well formed (Property 1) and thanks to Lemma 3, we know that $\mathsf{C}\lfloor Y\mathsf{mgu}(E_\Pi(\mathcal{C}_1))\rfloor_{\Phi(\mathcal{C}_1)} = \mathsf{C}\lfloor Y\mathsf{mgu}(E_\Pi(\mathcal{C}))\rfloor_{\Phi(\mathcal{C})}\{X \to \mathsf{path}\}$. Thus, since $\mathsf{path}(\zeta) = \mathsf{path}(\zeta')$, we have that if $\mathsf{path}(\zeta) \in st(\mathsf{C}\lfloor Y\mathsf{mgu}(E_\Pi(\mathcal{C}_1))\rfloor_{\Phi(\mathcal{C}_1)})$, then either $\mathsf{path}(\zeta') \in st(\mathsf{C}\lfloor Y\mathsf{mgu}(E_\Pi(\mathcal{C}))\rfloor_{\Phi(\mathcal{C})})$ or $\mathsf{path}(\zeta') = \mathsf{path}(\xi)$. In the former case, we know by Property 3 of $\mathsf{InvGeneral}$ satisfied by $\mathcal{M}$ that $(\zeta', k \rhd t') \notin \mathsf{NoUse}(\mathcal{C})$ which would allows us to deduce that $(\zeta, k \rhd t) \notin \mathsf{NoUse}(\mathcal{C}_1)$. In the latter case, we know by the application conditions of the rule that $(\xi, i \rhd v) \notin \mathsf{NoUse}(\mathcal{C})$ and so $(\xi, i \rhd v) \notin \mathsf{NoUse}(\mathcal{C}_1)$. This allows us to conclude that $\mathcal{M}_2$ satisfies Property 3 of $\mathsf{InvGeneral}$.

Assume now that $(\zeta, k \rhd t) \notin \mathsf{NoUse}(\mathcal{C}_1)$. Let $\beta \in st(\zeta)$ and ℓ, w such that $(\beta, \ell \rhd w) \in \Phi(\mathcal{C}_1)$. We know that $\zeta = \zeta'\theta'$. Hence either $\beta \in st(\xi)$ or there exists $\beta' \in st(\zeta')$ such that $\beta'\theta' = \beta$. In the former case, since $X \notin vars^2(\xi)$, we deduce that there exists w' such that $w'\sigma = w$ and $(\beta, \ell \rhd w') \in \Phi(\mathcal{C})$. But we know that $\mathcal{M}$ satisfies $\mathsf{InvGeneral}$. Hence by Property 4, we obtain that $(\beta, \ell \rhd w') \notin \mathsf{NoUse}(\mathcal{C})$ and so $(\beta, \ell \rhd w) \notin \mathsf{NoUse}(\mathcal{C}_1)$. In the latter case, if there exists w, ℓ such that $(\beta, \ell \rhd w) \in \Phi(\mathcal{C}_1)$ then it implies that $(\beta', j \rhd w') \in \Phi(\mathcal{C})$ for some w' with $w'\sigma' = w$. But $\mathcal{M}$ satisfies $\mathsf{InvGeneral}$ hence $(\beta', j \rhd w') \notin \mathsf{NoUse}(\mathcal{C})$ and so $(\beta, j \rhd w) \notin \mathsf{NoUse}(\mathcal{C}_1)$. This allows us to conclude that $\mathcal{M}_2$ satisfies Property 4.

Let us now focus on Properties 5, 6 and 7 of Invariant $\mathsf{InvGeneral}$. Let $\mathcal{C}_1, \mathcal{C}_1'$ be two constraint systems in the same column of $\mathcal{M}_1$. Let $\mathcal{C}, \mathcal{C}'$ the constraint systems in $\mathcal{M}$ from which $\mathcal{C}_1, \mathcal{C}_1'$ are respectively obtained. In such a case, we already shown above that $\mathsf{mgu}(E_\Pi(\mathcal{C}_1)) = \mathsf{mgu}(E_\Pi(\mathcal{C}))\theta_1$ and $\mathsf{mgu}(E_\Pi(\mathcal{C}_1')) = \mathsf{mgu}(E_\Pi(\mathcal{C}'))\theta_2$ where $\theta_1 = \{X \to \xi\}$, $\theta_2 = \{X \to \xi'\}$ and $\mathsf{path}(\xi) = \mathsf{path}(\xi') = \mathsf{path}$ for some $(\xi, i \rhd v) \in \Phi(\mathcal{C})$ and $(\xi', i' \rhd v') \in \Phi(\mathcal{C}')$. Thanks to Lemma 3, we deduce that for all $Y \in S_2(\mathcal{C})$, $\mathsf{C}\lfloor Y\mathsf{mgu}(E_\Pi(\mathcal{C}_1))\rfloor_{\Phi(\mathcal{C}_1)} = \mathsf{C}\lfloor Y\mathsf{mgu}(E_\Pi(\mathcal{C}))\rfloor_{\Phi(\mathcal{C})}\{X \to \mathsf{path}(\xi)\}$ and $\mathsf{C}\lfloor Y\mathsf{mgu}(E_\Pi(\mathcal{C}_1'))\rfloor_{\Phi(\mathcal{C}_1')} = \mathsf{C}\lfloor Y\mathsf{mgu}(E_\Pi(\mathcal{C}'))\rfloor_{\Phi(\mathcal{C}')}\{X \to \mathsf{path}(\xi')\}$. But since $\mathcal{M}$ satisfies Invariant $\mathsf{InvGeneral}$, by Property 5, we obtain that $\mathsf{C}\lfloor Y\mathsf{mgu}(E_\Pi(\mathcal{C}))\rfloor_{\Phi(\mathcal{C})} = \mathsf{C}\lfloor Y\mathsf{mgu}(E_\Pi(\mathcal{C}'))\rfloor_{\Phi(\mathcal{C}')}$ and so $\mathsf{C}\lfloor Y\mathsf{mgu}(E_\Pi(\mathcal{C}_1))\rfloor_{\Phi(\mathcal{C}_1)} = \mathsf{C}\lfloor Y\mathsf{mgu}(E_\Pi(\mathcal{C}_1'))\rfloor_{\Phi(\mathcal{C}_1')}$. This allows us to deduce that $\mathcal{M}_1$ satisfies Property 5 of Invariant $\mathsf{InvGeneral}$. Properties 6 and 7 directly hold since we do not add any disequalities in $\mathcal{M}_1$ compared to $\mathcal{M}$. We conclude that $\mathcal{M}_1$ satisfies Invariant $\mathsf{InvGeneral}$.

Rule EQ-FRAME-FRAME(ξ_1, ξ_2): This rule only add an equality or disequality between first-order terms. Hence the result directly hold since $\mathcal{M}$ satisfy $\mathsf{InvGeneral}$ and by applying Lemma 5.

Rule EQ-DED-DED(X, ξ): As before, we focus on the case where the rule is an external rule. On $\mathcal{M}_2$, we only added a disequality between first-order terms. Hence, by applying Lemma 5 and since $\mathcal{M}$ satisfy $\mathsf{InvGeneral}$, we directly obtain that $\mathcal{M}_2$ satisfied $\mathsf{InvGeneral}$.

Let us now consider $\mathcal{M}_1$. Let $\mathcal{C}_1$ be a constraint system from $\mathcal{M}_1$ and let $\mathcal{C}$ be the constraint system in $\mathcal{M}$ from which $\mathcal{C}_1$ is obtained. Let $(\sigma, \theta) \in \mathsf{Sol}(\mathcal{C}_1)$. Thanks to Lemma 5, we know that $(\sigma_{|vars^1(\mathcal{C})}, \theta_{|vars^2(\mathcal{C})}) \in \mathsf{Sol}(\mathcal{C})$. Moreover, we have $\Phi(\mathcal{C}_1)\theta'\sigma' = \Phi(\mathcal{C}_1)$, $\mathsf{NoUse}(\mathcal{C})\theta'\sigma'$ and $\mathsf{mgu}(E_\Pi(\mathcal{C}_1)) = \mathsf{mgu}(E_\Pi(\mathcal{C}))\theta'$ where $\theta' = \{X \to \xi\}$ and $\sigma' = \mathsf{mgu}(t, \mathsf{f}(x_1, \ldots, x_n))$. Note that $\Phi(\mathcal{C}_1)\theta\sigma = \Phi(\mathcal{C}_1)\theta'\sigma'\theta\sigma = \Phi(\mathcal{C})\theta\sigma$ and $\mathsf{C}\lfloor\xi\rfloor_{\Phi(\mathcal{C})} = \xi$.

Let $(\zeta, k \rhd t) \in \Phi(\mathcal{C}_1)$. We know that there exists ζ', t' such that $(\zeta', k \rhd t') \in \Phi(\mathcal{C})$ and $\zeta = \zeta'\theta'$, $t = t'\sigma'$, $\zeta\theta = \zeta'\theta$ and $u\sigma = u'\sigma$. Since $\mathcal{M}$ satisfies $\mathsf{InvGeneral}$, we directly then deduce that Properties 1 and 2 of Invariant $\mathsf{InvGeneral}$. are satisfied by $\mathcal{M}_1$. Let $Y \in vars^2(\mathcal{C}_1)$. We know that $Y \in vars^2(\mathcal{C})$ and $\mathsf{mgu}(E_\Pi(\mathcal{C}_1)) = \mathsf{mgu}(E_\Pi(\mathcal{C}))\theta'$. Moreover, $\mathsf{C}\lfloor\xi\rfloor_{\Phi(\mathcal{C}_1)} = \xi$. Therefore, thanks to $\mathcal{C}$ and $\mathcal{C}_1$ being well formed (Property 1) and thanks to Lemma 3, we know that $\mathsf{C}\lfloor Y\mathsf{mgu}(E_\Pi(\mathcal{C}_1))\rfloor_{\Phi(\mathcal{C}_1)} = \mathsf{C}\lfloor Y\mathsf{mgu}(E_\Pi(\mathcal{C}))\rfloor_{\Phi(\mathcal{C})}\theta'$. Thus, since $\mathsf{path}(\zeta) = \mathsf{path}(\zeta')$, we have that if $\mathsf{path}(\zeta) \in st(\mathsf{C}\lfloor Y\mathsf{mgu}(E_\Pi(\mathcal{C}_1))\rfloor_{\Phi(\mathcal{C}_1)})$, then $\mathsf{path}(\zeta') \in st(\mathsf{C}\lfloor Y\mathsf{mgu}(E_\Pi(\mathcal{C}))\rfloor_{\Phi(\mathcal{C})})$ which would lead to $(\zeta', k \rhd t') \notin \mathsf{NoUse}(\mathcal{C})$ which would allows us to deduce that $(\zeta, k \rhd t) \notin \mathsf{NoUse}(\mathcal{C}_1)$.

Assume now that $(\zeta, k \rhd t) \notin \mathsf{NoUse}(\mathcal{C}_1)$. Let $\beta \in st(\zeta)$. We know that $\zeta = \zeta'\theta'$. Hence either $\zeta \in st(\xi)$ or there exists $\beta' \in st(\zeta')$ such that $\beta'\theta' = \beta$. In the former case, Property 4 directly holds since $\xi \in \mathcal{T}(\mathcal{F}_c, \mathcal{X}^2)$. In the latter case, if there exists w, ℓ such that $(\beta, \ell \rhd w) \in \Phi(\mathcal{C}_1)$ then it implies that $(\beta', \ell \rhd w') \in \Phi(\mathcal{C})$ for some w' with $w'\sigma' = w$. But $\mathcal{M}$ satisfies $\mathsf{InvGeneral}$ hence $(\beta', \ell \rhd w') \notin \mathsf{NoUse}(\mathcal{C})$ and so $(\beta, \ell \rhd w) \notin \mathsf{NoUse}(\mathcal{C}_1)$.

Let us now focus on Properties 5, 6 and 7 of Invariant $\mathsf{InvGeneral}$. Let $\mathcal{C}_1, \mathcal{C}_1'$ be two constraint systems in the same column of $\mathcal{M}_1$. Let $\mathcal{C}, \mathcal{C}'$ the constraint systems in $\mathcal{M}$ from which $\mathcal{C}_1, \mathcal{C}_1'$ are respectively obtained. In such a case, we already shown above that $\mathsf{mgu}(E_\Pi(\mathcal{C}_1)) = \mathsf{mgu}(E_\Pi(\mathcal{C}))\theta'$ and $\mathsf{mgu}(E_\Pi(\mathcal{C}_1')) = \mathsf{mgu}(E_\Pi(\mathcal{C}'))\theta'$ where $\theta' = \{X \to \xi\}$. Thanks to Lemma 3, we deduce that for all $Y \in S_2(\mathcal{C})$, $\mathsf{C}\lfloor Y\mathsf{mgu}(E_\Pi(\mathcal{C}_1))\rfloor_{\Phi(\mathcal{C}_1)} = \mathsf{C}\lfloor Y\mathsf{mgu}(E_\Pi(\mathcal{C}))\rfloor_{\Phi(\mathcal{C})}\theta'$ and $\mathsf{C}\lfloor Y\mathsf{mgu}(E_\Pi(\mathcal{C}_1'))\rfloor_{\Phi(\mathcal{C}_1')} = \mathsf{C}\lfloor Y\mathsf{mgu}(E_\Pi(\mathcal{C}'))\rfloor_{\Phi(\mathcal{C}')}\theta'$. But since $\mathcal{M}$ satisfies Invariant $\mathsf{InvGeneral}$, by Property 5, we obtain $\mathsf{C}\lfloor Y\mathsf{mgu}(E_\Pi(\mathcal{C}))\rfloor_{\Phi(\mathcal{C})} = \mathsf{C}\lfloor Y\mathsf{mgu}(E_\Pi(\mathcal{C}'))\rfloor_{\Phi(\mathcal{C}')}$ and so $\mathsf{C}\lfloor Y\mathsf{mgu}(E_\Pi(\mathcal{C}_1))\rfloor_{\Phi(\mathcal{C}_1)} = \mathsf{C}\lfloor\mathsf{mgu}(E_\Pi(\mathcal{C}_1'))\rfloor_{\Phi(\mathcal{C}_1')}$. Lastly since $S_2(\mathcal{C}_1) = S_2(\mathcal{C})$ we deduce that $\mathcal{M}_1$ satisfies Property 5 of Invariant $\mathsf{InvGeneral}$. Properties 6 and 7 directly hold since we do not add any disequalities in $\mathcal{M}_1$ compared to $\mathcal{M}$. We conclude that $\mathcal{M}_1$ satisfies Invariant $\mathsf{InvGeneral}$.

Rule DED-ST(ξ, f): This rule preserves E_Π and only apply a first order substitution on Φ and NoUse. Moreover, the recipe variables $X_1, \ldots, X_n$ of the added constraints are fresh and not external (i.e. not in $S_2(\mathcal{C}_1)$ for some $\mathcal{C}_1$ in $\mathcal{M}_1$). Hence, by applying Lemma 5, we directly obtain from $\mathcal{M}$ satisfying $\mathsf{InvGeneral}$ that $\mathcal{M}_1$ satisfies $\mathsf{InvGeneral}$. □

Appendix C.4. Preservation of the invariants for Phase 1 (step by step)

In this subsection, we will establish invariants that are specific to Phase 1. Actually, we have to define an invariant for each step and also an invariant for the link between each step, *i.e.* we have to show that the invariant of the end of a step corresponds to the invariant at the beginning of the next step.

Let $(\mathcal{M}_0, \mathcal{M}_0')$ be a pair of matrices of constraint systems. We say that a pair of matrices of constraint systems $(\mathcal{M}_1, \mathcal{M}_1')$ is obtained from $(\mathcal{M}_0, \mathcal{M}_0')$ by applying Step i of Phase j of the strategy with parameters s (and k), for some $i \in \{a, b, c, d, e\}$, $j \in \{1, 2\}$ if $(\mathcal{M}_0, \mathcal{M}_0') \to^* (\mathcal{M}_1, \mathcal{M}_1')$ and the rules applied follow exactly the description of Step i of Phase j with parameters s (and k) given in Section 4.

Moreover, we will say that $(\mathcal{M}_1, \mathcal{M}'_1)$ is obtained from $(\mathcal{M}_0, \mathcal{M}'_0)$ at the end of Step i of Phase j of the strategy with parameters s (and k) if $(\mathcal{M}_0, \mathcal{M}'_0) \rightarrow^* (\mathcal{M}_1, \mathcal{M}'_1)$, the rules applied follow exactly the description of Step i of Phase j with parameters s (and k) given in Section 4 and no rule following the description of Step i of Phase j with parameters s (and k) is applicable on $(\mathcal{M}_1, \mathcal{M}'_1)$.

Invariant 9 ($\mathsf{PP1}(s)$)**.** *We say that a pair of matrices of constraint systems $(\mathcal{M}, \mathcal{M}')$ satisfies $\mathsf{PP1}(s)$ if $\mathcal{M}$ and $\mathcal{M}'$ have the same structure, satisfy $\mathsf{InvMatrix}(s)$ and $\mathsf{InvGeneral}$, and for all constraint systems $\mathcal{C}$ in $\mathcal{M}$ or $\mathcal{M}'$, $\mathcal{C}$ satisfies the invariants $\mathsf{InvVarConstraint}(s)$, $\mathsf{InvVarFrame}(s)$, $\mathsf{InvDest}(s)$, $\mathsf{InvNoUse}(s)$ and $\mathsf{InvUntouched}(s)$.*

Moreover, if $s = \mathsf{s}_{max}$ then $(\mathcal{M}, \mathcal{M}')$ satisfies also $\mathsf{InvDedsub}$.

Lemma 15. *Let $(\mathcal{M}, \mathcal{M}')$ be a pair of row matrices of initial constraint systems having the same structure. We have that $(\mathcal{M}, \mathcal{M}')$ satisfies $\mathsf{PP1}(0)$.*

Proof. We start by proving that $\mathcal{M}$ and $\mathcal{M}'$ satisfy $\mathsf{InvGeneral}$ (Invariant 1). First of all, item 5, 6 and 7 trivially hold since $\mathcal{M}$ and $\mathcal{M}'$ are row matrices, *i.e.* there is only one constraint system in each column of $\mathcal{M}$ and $\mathcal{M}'$. Furthermore, by definition of an initial constraint system, we know that for all $\mathcal{C}$ different from $\bot$, for all $(\xi, i \rhd u) \in \Phi(\mathcal{C})$, $\xi = ax_i$. Hence item 1 is trivially true. Moreover, for all $\xi' \in \Pi_r$ with $\mathsf{root}(\xi') \notin \mathcal{F}_c$, if $\mathsf{path}(\xi') = \mathsf{path}(\xi\theta)$ then $\mathsf{path}(\xi\theta) = \mathsf{path}(ax_i\theta) = \mathsf{path}(ax_i) = ax_i$. Hence, $\mathsf{path}(\xi') = ax_i$ implies $ax_i = \xi'$ and so item 2 holds. Since $\xi = ax_i$, then item 4 also holds. At last, $\mathcal{C}$ is an initial constraint system also implies $\mathsf{NoUse}(\mathcal{C}) = \emptyset$. Hence item 3 holds.

The invariants $\mathsf{InvMatrix}(0)$, $\mathsf{InvVarConstraint}(0)$, $\mathsf{InvVarFrame}(0)$, $\mathsf{InvDest}(0)$, $\mathsf{InvNoUse}(0)$ are trivially satisfied since their no deducible constraint $(X, i \vdash^? u)$ or frame element $(\xi, i \vdash^? u)$ such that $i \leq 0$.

It remains to prove that $(\mathcal{M}, \mathcal{M}')$ satisfies the invariant $\mathsf{InvUntouched}(0)$. We already know that for all constraint systems $\mathcal{C}$ in $\mathcal{M}$ or $\mathcal{M}'$. If $\mathcal{C}$ is different from $\bot$ then for all $(\xi, i \rhd u) \in \Phi(\mathcal{C})$, $\xi = ax_i$. Furthermore we know that $E_\Pi(\mathcal{C}) = \top$. At last, by definition of an initial constraint system $vars^2(D(\mathcal{C})) \subseteq S_2(\mathcal{C})$. Hence $\mathcal{C}$ satisfies the invariant $\mathsf{InvUntouched}(0)$. □

Appendix C.4.1. Invariants at Step a

We will show that the matrices satisfy the invariant $\mathsf{PP1Sa}(s)$. Moreover, at the end of this step, the matrices satisfy additional properties useful for the next steps. These properties are described in the invariant $\mathsf{PP1SaE}(s)$.

Invariant 10 ($\mathsf{PP1Sa}(s)$)**.** *We say that a pair of matrices of constraint systems $(\mathcal{M}, \mathcal{M}')$ satisfy $\mathsf{PP1Sa}(s)$ if $\mathcal{M}$ and $\mathcal{M}'$ have the same structure, satisfy $\mathsf{InvMatrix}(s-1)$ and $\mathsf{InvGeneral}$, and for all constraint system $\mathcal{C}$ in $\mathcal{M}$ or $\mathcal{M}'$, if $\mathcal{C} \neq \bot$ then*

1. *$\mathcal{C}$ satisfies invariants $\mathsf{InvDest}(s-1)$, $\mathsf{InvVarFrame}(s-1)$, $\mathsf{InvNoUse}(s-1)$, $\mathsf{InvUntouched}(s)$; and*
2. *for all $(\xi, s \rhd u) \in \Phi(\mathcal{C})$ with $u \in \mathcal{X}^1$, there exists $X \in S_2(\mathcal{C})$ and $\ell < s$ such that $(X, \ell \vdash^? u) \in D(\mathcal{C})$; and*
3. *for all $(\xi, s \rhd u) \in \Phi(\mathcal{C})$, either $\xi \in \mathcal{AX}$ or there exists $X_2, \ldots, X_n \in \mathcal{X}^2 \setminus S_2(\mathcal{C})$, $\mathsf{f} \in \mathcal{F}_d$ and $(\xi', p \rhd v) \in \Phi(\mathcal{C})$ such that $\xi = \mathsf{f}(\xi', X_2, \ldots, X_n)$ and $p \leq s$; and*

4. *for all* $(X, i \vdash^? u) \in D(\mathcal{C})$*, for all* $\mathsf{f} \in \mathcal{F}_c$*, for all* $(\xi, j \rhd v) \in \Phi(\mathcal{C})$*,* $E_\Pi(\mathcal{C}) \not\vdash X \neq^? \xi$ *and* $E_\Pi(\mathcal{C}) \not\vdash \mathsf{root}(X) \neq^? \mathsf{f}$*; and*

5. *for all* $(X, i \vdash^? u) \in D(\mathcal{C})$*,* $X \in S_2(\mathcal{C})$ *implies* $i = s$ *and there exists a unique frame element* $(\mathsf{g}(\xi_1, \ldots, \xi_n), j \rhd v) \in \Phi(\mathcal{C})$ *and* $k \in \{2, \ldots, n\}$ *such that* $j = s$ *and* $\xi_k = X$

Lemma 16. *Let* $(\mathcal{M}, \mathcal{M}')$ *be a pair of matrices of constraint systems that satisfies* $\mathsf{PP1}(s-1)$*. For all pair of matrices of constraint systems* $(\mathcal{M}_1, \mathcal{M}'_1)$ *obtained during Step a of the first phase on* $(\mathcal{M}, \mathcal{M}')$ *with support* s*, we have that* $(\mathcal{M}_1, \mathcal{M}'_1)$ *satisfies* $\mathsf{PP1Sa}(s)$*.*

Proof. Let $(\mathcal{M}_1, \mathcal{M}'_1)$ be a pair of matrices obtained during Step a of the first phase on $(\mathcal{M}, \mathcal{M}')$. We show by induction on the size N of the branch yielding to $(\mathcal{M}_1, \mathcal{M}'_1)$ that $(\mathcal{M}_1, \mathcal{M}'_1)$ satisfies the expected properties, and in addition we have that: for all $\mathcal{C}$ in $(\mathcal{M}_1, \mathcal{M}'_1)$,

6. for all $x \in vars^2(\{u \mid X, i \vdash^? u \in D(\mathcal{C}) \wedge i < s\})$, if for all $(X, i \vdash^? u) \in D(\mathcal{C})$, $X \in S_2(\mathcal{C})$ and $i < s$ implies $x \neq u$, then for all $u \in \{v \mid (\xi, i \rhd v) \in \Phi(\mathcal{C})$ or $(X, i \vdash^? v) \in D(\mathcal{C})\}$, for all position p, if $u|_p = x$ then there exists p' such that $p = p' \cdot 1$ and $u|_{p'} = \mathsf{pk}(x)$.

This property stated that when a variable is never a right hand term of a deducible constraint, then this variable is always used under the constructor pk.

Base case $N = 0$*:* In such a case we have that $(\mathcal{M}_1, \mathcal{M}'_1) = (\mathcal{M}, \mathcal{M}')$. Hence, we trivially have that $\mathcal{M}_1$ and $\mathcal{M}'_1$ satisfy $\mathsf{InvMatrix}(s-1)$ and $\mathsf{InvGeneral}$. Furthermore, we also have that for all $\mathcal{C}$ in $\mathcal{M}_1$ and $\mathcal{M}'_1$, $\mathcal{C}$ satisfies the invariant $\mathsf{InvVarFrame}(s-1)$ and $\mathsf{InvNoUse}(s-1)$. Furthermore, thanks to Lemma 13, we also have that $\mathcal{C}$ satisfies $\mathsf{InvUntouched}(s)$. We now prove the other properties:

6. We know that $\mathcal{C}$ satisfies $\mathsf{InvVarConstraint}(s-1)$ hence for all $x \in vars^2(\{u \mid X, i \vdash^? u \wedge i < s\})$, there exists $(X, i \vdash^? u) \in D(\mathcal{C})$ such that $x = u$ and $X \in S_2(\mathcal{C})$. Hence the property holds.

3. for all $(\xi, s \rhd x) \in \Phi(\mathcal{C})$, thanks to the property of origination of a constraint system, we know that there exists $(X, \ell \rhd u) \in D(\mathcal{C})$ such that $\ell < s$ and $x \in vars^1(u)$. But $\mathcal{C}$ satisfies $\mathsf{InvVarConstraint}(s-1)$ which means that $u \in \mathcal{X}^1$ and so $x = u$.

4. Since $\mathcal{C}$ satisfies $\mathsf{InvUntouched}(s-1)$, we know that for all $(\xi, s \rhd u) \in \Phi(\mathcal{C})$, $\xi = ax_s \in \mathcal{AX}$.

5. Since $\mathcal{C}$ satisfies $\mathsf{InvUntouched}(s-1)$, we know that for all $(X, k \vdash^? u) \in D(\mathcal{C})$, if $k \geq s$ then $X \notin vars^2(E_\Pi(\mathcal{C}))$. Hence for all $\mathsf{f} \in \mathcal{F}_c$, for all recipe ξ on a frame element of $\Phi(\mathcal{C})$, we have that $E_\Pi(\mathcal{C}) \not\vdash X \neq^? \xi$ and $E_\Pi(\mathcal{C}) \not\vdash \mathsf{root}(X) \neq^? \mathsf{f}$.

Inductive step $N > 0$*:* In such a case, there exists a pair $(\mathcal{M}_2, \mathcal{M}'_2)$ such that $(\mathcal{M}_2, \mathcal{M}'_2)$ is the father of $(\mathcal{M}_1, \mathcal{M}'_1)$. By our inductive hypothesis, we know that $(\mathcal{M}_2, \mathcal{M}'_2)$ satisfies the properties stated by the lemma. For all $\mathcal{C}$ in $(\mathcal{M}_1, \mathcal{M}'_1)$, there exists a constraint system $\mathcal{C}'$ in $(\mathcal{M}_2, \mathcal{M}'_2)$ such that $\mathcal{C}' \to \mathcal{C}$.

1. We know that $\mathcal{M}_2$ and $\mathcal{M}'_2$ satisfy $\mathsf{InvMatrix}(s-1)$, $\mathcal{M}_2 \to \mathcal{M}_1$, $\mathcal{M}'_2 \to \mathcal{M}_1$. Since the rule applied are of support s, then thanks to Lemma 12 we have that $\mathcal{M}_1$ and $\mathcal{M}'_1$ satisfy $\mathsf{InvMatrix}(s-1)$.

   Thanks to Lemma 14, we already know that Property 5 of $\mathsf{InvGeneral}$ is satisfied. Thus, it remains to prove the others properties. Let $(\sigma, \theta) \in \mathsf{Sol}(\mathcal{C})$ and let $(\xi, i \rhd u) \in \Phi(\mathcal{C})$. Thanks to Lemma 5, we know that there exists $(\sigma', \theta') \in \mathsf{Sol}(\mathcal{C}')$ such that $\theta' = \theta|_{vars^2(\mathcal{C}')}$ and $\sigma' = \sigma|_{vars^1(\mathcal{C}')}$ We do a case analysis on the rule applied

   - Case Eq-frame-ded: In such a case, we have that $E_\Pi(\mathcal{C}') = E_\Pi(\mathcal{C})$ and if $\Sigma = \mathsf{mgu}(E(\mathcal{C}))$, we have that $\Phi(\mathcal{C}) = \Phi(\mathcal{C}')\Sigma$ and $D(\mathcal{C}) = D(\mathcal{C}')\Sigma$. Hence we have $\theta = \theta'$. Thus since, by hypothesis, $\mathcal{C}'$ satisfies the Property 1 of $\mathsf{InvGeneral}$, we have $param(\xi\theta') \subseteq \{ax_1, \ldots, ax_i\}$ and so $param(\xi\theta) \subseteq \{ax_1, \ldots, ax_i\}$.
     Let $\xi' \in \Pi_r$ with $\mathsf{root}(\xi') \notin \mathcal{F}_c$, $\mathsf{path}(\xi') = \mathsf{path}(\xi\theta)$ and $\xi'(\Phi(\mathcal{C})\sigma)\downarrow \in \mathcal{T}(\mathcal{F}_c, \mathcal{N})$. Since $\theta = \theta'$, we have that $\mathsf{path}(\xi') = \mathsf{path}(\xi\theta')$. Furthermore, $\sigma' = \sigma|_{vars^1(\mathcal{C}')}$ implies that $\xi'(\Phi(\mathcal{C})\sigma)\downarrow = \xi'(\Phi(\mathcal{C}')\sigma')\downarrow$. Hence by hypothesis, since $\mathcal{C}$ satisfies Property 2 of $\mathsf{InvGeneral}$, we have $param(\xi') \not\subseteq \{ax_1, \ldots, ax_{i-1}\}$.
   - Case Dest when the guess is negative: The proof is similar to the case Eq-frame-ded.
   - Case Dest: Otherwise, we have that $E_\Pi(\mathcal{C}') = E_\Pi(\mathcal{C})$ and if $\Sigma = \mathsf{mgu}(E(\mathcal{C}))$, we have that $\Phi(\mathcal{C}) = \Phi(\mathcal{C}')\Sigma \cup \{\mathsf{g}(\zeta, X_2, \ldots, X_n), s \rhd w\}$ and $D(\mathcal{C}) = D(\mathcal{C}')\Sigma \cup \{X_i, s \rhd v_i\}_{i=2..n}$ where $X_2, \ldots, X_2$ are fresh variables, $(\zeta, j \rhd t) \in \Phi(\mathcal{C})$ and $j \leq s$. Let's denote $\zeta' = \mathsf{g}(\zeta, X_2, \ldots, X_n)$.
     Since $\mathcal{C}'$ satisfies $\mathsf{InvGeneral}$, we already know that $\mathsf{param}^{\mathcal{C}'}_{\mathsf{max}}(\zeta\theta) \leq j$. Furthermore, by definition of $(\sigma, \theta) \in \mathsf{Sol}(\mathcal{C})$, we have that $\mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(X_k\theta) \leq s$, for all $k = 2 \ldots n$. Hence we can conclude that $param(\zeta'\theta) \subseteq \{ax_1, \ldots, ax_s\}$.
     We now show that $ax_s \in st(\zeta'\theta)$. If $j = s$, then we have that $ax_s \in st(\zeta\theta)$ since $\mathcal{C}'$ satisfies $\mathsf{InvGeneral}$. Thus we conclude that $ax_s \in st(\zeta'\theta)$. Else $j < s$. $(\sigma', \theta') \in \mathsf{Sol}(\mathcal{C}')$ implies that $\sigma' \vDash ND(\mathcal{C}')$. But we know that $\mathcal{C}'$ also satisfies $\mathsf{InvDest}(s-1)$. Hence, $j < s$ and $\sigma' \vDash ND(\mathcal{C}')$ implies that there exists no recipe $(\xi_2, \ldots, \xi_n) \in \Pi_r$ such that $param(\xi_2, \ldots, \xi_n) \subseteq \{ax_1, \ldots, ax_{s-1}\}$ such that $\mathsf{g}(\zeta\theta', \xi_2, \ldots, \xi_n)(\Phi(\mathcal{C}')\sigma')\downarrow \in \mathcal{T}(\mathcal{F}_c, \mathcal{N})$. But we know that $\mathsf{g}(\zeta\theta', \xi_2, \ldots, \xi_n)(\Phi(\mathcal{C}')\sigma')\downarrow = \mathsf{g}(\zeta\theta, \xi_2, \ldots, \xi_n)(\Phi(\mathcal{C})\sigma)\downarrow$. At last, since $(\sigma, \theta) \in \mathsf{Sol}(\mathcal{C})$ implies $\zeta'\theta(\Phi(\mathcal{C})\sigma)\downarrow \in \mathcal{T}(\mathcal{F}_c, \mathcal{N})$, we can conclude that there exists $k \in \{2, \ldots, n\}$ such that $ax_s \in st(X_k\theta)$ and so $ax_s \in st(\zeta')$. Thus, $\mathcal{C}$ satisfies Properties 1 and 2 of $\mathsf{InvGeneral}$.

   It remains to prove Property 3 and 4 of the invariant $\mathsf{InvGeneral}$. Let $X \in vars^2(\mathcal{C})$ such that $\mathsf{path}(\xi) \in st(\mathsf{C}\lfloor X\mathsf{mgu}(E_\Pi(\mathcal{C}))\rfloor_\Phi)$. We know that the rule Eq-frame-ded and Dest do not modify E_Π. Furthermore, all new recipe variables introduced by the Dest are not instantiated during Step a. Hence if $\mathcal{C}''$ is the constraint system in $\mathcal{M}$ or $\mathcal{M}'$ such that $\mathcal{C}'' \to^* \mathcal{C}$, then we have we have that $\mathsf{path}(\xi) \in st(\mathsf{C}\lfloor X\mathsf{mgu}(E_\Pi(\mathcal{C}))\rfloor_\Phi)$ implies that $X \in vars^2(\mathcal{C}'')$ and $\mathsf{path}(\xi) \in st(\mathsf{C}\lfloor X\mathsf{mgu}(E_\Pi(\mathcal{C}''))\rfloor_\Phi)$. Furthermore, since $\mathcal{C}''$ satisfies $\mathsf{InvUntouched}(s-1)$, we can deduce that $i < s$. Hence, by hypothesis on $\mathcal{C}''$, we have that $(\xi, i \rhd u'') \notin \mathsf{NoUse}(\mathcal{C}'')$ where $u''\mathsf{mgu}(E(\mathcal{C}'')) = u$. At last, since during Step a with support s, Eq-frame-ded

only add frame element of the form $(\xi', s \rhd v)$ and $i < s$, we can conclude that $(\xi, i \rhd u) \notin \mathsf{NoUse}(\mathcal{C})$. Hence $\mathcal{C}$ satisfies Property 3 of $\mathsf{InvGeneral}$.

Assume now that $(\xi, i \rhd u) \notin \mathsf{NoUse}(\mathcal{C})$ and let $\xi' \in st(\xi)$ such that $(\xi', j \rhd v) \in \Phi(\mathcal{C}) \cap \mathsf{NoUse}(\mathcal{C})$. Since Eq-frame-ded only add frame elements of the form $(\zeta, s \rhd w)$ and $\mathcal{C}'$ satisfies Property 4 of $\mathsf{InvGeneral}$, we can deduce that $i = j = s$. Thus, the only way this case occur is if Dest was applied on a frame element which belong to NoUse or if Eq-frame-ded was applied on $(\xi', j \rhd v)$ after that Dest was applied on it. But this case is impossible since it would imply that $v \in \mathcal{X}^1$ and we now by definition of Dest that u is a strict subterm of v. Hence we have that $(\xi', j \rhd v) \notin \mathsf{NoUse}(\mathcal{C})$ and so $\mathcal{C}$ satisfies Property 4 of $\mathsf{InvGeneral}$.

2. Since $\mathcal{C}'$ is a constraint system in $(\mathcal{M}_2, \mathcal{M}_2')$, $\mathcal{C}'$ satisfies $\mathsf{InvVarFrame}(s-1)$, $\mathsf{InvNoUse}($ $s-1)$ and $\mathsf{InvUntouched}(s)$. Thanks to Lemmas 10 and 11, we can deduce that $\mathcal{C}$ satisfies $\mathsf{InvVarFrame}(s-1)$, $\mathsf{InvNoUse}(s-1)$ and $\mathsf{InvUntouched}(s)$.

6. Let $x \in vars^2(\{u \mid X, i \vdash^? u \in D(\mathcal{C}) \wedge i < s\})$ such that for all $(X, i \vdash^? u) \in D(\mathcal{C})$ such that $i < s$ and $X \in S_2(\mathcal{C})$, $x \neq u$. We know that $\mathcal{C}' \to \mathcal{C}$ hence we do a case analysis on the rule applied Dest or Eq-frame-ded:

   Case Eq-frame-ded(X, ξ)*:* We focus on the son which modifies the terms in the constraint systems, i.e. when the equality guess is true. Since Eq-frame-ded(X, ξ) is applicable then there exist i, u_0, v_0 such that $(X, i \vdash^? u_0) \in D(\mathcal{C}')$, $X \in S_2(\mathcal{C}')$ and $(\xi, s \rhd v_0) \in \Phi(\mathcal{C}')$. Let $\sigma = \mathsf{mgu}(u, v)$. We know that $\Phi(\mathcal{C}) = \Phi(\mathcal{C}')\sigma$ and $D(\mathcal{C}) = D(\mathcal{C}')\sigma$. But $x \in vars^2(\{(u \mid X, i \vdash^? u) \in D(\mathcal{C}) \wedge i < s\})$, thus it implies that $x \notin \mathrm{dom}(\sigma)$ and so $x' \in vars^2(\{(u \mid X, i \vdash^? u) \in D(\mathcal{C}') \wedge i < s\})$. Furthermore, it also implies that for all $(X, i \vdash^? u) \in D(\mathcal{C}')$ such that $i < s$ and $X \in S_2(\mathcal{C}')$, $x \neq u$. Indeed, if there exists $(X, i \vdash^? x) \in D(\mathcal{C}')$ then $(X, i \vdash^? x) \in D(\mathcal{C})$ which is a contradiction with our hypothesis.

   Let $t \in \{v \mid (\xi, i \rhd v) \in \Phi(\mathcal{C}) \text{ or } (X, i \rhd v) \in D(\mathcal{C})\}$, thus there exists $t' \in \{v \mid (\xi, i \rhd v) \in \Phi(\mathcal{C}') \text{ or } (X, i \rhd v) \in D(\mathcal{C}')\}$ such that $t'\sigma = t$. Let p a position such that $t|_p = x$.

   If $x \notin \mathrm{img}(\sigma)$, then we can deduce that $t'|_p = x$. Hence, by our inductive hypothesis, we have that there exists p' such that $p = p' \cdot 1$ and $t'|_{p'} = \mathsf{pk}(x)$ and so $t'\sigma|_{p'} = \mathsf{pk}(x)$.

   If $x \in \mathrm{img}(\sigma)$, then $x \in u_0$ or $x \in v_0$. But by our inductive hypothesis we have that for all p, if $u_0|_p = x$ then there exists p' such that $p = p' \cdot 1$ and $u_0|_{p'} = \mathsf{pk}(x)$. Hence by definition of the mgu, for all $y \in \mathrm{dom}(\sigma)$, $x \in vars(y\sigma)$ implies that either (a) $x = y\sigma$ or (b) there for all p, if $y\sigma|_p = x$ then there exists p' such that $p = p' \cdot 1$ and $y\sigma|_{p'} = \mathsf{pk}(x)$.

   Case (a): In such a case, we have that for all $(X, i \vdash^? u) \in D(\mathcal{C}')$ such that $i < s$ and $X \in S_2(\mathcal{C}')$, $y \neq u$. Indeed, if there exists $(X, i \vdash^? y) \in D(\mathcal{C}')$ then $(X, i \vdash^? x) \in D(\mathcal{C})$ which is a contradiction with our hypothesis. Hence, $t|_p = x$ implies that $t'|_p = y$ or $t'|_p = x$. If $t'|_p = x$ then the result holds similarly to the case $x \notin \mathrm{img}(\sigma)$. If $t'|_p = y$, we know by our inductive hypothesis that $t'|_{p'} = \mathsf{pk}(y)$ with $p = p' \cdot 1$ and so $t'\sigma|_{p'} = \mathsf{pk}(x)$. Hence the result holds.

   Case (b): Otherwise, $t|_p = x$ implies that $t'|_p = x$ or there exists p', p'' such that $p = p' \cdot p''$ and $t'|_{p'} = y$ and $y\sigma|_{p''} = x$. But by hypothesis on y, there exists p'''

such that $p'' = p''' \cdot 1$ and $y\sigma|_{p'''} = \mathsf{pk}(x)$, hence we have that $t'\sigma|_{p'\cdot p'''} = \mathsf{pk}(x)$. Hence the result holds.

Case $\textsc{Dest}(\xi, \ell \to r, s)$*:* Once again, we focus on the son which may instantiate the terms in the constraint system, i.e. when the guess is positive. Since $\textsc{Dest}(\xi, \ell \to r, s)$ is applicable then there exists $i \leq s, u_0$ such that $(\xi, i \rhd u_0) \in \Phi(\mathcal{C}')$. First of all, we deduce $u_0 \notin \mathcal{X}^1$. Indeed, if $u_0 \in \mathcal{X}^1$, then since $\mathcal{C}'$ satisfies the properties the lemma, we have that either $(\xi, i \rhd u_0) \in \mathsf{NoUse}(\mathcal{C}')$ if $i < s$, or else there exists $(X, j \vdash^? u_0) \in D(\mathcal{C}')$. Thus we would have that the rule $\textsc{Eq-frame-ded}(X, \xi)$ would be applicable which contradict the strategy that imposes that the rule Eq-frame-ded are prioritised over the rule Dest.

By definition of the rule Dest, we know that $\Phi(\mathcal{C}')\sigma \cup \{\xi', s \rhd w\sigma\} = \Phi(\mathcal{C})$ and $\{(X, i \vdash^? u) \in D(\mathcal{C}') \mid X \in S_2\}\sigma = \{(X, i \vdash^? u) \in D(\mathcal{C}) \mid X \in S_2\}$ where $\sigma = \mathsf{mgu}(u_0, v_1)$ and $\mathsf{g}(v_1, \ldots, v_n) \to x_1$ is a fresh instance of $\ell \to r$.

But the definition of $\ell \to r$ implies that $v_1 = \mathsf{f}(x_1, x_2)$, for $\mathsf{f} \in \{\mathsf{senc}, \langle\rangle, \mathsf{sign}\}$; or $v_1 = \mathsf{aenc}(x_1, \mathsf{pk}(x_2))$. Thus, since $u_0 \notin \mathcal{X}^1$, then we have $vars^2(D(\mathcal{C}')) \cap \mathrm{dom}(\sigma) = \emptyset$ when $\mathsf{f} \in \{\mathsf{senc}, \langle\rangle, \mathsf{sign}\}$. Hence the result holds. When $v_1 = \mathsf{aenc}(x_1, \mathsf{pk}(x_2))$, the only way to have $vars^2(D(\mathcal{C}')) \cap \mathrm{dom}(\sigma) \neq \emptyset$ is if $u_0 = \mathsf{aenc}(u_1, y)$ with $y \in vars^2(D(\mathcal{C}'))$. But in such a case, it implies that we have that $y\sigma = \mathsf{pk}(x_2)$. Thus if $x = x_2$ then x satisfies the properties since $x_2 \notin vars^1(\mathcal{C}')$ and $y\sigma = \mathsf{pk}(x_2)$.

3. Let $(\xi, s \rhd x) \in \Phi(\mathcal{C})$ with $x \in \mathcal{X}^1$. Thanks to the additional property (item 6), we know that if for all $(X, i \rhd v) \in D(\mathcal{C})$, $X \in S_2(\mathcal{C})$ and $i < s$ implies $v \neq x$, then all term in the frame, x are always used under the constructor pk. But it is not the case for $(\xi, s \rhd x)$. Hence, we deduce that there exists $(X, i \vdash^? v) \in D(\mathcal{C})$ such that $X \in S_2(\mathcal{C})$,$i < s$ and $v = x$.

4. The rule Eq-frame-ded and Dest do not modify $E_\Pi(\mathcal{C}')$. Hence, we only have to look at the new frame element that are added on the frame. But by definition of Dest, the application of $\textsc{Dest}(\xi, \ell \to r, s)$ implies the addition of a new element $(\mathsf{g}(\xi, X_2, \ldots, X_n), s \rhd w)$ where $\mathsf{g} \in \mathcal{F}_d$, $X_2, \ldots X_n$ are fresh, and there exists i, u such that $(\xi, i \rhd u) \in \Phi(\mathcal{C})$. Hence the result holds.

5. Once again, the rule Eq-frame-ded and Dest no not modify $E_\Pi(\mathcal{C}')$ hence $E_\Pi(\mathcal{C}') = E_\Pi(\mathcal{C})$. Hence, $\mathcal{C}'$ satisfies item 4 of Invariant 10 implies that $\mathcal{C}$ satisfies item 4 of Invariant 10. □

Lemma 17. *Let $(\mathcal{M}_1, \mathcal{M}_1')$ be a pair of matrices satisfying $\mathsf{PP1}(s-1)$. We consider a pair $(\mathcal{M}_2, \mathcal{M}_2')$ of matrices obtained from $(\mathcal{M}_1, \mathcal{M}_1')$ by applying Step a of Phase 1 of the strategy with parameters s. Moreover, we assume that* Dest *and* Eq-frame-ded *have been applied on each row as indicated in the strategy, and we consider a pair $(\mathcal{M}_2, \mathcal{M}_2')$ obtained at the end of such a sequence. For all constraint system $\mathcal{C}, \mathcal{C}'$ in $(\mathcal{M}_2, \mathcal{M}_2')$,*

1. *for all $(\xi, s \rhd u) \in \mathsf{NoUse}(\mathcal{C})$, there exists $X \in S_2(\mathcal{C})$ such that for all $\mathcal{C}''$ in $\mathcal{M}$ or $\mathcal{M}'$, if there exists $(\xi', s \rhd u') \in \mathsf{NoUse}(\mathcal{C}'')$ such that $\mathsf{path}(\xi') = \mathsf{path}(\xi)$ then $\mathsf{C}\lfloor X\mathsf{mgu}(E_\Pi(\mathcal{C}''))\rfloor_{\Phi(\mathcal{C}'')}\delta^1(\mathcal{C}'') = u'$. Else, by denoting $v' = \mathsf{C}\lfloor X\mathsf{mgu}(E_\Pi(\mathcal{C}''))\rfloor_{\Phi(\mathcal{C}'')}$ $\delta^1(\mathcal{C}'')$, we have that $E(\mathcal{C}'') \vDash v' \neq^? u'$.*

2. *for all* $(\xi, i \rhd u) \in \Phi(\mathcal{C}) \setminus \mathsf{NoUse}(\mathcal{C})$*, for all* $(\xi', i' \rhd u') \in \Phi(\mathcal{C}') \setminus \mathsf{NoUse}(\mathcal{C}')$*, if* $\mathsf{path}(\xi) = \mathsf{path}(\xi')$ *then* $\textsc{Dest}(\xi, \ell \to r, s)$ *is applicable on* $\mathcal{C}$ *is equivalent to* $\textsc{Dest}(\xi', \ell \to r, s)$ *is applicable on* $\mathcal{C}'$

Proof. The proof of this lemma follows the application of Dest and Eq-frame-ded in sequence. □

Invariant 11 ($\mathsf{PP1SaE}(s)$)**.** *We say that a pair of matrices* $(\mathcal{M}, \mathcal{M}')$ *satisfies* $\mathsf{PP1SaE}(s)$ *if* $\mathcal{M}$ *and* $\mathcal{M}'$ *have the same structure, satisfy* $\mathsf{InvMatrix}(s-1)$ *and* $\mathsf{InvGeneral}$*, and for each constraint system* $\mathcal{C}$ *in* $\mathcal{M}$ *or* $\mathcal{M}'$*, if* $\mathcal{C} \neq \bot$ *then* $\mathcal{C}$ *satisfies the invariants* $\mathsf{InvVarFrame}(s-1)$*,* $\mathsf{InvDest}(s)$*,* $\mathsf{InvNoUse}(s)$ *and* $\mathsf{InvUntouched}(s)$*. Moreover, for all* $(X, i \vdash^? u) \in D(\mathcal{C})$*,*

- $X \notin S_2(\mathcal{C})$ *implies that* $i = s$*.*
- *for all* $\mathsf{f} \in \mathcal{F}_c$*, for all* $\xi \in \Pi_r$*,* $E_\Pi(\mathcal{C}) \not\Vdash X \neq^? \xi$ *and* $E_\Pi(\mathcal{C}) \not\Vdash \mathsf{root}(X) \neq^? \mathsf{f}$*.*

Lemma 18. *Let* $(\mathcal{M}, \mathcal{M}')$ *be a pair of matrices satisfying* $\mathsf{PP1}(s-1)$*. For any pair of matrices* $(\mathcal{M}_1, \mathcal{M}'_1)$ *obtained from* $(\mathcal{M}, \mathcal{M}')$ *at the end of Step a of Phase 1 of the strategy with parameter* s*, we have that* $(\mathcal{M}_1, \mathcal{M}'_1)$ *satisfies* $\mathsf{PP1SaE}(s)$*.*

Proof. We know that each constraint system in $\mathcal{M}$ and $\mathcal{M}'$ satisfies $\mathsf{InvVarConstraint}(s-1)$. Hence, for all $\mathcal{C} \in M$ (resp. $\mathcal{M}'$), for all $(X, i \vdash^? u) \in D(\mathcal{C})$, $i \leq s-1$ implies that $X \in S_2(\mathcal{C})$. Moreover, $\mathcal{C}$ satisfies $\mathsf{InvUntouched}(s-1)$ which implies that if $i > s-1$ then $X \in S_2(\mathcal{C})$. Thus we deduce that $X \in S_2(\mathcal{C})$. But during the step a of Phase 1, only the rule Dest add new deducible constraint. Furthermore, Dest is applied with support s. Hence, Dest can only add deducible constraint of the form $Y, s \vdash^? v$. Thus for all $\mathcal{C}$, for all $(X, i \vdash^? u) \in D(\mathcal{C})$, if $X \notin S_2(\mathcal{C})$ then $i = s$.

Since $(\mathcal{M}, \mathcal{M}')$ satisfies $\mathsf{PP1}(s-1)$, we already know that $\mathcal{M}$ and $\mathcal{M}'$ satisfy the invariant $\mathsf{InvMatrix}(s-1)$. Furthermore, Lemma 16 also indicates that for all constraint system $\mathcal{C}$ in $\mathcal{M}$ or $\mathcal{M}'$, $\mathcal{C}$ satisfies the invariants $\mathsf{InvGeneral}$, $\mathsf{InvVarFrame}(s-1)$, $\mathsf{InvDest}(s-1)$, $\mathsf{InvNoUse}(s-1)$ and $\mathsf{InvUntouched}(s)$. Hence it remains to prove that $\mathcal{C}$ satisfies $\mathsf{InvDest}(s)$ and $\mathsf{InvNoUse}(s)$.

At the end of Step a, we know that the rules Dest and Eq-frame-ded are not applicable on a constraint system in $\mathcal{M}$ or $\mathcal{M}'$ for any parameter with support less or equal to s.

Invariant $\mathsf{InvNoUse}(s)$*:* Let $(\xi, p \rhd v) \in \Phi(\mathcal{C})$. If $p < s$ then, thanks to $\mathsf{InvNoUse}(s-1)$, the result holds. Else assume that $p = s$ and $v \in \mathcal{X}^1$. But, thanks to Lemma 16, we have that there exists $(X, i \vdash^? u) \in D(\mathcal{C})$ such that $u = v$ and $i < s$. Thus, since Eq-frame-ded is not applicable on $\mathcal{C}$, we have that either $(\xi, p \rhd v) \in \mathsf{NoUse}(\mathcal{C})$ or $E(\mathcal{C}) \vDash u \neq^? v$. But $u = v$ implies $E(\mathcal{C}) \vDash u \neq^? u$ which implies that $C{\downarrow} = \bot$ by normalisation, which is a contradiction with a fact that $\Phi(\mathcal{C})$. Thus we have that $(\xi, p \rhd v) \in \mathsf{NoUse}(\mathcal{C})$ and so $\mathcal{C}$ satisfies $\mathsf{InvNoUse}(s)$.

Invariant $\mathsf{InvDest}(s)$*:* Let $(\xi, p \rhd v) \in \Phi(\mathcal{C})$, $\mathsf{f} \in \mathcal{F}_d$ and $(\xi, p \rhd v) \notin \mathsf{NoUse}(\mathcal{C})$ and $p \leq s$. We do a case analysis on p:

- Case $p = s$: In such a case, we only have to show that either $(\xi', s \rhd v') \in \Phi(\mathcal{C})$ for some ξ' such that $\mathsf{path}(\xi') = \mathsf{f} \cdot \mathsf{path}(\xi)$; or else $ND \vDash \forall \tilde{x}, v \neq u_1 \vee s \not\vdash^? u_2 \vee$

$\ldots \vee s \not\vdash^? u_n$ where $\mathsf{f}(u_1, \ldots, u_n) \to w$ is a fresh renaming of a rewriting rule with $vars^1(u_1, \ldots, u_n, w) = \tilde{x}$.

But we know that DEST is not applicable on $\mathcal{C}$ for any parameter with support s. Hence $\text{DEST}(\xi, \mathsf{f}(u_1, \ldots, u_n) \to w, s)$ is not applicable. But since $\xi, \mathsf{f}(u_1, \ldots, u_n) \to w$ and s are valid parameter for $\mathcal{C}$, it implies that $\text{DEST}(\xi, \mathsf{f}(u_1, \ldots, u_n) \to w, s)$ was already applied and so the definition of the rule DEST in Figure 1 allows us to conclude.

- Case $p < s$: We know that $\mathcal{C}$ satisfies $\mathsf{InvDest}(s-1)$. Hence, we have to show that if for every $p \leq k \leq s-1$, $ND \vDash \forall \tilde{x}, v \neq u_1 \vee s-1 \not\vdash^? u_2 \vee \ldots \vee s-1 \not\vdash^? u_n$ where $\mathsf{f}(u_1, \ldots, u_n) \to w$ is a fresh rewriting rule with $vars^1(u_1, \ldots, u_n, w) = \tilde{x}$, then either $(\xi', s \rhd v') \in \Phi(\mathcal{C})$ for some ξ' such that $\mathsf{path}(\xi') = \mathsf{f} \cdot \mathsf{path}(\xi)$; or else $ND \vDash \forall \tilde{x}, v \neq u_1 \vee s \not\vdash^? u_2 \vee \ldots \vee s \not\vdash^? u_n$.

  But once again, we know that DEST is not applicable on $\mathcal{C}$ for any parameter with support s. Hence $\text{DEST}(\xi, \mathsf{f}(u_1, \ldots, u_n) \to w, s)$ is not applicable. But since ξ, $\mathsf{f}(u_1, \ldots, u_n) \to w$ and s are valid parameter for $\mathcal{C}$, it implies that $\text{DEST}(\xi, \mathsf{f}(u_1, \ldots, u_n) \to w, s)$ was already applied and so the definition of the rule DEST in Figure 1 allows us to conclude. □

Appendix C.4.2. Invariants at Step b

Given a pair of matrices $(\mathcal{M}, \mathcal{M}')$ such that $\mathcal{M}$ (resp. $\mathcal{M}'$) has n columns (resp. n'), we say that the k^{th} column of $(\mathcal{M}, \mathcal{M}')$ is either the k^{th} column of $\mathcal{M}$ if $k \leq n$; or else the $(k-n)^{\text{th}}$ column of $\mathcal{M}'$ if $k > n$. If $n + n' < k$ then the k^{th} column of $(\mathcal{M}, \mathcal{M}')$ is not defined. Moreover, will assume from now on that m is the size of a frame of a constraint system in $\mathcal{M}$ or $\mathcal{M}'$.

Invariant 12 ($\mathsf{PP1Sb}(s,k)$)**.** *We say that a pair of matrices of constraint systems $(\mathcal{M}, \mathcal{M}')$ satisfy $\mathsf{PP1Sb}(s,k)$ if $(\mathcal{M}, \mathcal{M}')$ satisfies $\mathsf{PP1SaE}(s)$ and for all $i \leq k$, for all constraint systems $\mathcal{C}$ in the i^{th} column of $(\mathcal{M}_1, \mathcal{M}'_1)$, $\mathcal{C}$ also satisfies $\mathsf{InvVarConstraint}(s)$ and $\mathsf{InvVarFrame}(s)$ (and $\mathsf{InvDedsub}$ when $s = \mathsf{s}_{max}$)*

First, we trivially have the following result.

Lemma 19. *Let $(\mathcal{M}, \mathcal{M}')$ be a pair of matrices satisfying $\mathsf{PP1SaE}(s)$. We have that $(\mathcal{M}, \mathcal{M}')$ satisfies $\mathsf{PP1Sb}(s, 0)$.*

Invariant 13 ($\mathsf{PP1SbE}(s,k)$)**.** *A pair of matrices $(\mathcal{M}, \mathcal{M}')$ satisfies $\mathsf{PP1SbE}(s,k)$ if $\mathcal{M}$ and $\mathcal{M}'$ have the same structure, satisfy $\mathsf{InvMatrix}(s-1)$ and $\mathsf{InvGeneral}$, and for all constraint systems $\mathcal{C}$ in $\mathcal{M}$ or $\mathcal{M}'$, if $\mathcal{C} \neq \bot$ then $\mathcal{C}$ satisfies the invariants $\mathsf{InvVarFrame}(s-1)$, $\mathsf{InvDest}(s)$, $\mathsf{InvNoUse}(s)$ and $\mathsf{InvUntouched}(s)$. Moreover, for all constraint systems $\mathcal{C}$ in the k^{th} column of $(\mathcal{M}_1, \mathcal{M}'_1)$, for all $(X, i \vdash^? u) \in D(\mathcal{C})$,*

- *$X \notin S_2(\mathcal{C})$ implies $u \in \mathcal{X}^1$ and $i = s$.*
- *for all $\mathsf{f} \in \mathcal{F}_c$, for all $\xi \in \Pi_r$, $E_\Pi(\mathcal{C}) \nvDash X \neq^? \xi$ and $E_\Pi(\mathcal{C}) \nvDash \mathsf{root}(X) \neq^? \mathsf{f}$.*
- *if $s = \mathsf{s}_{max}$ then $\mathcal{C}$ satisfies $\mathsf{InvDedsub}$.*

At last, for all $i \leq k$, for all constraint systems $\mathcal{C}$ in the i^{th} column of $(\mathcal{M}_1, \mathcal{M}'_1)$, $\mathcal{C}$ also satisfies $\mathsf{InvVarConstraint}(s)$ and $\mathsf{InvVarFrame}(s)$ (and $\mathsf{InvDedsub}$ when $s = \mathsf{s}_{max}$).

Lemma 20. *Let $(\mathcal{M}, \mathcal{M}')$ be a pair of matrices satisfying* $\mathsf{PP1Sb}(s,k)$. *For all pair $(\mathcal{M}_1, \mathcal{M}'_1)$ obtained at the end of Step b of the first phase with support s and column k on $(\mathcal{M}, \mathcal{M}')$, we have that $(\mathcal{M}_1, \mathcal{M}'_1)$ satisfies* $\mathsf{PP1SbE}(s,k)$.

Proof. During Step b of the first phase, the rule DEST and EQ-FRAME-DED are not applied. Furthermore, the rules that are applied have a support less or equal to s. Hence, thanks to Lemmas 14, 10, 11 and 12, we can deduce that $\mathcal{M}_1$ and $\mathcal{M}'_1$ satisfy $\mathsf{InvMatrix}(s-1)$, and for all $\mathcal{C}$ in $\mathcal{M}_1$ or $\mathcal{M}'_1$, $\mathcal{C}$ satisfies $\mathsf{InvGeneral}$, $\mathsf{InvVarFrame}(s-1)$, $\mathsf{InvNoUse}(s)$, $\mathsf{InvDest}(s)$, $\mathsf{InvDedsub}$ (when $s = \mathsf{s}_{max}$) and $\mathsf{InvUntouched}(s)$.

At the end of Step b, we cannot applied the rule DED-ST. Hence for all $(\xi, p \rhd v) \in \Phi(\mathcal{C})$, we know that DED-ST$(\xi, \mathsf{f})$ is useless for any $\mathsf{f} \in \mathcal{F}_c$. However, the definition of DED-ST(ξ, f) being useless for all ξ and path implies the invariant $\mathsf{InvDedsub}$. Thus we deduce that $\mathcal{C}$ satisfies the invariant $\mathsf{InvDedsub}$.

Let $(X, i \vdash^? u) \in D(\mathcal{C})$. Since $(\mathcal{M}_1, \mathcal{M}'_1)$ is obtained at the end of step b, we know that CONS(X, f) is not strongly applicable on $\mathcal{C}$, for all $\mathsf{f} \in \mathcal{F}_c$. Hence it implies that $u \in \mathcal{X}^1$ and either (a) for all $\mathsf{f} \in \mathcal{F}_c$, $E_\Pi(\mathcal{C}) \vDash \mathsf{root}(X) \neq^? \mathsf{f}$; or (b) for all $\mathsf{f} \in \mathcal{F}_c$, $E_\Pi(\mathcal{C}) \nvDash \mathsf{root}(X) \neq^? \mathsf{f}$.

In case (a), since AXIOM(X, ξ) is not strongly applicable on $\mathcal{C}$, for all ξ, we deduce that for all $(\xi, j \rhd v) \in \Phi(\mathcal{C})$, if $j \leq i$ then $E_\Pi(\mathcal{C}) \vDash X \neq^? \xi$. But $\mathcal{C}$ satisfies $\mathsf{InvNoUse}(s)$, $\mathsf{InvDest}(s)$, i.e. the rule DEST$(\xi, \ell \to r, s)$ is useless for all ξ and $\ell \to r$. Thus, by Definition 11 of the normalisation, we would have that $\mathcal{C}{\downarrow} = \bot$ which is a contradiction with the fact that $D(\mathcal{C}) \neq \emptyset$. Hence this case is impossible.

In Case (b), the rule AXIOM can only be applied during Step b if the strong application conditions of the rule are satisfied. But since $u \in \mathcal{X}^1$ and for all $\mathsf{f} \in \mathcal{F}_c$, $E_\Pi(\mathcal{C}) \nvDash \mathsf{root}(X) \neq^? \mathsf{f}$, we deduce that the rule AXIOM(X, path) was never applied during step b for any path. Hence, we deduce that for all ξ, $E_\Pi \nvDash X \neq^? \xi$. Hence the result holds.

At last, we know that the only rules that add deducible constraints during step b are CONS and DED-ST. But DED-ST is only applied when $i = s$ and it creates deducible constraints of the form $X, s \vdash^? u$. On the other hand, thanks to Lemma 18, we know that for all $\mathcal{C}$ in $\mathcal{M}$ or $\mathcal{M}'$, for all $(X, i \vdash^? u) \in D(\mathcal{C})$, if $X \notin S_2$ then $i = s$. But, according to Figure 1, by applying CONS(Y, f) for some $\mathsf{f} \in \mathcal{F}_c$ and $Y, i \vdash^? v$, if $Y \in S_2$ (resp. $\notin S_2$) then the rule CONS creates new deducible constraint of the form $(Z, i \vdash^? w)$ where Z is in S_2 (resp. not in S_2). Since for all $\mathcal{C}$ in $\mathcal{M}$ or $\mathcal{M}'$, for all $(X, i \vdash^? u) \in D(\mathcal{C})$, if $X \notin S_2$ then $i = s$, we deduce that the index of any new deducible constraints created by CONS whose recipe variables are not in S_2 is necessary s. Thus the result holds. □

Appendix C.4.3. Invariants at Step c

Before focusing on the invariants satisfied during the step c of Phase 1 of the strategy, we need to prove the following lemma.

Lemma 21. *Let $\mathcal{C}$ be a well-formed constraint system. For all $(Y, p \vdash^? u) \in D$, for all $x \in vars^1(u)$, we have that there exists $(X, q \vdash^? v) \in D$ such that $x \in vars^1(v)$, $q \leq p$ and $X \in S_2$.*

Proof. Let $\mathcal{C}$ be a well-formed constraint system and $\mathcal{C}_1$, $\mathcal{C}_2$ the two constraint systems obtained by application of the rule on $\mathcal{C}$.

For any rule, only disequations and non-deducibility constraint are added on $\mathcal{C}_2$. Thus, we trivially have that $D(\mathcal{C}) = D(\mathcal{C}_2)$, $\Phi(\mathcal{C}) = \Phi(\mathcal{C}_2)$ and $S_2(\mathcal{C}) = S_2(\mathcal{C}_2)$. Therefore, we can conclude that $\mathcal{C}_2$ satisfies the property.

We focus now $\mathcal{C}_1$. First of all, we prove that the application of a substitution preserves the property. Let σ be a substitution such that $\mathrm{dom}(\sigma) \cap \mathrm{img}(\sigma) = \emptyset$. Let $(Y, p \vdash^? u\sigma) \in D(\mathcal{C}\sigma)$, let $x \in vars^1(u\sigma)$.

- if $x \in vars^1(u)$, then by hypothesis, there exists $(X, q \vdash^? v) \in D(\mathcal{C})$ such that $x \in vars^1(v)$, $q \leq p$ and $X \in S_2(\mathcal{C})$. But $\mathrm{dom}(\sigma) \cap \mathrm{img}(\sigma) = \emptyset$, which means that $x \in vars^1(v\sigma)$. Since $S_2(\mathcal{C}) = S_2(\mathcal{C}\sigma)$, the result holds.
- if $x \notin vars^1(u)$, it means that $x \in \mathrm{img}(\sigma)$ and that there exists $y \in vars^1(u)$ such that $x \in vars^1(y\sigma)$. Thus by hypothesis, we have that there exists $(X, q \vdash^? v) \in D(\mathcal{C})$ such that $y \in vars^1(v)$, $q \leq p$ and $X \in S_2(\mathcal{C})$. Therefore, we have $x \in vars^1(v\sigma)$ which prove the result.

We prove the result by case analysis on the rule applied on a constraint system :

Rule Cons: The substitution $\sigma = \mathsf{mgu}(t =^? \mathsf{f}(x_1, \ldots, x_n))$ was applied on $\mathcal{C}$, with $x_1, \ldots, x_n$ fresh variables. Hence we know that $\mathcal{C}\sigma$ satisfies the property. Let first assume that the rule Cons was applied on $(X, i \vdash^? t)$ such that $X \notin S_2(\mathcal{C})$. In such a case, we have that $S_2(\mathcal{C}) = S_2(\mathcal{C}_1)$. On $\mathcal{C}_1$, the deducible constraints $(X_k, i \vdash^? x_k\sigma)$ are added, for all $j \in \{1, \ldots, n\}$. Since $\sigma = \mathsf{mgu}(t =^? \mathsf{f}(x_1, \ldots, x_n))$, we know that $vars^1(x_1\sigma, \ldots, x_n\sigma) = vars^1(t\sigma)$. Thus for all $x \in vars^1(x_k\sigma)$, there exists $(Y, q \vdash^? v\sigma) \in D(\mathcal{C})$ such that $x \in vars^1(v)$, $q \leq i$ and $Y \in S_2(\mathcal{C}\sigma) = S_2(\mathcal{C}_1)$, which proves the result.

If we assume now that $X \in S_2(\mathcal{C})$, by application of the rule, we have $S_2(\mathcal{C}_1) = S_2(\mathcal{C}) \cup \{X_1, \ldots X_n\}$. Thus for all $(Y, p \vdash^? u\sigma) \in D(\mathcal{C}_1)$, for all $x \in u\sigma$, we know by hypothesis that there exists $(Z, q \vdash^? v\sigma) \in D(\mathcal{C}\sigma)$ such that $x \in vars^1(v\sigma)$, $q \leq p$ and $Z \in S_2(\mathcal{C}\sigma)$. If $Z \neq X$ then the result holds, else we know that $\sigma = \mathsf{mgu}(t =^? \mathsf{f}(x_1, \ldots, x_n))$ and so $vars^1(x_1\sigma, \ldots, x_n\sigma) = vars^1(t\sigma)$. Therefore, there exists $k \in \{1 \ldots n\}$ such that $x \in vars^1(x_k\sigma)$, which also proves the result.

Rule Axiom(X, path): Assume that the rule is applied on $(X, i \vdash^? u) \in D$ and $(\xi, j \rhd v) \in \Phi$ with $\mathsf{path}(\xi) = \mathsf{path}$. The substitution $\sigma = \mathsf{mgu}(u =^? v)$ was applied on $\mathcal{C}$ thus we know that $\mathcal{C}\sigma$ satisfies the property. Furthermore, the deducible constraint $X, i \vdash^? u$ was removed from $D(\mathcal{C})$ in $\mathcal{C}_1$. If $X \notin S_2(\mathcal{C}_1)$ then the result trivially holds. Else, let $(Y, p \vdash^? w\sigma) \in D(\mathcal{C}_1)$ such that $Y \notin S_2(\mathcal{C}_1)$. By hypothesis, we know that for all $x \in vars^1(w\sigma)$, there exists $(Z, q \vdash^? t\sigma) \in D(\mathcal{C}\sigma)$ such that $x \in vars^1(t\sigma)$, $Z \in S_2(\mathcal{C}\sigma)$ and $q \leq p$. If $Z \neq X$ then the result holds, else $x \in vars^1(u\sigma)$ implies that $x \in vars^1(v\sigma)$ since $\sigma = \mathsf{mgu}(u =^? v)$. But the rule tells us that $j \leq i$ and so $j \leq p$. Furthermore, by Definition of a constraint system, we know that there exists $(Z', k \vdash^? u') \in D(\mathcal{C}_1)$ such that $x \in vars^1(u')$ and $k < j$. But $(Z', k \vdash^? u') \in D(\mathcal{C}\sigma)$ and so by hypothesis, there exists $(Y', k' \vdash^? v') \in D(\mathcal{C}\sigma)$ such that $x \in vars^1(v')$, $k' \leq k$ and $Y' \in S_2(\mathcal{C}\sigma)$. Since $k' \leq k < i$ then we have $Y' \neq X$ which implies that $(Y', k' \vdash^? v') \in D(\mathcal{C}_1)$ and $Y' \in S_2(\mathcal{C}_1)$. Hence the result holds.

Rule Dest$(\xi, \ell \to r, i)$: Assume that the rule is applied on $(\xi, j \rhd v) \in \Phi(\mathcal{C})$ with $\mathsf{f}(u_1, \ldots, u_n) \to w$ a fresh variant of $\ell \to r$. The substitution $\sigma = \mathsf{mgu}(v =^? u_1)$ was

applied on $\mathcal{C}$ thus we know that $\mathcal{C}\sigma$ satisfies the property. Furthermore, only deducible constraints $(X_i, j \vdash^? u_i\sigma)$ were added on $\mathcal{C}_1$ such that $X_i \notin S_2(\mathcal{C}_1)$, for all $i \in \{2, \ldots, n\}$. Since by definition of our rewriting rules, $vars^1(u_2, \ldots, u_n) \subseteq vars^1(u_1)$, we have for all $i \in \{2 \ldots n\}$, for all $x \in vars^1(u_i\sigma)$, $x \in vars^1(v\sigma)$. Thus by Definition of a constraint system, we have that there exists $(Z, k \vdash^? t) \in D(\mathcal{C}_1)$ such that $x \in vars^1(t)$, $k < j$and so $k < i$. But $k < i$ implies that $(Z, k \vdash^? t) \in D(\mathcal{C}\sigma)$. Hence there exists $(Z', k' \vdash^? t') \in D(\mathcal{C}\sigma)$ such that $Z' \in S_2(\mathcal{C}\sigma)$, $k' \leq k'$ and $x \in vars^1(\mathcal{C}\sigma)$. But, it implies that $(Z, k' \vdash^? t') \in D(\mathcal{C}_1)$ and $Z' \in S_2(\mathcal{C}_1)$. Hence the result holds.

Rule Eq-frame-frame, Eq-frame-ded and Eq-ded-ded: For those rules, $D(\mathcal{C}\sigma) = D(\mathcal{C}_1)$ and $S_2(\mathcal{C}\sigma) = S_2(\mathcal{C}_1)$ hence the result trivially holds.

Rule Ded-st(ξ, f): Assume that the rule is applied on $(\xi, i \rhd u)$. The substitution $\sigma = \mathsf{mgu}(u =^? \mathsf{f}(x_1, \ldots, x_n))$ was applied on $\mathcal{C}$ with $x_1, \ldots, x_n$ fresh variables. Thus we know that $\mathcal{C}\sigma$ satisfies the property. Furthermore, only deducible constraints $(X_i, \mathsf{s}_{max} \vdash^? x_i\sigma)$ were added on $\mathcal{C}_1$ such that $X_i \notin S_2(\mathcal{C}_1)$, for all $i \in \{1, \ldots, n\}$. Since $\sigma = \mathsf{mgu}(u =^? \mathsf{f}(x_1, \ldots, x_n))$, we have for all $i \in \{1 \ldots n\}$, for all $x \in vars^1(x_i\sigma)$, $x \in vars^1(u\sigma)$. Thus by definition of a constraint system, we have that there exists $(X, k \vdash^? t) \in D(\mathcal{C}_1)$ with $x \in vars^1(t)$, $t < i$ and so $t < \mathsf{s}_{max}$. But $t < \mathsf{s}_{max}$ implies that $(X, k \vdash^? t) \in D(\mathcal{C}\sigma)$ which means that there exists $(X', k' \vdash^? t') \in D(\mathcal{C}\sigma)$ with $x \in vars^1(t)$, $X' \in S_2(\mathcal{C}\sigma)$ and $k' \leq k$ and so $k' < \mathsf{s}_{max}$. It implies that $(X', k', \vdash^? t') \in D(\mathcal{C}_1)$ and $X' \in S_2(\mathcal{C}_1)$. Hence the result holds. □

Invariant 14 ($\mathsf{PP1ScE}(s, k)$)**.** *We say that a pair of matrices $(\mathcal{M}, \mathcal{M}')$ satisfy $\mathsf{PP1ScE}(s, k)$ if $\mathcal{M}$ and $\mathcal{M}'$ have the same structure, satisfy $\mathsf{InvMatrix}(s-1)$ and $\mathsf{InvGeneral}$, and for all constraint system $\mathcal{C}$ in $\mathcal{M}$ or $\mathcal{M}'$, if $\mathcal{C} \neq \bot$ then $\mathcal{C}$ satisfies the invariants $\mathsf{InvVarFrame}(s-1)$, $\mathsf{InvDest}(s)$, $\mathsf{InvNoUse}(s)$ and $\mathsf{InvUntouched}(s)$. Moreover, for all constraint systems $\mathcal{C}$ in the k^{th} column of $(\mathcal{M}_1, \mathcal{M}'_1)$, for all $(X, i \vdash^? u) \in D(\mathcal{C})$, we have that:*

- *$X \notin S_2(\mathcal{C})$ implies $u \notin \mathcal{X}^1$.*
- *for all $\mathsf{f} \in \mathcal{F}_c$, for all $\xi \in \Pi_r$, $E_\Pi \nVdash \mathsf{root}(X) \neq^? \mathsf{f}$ and $E_\Pi \nVdash X \neq^? \xi$*
- *if $s = \mathsf{s}_{max}$ then $\mathcal{C}$ satisfies $\mathsf{InvDedsub}$.*

At last, for all $i \leq k$, for all constraint systems $\mathcal{C}$ in the i^{th} column of $(\mathcal{M}_1, \mathcal{M}'_1)$, $\mathcal{C}$ also satisfies $\mathsf{InvVarConstraint}(s)$, $\mathsf{InvVarFrame}(s)$ (and $\mathsf{InvDedsub}$ when $s = \mathsf{s}_{max}$).

Lemma 22. *Let $(\mathcal{M}, \mathcal{M}')$ be a pair of matrices of constraint systems satisfying $\mathsf{PP1SbE}(s, k)$. For all pair of matrices of constraint systems $(\mathcal{M}_1, \mathcal{M}'_1)$ obtained at the end of Step c of the first phase with support s and column k on $(\mathcal{M}, \mathcal{M}')$, we have that $(\mathcal{M}_1, \mathcal{M}'_1)$ satisfies $\mathsf{PP1ScE}(s, k)$.*

Proof. Let $(\mathcal{M}_0, \mathcal{M}'_0)$ be the pair of matrices of constraint systems, ancestor of $(\mathcal{M}, \mathcal{M}')$, obtained at the end of step b. Thanks to Lemma 20, we know that $(\mathcal{M}_0, \mathcal{M}'_0)$ satisfies $\mathsf{InvMatrix}(s-1)$. Furthermore, we know that for all constraint systems $\mathcal{C}$ in the k^{th} column of $(\mathcal{M}_0, \mathcal{M}'_0)$, $\mathcal{C}$ satisfies $\mathsf{InvGeneral}$, $\mathsf{InvVarFrame}(s-1)$, $\mathsf{InvNoUse}(s)$, $\mathsf{InvDest}(s)$ and $\mathsf{InvUntouched}(s)$. Hence thanks to Lemmas 10, 11, 12 and 14, we deduce, by a simple induction on the size of the branch between $(\mathcal{M}_0, \mathcal{M}'_0)$ and $(\mathcal{M}, \mathcal{M}')$, that $(\mathcal{M}, \mathcal{M}')$ satisfes $\mathsf{InvMatrix}(s-1)$ and for all constraint systems $\mathcal{C}$ in the k^{th} column of $(\mathcal{M}, \mathcal{M}')$, $\mathcal{C}$ satisfies $\mathsf{InvGeneral}$, $\mathsf{InvVarFrame}(s-1)$, $\mathsf{InvNoUse}(s)$, $\mathsf{InvDest}(s)$ and $\mathsf{InvUntouched}(s)$.

It remains to prove that for all $i \in \{1,\ldots,n\}$, for all $(X, j \vdash^? u) \in D(M_{i,k})$, if $X \notin S_2(\mathcal{C})$ then $u \notin \mathcal{X}^1$. Let us denote $\mathcal{C} = M_{i,k}$. Let $(X, j \vdash^? u) \in D(\mathcal{C})$ such that $X \notin S_2(\mathcal{C})$ and $u \in \mathcal{X}^1$. Thus we have that $\mathsf{X}^1(\mathcal{C}) \neq \emptyset$. Thanks to $\mathcal{C}$ being well-formed (Definition 18, item 10) and Lemma 21, we know that there exists $(Y, \ell \vdash^? v) \in D(\mathcal{C})$ such that $Y \in S_2(\mathcal{C})$, $\ell < j$ and $u \in vars^1(v)$.

Assume first that $v \in \mathcal{X}^1$ and so $u = v$. Thanks to Lemma 20 and the fact that the rules applied in step c do not add second order inequation in E_Π with a variable not in S_2, we deduce that for all $\mathsf{f} \in \mathcal{F}_c$, $E_\Pi(\mathcal{C}) \not\vDash \mathsf{root}(X) \neq^? \mathsf{f}$. But if there exists $\mathsf{f} \in \mathcal{F}_c$ such that $E_\Pi(\mathcal{C}) \vDash \mathsf{root}(Y) \neq^? \mathsf{f}$, then it would implies that either a rule Axiom or Cons would be applicable on $(Y, \ell \vdash^? v)$; or else $\mathcal{C} = \bot$ by normalisation. Hence, we have that for all $\mathsf{f} \in \mathcal{F}_c$, $E_\Pi(\mathcal{C}) \not\vDash \mathsf{root}(Y) \neq^? \mathsf{f}$. Therefore we have that Eq-ded-ded(X, Y) is applicable which contradicts the fact that $(\mathcal{M}, \mathcal{M}')$ was obtained at the end of step c.

Similarly, if $v \notin \mathcal{X}^1$, it implies that either $\mathcal{C} = \bot$ by normalisation or that a rule Axiom or Cons would be applicable on $(Y, \ell \vdash^? v)$, which contradicts our hypothesis.

Thus we deduce that for all $i \in \{1,\ldots,n\}$, for all $(X, j \vdash^? u) \in D(M_{i,k})$, if $X \notin S_2$ then $u \notin \mathcal{X}^1$. □

Appendix C.4.4. Invariants at Steps b/c (end of a cycle)

In the previous two subsections, we have shown some properties satisfied by the pairs of matrices at the end of Step b (resp. Step c). However, at the end of a cycle Steps b/c, we can prove additional properties.

Invariant 15 (PP1SbcE(s,k))**.** *A pair of matrices $(\mathcal{M}, \mathcal{M}')$ satisfies* PP1SbcE(s,k) *if $\mathcal{M}$ and $\mathcal{M}'$ have the same structure, satisfy* InvMatrix$(s-1)$ *and* InvGeneral*, and for all constraint systems $\mathcal{C}$ in $\mathcal{M}$ or $\mathcal{M}'$, if $\mathcal{C} \neq \bot$ then $\mathcal{C}$ satisfies the invariants* InvVarFrame$(s-1)$*,* InvDest(s)*,* InvNoUse(s) *and* InvUntouched(s)*. Moreover, for all constraint systems $\mathcal{C}$ in the k^{th} column of $(\mathcal{M}_1, \mathcal{M}'_1)$, for all $(X, i \vdash^? u) \in D(\mathcal{C})$, we have that:*

- $X \in S_2(\mathcal{C})$
- *for all $\mathsf{f} \in \mathcal{F}_c$, for all $\xi \in \Pi_r$, $E_\Pi \not\vDash \mathsf{root}(X) \neq^? \mathsf{f}$ and $E_\Pi \not\vDash X \neq^? \xi$*
- *if $s = \mathsf{s}_{max}$ then $\mathcal{C}$ satisfies* InvDedsub*.*

At last, for all $i \leq k$, for all constraint systems $\mathcal{C}$ in the i^{th} column of $(\mathcal{M}_1, \mathcal{M}_1)$, $\mathcal{C}$ also satisfies InvVarConstraint(s) *and* InvVarFrame(s) *(and* InvDedsub *when $\mathsf{s}_{max} = s$).*

Lemma 23. *Let $(\mathcal{M}, \mathcal{M}')$ be a pair of matricessatisfying* PP1Sb(s,k)*. For all pair of matrices of constraint systems $(\mathcal{M}_1, \mathcal{M}'_1)$ obtained at the end of a cycle Steps b/c with support s and column k on $(\mathcal{M}, \mathcal{M}')$, we have that $(\mathcal{M}_1, \mathcal{M}'_1)$ satisfies* PP1SbcE(s,k)*.*

Proof. $(\mathcal{M}, \mathcal{M}')$ being obtained at the end of a cycle Steps b/c, we know that $(\mathcal{M}, \mathcal{M}')$ is also obtained at the end of step c. Hence thanks to Lemma 22, we know that $(\mathcal{M}, \mathcal{M}')$ satisfies InvMatrix$(s-1)$ and for all constraint system $\mathcal{C}$ in the k^{th} of $(\mathcal{M}, \mathcal{M}')$, we have that $\mathcal{C}$ satisfies the invariants InvGeneral, InvVarFrame$(s-1)$, InvNoUse(s), InvDest(s) and InvUntouched(s). Hence it remains to prove that for all $(X, i \vdash^? u) \in D(\mathcal{C})$, $X \in S_2(\mathcal{C})$.

Assume that there exists $(X, i \vdash^? u) \in D(\mathcal{C})$ such that $X \notin S_2(\mathcal{C})$. Thus, thanks to Lemma 22, we have that $u \notin \mathcal{X}^1$. But thanks to Lemma 20, we know that if no rule of step b is applicable than it would imply that $u \in \mathcal{X}^1$ which is a contradiction. Hence a rule of step b is applicable on $(\mathcal{M}, \mathcal{M}')$ which contradicts the fact that $(\mathcal{M}, \mathcal{M}')$ is obtained at the end of a cycle of Steps b/c. Hence we have that $X \in S_2(\mathcal{C})$. □

Appendix C.4.5. Invariants at Step d

Lemma 24. *Let $(\mathcal{M}, \mathcal{M}')$ be a pair of matrices satisfying* $\mathsf{PP1SbcE}(s,k)$*. For all pair of matrices $(\mathcal{M}_1, \mathcal{M}'_1)$ obtained at the end of the Step d of the first phase with support s and column k on $(\mathcal{M}, \mathcal{M}')$, we have that $(\mathcal{M}_1, \mathcal{M}'_1)$ satisfies* $\mathsf{PP1Sb}(s, k+1)$*.*

Proof. Let $(\mathcal{M}_1, \mathcal{M}'_1)$ be the pair of matrices, ancestor of $(\mathcal{M}, \mathcal{M}')$, obtained at the end of the cycle b/c. Thanks to Lemma 22, we already know that $(\mathcal{M}_1, \mathcal{M}'_1)$ satisfies $\mathsf{InvMatrix}(s-1)$ and $\mathsf{InvGeneral}$. Furthermore, for all constraint systems $\mathcal{C}$ in the k^{th} column on $(\mathcal{M}_1, \mathcal{M}'_1)$, we have that $\mathcal{C}$ satisfies the invariants $\mathsf{InvVarFrame}(s-1)$, $\mathsf{InvNoUse}(s)$, $\mathsf{InvDest}(s)$ and $\mathsf{InvUntouched}(s)$. But thanks to Lemmas 14, 12, 11, 10 and 9, we have that $(\mathcal{M}, \mathcal{M}')$ satisfies $\mathsf{InvMatrix}(s-1)$ and $\mathsf{InvGeneral}$. Furthermore, for all constraint systems $\mathcal{C}$ in the k^{th} column on $(\mathcal{M}, \mathcal{M}')$, we have that $\mathcal{C}$ satisfies the invariants $\mathsf{InvVarFrame}(s-1)$, $\mathsf{InvNoUse}(s)$, $\mathsf{InvDest}(s)$ and $\mathsf{InvUntouched}(s)$.

Using a similar proof as in Lemma 20, we also show that $\mathcal{C}$ satisfies $\mathsf{InvVarConstraint}(s)$ and for all $(X, i \rhd x) \in D(\mathcal{C})$, for all $(\xi, j \rhd u) \in \Phi(\mathcal{C})$, for all $\mathsf{f} \in \mathcal{F}_c$, $E_\Pi \not\Vdash \mathsf{root}(X) \neq^? \mathsf{f}$ and $E_\Pi \not\Vdash X \neq^? \xi$.

Hence it remains to prove that $\mathcal{C}$ satisfies the invariant $\mathsf{InvVarFrame}(s)$. Let $(\xi, s \rhd v) \in \Phi(\mathcal{C})$ and $Z \in vars^2(\xi)$. Thanks to $\mathcal{C}$ being well-formed, we know that there exists $j \leq s$ and a term u such that $(Z, j \vdash^? u) \in D(\mathcal{C})$. Furthermore, for all $x \in vars^1(u)$, there exists $(\zeta, k \rhd w) \in \Phi$ such that $k \leq s$ and $x \in vars^1(w)$. But since $\mathcal{C}$ satisfies $\mathsf{InvVarConstraint}(s)$, we know that $u \in \mathcal{X}^1$ and so $x = u$. But by the property of origination of a constraint system, we deduce that there exists $(X, q \vdash^? t) \in D$ with $q < k \leq s$ and $u \in vars^1(t)$. Once again since $\mathcal{C}$ satisfies $\mathsf{InvVarConstraint}(s)$, we deduce that $t = u$. Moreover, the invariant $\mathsf{InvVarConstraint}(s)$ stipulates that all right hand term of the deducible constraints with index inferior to s are distinct. Hence, we deduce that $(X, q \vdash^? t)$ and $(Z, j \vdash^? u)$ are the same constraint and so $q = j$. But we proved that $q < k$ and $k \leq s$ which means that $j < s$ and so the result holds. □

Appendix C.4.6. Invariant at Step e

Lemma 25. *Let $(\mathcal{M}, \mathcal{M}')$ be a pair of matrices obtained by following the strategy. Assume that $\mathcal{M}$ and $\mathcal{M}'$ satisfy the invariant* $\mathsf{InvGeneral}$*. Let $\mathcal{C}$ and $\mathcal{C}'$ be two constraint systems occurring in the same column of $\mathcal{M}$. Assume that $\mathcal{C}$ and $\mathcal{C}'$ satisfy the invariants* $\mathsf{InvVarConstraint}(s)$ *and* $\mathsf{InvUntouched}(s)$ *for some s. We have that there exists a variable renaming $\rho : \mathcal{X}^1 \setminus S_1(\mathcal{C}) \to \mathcal{X}^1 \setminus S_1(\mathcal{C}')$ such that:*

1. $\mathsf{mgu}(E(\mathcal{C}))_{|S_1(\mathcal{C})}\rho = \mathsf{mgu}(E(\mathcal{C}'))_{|S_1(\mathcal{C}')}$*, and* $D(\mathcal{C})\rho = D(\mathcal{C}')$*;*
2. $\{(u\rho, u') \mid (\xi, i \rhd u) \in \Phi \wedge (\xi', i' \rhd u') \in \Phi' \wedge \mathsf{path}(\xi) = \mathsf{path}(\xi')\} \subseteq \{(u,u) \mid u \in \mathcal{T}(\mathcal{F}_c, \mathcal{N} \cup \mathcal{X}^1)\}$.

Proof. First, we define the renaming ρ, and then we show that the two properties are satisfied.

Definition of the renaming ρ. By Lemma 1, we know that the matrices $\mathcal{M}$ and $\mathcal{M}'$ have the same structure, and so the systems $\mathcal{C}$ and $\mathcal{C}'$ have the same shape. Hence, we have:

- $S_2(\mathcal{C}) = S_2(\mathcal{C}')$, and
- $\{(X,i) \mid X, i \vdash^? u \in D(\mathcal{C}) \text{ and } X \in S_2(\mathcal{C})\} = \{(X,i) \mid X, i \vdash^? u \in D(\mathcal{C}') \text{ and } X \in S_2(\mathcal{C}')\}$.

Since the system $\mathcal{C}$ satisfies the invariants $\mathsf{InvVarConstraint}(s)$ and $\mathsf{InvUntouched}(s)$, we have that $X \in S_2(\mathcal{C})$ for each $(X, i \vdash^? u) \in D(\mathcal{C})$, and similarly, we have that $X \in S_2(\mathcal{C}')$ for each $(X, i \vdash^? u) \in D(\mathcal{C}')$. This allows us to conclude that $\{(X,i) \mid X, i \vdash^? u \in D(\mathcal{C})\} = \{(X,i) \mid X, i \vdash^? u \in D(\mathcal{C}')\}$.
Actually, the invariant $\mathsf{InvVarConstraint}(s)$ also tells us that:

- for all $(X, i \vdash^? u) \in D(\mathcal{C})$ such that $i \leq s$, we have that u is a variable (distinct of the ones introduced by the other constraints); and
- for all $(X, i \vdash^? u) \in D(\mathcal{C}')$ such that $i \leq s$, we have that u is a variable (distinct of the ones introduced by the other constraints).

Hence, this allows us to define a renaming ρ such that $\mathrm{dom}(\rho) = \{x \mid (X, i \vdash^? x) \in D(\mathcal{C}) \wedge i \leq s\}$, and $\rho(x) = X\delta^1(\mathcal{C}')$ where $(X, i \vdash^? x) \in D(\mathcal{C})$.

Property 1. With such renaming, we trivially have that $D(\mathcal{C})\rho = D(\mathcal{C}')$ but only for the deducibility constraints $(X, i \rhd u)$ with $i \leq s$. Hence, we still have to prove this result for $i > s$. Since the systems $\mathcal{C}$ and $\mathcal{C}'$ occur on the same column of the matrix $\mathcal{M}$, there exists an initial constraint system $\mathcal{C}_0$ that is an ancestor of $\mathcal{C}$ and $\mathcal{C}'$. Moreover, we know that $\mathcal{C}$ and $\mathcal{C}'$ satisfy the invariant $\mathsf{InvUntouched}(s)$. Hence, we deduce that:

- for all $(X, i \vdash^? u) \in D(\mathcal{C})$ such that $i > s$, we have that $X \in vars^2(D(\mathcal{C}_0))$; and
- for all $(X, i \vdash^? u') \in D(\mathcal{C}')$ such that $i > s$, we have that $X \in vars^2(D(\mathcal{C}_0))$.

Let $\sigma = \mathsf{mgu}(E(\mathcal{C}))$ and $\sigma' = \mathsf{mgu}(E(\mathcal{C}'))$. Since $\mathcal{C}$ and $\mathcal{C}'$ are normalised, for $i > s$, we deduce that $(X, i \vdash^? u) \in D(\mathcal{C})$, $(X, i \vdash^? u') \in D(\mathcal{C}')$, and $(X, i \vdash^? u_0) \in D(\mathcal{C}_0)$ imply that $u = u_0\sigma$ and $u' = u_0\sigma'$. Let $S_1 \stackrel{\mathsf{def}}{=} S_1(\mathcal{C}) = S_1(\mathcal{C}') = S_1(\mathcal{C}_0)$. Hence, to conclude the proof of $D(\mathcal{C})\rho = D(\mathcal{C}')$, it remains to show that $\sigma_{|S_1}\rho = \sigma'_{|S_1}$.

By definition of an initial constraint system, we know that for all $x \in S_1$, there exists $(X, k \vdash^? u) \in D(\mathcal{C}_0)$ such that $x \in vars^1(u)$ and $X \in S_2(\mathcal{C}_0)$. Since $\mathcal{C}$ and $\mathcal{C}'$ satisfy the invariant $\mathsf{InvUntouched}(s)$, we have that no rule was applied with support strictly superior to s, and we deduce that for all $(Y, j \vdash^? v) \in D(\mathcal{C}_0)$, for all $y \in vars^1(v)$, $\mathcal{L}^1_{\mathcal{C}_0}(y) > s$ implies that $y \notin \mathrm{dom}(\sigma)$ and $y \notin \mathrm{dom}(\sigma')$. Hence, we only focus on variable $x \in S_1$ such that there exists $(X, k \vdash^? u) \in D(\mathcal{C}_0$, $x \in vars^1(u)$ and $k \leq s$. We prove by induction on $k \leq s$ that $X\delta^1(\mathcal{C}_0)\sigma\rho = X\delta^1(\mathcal{C}_0)\sigma'$.

Base case $k = 0$. There is no constraint $X, k \vdash^? u$ with $k = 0$. Hence, the result trivially holds.

Inductive step $k > 0$. Let $(X, k \vdash^? u) \in D(\mathcal{C}_0)$. By Lemma 6, we know that:

$$\begin{cases} u\sigma = \mathsf{C}\lfloor X \rfloor_{\Phi_0}\delta^1(\mathcal{C}_0)\sigma = \mathsf{C}\lfloor X\Theta \rfloor_{\Phi}\delta^1(\mathcal{C}) \text{ and } \mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(X\Theta) \leq k \\ u\sigma' = \mathsf{C}\lfloor X \rfloor_{\Phi_0}\delta^1(\mathcal{C}_0)\sigma' = \mathsf{C}\lfloor X\Theta' \rfloor_{\Phi'}\delta^1(\mathcal{C}') \text{ and } \mathsf{param}^{\mathcal{C}'}_{\mathsf{max}}(X\Theta') \leq k \end{cases}$$

where $\Theta = \mathsf{mgu}(E_\Pi(\mathcal{C}))$ and $\Theta' = \mathsf{mgu}(E_\Pi(\mathcal{C}'))$.

However, $X \in S_2(\mathcal{C}_0)$ implies that $X \in S_2(\mathcal{C}) = S_2(\mathcal{C}')$ and so thanks to $\mathcal{M}$ satisfying the invariant $\mathsf{InvGeneral}$ (item 5), we deduce that $\mathsf{C}\lfloor X\Theta \rfloor_{\Phi} = \mathsf{C}\lfloor X\Theta' \rfloor_{\Phi'}$. Furthermore, for all $i \leq k$, for all $w \cdot ax_i \in st(\mathsf{C}\lfloor X\Theta \rfloor_{\Phi})$, we know that there exists u_0 such that $(ax_i, i \rhd u_0) \in \Phi(\mathcal{C}_0)$. Thus by Lemma 7, $(ax_i, i \rhd u_0\sigma) \in \Phi$ and $(ax_i, i \rhd u_0\sigma') \in \Phi'$. But by definition of a constraint system, for all $y \in vars^1(u_0)$, there exists $(Y, \ell \vdash^? v) \in$

$D(\mathcal{C}_0)$ such that $\ell < k$ and $y \in vars^1(v)$. By our inductive hypothesis, we know that $v\sigma\rho = v\sigma'$ which implies that $y\sigma\rho = y\sigma'$ and so we can deduce that $u_0\sigma\rho = u_0\sigma'$.

But thanks to the definition of a context, for all w, $w \cdot ax_i \in st(\mathsf{C}\lfloor X\Theta\rfloor_\Phi) = st(\mathsf{C}\lfloor X\Theta\rfloor_{\Phi'})$ implies that there exists $(\xi, j \rhd v) \in \Phi$ and $(\xi', j' \rhd v') \in \Phi'$ such that $\mathsf{path}(\xi) = \mathsf{path}(\xi') = w \cdot ax_i$. Since $ax_i\delta^1(\mathcal{C})\rho = u_0\sigma\rho = u_0\sigma' = ax_i\delta^1(\mathcal{C}')$, then thanks to Lemma 8, we can deduce that $v\rho = v'$ and so $(w \cdot ax_i)\delta^1(\mathcal{C})\rho = (w \cdot ax_i)\delta^1(\mathcal{C}')$.

At last, since $\mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(X\Theta) \leq k$ and $\mathsf{param}^{\mathcal{C}'}_{\mathsf{max}}(X\Theta') \leq k$, then for all $(w \cdot ax_i) \in st(\mathsf{C}\lfloor X\Theta\rfloor_\Phi)$, we have $i \leq k$. The same holds for $(w \cdot ax_i) \in st(\mathsf{C}\lfloor X\Theta'\rfloor_{\Phi'})$. Hence, since we proved that for all w, for all $i \leq k$, $(w \cdot ax_i)\delta^1(\mathcal{C})\rho = (w \cdot ax_i)\delta^1(\mathcal{C}')$, since $\mathsf{C}\lfloor X\Theta\rfloor_\Phi = \mathsf{C}\lfloor X\Theta'\rfloor_{\Phi'}$, and since for all $(X, i \vdash^? x) \in D(\mathcal{C})$, for all $(X, i \vdash^? x') \in D(\mathcal{C}')$, $i \leq s$ implies $x\rho = x'$, then we can deduce that $\mathsf{C}\lfloor X\Theta\rfloor_\Phi\delta^1(\mathcal{C})\rho = \mathsf{C}\lfloor X\Theta'\rfloor_\Phi\delta^1(\mathcal{C}')$. Thus we conclude that $X\delta^1(\mathcal{C}_0)\sigma\rho = u\sigma\rho = u\sigma' = X\delta^1(\mathcal{C}_0)\sigma'$.

Property 2. Let $(\xi, i \rhd u) \in \Phi$ and $(\xi', i' \rhd u') \in \Phi'$ such that $\mathsf{path}(\xi) = \mathsf{path}(\xi') = w{\cdot}ax_k$. Since the constraint systems $\mathcal{C}$ and $\mathcal{C}'$ are well-formed, there exist $(ax_k, k \rhd v) \in \Phi$ and $(ax_k, k \rhd v') \in \Phi'$. Thanks to Lemma 7, we know that there exits v_0 such that $(ax_k, k \rhd v_0) \in \Phi_0$ with $v_0\sigma = v$ and $v_0\sigma' = v'$. Since $\sigma_{|S_1}\rho = \sigma'_{|S_1}$, we deduce that $v_0\sigma\rho = v_0\sigma'$ and so $v\rho = v'$. □

Lemma 26. *Let $(\mathcal{M}, \mathcal{M}')$ be a pair of matrices satisfying $\mathsf{PP1}(s)$. For all pair of matrices of constraint systems $(\mathcal{M}_1, \mathcal{M}'_1)$ obtained by applying all the steps of Phase 1 of the strategy with support s, we have that $(\mathcal{M}_1, \mathcal{M}'_1)$ satisfies $\mathsf{PP1}(s+1)$.*

Proof. The step e of the strategy consists of transforming some of the constraint systems into $\bot$. Moreover, Step e is applied only once step d was applied on all columns of $(\mathcal{M}, \mathcal{M}')$. Thus, thanks to Lemma 24, we can already deduce that $\mathcal{M}$ and $\mathcal{M}'$ satisfy $\mathsf{InvGeneral}$ and for all constraint systems $\mathcal{C}$ in $(\mathcal{M}, \mathcal{M}')$, $\mathcal{C}$ satisfies the invariants $\mathsf{InvVarConstraint}(s)$, $\mathsf{InvVarFrame}(s)$, $\mathsf{InvNoUse}(s)$, $\mathsf{InvDest}(s)$, $\mathsf{InvUntouched}(s)$, and for all $(X, i \rhd x) \in D(\mathcal{C})$, for all $(\xi, j \rhd u) \in \Phi(\mathcal{C})$, for all $\mathsf{f} \in \mathcal{F}_c$, $E_\Pi \not\Vdash \mathsf{root}(X) \neq^? \mathsf{f}$ and $E_\Pi \not\Vdash X \neq^? \xi$.

Similarly, we have that $(\mathcal{M}, \mathcal{M}')$ satisfies the invariant $\mathsf{InvGeneral}$ and $\mathsf{InvMatrix}(s-1)$. Thus it remains to prove that $(\mathcal{M}, \mathcal{M}')$ satisfies the invariant $\mathsf{InvMatrix}(s)$. But by the definition of the transformation in Step e, we can deduce that for all $\mathcal{C}$, for all $\mathcal{C}'$ in the same column of $(\mathcal{M}, \mathcal{M}')$, we have that:

$$\{\mathsf{path}(\xi), i \mid (\xi, i \rhd u) \in \Phi(\mathcal{C}) \wedge i \leq s\} = \{\mathsf{path}(\xi), i \mid (\xi, i \rhd u) \in \Phi(\mathcal{C}') \wedge i \leq s\}.$$

At last, let $(\mathcal{M}_1, \mathcal{M}'_1)$ be the matrices that are ancestors of $(\mathcal{M}, \mathcal{M}')$ obtained at the end of Step a of Phase 1 with support s. Let $\mathcal{C}$ be a constraint system in $(\mathcal{M}, \mathcal{M}')$ such that $(\xi, s \rhd u) \in \mathsf{NoUse}(\mathcal{C})$. Let $\mathcal{C}'$ be a constraint system in $(\mathcal{M}, \mathcal{M}')$ in the column on $\mathcal{C}$. We proved that there exists $(\xi', s \rhd u') \in \Phi(\mathcal{C}')$ such that $\mathsf{path}(\xi') = \mathsf{path}(\xi)$. Assume that $(\xi', s \rhd u') \notin \Phi(\mathcal{C}')$. Since the frame is not modify during step $b - c - d$, other than applying substitution, we can deduce that there exists $\mathcal{C}_1, \mathcal{C}'_1$ in $(\mathcal{M}_1, \mathcal{M}'_1)$, $\xi_1, \xi'_1 \in \Pi_r$, $u_1, u'_1 \in \mathcal{T}(\mathcal{F}_c, \mathcal{N} \cup \mathcal{X}^1)$ such that $\mathcal{C}_1 \rightarrow^* \mathcal{C}$, $\mathcal{C}'_1 \rightarrow^* \mathcal{C}'$, $(\xi_1, s \rhd u_1) \in \mathsf{NoUse}(\mathcal{C}_1)$, $(\xi'_1, s \rhd u'_1) \in \Phi(\mathcal{C}'_1) \setminus \mathsf{NoUse}(\mathcal{C}'_1)$ and $\mathsf{path}(\xi_1) = \mathsf{path}(\xi'_1)$

Thanks to Lemma 17, there exists $X \in S_2(\mathcal{C}_1)$ such that $\mathsf{C}\lfloor X\mathsf{mgu}(E_\Pi(\mathcal{C}_1))\rfloor_{\Phi(\mathcal{C}_1)}\delta^1(\mathcal{C}_1) = u_1$ and either (a) $(\xi'_1, s \rhd u'_1) \in \mathsf{NoUse}(\mathcal{C}'')$ and $\mathsf{C}\lfloor X\mathsf{mgu}(E_\Pi(\mathcal{C}'_1))\rfloor_{\Phi(\mathcal{C}'_1)}\delta^1(\mathcal{C}'_1) = u'_1$. Or else, (b) by denoting $v'_1 = \mathsf{C}\lfloor X\mathsf{mgu}(E_\Pi(\mathcal{C}'_1))\rfloor_{\Phi(\mathcal{C}'_1)}\delta^1(\mathcal{C}'_1)$, we have that $E(\mathcal{C}'_1) \vDash v'_1 \neq^? u'_1$. We show that case (b) can not happen.

Let's denote $\sigma = \mathsf{mgu}(E(\mathcal{C}))$, $\sigma' = \mathsf{mgu}(E(\mathcal{C}'))$, $\theta = \mathsf{mgu}(E_\Pi(\mathcal{C}))$ and $\theta' = \mathsf{mgu}(E_\Pi(\mathcal{C}'))$. Thanks to Lemma 6, we deduce that $v'_1\sigma' = \mathsf{C}\lfloor X\theta' \rfloor_{\Phi(\mathcal{C}')}\delta^1(\mathcal{C}')$ and $u_1\sigma = \mathsf{C}\lfloor X\theta' \rfloor_{\Phi(\mathcal{C})}\delta^1(\mathcal{C})$. However, since $X \in S_2(\mathcal{C}_1)$ and $(\mathcal{M}, \mathcal{M}')$ have the same structure, we deduce that $X \in S_2(\mathcal{C})$ and $X \in S_2(\mathcal{C}')$. But $(\mathcal{M}, \mathcal{M}')$ satisfies the invariant $\mathsf{InvGeneral}$, hence thanks to item 5 of invariant $\mathsf{InvGeneral}$, we have that $\mathsf{C}\lfloor X\theta' \rfloor_{\Phi(\mathcal{C}')} = \mathsf{C}\lfloor X\theta \rfloor_{\Phi(\mathcal{C})}$.

On the other hand, since $\mathcal{C}$ and $\mathcal{C}'$ satisfies $\mathsf{InvVarConstraint}(s)$ and $\mathsf{InvUntouched}(s)$, then by Lemma 25, we have that there exists a variable renaming $\rho : \mathcal{X}^1 \setminus S_1(\mathcal{C}) \to \mathcal{X}^1 \setminus S_1(\mathcal{C}')$ such that:

1. $\mathsf{mgu}(E(\mathcal{C}))_{|S_1(\mathcal{C})}\rho = \mathsf{mgu}(E(\mathcal{C}'))_{|S_1(\mathcal{C}')}$, and $D(\mathcal{C})\rho = D(\mathcal{C}')$;
2. $\{(u\rho, u') \mid (\xi, i \rhd u) \in \Phi \wedge (\xi', i' \rhd u') \in \Phi' \wedge \mathsf{path}(\xi) = \mathsf{path}(\xi')\}$ is include in $\{(u, u) \mid u \in \mathcal{T}(\mathcal{F}_c, \mathcal{N} \cup \mathcal{X}^1)\}$;

Thus we have that $\delta^1(\mathcal{C})\rho = \delta^1(\mathcal{C}')$ and so $v'_1\sigma' = \mathsf{C}\lfloor X\theta' \rfloor_{\Phi(\mathcal{C}')}\delta^1(\mathcal{C}') = \mathsf{C}\lfloor X\theta \rfloor_{\Phi(\mathcal{C})}\delta^1(\mathcal{C})\rho = u_1\sigma\rho = u\rho = u' = u'_1\sigma'$. Hence, we have that $v'_1\sigma' = u'_1\sigma'$. However, we assume that $E(\mathcal{C}'_1) \vDash v'_1 \neq^? u'_1$ which implies that $E(\mathcal{C}') \vDash v'_1\sigma' \neq^? u'_1\sigma'$. But $v'_1\sigma' = u'_1\sigma'$ and by the normalisation, we would have that $\mathcal{C}' = \bot$ which is a contradiction with our hypothesis. Hence, we proved that only case (a) can happen which implies that $(\xi, s \rhd u) \in \mathsf{NoUse}(\mathcal{C})$ implies $(\xi', s \rhd u') \in \mathsf{NoUse}(\mathcal{C}')$. It allows us to conclude that $\{\mathsf{path}(\xi), i \mid (\xi, i \rhd u) \in \mathsf{NoUse}(\mathcal{C}) \wedge i \leq s\} = \{\mathsf{path}(\xi), i \mid (\xi, i \rhd u) \in \mathsf{NoUse}(\mathcal{C}') \wedge i \leq s\}$. □

Appendix C.4.7. Invariant at the end of Phase 1

In this subsection, we describe the properties satisfied at the end of Phase 1.

Invariant 16 (PP1E)**.** *A pair of matrices $(\mathcal{M}, \mathcal{M}')$ satisfies* PP1E *if $(\mathcal{M}, \mathcal{M}')$ satisfies* $\mathsf{PP1}(\mathsf{s}_{max})$ *and for all constraint system $\mathcal{C}$ in $\mathcal{M}$ or $\mathcal{M}'$, $\mathcal{C}$ also satisfies* InvDedsub*.*

Lemma 27. *Let $(\mathcal{M}, \mathcal{M}')$ be a pair of row matrices of initial constraint systems having the same structure. For all $(\mathcal{M}'_1, \mathcal{M}'_1)$ obtained at the end of Phase 1 from $(\mathcal{M}, \mathcal{M}')$, we have that $(\mathcal{M}, \mathcal{M}')$ satisfies* PP1E*. Moreover, for all $(\mathcal{M}_2, \mathcal{M}'_2)$ such that $(\mathcal{M}, \mathcal{M}') \to^* (\mathcal{M}_2, \mathcal{M}'_2) \to^* (\mathcal{M}'_1, \mathcal{M}'_1)$,*

- *if $(\mathcal{M}_2, \mathcal{M}'_2)$ is obtained from Step a with support s then $(\mathcal{M}_2, \mathcal{M}'_2)$ satisfies* $\mathsf{PP1Sa}(s)$*;*
- *if $(\mathcal{M}_2, \mathcal{M}'_2)$ is obtained at the end of Step a with support s then $(\mathcal{M}_2, \mathcal{M}'_2)$ satisfies* $\mathsf{PP1SaE}(s)$*;*
- *if $(\mathcal{M}_2, \mathcal{M}'_2)$ is obtained at the end Step b with support s and column k then $(\mathcal{M}_2, \mathcal{M}'_2)$ satisfies* $\mathsf{PP1SbE}(s, k)$*;*
- *if $(\mathcal{M}_2, \mathcal{M}'_2)$ is obtained at the end Step c with support s and column k then $(\mathcal{M}_2, \mathcal{M}'_2)$ satisfies* $\mathsf{PP1ScE}(s, k)$*;*
- *if $(\mathcal{M}_2, \mathcal{M}'_2)$ is obtained at the end of the cycle of steps $b + c$ with support s and column k then $(\mathcal{M}_2, \mathcal{M}'_2)$ satisfies* $\mathsf{PP1SbcE}(s, k)$*;*
- *if $(\mathcal{M}_2, \mathcal{M}'_2)$ is obtained at the end of Step d with support s and column k then $(\mathcal{M}_2, \mathcal{M}'_2)$ satisfies* $\mathsf{PP1Sb}(s, k+1)$ *and* $\mathsf{PP1SbE}(s, j)$ *for all $j \leq k$.*

Proof. This proof relies on all the previous lemmas and can be established by induction on the parameters s and k. □

Lemma 28. *Let $(\mathcal{M}, \mathcal{M}')$ be a pair of row matrices of initial constraint systems having the same structure. Let $(\mathcal{M}_1, \mathcal{M}'_1)$ be a pair of matrices of constraint systems obtained by following the strategy on $(\mathcal{M}, \mathcal{M}')$. We have that $(\mathcal{M}_1, \mathcal{M}'_1)$ satisfies* InvGeneral.

Proof. We rely on Lemma 27 to prove that if $(\mathcal{M}_1, \mathcal{M}'_1)$ is obtained from Step a with support s, $s \in \mathbb{N}$, then $(\mathcal{M}_1, \mathcal{M}'_1)$ satisfies $\mathsf{PP1Sa}(s)$ and so InvGeneral. For any other step and phase, we rely on Lemma 14 to conclude. □

Appendix C.5. Preservation of the invariants for Phase 2 (step by step)

This phase is made of 2 steps that we consider separately.

Appendix C.5.1. Invariant at Step a

Lemma 29. *Let $(\mathcal{M}, \mathcal{M}')$ be a pair of matrices obtained at the end of Step a. For all constraint systems $\mathcal{C}$ in $(\mathcal{M}, \mathcal{M}')$, we have that $vars^1(E(\mathcal{C}))$ does not contain variable that are universally quantified.*

Proof. Thanks to the normalisation, we know that for all constraint systems $\mathcal{C}$ in $\mathcal{M}$, the disjunctions of inequations in $E(\mathcal{C})$ are of the form $\forall \tilde{y}. \bigvee_i x_i \neq^? u_i$ where $\tilde{y}$ is a set of universal variable and x_i are not universal for any i. Furthermore, thanks to the normalisation, $x_i \notin \tilde{y}$, for all i and for all $y \in \tilde{y}$, there exists i such that $y \in vars^1(u_i)$. Let $x_i \neq^? u_i$ and $y \in vars^1(u_i) \cap \tilde{y}$. Since x_i is not a universal variable, there exists $(X, j \vdash^? x_i) \in D(\mathcal{C})$. But we assumed that the rules Cons and Axiom are no longer applicable. Thus, we deduce that for all $\mathsf{f} \in \mathcal{F}_c$, $E_\Pi(\mathcal{C}) \vDash \mathsf{root}(X) \neq^? \mathsf{f}$ and for all $(\xi, k \vdash^? u) \in \Phi(\mathcal{C})$, $E_\Pi(\mathcal{C}) \vDash X \neq^? \xi$. Moreover, we know that $\mathcal{C}$ satisfies the invariant $\mathsf{InvDest}(\infty)$ hence by the definition of the normalisation, we should have $\mathcal{C} = \bot$ which is a contradiction with our hypothesis on $\mathcal{C}$. Hence $vars^1(u_i) \cap \tilde{y} = \emptyset$ for all $x_i \neq^? u_i$. Hence by normalisation, we deduce that $E(\mathcal{C})$ do not contain universal variable. □

Appendix C.5.2. Invariant at Step b

Remember that the measure $\mathcal{L}^1_{\mathcal{C}}(u)$ is defined as follows:

$$\mathcal{L}^1_{\mathcal{C}}(u) = max\left(\{i \mid (X, i \vdash^? x) \in D(\mathcal{C}) \wedge x \in vars(u)\} \cup \{0\}\right).$$

Lemma 30. *Let $(\mathcal{M}, \mathcal{M}')$ be a pair of matrices obtained at the end of Step b. For any constraint system $\mathcal{C}$ in $\mathcal{M}$ (resp. $\mathcal{M}'$), for any disjunction $\bigvee_{i=1}^n u_i \neq^? v_i$ occurring in $E(\mathcal{C})$, i.e. such that $E(\mathcal{C}) = E \wedge \bigvee_{i=1}^n u_i \neq^? v_i$ for some E, we have that either $n = 1$, $u_1 \in \mathcal{X}^1$, v_1 does not contain any name and $\mathcal{L}^1_{\mathcal{C}}(v_1) \leq \mathcal{L}^1_{\mathcal{C}}(u_1)$; or for all $i \in \{1, \ldots, n\}$, we have that $u_i \neq^? v_i$ satisfies one of the following properties:*

1. *$u_i \in \mathcal{X}^1$ and $v_i \in \mathcal{N}$.*
2. *$u_i, v_i \in \mathcal{X}^1$, and $E_\Pi(\mathcal{C}) \nvDash \mathsf{root}(X) \neq^? \mathsf{f}$, $E_\Pi(\mathcal{C}) \vDash \mathsf{root}(Y) \neq^? \mathsf{g}$, for all $\mathsf{f}, \mathsf{g} \in \mathcal{F}_c$, where $(X, p \vdash^? u_i), (Y, q \vdash^? v_i) \in D(\mathcal{C})$.*
3. *$u_i \in \mathcal{X}^1$, $\mathsf{root}(v_i) \in \mathcal{F}_c$ and for all $\mathsf{f} \in \mathcal{F}_c$, $E_\Pi(\mathcal{C}) \vDash \mathsf{root}(X) \neq^? \mathsf{f}$, where $(X, p \vdash^? u_i) \in D(\mathcal{C})$.*

Proof. By definition of Step b of Phase 2 of the strategy, for any constraint system $\mathcal{C}$, we know that $\textsc{Cons}(X, \mathsf{f})$ and $\textsc{Eq-ded-ded}(X, \xi)$ are not applicable (for any $\mathsf{f} \in \mathcal{F}_c$ and any ξ). Consider a disjunction $\bigvee_i^n u_i \neq^? v_i$ such that $E(\mathcal{C}) = E \wedge \bigvee_i^n u_i \neq^? v_i$, and $i \in \{1, \ldots, n\}$. We do a case analysis on u_i and v_i.

- Case $u_i \notin \mathcal{X}^1$ and $v_i \notin \mathcal{X}^1$. In such a case, since $\mathcal{C}$ is normalized, we know that this equality is necessarily reduced, and therefore this case is impossible.
- Case $u_i \in \mathcal{X}^1$ and $v_i \in \mathcal{N}$ (or the reverse). In such a case, the results holds trivially.
- Case $u_i, v_i \in \mathcal{X}^1$. In such a case, we know that there exist $(X, k \vdash^? u_i) \in D(\mathcal{C})$ and $(Y, \ell \vdash^? v_i) \in D(\mathcal{C})$. We assume w.l.o.g. that $\ell \leq k$. Since Eq-ded-ded is not applicable for Step b, we deduce that the conditions of application of the rule $\textsc{Eq-ded-ded}(X, Y)$ in Figure 2 are not satisfied or that Eq-ded-ded is useless on $\mathcal{C}$. In the latter case, we deduce that $n = 1$ and so the result directly holds. In the former case, we deduce that there exists $\mathsf{f} \in \mathcal{F}_c$ such that $E_\Pi(\mathcal{C}) \vDash \mathsf{root}(X) \neq^? \mathsf{f}$ and $E_\Pi(\mathcal{C}) \nvDash \mathsf{root}(Y) \neq^? \mathsf{f}$ (or the reverse). Assume w.l.o.g. that $E_\Pi(\mathcal{C}) \vDash \mathsf{root}(X) \neq^? \mathsf{f}$ and $E_\Pi(\mathcal{C}) \nvDash \mathsf{root}(Y) \neq^? \mathsf{f}$.

  Since $\textsc{Cons}(X, \mathsf{g})$ is not applicable for Step b, we have that $E_\Pi(\mathcal{C}) \vDash \mathsf{root}(X) \neq^? \mathsf{f}$ for some $\mathsf{f} \in \mathcal{F}_c$ implies that $E_\Pi(\mathcal{C}) \vDash \mathsf{root}(X) \neq^? \mathsf{g}$ for all $\mathsf{g} \in \mathcal{F}_c$. Similarly, $E_\Pi(\mathcal{C}) \nvDash \mathsf{root}(Y) \neq^? \mathsf{f}$ for some $\mathsf{f} \in \mathcal{F}_c$ implies that $E_\Pi(\mathcal{C}) \nvDash \mathsf{root}(Y) \neq^? \mathsf{g}$ for all $\mathsf{g} \in \mathcal{F}_c$ (otherwise $\textsc{Cons}(Y, \mathsf{g})$ would be applicable). Hence we deduce that for all $\mathsf{f}, \mathsf{g} \in \mathcal{F}_c$, $E_\Pi(\mathcal{C}) \nvDash \mathsf{root}(X) \neq^? \mathsf{f}$ and $E_\Pi(\mathcal{C}) \vDash \mathsf{root}(Y) \neq^? \mathsf{g}$. Thus, the result holds.
- Case $u_i \in \mathcal{X}^1$ and $\mathsf{root}(v_i) = \mathsf{f} \in \mathcal{F}_c$ (or the reverse). In such a case, we know that there exists $(X, k \vdash^? u_i) \in D(\mathcal{C})$. Since $\textsc{Cons}(X, \mathsf{g})$ is not applicable for Step b, for all $\mathsf{g} \in \mathcal{F}_c$, we deduce that either $st(v_i) \cap \mathcal{N} = \emptyset$ and $\mathcal{L}^1_{\mathcal{C}}(v_i) \leq k$ or for all $\mathsf{g} \in \mathcal{F}_c$, $E_\Pi(\mathcal{C}) \vDash \mathsf{root}(X) \neq^? \mathsf{g}$. In the latter case, the result holds. In the former case, $st(v_i) \cap \mathcal{N} = \emptyset$ implies that there exists $\xi \in \mathcal{T}(\mathcal{F}_c, \mathcal{X}^2)$ such that $\xi\delta^1(\mathcal{C}) = v_i$. But $\textsc{Eq-ded-ded}(X, \xi)$ is not applicable for Step b. Thus either (a) the conditions of application of the rule $\textsc{Eq-ded-ded}(X, \xi)$ in Figure 2 are not satisfied or (b) $\textsc{Eq-ded-ded}(X, \xi)$ is useless on $\mathcal{C}$. In Case (b), we deduce that $n = 1$ and since we assume that $st(v_i) \cap \mathcal{N} = \emptyset$ and $\mathcal{L}^1_{\mathcal{C}}(v_i) \leq k$, the result holds. In Case (a), we deduce that $E_\Pi(\mathcal{C}) \vDash \mathsf{root}(X) \neq^? \mathsf{root}(\xi)$. Hence using what we proved thanks to Cons not being applicable, we deduce that for all $\mathsf{g} \in \mathcal{F}_c$, $E_\Pi(\mathcal{C}) \vDash \mathsf{root}(X) \neq^? \mathsf{g}$. Hence, the result holds.

□

Appendix D. Proof of soundness

This section is dedicated to the proof of soundness of the algorithm. However, unlike the proof of completeness, this proof depends heavily on the strategy that has been described in Section 4, and on the invariants described in Appendix C.

Appendix D.1. Preliminaries

For a recipe ξ and a frame Φ, we say that $\mathsf{root}(\xi)$ is *not reduced* if $\mathsf{f}(\xi_1,\ldots,\xi_n)\Phi{\downarrow} = \mathsf{f}(\xi_1\Phi{\downarrow},\ldots,\xi_n\Phi{\downarrow})$ and $\mathsf{root}(\xi) \in \mathcal{F}_d$ with $\xi = \mathsf{f}(\xi_1,\ldots,\xi_n)$ for some $\xi_1,\ldots,\xi_n$. We establish three properties on the recipes in Π_r:

Lemma 31. *Let Φ be a ground frame. Let ξ be a recipe such that $param(\xi) \subseteq \mathrm{dom}(\Phi)$, $\xi\Phi{\downarrow} \notin \mathcal{T}(\mathcal{F}_c,\mathcal{N})$. If for every $\xi' \in st(\xi)$,*

$$\xi' = \mathsf{f}(\mathsf{g}(\xi_1,\ldots,\xi_n),\ldots,\beta_m),\ \mathsf{f} \in \mathcal{F}_d \text{ and } \mathsf{g} \in \mathcal{F}_c \text{ implies } \mathsf{f} \text{ is not reduced,}$$

then, either $\mathsf{root}(\xi) \in \mathcal{F}_c$ or $\mathsf{root}(\xi)$ is not reduced.

Proof. We prove this result by induction on the size of ξ.

Base case: $|\xi| = 1$. In such a case, $\xi \in \mathrm{dom}(\Phi)$ and so $\xi\Phi{\downarrow} \in \mathcal{T}(\mathcal{F}_c,\mathcal{N})$ by hypothesis on the frame. Hence the result trivially holds.

Induction step: $|\xi| > 1$. If $\mathsf{root}(\xi) \in \mathcal{F}_c$ or $\mathsf{root}(\xi)$ is not reduced then the property trivially holds. Else we have that $\xi = \mathsf{f}(\xi_1,\ldots,\xi_m)$ with $\mathsf{f} \in \mathcal{F}_d$ and f is reduced. We show that this case is impossible.

f is reduced implies that there is a rewrite rule $\mathsf{f}(u_1,\ldots,u_n) \to u$ such that $\mathsf{f}(u_1,\ldots,u_n)$ and $\mathsf{f}(\xi_1\Phi{\downarrow},\ldots,\xi_n\Phi{\downarrow})$ are unifiable. Since $\xi\Phi{\downarrow} \notin \mathcal{T}(\mathcal{F}_c,\mathcal{N})$ and $\xi\Phi{\downarrow} \in st(\xi_1\Phi{\downarrow})$ (since $u \in st(u_1)$), we have that $\xi_1\Phi{\downarrow} \notin \mathcal{T}(\mathcal{F}_c,\mathcal{N})$. By applying our induction hypothesis on ξ_1, we deduce that either $\mathsf{root}(\xi_1) \in \mathcal{F}_c$ or $\mathsf{root}(\xi_1)$ is not reduced.

- If $\mathsf{root}(\xi_1) \in \mathcal{F}_c$ then by hypothesis on the subterms of ξ, we deduce that f is not reduced which is in contradiction with the hypothesis.
- If $\mathsf{root}(\xi_1)$ is not reduced, then $\mathsf{root}(\xi_1\Phi{\downarrow}) \in \mathcal{F}_d$. This contradicts the fact that $\mathsf{f}(u_1,\ldots,u_n)$ and $\mathsf{f}(\xi_1\Phi{\downarrow},\ldots,\xi_n\Phi{\downarrow})$ are unifiable since we have that $\mathsf{root}(u_1) \in \mathcal{F}_c$.

This allows us to conclude that either $\mathsf{root}(\xi) \in \mathcal{F}_c$ or $\mathsf{root}(\xi)$ is not reduced. □

The following corollary is a direct consequence of Lemma 31 since by definition of $\xi \in \Pi_r$, there is no $\xi' \in st(\xi)$ of form $\mathsf{f}(\xi_1,\ldots,\xi_n)$ with $\mathsf{f} \in \mathcal{F}_d$ and $\mathsf{root}(\xi_1) \in \mathcal{F}_c$.

Corollary 2. *Let Φ be a ground frame. Let $\xi \in \Pi_r$ such that $param(\xi) \subseteq \mathrm{dom}(\Phi)$ and $\xi\Phi{\downarrow} \notin \mathcal{T}(\mathcal{F}_c,\mathcal{N})$. We have that either $\mathsf{root}(\xi) \in \mathcal{F}_c$ or $\mathsf{root}(\xi)$ is not reduced.*

Lemma 32. *Let Φ be a ground frame. Let $\xi \in \Pi_r$ a ground recipe such that $param(\xi) \in \mathrm{dom}(\Phi)$. $\xi\Phi{\downarrow} \in \mathcal{T}(\mathcal{F}_c,\mathcal{N})$ if, and only if, $\mathsf{Message}(\xi\Phi)$ holds.*

Proof. We prove this result by induction on the size of ξ.

Base case: $|\xi| = 1$. In such a case, $\xi \in \mathrm{dom}(\Phi)$ thus there exists $(ax_i \rhd u_i) \in \Phi$ such $ax_i = \xi$ and $\xi\Phi{\downarrow} = u_i{\downarrow}$. But $u_i \in \mathcal{T}(\mathcal{F}_c,\mathcal{N})$. Hence, the result holds.

Induction case: $|\xi| > 1$. In such a case, we have that $\xi = \mathsf{f}(\xi_1,\ldots,\xi_n)$ with $\mathsf{f} \in \mathcal{F}_c \cup \mathcal{F}_d$. Assume first that $\mathsf{f} \in \mathcal{F}_c$. In such a case, $\xi_i\Phi{\downarrow} \in \mathcal{T}(\mathcal{F}_c,\mathcal{N})$ for every $i \in \{1\ldots n\}$. Hence, we can apply our induction hypothesis on each ξ_i. This allows us to conclude.

Assume now that $\mathsf{f} \in \mathcal{F}_d$. By hypothesis, we have that $\xi\Phi{\downarrow} \in \mathcal{T}(\mathcal{F}_c,\mathcal{N})$ and so f is reduced by the rewriting system. Let $\mathsf{f}(u_1,\ldots,u_n) \to u$ be the rewrite rule involved in $\mathsf{f}(\xi_1\Phi{\downarrow},\ldots,\xi_n\Phi{\downarrow}) \to \xi\Phi{\downarrow}$. We distinguish two cases:

- *Case 1:* $\xi_1\Phi\downarrow \in \mathcal{T}(\mathcal{F}_c,\mathcal{N})$. Since $vars(\{u_2,\ldots,u_n\}) \subseteq vars(u_1)$, we deduce that for every $i \in \{1,\ldots,n\}$, $\xi_i\Phi\downarrow \in \mathcal{T}(\mathcal{F}_c,\mathcal{N})$. Hence, we easily conclude by applying our induction hypothesis.

- *Case 2:* $\xi_1\Phi\downarrow \notin \mathcal{T}(\mathcal{F}_c,\mathcal{N})$. Thanks to Corollary 2, we deduce that either $\mathsf{root}(\xi_1) \in \mathcal{F}_c$ or $\mathsf{root}(\xi_1)$ is not reduced. Since $\xi \in \Pi_r$, we have that $\mathsf{root}(\xi_1) \notin \mathcal{F}_c$, hence $\mathsf{root}(\xi_1)$ is not reduced. It implies that $\mathsf{root}(\xi_1\Phi\downarrow) \in \mathcal{F}_d$. By definition of a rewriting rule, we know that $\mathsf{root}(u_1) \in \mathcal{F}_c$. This contradicts the fact that $\mathsf{f}(u_1,\ldots,u_n)$ and $\mathsf{f}(\xi_1\Phi\downarrow,\ldots,\xi_n\Phi\downarrow)$ are unifiable. Hence, this case is impossible. □

Lemma 33. *Let Φ be a closed frame and ξ,ξ' be two ground recipes in Π_r with $\mathsf{root}(\xi)$, $\mathsf{root}(\xi') \notin \mathcal{F}_c$ and such that $\mathsf{path}(\xi) = \mathsf{path}(\xi')$. If $\xi\Phi\downarrow,\xi'\Phi\downarrow \in \mathcal{T}(\mathcal{F}_c,\mathcal{N})$, then we have that $\xi\Phi\downarrow = \xi'\Phi\downarrow$.*

Proof. We prove this result by induction of the length n of $\mathsf{path}(\xi)$:

Base case $n = 1$: In such a case, we have that $\mathsf{path}(\xi) = \mathsf{path}(\xi') \in \mathcal{AX}$. Hence, we have that $\xi = \xi'$, and so $\xi\Phi\downarrow = \xi'\Phi\downarrow$.

Inductive step $n > 1$: Since $\mathsf{path}(\xi) = \mathsf{path}(\xi')$, we know that there exists $\mathsf{f} \in \mathcal{F}_d$ and there exist $\xi_1,\ldots,\xi_n,\xi'_1,\ldots,\xi'_n \in \Pi_r$ such that $\xi = \mathsf{f}(\xi_1,\ldots,\xi_n)$ and $\xi' = \mathsf{f}(\xi'_1,\ldots,\xi'_n)$. By Lemma 32, for all $\zeta \in st(\xi) \cup st(\xi')$, we have that $\zeta\Phi\downarrow \in \mathcal{T}(\mathcal{F}_c,\mathcal{N})$. Hence, for all $i = 1,\ldots,n$, for all $\zeta \in st(\xi_i) \cup st(\xi'_i)$, we have that $\zeta\Phi\downarrow \in \mathcal{T}(\mathcal{F}_c,\mathcal{N})$. By definition of path, we have that $\mathsf{path}(\xi_1) = \mathsf{path}(\xi'_1)$ (since $\mathsf{path}(\xi) = \mathsf{path}(\xi')$).

Applying our induction hypothesis on (ξ_1,ξ'_1), we obtain that $\xi_1\Phi\downarrow = \xi'_1\Phi\downarrow$. We have that $\xi\Phi\downarrow,\xi'\Phi\downarrow \in \mathcal{T}(\mathcal{F}_c,\mathcal{N})$. Hence, we have that

$$\mathsf{f}(\xi_1\Phi\downarrow,\ldots,\xi_n\Phi\downarrow) \to \xi\Phi\downarrow \quad \text{and} \quad \mathsf{f}(\xi'_1\Phi\downarrow,\ldots,\xi'_n\Phi\downarrow) \to \xi'\Phi\downarrow$$

using the rewriting rule associated to f. This rule is of the form $\mathsf{f}(u_1,\ldots,u_n) \to u$ with $u \in st(u_1)$. Since $\xi_1\Phi\downarrow = \xi'_1\Phi\downarrow$, we easily conclude that $\xi\Phi\downarrow = \xi'\Phi\downarrow$. □

Lemma 34. *Let $\mathcal{C} = (S_1;S_2;\Phi;D;E;E_\Pi;ND;\mathsf{NoUse})$ be a well-formed constraint system obtained by following the strategy and $(\sigma,\theta) \in \mathsf{Sol}(\mathcal{C})$. Let $\xi \in \Pi_r$ be a ground recipe conforms to $\Phi\theta$ w.r.t. $\mathsf{NoUse}\theta$. For all $\xi' \in st(\xi)$, ξ' conforms to $\Phi\theta$ w.r.t. $\mathsf{NoUse}\theta$.*

Proof. First, thanks to Lemma 28, we know that $\mathcal{C}$ satisfies $\mathsf{InvGeneral}$, and this will be used in the proof. We prove the result by induction on $|\xi|$.

Base case $|\xi| = 1$: In such a case, $\xi \in \mathcal{AX}$. Hence for all $\xi' \in st(\xi)$, $\xi' = \xi$ and so the result trivially holds.

Inductive step $|\xi| > 1$: Otherwise, $\xi = \mathsf{f}(\xi_1,\ldots,\xi_n)$. We do a case analysis on $\mathsf{C}\lfloor\xi\rfloor_\Phi$.

- Case $|\mathsf{C}\lfloor\xi\rfloor_\Phi| > 1$: In such a case, we have that $\mathsf{C}\lfloor\xi\rfloor_\Phi = \mathsf{f}(\mathsf{C}\lfloor\xi_1\rfloor_\Phi,\ldots,\mathsf{C}\lfloor\xi_n\rfloor_\Phi)$. Moreover, ξ conforms to $\Phi\theta$ w.r.t. $\mathsf{NoUse}\theta$ implies that for all $i \in \{1,\ldots,n\}$, ξ_i conforms to $\Phi\theta$ w.r.t. $\mathsf{NoUse}\theta$. Hence by inductive hypothesis on ξ_i, for all $i \in \{1,\ldots,n\}$, the result holds.

- Case $|\mathsf{C}\lfloor\xi\rfloor_\Phi| = 1$: Otherwise, since ξ conforms to $\Phi\theta$, we deduce that there exists $(\zeta, i \rhd u) \in \Phi$ such that $(\zeta, i \rhd u) \notin \mathsf{NoUse}\theta$ and $\zeta\theta = \xi$. Thanks to $\mathcal{C}$ being well-formed, (Definition 18, item 9), we deduce that $\mathsf{path}(\zeta)$ is closed. Hence there exists $\zeta_1,\ldots,\zeta_n$ such that $\zeta = \mathsf{f}(\zeta_1,\ldots,\zeta_n)$ and $\zeta_i\theta = \xi_i$ for all $i \in \{1,\ldots,n\}$.

But thanks to $\mathcal{C}$ being well-formed (Definition 18, item 9), we deduce that for all $\zeta' \in st(\zeta)$, $\mathsf{C}\lfloor\zeta'\rfloor_\Phi \in \mathcal{T}(\mathcal{F}_c, \mathcal{F}_d^* \cdot \mathcal{AX} \cup \mathcal{X}^2)$ and if $\mathsf{path}(\zeta') \in \mathcal{F}_d^* \cdot \mathcal{AX}$ then there exists j and v such that $(\zeta', j \rhd v) \in \Phi$. Hence for all $i \in \{1, \ldots, n\}$, $\zeta_i\theta$ conforms to $\Phi\theta$ w.r.t. $\mathsf{NoUse}\theta$ if for all $X \in vars^2(\mathsf{C}\lfloor\zeta'\rfloor_\Phi)$, $X\theta$ conforms to $\Phi\theta$ w.r.t. $\mathsf{NoUse}\theta$; and for all $\zeta'' \in st(\zeta_i)$, if $(\zeta'', j' \rhd v') \in \Phi$ for some j', v' then $(\zeta'', j' \rhd v') \notin \mathsf{NoUse}\theta$.

Since $(\zeta, i \rhd u) \notin \mathsf{NoUse}$, and relying on the fact that $\mathcal{C}$ satisfies $\mathsf{InvGeneral}$ (item 4), we deduce that for all $\zeta'' \in st(\zeta_i)$, if $\mathsf{path}(\zeta'') \in \mathcal{F}_d^* \cdot \mathcal{AX}$ then there exists j and v such that $(\zeta'', j \rhd v) \in \Phi$ and $(\zeta'', j \rhd v) \notin \mathsf{NoUse}$. At last, $(\sigma, \theta) \in \mathsf{Sol}(\mathcal{C})$ implies that for all $X \in vars^2(\mathcal{C})$, $X\theta$ conforms to $\Phi\theta$ w.r.t. $\mathsf{NoUse}\theta$. Hence we deduce that for all $i \in \{1, \ldots, n\}$, $\zeta_i\theta$ conforms to $\Phi\theta$ w.r.t. $\mathsf{NoUse}\theta$. We conclude by applying our inductive hypothesis on $\zeta_i\theta$, for all $i \in \{1, \ldots, n\}$. □

Lemma 35. *Let $\mathcal{C} = (S_1; S_2; \Phi; D; E; E_\Pi; ND; \mathsf{NoUse})$ be a well-formed constraint system obtained by following the strategy and $(\sigma, \theta) \in \mathsf{Sol}(\mathcal{C})$. Let ξ be a ground recipe in Π_r such that $\xi(\Phi\sigma)\downarrow \in \mathcal{T}(\mathcal{F}_c, \mathcal{N})$. We have that there exists ξ' a recipe in Π_r such that:*

- *ξ' conforms with $\Phi\theta$ w.r.t $\mathsf{NoUse}\theta$;*
- *$\xi(\Phi\sigma)\downarrow = \xi'(\Phi\sigma)\downarrow$; and*
- *$\mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(\xi') \leq \mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(\xi)$.*

Proof. First, thanks to Lemma 28, we know that $\mathcal{C}$ satisfies $\mathsf{InvGeneral}$, and this will be used in the proof. We prove this lemma by induction on $|\xi|$.

Base case $|\xi| = 0$: In such a case, the result trivially holds.

Inductive step $|\xi| > 0$: We do a case analysis on $\mathsf{C}\lfloor\xi\rfloor_\Phi$:

- *Case 1:* $\mathsf{C}\lfloor\xi\rfloor_\Phi \in (\mathcal{F}_d^* \cdot \mathcal{AX})$. By definition of $\mathsf{C}\lfloor\xi\rfloor_\Phi$, we know that there exists $(\zeta, i \rhd u) \in \Phi$ such that $\mathsf{path}(\zeta) = \mathsf{path}(\xi)$. Since $(\sigma, \theta) \in \mathsf{Sol}(\mathcal{C})$ and we know that $\mathcal{C}$ satisfies item 2 of $\mathsf{InvGeneral}$, we deduce that $i \leq \mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(\xi)$. Note that $\mathcal{C}$ is a well-formed constraint system and $(\sigma, \theta) \in \mathsf{Sol}(\mathcal{C})$, thus by Definition 18 (item 5), we have that $(\zeta\theta)(\Phi\sigma)\downarrow = u\sigma$. Moreover, relying on Lemma 33, we can deduce that $\xi(\Phi\sigma)\downarrow = (\zeta\theta)(\Phi\sigma)\downarrow$.

  Case 1.a : $(\zeta, i \rhd u) \in \mathsf{NoUse}$. Let $\Theta = \mathsf{mgu}(E_\Pi)$. In such a case, since $\mathcal{C}$ is a well-formed constraint system (Definition 18, item 8), we know that there exists $X \in vars^2(\mathcal{C})$ such that $\mathsf{C}\lfloor X\Theta\rfloor_\Phi \delta^1(\mathcal{C}) = u$ and $\mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(X\Theta) < i$. Since we proved that $i \leq \mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(\xi)$, we can deduce that $\mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(X\Theta) < \mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(\xi)$.

  But since $(\sigma, \theta) \in \mathsf{Sol}(\mathcal{C})$, we know that $\theta \vDash E_\Pi$, $X\theta \in \Pi_r$, $X\theta$ conforms with $\Phi\theta$ w.r.t. $\mathsf{NoUse}\theta$ and $(X\theta)\Phi\sigma\downarrow = (\zeta\theta)\Phi\sigma\downarrow$. Note that $\xi(\Phi\sigma)\downarrow = (\zeta\theta)(\Phi\sigma)\downarrow$ and so $\xi\Phi\sigma\downarrow = (X\theta)\Phi\sigma\downarrow$.

  Furthermore, $(\sigma, \theta) \in \mathsf{Sol}(\mathcal{C})$ also implies that for all $Z \in vars^2(X\Theta)$, $\mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(Z\theta) \leq \mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(Z)$. With $\theta \vDash E_\Pi$ and $\mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(X\Theta) < i$, we deduce that $\mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(X\theta) < i$. This allows us to conclude for $\xi' = X\theta$.

  Case 1.b: $(\zeta, i \rhd u) \notin \mathsf{NoUse}$. In such a case, let $\xi' = \zeta\theta$. Since $\mathcal{C}$ is a well formed constraint system (Definition 18, item 3), we know that $\mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(\zeta) \leq i$. Since

$(\sigma, \theta) \in \mathsf{Sol}(\mathcal{C})$ implies that for all $Z \in vars^2(\zeta)$, $\mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(Z\theta) \leq \mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(Z)$, we deduce that $\mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(\zeta\theta) \leq i$. Since we proved that $i \leq \mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(\xi)$, we deduce that $\mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(\zeta\theta) \leq \mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(\xi)$.

At last, since we assumed that $(\zeta, i \rhd u) \notin \mathsf{NoUse}$ then $(\zeta\theta, i \rhd u) \notin \mathsf{NoUse}\theta$. Hence $\xi' = \zeta\theta$ conforms to $\Phi\theta$ w.r.t. $\mathsf{NoUse}\theta$. Hence, we conclude.

- *Case 2:* $\mathsf{root}(\mathsf{C}\lfloor\xi\rfloor_\Phi) \in \mathcal{F}_c$. By definition of $\mathsf{C}\lfloor\xi\rfloor_\Phi$, there exists $\xi_1, \ldots, \xi_n \in \Pi_r$ such that $\xi = \mathsf{f}(\xi_1, \ldots, \xi_n)$ and $\mathsf{f} \in \mathcal{F}_c$. But for any $i = 1 \ldots n$, we have $\mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(\xi_i) \leq \mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(\xi)$ and $|\xi_i| < |\xi|$. Thus, by our inductive hypothesis, we can deduce that there exists $\xi'_1, \ldots, \xi'_n \in \Pi_r$ such that for all $i = 1 \ldots n$,
  - ξ'_i conforms with $\Phi\theta$ w.r.t $\mathsf{NoUse}\theta$;
  - $\xi_i(\Phi\sigma)\downarrow = \xi'_i(\Phi\sigma)\downarrow$; and
  - $param(\xi_i) \subseteq \{ax_1, \ldots, ax_j\}$ implies $param(\xi'_i) \subseteq \{ax_1, \ldots, ax_j\}$, for any j.

  Let $\xi' = \mathsf{f}(\xi'_1, \ldots, \xi'_n)$. Since $\mathsf{f} \in \mathcal{F}_c$, we can deduce that:
  - $\mathsf{f}(\xi'_1, \ldots, \xi'_n)$ conforms with $\Phi\theta$ w.r.t. $\mathsf{NoUse}\theta$;
  - $\xi\Phi\sigma\downarrow = \mathsf{f}(\xi_1, \ldots, \xi_n)\Phi\sigma\downarrow = \mathsf{f}(\xi'_1, \ldots, \xi'_n)\Phi\sigma\downarrow = \xi'\Phi\sigma\downarrow$; and
  - $\mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(\xi') = \max\{\mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(\xi'_i) \mid i \in \{1, \ldots, n\}\}$ and so $\mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(\xi') \leq \mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(\xi)$.

- $\mathsf{root}(\mathsf{C}\lfloor\xi\rfloor_\Phi) \in \mathcal{F}_d$. By definition of $\mathsf{C}\lfloor\xi\rfloor_\Phi$, there exists $\xi_1, \ldots, \xi_n \in \Pi_r$ such that $\xi = \mathsf{g}(\xi_1, \ldots, \xi_n)$ and $\mathsf{g} \in \mathcal{F}_d$. As in Case 2, we can apply our inductive hypothesis on each ξ_i. Thus, we will also have that there exists $\xi'_1, \ldots, \xi'_n$ such that:
  - ξ'_i conforms with $\Phi\theta$ w.r.t $\mathsf{NoUse}\theta$;
  - $\xi_i(\Phi\sigma)\downarrow = \xi'_i(\Phi\sigma)\downarrow$; and
  - $\mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(\xi'_i) \leq \mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(\xi_i)$.

  Let $\xi' = \mathsf{g}(\xi'_1, \ldots, \xi'_n)$. In order to conclude, we have to show that $\xi' = \mathsf{g}(\xi'_1, \ldots, \xi'_n)$ conforms with $\Phi\theta$ w.r.t. $\mathsf{NoUse}\theta$. We do a case analysis:

  Case 3.a: if $\mathsf{root}(\xi'_1) \in \mathcal{F}_c$, then we have that $\mathsf{g}(\xi'_1, \ldots, \xi'_n) \notin \Pi_r$. But we know that $\mathsf{g}(\xi'_1, \ldots, \xi'_n)\Phi\sigma\downarrow \in \mathcal{T}(\mathcal{F}_c, \mathcal{N})$ which means that g is reduced by a rewriting rule $\ell \to r$. But all the rewriting rules we consider are defined such that if g is reduced then it implies there exists a substerm ζ of ξ'_1 such that $\zeta\Phi\sigma\downarrow = \mathsf{g}(\xi'_1, \ldots, \xi'_n)\Phi\sigma\downarrow = \mathsf{g}(\xi_1, \ldots, \xi_n)\Phi\sigma\downarrow$. Since ξ'_1 conforms with $\Phi\theta$ w.r.t. $\mathsf{NoUse}\theta$, then so does ξ', which allow us to conclude.

  Case 3.b: Otherwise, we deduce that $\xi' \in \Pi_r$. Moreover, if there exists $(\zeta, i \rhd u) \in \Phi$ such that $\mathsf{path}(\zeta) = \mathsf{g} \cdot \mathsf{path}(\xi'_1)$, then we apply the same reasoning as the one done in Case 1. Else it implies that $\mathsf{C}\lfloor\xi'\rfloor_\Phi = \mathsf{g}(\mathsf{C}\lfloor\xi'_1\rfloor_\Phi, \ldots, \mathsf{C}\lfloor\xi'_n\rfloor_\Phi)$ and since ξ'_i, $i = 1 \ldots n$ are all conforms to $\Phi\theta$ w.r.t. $\mathsf{NoUse}\theta$, we conclude that ξ' conforms to $\Phi\theta$ w.r.t. $\mathsf{NoUse}\theta$. □

Lemma 36. *Let $\mathcal{C} = (S_1; S_2; \Phi; D; E; E_\Pi; ND; \mathsf{NoUse})$ be a well-formed constraint system obtained by following the strategy and $(\sigma, \theta) \in \mathsf{Sol}(\mathcal{C})$. Let $s \in \mathbb{N}$. Assume that $\textsc{Dest}(\zeta, \ell \to r, s)$ is useless $\mathcal{C}$ for any $\zeta, \ell \to r$. For all ground recipe $\xi \in \Pi_r$, if ξ conforms to $\Phi\theta$ w.r.t. $\mathsf{NoUse}\theta$, $\xi\Phi\sigma\downarrow \in \mathcal{T}(\mathcal{F}_c, \mathcal{N})$ and $param(\xi) \subseteq \{ax_1, \dots ax_s\}$ then $\mathsf{C}\lfloor\xi\rfloor_\Phi \in \mathcal{T}(\mathcal{F}_c, \mathcal{F}_d^* \cdot \mathcal{AX})$.*

Proof. Let p the position of the smallest subterm of $\mathsf{C}\lfloor\xi\rfloor_\Phi$ such that $\mathsf{root}(\mathsf{C}\lfloor\xi\rfloor_\Phi|_p) \in \mathcal{F}_d$. Hence, we deduce that $\xi|_p = \mathsf{g}(\xi_1, \dots, \xi_n)$ and $\mathsf{g} \in \mathcal{F}_d$. Moreover, since ξ conforms to $\Phi\theta$ w.r.t. $\mathsf{NoUse}\theta$, $\xi \in \Pi_r$ and by the minimality of $\mathsf{C}\lfloor\xi\rfloor_\Phi|_p$, we deduce that there exists $(\zeta, i \rhd u) \in \Phi$ such that $\xi_1 = \zeta\theta$ and $(\zeta, i \rhd u) \notin \mathsf{NoUse}$. Since $\mathcal{C}$ is well-formed, we know that $\mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(\zeta) \leq i$. Furthermore, since $(\sigma, \theta) \in \mathsf{Sol}(\mathcal{C})$, we deduce that $\mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(\zeta\theta) \leq i$. Moreover, since $\mathcal{C}$ is obtained by following the strategy then thanks to Lemma 28, $\mathcal{C}$ satisfies $\mathsf{InvGeneral}$. Thus we deduce that $ax_i \in st(\zeta\theta)$ and so $\mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(\zeta\theta) = i$. But $\zeta\theta \in st(\xi)$ and $param(\xi) \subseteq \{ax_1, \dots ax_s\}$ hence $i \leq s$.

Thus thanks $\textsc{Dest}(\zeta, \ell \to r, s)$ being useless on $\mathcal{C}$ with $\ell \to r$ the rewrite rule associated to g, we deduce that :

- either there exists $(\zeta', p' \rhd v') \in \Phi$ for some ξ' such that $\mathsf{path}(\zeta') = \mathsf{g} \cdot \mathsf{path}(\zeta)$ and some p' such that $p' \leq s$. But $\mathsf{path}(\xi|_p) = \mathsf{g} \cdot \mathsf{path}(\xi_1) = \mathsf{g} \cdot \mathsf{path}(\zeta\theta)$. Thanks to $\mathcal{C}$ being well-formed (Definition 18, item 1), we know that $\mathsf{path}(\zeta)$ is closed hence $\mathsf{path}(\xi|_p) = \mathsf{path}(\zeta')$. This is a contradiction with the fact that $\mathsf{root}(\mathsf{C}\lfloor\xi\rfloor_\Phi|_p) \in \mathcal{F}_d$.
- else $ND \vDash \forall\tilde{x}.u \neq^? u_1 \vee s \not\vdash^? u_2 \vee \dots \vee s \not\vdash^? u_n$ where $\mathsf{g}(u_1, \dots, u_n) \to w$ is a renaming of $\ell \to r$. But $(\sigma, \theta) \in \mathsf{Sol}(\mathcal{C})$ implies $\sigma \vDash ND$. Moreover, $\xi \in \Pi_r$ and $\xi(\Phi\sigma)\downarrow$ implies, thanks to Lemma 32, that $\xi|_p = \mathsf{g}(\xi_1, \dots, \xi_n)(\Phi\sigma)\downarrow$. Hence along with the hypothesis $param(\xi) \subseteq \{ax_1, \dots ax_s\}$, this is a contradiction with $\sigma \vDash ND$.

We conclude that such position p does not exist and so $\mathsf{C}\lfloor\xi\rfloor_\Phi \in \mathcal{T}(\mathcal{F}_c, \mathcal{F}_d^* \cdot \mathcal{AX})$. □

Appendix D.2. Relations on recipes variables

In our main proof of soundness, we usually assume an existing solution in a well-formed constraint system and then we transform this solution such that it becomes a solution of an another constraint system. In most cases, the transformation consists of replacing a recipe by another one which deduces the same message. The main issue of this replacement is that the new recipe has to satisfy several properties such that the conformity to the frame, its belonging to Π_r, *etc*

Example 49. *Let $\mathcal{C}$ be a constraint system with the following frame :*

$$\{ax_1, 1 \rhd \mathsf{senc}(a, b); ax_2, 2 \rhd \mathsf{senc}(b, a); ax_3, 3 \rhd a\}$$

A possible and natural execution of the rules would be to guess that the messages $\mathsf{senc}(a, b)$ and $\mathsf{senc}(b, a)$ can be decrypted, and so by application of the rule Dest*, we would have a constraint system such that:*

- $\Phi = \{ax_1, 1 \rhd \mathsf{senc}(a, b);\ ax_2, 2 \rhd \mathsf{senc}(b, a);\ ax_3, 3 \rhd a;\ \mathsf{sdec}(ax_1, X), 3 \rhd a;\ \mathsf{sdec}(ax_2, Y), 3 \rhd b\}$
- $D = \{X, 3 \vdash^? b\ ; Y, 3 \vdash^? a\}$

Thus one possible solution for this constraint system would be θ with $X\theta = \mathsf{sdec}(ax_2, ax_3)$ and $Y\theta = ax_3$. We can see that θ belongs to Π_r and also conforms to the frame Φ.

Since the two recipes ax_3 and $\mathsf{sdec}(ax_1, X)$ both deduce the same message, we could replace any instance of ax_3 by $\mathsf{sdec}(ax_1, X)$ and then forbid the use of the recipe ax_3 (equivalent to adding the frame element $(ax_3, 3 \rhd a)$ into the set NoUse).

Thus to ensure the soundness of this transformation, we need to ensure that we can transform θ in θ' such that θ' is a solution of the constraint system and such that it satisfies the belonging to Π_r and the conformity to the frame. But on this example, the only way to deduce a (for the constraint $Y, 3 \vdash^? a$) without using ax_3 is to use the recipe $\mathsf{sdec}(ax_1, X)$ and the only way to deduce b (for the constraint $X, 3 \vdash^? b$) is to use $\mathsf{sdec}(ax_2, Y)$ which produces a loop. Therefore, on this example, the replacement of the recipe ax_3 by $\mathsf{sdec}(ax_1, X)$, that deduces the same message, does not lead to a solution.

To formalise this, we introduce the following order.

Definition 19 (relation $<_\theta$)**.** *Let $\mathcal{C} = (S_1; S_2; \Phi; D; E; E_\Pi; ND; \mathsf{NoUse})$ be a well-formed constraint system, and θ be a mapping from $vars^2(\mathcal{C})$ to ground recipes such that for all $(X, i \rhd u) \in D$, we have that $param(X\theta) \subseteq \{ax_1, \ldots, ax_i\}$.*

We define a relation on $vars^2(D)$, denoted $<_\theta$, as the smallest relation that is closed by transitivity and such that: $X <_\theta Y$ if $X \in vars^2(\mathsf{C}\lfloor Y\theta \rfloor \delta^2(\mathcal{C}))$ and $X \neq Y$.

Intuitively, $X <_\theta Y$ represents the fact that in the solution θ, $X\theta$ is used in $Y\theta$. Thus, if you replace $X\theta$ by another recipe, the recipe $Y\theta$ will also need to be changed accordingly in order to conform to the frame.

Example 50. *Going back to our previous example, we have that $Y <_\theta X$ since we have $\mathsf{C}\lfloor X\theta \rfloor \delta^2(\mathcal{C}) = \mathsf{sdec}(ax_2, Y)$.*

We stated at the beginning of this subsection that the replacement has to preserve the belonging to Π_r. But a simple example with the application of the rule Eq-frame-ded shows that it is generally not true.

Example 51. *Let $\mathcal{C}$ be a constraint system with the following frame:*

$$\Phi = \{ax_1, 1 \rhd a \; ; ax_2, 2 \rhd \mathsf{senc}(a, a) \; ; ax_3, 3 \rhd a\}$$

and the following set of deducibility constraints:

$$D = \{X, 1 \vdash^? \mathsf{senc}(a, a) \; ; Y, 3 \vdash^? a\}$$

One possible solution for this constraint system would be θ with $X\theta = \mathsf{senc}(ax_1, ax_1)$ and $Y\theta = \mathsf{sdec}(ax_2, ax_3)$. We can see that θ belongs to Π_r and also conforms to the frame Φ. By applying the rule Eq-frame-ded *on $(ax_2, 2 \rhd \mathsf{senc}(a, a))$ and $(X, 1 \vdash^? \mathsf{senc}(a, a))$, the frame element $(ax_2, 2 \rhd \mathsf{senc}(a, a))$ will be added in the set NoUse and thus, we now have to replace each instance of ax_2 with $X\theta$. But in such a case, $Y\theta$ will become the recipe $\mathsf{sdec}(\mathsf{senc}(ax_1, ax_1), ax_3)$ which does not belong to Π_r. Thus, instead of just replacing ax_2 by $\mathsf{senc}(ax_1, ax_2)$, we will replace $Y\theta$ with ax_1.*

Lemma 37. *Let $\mathcal{C} = (S_1; S_2; \Phi; D; E; E_\Pi; ND; \mathsf{NoUse})$ be a well-formed constraint system. Let (σ, θ) be a pre-solution of $\mathcal{C}$. Let $X, Y \in vars^2(D)$ such that $X <_\theta Y$. We have that $X\theta$ is a strict subterm of $Y\theta$.*

Proof. $X <_\theta Y$ implies that there exist $X_1, \ldots, X_n \in vars^2(D)$ such that $X <_\theta X_1 <_\theta \ldots <_\theta X_n <_\theta Y$, and if we rename X, Y into X_0, X_{n+1} then we have that for all $i \in \{0, \ldots, n\}$, $X_i \in vars^2(\mathsf{C}\lfloor X_{i+1}\theta \rfloor \delta^2(\mathcal{C}))$ and $X_i \neq X_{i+1}$.

Since (σ, θ) is a pre-solution of $\mathcal{C}$, we know that for all $X \in vars^2(\mathcal{C})$, $X\theta$ conforms to the $\Phi\theta$ w.r.t. $\mathsf{NoUse}\theta$. Moreover, for all $i \in \{0, \ldots, n\}$, $X_i \in vars^2(\mathsf{C}\lfloor X_{i+1}\theta \rfloor_\Phi \delta^2(\mathcal{C}))$ implies that there exists $(\xi, k \rhd u) \in \Phi$ such that $X_i \in vars^2(\xi)$ and $\mathsf{path}(\xi) \in st(\mathsf{C}\lfloor X_{i+1}\theta \rfloor_\Phi)$. Thanks to $\mathcal{C}$ being well-formed, we know that $\mathsf{path}(\xi) \in \mathcal{F}_d^* \cdot \mathcal{AX}$ and exists hence X_i is a strict subterm of ξ which implies that $X_i\theta$ is a strict subterm of $\xi\theta$. But $X_{i+1}\theta$ is conformed to $\Phi\theta$ w.r.t. NoUse, and thus we have that $\xi\theta \in st(X_{i+1}\theta)$. Thus, we can deduce that $X_i\theta$ is a strict subterm of $X_{i+1}\theta$.

A simple induction on n allows us to conclude that $X_0\theta$ is a strict subterm of $X_{n+1}\theta$ and so $X\theta$ is a strict subterm of $Y\theta$. □

Lemma 38. *Let $\mathcal{C} = (S_1; S_2; \Phi; D; E; E_\Pi; ND; \mathsf{NoUse})$ be a well-formed constraint system. Let (σ, θ) be a pre-solution of $\mathcal{C}$. We have that $<_\theta$ is a strict partial order.*

Proof. Since (σ, θ) is a pre-solution of $\mathcal{C}$, we have that for all $X \in vars^2(D)$, $X\theta$ conforms to $\Phi\theta$ w.r.t. NoUse. By definition, $<_\theta$ is a strict partial order if, and only if:

- $\neg(X <_\theta X)$ (irreflexivity)
- if $X <_\theta Y$ then $\neg(Y <_\theta X)$ (asymmetry)
- if $X <_\theta Y$ and $Y <_\theta Z$ then $X <_\theta Z$ (transitivity)

By Definition 19, we already know that $<_\theta$ is closed by transitivity. Assume first that $X <_\theta X$. Thanks to Lemma 37, we know that $X\theta$ is a strict subterm of $X\theta$ which is impossible. For the same reason, $X <_\theta Y$ and $Y <_\theta X$ would imply that $X\theta$ is a strict subterm of $X\theta$, hence the contradiction. □

Lemma 39. *Let $\mathcal{C} = (S_1; S_2; \Phi; D; E; E_\Pi; ND; \mathsf{NoUse})$ be a well-formed constraint system obtained by following the strategy. Let $(\sigma, \theta) \in \mathsf{Sol}(\mathcal{C})$. Let $X, Y \in vars^2(D)$, we have that $X <_\theta Y$ implies that $\mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(X) \leq \mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(Y)$.*

Proof. First, thanks to Lemma 28, we know that $\mathcal{C}$ satisfies $\mathsf{InvGeneral}$ (in particular item 1). Therefore, we know that for all $(\xi, i \rhd u) \in \Phi$, $ax_i \in st(\xi\theta)$. Furthermore, since $\mathcal{C}$ is well formed (Definition 18, item 3), we deduce that $\mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(\xi) \leq i$. Moreover, $(\sigma, \theta) \in \mathsf{Sol}(\mathcal{C})$ implies that for all $Y \in vars^2(\xi)$, $\mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(Y\theta) \leq \mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(Y)$. Thus with $ax_i \in st(\xi\theta)$, we deduce that $\mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(\xi\theta) = i$.

We have that $X <_\theta Y$, and thus there exist $X_1, \ldots, X_n \in vars^2(D)$ such that $X <_\theta X_1 <_\theta \ldots <_\theta X_n <_\theta Y$ and if we rename X, Y into X_0, X_{n+1} then for all $i \in \{0, \ldots, n\}$, $X_i \in vars^2(\mathsf{C}\lfloor X_{i+1}\theta \rfloor \delta^2(\mathcal{C}))$ and $X_i \neq X_{i+1}$.

Let $i \in \{0, \ldots, n, n+1\}$. We know that there exist u_i and k_i such that $(X_i, k_i \vdash^? u_i) \in D$. Since $(\sigma, \theta) \in \mathsf{Sol}(\mathcal{C})$, we have that $param(X_i\theta) \subseteq \{ax_1, \ldots, ax_{k_i}\}$.

But $X_i \in vars^2(\mathsf{C}\lfloor X_{i+1}\theta \rfloor \delta^2(\mathcal{C}))$ implies that there exists $(\xi, j \rhd v) \in \Phi$ such that $\mathsf{path}(\xi) \in st(\mathsf{C}\lfloor X_{i+1}\theta \rfloor)$ and $X_i \in vars^2(\xi)$. Furthermore, since $X_{i+1}\theta$ conforms with $\Phi\theta$ w.r.t. NoUse, we can deduce that $\xi\theta \in st(X_{i+1}\theta)$. We have seen that $ax_j \in st(\xi\theta)$, we can deduce that $j \leq k_{i+1}$. At last, since $X_i\theta \in st(\xi\theta)$, $param(X_i\theta) \subseteq \{ax_1, \ldots, ax_{k_i}\}$ and $param(\xi\theta) \subseteq \{ax_1, \ldots, ax_j\}$, we can deduce that $k_i \leq j$ which implies $k_i \leq k_{i+1}$ and so $\mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(X_i) \leq \mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(X_{i+1})$. Altogether, this allows us to conclude that $\mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(X_0) \leq \ldots \leq \mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(X_{n+1})$ and so $\mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(X) \leq \mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(Y)$. □

Lemma 40. *Let $\mathcal{C} = (S_1; S_2; \Phi; D; E; E_\Pi; ND; \mathsf{NoUse})$ be a well-formed constraint system obtained by following the strategy. Let $(\sigma, \theta) \in \mathsf{Sol}(\mathcal{C})$. Let ξ be a ground recipe in Π_r and $(X, i \vdash^? u) \in D$ such that:*

- *ξ conforms to $\Phi\theta$ w.r.t. $\mathsf{NoUse}\theta$ and $param(\xi) \subseteq \{ax_1, \ldots, ax_i\}$.*
- *there exists a position p, such that $\xi' = X\theta_{|p}$, $\xi'\Phi\sigma{\downarrow} = \xi\Phi\sigma{\downarrow}$, and $\mathsf{C}_0 = \mathsf{C}_1[\mathsf{C}_2]_p$ where $\mathsf{C}_0 = \mathsf{C}\lfloor X\theta[\xi]_p \rfloor$, $\mathsf{C}_1 = \mathsf{C}\lfloor X\theta \rfloor$ and $\mathsf{C}_2 = \mathsf{C}\lfloor \xi \rfloor$.*
- *for all $Y \in vars^2(\mathsf{C}\lfloor\xi\rfloor\delta^2(\mathcal{C}))$, $\neg(X <_\theta Y)$.*

Then there exists θ' such that (σ, θ') is a pre-solution of $\mathcal{C}$ with $\theta' \vDash \mathsf{mgu}(E_\Pi)$, $X\theta' = X\theta[\xi]_p$ and for all $Y \in vars^2(D) \setminus \{X\}$, $\mathsf{C}\lfloor Y\theta \rfloor_{\Phi\theta} = \mathsf{C}\lfloor Y\theta' \rfloor_{\Phi\theta'}$.

Proof. First, thanks to Lemma 28, we know that $\mathcal{C}$ satisfies $\mathsf{InvGeneral}$, and this will be used in the proof. Since we assume that $\mathcal{C}$ is well-formed (Definition 18, item 2), the path of any recipe of a frame element of Φ is closed hence for all ξ, for all θ, $\mathsf{C}\lfloor\xi\rfloor_\Phi = \mathsf{C}\lfloor\xi\rfloor_{\Phi\theta}$. Hence we omit the substitution in the context. Let θ' be a substitution defined as follows:

- for all $Y \in vars^2(D)$ such that $\neg(X <_\theta Y)$, $Y\theta' \stackrel{\mathsf{def}}{=} Y\theta$
- $X\theta' \stackrel{\mathsf{def}}{=} X\theta[\xi]_p$
- Otherwise, $Y\theta' \stackrel{\mathsf{def}}{=} \mathsf{C}\lfloor Y\theta \rfloor_\Phi \delta^2(\mathcal{C})\theta'$, where $Y \in vars^2(D)$
- for all $Y \in vars^2(\mathcal{C}) \setminus vars^2(D)$, $Y\theta' = Y\mathsf{mgu}(E_\Pi)\theta'$

First, we need to justify that the substitution θ' is well-defined. By Lemma 38, we know that the relation $<_\theta$ is a strict partial order. Let $Y \in vars^2(D)$ such that $X <_\theta Y$ and so $Y\theta' = \mathsf{C}\lfloor Y\theta \rfloor_\Phi \delta^2(\mathcal{C})\theta'$. But for all $Z \in vars^2(\mathsf{C}\lfloor Y\theta \rfloor_\Phi \delta^2(\mathcal{C}))$, we have $Z <_\theta Y$. Since the relation $<_\theta$ is a strict partial order on $vars^2(D)$, we conclude that $Y\theta'$ is well-defined. At last, for all $Y \in vars^2(\mathcal{C}) \setminus vars^2(D)$, for all $X \in vars^2(Y\mathsf{mgu}(E_\Pi))$, $X \in vars^2(D)$. Since θ' is well defined on any variables in $vars^2(D)$, we conclude that θ' is well-defined on all variable of $\mathcal{C}$.

Now, it remains to prove the four expected properties.

Property 1. $X\theta' = X\theta[\xi]_p$*:* By definition of θ', we know that $X\theta' = X\theta[\xi]_p$ hence the result trivially holds.

Property 2. $\theta' \vDash \mathsf{mgu}(E_\Pi)$*:* By definition, for all $Y \in vars^2(\mathcal{C}) \setminus vars^2(D)$, $Y\theta' = Y\mathsf{mgu}(E_\Pi)\theta'$. Hence, we trivially deduce that $\theta' \vDash \mathsf{mgu}(E_\Pi)$.

Property 3. for all $Y \in vars^2(D) \setminus \{X\}$, $\mathsf{C}\lfloor Y\theta \rfloor_{\Phi\theta} = \mathsf{C}\lfloor Y\theta' \rfloor_{\Phi\theta'}$: For any variable $Y \in vars^2(D)$ such that $\neg(X <_\theta Y)$, we have that $Y\theta' = Y\theta$ which means that $\mathsf{C}\lfloor Y\theta \rfloor_\Phi = \mathsf{C}\lfloor Y\theta' \rfloor_\Phi$. Moreover, for all $Y \in vars^2(\mathcal{C}) \setminus \{X\}$, if $X <_\theta Y$ then $Y\theta' = \mathsf{C}\lfloor Y\theta \rfloor_\Phi \delta^2(\mathcal{C})\theta'$. But since $Y\theta$ is a ground recipe, then $st(\mathsf{C}\lfloor Y\theta \rfloor_\Phi) \cap \mathrm{dom}(\delta^2(\mathcal{C})) \subseteq (\mathcal{F}_d^* \cdot \mathcal{AX})$ and for all $w \in \mathrm{dom}(\delta^2(\mathcal{C})) \cap (\mathcal{F}_d^* \cdot \mathcal{AX})$, we have that $\mathsf{C}\lfloor w\delta^2(\mathcal{C})\theta \rfloor_\Phi = \mathsf{C}\lfloor w\delta^2(\mathcal{C})\theta' \rfloor_\Phi$ $(= w)$. Therefore, we have that $\mathsf{C}\lfloor Y\theta' \rfloor_\Phi = \mathsf{C}\lfloor Y\theta \rfloor_\Phi$.

Property 4. (σ, θ') is a pre-solution of $\mathcal{C}$, *i.e.*

- for every $Y \in vars^2(\mathcal{C})$, we have that $Y\theta'$ conforms to the frame $\Phi\theta'$ w.r.t. $\mathsf{NoUse}\theta$, and
- for every $(Y, j \vdash^? v)$ in D, we have that $(Y\theta')(\Phi\sigma)\downarrow = v\sigma\downarrow$ and $param(Y\theta') \subseteq \{ax_1, \ldots, ax_j\}$.

Thanks to $\mathcal{C}$ being well-formed (Definition 18, item 7), we know that for all $Y \in vars^2(\mathcal{C})$, $\mathsf{C}\lfloor Y\mathsf{mgu}(E_\Pi)\rfloor \in \mathcal{T}(\mathcal{F}_c, \mathcal{F}_d^* \cdot \mathcal{AX} \cup \mathcal{X}^2)$ and for all $\zeta \in st(Y\mathsf{mgu}(E_\Pi))$, $\mathsf{path}(\zeta) \in \mathcal{F}_d^* \cdot \mathcal{AX}$ implies that there exists j and v such that $(\zeta, j \rhd v) \in \Phi$. Since $\theta \vDash E_\Pi$, we deduce that $\mathsf{C}\lfloor Y\theta\rfloor = \mathsf{C}\lfloor Y\mathsf{mgu}(E_\Pi)\rfloor_{\{Z \mapsto \mathsf{C}\lfloor Z\theta\rfloor \mid Z \in vars^2(\mathsf{C}\lfloor Y\mathsf{mgu}(E_\Pi)\rfloor)\}}$. But by definition, for all $Y \in vars^2(\mathcal{C}) \setminus vars^2(D)$, $Y\theta' = \mathsf{mgu}(E_\Pi)\theta'$. Hence, along with $\mathcal{C}$ satisfying $\mathsf{InvGeneral}$ (item 3), we deduce that $Y\theta'$ conforms to $\Phi\theta'$ w.r.t. $\mathsf{NoUse}\theta'$ if and only if for all $Z \in vars^2(\mathsf{C}\lfloor Y\mathsf{mgu}(E_\Pi)\rfloor)$, $Z\theta'$ conforms to $\Phi\theta'$ w.r.t. $\mathsf{NoUse}\theta'$. Thus it remains to prove that for all $Y \in vars^2(D)$, $Y\theta'$ conforms to $\Phi\theta'$ w.r.t. $\mathsf{NoUse}\theta'$

Let $Y, j \vdash^? v$ be a deducibility constraint in D. We prove the results by induction on $<_\theta$.
Base case 1: $\neg(X <_\theta Y)$. In such a case, we have that $Y\theta' = Y\theta$. Thus, we have $(Y\theta')\Phi\sigma\downarrow = (Y\theta)\Phi\sigma\downarrow$ and $param(Y\theta') = param(Y\theta) \subseteq \{ax_1, \ldots, ax_j\}$. Furthermore, by definition of $<_\theta$, we have that for all $Z \in vars^2(\mathsf{C}\lfloor Y\theta\rfloor_\Phi \delta^2(\mathcal{C}))$, $Z <_\theta Y$ and so $\neg(X <_\theta Z)$. Thus, $Z\theta = Z\theta'$. With $Y\theta' = Y\theta$ and $Y\theta$ conforms with $\Phi\theta$ w.r.t. $\mathsf{NoUse}\theta$, we can deduce that $Y\theta'$ also conforms with $\Phi\theta'$ w.r.t. $\mathsf{NoUse}\theta'$.

Base case 2: $Y = X$. In such a case, we have that $X\theta = X\theta[\xi]_p$. By hypothesis, we know that $\xi(\Phi\sigma)\downarrow = X\theta|_p\Phi\sigma\downarrow$. Thus, we have that $X\theta[\xi]_p\Phi\sigma\downarrow = X\theta\Phi\sigma\downarrow$. Furthermore, we also know that $param(\xi) \subseteq \{ax_1, \ldots, ax_i\}$ and $param(X\theta) \subseteq \{ax_1, \ldots, ax_i\}$. Thus we can conclude that $param(X\theta[\xi]_p) \subseteq \{ax_1, \ldots, ax_i\}$.

By hypothesis, we know that for all $Z \in vars^2(\mathsf{C}\lfloor \xi\rfloor_\Phi \delta^2(\mathcal{C}))$, $\neg(X <_\theta Z)$ which means that $Z\theta' = Z\theta$ and so ξ conforms with $\Phi\theta'$ w.r.t. $\mathsf{NoUse}\theta$. By definition of $<_\theta$, we have that for all $Z \in vars^2(\mathsf{C}\lfloor X\theta\rfloor_\Phi \delta^2(\mathcal{C}))$, $Z <_\theta X$ which means that $Z\theta' = Z\theta$ and so $X\theta$ conforms with $\Phi\theta'$ w.r.t. $\mathsf{NoUse}\theta'$. Therefore, since by hypothesis we have that $\mathsf{C}\lfloor X\theta'\rfloor = \mathsf{C}\lfloor X\theta\rfloor[\mathsf{C}\lfloor\xi\rfloor]_p$, we can conclude that $X\theta' = X\theta[\xi]_p$ conforms with $\Phi\theta'$ w.r.t. $\mathsf{NoUse}\theta'$.

Inductive case $X <_\theta Y$*:* In such a case, $Y\theta' = \mathsf{C}\lfloor Y\theta\rfloor_\Phi \delta^2(\mathcal{C})\theta'$. We know by definition of $<_\theta$ that if $Z \in vars^2(\mathsf{C}\lfloor Y\theta\rfloor_\Phi \delta^2(\mathcal{C}))$ then $Z <_\theta Y$. Hence by Lemma 39, $\mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(Z) \leq \mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(Y)$ which implies that there exists a constraint $(Z, \ell \vdash^? r) \in D$ with $\ell \leq j$. Therefore, thanks to our induction hypothesis, we deduce that $(Z\theta')(\phi\sigma)\downarrow = r\sigma\downarrow$ and $param(Z\theta') \subseteq \{ax_1, \ldots, ax_\ell\}$.

Let $w \in st(\mathsf{C}\lfloor Y\theta\rfloor_\Phi) \cap (\mathcal{F}_d^* \cdot \mathcal{AX})$. Hence there exists $(\zeta, \ell \rhd r) \in \Phi$ such that $\zeta = w\delta^2(\mathcal{C})\theta'$. We already show that for all $Z \in vars^2(\zeta)$ with $(Z, \ell' \vdash^? r') \in D$, $Z\theta'(\Phi\sigma)\downarrow = r'\sigma\downarrow$ and $param(Z\theta') \subseteq \{ax_1, \ldots, ax'_\ell\}$. Hence, thanks to $\mathcal{C}$ being well-formed (Definition 18, item 5), we deduce that $\zeta\theta'(\Phi\sigma)\downarrow = r\downarrow = \zeta\theta(\Phi\sigma)\downarrow$. Moreover, once again thanks to $\mathcal{C}$ being well-formed (Definition 18, item 3), $param(\zeta\theta') \subseteq \{ax_1, \ldots, ax_\ell\}$ and so $param(w\delta^2(\mathcal{C})\theta') \subseteq \{ax_1, \ldots, ax_\ell\}$. At last, since $(\sigma, \theta) \in \mathsf{Sol}(\mathcal{C})$ and thanks to $\mathcal{C}$ satisfying $\mathsf{InvGeneral}$ (item 1), we deduce that $ax_\ell \in st(\zeta\theta)$ which implies that $ax_\ell \in st(Y\theta)$ and so $\ell \leq j$. Hence, we can conclude that $Y\theta'(\Phi\sigma)\downarrow = Y\theta(\Phi\sigma)\downarrow = v\sigma\downarrow$ and $param(Y\theta') \subseteq \{ax_1, \ldots, ax_j\}$.

Lastly, by definition of θ', we have that $Y\theta' = \mathsf{C}\lfloor Y\theta\rfloor \delta^2(\mathcal{C})\theta'$ thus, since $Y\theta$ conforms with $\Phi\theta$ w.r.t. $\mathsf{NoUse}\theta$, we deduce that $Y\theta'$ conforms with the frame $\Phi\theta'$ w.r.t. $\mathsf{NoUse}\theta'$.
□

Appendix D.3. Preliminaries for soundness of Phase 1 Step a

In this subsection, we are only showing some properties to help proving the soundness for the first step of Phase . The only rules that can be applied during this phase are DEST and EQ-FRAME-DED. Therefore, thanks to Lemma 27, the constraint systems or matrices of constraint systems satisfy the invariants $\mathsf{PP1Sa}(s)$ for some s that depends on the parameter of the rules DEST and EQ-FRAME-DED.

Let T be a set of terms, and u be a term, we denote by $\mathsf{nb_{occ}}(u, T)$ the number of occurrences of u in T.

Lemma 41. *Let $\mathcal{M}$ be a matrix of constraint systems obtained during phase 1.a with support s by following the strategy. Let $\mathcal{C}$ be a constraint system in M with Φ its associated frame, and $(\sigma, \theta) \in \mathsf{Sol}(\mathcal{C})$. Moreover, let $(\xi, s \rhd u) \in \Phi$ and let $\zeta \in \Pi_r$ such that:*

- *$param(\zeta) \subseteq \{ax_1, \ldots, ax_{s-1}\}$,*
- *$\zeta\Phi\sigma\downarrow = u\sigma$,*
- *for all $Y \in vars^2(\mathcal{C})$, $\xi \notin st(Y\mathsf{mgu}(E_\Pi))$, and*
- *for all $\mathsf{g} \in \mathcal{F}_d$, for all $(\xi', i \rhd v) \in \Phi$, $\mathsf{path}(\xi') \neq \mathsf{g} \cdot \mathsf{path}(\xi)$.*

Either $\mathsf{nb_{occ}}(\xi\theta, \{X\theta \mid X \in vars^2(\mathcal{C})\}) = 0$ or else there exists θ' such that $(\sigma, \theta') \in \mathsf{Sol}(\mathcal{C})$ and:

$$\mathsf{nb_{occ}}(\xi\theta', \{X\theta' \mid X \in vars^2(\mathcal{C})\}) < \mathsf{nb_{occ}}(\xi\theta, \{X\theta \mid X \in vars^2(\mathcal{C})\}).$$

Proof. Let $\mathcal{C} = (S_1; S_2; \Phi; D; E; E_\Pi; ND; \mathsf{NoUse})$, $(\sigma, \theta) \in \mathsf{Sol}(\mathcal{C})$. Let $(X, k \vdash^? v) \in D$ such that $k \geq s$ and $\mathsf{C}\lfloor\xi\rfloor \in st(\mathsf{C}\lfloor X\theta\rfloor)$. We first show that if such $(X, k \vdash^? v)$ does not exist, then $\mathsf{nb_{occ}}(\xi\theta, \{X\theta \mid X \in vars^2(\mathcal{C})\}) = 0$. By hypothesis, we know that for all $\mathsf{g} \in \mathcal{F}_d$, for all $(\xi', i \rhd v) \in \Phi$, $\mathsf{path}(\xi') \neq \mathsf{g} \cdot \mathsf{path}(\xi)$. Moreover, since $\mathcal{C}$ satisfies $\mathsf{PP1Sa}(s)$, we know that for all $(\beta, s \rhd v) \in \Phi(\mathcal{C})$, either $\beta \in \mathcal{AX}$ or there exist $X_2, \ldots, X_n \in \mathcal{X}^2$, $\mathsf{f} \in \mathcal{F}_d$ and $(\beta', p \rhd v) \in \Phi(\mathcal{C})$ such that $\beta = \mathsf{f}(\beta', X_2, \ldots, X_n)$ and $p \leq s$. Hence we deduce that for all $(\beta, s \rhd v) \in \Phi(\mathcal{C})$, if $\xi \in st(\beta)$ then $\xi = \beta$. Furthermore, since for all $Y \in vars^2(\mathcal{C})$, $\xi \notin st(Y\mathsf{mgu}(E_\Pi))$, then for all $Y \in vars^2(\mathcal{C})$, $\xi\theta \in st(Y\theta)$ implies that there exists $Z \in vars^2(D)$ such that $\xi\theta \in st(Z\theta)$. We select $X \in vars^2(D)$ such that $X\theta$ is the smallest recipe that contains $\xi\theta$. If X does not exist then $\mathsf{nb_{occ}}(\xi\theta, \{X\theta \mid X \in vars^2(\mathcal{C})\}) = 0$ else since $X\theta$ conforms with $\Phi\theta$ w.r.t. $\mathsf{NoUse}\theta$ and for all $(\beta, s \rhd v) \in \Phi(\mathcal{C})$, if $\xi \in st(\beta)$ then $\xi = \beta$, we conclude that $\mathsf{C}\lfloor\xi\rfloor \in st(\mathsf{C}\lfloor X\theta\rfloor)$.

Property 1. We first show for all $\zeta \in \Pi_r$, for all position p in $X\theta$, if $\zeta\Phi\sigma\downarrow = (X\theta)_{|p}\Phi\sigma\downarrow$, then there exist $\zeta' \in st(\zeta)$ and a position p' such that p' is a prefix of p and $X\theta[\zeta]_p(\Phi\sigma)\downarrow = X\theta[\zeta']_{p'}(\Phi\sigma)\downarrow$ and $X\theta[\zeta']_{p'} \in \Pi_r$. We prove this result by induction on the length $|p|$ of p.

Base case $|p| = 0$. In such a case we have that $p = \epsilon$. Let $\zeta' = \zeta$ and $p' = p$. We have that $X\theta[\zeta']_{p'} = \zeta' = \zeta$. Since by hypothesis, we have that $\zeta \in \Pi_r$, the result trivially holds.

Inductive step $|p| > 0$. In such a case, we have that $p = p_1 \cdot r$ for some $r \in \mathbb{N}$ and some p_1 such that $|p_1| < |p|$. Assume that $X\theta_{|p_1} = \mathsf{f}(\xi_1, \ldots, \xi_n)$. We have to distinguish two cases:

1. $r = 1$, $\mathsf{f} \in \mathcal{F}_d$ *and* $\mathsf{root}(\zeta) \in \mathcal{F}_c$*:* We know that $X\theta(\Phi\sigma)\downarrow \in \mathcal{T}(\mathcal{F}_c, \mathcal{N})$ and $X\theta \in \Pi_r$. Thus, by Lemma 32, we can deduce that $\mathsf{f}(\xi_1, \ldots, \xi_n)\Phi\sigma\downarrow \in \mathcal{T}(\mathcal{F}_c, \mathcal{N})$, and thus f has been reduced. But by hypothesis, we also know that $\zeta\Phi\sigma\downarrow = \xi_1\Phi\sigma\downarrow$. If we denote $\zeta = \mathsf{g}(\zeta_1, \ldots, \zeta_m)$, then by definition of our rewrite rule, we have that $\zeta_1\Phi\sigma\downarrow = \mathsf{f}(\xi_1, \ldots, \xi_n)\Phi\sigma\downarrow$. Since $\zeta \in \Pi_r$, we have also that $\zeta_1 \in \Pi_r$. Furthermore, we have $\zeta_1\Phi\sigma\downarrow = X\theta_{|p_1}\Phi\sigma\downarrow$. Thanks to our induction hypothesis, we deduce that there exist $\zeta_1' \in st\zeta_1$ and p_1' a prefix of p_1 such $X\theta[\zeta_1]_{p_1}(\Phi\sigma)\downarrow = X\theta[\zeta_1']_{p_1'}(\Phi\sigma)\downarrow$ and $X\theta[\zeta_1']_{p_1'} \in Rr$. Let $\zeta' = \zeta_1'$ and $p' = p_1'$. This allows us to conclude.

2. *Otherwise:* By definition of Π_r, we have that $X\theta[\zeta]_p \in \Pi_r$, and thus the result holds with $\zeta' = \zeta$ and $p' = p$.

Property 2. We show that for all $\zeta \in \Pi_r$ such that $param(\zeta) \subseteq \{ax_1, \ldots, ax_k\}$, for all $(\sigma, \theta) \in \mathsf{Sol}(\mathcal{C})$, for all position $p \in \mathcal{P}os(\mathsf{C}\lfloor X\theta \rfloor)$, if $\zeta(\Phi\sigma)\downarrow = (X\theta)_{|p}(\Phi\sigma)\downarrow$, ζ conforms to $\Phi\theta$ w.r.t. $\mathsf{NoUse}\theta$, for all $Y \in vars^2(\mathsf{C}\lfloor\zeta\rfloor\delta^2(\mathcal{C}))$, $\neg(X <_\theta Y)$ and $\mathsf{nb}_{\mathsf{occ}}(\mathsf{C}\lfloor\xi\rfloor, \mathsf{C}\lfloor X\theta[\zeta]_p\rfloor) < \mathsf{nb}_{\mathsf{occ}}(\mathsf{C}\lfloor\xi\rfloor, \mathsf{C}\lfloor X\theta\rfloor)$ then there exists θ' such that $(\sigma, \theta') \in \mathsf{Sol}(\mathcal{C})$ and $\mathsf{nb}_{\mathsf{occ}}(\mathsf{C}\lfloor\xi\rfloor, \{\mathsf{C}\lfloor Y\theta'\rfloor \mid Y \in vars^2(\mathcal{C})\}) < \mathsf{nb}_{\mathsf{occ}}(\mathsf{C}\lfloor\xi\rfloor, \{\mathsf{C}\lfloor Y\theta\rfloor \mid Y \in vars^2(\mathcal{C})\})$.

We prove this property by induction on the length $|p|$ of p.

Base case $|p| = 0$. In such a case, we can apply Lemma 40. Indeed, ζ conforms to $\Phi\theta$ w.r.t. $\mathsf{NoUse}\theta$ and $param(\zeta) \subseteq \{ax_1, \ldots, ax_k\}$. Furthermore we have $\zeta(\Phi\sigma)\downarrow = X\theta(\Phi\sigma)\downarrow$ and for all $Y \in vars^2(\mathsf{C}\lfloor\zeta\rfloor\delta^2(\mathcal{C}))$, $\neg(X <_\theta Y)$. Hence, we deduce that there exists θ' such that (σ, θ') is a pre-solution of $\mathcal{C}$ with $X\theta' = \zeta$ and for all $Y \in vars^2(D)\backslash\{X\}$, we have that $\mathsf{C}\lfloor Y\theta\rfloor = \mathsf{C}\lfloor Y\theta'\rfloor$, $\theta' \vDash \mathsf{mgu}(E_\Pi)$. By hypothesis, we know that $\mathsf{nb}_{\mathsf{occ}}(\mathsf{C}\lfloor\xi\rfloor, \{\mathsf{C}\lfloor\zeta\rfloor\}) < \mathsf{nb}_{\mathsf{occ}}(\mathsf{C}\lfloor\xi\rfloor, \{\mathsf{C}\lfloor X\theta\rfloor\})$ and since $\mathsf{C}\lfloor Y\theta\rfloor = \mathsf{C}\lfloor Y\theta'\rfloor$, for all $Y \in vars^2(D)\backslash\{X\}$, we can deduce that

$$\mathsf{nb}_{\mathsf{occ}}(\mathsf{C}\lfloor\xi\rfloor, \{\mathsf{C}\lfloor Y\theta'\rfloor \mid Y \in vars^2(D)\}) < \mathsf{nb}_{\mathsf{occ}}(\mathsf{C}\lfloor\xi\rfloor, \{\mathsf{C}\lfloor Y\theta\rfloor \mid Y \in vars^2(D)\}).$$

Moreover, by hypothesis on ξ, we know that for all $Y \in vars^2(\mathcal{C})$, $\xi \notin st(Y\mathsf{mgu}(E_\Pi))$. Hence, since $\theta \vDash \mathsf{mgu}(E_\Pi)$ and $\theta' \vDash \mathsf{mgu}(E_\Pi)$, we deduce that:

$$\mathsf{nb}_{\mathsf{occ}}(\mathsf{C}\lfloor\xi\rfloor, \{\mathsf{C}\lfloor Y\theta'\rfloor \mid Y \in vars^2(\mathcal{C})\}) < \mathsf{nb}_{\mathsf{occ}}(\mathsf{C}\lfloor\xi\rfloor, \{\mathsf{C}\lfloor Y\theta\rfloor \mid Y \in vars^2(\mathcal{C})\}).$$

Furthermore, $(\sigma, \theta) \in \mathsf{Sol}(\mathcal{C})$ implies $\sigma \vDash E \wedge ND$. At last, $\mathcal{C}$ satisfies $\mathsf{PP1Sa}(s)$ (item 4) thus along with $\theta' \vDash \mathsf{mgu}(E_\Pi)$, we deduce that $\theta' \vDash E_\Pi$ and so the result holds. Hence the result holds.

Inductive step $|p| > 0$. In such a case, we have that $p = p' \cdot r$ with $r \in \mathbb{N}$ and $|p'| < |p|$. Assume that $X\theta_{|p'} = \mathsf{f}(\xi_1, \ldots, \xi_n)$. Since $\zeta(\Phi\sigma)\downarrow = X\theta_{|p}(\Phi\sigma)\downarrow$, we have that $(X\theta_{|p'})[\zeta]_r(\Phi\sigma)\downarrow = X\theta_{|p'}(\Phi\sigma)\downarrow$. By definition of $(\sigma, \theta) \in \mathsf{Sol}(\mathcal{C})$, we know that $\mathsf{f}(\xi_1, \ldots, \xi_n)$ conforms to $\Phi\theta$. Now, we distinguish several cases:

Case (a): $\mathsf{f} \in \mathcal{F}_c$. In such a case, let $\zeta' = (X\theta_{|p'})[\zeta]_r$. Hence we have that $X\theta[\zeta']_{p'} = X\theta[\zeta]_p$ which implies that $X\theta[\zeta']_{p'}(\Phi\sigma)\downarrow = X\theta(\Phi\sigma)\downarrow$ and $X\theta[\zeta']_{p'} \in \Pi_r$. Moreover, since $\mathsf{f} \in \mathcal{F}_c$, we have that $\mathsf{C}\lfloor\zeta'\rfloor = \mathsf{f}(\mathsf{C}\lfloor\xi_1\rfloor, \ldots, \mathsf{C}\lfloor\xi_{r-1}\rfloor, \mathsf{C}\lfloor\zeta\rfloor, \mathsf{C}\lfloor\xi_{r+1}\rfloor, \ldots, \mathsf{C}\lfloor\xi_n\rfloor)$. But by hypothesis, ζ and $X\theta_{|p'}$ are conform to $\Phi\theta$ w.r.t. NoUse. Hence, $\xi_1, \ldots, \xi_n$ also

conforms to $\Phi\theta$ w.r.t. NoUse which implies that ζ' conforms to $\Phi\theta$ w.r.t. $\mathsf{NoUse}\theta$. Furthermore, we know that $X\theta$ conforms to $\Phi\theta$ w.r.t. $\mathsf{NoUse}\theta$ and $p \in \mathcal{P}os(\mathsf{C}\lfloor X\theta \rfloor)$ hence $\mathsf{C}\lfloor \xi_1 \rfloor, \ldots, \mathsf{C}\lfloor \xi_n \rfloor \in st(\mathsf{C}\lfloor X\theta \rfloor)$. Moreover, by definition of $<_\theta$, we have for all $i \in \{1, \ldots, n\}$, for all $Y \in vars^2(\mathsf{C}\lfloor \xi_i \rfloor \delta^2(\mathcal{C}))$, $Y <_\theta X$. But by Lemma 38, $<_\theta$ is a strict partial order which means that $Y <_\theta X$ implies $\neg(X <_\theta Y)$. Since by hypothesis, we have that for all $Y \in vars^2(\mathsf{C}\lfloor \zeta \rfloor \delta^2(\mathcal{C}))$, $\neg(X <_\theta Y)$, then we can deduce that for all $Y \in vars^2(\mathsf{C}\lfloor \zeta' \rfloor \delta^2(\mathcal{C}))$, $\neg(X <_\theta Y)$.

At last, $X\theta[\zeta']_{p'} = X\theta[\zeta]_p$ and $\#\{\mathsf{C}\lfloor \xi \rfloor \in st(\mathsf{C}\lfloor X\theta[\zeta]_p \rfloor)\} < \#\{\mathsf{C}\lfloor \xi \rfloor \in st(\mathsf{C}\lfloor X\theta \rfloor)\}$ trivially implies that $\#\{\mathsf{C}\lfloor \xi \rfloor \in st(\mathsf{C}\lfloor X\theta[\zeta']_{p'} \rfloor)\} < \#\{\mathsf{C}\lfloor \xi \rfloor \in st(\mathsf{C}\lfloor X\theta \rfloor)\}$.

Hence we conclude by applying our inductive hypothesis on θ, ζ' and p'.

Case (b): $\mathsf{f} \in \mathcal{F}_d$, $r \neq 1$. This case is similar to Case (a). Indeed, let $\zeta' = (X\theta_{|p'})[\zeta]_r$. We have $p \in \mathcal{P}os(\mathsf{C}\lfloor X\theta \rfloor)$. Hence $\mathsf{C}\lfloor X\theta_{|p'} \rfloor = \mathsf{f}(\mathsf{C}\lfloor \xi_1 \rfloor, \ldots, \mathsf{C}\lfloor \xi_n \rfloor)$ and $\mathsf{C}\lfloor \zeta' \rfloor = \mathsf{f}(\mathsf{C}\lfloor \xi_1 \rfloor, \ldots, \mathsf{C}\lfloor \xi_{r-1} \rfloor, \mathsf{C}\lfloor \zeta \rfloor, \mathsf{C}\lfloor \xi_{r+1} \rfloor, \ldots, \mathsf{C}\lfloor \xi_n \rfloor)$. Thus we can apply the same reasoning as Case (a).

Case (c): $\mathsf{f} \in \mathcal{F}_d$, $r = 1$ *and* $|\mathsf{C}\lfloor X\theta_{|p'}[\zeta]_r \rfloor| > 1$. In such a case, we know that $\mathsf{C}\lfloor X\theta_{|p'}[\zeta]_r \rfloor = \mathsf{f}(\mathsf{C}\lfloor \zeta \rfloor, \mathsf{C}\lfloor \xi_2 \rfloor, \ldots, \mathsf{C}\lfloor \xi_n \rfloor)$ since $|\mathsf{C}\lfloor X\theta_{|p'}[\zeta]_r \rfloor| > 1$. Thus, similarly to Case (a), we can apply our inductive hypothesis.

Case (d): $\mathsf{f} \in \mathcal{F}_d$, $r = 1$ *and* $|\mathsf{C}\lfloor X\theta_{|p'}[\zeta]_r \rfloor| = 1$. In such a case, we have that there exists $(\gamma, \ell \rhd w) \in \Phi$ such that $\mathsf{path}(\gamma) = \mathsf{f} \cdot \mathsf{path}(\zeta)$. Since ζ conforms to $\Phi\theta$ w.r.t. NoUse, we can denote $\gamma\theta = \mathsf{f}(\zeta, \gamma_2\theta, \ldots, \gamma_n\theta)$. Since $\mathcal{C}$ is well-formed and $(\sigma, \theta) \in \mathsf{Sol}(\mathcal{C})$, we also know that $\gamma\theta(\Phi\sigma)\downarrow = w\sigma$ and $X\theta(\Phi\sigma\downarrow) \in \mathcal{T}(\mathcal{F}_c, \mathcal{N})$. Thus by Lemma 32, we can deduce that $X\theta_{|p'}(\Phi\sigma)\downarrow \in \mathcal{T}(\mathcal{F}_c, \mathcal{N})$. Therefore, since we have seen that $\zeta\Phi\sigma\downarrow = \xi_1\Phi\sigma\downarrow$, we can deduce that for all $i \in \{2, \ldots, n\}$, $\xi_i(\Phi\sigma)\downarrow = \gamma_i\theta(\Phi\sigma)\downarrow$. We now distinguish three cases:

- $\ell < s$: In such a case, let $\zeta' = \gamma\theta$. Since $(X, k \vdash^? v) \in D(M_{i,j})$, $k \geq s > \ell$ and $\mathcal{C}$ is well formed, we know that for all $Y \in vars^2(\gamma)$, $\mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(Y) < k = \mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(X)$. Hence by Lemma 39, $\neg(X <_\theta Y)$.

  At last, we know that $\mathsf{nb}_{\mathsf{occ}}(\mathsf{C}\lfloor \xi \rfloor, \mathsf{C}\lfloor X\theta[\zeta]_p \rfloor) < \mathsf{nb}_{\mathsf{occ}}(\mathsf{C}\lfloor \xi \rfloor, \mathsf{C}\lfloor X\theta \rfloor)$ hence we deduce that $\mathsf{C}\lfloor \xi \rfloor \in st(\mathsf{C}\lfloor X\theta_{|p'} \rfloor)$. Thus along with $|\mathsf{C}\lfloor \zeta' \rfloor| = 1$, $\mathsf{C}\lfloor \zeta' \rfloor \neq \mathsf{C}\lfloor \xi \rfloor$ (since $s \neq \ell$), we can deduce that $\#\{\mathsf{C}\lfloor \xi \rfloor \in st(\mathsf{C}\lfloor X\theta[\zeta']_{p'} \rfloor)\} < \#\{\mathsf{C}\lfloor \xi \rfloor \in st(\mathsf{C}\lfloor X\theta \rfloor)\}$. Hence, we can apply our inductive hypothesis on ζ', θ and p'.

- $\ell > s$: Such a case is impossible. Indeed, by Property $\mathsf{PP1Sa}(s)$, $\ell > s$ implies that $\gamma \in \mathcal{A}\mathcal{X}$ which is in contradiction with $\mathsf{path}(\gamma) = \mathsf{f} \cdot \mathsf{path}(\zeta)$.

- $\ell = s$: Thanks to $\mathcal{C}$ satisfying Property $\mathsf{PP1Sa}(s)$, we know that $\gamma_2, \ldots, \gamma_n \in \mathcal{X}^2$. We prove our result now by induction on $N = \#\{\gamma_i \mid X <_\theta \gamma_i, i \in \{2, \ldots, n\}\}$.

  Base case $N = 0$*:* Such a case is similar to the case $\ell < s$. Indeed, by hypothesis, we know that for all $Y \in vars^2(\gamma)$, $\neg(X <_\theta Y)$ (note that the first argument of γ can not be a variable). We can apply our inductive hypothesis on ζ', θ and p'.

  Inductive case $N > 0$. We know that there exists $i_0 \in \{2, \ldots, n\}$ such that $X <_\theta \gamma_{i_0}$. Since $\mathcal{C}$ is well-formed, we know that $\mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(\gamma_{i_0}) \leq \ell = s$. Moreover, by Lemma 39, $X <_\theta \gamma_{i_0}$ implies that $\mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(X) \leq \mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(\gamma_{i_0})$. Since

$\mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(X) = k$ and $k \geq s$, we can deduce that $k = s = \ell$ and so there exists v such that $(\gamma_{i_0}, s \vdash^? v) \in D$. Furthermore, we already know that $\xi_{i_0}(\Phi\sigma)\downarrow = \gamma_{i_0}\theta(\Phi\sigma)\downarrow$ and $\mathsf{C}\lfloor\xi_{i_0}\rfloor \in st(\mathsf{C}\lfloor X\theta\rfloor)$ thanks $p \in \mathcal{P}os(\mathsf{C}\lfloor X\theta\rfloor)$. Hence, for all $Y \in vars^2(\mathsf{C}\lfloor\xi_{i_0}\rfloor\delta^2(\mathcal{C}))$ we have that $Y <_\theta X$, and thus $Y <_\theta \gamma_{i_0}$ (and so $\neg(\gamma_{i_0} <_\theta Y)$). Thus, thanks to Lemma 40, we know that there exists θ' such that (σ, θ') is a pre-solution of $\mathcal{C}$, $\gamma_{i_0}\theta' = \xi_{i_0}$, $\theta' \vDash \mathsf{mgu}(E_\Pi)$ and for all $Y \in vars^2(D)\backslash\{\gamma_{i_0}\}$, $\mathsf{C}\lfloor Y\theta'\rfloor = \mathsf{C}\lfloor Y\theta\rfloor$.

Let $j \in \{2, \ldots, n\}$ such that $i_0 \neq j$. We show that if $X <_{\theta'} \gamma_j$ then $X <_\theta \gamma_j$: $X <_{\theta'} \gamma_j$ implies that there exists $Y_1, \ldots, Y_m$ such that $X <_{\theta'} Y_1 <_{\theta'} \ldots <_{\theta'} Y_m <_{\theta'} \gamma_j$. But we know that for all $Y \in vars^2(\mathcal{C})\backslash\{\gamma_{i_0}\}$, $\mathsf{C}\lfloor Y\theta'\rfloor = \mathsf{C}\lfloor Y\theta\rfloor$. Hence, if for all $q \in \{1, \ldots, m\}$, $Y_q \neq \gamma_{i_0}$, we trivially have that $X <_\theta \gamma_j$. If there exists $q \in \{1, \ldots, m\}$ such that $Y_q = \gamma_{i_0}$, it would imply that $X <_{\theta'} \gamma_{i_0}$. However $X <_{\theta'} \gamma_{i_0}$ is impossible. Indeed, assume that $X <_{\theta'} \gamma_{i_0}$. We have that $\mathsf{C}\lfloor X\theta\rfloor = \mathsf{C}\lfloor X\theta'\rfloor$ and we have seen that $\mathsf{C}\lfloor\zeta_{i_0}\rfloor \in st(\mathsf{C}\lfloor X\theta\rfloor)$. Hence, we have that $\mathsf{C}\lfloor\zeta_{i_0}\rfloor \in st(\mathsf{C}\lfloor X\theta'\rfloor)$, and thus for all $Y \in vars^2(\mathsf{C}\lfloor\xi_{i_0}\rfloor\delta^2(\mathcal{C}))$ we have that $Y <_{\theta'} X$. Since we have assumed that $X <_{\theta'} \gamma_{i_0}$, we have that either (a) $X \in vars^2(\mathsf{C}\lfloor\gamma_{i_0}\theta'\rfloor\delta^2(\mathcal{C}))$, or (b) there exists Z such that $X <_{\theta'} Z$ and $Z \in vars^2(\mathsf{C}\lfloor\gamma_{i_0}\theta'\rfloor\delta^2(\mathcal{C}))$. The case (a) is impossible since this would imply that $X <_{\theta'} X$. The case (b) is impossible too since it would imply that $Z <_{\theta'} X$, and thus $X <_{\theta'} X$. Hence we have that:

$$\{\gamma_i \mid X <_{\theta'} \gamma_i, i \in \{2, \ldots, n\}\} \subset \{\gamma_i \mid X <_\theta \gamma_i, i \in \{2, \ldots, n\}\}.$$

Note that $X <_\theta \gamma_{i_0}$ by hypothesis whereas we have seen that $\neg(X <_{\theta'} \gamma_{i_0})$.

At last, we know that $(\sigma, \theta) \in \mathsf{Sol}(\mathcal{C})$ and (σ, θ') is a pre-solution of $\mathcal{C}$. But thanks to $\mathcal{C}$ satisfying Property $\mathsf{PP1Sa}(s)$, we know that for all $Y, q \vdash^? v$, if $q \geq s$ then $Y \notin vars^2(E_\Pi)$. Hence, since $(\gamma_i, s \vdash^? v) \in D$, $\theta' \vDash \mathsf{mgu}(E_\Pi)$ and for all $Y \in vars^2(D)\backslash\{\gamma_i\}$, $\mathsf{C}\lfloor Y\theta'\rfloor = \mathsf{C}\lfloor Y\theta\rfloor$, we can conclude that $\theta' \vDash E_\Pi$ (we rely on the form of the inequations to conclude on this point). Moreover, since ND only depend on σ, we can conclude that $(\sigma, \theta') \in \mathsf{Sol}(\mathcal{C})$ which allows us to apply our inductive hypothesis on $\zeta' = \gamma\theta'$, θ' and p.

Proof of the lemma. Relying on Property 1 and Property 2, we are now able to conclude.

We have $\zeta \in \Pi_r$, $param(\zeta) \subseteq \{ax_1, \ldots, ax_{s-1}\}$, $\zeta\Phi\sigma\downarrow = u\sigma$ where $(\xi, s \rhd u) \in \Phi$ and $X\theta_{|p} = \xi\theta$ where $p \in \mathcal{P}os(\mathsf{C}\lfloor X\theta\rfloor)$. But since $\mathcal{C}$ is well formed and $(\sigma, \theta) \in \mathsf{Sol}(\mathcal{C})$, we know that $\xi\theta(\Phi\sigma)\downarrow = u\sigma = \zeta(\Phi\sigma)\downarrow$.

Hence by the first property, we can deduce that there exists $\zeta' \in st(\zeta)$, a position p' prefix of p such that $X\theta[\zeta]_p(\Phi\sigma)\downarrow = X\theta[\zeta']_{p'}(\Phi\sigma)\downarrow$ and $X\theta[\zeta']_{p'} \in \Pi_r$. But we already know that $X\theta[\zeta]_p(\Phi\sigma)\downarrow = X\theta(\Phi\sigma)\downarrow$ so $X\theta[\zeta']_{p'}(\Phi\sigma)\downarrow = X\theta(\Phi\sigma)\downarrow$. Furthermore $\zeta' \in st(\zeta)$, ζ conforms to $\Phi\theta$ w.r.t. NoUse thus we have that ζ' also conforms to $\Phi\theta$ w.r.t. NoUse. At last, $param(\zeta) \subseteq \{ax_1, \ldots, ax_{s-1}\}$ and $\zeta' \in st(\zeta)$ implies that $param(\zeta') \subseteq \{ax_1, \ldots, ax_{s-1}\}$.

Let $Y \in vars^2(\mathsf{C}\lfloor\zeta'\rfloor\delta^2(\mathcal{C}))$ and assume that $X <_\theta Y$. Thanks to Lemma 39, it implies that $\mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(X) \leq \mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(Y)$ and so $s \leq k \leq \mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(Y)$. Furthermore $Y \in vars^2(\mathsf{C}\lfloor\zeta'\rfloor\delta^2(\mathcal{C}))$ also implies that there exists $(\gamma, i \rhd u) \in \Phi$ such that $\gamma\theta \in st(\zeta')$ and $Y \in vars^2(\gamma)$. But thanks to $\mathcal{C}$ satisfying $\mathsf{InvGeneral}$, $ax_i \in st(\gamma\theta)$. Thus with $param(\zeta') \subseteq \{ax_1, \ldots, ax_{s-1}\}$, we deduce that $i \leq s-1$. On the other hand, $Y \in vars^2(\gamma)$

implies that $\mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(Y) \leq i$. Hence we deduce that $s \leq \mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(Y) \leq i \leq s-1$ which is a contradiction. Therefore, for all $Y \in vars^2(\mathsf{C}\lfloor\zeta'\rfloor\delta^2(\mathcal{C}))$, $\neg(X <_\theta Y)$.

At last, since $param(\zeta') \subseteq \{ax_1, \ldots, ax_{s-1}\}$ and $ax_s \in st(\xi\theta)$ by the invariant InvGeneral, we can deduce $\xi\theta \notin st(\zeta')$, and thus $\mathsf{C}\lfloor\xi\rfloor \notin st(\mathsf{C}\lfloor\zeta'\rfloor)$. Furthermore, by hypothesis, for all $(\xi', i \rhd v) \in \Phi$, for all $\mathsf{g} \in \mathcal{F}_d$, we have that $\mathsf{path}(\xi') \neq \mathsf{g} \cdot \mathsf{path}(\xi)$. Since $\xi\theta = X\theta_{|p}$ and p' is a prefix of p, then $\mathsf{C}\lfloor\xi\theta\rfloor = (\mathsf{C}\lfloor X\theta\rfloor)_{|p}$ and we can conclude that $\mathsf{nb}_{\mathsf{occ}}(\mathsf{C}\lfloor\xi\rfloor, \{\mathsf{C}\lfloor X\theta[\zeta]_p\rfloor\}) < \mathsf{nb}_{\mathsf{occ}}(\mathsf{C}\lfloor\xi\rfloor, \{\mathsf{C}\lfloor X\theta\rfloor\})$.

We can now apply the second property which means that there exists θ' such that $(\sigma, \theta') \in \mathsf{Sol}(\mathcal{C})$ and

$$\mathsf{nb}_{\mathsf{occ}}(\mathsf{C}\lfloor\xi\rfloor, \{\mathsf{C}\lfloor Y\theta'\rfloor \mid Y \in vars^2(\mathcal{C})\}) < \mathsf{nb}_{\mathsf{occ}}(\mathsf{C}\lfloor\xi\rfloor, \{\mathsf{C}\lfloor Y\theta\rfloor \mid Y \in vars^2(\mathcal{C})\})$$

Once again, since for all $(\xi', i \rhd v) \in \Phi$, for all $\mathsf{g} \in \mathcal{F}_d$, we have that $\mathsf{path}(\xi') \neq \mathsf{g} \cdot \mathsf{path}(\xi)$ and for all $Y \in vars^2(\mathcal{C})$, $Y\theta'$ conforms to $\Phi\theta'$ w.r.t. NoUse, then we can deduce that:

$$\mathsf{nb}_{\mathsf{occ}}(\xi\theta', \{Y\theta' \mid Y \in vars^2(\mathcal{C})\}) < \mathsf{nb}_{\mathsf{occ}}(\xi\theta, \{Y\theta \mid Y \in vars^2(\mathcal{C})\}).$$

□

Appendix D.4. Soundness

The purpose of this section is to prove the soundness of our procedure, included Step e of Phase 1. We also establish the soundness of our normalisation step.

Lemma 42 (soundness)**.** *Let $\mathcal{C}$ be a normalised constraint system obtained by following the strategy and* Rule$(\tilde{p})$ *be a transformation rule applicable on $\mathcal{C}$. Let $\mathcal{C}_1$ and $\mathcal{C}_2$ be the two resulting constraint systems obtained by applying* Rule$(\tilde{p})$ *on $\mathcal{C}$. We denote by Φ, Φ_1 and Φ_2 the respective frames of $\mathcal{C}$, $\mathcal{C}_1$ and $\mathcal{C}_2$ and we denote by S_1 the set of free variables of $\mathcal{C}$.*

Let $(\sigma, \theta) \in \mathsf{Sol}(\mathcal{C})$. There exist σ', θ', and $i_0 \in \{1, 2\}$ such that $(\sigma', \theta') \in \mathsf{Sol}(\mathcal{C}_{i_0})$, $\sigma = \sigma'|_{vars^1(\mathcal{C})}$ and $\mathsf{Init}(\Phi)\sigma = \mathsf{Init}(\Phi_{i_0})\sigma'$.

Proof. We distinguish two cases:

- An application of a rule during Phase 1, Step a. Note that in such a case, only the rules Dest and Eq-frame-ded are applicable.
- An application of a rule during 1.b, 1.c, 1.d or Phase 2. Note that in such a case, only the rules Cons, Axiom, Eq-frame-frame, Eq-ded-ded and Ded-st are applicable.

An application during Phase 1.a. In such a phase, only the rules Dest and Eq-frame-ded are applicable. Assume that we are on the cycle with parameter for support equal to s. We prove the result by case analysis on the rules.

Rule Dest$(\xi, l \to r, s)$: Let $\mathsf{g}(u_1, \ldots, u_n) \to u$ be a fresh variant of $l \to r$ and $\tilde{x}$ be the variables that occur in this variant. Note that $\mathsf{g} \in \mathcal{F}_d$. Let $(\sigma, \theta) \in \mathsf{Sol}(\mathcal{C})$. We distinguish two cases.

Case 1: there exist ground recipes $\xi_2, \ldots, \xi_n$ in Π_r such that $\mathsf{g}(\xi\theta, \xi_2, \ldots, \xi_n)\Phi\sigma\downarrow \in \mathcal{T}(\mathcal{F}_c, \mathcal{N})$ and $param(\{\xi_2, \ldots, \xi_n\}) \subseteq \{ax_1, \ldots, ax_s\}$. To be more specific, since the

rule $\textsc{Dest}(\xi, \ell \to r, s)$ is applicable and the constraint system was obtained by following the strategy, we deduce that $ax_s \in \mathit{param}(\{\xi_2, \ldots, \xi_n\})$ (else σ would not satisfy *ND*).

First, w.l.o.g., we can assume that for any strict subterm ξ'_k of ξ_k with $k \in \{2, \ldots, n\}$, we have that $\xi'_k(\Phi\sigma) \neq \xi_k(\Phi\sigma)$ (otherwise, we can simply choose ξ'_k instead of ξ_k). Moreover, by Lemma 35, we can also assume that $\xi_2, \ldots, \xi_n$ conform to the frame $\Phi\theta$. Let $\tau = \mathsf{mgu}(\{(\xi\theta)\phi\sigma\downarrow = u_1,\ \xi_2(\phi\sigma)\downarrow = u_2,\ \ldots,\ \xi_n(\phi\sigma)\downarrow = u_n\})$, and $\sigma_1 = \sigma \cup \tau$.

Our goal is to build a substitution θ' such that for all $X \in \mathit{vars}^2(\mathcal{C}_1)$, $X\theta'$ conforms to the frame $\Phi_1\theta'$ (where Φ_1 is the frame associated to $\mathcal{C}_1$). In particular, we have to ensure that there is a unique "key" that is used to decrypt $\xi\theta'$. Actually, we show how to build θ' in order to ensure that $X\theta'$ conforms to $\Phi_1\theta'$ for every $X \in \{Y \mid Y, j \vdash^? r \text{ in } \mathcal{C}_1\}$, we conclude for the remaining variables.

Let $S = \{Y \mid \{Y, j \vdash^? r\} \in \mathcal{C} \text{ and } \mathsf{g}(\xi\theta, \zeta_2, \ldots, \zeta_n) \in \mathit{st}(Y\theta) \text{ for some } \zeta_2, \ldots, \zeta_n\}$. Notice that for all $Y \in S$, $s \leq \mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(Y)$ else σ would not satisfy *ND*. We distinguish two cases:

Case a: $S = \emptyset$. Let θ' be a substitution defined as follows:

- $X_i\theta' = \xi_i$ for $i = 2 \ldots n$, and
- $X\theta' = X\theta$ otherwise.

In such a case, it is relatively easy to conclude that $(\sigma_1, \theta') \in \mathsf{Sol}(\mathcal{C}_1)$. In particular, we have that $X\theta'$ conforms to $\Phi_1\theta'$ for all variable X. First $\Phi_1 = \Phi \cup \{\mathsf{g}(\xi, X_2, \ldots, X_n), i \rhd w\}$. For every variable $X \notin \{X_2, \ldots, X_n\}$, we have $X\theta' = X\theta$, which means that $\Phi\theta = \Phi\theta'$. Since $S = \emptyset$, we easily conclude that $Y\theta'$ conforms to $\Phi_1\theta'$ for all variables in $\{Y \mid Y, j \vdash^? r \in D(\mathcal{C}_1)\} \setminus \{X_2, \ldots, X_n\}$. Furthermore, since ξ_i conforms to $\Phi\theta'$ and by the choice of ξ_i, we deduce that ξ_i conforms to $\Phi_1\theta'$. At last, also by the choice of ξ_i, we also deduce that $(X_i\theta')\Phi_1\sigma_1\downarrow = u_i\sigma_1$ which allows us to conclude.

Case b: $S \neq \emptyset$. Otherwise, we chose Y_0 a minimal variable w.r.t. the relation $<_\theta$ and the maximal parameter. Such minimal exists since by Lemma 38, the relation $<_\theta$ is a strict partial order. We have that $\mathsf{g}(\xi, \zeta_2, \ldots, \zeta_n) \in \mathit{st}(Y_0\theta)$ for some recipe $\zeta_2, \ldots, \zeta_n$.

If $\mathit{param}(\{\zeta_2, \ldots, \zeta_n\}) \not\subseteq \{ax_1, \ldots, ax_s\}$ then for each $i \in \{2, \ldots, n\}$, we denote by $\zeta_i^0 = \xi_i$, else for each $i \in \{2, \ldots, n\}$, we denote by ζ_i^0 a minimal (for the size) subterm of ζ_i such that $\zeta_i(\Phi\sigma)\downarrow = \zeta_i^0(\Phi\sigma)\downarrow$.

Note that in both cases, for all $i \in \{2, \ldots, n\}$, $\zeta_i(\Phi\sigma)\downarrow = \zeta_i^0(\Phi\sigma)\downarrow$. Indeed, we know that $\mathsf{g}(\xi\theta, \zeta_2, \ldots, \zeta_n) \in \mathit{st}(Y\theta)$, $\mathsf{g}(\xi\theta, \zeta_2, \ldots, \zeta_n) \in \Pi_r$ and $Y\theta(\Phi\sigma)\downarrow \in \mathcal{T}(\mathcal{F}_c, \mathcal{N})$. Hence by Lemma 32, $\mathsf{g}(\xi, \zeta_2, \ldots, \zeta_n)(\Phi\sigma)\downarrow \in \mathcal{T}(\mathcal{F}_c, \mathcal{N})$. Furthermore, we know that $\mathsf{g}(\xi\theta, \xi_2, \ldots, \xi_n)\Phi\sigma\downarrow \in \mathcal{T}(\mathcal{F}_c, \mathcal{N})$. Hence since $\mathsf{path}(\mathsf{g}(\xi\theta, \zeta_2, \ldots, \zeta_n)) = \mathsf{path}(\mathsf{g}(\xi\theta, \xi_2, \ldots, \xi_n))$, then by Lemma 33, $\zeta_i(\Phi\sigma)\downarrow = \xi_i(\Phi\sigma)\downarrow$, for all $i \in \{2, \ldots, n\}$.

We rely on Lemma 40 to build a substitution θ' that will be conformed to the frame $\Phi_1\theta'$. To achieve this, the idea is to replace any occurrence of $\mathsf{g}(\xi, \ldots)$ that occur in $Y\theta$ with $Y \in S$ by $\mathsf{g}(\xi, \zeta_2^0, \ldots, \zeta_n^0)$. We prove our result by induction on:

$$m = \mathsf{nb}_{\mathsf{occ}}(\mathsf{g}(\xi\theta, \__2, \ldots, \__n), \{Y\theta \mid Y \in S\}) - \mathsf{nb}_{\mathsf{occ}}(\mathsf{g}(\xi\theta, \zeta_2^0, \ldots, \zeta_n^0), \{Y\theta \mid Y \in S\})$$

where $\__i$ is used to represent any value.

Base case $m = 0$*:* Let θ' be the substitution defined as follows:

- $X_i\theta' = \zeta_i^0$ for $i = 2, \ldots, n$, and

- $X\theta' = X\theta$ otherwise.

We conclude as in the previous case ($S = \emptyset$).

Inductive case $m > 0$: Let $Y \in S$ such that there exists $p \in \mathcal{P}os(\mathsf{C}\lfloor Y\theta \rfloor)$ such that $\mathsf{path}(Y\theta_{|p}) = \mathsf{g} \cdot \mathsf{path}(\xi)$ and $Y\theta_{|p} \neq \mathsf{g}(\xi\theta, \zeta_2^0, \ldots, \zeta_n^0)$. We first show that such Y and p exists. We know that there is no frame element in Φ whose recipe has a path equal to $\mathsf{g} \cdot \mathsf{path}(\xi)$. Furthermore, thanks to $\mathcal{C}$ being well-formed (Definition 18, item 9), we deduce that no subterm of a recipe of a frame element in Φ has a path equal to $\mathsf{g} \cdot \mathsf{path}(\xi)$. Hence, we choosing Y minimal w.r.t. $<_\theta$ such that $\mathsf{g}(\xi\theta, \gamma_2, \ldots, \gamma_n) \in st(Y\theta)$ for some $\gamma_2 \ldots, \gamma_n$ and $\mathsf{g}(\xi\theta, \gamma_2, \ldots, \gamma_n) \neq \mathsf{g}(\xi\theta, \zeta_2^0, \ldots, \zeta_n^0)$, we can conclude that there exists $p \in \mathcal{P}os(\mathsf{C}\lfloor Y\theta \rfloor)$ such that $\mathsf{path}(Y\theta_{|p}) = \mathsf{g} \cdot \mathsf{path}(\xi)$ and $Y\theta_{|p} \neq \mathsf{g}(\xi\theta, \zeta_2^0, \ldots, \zeta_n^0)$ (otherwise Y would not be minimal w.r.t. $<_\theta$).

Let $\zeta^0 \stackrel{\mathsf{def}}{=} \mathsf{g}(\xi\theta, \zeta_2^0, \ldots, \zeta_n^0)$.

- Since ζ^0 is a subterm of $Y_0\theta$, we know that ζ^0 conforms to $\Phi\theta$. Furthermore, by definition of each ζ_i^0, $i \in \{1, \ldots, n\}$, we know that $param(\zeta^0) \subseteq \{ax_1, \ldots, ax_s\}$. Moreover, $(\sigma, \theta) \in \mathsf{Sol}(\mathcal{C})$ implies $param(Y_0\theta) \subseteq \{ax_1, \ldots, ax_j\}$ hence ζ^0 subterm of $Y_0\theta$ implies that $param(\zeta^0)\{ax_1, \ldots, ax_s\} \subseteq \{ax_1, \ldots, ax_j\}$.

- Since $Y\theta_{|p}$ conforms with $\Phi\theta$ and $\mathsf{path}(Y\theta_{|p}) = g \cdot \mathsf{path}(\xi)$, there exists $\xi_2, \ldots, \xi_n$ such that $Y\theta = \mathsf{g}(\xi\theta, \xi_2, \ldots, \xi_n)$. Furthermore ξ is a recipe of a frame element in Φ, and there is no frame element in Φ having $\mathsf{g} \cdot \mathsf{path}(\xi)$ as a path. Hence, we have that $\mathsf{C}\lfloor Y\theta_{|p} \rfloor_{\Phi\theta} = \mathsf{g}(\mathsf{path}(\xi), \mathsf{C}\lfloor \xi_2 \rfloor_{\Phi\theta}, \ldots, \mathsf{C}\lfloor \xi_n \rfloor_{\Phi\theta})$ and $\mathsf{C}\lfloor \zeta^0 \rfloor_{\Phi\theta} = \mathsf{g}(\mathsf{path}(\xi), \mathsf{C}\lfloor \zeta_2^0 \rfloor_{\Phi\theta}, \ldots, \mathsf{C}\lfloor \zeta_n^0 \rfloor_{\Phi\theta})$. Thus, we deduce that $\mathsf{C}\lfloor Y\theta[\zeta^0]_p \rfloor = \mathsf{C}\lfloor Y\theta \rfloor [\mathsf{C}\lfloor \zeta^0 \rfloor]_p$. We have that $(\sigma, \theta) \in \mathsf{Sol}(\mathcal{C})$, thus $(Y\theta)(\Phi\sigma)\downarrow \in \mathcal{T}(\mathcal{F}_c, \mathcal{N})$ and $(Y_0\theta)(\Phi\sigma)\downarrow \in \mathcal{T}(\mathcal{F}_c, \mathcal{N})$. Thanks to Lemma 32, $(Y\theta|_p)(\Phi\sigma)\downarrow \in \mathcal{T}(\mathcal{F}_c, \mathcal{N})$ and $\zeta^0(\Phi\sigma)\downarrow \in \mathcal{T}(\mathcal{F}_c, \mathcal{N})$. Since $\mathsf{path}(Y\theta|_p) = \mathsf{path}(\zeta^0)$, by Lemma 33, we conclude that$(Y\theta|_p)(\Phi\sigma)\downarrow = \zeta^0(\Phi\sigma)\downarrow$.

- Lastly, by definition of $\zeta_2^0, \ldots, \zeta_n^0$, either (a) $\zeta_i^0 = \zeta_i$, for $i \in \{2, \ldots, n\}$ and ζ_i^0 are subterms of $Y_0\theta$; or (b) $param(\mathsf{g}(\xi\theta, \zeta_2, \ldots, \zeta_n)) \not\subseteq \{ax_1, \ldots, ax_s\}$ and $\zeta_i^0 = \xi_i$, for $i \in \{2, \ldots, n\}$.

  In case (a), since $Y, Y_0 \in S$ and Y_0 is a minimal variable w.r.t. $<_\theta$ then we deduce that for all $Z \in vars^2(\mathsf{C}\lfloor \zeta^0 \rfloor_\Phi \delta^2(\mathcal{C}))$, $\neg(Y <_\theta Z)$. In case (b), we know that Y_0 is also minimal w.r.t. the maximal parameter. Hence $\mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(Y_0) \leq \mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(Y)$. But $param(\mathsf{g}(\xi\theta, \zeta_2, \ldots, \zeta_n)) \not\subseteq \{ax_1, \ldots, ax_s\}$ and $(\sigma, \theta) \in \mathsf{Sol}(\mathcal{C})$ implies that $\mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(Y_0) > s$ and so $\mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(Y) > s$. Since $param(\mathsf{g}(\xi\theta, \xi_2, \ldots, \xi_n)) \subseteq \{ax_1, \ldots, ax_s\}$, $\mathcal{C}$ satisfies $\mathsf{InvUntouched}(s)$, $\mathcal{C}$ is a well-formed constraint system (item 3) and by Lemma 39, then we deduce that for all $Z \in vars^2(\mathsf{C}\lfloor \zeta^0 \rfloor_\Phi \delta^2(\mathcal{C}))$, $\neg(Y <_\theta Z)$.

We satisfy all the conditions required to apply Lemma 40, Hence, there exists θ' such that (σ, θ') is a pre-solution of $\mathcal{C}$ with $Y\theta' = Y\theta[\zeta^0]_p$ and for all $Z \in vars^2(\mathcal{C}) \setminus \{Y\}$, we have that $\mathsf{C}\lfloor Z\theta \rfloor_{\Phi\theta} = \mathsf{C}\lfloor Z\theta' \rfloor_{\Phi\theta'}$,

Hence, we have that the measure m strictly decreases. Furthermore, since $(\sigma, \theta) \in \mathsf{Sol}(\mathcal{C})$ and using the fact that (σ, θ') is a pre-solution of $\mathcal{C}$, it only remains to prove that $\theta' \models E_\Pi$ in order to conclude that $(\sigma, \theta') \in \mathsf{Sol}(\mathcal{C})$. Actually, we know that $\theta' \vDash \mathsf{mgu}(E_\Pi)$ and thanks to $\mathcal{C}$ satisfying $\mathsf{PP1Sa}(s)$ (item 4), we have trivially have that $\theta' \vDash E_\Pi$ and so $(\sigma, \theta') \in \mathsf{Sol}(\mathcal{C})$. Then, we conclude by relying on our induction hypothesis.

Case 2: for all ground recipes $\xi_2, \ldots, \xi_n$ in Π_r, either $param(\{\xi_2, \ldots, \xi_n\}) \not\subseteq \{ax_1, \ldots, ax_s\}$ or we have that $\mathsf{g}(\xi\theta, \xi_2 \ldots, \xi_n)\Phi\sigma\downarrow \notin \mathcal{T}(\mathcal{F}_c, \mathcal{N})$. Since $\mathsf{g} \in \mathcal{F}_d$, $\mathsf{g}(\xi\theta, \xi_2 \ldots, \xi_n)\Phi\sigma\downarrow \in \mathcal{T}(\mathcal{F}_c, \mathcal{N})$ means that there exists a substitution τ which maps variable in $\tilde{x}$ to ground constructor terms such that

$$\mathsf{g}(u_1\tau, \ldots, u_n\tau) = \mathsf{g}(\xi\theta(\Phi\sigma)\downarrow, \xi_2(\Phi\sigma)\downarrow, \ldots, \xi_n(\Phi\sigma)\downarrow).$$

This means that $u_1\tau = \xi\theta(\Phi\sigma)\downarrow$, $u_2\tau = \xi_2(\Phi\sigma)\downarrow$, ..., and $u_n\tau = \xi_n(\Phi\sigma)\downarrow$. Moreover, since $(\sigma, \theta) \in \mathsf{Sol}(\mathcal{C})$, we have that $(\xi\theta)(\Phi\sigma)\downarrow = v\sigma$. Therefore, we have that:

$$\sigma \models \forall \tilde{x} \cdot [v \neq u_1 \vee s \not\vdash^? u_2 \vee \ldots \vee s \not\vdash^? u_n]$$

This allows us to conclude that $(\sigma, \theta) \in \mathsf{Sol}(\mathcal{C}_2)$.

Rule Eq-frame-ded(X, ξ): By hypothesis we know that there exists u, v and k such that $(X, k \vdash^? u) \in D(\mathcal{C})$, $(\xi, s \rhd v) \in \Phi(\mathcal{C})$ and $k < s$. Furthermore, according to the strategy, we know that the rule Eq-frame-ded is prioritised over the rule Dest, and that the rule Eq-frame-ded is strongly applicable on at least on constraint system on the row of the matrix of constraint system. Assume that $\mathcal{C}'$ is such constraint system. By hypothesis, $\mathcal{C}'$ is normalised. It would imply that there exists $x \in \mathcal{X}^1$ such that $(X, k \vdash^? x) \in D(\mathcal{C}')$ and $(\xi, s \rhd x) \in \Phi(\mathcal{C}')$. Assume now that there exists $(\xi', \ell \rhd w) \in \Phi(\mathcal{C}')$ and $\mathsf{g} \in \mathcal{F}_d$ such that $\mathsf{path}(\xi') = \mathsf{g} \cdot \mathsf{path}(\xi)$, hence it means that an instance of the rule Dest was previously applied on $(\xi, s \rhd x)$. But according to the definition of our rewrite rules and since $\mathcal{C}'$ is normalised, it would imply that x is instantiated by a term different from a variable and so $x \notin \mathcal{X}^1$ which is a contraction. Hence, for all $(\xi', \ell \rhd w) \in \Phi(\mathcal{C}')$, for all $\mathsf{g} \in \mathcal{F}_d$, $\mathsf{path}(\xi') \neq \mathsf{g} \cdot \mathsf{path}(\xi)$. But by Lemma 1 and since $\mathcal{C}$ and $\mathcal{C}'$ are on the same row of $\mathcal{M}$, we can deduce that $\mathcal{C}'$ and $\mathcal{C}$ have the same structure and so for all $(\xi', \ell \rhd w) \in \Phi(\mathcal{C})$, for all $\mathsf{g} \in \mathcal{F}_d$, $\mathsf{path}(\xi') \neq \mathsf{g} \cdot \mathsf{path}(\xi)$.

Let $(\sigma, \theta) \in \mathsf{Sol}(\mathcal{C})$. We distinguish two cases:

1. $u\sigma\downarrow = v\sigma\downarrow$. In such a case, we need to transform θ such that the frame element $(\xi, s \rhd v)$ will not be used anymore. Let denote $Nb(\theta) = \mathsf{nb}_{\mathsf{occ}}(\xi\theta, \{Y\theta \mid Y \in vars^2(\mathcal{C})\})$. We show that there exists θ' such that $(\sigma, \theta') \in \mathsf{Sol}(\mathcal{C}_1)$. We prove this result by induction on $Nb(\theta)$.

   Base case $Nb(\theta) = 0$: We know that $\mathcal{C}_1$ is $\mathcal{C}$ where $\mathsf{NoUse}(\mathcal{C}_1) = \mathsf{NoUse}(\mathcal{C}) \cup (\xi, s \rhd v)$ and $E(\mathcal{C}_1) = E(\mathcal{C}) \wedge u =^? v$. By hypothesis, we already know that $u\sigma\downarrow = v\sigma\downarrow$, hence $\sigma \vDash E(\mathcal{C}_1)$. Hence it remains to prove that for all $Y \in vars^2(\mathcal{C})$, $Y\theta$ conforms to $\Phi\theta$ w.r.t. $\mathsf{NoUse}(\mathcal{C}_1)$. But we already know thanks to $(\sigma, \theta) \in \mathsf{Sol}(\mathcal{C})$ that $Y\theta$ conforms to $\Phi\theta$ w.r.t. $\mathsf{NoUse}(\mathcal{C})$. And since $Nb(\theta) = 0$, we can conclude that $Y\theta$ conforms to $\Phi\theta$ w.r.t. $\mathsf{NoUse}(\mathcal{C}_1)$ and so $(\sigma, \theta) \in \mathsf{Sol}(\mathcal{C}_1)$.

   Inductive step $Nb(\theta) > 0$: Since $(\sigma, \theta) \in \mathsf{Sol}(\mathcal{C})$ and $u\sigma\downarrow = v\sigma\downarrow$, we have that $X\theta(\Phi\sigma)\downarrow = \xi\theta(\Phi\sigma)\downarrow$ and $param(X\theta) \subseteq \{ax_1, \ldots, ax_k\}$ with $k < s$. Moreover, we proved that for all $(\xi', \ell \rhd w) \in \Phi(\mathcal{C})$, for all $\mathsf{g} \in \mathcal{F}_d$, $\mathsf{path}(\xi') \neq \mathsf{g} \cdot \mathsf{path}(\xi)$. At last, since the rule Dest and Eq-frame-ded does not add equations in E_Π and Step a is the first step applied during Phase 1 with parameter s, we deduce that $\xi \notin st(\mathsf{mgu}(E_\Pi))$. Hence by Lemma 41, we can deduce that there exists θ' such that $(\sigma, \theta') \in \mathsf{Sol}(\mathcal{C})$ and $Nb(\theta') < Nb(\theta)$. Since $(\sigma, \theta') \in \mathsf{Sol}(\mathcal{C})$ and $u\sigma\downarrow = v\sigma\downarrow$, we

have still have that $X\theta'(\Phi\sigma)\downarrow) = \xi\theta'(\Phi\sigma)\downarrow$. Hence, by our inductive hypothesis on θ', we can deduce that there exists θ'' such that $(\sigma, \theta'') \in \mathsf{Sol}(\mathcal{C}_1)$.

2. $u\sigma\downarrow \neq v\sigma\downarrow$. In such a case, it is easy to see that $(\sigma, \theta) \in \mathsf{Sol}(\mathcal{C}_2)$.

An application during Phase 1.*b,* 1.*c,* 1.*d or* 2. We do a case analysis on the rule applied.
Rule $\textsc{Cons}(X, \mathsf{f})$: Let $(\sigma, \theta) \in \mathsf{Sol}(\mathcal{C})$. We distinguish two cases:

1. $\mathsf{root}(X\theta) = \mathsf{f}$. In such a case, there exists $\xi_1, \ldots, \xi_n \in \Pi_r$ such that $X\theta = \mathsf{f}(\xi_1, \ldots, \xi_n)$. Since $(\sigma, \theta) \in \mathsf{Sol}(\mathcal{C})$ and $\mathsf{f} \in \mathcal{F}_c$, we deduce that $\mathit{param}(X\theta) \subseteq \{ax_1, \ldots, ax_i\}$, and

$$(X\theta)(\Phi\sigma)\downarrow = \mathsf{f}(\xi_1(\Phi\sigma)\downarrow, \ldots, \xi_n(\Phi\sigma)\downarrow) = \mathsf{f}(t_1, \ldots, t_n) = t\sigma\downarrow$$

for some terms $t_1, \ldots, t_n$.

Let $\theta' = \theta \cup \{X_1 \mapsto \xi_1, \ldots, X_n \mapsto \xi_n\}$ and $\sigma' = \sigma \cup \{x_1 \mapsto t_1, \ldots, x_n \mapsto t_n\}$. Since $\Phi(\mathcal{C}_1) = \Phi(\mathcal{C})$, we trivially have that $\Phi\sigma = \Phi\sigma'$ and thus for every $i \in \{1, \ldots, n\}$, we have that $(X_i\theta')(\Phi\sigma')\downarrow = t_i\downarrow$ and $\mathit{param}(X_i\theta') \subseteq \mathit{param}(X\theta) \subseteq \{ax_1, \ldots, ax_i\}$. Furthermore, $t\sigma' = \mathsf{f}(t_1, \ldots, t_n)$ and $x_i\sigma' = t_i$, for all $i \in \{1, \ldots, n\}$ implies that $t\sigma'\downarrow = \mathsf{f}(x_1, \ldots, x_n)\sigma'\downarrow$. At last, by definition of θ', we also have that $X\theta' = \mathsf{f}(X_1, \ldots, X_n)\theta'$. This allows us to conclude that $(\sigma', \theta') \in \mathsf{Sol}(\mathcal{C}_1)$.

2. $\mathsf{root}(X\theta) \neq \mathsf{f}$. In such a case, we have that $\theta \models E_\Pi \wedge \mathsf{root}(X) \neq \mathsf{f}$ and so we can conclude that $(\sigma, \theta) \in \mathsf{Sol}(\mathcal{C}_2)$.

Rule $\textsc{Axiom}(X, \mathsf{path})$. Let $(\sigma, \theta) \in \mathsf{Sol}(\mathcal{C})$. We distinguish two cases:

1. $\mathsf{path}(X\theta) = \mathsf{path}$. In such a case, by definition of $(\sigma, \theta) \in \mathsf{Sol}(\mathcal{C})$, we have that $X\theta$ conforms to $\Phi\theta$ w.r.t. NoUse, and thus $X\theta = \xi\theta$. We have also that $(X\theta)(\Phi\sigma)\downarrow = u\sigma\downarrow$. Lastly, since $\mathcal{C}$ is well-formed, we know that $(\xi\theta)(\Phi\sigma)\downarrow = v\sigma\downarrow$. Altogether, this allows us to deduce that $u\sigma\downarrow = v\sigma\downarrow$. We conclude that $(\sigma, \theta) \in \mathsf{Sol}(\mathcal{C}_1)$.

2. $\mathsf{path}(X\theta) \neq \mathsf{path}$. Since $\mathsf{path}(\xi) = \mathsf{path}$, $\mathsf{path}(X\theta) \neq \mathsf{path}$ implies that $X\theta \neq \xi$. Thus, $\theta \models E_\Pi \wedge X \neq \xi$. We can conclude that $(\sigma, \theta) \in \mathsf{Sol}(\mathcal{C}_2)$.

Rule $\textsc{Eq-frame-frame}(\xi_1, \xi_2)$. Let $(\sigma, \theta) \in \mathsf{Sol}(\mathcal{C})$. We distinguish two cases:

1. $u_1\sigma\downarrow = u_2\sigma\downarrow$. In such a case, it is easy to see that $(\sigma, \theta) \in \mathsf{Sol}(\mathcal{C}_1)$.

2. $u_1\sigma\downarrow \neq u_2\sigma\downarrow$. In such a case, it is easy to see that $(\sigma, \theta) \in \mathsf{Sol}(\mathcal{C}_2)$.

Thus, in both cases, we easily conclude.

Rule $\textsc{Eq-ded-ded}(X, \xi)$. Let $(\sigma, \theta) \in \mathsf{Sol}(\mathcal{C})$. We distinguish two cases:

1. $u\sigma\downarrow = v\sigma\downarrow$. In such a case, since $(\sigma, \theta) \in \mathsf{Sol}(\mathcal{C})$, then for all $Y \in \mathit{vars}^2(\xi)$, we have that $Y\theta$ conforms to the frame $\Phi\theta$ w.r.t. NoUse. But the conditions of the rule Eq-ded-ded tell us that $\xi \in \mathcal{T}(\mathcal{F}_c, \mathit{vars}^2(\alpha))$ where $\alpha = \{Y \to w \mid (Y, j \vdash^? w) \in D(\mathcal{C}) \wedge j \leq i \wedge Y \in S_2(\mathcal{C})\}$ which means that $\mathsf{C}\lfloor\xi\theta\rfloor_{\Phi\theta} = \xi\{Y \to \mathsf{C}\lfloor Y\theta\rfloor_{\Phi\theta} \mid Y \in \mathit{vars}^2(\xi)\}$. Thus, we deduce that $\xi\theta$ conforms to $\Phi\theta$ too.

Moreover, the conditions of the rule Eq-ded-ded also tell us that $v = \xi\alpha$. By $(\sigma, \theta) \in \mathsf{Sol}(\mathcal{C})$, we deduce that for all $Y \in vars^2(\xi)$, $(Y\theta)\Phi\sigma\downarrow = (Y\alpha)\sigma\downarrow$. Once again, since $\xi \in \mathcal{T}(\mathcal{F}_c, \mathrm{dom}(\alpha))$, we have that $(\xi\theta)\Phi\sigma\downarrow = v\sigma = u\sigma = (X\theta)\Phi\sigma\downarrow$.

We want to conclude the result by applying Lemma 40. But in order to do that, we need to prove that for all $Y \in vars^2(\mathsf{C}\lfloor\xi\theta\rfloor_\Phi\delta^2(\mathcal{C}))$, $\neg(X <_\theta Y)$. We prove this property by case analysis on ξ:

Case $\xi \in vars^2(D)$*:* In such a case, we denote ξ by Z and so there exists $(Z, j \vdash^? v) \in D$. For all $Y \in vars^2(\mathsf{C}\lfloor\xi\theta\rfloor_\Phi\delta^2(\mathcal{C}))$, we have that $Y <_\theta Z$ by definition of $<_\theta$. Hence, if $\neg(X <_\theta Z)$ then for all $Y \in vars^2(\mathsf{C}\lfloor\xi\theta\rfloor_\Phi\delta^2(\mathcal{C}))$, $\neg(X <_\theta Y$. We apply Lemma 40 on the deducibility constraint $X, i \vdash^? u$ with the recipe $Z\theta$; otherwise we have $X <_\theta Z$ and so since $<_\theta$ is a strict partial order by Lemma 38, we deduce that $\neg(Z <_\theta X)$. Thus, we apply Lemma 40 on the deducible constraint $Z, j \vdash^? v$ with the recipe $X\theta$. Therefore, in both case, we know that there exists θ' such that (σ, θ') is a pre-solution of $\mathcal{C}$ with $X\theta' = Z\theta'$, $\theta' \vDash \mathsf{mgu}(E_\Pi)$ and for all $Y \in vars^2(D)\backslash\{X, Z\}$, we have $\mathsf{C}\lfloor Y\theta\rfloor_{\Phi\theta} = \mathsf{C}\lfloor Y\theta'\rfloor_{\Phi\theta'}$. At last, by the condition of Eq-ded-ded, we know that $\mathsf{root}(X) \neq^? \mathsf{f} \in E_\Pi$ is equivalent to $\mathsf{root}(Z) \neq^? \mathsf{f} \in E_\Pi$, thus (relying on the form of the inequations in E_Π) we can deduce that $\theta' \vDash E_\Pi$ and so $(\sigma, \theta') \in \mathsf{Sol}(\mathcal{C}_1)$.

Case $\xi \notin vars^2(D)$*:* As explained in the strategy (Section 4), the rule Eq-ded-ded with such parameter is only applied when the strategy is on the second phase. But, in such a case, since $\mathcal{C}$ satisfies the invariant $\mathsf{InvVarFrame}(\infty)$, we have that $(\star)$:

$$\text{for all } (\zeta, k \rhd u) \in \Phi, \text{ for all } Z \in vars^2(\zeta), \text{ there exists } j < k \text{ and } z \in \mathcal{X}^1 \text{ such that } (Z, j \vdash^? z) \in D.$$

Moreover, we proved that $\mathsf{C}\lfloor\xi\theta\rfloor_{\Phi\theta} = \xi\{Y \to \mathsf{C}\lfloor Y\theta\rfloor_{\Phi\theta} \mid Y \in vars^2(\xi)\}$, hence for all $Y \in vars^2(\mathsf{C}\lfloor\xi\theta\rfloor_\Phi\delta^2(\mathcal{C}))$, there exists $Z \in vars^2(\xi)$ such that $Y \in vars^2(\mathsf{C}\lfloor Z\theta\rfloor_\Phi \delta^2(\mathcal{C}))$. It implies that there exists $(\zeta, k \rhd u) \in \Phi$ such that $Y \in vars^2(\zeta)$ and $\zeta\theta \in st(Z\theta)$. Since $\mathcal{C}$ also satisfies $\mathsf{InvGeneral}$, we know that $ax_k \in st(\zeta\theta)$ and so we have that $k \leq \mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(Z)$. But thanks to $(\star)$, we have that $\mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(Y) < k$, which implies that $\mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(Y) < \mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(Z)$. But by definition of ξ, we have that $Z \in vars^2(\xi)$, and thus we have that $\mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(Z) \leq \mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(X)$, hence we conclude, thanks to Lemma 39, that $\neg(X <_\theta Y)$.

Thus we apply Lemma 40 on the deducible constraint $X, i \vdash^? u$ with the recipe $\xi\theta$. Therefore, there exists θ' such that (σ, θ') is a pre-solution of $\mathcal{C}$ with $X\theta' = \xi\theta$ and for all $Y \in vars^2(\mathcal{C})\backslash\{X\}$, we have $\mathsf{C}\lfloor Y\theta\rfloor_{\Phi\theta} = \mathsf{C}\lfloor Y\theta'\rfloor_{\Phi\theta'}$. At last, by the condition of Eq-ded-ded, we know that $\mathsf{root}(\xi) = \mathsf{f}$ implies $\mathsf{root}(X) \neq^? \mathsf{f} \in E_\Pi$, thus we can deduce that $\theta' \vDash E_\Pi$ and so $(\sigma, \theta') \in \mathsf{Sol}(\mathcal{C}_1)$.

2. $u\sigma\downarrow \neq v\sigma\downarrow$. In such a case, it is easy to see that $(\sigma, \theta) \in \mathsf{Sol}(\mathcal{C}_2)$.

Rule Ded-st(ξ, f). Let $(\sigma, \theta) \in \mathsf{Sol}(\mathcal{C})$. We distinguish two cases:

1. There exist ground recipes $\xi_1, \ldots, \xi_n$ in Π_r such that $\mathsf{f}(\xi_1, \ldots, \xi_n)(\Phi\sigma)\downarrow = u\sigma\downarrow$. In such a case, we can assume w.l.o.g. (see Lemma 35) that $\mathsf{f}(\xi_1, \ldots, \xi_n)$ conforms to

$\Phi\theta$ w.r.t. NoUse, and thus $\xi_1, \ldots, \xi_n$ conform also to the frame $\Phi\theta$ w.r.t. NoUse. For every $j \in \{1, \ldots, n\}$, let $t_j = \xi_j(\Phi\sigma)\downarrow$. Let $\theta' = \theta \cup \{X_1 \mapsto \xi_1, \ldots, X_n \mapsto \xi_n\}$, and $\sigma' = \sigma \cup \{x_1 \mapsto t_1, \ldots, x_n \mapsto t_n\}$. Clearly, we have that $X\theta'$ conforms to $\Phi\theta'$ for every $X \in vars^2(\mathcal{C}_1)$. Since f is a constructor symbol, $\mathsf{f}(\xi_1, \ldots, \xi_n)\Phi\sigma\downarrow = u\sigma\downarrow$ implies $\sigma' \vDash u = \mathsf{f}(x_1, \ldots, x_n)$. Moreover, since s_{max} is the maximal index that occurs in $\mathcal{C}$, we have that $param(X_i\theta') \subseteq \{ax_1, \ldots, ax_{\mathsf{s}_{max}}\}$ and thus $(\sigma, \theta) \in \mathsf{Sol}(\mathcal{C}_1)$.

2. Otherwise, for all ground recipes $\xi_1, \ldots, \xi_n$ in Π_r, we necessarily have that $\mathsf{f}(\xi_1, \ldots, \xi_n)\Phi\sigma\downarrow \neq u\sigma\downarrow$. Since f is a constructor symbol, we have that

$$\mathsf{f}(\xi_1, \ldots, \xi_n)\Phi\sigma\downarrow = \mathsf{f}(\xi_1\Phi\sigma\downarrow, \ldots, \xi_n\Phi\sigma\downarrow).$$

We can distinguish two cases: either $\mathsf{root}(u\sigma) \neq \mathsf{f}$ or else there exists $i \in \{1 \ldots n\}$, terms $t_1, \ldots, t_n$ such that $u\sigma = \mathsf{f}(t_1, \ldots, t_n)$ and $\xi_i\Phi\sigma\downarrow \neq t_i\downarrow$ for any ground recipe ξ_i. Therefore, we have that:

$$\sigma \vDash \forall \tilde{x} \cdot [u \neq \mathsf{f}(x_1, \ldots, x_n) \vee \mathsf{s}_{max} \not\vdash^? x_1 \vee \ldots \vee \mathsf{s}_{max} \not\vdash^? x_n].$$

This allows us to conclude that $(\sigma, \theta) \in \mathsf{Sol}(\mathcal{C}_2)$.

Hence, the result. □

Lemma 43. *Let $\mathcal{C}$ be a constraint system obtained by following the strategy.* $\mathsf{Sol}(\mathcal{C}) = \mathsf{Sol}(\mathcal{C}\downarrow)$.

Proof. The rules for normalisation presented in Figure 3 corresponds to classic transformation on formula of first order logic. Once can easily prove that all the rules in Figure 3 preserves the set of solutions. Hence we focus on the two rules presented in Figure 4.

Rule 1: In such a case, $E = E' \wedge \forall \tilde{x}.[E'' \vee x \neq^? a]$, $a \in \mathcal{N}$ and $(X, i \vdash^? x) \in D$. Thus $x \notin \tilde{x}$. Moreover, we have that $\textsc{Axiom}(X, \mathsf{path})$ is useless for any path, and $\textsc{Dest}(\xi, \ell \to r, i)$ is useless for any ξ, $\ell \to r$.

Let $(\sigma, \theta) \in \mathsf{Sol}(\mathcal{C})$. We show that $x\sigma \neq a$. Thanks to Lemma 36, $\mathsf{C}\lfloor X\theta \rfloor_\Phi \in \mathcal{T}(\mathcal{F}_c, \mathcal{F}_d^* \cdot \mathcal{AX})$. Moreover, But $\textsc{Axiom}(X, \mathsf{path})$ is useless for any path. Hence either $\textsc{Axiom}(X, \mathsf{path})$ is not applicable or its application results in two constraint systems $\mathcal{C}_1$ and $\mathcal{C}_2$ such that $\mathcal{C}_1$ simplifies to $\bot$ using the rules in Figure 3 and $\mathcal{C}_2$ simplifies into $\mathcal{C}$. But if there exists $(\xi, j \rhd v) \in \Phi$ such that $\mathsf{path}(\xi)$, $j \leq i$ and $(\xi, j \rhd u) \notin \mathsf{NoUse}$ then the application of $\mathcal{C}_1$ add the equation $X =^? \xi$ in E_Π, and the equation $x =^? v$ in E. Hence $\mathcal{C}_1$ simplifies in $\bot$ implies that $X\theta \neq \xi\theta$ or $x\sigma \neq v\sigma$. However, thanks to $\mathcal{C}$ being well-formed (Definition 18, item 5) and $(\sigma, \theta) \in \mathsf{Sol}(\mathcal{C})$, we deduce that $X\theta(\Phi\sigma)\downarrow = x\sigma$ and $\xi\theta(\Phi\sigma)\downarrow = v\sigma$. Hence $x\sigma \neq v\sigma$ implies $X\theta \neq \xi\theta$.

Hence $\textsc{Axiom}(X, \mathsf{path})$ is useless for any path implies that for all $(\zeta, j \rhd v) \in \Phi(\mathcal{C})$, if $j \leq i$ and $(\zeta, j \rhd v) \notin \mathsf{NoUse}$ then $X\theta \neq \zeta\theta$. But we know that $\mathcal{C}$ satisfies $\mathsf{InvGeneral}$ thus for all $(\zeta, j \rhd v) \in \Phi(\mathcal{C})$, $ax_j \in st(\zeta\theta)$. Thus, $paramX\theta \subseteq \{ax_1, \ldots, ax_i\}$ and $X\theta$ conforms to $\Phi\theta$ w.r.t. $\mathsf{NoUse}\theta$ implies that for all $w \in \mathsf{C}\lfloor X\theta \rfloor_\Phi \cap \mathcal{F}_d^* \cdot \mathcal{AX}$, there exists $(\zeta, j \rhd v) \in \Phi(\mathcal{C})$ such that $\mathsf{path}(\zeta) = w$ and $j \leq s$. Since we already proved that in this case, $X\theta \neq \xi\theta$, then we deduce that $\mathsf{C}\lfloor X\theta \rfloor_\Phi \in \mathcal{T}(\mathcal{F}_c, \mathcal{F}_d^* \cdot \mathcal{AX})$ and $|\mathsf{C}\lfloor X\theta \rfloor_\Phi| > 1$. Along with $X\theta(\Phi\sigma)\downarrow = x\sigma$, it implies that $|x\sigma| > 1$ and so $x\sigma \neq a$.

Rule 2: In such a case, we have $(X, i \vdash^? u) \in D$, $\textsc{Cons}(X, \mathsf{f})$ is useless for any $\mathsf{f} \in \mathcal{F}_c$, $\textsc{Axiom}(X, \mathsf{path})$ is useless for any path and $\textsc{Dest}(\xi, \ell \to r, i)$ is useless for all $\xi, \ell \to r$.

Let $(\sigma, \theta) \in \mathsf{Sol}(\mathcal{C})$. In the case of rule (Nname), we showed that $\mathsf{C}\lfloor X\theta \rfloor_\Phi \in \mathcal{T}(\mathcal{F}_c, \mathcal{F}_d^* \cdot \mathcal{AX})$ and $|\mathsf{C}\lfloor X\theta \rfloor_\Phi| > 1$. But $\textsc{Cons}(X, \mathsf{f})$ is useless for any $\mathsf{f} \in \mathcal{F}_c$. Hence either $\textsc{Cons}(X, \mathsf{f})$ is not applicable or its application results in two constraint systems $\mathcal{C}_1$ and $\mathcal{C}_2$ such that $\mathcal{C}_1$ simplifies to $\bot$ using the rules in Figure 3 and $\mathcal{C}_2$ simplifies into $\mathcal{C}$.

Let $\mathsf{f} \in \mathcal{F}_c$. Since $(X, i \vdash^? u) \in D$, then $\textsc{Cons}(X, \mathsf{f})$ is applicable. According to Figure 1, its application adds an equation $X =^? \mathsf{f}(X_1, \ldots, X_n)$ in E_Π and $u =^? \mathsf{f}(x_1, \ldots, x_n)$ where $X_1, \ldots, X_n$ and $x_1, \ldots, x_n$ are fresh variables. Since $X_1, \ldots, X_n$, $x_1, \ldots, x_n$ are fresh, C_1 simplifying to $\bot$ implies that $\mathsf{root}(X\theta) \neq \mathsf{f}$ or $\mathsf{root}(u\sigma) \neq \mathsf{f}$. But $(\sigma, \theta) \in \mathsf{Sol}(\mathcal{C})$ implies that $(X\theta)(\Phi\sigma)\downarrow = u\sigma$. Moreover, along with $\mathsf{C}\lfloor X\theta \rfloor_\Phi \in \mathcal{T}(\mathcal{F}_c, \mathcal{F}_d^* \cdot \mathcal{AX})$ and $|\mathsf{C}\lfloor X\theta \rfloor_\Phi| > 1$, C_1 simplifying to $\bot$ implies that $\mathsf{root}(u\sigma) = \mathsf{root}(X\theta)$. Hence we deduce that $\mathsf{root}(X\theta) \neq \mathsf{f}$. Hence, we proved that for all $\mathsf{f} \in \mathcal{F}_c$, $\mathsf{root}(X\theta) \neq \mathsf{f}$ which is a contradiction with $\mathsf{C}\lfloor X\theta \rfloor_\Phi \in \mathcal{T}(\mathcal{F}_c, \mathcal{F}_d^* \cdot \mathcal{AX})$ and $|\mathsf{C}\lfloor X\theta \rfloor_\Phi| > 1$. Hence $(\sigma, \theta) \notin \mathsf{Sol}(\mathcal{C})$ and so $\mathsf{Sol}(\mathcal{C}) = \emptyset = \mathsf{Sol}(\bot)$. □

Lemma 44. *Let $(\mathcal{M}, \mathcal{M}')$ be a pair of matrices of constraint systems. Let k be the number of columns in $\mathcal{M}$ and $\mathcal{M}'$. Assume that $(\mathcal{M}, \mathcal{M}')$ is obtained at the end of Step d of Phase 1 of the strategy with parameter s for the support and k for the index of the column. Let $\mathcal{C}$ be a constraint system in $\mathcal{M}$ or $\mathcal{M}'$. If $\mathcal{C}$ is replaced by $\bot$ when applying Step e of Phase 1 of the strategy, then we have that $\mathsf{Sol}(\mathcal{C}) = \emptyset$.*

Proof. Let $\mathcal{C}$ be a constraint system in $\mathcal{M}$ or $\mathcal{M}'$ such that $\mathcal{C}$ is replaced by $\bot$ when applying Step e of Phase 1 of the strategy. By definition, we know that there is two conditions that trigger the replacement of $\mathcal{C}$ by $\bot$. We prove that if one of the two conditions is satisfied then $\mathsf{Sol}(\mathcal{C}) = \emptyset$.

Condition 1: By definition, we know that there exists a constraint system $\mathcal{C}'$ in the same column as $\mathcal{C}$, a recipe ξ, such that:

- $(\xi, i \rhd u) \in \Phi(\mathcal{C}')$ for some $i \leq s$ and u
- for all $(\xi', j \rhd v) \in \Phi(\mathcal{C})$, $\mathsf{path}(\xi) \neq \mathsf{path}(\xi')$

Let $w \cdot ax_k = \mathsf{path}(\xi)$. We prove by induction on $|w|$ that there exists w' suffix of w, $(\zeta, j \in u) \in \Phi(\mathcal{C})$, $(\zeta', j' \in u') \in \Phi(\mathcal{C}')$ such that:

- $\mathsf{path}(\zeta) = \mathsf{path}(\zeta') = w' \cdot ax_k$, $j \leq s$ and $j' \leq s$.
- there exists $(\zeta'', j'' \rhd u'') \in \Phi(\mathcal{C}')$ such that $\mathsf{path}(\zeta'') = \mathsf{g} \cdot \mathsf{path}(\zeta)$ for some $\mathsf{g} \in \mathcal{F}_d$.
- for all $(\zeta''', j''' \rhd u''') \in \Phi(\mathcal{C})$, $\mathsf{path}(\zeta''') \neq \mathsf{path}(\zeta'')$.

Base case $|w| = 0$: In such a case, we have that $\xi = ax_k$. But $\mathcal{C}$ and $\mathcal{C}'$ are both originated from the same initial constraint system, thus we know that there exists u, u' such that $(ax_k, k \rhd u) \in \Phi(\mathcal{C})$ and $(ax_k, k \rhd u') \in \Phi(\mathcal{C}')$. Hence there is a contradiction with our hypothesis on ξ.

Inductive step $|w| > 0$: Otherwise, there exists w' and $\mathsf{g} \in \mathcal{F}_d$ such that $w = \mathsf{g} \cdot w' \cdot ax_k$. But $\mathcal{C}'$ is a well-formed constraint system, hence by Property 2 of a well formed constraint

system, $(\xi, i \rhd u) \in \Phi(\mathcal{C}')$ implies that there exists $(\zeta', j' \rhd v') \in \Phi(\mathcal{C}')$ such that $\mathsf{path}(\zeta') = w' \cdot ax_k$ and $i \leq j'$.

Hence if there exists $(\zeta, j \rhd v) \in \Phi(\mathcal{C})$ such that $\mathsf{path}(\zeta) = \mathsf{path}(\zeta')$ then the result holds with $(\zeta'', j'' \rhd u'') = (\xi, i \rhd u)$. Else, since $|w'| < |w|$, we can apply our inductive hypothesis on $(\zeta', j' \rhd v')$ and so the result also holds.

Main proof for Condition 1: Thanks to Lemma 27, we know that $(\mathcal{M}, \mathcal{M}')$ satisfies $\mathsf{PP1Sb}(s, k+1)$. Since k corresponds to the number of column in $\mathcal{M}$ and $\mathcal{M}'$, we deduce that all constraint systems in $\mathcal{M}$ or $\mathcal{M}'$ satisfies $\mathsf{InvVarConstraint}(s)$, $\mathsf{InvUntouched}(s)$ and $\mathsf{InvDest}(s)$.

Let $(\sigma, \theta) \in \mathsf{Sol}(\mathcal{C})$. Thanks to $\mathcal{C}$ satisfying $\mathsf{InvDest}(s)$, $(\zeta, j \in u) \in \Phi(\mathcal{C})$ and for all $(\zeta''', j''' \rhd u''') \in \Phi(\mathcal{C})$, $\mathsf{path}(\zeta''') \neq \mathsf{g} \cdot \mathsf{path}(\zeta)$, we deduce that $\sigma \vDash ND(\mathcal{C})$ implies that there is no recipe $\zeta_2, \ldots, \zeta_n \in \Pi_r$ such that $\mathsf{g}(\zeta\theta, \zeta_2, \ldots, \zeta_n)(\Phi(\mathcal{C})\sigma)\downarrow \in \mathcal{T}(\mathcal{F}_c, \mathcal{N})$ and $\mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(\zeta_i) \leq s$ for all $i \in \{2, \ldots, n\}$.

But $(\zeta'', j'' \rhd u'') \in \Phi(\mathcal{C}')$ with $\mathsf{path}(\zeta'') = \mathsf{g} \cdot \mathsf{path}(\zeta)$. Hence there exists $\xi_2, \ldots, \xi_n$ such that $\zeta'' = \mathsf{g}(\zeta', \xi_2, \ldots, \xi_n)$. We will show that $\zeta'\theta(\Phi(\mathcal{C})\sigma)\downarrow = \zeta\theta(\Phi(\mathcal{C})\sigma)\downarrow$ and $\zeta''\theta(\Phi(\mathcal{C})\sigma)\downarrow \in \mathcal{T}(\mathcal{F}_c, \mathcal{N})$ with $\mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(\xi_i\theta) \leq s$, for all $i \in \{2, \ldots, n\}$. Hence it will contradict the fact that $\sigma \vDash ND(\mathcal{C})$ and so it will implies that $\mathsf{Sol}(\mathcal{C}) = \emptyset$.

We know that $\mathcal{C}$ and $\mathcal{C}'$ satisfy $\mathsf{InvVarConstraint}(s)$ and $\mathsf{InvUntouched}(s)$. Moreover, thanks to Lemma 25, we also know that there exists a variable renaming $\rho : \mathcal{X}^1 \setminus S_1(\mathcal{C}) \to \mathcal{X}^1 \setminus S_1(\mathcal{C}')$ such that:

1. $\mathsf{mgu}(E(\mathcal{C}))_{|S_1(\mathcal{C})}\rho = \mathsf{mgu}(E(\mathcal{C}'))_{|S_1(\mathcal{C}')}$, and $D(\mathcal{C})\rho = D(\mathcal{C}')$;
2. $\{(u\rho, u') \mid (\xi, i \rhd u) \in \Phi \wedge (\xi', i' \rhd u') \in \Phi' \wedge \mathsf{path}(\xi) = \mathsf{path}(\xi')\}$ is include in $\{(u, u) \mid u \in \mathcal{T}(\mathcal{F}_c, \mathcal{N} \cup \mathcal{X}^1)\}$;

$(\sigma, \theta) \in \mathsf{Sol}(\mathcal{C})$ implies that for all $X, k \vdash^? t \in D(\mathcal{C})$, we have $(X\theta)(\Phi(\mathcal{C})\sigma)\downarrow = t\sigma$. Moreover, we know that for all $(ax_\ell, \ell \rhd v) \in \Phi(\mathcal{C})$, $(ax_\ell, \ell \rhd v') \in \Phi(\mathcal{C}')$, $v\rho = v'$ which means that $(X\theta)(\Phi(\mathcal{C})\sigma)\downarrow = t\sigma$ implies $(X\theta)(\Phi(\mathcal{C}')\rho^{-1}\sigma)\downarrow = t'\rho^{-1}\sigma$ with $(X, k \vdash^? t') \in D(\mathcal{C}')$ and $t\rho = t'$.

But, for all $X \in vars^2(\zeta')$, by Property 3 of a well formed constraint system, we know that $\mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(\zeta') \leq j'$ and so there exists $(X, k \vdash^? t') \in D(\mathcal{C}')$ such that $k \leq j'$. Thus $(X\theta)(\Phi(\mathcal{C}')\rho^{-1}\sigma)\downarrow = t'\rho^{-1}\sigma$. $\mathcal{C}$ being well-formed (item 5) allows us to deduce that $(\zeta'\theta)(\Phi(\mathcal{C}')\rho^{-1}\sigma)\downarrow = u'\rho^{-1}\sigma\downarrow \in \mathcal{T}(\mathcal{F}_c, \mathcal{N})$. Hence, we have that $(\zeta'\theta)(\Phi(\mathcal{C})\sigma)\downarrow = u\sigma\downarrow = (\zeta\theta)(\Phi(\mathcal{C})\sigma)\downarrow$.

Similarly, we have that $(\zeta''\theta)(\Phi(\mathcal{C})\sigma)\downarrow = u''\rho^{-1}\sigma\downarrow \in \mathcal{T}(\mathcal{F}_c, \mathcal{N})$. It remains to show that for all $i \in \{2, \ldots, n\}$, $param(\xi_i\theta) \subseteq \{ax_1, \ldots, ax_s\}$. Since $\mathcal{C}'$ satisfies the invariant $\mathsf{InvUntouched}(s)$, we know that $j'' \leq s$. But $\mathcal{C}'$ is well-formed (item 3) hence we deduce that $\mathsf{param}^{\mathcal{C}'}_{\mathsf{max}}(\zeta'') \leq j''$. Since $\mathcal{C}$ and $\mathcal{C}'$ have the same shape and satisfy $\mathsf{InvVarConstraint}(s)$, we deduce that $\mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(\zeta'') = \mathsf{param}^{\mathcal{C}'}_{\mathsf{max}}(\zeta'')$. But for all $X \in vars^2(\zeta'')$, $(\sigma, \theta) \in \mathsf{Sol}(\mathcal{C})$ implies $\mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(X\theta) \leq \mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(X)$. Hence, along with $\mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(\zeta'') \leq j''$, it implies that $\mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(\zeta''\theta) \leq j'' \leq s$. Since for all $i \in \{2, \ldots, n\}$, $\xi_i \in st(\zeta'')$, we can deduce that $\mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(\xi_i\theta) \leq s$.

Condition 2: By hypothesis, there exists a constraint system $\mathcal{C}'$ in the column of $\mathcal{C}$, $(\xi, i \rhd u) \in \Phi(\mathcal{C})$, $(\xi', i' \rhd u') \in \Phi(\mathcal{C}')$, $\mathsf{f} \in \mathcal{F}_c$ such that

- $\mathsf{path}(\xi) = \mathsf{path}(\xi')$, $i \leq s$ and $i' \leq s$

- $ND(\mathcal{C}) \vDash \forall \tilde{x}.u \neq \mathsf{f}(x_1,\ldots,x_n) \vee s \not\vdash^? x_1 \vee \ldots \vee s \not\vdash^? x_n$ where $\tilde{x} = x_1 \ldots x_n$ are variables.
- there exists $X_1,\ldots,X_n \in vars^2(\mathcal{C}')$ such that $\mathsf{C}\lfloor \mathsf{f}(X_1,\ldots,X_n)\Theta' \rfloor_{\Phi(\mathcal{C}')}\delta^1(\mathcal{C}') = u'$ and such that $\mathsf{param}^{\leq}_{\mathsf{max}}(\mathsf{f}(X_1,\ldots,X_n)\Theta')s$ where $\Theta' = \mathsf{mgu}(E_\Pi(\mathcal{C}'))$.

We prove in Condition 1 that $(\sigma,\theta) \in \mathsf{Sol}(\mathcal{C})$ implies that for all $(X, k \vdash^? t') \in D(\mathcal{C}')$, $X\theta(\Phi(\mathcal{C})\sigma)\downarrow = X\theta(\Phi(\mathcal{C}')\rho^{-1}\sigma)\downarrow = t'\rho^{-1}\sigma$. Hence, for all $(\zeta, i \vdash^? v') \in \Phi(\mathcal{C}')$, Property 5 of a well formed constraint systems for $\mathcal{C}'$ implies that $\zeta\theta(\Phi(\mathcal{C}')\rho^{-1}\sigma)\downarrow = v'\rho^{-1}\sigma$ with $\mathsf{param}^{\leq}_{\mathsf{max}}(\zeta\theta)i$.

Let $\Theta = \mathsf{mgu}(E_\Pi(\mathcal{C}))$ and $\Theta' = \mathsf{mgu}(E_\Pi(\mathcal{C}'))$. By hypothesis, we know that $X_1,\ldots,X_n \in vars^2(\mathcal{C}')$, hence thanks to Property 7 of a well formed constraint system, we have that for all $i \in \{1,\ldots,n\}$, $\mathsf{C}\lfloor X_i\Theta' \rfloor_{\Phi(\mathcal{C}')} \in \mathcal{T}(\mathcal{F}_c, \mathcal{F}_d^* \cdot \mathcal{A}\mathcal{X} \cup \mathcal{X}^2)$ and for all $\xi \in st(X\Theta')$, $\mathsf{path}(\xi)$ exists implies that there exists j and v such that $(\xi, j \rhd v) \in \Phi(\mathcal{C}')$. Hence, $\mathsf{C}\lfloor \mathsf{f}(X_1,\ldots,X_n)\Theta' \rfloor_{\Phi(\mathcal{C}')}\delta^1(\mathcal{C}') = u'$ implies that $\mathsf{f}(X_1,\ldots,X_n)\Theta'\theta(\Phi(\mathcal{C}')\rho^{-1}\sigma)\downarrow = u'\rho^{-1}\sigma$. Since $\mathsf{f}(X_1,\ldots,X_n)\Theta'\theta(\Phi(\mathcal{C}')\rho^{-1}\sigma)\downarrow = \mathsf{f}(X_1,\ldots,X_n)\Theta'\theta(\Phi(\mathcal{C})\sigma)\downarrow$ and $u\rho = u'$, we can deduce that $\mathsf{f}(X_1,\ldots,X_n)\Theta'\theta(\Phi(\mathcal{C})\sigma)\downarrow = u\sigma$.

Moreover, we know that $\mathsf{param}^{\mathcal{C}'}_{\mathsf{max}}(\mathsf{f}(X_1,\ldots,X_n)\Theta') \leq s$ which implies that for all $Y \in vars^2(\mathsf{f}(X_1,\ldots,X_n)\Theta')$, $\mathsf{param}^{\mathcal{C}'}_{\mathsf{max}}(Y) \leq s$. But $\mathcal{C}$ and $\mathcal{C}'$ have the same shape and both satisfy the invariant $\mathsf{InvVarConstraint}(s)$. Hence $\mathsf{param}^{\mathcal{C}'}_{\mathsf{max}}(Y) = \mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(Y)$. Since $(\sigma,\theta) \in \mathsf{Sol}(\mathcal{C})$, we have that $\mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(Y) \leq s$ implies $\mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(Y\theta) \leq s$. We conclude that $\mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(\mathsf{f}(X_1,\ldots,X_n)\Theta'\theta) \leq s$.

Hence, we proved that there exists $\xi_1,\ldots,\xi_n \in \Pi_r$ such that $\mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(\xi_i) \leq s$ for all $i \in \{1,\ldots,n\}$, and $\mathsf{f}(\xi_1,\ldots,\xi_n)(\Phi(\mathcal{C})\sigma)\downarrow = u\sigma$. But $ND(\mathcal{C}) \vDash \forall \tilde{x}.u \neq \mathsf{f}(x_1,\ldots,x_n) \vee s \not\vdash^? x_1 \vee \ldots \vee s \not\vdash^? x_n$ where $\tilde{x} = x_1 \ldots x_n$ are variables. Moreover, $(\sigma,\theta) \in \mathsf{Sol}(\mathcal{C})$ implies that $\sigma \vDash ND(\mathcal{C})$ which is a contradiction with the fact that $\mathsf{f}(\xi_1,\ldots,\xi_n)(\Phi(\mathcal{C})\sigma)\downarrow = u\sigma$. Hence, $\mathsf{Sol}(\mathcal{C}) = \emptyset$. □

Appendix D.5. Link between solutions of two constraint systems

With the previous to establish soundness (Lemma 42) and completeness (Lemma 5), we can see that our rules preserve the set of first-order solution of a constraint system. On the other hand, Lemma 42 indicates that it is possible that some second-order solutions are not preserved, for example the solutions that use several recipes to deduce the same key. Even if the non-preservation of the whole set of second-order solutions could be surprising at first sight, the idea is to preserve enough second-order solutions to be able to establish symbolic equivalence as stated in the following lemma.

Lemma 45. *Let $(\mathcal{C},\mathcal{C}')$ be a pair of normalised constraint systems having the same structure and obtained by following the strategy. We denote by Φ and Φ' their associated frame. We denote by S_1, S_1' their associated set of free variables. Let* Rule$(\tilde{p})$ *be a transformation rule applicable on $(\mathcal{C},\mathcal{C}')$. Let $(\mathcal{C}_1,\mathcal{C}_1')$ and $(\mathcal{C}_2,\mathcal{C}_2')$ the two resulting pairs of constraint systems obtained by applying* Rule$(\tilde{p})$ *on $(\mathcal{C},\mathcal{C}')$, and we denote by Φ_1, Φ_1', Φ_2, and Φ_2' their associated frame.*

Let σ,θ and σ' be three substitutions such that $(\sigma,\theta) \in \mathsf{Sol}(\mathcal{C})$, $(\sigma',\theta) \in \mathsf{Sol}(\mathcal{C}')$, and $\Phi\sigma \sim \Phi'\sigma'$. For all substitution θ',

1. *$(\sigma,\theta') \in \mathsf{Sol}(\mathcal{C})$ if, and only, if $(\sigma',\theta') \in \mathsf{Sol}(\mathcal{C}')$.*

2. *Let $i \in \{1,2\}$, and σ_i be a substitution such that $\sigma|_{S_1} = \sigma_i|_{S_1}$ and $(\sigma_i, \theta') \in \mathsf{Sol}(\mathcal{C}_i)$. Then, $(\sigma'_i, \theta') \in \mathsf{Sol}(\mathcal{C}'_i)$ for some substitution σ'_i such that $\sigma'|_{S'_1} = \sigma'_i|_{S'_1}$. Moreover, we have that $\mathsf{Init}(\Phi_i)\sigma_i = \mathsf{Init}(\Phi)\sigma$ and $\mathsf{Init}(\Phi'_i)\sigma'_i = \mathsf{Init}(\Phi')\sigma'$.*

Proof. Let σ, θ and σ' be three substitutions such that $(\sigma, \theta) \in \mathsf{Sol}(\mathcal{C})$, $(\sigma', \theta) \in \mathsf{Sol}(\mathcal{C}')$, and $\Phi\sigma \sim \Phi'\sigma$. Let θ' be another substitution. We prove the two properties separately. The variation can be proved in a similar way.

1. We assume that $(\sigma, \theta') \in \mathsf{Sol}(\mathcal{C})$, and we show that $(\sigma', \theta') \in \mathsf{Sol}(\mathcal{C}')$. The other implication can be done in a similar way. Let $\mathcal{C} = (S_1; S_2; \Phi; D; E; E_\Pi; ND; \mathsf{NoUse})$ and $\mathcal{C}' = (S'_1; S'_2; \Phi'; D'; E'; E'_\Pi; ND'; \mathsf{NoUse}')$. First, since $(\sigma', \theta) \in \mathsf{Sol}(\mathcal{C}')$, we have that $\sigma' \models ND' \wedge E'$. Second, since $\mathcal{C}$ and $\mathcal{C}'$ have the same structure, we have that $E_\Pi = E'_\Pi$, and so $\theta' \models E'_\Pi$. Moreover, for any $X, i \vdash^? u' \in D'$, we have that $\mathit{param}(X\theta') \subseteq \{ax_1, \ldots, ax_i\}$ and for any ground recipe ξ in Π_r, ξ conforms to $\Phi\theta'$ w.r.t. $\mathsf{NoUse}\theta'$ if, and only if, ξ conforms to $\Phi'\theta'$ w.r.t. $\mathsf{NoUse}'\theta'$. In order to conclude, it remains to show that $(X\theta')\Phi\sigma'{\downarrow} = u'\sigma'{\downarrow}$ for any $(X, i \vdash^? u') \in D'$.

   Since $(\sigma, \theta) \in \mathsf{Sol}(\mathcal{C})$ and $(\sigma, \theta') \in \mathsf{Sol}(\mathcal{C})$, we have $(X\theta)\Phi\sigma{\downarrow} = (X\theta')\Phi\sigma{\downarrow}$ for each constraint $(X, i \vdash^? u) \in D$. Since $\Phi\sigma \sim \Phi'\sigma'$, we have that $(X\theta)\Phi'\sigma'{\downarrow} = (X\theta')\Phi'\sigma'{\downarrow}$ for each constraint $(X, i \vdash^? u') \in D'$ (by relying also on the fact that $\mathcal{C}$ and $\mathcal{C}'$ have the same structure). Moreover, since $(\sigma', \theta) \in \mathsf{Sol}(\mathcal{C}')$, we have that $(X\theta)\Phi'\sigma'{\downarrow} = u'\sigma'{\downarrow}$ for each constraint $(X, i \vdash^? u') \in D'$. Altogether, this allows us to obtain that $(X\theta')\Phi'\sigma'{\downarrow} = u'\sigma'{\downarrow}$ for each constraint $(X, i \vdash^? u') \in D'$. This allows us to conclude.

2. Let $i \in \{1,2\}$ and σ_i be a substitution such that $\sigma = \sigma_i|_{vars^1(\mathcal{C})}$ and $(\sigma_i, \theta') \in \mathsf{Sol}(\mathcal{C}_i)$. First, by inspection of the rules, it is easy to see that $\mathsf{Init}(\Phi_i)\sigma_i = \mathsf{Init}(\Phi)\sigma$ and $\mathsf{Init}(\Phi'_i)\sigma'_i = \mathsf{Init}(\Phi')\sigma'$. Since $\mathcal{C}_i$ and $\mathcal{C}'_i$ have the same structure, we have that $E_\Pi(\mathcal{C}_i) = E_\Pi(\mathcal{C}'_i)$, and so $\theta' \models E_\Pi(\mathcal{C}'_i)$. Moreover, for any $X, j \vdash^? u \in D(\mathcal{C}'_i)$, we have that $\mathit{param}(X\theta') \subseteq \{ax_1, \ldots, ax_i\}$ and for any ground recipe ξ in Π_r, ξ conforms to $\Phi_i\theta'$ w.r.t. $\mathsf{NoUse}\theta'$ if, and only if, ξ conforms to $\Phi'_i\theta'$ w.r.t. $\mathsf{NoUse}'\theta'$. In order to conclude, it remains to show that there exists a substitution σ'_i such that $(\sigma'_i, \theta') \in \mathsf{Sol}(\mathcal{C}'_i)$, *i.e.* such that $(X\theta')\Phi_i\sigma'_i{\downarrow} = u'\sigma'_i{\downarrow}$ for any $(X, j \vdash^? u') \in D'_i$ and $\sigma'_i \models ND'_i \wedge E'_i$.

   Thanks to Lemma 5, we have that $(\sigma, \theta'|_{vars^2(\mathcal{C})}) \in \mathsf{Sol}(\mathcal{C})$. Thanks to *Item 1*, we know that $(\sigma', \theta'|_{vars^2(\mathcal{C})}) \in \mathsf{Sol}(\mathcal{C}')$. Then, we prove the results by case analysis on the rule $\textsc{Rule}(\tilde{p})$ (we rely on the notation of Figures 1 and 2) foccusing on the additional constraints that have been added in $\mathcal{C}'_i$.

   Rule Cons, $i = 1$: Since $(\sigma', \theta'|_{vars^2(\mathcal{C})}) \in \mathsf{Sol}(\mathcal{C}')$ and $\theta' \vDash E'_{\Pi i}$, we have $(X\theta')\Phi'\sigma'{\downarrow} = t'\sigma'$ and $\mathsf{root}(X\theta') = \mathsf{f}$. Thus, we can deduce that $\mathsf{root}(t'\sigma') = \mathsf{f}$. Let $\sigma'_i = \sigma' \cup \{x'_1 \mapsto t'_1, \ldots, x'_n \mapsto t'_n\}$ where $t'\sigma' = \mathsf{f}(t'_1, \ldots, t'_n)$ and so $\sigma'_i \vDash t' =^? \mathsf{f}(x'_1, \ldots, x'_n)$. Moreover, $(\sigma', \theta'|_{vars^2(\mathcal{C})}) \in \mathsf{Sol}(\mathcal{C}')$ implies that $\sigma' \vDash ND' \wedge E'$ which means that $\sigma'_i \vDash ND' \wedge E' \wedge t' =^? \mathsf{f}(x'_1, \ldots, x'_n)$ and so $\sigma'_i \vDash ND'_i \wedge E'_i$. At last, since we already know that $X\theta' = \mathsf{f}(X_1\theta', \ldots, X_n\theta')$ and $(X\theta')\Phi'\sigma'{\downarrow} = t'\sigma' = \mathsf{f}(x'_1\sigma'_i, \ldots, x'_n\sigma'_i)$, we can deduce that $(X_j\theta')(\Phi'\sigma'_i){\downarrow} = x'_j\sigma'_i$ for $j = \{1 \ldots n\}$.

Rule CONS, $i = 2$: We have that $(\sigma', \theta') \in \mathsf{Sol}(\mathcal{C}')$, thus it remains to prove that $\theta' \vDash \mathsf{root}(X) \neq \mathsf{f}$. We know that $\theta' \vDash E'_{\Pi_i}$ which means that $\theta' \vDash \mathsf{root}(X) \neq \mathsf{f}$.

Rule AXIOM, $i = 1$: We already know that $\theta' \vDash E'_{\Pi_i}$ thus $\theta' \vDash X =^? \xi$. Thus it remains to prove that $\sigma' \vDash u' =^? v'$. We know that $(\sigma', \theta') \in \mathsf{Sol}(\mathcal{C}')$, and thus we have that $X\theta'(\Phi'\sigma')\downarrow = u'\sigma'$ and $\xi\theta'(\Phi'\sigma')\downarrow = v'\sigma'$. Moreover, thanks to Item 1, we have that $(\sigma, \theta') \in \mathsf{Sol}(\mathcal{C})$. This implies that $X\theta'(\Phi\sigma)\downarrow = u\sigma$ and $\xi\theta'(\Phi\sigma)\downarrow = v\sigma$. But, we know that $\Phi\sigma \sim \Phi'\sigma'$ and we have that $\sigma \vDash u =^? v$. Thus, we can deduce that $\xi\theta'(\Phi'\sigma')\downarrow = X\theta'(\Phi'\sigma')\downarrow$ and so $\sigma' \vDash u' =^? v'$.

Rule AXIOM, $i = 2$: We already shown that $\theta' \models E'_{\Pi_i}$ and so $\theta' \models X \neq^? \xi$. We have nothing else to prove.

Rule DEST, $i = 1$: Since $(\sigma_i, \theta') \in \mathsf{Sol}(\mathcal{C}_i)$, we can deduce $\mathsf{f}(\xi, X_2, \ldots, X_n)\theta'(\Phi\sigma)\downarrow = w\sigma_i \in \mathcal{T}(\mathcal{F}_c, \mathcal{N})$. Moreover, we know $\Phi\sigma \sim \Phi'\sigma'$, thus $\mathsf{f}(\xi, X_2, \ldots, X_n)\theta'(\Phi\sigma)\downarrow \in \mathcal{T}(\mathcal{F}_c, \mathcal{N})$ implies $\mathsf{f}(\xi, X_2, \ldots, X_n)\theta'(\Phi'\sigma')\downarrow \in \mathcal{T}(\mathcal{F}_c, \mathcal{N})$ which means that $\xi\theta'(\Phi'\sigma')\downarrow$ can be reduced by the destructor f. Thus, $\mathsf{f}(u'_1, \ldots, u'_n) \to w'$ being a fresh renaming of $\ell \to r$, we can extend σ' into σ'_i such that $u'_1\sigma'_i = v'\sigma'_i$. Moreover, for each rewriting rule, we have that $vars^1(u'_j) \subseteq vars^1(u'_1)$ for $j = 2 \ldots n$, thus $\mathsf{f}(\xi, X_2, \ldots, X_n)\theta'(\Phi'\sigma')\downarrow \in \mathcal{T}(\mathcal{F}_c, \mathcal{N})$ implies that $X_j\theta'(\Phi'_i\sigma'_i)\downarrow = u'_j\sigma'$ for $j = 2 \ldots n$.

Rule DEST, $i = 2$: The non deducibility constraint added in $\mathcal{C}'_2$ corresponds to the fact that for all $(\xi_1, \ldots, \xi_n) \in \Pi_r$ with parameter included in $\{ax_1, \ldots, ax_i\}$, we have $\xi_1\Phi'\sigma'\downarrow \neq \xi\theta\Phi'\sigma'\downarrow \vee f(\xi_1, \ldots, \xi_n)\Phi'\sigma'\downarrow \notin \mathcal{T}(\mathcal{F}_c, \mathcal{N})$. But, by hypothesis, we know that $(\sigma_2, \theta') \in \mathsf{Sol}(\mathcal{C}_2)$ and $\sigma = \sigma_2|_{vars^1(\mathcal{C})} = \sigma_2$. Thus, $\sigma_2 \vDash ND_2$ and so for all recipes $(\xi_1, \ldots, \xi_n) \in \Pi_r$ with parameter included in $\{ax_1, \ldots, ax_i\}$, we have $\xi_1\Phi\sigma\downarrow \neq \xi\theta\Phi\sigma\downarrow \vee f(\xi_1, \ldots, \xi_n)\Phi\sigma\downarrow \notin \mathcal{T}(\mathcal{F}_c, \mathcal{N})$. Lastly, since we have that $\Phi\sigma \sim \Phi'\sigma'$, the result holds.

Rule EQ-FRAME-FRAME: We add an equation $u_1 =^? u_2$ (resp. a disequation $u_1 \neq^? u_2$). Moreover, we have that $u_j\sigma = \xi_j\theta'(\Phi\sigma)\downarrow$ for $j = 1, 2$. Thanks to Item 1, we know that $(\sigma', \theta') \in \mathsf{Sol}(\mathcal{C}')$ which means that $u'_j\sigma' = \xi_j\theta'(\Phi'\sigma')\downarrow$, for $j = 1, 2$. Since $\Phi\sigma \sim \Phi'\sigma'$, we have that $u_1\sigma = u_2\sigma$ (resp. $u'_1\sigma' \neq u'_2\sigma'$) and this allows us to conclude.

The case of the rule EQ-FRAME-DED can be done in a similar way.

Rule EQ-DED-DED: We know that $(\sigma', \theta') \in \mathsf{Sol}(\mathcal{C}')$, and thus we have $X\theta'(\Phi'\sigma')\downarrow = u'\sigma'$ and for all $Y \in vars^2(\xi)$, $Y\theta'(\Phi'\sigma')\downarrow = w'\sigma'$ where $(Y, k \vdash^? w') \in D(\mathcal{C}')$. Hence, by construction of v', we deduce that $\xi\theta'(\Phi'\sigma')\downarrow = v'\sigma'$. Moreover, thanks to Item 1, we have that $(\sigma, \theta') \in \mathsf{Sol}(\mathcal{C})$. Similarly, this implies that $X\theta'(\Phi\sigma)\downarrow = u\sigma$ and $\xi\theta'(\Phi\sigma)\downarrow = v\sigma$. We do a case analysis on i.

Case $i = 1$*:* In such a case, $\theta' \vDash E_\Pi(\mathcal{C}'_i)$ and so $\theta' \vDash X =^? \xi$. Thus it remains to prove that $\sigma' \vDash u' =^? v'$. But, we know that $\Phi\sigma \sim \Phi'\sigma'$ and we have that $\sigma \vDash u =^? v$. Thus, we can deduce that $\xi\theta'(\Phi'\sigma')\downarrow = X\theta'(\Phi'\sigma')\downarrow$ and so $\sigma' \vDash u' =^? v'$.

Case $i = 2$*:* In such a case, we only have to prove that $u'\sigma' \neq v'\sigma'$. We know that $u\sigma \neq v\sigma$ which implies that $X\theta'(\Phi\sigma)\downarrow \neq \xi\theta'(\Phi\sigma)\downarrow$. But we have $\Phi\sigma \sim \Phi'\sigma'$ hence

$X\theta'(\Phi\sigma)\downarrow \neq \xi\theta'(\Phi\sigma)\downarrow$ implies $X\theta'(\Phi'\sigma')\downarrow \neq \xi\theta'(\Phi'\sigma')\downarrow$ and so $u'\sigma' \neq v'\sigma'$. This allow us to conclude.

Rule DED-ST : Since $(\sigma_i, \theta') \in \mathsf{Sol}(\mathcal{C}_i)$, we know that $\xi\theta'(\Phi\sigma_i)\downarrow = u\sigma_i$ and depending on the value of i, the constraints added on $\mathcal{C}_i$ indicates whether there exists $\xi_1, \ldots, \xi_n \in \Pi_r$ such that $\mathsf{f}(\xi_1, \ldots, \xi_n)\Phi\sigma\downarrow = \xi\theta'(\Phi\sigma)\downarrow$, or not. But once again, since we have $\Phi\sigma \sim \Phi'\sigma'$ by hypothesis, we can transfer this property on σ'. This allows us to conclude. □

Appendix E. Soundness and completeness at the matrices level

Using the lemmas 5, 42 and 45, we now establish completeness and soundness at the matrices level.

Lemma 46. *Let $\mathcal{V}$, $\mathcal{V}'$ be two row matrices of constraint systems obtained by following the strategy. Let* RULE($\tilde{p}$) *be a transformation rule applicable on $(\mathcal{V}, \mathcal{V}')$. Let $(\mathcal{W}_1, \mathcal{W}_1')$ and $(\mathcal{W}_2, \mathcal{W}_2')$ be the two resulting pairs of row matrices of constraints systems obtained by the application of* RULE($\tilde{p}$).

$$\mathcal{W}_1 \approx_s \mathcal{W}_1' \text{ and } \mathcal{W}_2 \approx_s \mathcal{W}_2' \text{ is equivalent to } \mathcal{V} \approx_s \mathcal{V}'$$

Proof. We prove the two directions of the equivalence separately. We assume w.l.o.g. that $\mathcal{V}$ (resp. $\mathcal{V}'$) is a row matrix of size n (resp. n'). Let $\mathcal{V} = [\mathcal{C}_1, \ldots, \mathcal{C}_n]$ and $\mathcal{V}' = [\mathcal{C}_1' \ldots, \mathcal{C}_{n'}']$. We know that $\mathcal{W}_1$ and $\mathcal{W}_2$ (resp. $\mathcal{W}_1'$ and $\mathcal{W}_2'$) are row matrices of size n (resp. n'). Let $\mathcal{W}_i = [\mathcal{C}_1^i, \ldots, \mathcal{C}_n^i]$ and $\mathcal{W}_i' = [\mathcal{C}_1'^i, \ldots, \mathcal{C}_{n'}'^i]$ for $i = 1, 2$.

Let $1 \leq j \leq n$ and $1 \leq k \leq n'$. We denote by Φ_j the frame associated to $\mathcal{C}_j$ and by Φ_k' the frame associated to $\mathcal{C}_k'$. Let $i \in \{1, 2\}$. Similarly, we denote by Φ_j^i the frame associated to $\mathcal{C}_j^i$ and by $\Phi_k'^i$ the frame associated to $\mathcal{C}_k'^i$.

Right implication: Let $1 \leq j \leq n$ and let $(\sigma, \theta) \in \mathsf{Sol}(\mathcal{C}_j)$. By Lemma 42, we know that there exists θ', $i \in \{1, 2\}$ and σ_i such that $(\sigma_i, \theta') \in \mathsf{Sol}(\mathcal{C}_j^i)$ and $\sigma|_{S_1(\mathcal{C}_j)} = \sigma_i|_{S_1(\mathcal{C}_j)}$. By hypothesis, we have that $W_i \approx_s W_i'$. Hence, there exist $1 \leq k \leq n'$ and a substitution σ_i' such that $(\sigma_i', \theta') \in \mathsf{Sol}(\mathcal{C}_k'^i)$ and $\Phi_j^i\sigma_i \sim \Phi_k'^i\sigma_i'$. Thanks to Lemma 5, we deduce that:

$$(\sigma_i|_{vars^1(\mathcal{C}_j)}, \theta'|_{vars^2(\mathcal{C}_j)}) \in \mathsf{Sol}(\mathcal{C}_j) \text{ and } (\sigma_i'|_{vars^1(\mathcal{C}_k')}, \theta'|_{vars^2(\mathcal{C}_k')}) \in \mathsf{Sol}(\mathcal{C}_k').$$

with $\mathsf{Init}(\Phi_j^i)\sigma_i = \mathsf{Init}(\Phi_j)\sigma_i|_{vars^1(\mathcal{C}_j)}$ and $\mathsf{Init}(\Phi_k'^i)\sigma_i' = \mathsf{Init}(\Phi_k')\sigma_i'|_{vars^1(\mathcal{C}_k')}$. Note that $\theta'|_{vars^2(\mathcal{C}_k')} = \theta'|_{vars^2(\mathcal{C}_j)}$ since $\mathcal{C}_k'$ and $\mathcal{C}_j$ have the same structure. Moreover, by hypothesis, we have that $\sigma = \sigma_i|_{vars^1(\mathcal{C}_j)}$. Thus, we can apply Lemma 45 on $\mathcal{C}_j$ and $\mathcal{C}_k'$. Since $(\sigma, \theta) \in \mathsf{Sol}(\mathcal{C}_j)$, we deduce that $(\sigma', \theta) \in \mathsf{Sol}(\mathcal{C}_k')$ where $\sigma' = \sigma_i'|_{vars^1(\mathcal{C}_k')}$. Lastly, since $\Phi_j^i\sigma_i \sim \Phi_k'^i\sigma_i'$, $\mathsf{Init}(\Phi_j^i)\sigma_i = \mathsf{Init}(\Phi_j)\sigma$ and $\mathsf{Init}(\Phi_k'^i)\sigma_i' = \mathsf{Init}(\Phi_k')\sigma'$, we easily deduce that $\Phi_j\sigma \sim \Phi_k'\sigma'$. The other implication can be done in a similar way.

Left implication: Let $1 \leq j \leq n$, $i \in \{1, 2\}$ and let $(\sigma_i, \theta') \in \mathsf{Sol}(\mathcal{C}_j^i)$. By Lemma 5, we know that there exists σ and θ such that $(\sigma, \theta) \in \mathsf{Sol}(\mathcal{C}_j)$ with $\sigma = \sigma_i|_{vars^1(\mathcal{C}_j)}$ and $\theta = \theta'|_{vars^2(\mathcal{C}_j)}$. By hypothesis, we have that $V \approx_s V'$. Hence, there exists $1 \leq k \leq n'$ and a substitution σ' such that $(\sigma', \theta) \in \mathsf{Sol}(\mathcal{C}_k')$ and $\Phi_j\sigma \sim \Phi_k'\sigma'$. Thus, we can apply Lemma 45 (second item) on $\mathcal{C}_j$ and $\mathcal{C}_k'$. Since $(\sigma_i, \theta') \in \mathsf{Sol}(\mathcal{C}_j^i)$, we deduce that $(\sigma_i', \theta') \in \mathsf{Sol}(\mathcal{C}_k'^i)$ for some substitution σ_i' such that $\sigma' = \sigma_i'|_{vars^1(\mathcal{C}_k')}$. Moreover, we have that

$\mathsf{Init}(\Phi^i_j)\sigma_i = \mathsf{Init}(\Phi_j)\sigma$ and $\mathsf{Init}(\Phi'^i_k)\sigma'_i = \mathsf{Init}(\Phi'_k)\sigma'$. Since $\Phi_j\sigma \sim \Phi'_k\sigma'$, we easily deduce that $\Phi^i_j\sigma_i \sim \Phi'^i_k\sigma'_i$. The other implication can be done in a similar way. □

Theorem 2. *[soundness and completeness for internal rules] Let $\mathcal{M}_1$, $\mathcal{M}'_1$ be two matrices of constraint systems obtained from a pair of sets of initial constraint systems by following the strategy $\mathcal{S}$. Let* RULE$(\tilde{p})$ *be an internal transformation rule applicable on $(\mathcal{M}_1, \mathcal{M}'_1)$ on the i^{th} row. Let $(\mathcal{M}_2, \mathcal{M}'_2)$ be the resulting pair of matrices of constraint systems obtained by the application of* RULE$(\tilde{p})$*. We have that:*

$$\mathcal{M}_2 \approx_s \mathcal{M}'_2 \text{ is equivalent to } \mathcal{M}_1 \approx_s \mathcal{M}'_1$$

Proof. Since $\mathcal{M}_1$ and $\mathcal{M}'_1$ have the same structure, we know that they have the same number of lines, say m. Let $\mathcal{M}_1 = [\mathcal{V}_1, \ldots, \mathcal{V}_m]$ and $\mathcal{M}'_1 = [\mathcal{V}'_1, \ldots, \mathcal{V}'_m]$. Let $(\mathcal{W}_1, \mathcal{W}'_1)$ and $(\mathcal{W}_2, \mathcal{W}'_2)$ be the two resulting pairs of row matrices of constraint systems obtained by applying RULE$(\tilde{p})$ on $(\mathcal{V}_i, \mathcal{V}'_i)$. Hence $\mathcal{M}_2 = [\mathcal{V}_1, \ldots, \mathcal{V}_{i-1}, \mathcal{W}_1, \mathcal{W}_2, \mathcal{V}_{i+1}, \ldots, \mathcal{V}_m]$, and $\mathcal{M}'_2 = [\mathcal{V}'_1, \ldots, \mathcal{V}'_{i-1}, \mathcal{W}'_1, \mathcal{W}'_2, \mathcal{V}'_{i+1}, \ldots, \mathcal{V}'_m]$.

By Definition 13 of the symbolic equivalence of matrices of constraint systems, we have that $\mathcal{M}_1 \approx_s \mathcal{M}'_1$ is equivalent to $\mathcal{V}_j \approx_s \mathcal{V}'_j$ for every $j \in \{1, \ldots, m\}$. Thanks to Proposition 46, we easily deduce that $\mathcal{V}_i \approx_s \mathcal{V}'_i$ is equivalent to $\mathcal{W}_1 \approx_s \mathcal{W}'_1$ and $\mathcal{W}_2 \approx_s \mathcal{W}'_2$. This allows us to conclude. □

Theorem 3. *[soundness and completeness for external rules] Let $\mathcal{M}$, $\mathcal{M}'$ be two matrices of constraint systems obtained from a pair of sets of initial constraint systems by following the strategy $\mathcal{S}$. Let* RULE$(\tilde{p})$ *be an external transformation rule applicable on $(\mathcal{M}, \mathcal{M}')$. Let $(\mathcal{M}_1, \mathcal{M}'_1)$ and $(\mathcal{M}_2, \mathcal{M}'_2)$ be the two resulting pairs of matrices of constraint systems obtained by the application of* RULE$(\tilde{p})$*. We have that:*

$$\mathcal{M}_1 \approx_s \mathcal{M}'_1 \text{ and } \mathcal{M}_2 \approx_s \mathcal{M}'_2 \text{ is equivalent to } \mathcal{M} \approx_s \mathcal{M}'$$

Proof. Since $\mathcal{M}$ and $\mathcal{M}'$ have the same structure, we know that they have the same number of lines, say m. Let $\mathcal{M} = [\mathcal{V}_1, \ldots, \mathcal{V}_m]$ and $\mathcal{M}' = [\mathcal{V}'_1, \ldots, \mathcal{V}'_m]$. When RULE$(\tilde{p})$ is applicable on $(\mathcal{V}_i, \mathcal{V}'_i)$, let $(\mathcal{W}_{i,1}, \mathcal{W}'_{i,1})$ and $(\mathcal{W}_{i,2}, \mathcal{W}'_{i,2})$ be the two resulting pairs of row matrices of constraint system. Otherwise, let $(\mathcal{W}_{i,1}, \mathcal{W}'_{i,1}) = (\bot, \bot)$ and $(\mathcal{W}_{i,2}, \mathcal{W}'_{i,2}) = (\mathcal{V}_i, \mathcal{V}'_i)$. We have that:

- $\mathcal{M}_1 = [\mathcal{W}_{1,1}, \ldots, \mathcal{W}_{m,1}]$, $\mathcal{M}'_1 = [\mathcal{W}'_{1,1}, \ldots, \mathcal{W}'_{m,1}]$, and
- $\mathcal{M}_2 = [\mathcal{W}_{1,2}, \ldots, \mathcal{W}_{m,2}]$, $\mathcal{M}'_2 = [\mathcal{W}'_{1,2}, \ldots, \mathcal{W}'_{m,2}]$.

By Definition 13 of the symbolic equivalence of matrices of constraint systems, we have that $\mathcal{M} \approx_s \mathcal{M}'$ is equivalent to $\mathcal{V}_i \approx_s \mathcal{V}'_i$ for every $i \in \{1, \ldots, m\}$. Relying on Proposition 46 when the rule is effectively applied on $(\mathcal{V}_i, \mathcal{V}'_i)$ (when the rule is not applicable, the result trivially holds), we deduce that for every i, $\mathcal{V}_i \approx_s \mathcal{V}'_i$ is equivalent to $\mathcal{W}_{i,1} \approx_s \mathcal{W}'_{i,1}$ and $\mathcal{W}_{i,2} \approx_s \mathcal{W}'_{i,2}$ which is equivalent to $\mathcal{M}_1 \approx_s \mathcal{M}'_1$ and $\mathcal{M}_2 \approx_s \mathcal{M}'_2$. This allows us to conclude. □

Appendix F. Soundness and completeness of LeafTest

The purpose of this appendix is to establish the following result.

Theorem 4. *Let $(\mathcal{M}_0, \mathcal{M}'_0)$ be a pair of sets of initial constraint systems and $(\mathcal{M}, \mathcal{M}')$ be a leaf of the tree whose root is labeled with $(\mathcal{M}_0, \mathcal{M}'_0)$ and which is obtained following the strategy $\mathcal{S}$. We have that $\mathcal{M} \approx_s \mathcal{M}'$ if, and only if,* $\mathsf{LeafTest}(\mathcal{M}, \mathcal{M}') = \mathsf{true}$.

First, we will show that the pairs of matrices obtained at the leaves satisfy some nice properties (see Appendix F.1). Then, we will see that there is a need for a special treatment to deal with non-deducibility constraints, and this is explained in Appendix F.2. In Appendix F.3, we show that any constraint system obtained at the end (and which is different from $\bot$) has a solution, and we conclude by establishing Theorem 4.

Appendix F.1. Shape of the leaves

Following the idea developed *e.g.* in [25], the purpose of our transformation rules is to transform constraint systems until reaching constraint systems that are in *solved form*. Solved constraint systems enjoy some nice properties, *e.g.* they have a solution, and they are therefore convenient to decide satisfiability. In order to be able to decide symbolic equivalence between sets of constraint systems, we have to consider a slightly different notion of solved form and we have also to lift this notion at the matrix level.

Definition 20. *A well-formed constraint system $\mathcal{C} = (S_1; S_2; \Phi; D; E; E_\Pi; ND; \mathsf{NoUse})$ is* solved *(or in* solved form*) if:*

1. *$\mathcal{C}$ satisfies the invariants* $\mathsf{InvVarConstraint}(\mathsf{s}_{max})$, $\mathsf{InvNoUse}(\mathsf{s}_{max})$, $\mathsf{InvVarFrame}(\mathsf{s}_{max})$, $\mathsf{InvDest}(\mathsf{s}_{max})$, *and* $\mathsf{InvDedsub}$*;*
2. *E is a formula of the form $\bigwedge_k u_k =^? v_k \bigwedge_i [\bigvee_j x_{i,j} \neq^? w_{i,j}]$ where $w_{i,j} \in \mathcal{T}(\mathcal{F}_c, \mathcal{X}^1)$, $x_{i,j} \in \mathcal{X}^1$, and $u_k, v_k \in \mathcal{T}(\mathcal{F}_c, \mathcal{N} \cup \mathcal{X}^1)$.*
3. *for all $X \in vars^2(D)$, for all $\mathsf{f} \in \mathcal{F}_c$, for all $\xi, i \rhd u$ in Φ, we have that $E_\Pi \not\vdash X \neq^? \xi$ and $E_\Pi \not\vdash \mathsf{root}(X) \neq^? \mathsf{f}$.*

By convention, the constraint system $\bot$ is in solved formed.

Property 2 ensures that disequations do not involve names so that it will be possible to produce similar disequations on other constraint systems. Property 3 allows us to ensure that each deducibility constraint would be satisfied by considering any recipe made up of contructors above elements occurring in the frame Φ. As expected, we then need to lift the notion of solved form at the matrix level.

Definition 21. *We say that a pair $(\mathcal{M}, \mathcal{M}')$ is in* solved form *if all the constraint systems in this pair are in solved form, and $(\mathcal{M}, \mathcal{M}')$ satisfies* $\mathsf{InvMatrix}(\mathsf{s}_{max})$ *as well as* $\mathsf{InvGeneral}$*. Moreover, we have that:*
for all constraint systems $\mathcal{C}$, $\mathcal{C}'$ on the same column, there exists a variable renaming $\rho : \mathcal{X}^1 \setminus S_1(\mathcal{C}) \to \mathcal{X}^1 \setminus S_1(\mathcal{C}')$ such that:

1. *$\mathsf{mgu}(E(\mathcal{C}))_{|S_1(\mathcal{C})}\rho = \mathsf{mgu}(E(\mathcal{C}'))_{|S_1(\mathcal{C}')}$, and $D(\mathcal{C})\rho = D(\mathcal{C}')$;*
2. *$\{(u\rho, u') \mid (\xi, i \rhd u) \in \Phi \wedge (\xi', i' \rhd u') \in \Phi' \wedge \mathsf{path}(\xi) = \mathsf{path}(\xi')\}$ is included in $\{(u, u) \mid u \in \mathcal{T}(\mathcal{F}_c, \mathcal{N} \cup \mathcal{X}^1)\}$;*

for all constraint systems $\mathcal{C}$, $\mathcal{C}'$ in $(\mathcal{M}, \mathcal{M}')$, there exists a variable renaming $\rho : \mathcal{X}^1 \to \mathcal{X}^1$ such that:

3. *$E(\mathcal{C})\rho$ restricted to inequations is equal to $E(\mathcal{C}')$ restricted to inequations, and $D(\mathcal{C})\rho$ is equal to $D(\mathcal{C}')$.*

The two first properties of Definition 21 focus on the messages inside the constraint systems. Intuitively, Properties 1 and 2 will help us to prove that all the constraint systems have the same set of first-order solutions. To understand why these properties hold, we need to come back to the creation of new rows in a matrix of constraint systems, and so to the application of internal rules. In Subsection 3.4, we describe the application of internal rules as a way to keep the result of the guesses on static equivalence inside a single matrix. Thus, it is natural that the first-order solutions of different constraint systems in a same column are the same.

Property 3 indicates that there exists a matching on the inequations of message for all constraint systems on a same row. The purpose of this property is for us to prove that any substitution satisfying the inequations in one constraint systems will be match by an other first-order substitution that satisfies the inequations in an other constraint system.

Lemma 47. *Let $(\mathcal{M}_0, \mathcal{M}'_0)$ be a pair of sets of initial constraint systems and $(\mathcal{M}, \mathcal{M}')$ be a leaf of the tree whose root is labeled with $(\mathcal{M}_0, \mathcal{M}'_0)$ and which is obtained following the strategy $\mathcal{S}$. We have that $(\mathcal{M}, \mathcal{M}')$ is in solved form.*

Proof. We have that there exist $(\mathcal{M}_1, \mathcal{M}'_1)$ and $(\mathcal{M}_2, \mathcal{M}'_2)$ such that:

$$(\mathcal{M}_0, \mathcal{M}'_0) \to^* (\mathcal{M}_1, \mathcal{M}'_1) \to^* (\mathcal{M}_2, \mathcal{M}'_2) \to^* (\mathcal{M}, \mathcal{M}')$$

where:

- $(\mathcal{M}_1, \mathcal{M}'_1)$ is obtained at the end of Phase 1 of the strategy; and
- $(\mathcal{M}_2, \mathcal{M}'_2)$ is obtained at the end of Step a of Phase 2 of the strategy.

Thanks to Lemma 27, we know that $(\mathcal{M}_1, \mathcal{M}'_1)$ satisfies PP1E. Hence, any constraint system occurring in $\mathcal{M}_1$ or $\mathcal{M}'_1$ satisfies InvDedsub, InvVarFrame(s_{max}), InvDest(s_{max}), InvNoUse(s_{max}), InvUntouched(s_{max}) and InvVarConstraint(s_{max}). The rules applied on Phase 2 are instances of Cons, Eq-ded-ded and Axiom. Hence thanks to Lemma 11, we deduce that any constraint system in $(\mathcal{M}, \mathcal{M}')$ satisfies InvNoUse(s_{max}), InvDest(s_{max}), InvVarFrame(s_{max}) and InvDedsub. Moreover by Lemma 10, we deduce that any constraint system in $(\mathcal{M}, \mathcal{M}')$ satisfies InvUntouched(s_{max}). At last, by Lemma 9, we deduce that any constraint system in $(\mathcal{M}, \mathcal{M}')$ also satisfies InvVarConstraint(s_{max}).

Since $(\mathcal{M}_1, \mathcal{M}'_1)$ satisfies PP1E, we deduce that $(\mathcal{M}, \mathcal{M}')$ satisfies InvMatrix(s_{max}) and InvGeneral. Hence thanks to Lemma 12 and 14, we deduce that $(\mathcal{M}, \mathcal{M}')$ also satisfies InvMatrix(s_{max}) and InvGeneral.

Let $\mathcal{C}$ be a constraint system occurring in $\mathcal{M}$ or $\mathcal{M}'$ that is different from $\bot$. The pair $(\mathcal{M}, \mathcal{M}')$ being obtained at the end of the strategy implies that the rule Cons and Axiom are not applicable on any constraint system in $\mathcal{M}, \mathcal{M}'$. Hence we deduce that either Property 3 holds or there exists $X \in vars^2(D(\mathcal{C}))$ such that Axiom(X, path) and Cons(X, f) are useless for all path, f. But we know that $\mathcal{C}$ satisfies InvDest(s_{max}). Hence Dest$(\xi, \ell \to r, s)$ is useless for any $\xi, \ell \to r, s$. This case is impossible since $\mathcal{C}$ is normalised and we know that $\mathcal{C} \neq \bot$. Hence, we deduce that Property 3 holds on $\mathcal{C}$.

We now show the properties 1 and 2 that has to be satisfied by any pair $(\mathcal{M}, \mathcal{M}')$ of matrices in solved form. If we assumed that $\mathcal{C}$ and $\mathcal{C}'$ was in the same column. We know that $(\mathcal{M}, \mathcal{M}')$ satisfies the invariant $\mathsf{InvGeneral}$ and $\mathcal{C}, \mathcal{C}'$ both satisfy $\mathsf{InvVarConstraint}(\mathsf{s}_{max})$ and $\mathsf{InvUntouched}(\mathsf{s}_{max})$. Hence by Lemma 25, we deduce that the properties 1, 2 hold.

It remains to show property 2 of solved constraint system and property 3 of solved pair of matrices. Thanks to Lemma 29, we know that $(\mathcal{M}_2, \mathcal{M}'_2)$ does not contain universal variables. But the rules Cons, Axiom and Eq-ded-ded do not add new universal variable. Hence $(\mathcal{M}, \mathcal{M}')$ does not contain universal variables. $(\mathcal{M}, \mathcal{M}')$ being at the end of the strategy implies that the rule Axiom, Cons and Eq-ded-ded are no longer applicable. Consider $\mathcal{C}$ a constraint system in $(\mathcal{M}, \mathcal{M}')$.

Let $\bigvee_{i=1}^{n} u_i \neq^? v_i$ such that $E(\mathcal{C}) = E \wedge \bigvee_i u_i \neq^? v_i$ for some E. Thanks to Lemma 30, we know that either $n = 1$, $u_1 \in \mathcal{X}^1$, v_1 does not contain any names and $\mathcal{L}^1_{\mathcal{C}}(v_1) \leq \mathcal{L}^1_{\mathcal{C}}(u_1)$; or for all $i \in \{1, \ldots, n\}$, $u_i \neq^? v_i$ satisfies one of the following properties:

1. $u_i \in \mathcal{X}^1$ and $v_i \in \mathcal{N}$: In such a case, there exists $(X, k \vdash^? u_i) \in D$. But Axiom$(X, \mathsf{path})$ is useless for any path. Since $\mathcal{C}$ satisfies $\mathsf{InvDest}(\mathsf{s}_{max})$, Dest$(\xi, \ell \to r, s)$ is useless for any $\xi, \ell \to r, s$. But in such a case, a normalisation rule is applicable which is a contradiction with the fact that $\mathcal{C}$ is normalised. Hence this case is impossible.

2. $u_i, v_i \in \mathcal{X}^1$, $E_\Pi(\mathcal{C}) \not\vDash \mathsf{root}(X) \neq^? \mathsf{f}$ and $E_\Pi(\mathcal{C}) \vDash \mathsf{root}(Y) \neq^? \mathsf{g}$, for all $\mathsf{f}, \mathsf{g} \in \mathcal{F}_c$, where $(X, p \vdash^? u_i), (Y, q \vdash^? v_i) \in D(\mathcal{C})$: In such a case, for all $\mathsf{g} \in \mathcal{F}_c$, $E_\Pi(\mathcal{C}) \vDash \mathsf{root}(Y) \neq^? \mathsf{g}$ implies that Cons(Y, g) is useless. But Axiom(Y, path) is not applicable and $E_\Pi(\mathcal{C}) \vDash \mathsf{root}(Y) \neq^? \mathsf{g}$ implies that Axiom(Y, path) is useless for all path. Since $\mathcal{C}$ satisfies $\mathsf{InvDest}(\mathsf{s}_{max})$, Dest$(\xi, \ell \to r, s)$ is useless for any $\xi, \ell \to r, s$. But in such a case, a normalisation rule is applicable which is a contradiction with the fact that $\mathcal{C}$ is normalised. Hence this case is impossible.

3. $u_i \in \mathcal{X}^1$, $\mathsf{root}(v_i) \in \mathcal{F}_c$ and for all $\mathsf{f} \in \mathcal{F}_c$, $E_\Pi(\mathcal{C}) \vDash \mathsf{root}(X) \neq^? \mathsf{f}$, where $(X, p \vdash^? u_i) \in D(\mathcal{C})$: Since for all $\mathsf{f} \in \mathcal{F}_c$, $E_\Pi(\mathcal{C}) \vDash \mathsf{root}(X) \neq^? \mathsf{f}$, then similarly to the previous case, we prove that this case is impossible.

Since all cases are impossible, we can deduce that $n = 1$, $u_1 \in \mathcal{X}^1$, v_1 does not contain any names and $\mathcal{L}^1_{\mathcal{C}}(v_1) \leq \mathcal{L}^1_{\mathcal{C}}(u_1)$. Note that this already allows us to show Property 2. Lastly, by applying the same reasoning as above, the rules Axiom and Cons not being applicable allows us to prove that for all $\mathsf{g} \in \mathcal{F}_c$, $E_\Pi(\mathcal{C}) \not\vDash \mathsf{root}(X) \neq^? \mathsf{g}$ where $(X, i \vdash^? u_1) \in D(\mathcal{C})$, and if $v_1 \in \mathcal{X}^1$ then for all $\mathsf{g} \in \mathcal{F}_c$, $E_\Pi(\mathcal{C}) \not\vDash \mathsf{root}(Y) \neq^? \mathsf{g}$ where $(Y, j \vdash^? v_1) \in D(\mathcal{C})$. But Eq-ded-ded is not applicable. In particular, it is not applicable with parameter X and ξ where $\xi\delta^1(\mathcal{C}) = v_1$. However, the applications conditions of Figure 2 are satisfied for the rule Eq-ded-ded(X, ξ). Therefore, we deduce that Eq-ded-ded(X, ξ) is useless and so for all constraint system $\mathcal{C}'$ in $\mathcal{M}$ or $\mathcal{M}'$, we deduce that $E(\mathcal{C}') \vDash X\delta^1(\mathcal{C}') \neq^? \xi\delta^1(\mathcal{C}')$. This allows us to conclude that Property 3 of solved pair of matrices is satisfied by $(\mathcal{M}, \mathcal{M}')$. □

Appendix F.2. Dealing with the non-deducibility constraints

We may note that, due to the presence of non-deducibility constraints, systems in solved form are not trivially satisfiable. However, as explain in Section 4, our strategy

was specifically designed to take care of non-deducibility constraints (Step e in Phase 1). Actually, we only kept the constraint systems whose non-deducibility constraints could be satisfied. More precisely, we show that we do not need to take care of deducibility constraint to decide whether a constraint system obtained at the end (on a leaf) admits a solution.

Lemma 48. *Let $\mathcal{M}$ be matrix of constraint systems obtained by following the strategy. Let $\mathcal{C}$ and $\mathcal{C}'$ be two constraint systems from the same column in $\mathcal{M}$. Let $(\sigma, \theta) \in \mathsf{Sol}(\overline{\mathcal{C}})$ and $(\sigma', \theta') \in \mathsf{Sol}(\overline{\mathcal{C}'})$ such that $\sigma_{|S_1(\mathcal{C})} = \sigma'_{|S_1(\mathcal{C}')}$. We have that:*

1. $\mathsf{Init}(\Phi(\mathcal{C}))\sigma = \mathsf{Init}(\Phi(\mathcal{C}'))\sigma'$;
2. *for all $(\xi, i \rhd u) \in \Phi(\mathcal{C})$, for all $(\xi', i' \rhd u') \in \Phi(\mathcal{C}')$, if $\mathsf{path}(\xi) = \mathsf{path}(\xi')$ then $u\sigma = u'\sigma'$;*
3. *for all $X \in S_2(\mathcal{C}) = S_2(\mathcal{C}')$, if $(X, i \vdash^? u) \in D(\mathcal{C})$ and $(X, i \vdash^? u') \in D(\mathcal{C}')$, then $u\sigma = u'\sigma'$.*

Proof. Since $\mathcal{C}$ and $\mathcal{C}'$ are both from the same column of $\mathcal{M}$, we deduce that they have at least one common ancestor. Let $\mathcal{C}_0$ be the constraint system on the row matrix of initial constraint system such that $\mathcal{C}_0 \to^* \mathcal{C}$ and $\mathcal{C}_0 \to^* \mathcal{C}'$.

Property 1: Let $u, u' \in \mathcal{T}(\mathcal{F}_c, \mathcal{N} \cup \mathcal{X}^1)$ such that $(ax_i, i \rhd u) \in \Phi(\mathcal{C})$ and $(ax_i, i \rhd u') \in \Phi(\mathcal{C}')$, for some i. Furthermore let $u_0 \in \mathcal{T}(\mathcal{F}_c, \mathcal{N} \cup \mathcal{X}^1)$ such that $(ax_i, i \rhd u_0) \in \Phi(\mathcal{C}_0)$.

Since $\mathcal{C}_0 \to^* \mathcal{C}$ and $\mathcal{C}_0 \to^* \mathcal{C}'$, we obtain from Lemma 7 that $u = u_0\Sigma$ and $u' = u_0\Sigma'$ where $\Sigma = \mathsf{mgu}(E)$, $\Sigma' = \mathsf{mgu}(E')$. But $(\sigma, \theta) \in \mathsf{Sol}(\overline{\mathcal{C}})$ implies that $\sigma \vDash E(\mathcal{C})$ and so there exists σ_0 such that $\sigma = \Sigma\sigma_0$. Similarly, there exists σ'_0 such that $\sigma' = \Sigma'\sigma'_0$. Moreover, u_0 is a term in the initial constraint system $\mathcal{C}_0$, hence $vars^1(u_0) \subseteq S_1(\mathcal{C}_0) = S_1(\mathcal{C}) = S_1(\mathcal{C}')$ which also implies that $u_0\sigma_{|S_1(\mathcal{C})} = u_0\sigma$ and $u_0\sigma'_{|S_1(\mathcal{C}')} = u_0\sigma'$. At last, by applying the hypothesis $\sigma_{|S_1(\mathcal{C})} = \sigma'_{|S_1(\mathcal{C}')}$, which leads to $u_0\sigma = u_0\sigma'$. Hence, we have that:

$$u\sigma = u_0\Sigma(\Sigma\sigma_0) = u_0\sigma = u_0\sigma' = u\Sigma'(\Sigma'\sigma'_0) = u'\sigma'.$$

Property 2: Let $(\xi, i \rhd u) \in \Phi(\mathcal{C})$ and $(\xi', i' \rhd u') \in \Phi(\mathcal{C}')$. We know that $\mathcal{C}$ and $\mathcal{C}'$ are well-formed constraint systems. Thanks to Property 5 of a well-formed constraint system and the fact that $(\sigma, \theta) \in \mathsf{Sol}(\overline{\mathcal{C}})$ and $(\sigma', \theta') \in \mathsf{Sol}(\overline{\mathcal{C}'})$, we deduce that $\xi\theta(\Phi(\mathcal{C})\sigma)\downarrow = u\sigma$ and $\xi'\theta'(\Phi(\mathcal{C}')\sigma')\downarrow = u'\sigma'$. We have seen that $\mathsf{Init}(\Phi(\mathcal{C})\sigma = \mathsf{Init}(\Phi(\mathcal{C}'))\sigma'$. We have assumed that $\mathsf{path}(\xi) = \mathsf{path}(\xi')$, and we know that $u\sigma, u'\sigma' \in \mathcal{T}(\mathcal{F}_c, \mathcal{N})$. Hence we can apply Lemma 33 which leads to $\xi\theta(\Phi(\mathcal{C})\sigma)\downarrow = \xi'\theta'(\Phi(\mathcal{C}')\sigma')\downarrow$ and so $u\sigma = u'\sigma'$.

Property 3: Let $X \in S_2(\mathcal{C}) = S_2(\mathcal{C}')$. There exists $Y \in S_2(\mathcal{C}_0)$ such that $X \in vars^2(\mathsf{C}\lfloor Y\Theta \rfloor_{\Phi(\mathcal{C})})$ where $\Theta = \mathsf{mgu}(E_\Pi(\mathcal{C}))$. Let $\Theta' = \mathsf{mgu}(E_\Pi(\mathcal{C}'))$, $\Sigma = \mathsf{mgu}(E(\mathcal{C}))$ and $\Sigma' = \mathsf{mgu}(E(\mathcal{C}'))$. By applying Lemma 6 on Y, we have that $Y\delta^1(\mathcal{C}_0)\Sigma = \mathsf{C}\lfloor Y\Theta \rfloor_{\Phi(\mathcal{C})}\delta^1(\mathcal{C})$.

But $(\sigma, \theta) \in \mathsf{Sol}(\overline{\mathcal{C}})$ implies that $\sigma \models E(\mathcal{C})$ and so there exists σ_0 such that $\sigma = \Sigma\sigma_0$, and $\delta^1(\mathcal{C})\sigma = \delta^1(\mathcal{C})\sigma_0$ since $\mathcal{C}$ is normalised. Hence, $Y\delta^1(\mathcal{C}_0)\sigma = \mathsf{C}\lfloor Y\Theta \rfloor_{\Phi(\mathcal{C})}\delta^1(\mathcal{C})\sigma_0 = \mathsf{C}\lfloor Y\Theta \rfloor_{\Phi(\mathcal{C})}\delta^1(\mathcal{C})\sigma$. Similarly, we have that $Y\delta^1(\mathcal{C}_0)\sigma' = \mathsf{C}\lfloor Y\Theta' \rfloor_{\Phi(\mathcal{C}')}\delta^1(\mathcal{C}')\sigma'$.

Our inductive hypothesis tells us that $\sigma_{|S_1} = \sigma'_{|S_1}$ which implies that $\delta^1(\mathcal{C}_0)\sigma = \delta^1(\mathcal{C}_0)\sigma'$. Furthermore, $\mathcal{M}$ satisfies $\mathsf{InvGeneral}$, hence for all $Z \in S_2(\mathcal{C}) = S_2(\mathcal{C}')$, $\mathsf{C}\lfloor Z\Theta \rfloor_{\Phi(\mathcal{C})} = \mathsf{C}\lfloor Z\Theta' \rfloor_{\Phi(\mathcal{C}')}$. Since $Y \in S_2(\mathcal{C}_0)$ then $Y \in S_2(\mathcal{C})$ and so we deduce that

$\mathsf{C}\lfloor Y\Theta'\rfloor_{\Phi(\mathcal{C}')} = \mathsf{C}\lfloor Y\Theta\rfloor_{\Phi(\mathcal{C})}$. Hence, we deduce that $\mathsf{C}\lfloor Y\Theta\rfloor_{\Phi(\mathcal{C})}\delta^1(\mathcal{C})\sigma = \mathsf{C}\lfloor Y\Theta\rfloor_{\Phi(\mathcal{C})}\delta^1(\mathcal{C}')\sigma'$. Since $X \in vars^2(\mathsf{C}\lfloor Y\Theta\rfloor_{\Phi(\mathcal{C})})$, we can conclude that $X\delta^1(\mathcal{C})\sigma = X\delta^1(\mathcal{C}')\sigma'$ and so $u\sigma = u'\sigma'$. □

Lemma 49. *Let $(\mathcal{M}_0, \_)$ be a pair of sets of initial constraint systems, s be an integer, and $(\mathcal{M}, \_)$ (resp. $(\mathcal{M}_1, \_)$) be a pair obtained at the beginning (resp. end) of Step a of Phase* 1 *with support s, and such that $(\mathcal{M}_0, \_) \to^* (\mathcal{M}, \_) \to^* (\mathcal{M}_1, \_)$. Let $\mathcal{C}_1$ be a constraint system in $\mathcal{M}_1$. Assume that the constraint system $\mathcal{C}$ in $\mathcal{M}$ ancestor of $\mathcal{C}_1$ (denoted $\mathcal{C} \to^* \mathcal{C}_1$) satisfies $\mathsf{Sol}(\mathcal{C}) = \mathsf{Sol}(\overline{\mathcal{C}})$. Let $(\sigma, \theta) \in \mathsf{Sol}(\overline{\mathcal{C}_1})$ such that $(\sigma, \theta) \notin \mathsf{Sol}(\mathcal{C}_1)$. There exists a constraint system $\mathcal{C}'_1$ in $\mathcal{M}_1$ which is in the same column as $\mathcal{C}_1$, and such that:*

1. *$\mathcal{C}$ is ancestor of $\mathcal{C}'_1$,* i.e. *$\mathcal{C} \to^* \mathcal{C}'_1$;*
2. *$\{(\xi, i) \mid i < s \wedge (\xi, i \rhd u) \in \Phi(\mathcal{C}_1)\} = \{(\xi, i) \mid i < s \wedge (\xi, i \rhd u) \in \Phi(\mathcal{C}'_1)\}$;*
3. *$\{\mathsf{path}(\xi) \mid (\xi, s \rhd u) \in \Phi(\mathcal{C}_1)\} \subseteq \{\mathsf{path}(\xi) \mid (\xi, s \rhd u) \in \Phi(\mathcal{C}'_1)\}$;*
4. *$\{\mathsf{path}(\xi) \mid (\xi, s \rhd u) \in \mathsf{NoUse}(\mathcal{C}_1)\} = \{\mathsf{path}(\xi) \mid (\xi, s \rhd u) \in \mathsf{NoUse}(\mathcal{C}'_1)\} \cap \{\mathsf{path}(\xi) \mid (\xi, s \rhd u) \in \Phi(\mathcal{C}_1)\}$;*
5. *there exists $(\sigma', \theta') \in \mathsf{Sol}(\mathcal{C}'_1)$ such that $\sigma_{|S_1(\mathcal{C})} = \sigma'_{|S_1(\mathcal{C})}$.*

Proof. Let N be the length of the derivation $(\mathcal{M}, \_) \to^* (\mathcal{M}_1, \_)$. We prove this result by induction on N. According to the strategy, every application of the rule Dest or Eq-frame-ded implies the application of the same rule with the same parameters on each row of the matrix. Hence, for the induction, we assume that the sequence of applications of a rule Dest or Eq-frame-ded on each row is applied simultaneously.

Base case $N = 0$: In such a case, $\mathcal{M} = \mathcal{M}_1$, and therefore $\mathcal{C} = \mathcal{C}_1$, and $\mathsf{Sol}(\mathcal{C}_1) = \mathsf{Sol}(\overline{\mathcal{C}_1})$. By choosing $\mathcal{C}'_1 = \mathcal{C}_1 = \mathcal{C}$, properties 1, 2 and 3 trivially holds. Furthermore, since $\mathsf{NoUse}(\mathcal{C}'_1) \subseteq \Phi(\mathcal{C}'_1)$, property 4 holds. At last, by hypothesis we have $(\sigma, \theta) \in \mathsf{Sol}(\overline{\mathcal{C}_1})$ which implies that $(\sigma, \theta) \in \mathsf{Sol}(\mathcal{C}_1)$. With $\mathcal{C}_1 = \mathcal{C}'_1$, we conclude that $(\sigma, \theta) \in \mathsf{Sol}(\mathcal{C}'_1)$. Hence property 5 holds.

Inductive step $N > 0$: Let $\textsc{Rule}(\tilde{p})$ be the last rule applied. Let $\mathcal{M}_2$ be the matrix such that $\mathcal{M}_2 \to \mathcal{M}_1$ (note that since we are in Step a of the strategy, the rule applied is necessarily an internal rule) and let $\mathcal{C}_2$ be the constraint system in $\mathcal{M}_2$ ancestor of $\mathcal{C}_1$ (*i.e.* $\mathcal{C}_2 \to \mathcal{C}_1$). Thanks to Lemma 5, $(\sigma, \theta) \in \mathsf{Sol}(\overline{\mathcal{C}_1})$ implies that $(\sigma', \theta') \in \mathsf{Sol}(\overline{\mathcal{C}_2})$ with $\sigma'_{|S_1} = \sigma_{|S_1}$ and $\theta_{vars^2(\mathcal{C}_2)} = \theta'$.

Hence by induction hypothesis, we know that there exists a constraint system $\mathcal{C}'_2$ in $\mathcal{M}_2$ which is in the same column of $\mathcal{C}_2$, and such that:

1. $\mathcal{C}$ is ancestor of $\mathcal{C}'_2$, *i.e.* $\mathcal{C} \to^* \mathcal{C}'_2$
2. $\{(\xi, i) \mid i < s \wedge (\xi, i \rhd u) \in \Phi(\mathcal{C}_2)\} = \{(\xi, i) \mid i < s \wedge (\xi, i \rhd u) \in \Phi(\mathcal{C}'_2)\}$
3. $\{\mathsf{path}(\xi) \mid (\xi, s \rhd u) \in \Phi(\mathcal{C}_2)\} \subseteq \{\mathsf{path}(\xi) \mid (\xi, s \rhd u) \in \Phi(\mathcal{C}'_2)\}$
4. $\{\mathsf{path}(\xi) \mid (\xi, s \rhd u) \in \mathsf{NoUse}(\mathcal{C}_2)\} = \{\mathsf{path}(\xi) \mid (\xi, s \rhd u) \in \mathsf{NoUse}(\mathcal{C}'_2)\} \cap \{\mathsf{path}(\xi) \mid (\xi, s \rhd u) \in \Phi(\mathcal{C}_2)\}$
5. there exists $(\sigma'', \theta'') \in \mathsf{Sol}(\mathcal{C}'_2)$ such that $\sigma''_{|S_1} = \sigma'_{|S_1}$.

Thanks to the description of the strategy (see Section 4), we know that applying the rule Dest or Eq-frame-ded is always followed by the application of the same instance of the rule on each row of the matrix. However, when the parameters of the instance of the rule are not compatible with the constraint systems on a row of the matrix, this row stays untouched. Hence, we do a case analysis on the rule applied and on whether the parameters were compatible or not. Note that Property 3 of the inductive hypothesis on $\mathcal{C}_2$ and $\mathcal{C}'_2$ implies that if the parameters of the rule are compatible for $\mathcal{C}_2$, then they also are compatible for $\mathcal{C}'_2$.

- $\textsc{Rule}(\tilde{p}) = \textsc{Eq-frame-ded}(X_0, \xi_0)$ *where* X_0, ξ_0 *are not compatible parameters for* $\mathcal{C}'_2$*:* In such a case, it implies that there is no frame element in $\Phi(\mathcal{C}'_2)$ with $\mathsf{path}(\xi_0)$ as path. Hence, $\mathcal{C}'_2$ remains unchanged and so $\mathcal{C}'_2$ is a constraint system in $\mathcal{M}_1$. However, we know that for all $(\xi, s \rhd u) \in \Phi(\mathcal{C}_2)$, there exists $(\xi', s \rhd u') \in \Phi(\mathcal{C}'_2)$ such that $\mathsf{path}(\xi) = \mathsf{path}(\xi')$, thus we can deduce that X_0, ξ_0 are also not compatible parameters for $\mathcal{C}_2$ which means that $\mathcal{C}_1$ is in fact $\mathcal{C}_2$. Hence, by denoting $\mathcal{C}'_1 = \mathcal{C}'_2$, the result holds.

- $\textsc{Rule}(\tilde{p}) = \textsc{Dest}(\xi_0, \ell \to r, s)$ *where* $\xi_0, \ell \to r, s$ *are not compatible for* $\mathcal{C}'_2$*:* Similarly to the previous case, it implies that there is no frame element in $\Phi(\mathcal{C}'_2)$ with $\mathsf{path}(\xi_0)$ as path. Hence $\mathcal{C}_2 = \mathcal{C}_1$ and by denoting $\mathcal{C}'_1 = \mathcal{C}'_2$, the result holds.

- $\textsc{Rule}(\tilde{p}) = \textsc{Eq-frame-ded}(X_0, \xi_0)$ *where* X_0, ξ_0 *are compatible parameters for* $\mathcal{C}'_2$ *but not for* $\mathcal{C}_2$*:* In such a case, there exists a frame element $(\xi, s \rhd u) \in \Phi(\mathcal{C}'_2)$ such that $\mathsf{path}(\xi_0) = \mathsf{path}(\xi)$. Furthermore, there is not such frame element in $\mathcal{C}_2$. Since the rule is applied on $\mathcal{C}'_2$ and $(\sigma'', \theta'') \in \mathsf{Sol}(\mathcal{C}'_2)$, then by Lemma 42, we can deduce that there exists a constraint system $\mathcal{C}'_1$ in $\mathcal{M}_1$ such that:

  - $\mathcal{C}'_2 \to \mathcal{C}'_1$ which implies $\mathcal{C} \to^* \mathcal{C}'_1$ hence property 1 holds.
  - there exist $(\sigma''', \theta''') \in \mathsf{Sol}(\mathcal{C}'_1)$ such that $\sigma'''_{|S_1(\mathcal{C})} = \sigma''_{|S_1(\mathcal{C})}$ hence property 5 holds.

  Hence it remains to proves Properties 2, 3 and 4. But the rule Eq-frame-ded does not add new frame elements in the frame, thus properties 2 and 3 are trivially satisfied. At last, by the rule Eq-frame-ded, we may have:

  $$\mathsf{NoUse}(\mathcal{C}'_1) = \mathsf{NoUse}(\mathcal{C}'_2) \cup \{(\xi, s \rhd u)$$

  But, by hypothesis X_0, ξ_0 are not compatible parameters for $\mathcal{C}_2$ then it means that there is no frame element $(\zeta, s \rhd v) \in \Phi(\mathcal{C}_2)$ such that $\mathsf{path}(\zeta) = \mathsf{path}(\xi_0) = \mathsf{path}(\xi)$. Hence, we have that:

  $$\begin{array}{c} \{\mathsf{path}(\xi) \mid (\xi, s \rhd u) \in \mathsf{NoUse}(\mathcal{C}'_1)\} \cap \{\mathsf{path}(\xi) \mid (\xi, s \rhd u) \in \Phi(\mathcal{C}_2)\} \\ = \\ \{\mathsf{path}(\xi) \mid (\xi, s \rhd u) \in \mathsf{NoUse}(\mathcal{C}'_2)\} \cap \{\mathsf{path}(\xi) \mid (\xi, s \rhd u) \in \Phi(\mathcal{C}_2)\} \end{array}$$

  Therefore, property 4 holds.

- $\textsc{Rule}(\tilde{p}) = \textsc{Dest}(\xi_0, \ell \to r, s)$ *where* $\xi_0, \ell \to r, s$ *are compatible parameters for* $\mathcal{C}'_2$ *but not for* $\mathcal{C}_2$*:* Properties 1 and 5 are proved similarly to the previous case. It

remains to prove Properties 2, 3 and 4. Since $\xi_0, \ell \to r, s$ are compatible parameters for $\mathcal{C}_2'$, there exist $(\xi, i \rhd u) \in \Phi(\mathcal{C}_2')$ such that $\mathsf{path}(\xi) = \xi_0$ and $i \leq s$.

Let $\mathsf{g} \in \mathcal{F}_d$ be the destructor symbol of $\ell \to r$. This instance of the rule DEST may only add a frame element $(\zeta, s \rhd w)$ where $\mathsf{path}(\zeta) = \mathsf{g} \cdot \mathsf{path}(\xi_0)$. Hence Property 2 holds. Furthermore since $\Phi(\mathcal{C}_2') \subseteq \Phi(\mathcal{C}_1')$, Property 3 also holds. At last, since the rule DEST does not add frame in element in NoUse, we have that $\mathsf{NoUse}(\mathcal{C}_1') = \mathsf{NoUse}(\mathcal{C}_2')$ and so Property 4 holds.

- $\text{RULE}(\tilde{p}) = \text{EQ-FRAME-DED}(X_0, \xi_0)$ *where* X_0, ξ_0 *are compatible parameters for both* $\mathcal{C}_2$ *and* $\mathcal{C}_2'$*:* Thanks to Lemma 42, we can deduce that there exists a constraint system $\mathcal{C}_1'$ in $\mathcal{M}_1$ such that:
  - $\mathcal{C}_2' \to \mathcal{C}_1'$ which implies $\mathcal{C} \to^* \mathcal{C}_1'$ hence property 1 holds.
  - there exist $(\sigma''', \theta''') \in \mathsf{Sol}(\mathcal{C}_1')$ such that $\sigma'''_{|S_1(\mathcal{C})} = \sigma''_{|S_1(\mathcal{C})}$ hence property 5 holds.

  Moreover, since the rule EQ-FRAME-DED does not add new frame elements, properties 2 and 3 also holds.

  Let $u, u' \in \mathcal{T}(\mathcal{F}_c, \mathcal{N} \cup \mathcal{X}^1)$ such that $(X_0, i \vdash^? u) \in D(\mathcal{C}_1)$ and $(X_0, i \vdash^? u') \in D(\mathcal{C}_1')$. Furthermore, let $(\xi, s \rhd v) \in \Phi(\mathcal{C}_1)$ and $(\xi', s \rhd v') \in \Phi(\mathcal{C}_1')$ such that $\mathsf{path}(\xi) = \mathsf{path}(\xi') = \mathsf{path}(\xi_0)$.

  We already proved that $(\sigma, \theta) \in \mathsf{Sol}(\overline{\mathcal{C}_1})$, $(\sigma''', \theta''') \in \mathsf{Sol}(\mathcal{C}_1')$ and $\sigma_{|S_1(\mathcal{C})} = \sigma'''_{|S_1(\mathcal{C})}$. Thus, by Lemma 48, we can deduce that $u\sigma = u'\sigma'''$ and $v\sigma = v'\sigma'''$. Thus, $\sigma \vDash u =^? v$ is equivalent to $\sigma''' \vDash u' =^? v'$. But by the description of the rule, we have that $(\xi, s \rhd u) \in \mathsf{NoUse}(\mathcal{C}_1)$ is equivalent to $\sigma \vDash u =^? v$; and $(\xi', s \rhd u') \in \mathsf{NoUse}(\mathcal{C}_1')$ is equivalent to $\sigma''' \vDash u' =^? v'$. Hence we conclude that

  $$(\xi, s \rhd v) \in \mathsf{NoUse}(\mathcal{C}_1) \quad \text{is equivalent to} \quad (\xi', s \rhd v') \in \mathsf{NoUse}(\mathcal{C}_1')$$

  and so Property 4 holds.

- $\text{RULE}(\tilde{p}) = \text{DEST}(\xi_0, \ell \to r, s)$ *where* $\xi_0, \ell \to r, s$ *are compatible parameters for* $\mathcal{C}_2'$ *and* $\mathcal{C}_2$. Thanks to Lemma 42, we can deduce that there exists a constraint system $\mathcal{C}_1'$ in $\mathcal{M}_1$ such that:
  - $\mathcal{C}_2' \to \mathcal{C}_1'$ which implies $\mathcal{C} \to^* \mathcal{C}_1'$ hence property 1 holds.
  - there exist $(\sigma''', \theta''') \in \mathsf{Sol}(\mathcal{C}_1')$ such that $\sigma'''_{|S_1(\mathcal{C})} = \sigma''_{|S_1(\mathcal{C})}$ hence property 5 holds.

  Let $\mathsf{g} \in \mathcal{F}_d$ be the destructor symbol of $\ell \to r$. This instance of the rule DEST may only add a frame element $(\zeta, s \rhd w)$ where $\mathsf{path}(\zeta) = \mathsf{g} \cdot \mathsf{path}(\xi_0)$. Hence Property 2 holds.

  Let $(\xi, j \rhd u) \in \Phi(\mathcal{C}_1)$ and $(\xi', j' \rhd u') \in \Phi(\mathcal{C}_1')$ such that $\mathsf{path}(\xi) = \mathsf{path}(\xi') = \mathsf{path}(\xi_0)$. First of all, thanks to Property 2 of our inductive hypothesis, we deduce that $j = j'$.

  Assume now that there exists $(\zeta, s \rhd w) \in \Phi(\mathcal{C}_1)$ such that $\mathsf{path}(\zeta) = \mathsf{g} \cdot \mathsf{path}(\xi_0)$. We show that there necessary exists $(\zeta', s \rhd w') \in \Phi(\mathcal{C}_1')$ such that $\mathsf{path}(\zeta') = \mathsf{g} \cdot \mathsf{path}(\xi_0)$.

Since $\mathsf{path}(\zeta) = \mathsf{g} \cdot \mathsf{path}(\xi_0)$ then there exists $X_2, \ldots, X_n \in \mathcal{X}^2$ such that $\zeta = \mathsf{g}(\xi, X_2, \ldots, X_n)$. Furthermore, thanks to $(\sigma, \theta) \in \mathsf{Sol}(\overline{\mathcal{C}_1})$, to the definition of a solution of a constraint system and to Property 5 of a well-formed constraint system, we deduce that $\zeta\theta(\Phi(\mathcal{C}_1)\sigma)\downarrow = w\sigma$.

But $(\sigma''', \theta''') \in \mathsf{Sol}(\mathcal{C}'_1)$ and $\sigma_{|S_1(\mathcal{C})} = \sigma'''_{|S_1(\mathcal{C})}$. Thus, by Lemma 48, we can deduce that $\mathsf{Init}(\Phi(\mathcal{C}_1))\sigma = \mathsf{Init}(\Phi(\mathcal{C}'_1))\sigma'''$ which implies $\zeta\theta(\Phi(\mathcal{C}_1)\sigma)\downarrow = \zeta\theta(\Phi(\mathcal{C}'_1)\sigma''')\downarrow \in \mathcal{T}(\mathcal{F}_c, \mathcal{N})$. Furthermore, Lemma 48 also implies that $u\sigma = u'\sigma'''$. Hence we have that $\xi'\theta'''(\Phi(\mathcal{C}'_1)\sigma''')\downarrow = \xi\theta(\Phi(\mathcal{C}_1)\sigma)\downarrow = \xi\theta(\Phi(\mathcal{C}'_1)\sigma''')\downarrow$. Thus, $\mathsf{g}(\xi'\theta''', X_2\theta, \ldots, X_n\theta)(\Phi(\mathcal{C}'_1)\sigma''')\downarrow \in \mathcal{T}(\mathcal{F}_c, \mathcal{N})$. With $\sigma''' \vDash ND(\mathcal{C}'_1)$ thanks to $(\sigma''', \theta''') \in \mathsf{Sol}(\mathcal{C}'_1)$, the description of the rule DEST allows us to conclude that there exists $(\zeta', s \rhd w') \in \Phi(\mathcal{C}'_1)$ such that $\mathsf{path}(\zeta') = \mathsf{path}(\zeta)$. Hence Property 3 folds.

Since the rule DEST does not add a frame element in NoUse, we conclude that Property 4 holds. □

Lemma 50. *Let $\mathcal{M}, \mathcal{M}_1$ be two matrices of constraint systems obtained respectively at the beginning and end of Step a of Phase 1 with support s such that $\mathcal{M} \to^* \mathcal{M}_1$. Let $\mathcal{C}_1$ be a constraint system in $\mathcal{M}_1$. Assume that $\mathcal{C}$ the constraint system in $\mathcal{M}$ ancestor of $\mathcal{C}_1$ satisfies $\mathsf{Sol}(\mathcal{C}) = \mathsf{Sol}(\overline{\mathcal{C}})$, and let $(\sigma, \theta) \in \mathsf{Sol}(\overline{\mathcal{C}_1})$. Assume that*

1. *for all $X \in vars^2(D(\mathcal{C}_1))$, for all position p of $\mathsf{C}\lfloor X\theta \rfloor_{\Phi(\mathcal{C}_1)}$, if $\mathsf{root}(\mathsf{C}\lfloor X\theta \rfloor_{\Phi(\mathcal{C}_1)}) \in \mathcal{F}_d$, then there is no ground recipe $\xi \in \Pi_r$ such that $\xi(\Phi(\mathcal{C}_1)\sigma)\downarrow = X\theta'|_p(\Phi(\mathcal{C}_1)\sigma)\downarrow$ and $\mathsf{param}_{\mathsf{max}}(\xi') < \mathsf{param}_{\mathsf{max}}(X\theta|_p)$; and*
2. *for all $\xi, \xi' \in st(\{X\theta \mid X \in vars^2(D(\mathcal{C}_1))\})$, $\mathsf{path}(\xi) = \mathsf{path}(\xi')$ implies $\xi = \xi'$.*

There exists a constraint system $\mathcal{C}'_1$ in the same column of $\mathcal{C}_1$ and there exists $(\sigma', \theta') \in \mathsf{Sol}(\mathcal{C}'_1)$ such that $\sigma_{|S_1(\mathcal{C})} = \sigma'_{|S_1(\mathcal{C})}$ and for all $X \in S_2(\mathcal{C}_1)$, $X\theta = X\theta'$

Proof. Our hypothesis on $\mathcal{M}$, $\mathcal{M}_1$ and $\mathcal{C}_1$ allows us to apply Lemma 49. Hence we have that there exists a constraint system $\mathcal{C}'_1$ in the same column as $\mathcal{C}_1$ such that:

1. $\mathcal{C} \to^* \mathcal{C}'_1$;
2. $\{(\xi, i) \mid i \neq s \wedge (\xi, i \rhd u) \in \Phi(\mathcal{C}_1)\} = \{(\xi, i) \mid i < s \wedge (\xi, i \rhd u) \in \Phi(\mathcal{C}'_1)\}$;
3. $\{\mathsf{path}(\xi) \mid (\xi, s \rhd u) \in \Phi(\mathcal{C}_1)\} \subseteq \{\mathsf{path}(\xi) \mid (\xi, s \rhd u) \in \Phi(\mathcal{C}'_1)\}$;
4. $\{\mathsf{path}(\xi) \mid (\xi, s \rhd u) \in \mathsf{NoUse}(\mathcal{C}_1)\} = \{\mathsf{path}(\xi) \mid (\xi, s \rhd u) \in \mathsf{NoUse}(\mathcal{C}'_1)\} \cap \{\mathsf{path}(\xi) \mid (\xi, s \rhd u) \in \Phi(\mathcal{C}_1)\}$;
5. there exists $(\sigma', \theta') \in \mathsf{Sol}(\mathcal{C}'_1)$ such that $\sigma_{|S_1(\mathcal{C})} = \sigma'_{|S_1(\mathcal{C})}$.

However, Property 5 is not a sufficient for our result. Hence we will build a new substitution θ'' that satisfies the properties stated in the Lemma.

Since $\mathcal{C}_1$ and $\mathcal{C}'_1$ have the same shape, we have that $S_2(\mathcal{C}_1) = S_2(\mathcal{C}'_1)$. Furthermore, since during Step a of Phase 1 with support s, the only added deducible constraint are of the following form: $X, s \vdash^? u$, for some X and u where $X \notin S_2(\mathcal{C}_1)$.

We now show that there exists a renaming ρ of the recipe variables such that:

- $\{(X\rho, i) \mid (X, i \vdash^? u) \in D(\mathcal{C}_1)\} \subseteq \{(X, i) \mid (X, i \vdash^? u) \in D(\mathcal{C}'_1)\}$

- $\{(\xi\rho, i) \mid (\xi, i \rhd u) \in \Phi(\mathcal{C}_1)\} \subseteq \{(\xi, i) \mid (\xi, i \rhd u) \in \Phi(\mathcal{C}'_1)\}$

First of all, since $\mathcal{C}_1$ and $\mathcal{C}'_1$ have the same shape, we deduce that $S_2(\mathcal{C}_1) = S_2(\mathcal{C}'_1)$ and $\{(X, i) \mid (X, i \vdash^? u) \in D(\mathcal{C}_1) \wedge X \in S_2(\mathcal{C}_1)\} = \{(X, i) \mid (X, i \vdash^? u) \in D(\mathcal{C}'_1) \wedge X \in S_2(\mathcal{C}'_1)\}$. Hence, we define ρ on $S_2(\mathcal{C})$ is the identity. Let $(X, i \vdash^? u) \in D(\mathcal{C}_1)$ such that $X \notin S_2(\mathcal{C}_1)$. Since $\mathcal{M}_1$ satisfies $\mathsf{PP1Sa}(s)$, we deduce that there exists a unique frame element $(\mathsf{g}(\xi_1, \ldots, \xi_n), j \rhd v) \in \Phi(\mathcal{C}_1)$ and $k \in \{2, \ldots, n\}$ such that $j = s$ and $\xi_k = X$. But we already proved that $\{\mathsf{path}(\xi) \mid (\xi, s \rhd u) \in \Phi(\mathcal{C}_1)\} \subseteq \{\mathsf{path}(\xi) \mid (\xi, s \rhd u) \in \Phi(\mathcal{C}'_1)\}$. Hence along with Property 3 of the invariant $\mathsf{PP1Sa}(s)$ on $\mathcal{C}'_1$, we deduce that there exists $(\mathsf{g}(\xi'_1, X'_2, \ldots, X'_n), s \rhd v') \in \Phi(\mathcal{C}'_1)$ and $\mathsf{path}(\xi'_1) = \mathsf{path}(\xi_1)$. Thus, we define ρ on X such that $X\rho = X'_k$. Moreover, since $X'_k \notin S_2(\mathcal{C})$, we deduce that there exists u'_k such that $(X'_k, s \vdash^? u'_k) \in D(\mathcal{C}'_1)$. Hence we conclude that $\{(X\rho, i) \mid (X, i \vdash^? u) \in D(\mathcal{C}_1)\} \subseteq \{(X, i) \mid (X, i \vdash^? u) \in D(\mathcal{C}'_1)\}$.

We already know that $\{(\xi, i) \mid i \neq s \wedge (\xi, i \rhd u) \in \Phi(\mathcal{C}_1)\} = \{(\xi, i) \mid i < s \wedge (\xi, i \rhd u) \in \Phi(\mathcal{C}'_1)\}$. Moreover, for all $(\xi, i \rhd u) \in \Phi(\mathcal{C}_1)$, for all $X \in vars^2(\xi)$, $\mathsf{param}^{\mathcal{C}_1}_{\mathsf{max}}(X) \leq i$ (thanks to $\mathcal{C}_1$ being well-formed. But $\mathcal{C}_1$ satisfies $\mathsf{InvUntouched}(s)$. Hence if $i \neq s$ and $X \in vars^2(\xi)$, then $i < s$ and so $X \in S_2(\mathcal{C})$. Thus, if $i \neq s$ then $\xi\rho = \xi$. Let $(\xi, s \rhd u) \in \Phi(\mathcal{C}_1)$. Since $\mathcal{C}_1$ is well-formed (item 3), $\mathsf{param}^{\mathcal{C}_1}_{\mathsf{max}}(\xi)$ exists and so for all $Z \in vars^2(\xi)$, there exists $(Z, j \vdash^? u) \in D(\mathcal{C}_1)$. Thus by construction of ρ, we deduce that there exists u' such that $(\xi\rho, s \rhd u') \in \Phi(\mathcal{C}'_1)$ and so $\{(\xi\rho, i) \mid (\xi, i \rhd u) \in \Phi(\mathcal{C}_1)\} \subseteq \{(\xi, i) \mid (\xi, i \rhd u) \in \Phi(\mathcal{C}'_1)\}$.

Hence, for all $X \in vars^2(D(\mathcal{C}'_1)) \cap \mathrm{img}(\rho)$, we define $X\theta'' = X\rho^{-1}\theta$. It remains to define the variables that are not in $\mathrm{img}(\rho)$.

First of all, for all $Y \in vars^2(D(\mathcal{C}_1))$, for all position p, if $\mathsf{root}(\mathsf{C}\lfloor Y\theta_1 \rfloor_{\Phi(\mathcal{C}_1)}|_p) = \mathsf{g} \in \mathcal{F}_d$ then $\mathsf{path}(Y\theta|_p) \in \mathcal{F}_d^* \cdot \mathcal{AX}$. But since $(\sigma, \theta) \in \mathsf{Sol}(\overline{\mathcal{C}_1})$, then $Y\theta|_p(\Phi(\mathcal{C}_1)\sigma)\downarrow \in \mathcal{T}(\mathcal{F}_c, \mathcal{N})$. Moreover, we know that $(\sigma', \theta') \in \mathsf{Sol}(\mathcal{C}'_1)$ with $\sigma_{|S_1(\mathcal{C})} = \sigma'_{|S_1(\mathcal{C})}$. By Lemma 48, we know that $\mathsf{Init}(\Phi(\mathcal{C}_1))\sigma = \mathsf{Init}(\Phi(\mathcal{C}'_1))\sigma'$ and so $Y\theta|_p(\Phi(\mathcal{C}'_1)\sigma')\downarrow \in \mathcal{T}(\mathcal{F}_c, \mathcal{N})$.

Furthermore, the matrix $\mathcal{M}_1$ is obtained at the end of Step a of Phase 1 of the strategy, then $\mathcal{C}'_1$ satisfies the invariant $\mathsf{InvDest}(s)$. Thus, with $\sigma' \vDash ND(\mathcal{C}'_1)$, we can deduce that either (a) there exists a frame element $(\xi, s \rhd u) \in \Phi(\mathcal{C}'_1)$ such that $\mathsf{path}(\xi) = \mathsf{path}(Y\theta|_p)$ or else (b) there exist a frame element $(\xi', i \rhd v) \in \Phi(\mathcal{C}'_1)$ such that $\mathsf{path}(\xi')$ is a suffix of $\mathsf{path}(Y\theta|_p)$ and $(\xi', i \rhd v) \in \mathsf{NoUse}(\mathcal{C}'_1)$.

Case (b): Since $(\sigma, \theta) \in \mathsf{Sol}(\overline{\mathcal{C}_1})$, we deduce that $Y\theta$ conforms to $\Phi(\mathcal{C}_1)$ w.r.t. $\mathsf{NoUse}(\mathcal{C}_1)$. Hence, we deduce that there is no frame element on $\Phi(\mathcal{C}_1)$ which recipe have $\mathsf{path}(\xi')$ as path. Hence, thanks to property 2 of the well formed constraint system, we can also deduce that there exists a position p' of $\mathsf{C}\lfloor Y\theta \rfloor_{\Phi(\mathcal{C}_1)}$ such that $\mathsf{C}\lfloor Y\theta \rfloor_{\Phi(\mathcal{C}_1)}|_p = \mathsf{path}(\xi')$ and $i = s$. But by Property 8 of a well-formed constraint system, $(\xi', s \rhd v) \in \mathsf{NoUse}(\mathcal{C}'_1)$ implies that there exists $Z \in vars^2(\mathcal{C}'_1)$ such that $\mathsf{C}\lfloor Z\mathsf{mgu}(E_\Pi(\mathcal{C}'_1)) \rfloor_{\Phi(\mathcal{C}'_1)}\delta^1(\mathcal{C}'_1) = v$ and $\mathsf{param}^{\mathcal{C}'_1}_{\mathsf{max}}(Z\mathsf{mgu}(E_\Pi(\mathcal{C}'_1))) < s$.

Since we proved that $\mathsf{Init}(\Phi(\mathcal{C}_1))\sigma = \mathsf{Init}(\Phi(\mathcal{C}'_1))\sigma'$, then $Z\theta(\Phi(\mathcal{C}_1)\sigma)\downarrow = \xi'\theta(\Phi(\mathcal{C}_1)\sigma)\downarrow = Y\theta|_p(\Phi(\mathcal{C}_1)\sigma)\downarrow$. Hence we have that $Y\theta|_p(\Phi(\mathcal{C}_1)\sigma)\downarrow = Z\theta(\Phi(\mathcal{C}_1)\sigma)\downarrow$ where $\mathsf{param}_{\mathsf{max}}(Z\theta) < s$ which is a contradiction on the hypothesis on θ. Thus we can deduce that this case is impossible.

Case (a): Let's denote $Y\theta|_p = \mathsf{g}(\zeta_1, \ldots, \zeta_n)$. Thanks to $\mathcal{M}_1$ satisfying invariant $\mathsf{PP1Sa}(s)$, we know that there exists $X_2, \ldots, X_n \in vars^2(D(\mathcal{C}'_1))$ such that $\xi = \mathsf{g}(\xi_1, X_2, \ldots, X_n)$ for some ξ_1. Furthermore, we know, by definition of θ, that all recipe in θ with the same path is equal to $Y\theta|_p$. Hence for all $i \in \{2, \ldots, n\}$, we define $X_i\theta'' = \zeta_i$.

Let $\mathcal{S}_X$ be the set of all the others variables in $vars^2(D(\mathcal{C}'_1))$ not already defined at this stage. For all $X \in \mathcal{S}_X$, we define $X\theta'' = \mathsf{C}\lfloor X\theta' \rfloor_{\Phi(\mathcal{C}'_1)} \delta^2(\mathcal{C}'_1)\theta''$ which exists by following the order $<_{\theta'}$ on $\mathcal{S}_X$.

Typically, the variables in $\mathcal{S}_X$ represents the variables that could not be instantiate thanks to θ. Thus, since $(\sigma', \theta') \in \mathsf{Sol}(\mathcal{C}'_1)$, we used θ' to defined those variables. The expression $\mathsf{C}\lfloor X\theta' \rfloor_{\Phi(\mathcal{C}'_1)} \delta^2(\mathcal{C}'_1)\theta''$ represents the fact that the context of $X\theta'$ and $X\theta''$ are the same.

Finally, for all $X \in vars^2(\mathcal{C}'_1) \setminus vars^2(D(\mathcal{C}'_1))$, we define $X\theta'' = X\mathsf{mgu}(E_\Pi(\mathcal{C}'_1))\theta''$

To verify that $(\sigma', \theta'') \in \mathsf{Sol}(\mathcal{C}'_1)$, it remains to prove that $\theta'' \vDash E_\Pi(\mathcal{C}'_1)$. The others propriety are indeed satisfied by construction of θ''. Thanks to $\mathcal{M}_1$ satisfying invariant $\mathsf{PP1Sa}(s)$ (item 4), we know that the variable in $vars^2(D(\mathcal{C}'_1))$ do not appear in any inequation in $E_\Pi(\mathcal{C}'_1$. Furthermore, since by definition of θ'', θ'' satisfies $\mathsf{mgu}(E_\Pi(\mathcal{C}'_1))$, we can deduce that $\theta'' \vDash E_\Pi(\mathcal{C}'_1)$. □

Lemma 51. *Let $\mathcal{M}$ be a matrix of constraint systems obtained at the end of Step e of Phase 1 of the strategy with s as support. Let $\mathcal{C}$ be a constraint system in $\mathcal{M}$. Let $(\sigma, \theta) \in \mathsf{Sol}(\overline{\mathcal{C}})$. We have that there exists θ' such that $(\sigma, \theta') \in \mathsf{Sol}(\overline{\mathcal{C}})$ and*

1. *for all $X \in vars^2(D(\mathcal{C}))$, for all position p of $\mathsf{C}\lfloor X\theta' \rfloor_{\Phi(\mathcal{C})}$, if $\mathsf{root}(\mathsf{C}\lfloor X\theta' \rfloor_{\Phi(\mathcal{C})|_p}) \in \mathcal{F}_d$, then there is no ground recipe $\xi \in \Pi_r$ such that $\xi(\Phi(\mathcal{C})\sigma)\downarrow = X\theta'|_p(\Phi(\mathcal{C})\sigma)\downarrow \in \mathcal{T}(\mathcal{F}_c, \mathcal{N})$ and $\mathsf{param}_{\mathsf{max}}(\xi) < \mathsf{param}_{\mathsf{max}}(X\theta'|_p)$; and*
2. *for all $\xi, \xi' \in st(\{X\theta \mid X \in vars^2(D(\mathcal{C}))\})$, $\mathsf{path}(\xi) = \mathsf{path}(\xi')$ implies $\xi = \xi'$.*

Proof. We begin by proving the first property of the result: We show that there exists θ' such that $(\sigma, \theta') \in \mathsf{Sol}(\overline{\mathcal{C}})$ and for all $X \in vars^2(D(\mathcal{C}))$, for all position p of $\mathsf{C}\lfloor X\theta' \rfloor_{\Phi(\mathcal{C})}$, if $\mathsf{root}(\mathsf{C}\lfloor X\theta' \rfloor_{\Phi(\mathcal{C})|_p}) \in \mathcal{F}_d$, then there is no recipe $\xi \in \Pi_r$ such that $\xi(\Phi(\mathcal{C})\sigma)\downarrow = X\theta'|_p(\Phi(\mathcal{C})\sigma)\downarrow \in \mathcal{T}(\mathcal{F}_c, \mathcal{N})$ and $\mathsf{param}_{\mathsf{max}}(\xi) < \mathsf{param}_{\mathsf{max}}(X\theta'|_p)$.

We prove this property by induction on the number of positions p which do not satisfy the property. Let's denote this number $m(\theta)$

Base case $m(\theta) = 0$: In such a case, the result trivially holds.

Inductive step $m(\theta) > 0$: Otherwise, let $X \in vars^2(D(\mathcal{C}))$, a position p and a ground recipe $\xi \in \Pi_r$ such that $\mathsf{root}(\mathsf{C}\lfloor X\theta \rfloor_{\Phi(\mathcal{C})}|_p) \in \mathcal{F}_d$, $\xi(\Phi(\mathcal{C})\sigma)\downarrow = X\theta|_p(\Phi(\mathcal{C})\sigma)\downarrow \in \mathcal{T}(\mathcal{F}_c, \mathcal{N})$ and $\mathsf{param}_{\mathsf{max}}(\xi) < \mathsf{param}_{\mathsf{max}}(X\theta|_p)$.

First of all, thanks to Lemma 35, we know that there exists $\xi' \in \Pi_r$ such that ξ' conforms to $\Phi(\mathcal{C})\theta$ w.r.t. $\mathsf{NoUse}(\mathcal{C})\theta$, $\xi(\Phi(\mathcal{C})\sigma)\downarrow = \xi'(\Phi(\mathcal{C})\sigma)\downarrow$ and $\mathsf{param}_{\mathsf{max}}(\xi') \leq \mathsf{param}_{\mathsf{max}}(\xi)$.

Secondly, thanks to Property 1 shown in Lemma 41, we know that there exists a position p' and $\xi'' \in st(\xi')$, such that p' is a prefix of p and $X\theta[\xi']_p(\Phi(\mathcal{C})\sigma)\downarrow = X\theta[\xi'']_{p'}(\Phi(\mathcal{C})\sigma)\downarrow$ and $X\theta[\xi'']_{p'} \in \Pi_r$.

We want to apply Lemma 40 for the replacement. We know that $\mathcal{C}$ satisfies the invariants $\mathsf{InvVarFrame}(s)$ and $\mathsf{InvUntouched}(s)$. Thus for all $(\zeta, i \rhd u) \in \Phi(\mathcal{C})$, for all $Z \in vars^2(\zeta)$, $\mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(Z) < i$. But, for all $Z \in vars^2(\mathsf{C}\lfloor X\theta[\xi'']_{p'} \rfloor_{\Phi(\mathcal{C})})$, either $Z \in vars^2(\mathsf{C}\lfloor X\theta \rfloor_{\Phi(\mathcal{C})})$ else $Z \in vars^2(\mathsf{C}\lfloor \xi'' \rfloor_{\Phi(\mathcal{C})})$. Since $\xi'' \in st(\xi')$ and $\mathsf{param}_{\mathsf{max}}(\xi') \leq \mathsf{param}_{\mathsf{max}}(\xi) < \mathsf{param}_{\mathsf{max}}(X\theta|_p)$, we can deduce, thanks to Lemma 39, that $\neg(X < Z)$. Hence we can apply Lemma 40 which gives us that there exists θ' such that (σ, θ') is a

pre-solution of $\mathcal{C}$ with $X\theta' = X\theta[\xi'']_{p'}$, $\theta' \vDash \mathsf{mgu}(E_\Pi(\mathcal{C}))$ and for all $Y \in vars^2(D) \setminus \{X\}$, $\mathsf{C}\lfloor Y\theta' \rfloor_{\Phi(\mathcal{C})} = \mathsf{C}\lfloor Y\theta \rfloor_{\Phi(\mathcal{C})}$.

However, we know that $\mathcal{M}$ is obtained at the end of Step e of Phase 1 with support s. Hence thanks to Lemma 27, $\mathcal{M}$ satisfies $\mathsf{PP1SbE}(s,k)$ where k is the column $\mathcal{C}$ and so $\mathcal{C}$ satisfies: for all $(X, i \rhd x) \in D(\mathcal{C})$, for all $(\xi, j \rhd u) \in \Phi(\mathcal{C})$, for all $\mathsf{f} \in \mathcal{F}_c$, $E_\Pi \nvDash \mathsf{root}(X) \neq^? \mathsf{f}$ and $E_\Pi \nvDash X \neq^? \xi$. Hence, we can deduce that $\theta' \vDash E_\Pi(\mathcal{C})$ and so $(\sigma, \theta') \in \mathsf{Sol}(\overline{\mathcal{C}})$.

At last, since we replace a subterm of $X\theta$ by a recipe of strictly smaller maximal parameter and for all $Y \in vars^2(D) \setminus \{X\}$, $\mathsf{C}\lfloor Y\theta' \rfloor_\Phi = \mathsf{C}\lfloor Y\theta \rfloor_\Phi$, we can deduce that $m(\theta') < m(\theta)$. Hence we conclude by applying our inductive hypothesis.

We now show the second property of the result. First of all, we know that for all $X \in vars^2(D(\mathcal{C}))$, $X\theta$ conforms to $\Phi(\mathcal{C})\theta$ w.r.t. $\mathsf{NoUse}(\mathcal{C})$. Hence, if there exists $X, Y \in vars^2(D(\mathcal{C}))$, $\xi \in st(X\theta)$ and $\xi' \in st(Y\theta)$ such that $\mathsf{path}(\xi) = \mathsf{path}(\xi')$ and $\xi \neq \xi'$, it implies that $\mathsf{root}(\xi) \in \mathcal{F}_d$ and there is no frame element $(\zeta, i \rhd u) \in \Phi(\mathcal{C})$ such that $\mathsf{path}(\xi) = \mathsf{path}(\zeta)$ (otherwise it would contradict the conformity of $X\theta$ to $\Phi(\mathcal{C})\theta$ w.r.t. $\mathsf{NoUse}\theta$). Hence it implies that there exists p (resp. p') position of $\mathsf{C}\lfloor X\theta \rfloor_{\Phi(\mathcal{C})}$ (resp. $\mathsf{C}\lfloor Y\theta \rfloor_{\Phi(\mathcal{C})}$) such that $X\theta|_p = \xi$ (resp. $Y\theta|_p = \xi'$).

Hence, we do our proof by induction on the number of position that do not satisfies the wanted property: Let $\mu(\theta)$ be the set defined such that $\mu(\theta) = \{\mathsf{path} \mid X, Y \in vars^2(D(\mathcal{C}))$ and $\xi, \xi' \in st(X\theta, Y\theta)$ and $\mathsf{path}(\xi) = \mathsf{path}(\xi')$ and $\xi \neq \xi'\}$.

Base case $\mu(\theta) = \emptyset$: In such a case, the result trivially holds.

Inductive step $\mu(\theta) \neq \emptyset$: Let w be a minimal path in term of size in $\mu(\theta)$. Let X_0 be a minimal variable in term of $<_\theta$ of all variables X where there exists a position p of $\mathsf{C}\lfloor X\theta \rfloor_{\Phi(\mathcal{C})}$ such that $\mathsf{path}(X\theta|_p) = w$.

Hence we know that there exists p_0 position of $\mathsf{C}\lfloor X_0\theta \rfloor_{\Phi(\mathcal{C})}$ such that $\mathsf{path}(X_0\theta|_{p_0}) = w$. We will replace any recipe that have w as path by $X_0\theta|_{p_0}$ that we denote ξ_0. Hence, we do a new induction on:

$$m(\theta) = \sum_{\mathsf{path}(\xi)=w} \mathsf{nb}_{\mathsf{occ}}(\xi, \{Y\theta \mid Y \in vars^2(D(\mathcal{C}))\}) - \mathsf{nb}_{\mathsf{occ}}(\xi_0, \{Y\theta \mid Y \in vars^2(D(\mathcal{C}))\})$$

Base case $m = 0$: In such a case, it implies that any subterm whose path is equal to w, is in fact ξ_0. Hence it contradicts the fact that $w \in \mu(\theta)$.

Inductive case $m > 0$: Otherwise, we have that there exists $Y \in vars^2(D(\mathcal{C}))$ and p position of $\mathsf{C}\lfloor Y\theta \rfloor_{\Phi(\mathcal{C})}$ such that $\mathsf{path}(Y\theta|_p) = w$ but $Y\theta|_p \neq X\theta|_{p_0}$. We want to apply Lemma 40 hence we have to verify the application conditions of the lemma. Let $\xi = X\theta|_{p_0}$.

- Since ξ is a subterm of $X\theta$ and $(\sigma, \theta) \in \mathsf{Sol}(\overline{\mathcal{C}})$, we have that ξ conforms to $\Phi(\mathcal{C})\theta$ w.r.t. $\mathsf{NoUse}(\mathcal{C})\theta$. Furthermore, thanks to the first property we shown in this lemma, we know that $\mathsf{path}(\xi) = \mathsf{path}(Y\theta|_p)$ implies $\mathsf{param}_{\mathsf{max}}(\xi) = \mathsf{param}_{\mathsf{max}}(Y\theta|_p)$. Hence since $Y\theta|_p \in st(Y\theta)$ and $(\sigma, \theta) \in \mathsf{Sol}(\overline{\mathcal{C}})$, we deduce that $\mathsf{param}_{\mathsf{max}}(\xi) \leq \mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(Y)$.
- Since $\mathsf{path}(\xi) = \mathsf{path}(Y\theta|_p)$, $\xi(\Phi(\mathcal{C})\sigma)\downarrow \in \mathcal{T}(\mathcal{F}_c, \mathcal{N})$ and $Y\theta|_p(\Phi(\mathcal{C})\sigma)\downarrow \in \mathcal{T}(\mathcal{F}_c, \mathcal{N})$, then by Lemma 33, we have that $\xi(\Phi(\mathcal{C})\sigma)\downarrow = Y\theta|_p(\Phi(\mathcal{C})\sigma)\downarrow$. Furthermore $\mathsf{path}(\xi) = \mathsf{path}(Y\theta|_p)$ also implies that $\mathsf{C}\lfloor Y\theta[\xi]_p \rfloor_{\Phi(\mathcal{C})} = \mathsf{C}\lfloor Y\theta \rfloor_{\Phi(\mathcal{C})}[\mathsf{C}\lfloor \xi \rfloor_{\Phi(\mathcal{C})}]_p$.

- X_0 was chosen as minimal under $<_\theta$, hence for all $Z \in vars^2(\mathsf{C}\lfloor\xi\rfloor_{\Phi(\mathcal{C})}\delta^2(\mathcal{C}))$, if we had $Y <_\theta Z$ then it would imply that $Y <_\theta X_0$ since we have that $Z <_\theta X_0$. This is a contradiction, hence we have that $\neg(Y <_\theta Z)$.

Thus by Lemma 40, we have that there exists θ' such that (σ, θ') is a pre-solution of $\mathcal{C}$ with $Y\theta' = Y\theta[\xi]_p$, $\theta' \vDash \mathsf{mgu}(E_\Pi(\mathcal{C}))$ and for all $Z \in vars^2 D \setminus \{Y\}$, we have that $\mathsf{C}\lfloor Z\theta'\rfloor_{\Phi(\mathcal{C})} = \mathsf{C}\lfloor Z\theta\rfloor_{\Phi(\mathcal{C})}$.

But with $(\sigma, \theta) \in \mathsf{Sol}(\overline{\mathcal{C}})$, we trivially have that $\sigma \vDash E(\mathcal{C}_1)$. Moreover, since $\mathcal{C}$ is a constraint system obtained from Step e, we have shown that for all $Z \in vars^2(D(\mathcal{C}))$, for all $\mathsf{f} \in \mathcal{F}_c$, there is no inequation in $E_\Pi(\mathcal{C})$ of the form $Z \neq^? \xi$ or $\mathsf{root}(Z) \neq^? \mathsf{f}$ where ξ is a recipe of $\Phi(\mathcal{C})$. Hence we have that $\theta' \vDash E_\Pi(\mathcal{C})$ and so $(\sigma, \theta') \in \mathsf{Sol}(\overline{\mathcal{C}})$.

By construction, we have that $m(\theta') < m(\theta)$. Furthermore, the construction of θ', i.e. $Y\theta' = Y\theta[\xi]_p$ and for all $Z \in vars^2 D \setminus \{Y\}$, $\mathsf{C}\lfloor Z\theta'\rfloor_{\Phi(\mathcal{C})} = \mathsf{C}\lfloor Z\theta\rfloor_{\Phi(\mathcal{C})}$, imply that X_0 is also a minimal variable in term of $<_{\theta'}$ from all variables $X \in vars^2(D(\mathcal{C}))$ where there exists a position p of $\mathsf{C}\lfloor X\theta'\rfloor_{\Phi(\mathcal{C})}$ such that $\mathsf{path}(X\theta'|_p) = w$. Hence we can apply our inductive hypothesis on θ' which conclude the result. □

Definition 22. *The relation* $\mathcal{R}_{\mathcal{F}_c}$ *over* $\Pi_r \times \Pi_r$ *is the least relation that contains* $\xi\ \mathcal{R}_{\mathcal{F}_c}\ \xi'$ *when* $\mathsf{path}(\xi)$, $\mathsf{path}(\xi')$ *are defined and* $\mathsf{path}(\xi) = \mathsf{path}(\xi')$, *and that is closed by constructor application,* i.e. *for any* $\mathsf{f} \in \mathcal{F}_c$ *of arity* n,

$$\xi_1\ \mathcal{R}_{\mathcal{F}_c}\ \xi'_1,\ \ \ldots\ \ ,\xi'_n\ \mathcal{R}_{\mathcal{F}_c}\ \xi'_n\ \ \Rightarrow \mathsf{f}(\xi_1, \ldots, \xi_n)\ \mathcal{R}_{\mathcal{F}_c}\ \mathsf{f}(\xi'_1, \ldots, \xi'_n).$$

Lemma 52. *Let* Φ *a ground frame, and* ξ, ξ' *two ground recipes in* Π_r. *We have that* $\mathsf{C}\lfloor\xi\rfloor_\Phi = \mathsf{C}\lfloor\xi'\rfloor_\Phi$ *implies* $\xi\ \mathcal{R}_{\mathcal{F}_c}\ \xi'$.

Proof. We prove the result by induction on $|\mathsf{C}\lfloor\xi\rfloor_\Phi|$ but we will also prove in the same time that if $\mathsf{C}\lfloor\xi\rfloor_\Phi = \mathsf{C}\lfloor\xi'\rfloor_\Phi$, and $\mathsf{path}(\xi)$, $\mathsf{path}(\xi')$ exist then $\mathsf{path}(\xi') = \mathsf{path}(\xi)$.

Base case $|\mathsf{C}\lfloor\xi\rfloor_\Phi| = 1$*:* In such a case, there exists $(\zeta, i \rhd u) \in \Phi$ such that $\mathsf{path}(\zeta) = \mathsf{path}(\xi)$. Since $\mathsf{C}\lfloor\xi'\rfloor_\Phi = \mathsf{C}\lfloor\xi\rfloor_\Phi$, we deduce that $\mathsf{path}(\xi') = \mathsf{path}(\xi)$ and so $\xi\ \mathcal{R}_{\mathcal{F}_c}\ \xi'$.

Inductive step $|\mathsf{C}\lfloor\xi\rfloor_\Phi| > 1$*:* By definition of a context, it implies that $\xi = \mathsf{f}(\xi_1, \ldots, \xi_n)$ and $\mathsf{C}\lfloor\xi\rfloor_\Phi = \mathsf{f}(\mathsf{C}\lfloor\xi_1\rfloor_\Phi, \ldots, \mathsf{C}\lfloor\xi_n\rfloor_\Phi)$. Similarly, $\xi' = \mathsf{g}(\xi'_1, \ldots, \xi'_n)$ and $\mathsf{C}\lfloor\xi'\rfloor_\Phi = \mathsf{g}(\mathsf{C}\lfloor\xi'_1\rfloor_\Phi, \ldots, \mathsf{C}\lfloor\xi'_n\rfloor_\Phi)$. Since $\mathsf{C}\lfloor\xi\rfloor_\Phi = \mathsf{C}\lfloor\xi'\rfloor_\Phi$, we deduce that $\mathsf{g} = \mathsf{f}$ and for all $i \in \{1, \ldots, n\}$, $\mathsf{C}\lfloor\xi_i\rfloor_\Phi = \mathsf{C}\lfloor\xi'_i\rfloor_\Phi$. If $\mathsf{f} \in \mathcal{F}_c$ then by induction on ξ_i and ξ'_i, we deduce that for all $i \in \{1, \ldots, n\}$, $\xi_i\ \mathcal{R}_{\mathcal{F}_c}\ \xi'_i$. Along with $\mathsf{f} = \mathsf{g}$, we conclude that $\xi\ \mathcal{R}_{\mathcal{F}_c}\ \xi'$.

Else we have $\mathsf{f} = \mathsf{g} \in \mathcal{F}_d$. But ξ and ξ' are recipes in Π_r. Hence it implies that $\mathsf{root}(\xi_1) \notin \mathcal{F}_c$ and $\mathsf{root}(\xi'_1) \notin \mathcal{F}_c$. Hence $\mathsf{path}(\xi)$ and $\mathsf{path}(\xi')$ exists and $\mathsf{path}(\xi) = \mathsf{f} \cdot \mathsf{path}(\xi_1)$, $\mathsf{path}(\xi') = \mathsf{f} \cdot \mathsf{path}(\xi'_1)$. But by inductive hypothesis on ξ_1, ξ'_1, we deduce that $\mathsf{path}(\xi_1) = \mathsf{path}(\xi'_1)$. Hence we conclude that $\mathsf{path}(\xi) = \mathsf{path}(\xi')$ and so $\xi\ \mathcal{R}_{\mathcal{F}_c}\ \xi'$. □

Lemma 53. *Let* $\mathcal{M}$ *be a matrix of constraint system obtained during Step* b *to* d *of Phase* 1 *of the strategy. Let* $\mathcal{M}'$ *be the father of* $\mathcal{M}$. *Let* $\mathcal{C}_1$ *a constraint system in* $\mathcal{M}$ *and* $\mathcal{C}'_1$ *be its father in* $\mathcal{M}'$. *Let* $\mathcal{C}'_2$ *be a constraint system in the column of* $\mathcal{C}'_1$ *in* $\mathcal{M}'$. *Let* $(\sigma'_1, \theta'_1) \in \mathsf{Sol}(\overline{\mathcal{C}'_1})$, $(\sigma'_2, \theta'_2) \in \mathsf{Sol}(\mathcal{C}'_2)$ *and* $(\sigma_1, \theta_1) \in \mathsf{Sol}(\overline{\mathcal{C}_1})$. *If*

1. $\sigma_1|_{vars^1(\mathcal{C}'_1)} = \sigma'_1$, $\theta_1|_{vars^2(\mathcal{C}'_1)} = \theta'_1$;
2. $\sigma'_1|_{S_1(\mathcal{C}'_1)} = \sigma'_2|_{S_1(\mathcal{C}'_2)}$;

3. *for all* $X \in S_2(\mathcal{C}'_1)$, $X\theta'_1 \ \mathcal{R}_{\mathcal{F}_c} \ X\theta'_2$; *and*

4. *for all* $X, Y \in S_2(\mathcal{C}'_2)$, *for all* $p \in \mathcal{P}os(\mathsf{C}\lfloor X\theta'_2 \rfloor_{\Phi(\mathcal{C}'_2)})$, *for all* $p \in \mathcal{P}os(\mathsf{C}\lfloor Y\theta'_2 \rfloor_{\Phi(\mathcal{C}'_2)})$, *if* $\mathsf{path}(X\theta'_2|_p) = \mathsf{path}(X\theta'_2|_{p'})$ *then* $X\theta'_2|_p = X\theta'_2|_{p'}$

then we have that there is a constraint system $\mathcal{C}_2$ *in the same column as* $\mathcal{C}_1$ *in* $\mathcal{M}$ *and* $(\sigma_2, \theta_2) \in \mathsf{Sol}(\mathcal{C}_2)$ *such that*

1. $\mathcal{C}'_2 \to \mathcal{C}_2$

2. $\sigma_2|_{vars^1(\mathcal{C}'_2)} = \sigma'_2$, $\theta_2|_{vars^2(\mathcal{C}'_2)} = \theta'_2$

3. *for all* $X \in S_2(\mathcal{C}_1)$, $X\theta_1 \ \mathcal{R}_{\mathcal{F}_c} \ X\theta_2$

4. *for all* $X, Y \in S_2(\mathcal{C}_2)$, *for all* $p \in \mathcal{P}os(\mathsf{C}\lfloor X\theta_2 \rfloor_{\Phi(\mathcal{C}'_2)})$, *for all* $p \in \mathcal{P}os(\mathsf{C}\lfloor Y\theta_2 \rfloor_{\Phi(\mathcal{C}_2)})$, *if* $\mathsf{path}(X\theta_2|_p) = \mathsf{path}(X\theta_2|_{p'})$ *then* $X\theta_2|_p = X\theta_2|_{p'}$.

Proof. Since $\mathcal{M}'$ is the father of $\mathcal{M}$, we do a case analysis on the rule applied on $\mathcal{M}'$.

Case of internal rule not applied on $\mathcal{C}'_2$*:* In such a case, it implies that $\mathcal{C}'_2$ is also a constraint system in the column of $\mathcal{C}_1$ in the matrix $\mathcal{M}$. Hence, by denoting $\mathcal{C}_2 = \mathcal{C}'_2$, and $(\sigma_2, \theta_2) = (\sigma'_2, \theta'_2)$, we trivially have that the two first wanted properties. Hence, it remains to show that $X\theta_1 = X\theta_2$ for all $X \in S_2(\mathcal{C}_1)$. But since $\mathcal{C}_2$ is in $\mathcal{M}$, we know that $\mathcal{C}_2$ and $\mathcal{C}_1$ have the same structure and so $S_2(\mathcal{C}_1) = S_2(\mathcal{C}_2)$. Similarly, we have $S_2(\mathcal{C}'_1) = S_2(\mathcal{C}'_2)$. At last, the rule applied is an internal rule hence we have $S_2(\mathcal{C}_1) = S_2(\mathcal{C}'_1)$. Thus, $\theta_1|_{vars^2(\mathcal{C}'_1)} = \theta'_1$ implies that for all $X \in S_2(\mathcal{C}_1)$, $X\theta_1 = X\theta'_1$. Hence with $X\theta'_1 \ \mathcal{R}_{\mathcal{F}_c} \ X\theta'_2$ and $\theta_2 = \theta'_2$, then we deduce that $X\theta_1 \ \mathcal{R}_{\mathcal{F}_c} \ X\theta_2$. Moreover, $\theta_2 = \theta'_2$ and hypothesis 4 implies property 4.

Case of internal rule applied on $\mathcal{C}'_2$*:* In such a case, it implies that $\mathcal{C}_1 = \mathcal{C}'_1$ and so $(\sigma_1, \theta_1) = (\sigma'_1, \theta'_1)$. Let $\mathcal{C}_3$ and $\mathcal{C}_4$ be the two constraint system obtained by application of $\textsc{Rule}(\tilde{p})$ on $\mathcal{C}'_2$. By the definition of an internal rule, we know that both $\mathcal{C}_3$ and $\mathcal{C}_4$ are in the column of $\mathcal{C}_1$ in the matrix $\mathcal{M}$.

Thanks to Lemma 42, $(\sigma'_2, \theta'_2) \in \mathsf{Sol}(\mathcal{C}'_2)$ implies that there exists $i \in \{3, 4\}$ and $(\sigma, \theta) \in \mathsf{Sol}(\mathcal{C}_i)$ such that $\sigma|_{S_1(\mathcal{C}_i)} = \sigma'_2|_{S_1(\mathcal{C}'_2)}$. Furthermore, the only possible rule applicable in this case are Axiom, Cons, Eq-frame-frame, Eq-ded-ded and Ded-st. Since the strategy dictates that Eq-ded-ded can only be applied internally when ξ is a variable with $\mathsf{param}_{\mathsf{max}}(\xi) < s$ then, by following the proof of Lemma 42, we deduce for all $X \in S_2(\mathcal{C}'_2)$, $\mathsf{C}\lfloor X\theta \rfloor_{\Phi(\mathcal{C}_i)} = \mathsf{C}\lfloor X\theta'_2 \rfloor_{\Phi(\mathcal{C}_i)}$. But thanks to Lemma 52, we deduce that $X\theta \ \mathcal{R}_{\mathcal{F}_c} \ X\theta'_2$.

Let p, p' positions of $\mathsf{C}\lfloor X\theta \rfloor_{\Phi(\mathcal{C}_i)}$, $\mathsf{C}\lfloor Y\theta \rfloor_{\Phi(\mathcal{C}_i)}$ respectively where $X, Y \in S_2(\mathcal{C})$. Assume that $\mathsf{path}(X\theta|_p) = \mathsf{path}(Y\theta|_{p'})$. But $\mathsf{C}\lfloor X\theta \rfloor_{\Phi(\mathcal{C}_i)} = \mathsf{C}\lfloor X\theta'_2 \rfloor_{\Phi(\mathcal{C}'_1)}$ and $\mathsf{C}\lfloor Y\theta \rfloor_{\Phi(\mathcal{C}_i)} = \mathsf{C}\lfloor Y\theta'_2 \rfloor_{\Phi(\mathcal{C}'_1)}$. Hence $\mathsf{path}(X\theta|_p) = \mathsf{path}(Y\theta|_{p'})$ implies that $\mathsf{path}(X\theta'_2|_p) = \mathsf{path}(Y\theta'_2|_{p'})$. By hypothesis 4, we deduce that $X\theta'_2|_p = Y\theta'_2|_{p'}$. Hence, thanks to $\mathsf{C}\lfloor X\theta \rfloor_{\Phi(\mathcal{C}_i)} = \mathsf{C}\lfloor X\theta'_2 \rfloor_{\Phi(\mathcal{C}'_1)}$, $\mathsf{C}\lfloor Y\theta \rfloor_{\Phi(\mathcal{C}_i)} = \mathsf{C}\lfloor Y\theta'_2 \rfloor_{\Phi(\mathcal{C}'_1)}$ we deduce that $\mathsf{C}\lfloor X\theta|_p \rfloor_{\Phi(\mathcal{C}_i)} = \mathsf{C}\lfloor Y\theta|_p \rfloor_{\Phi(\mathcal{C}_i)}$. Since $X\theta, Y\theta$ conforms to $\Phi(\mathcal{C}_i)\theta$ w.r.t. $\mathsf{NoUse}\theta$, we deduce that $X\theta|_p = Y\theta|_p$. Moreover, since $X\theta$ (resp. $X\theta'_2$) conforms with $\Phi(\mathcal{C}'_1\theta)$ (resp. $\Phi(\mathcal{C}_i\theta'_2)$) and $\mathsf{C}\lfloor X\theta \rfloor_{\Phi(\mathcal{C}_i)} = \mathsf{C}\lfloor X\theta'_2 \rfloor_{\Phi(\mathcal{C}_i)}$ Since $S_2(\mathcal{C}'_2) = S_2(\mathcal{C}_i)$ and by hypothesis, $X\theta'_1 \ \mathcal{R}_{\mathcal{F}_c} \ X\theta'_2$, we have that $X\theta_1 \ \mathcal{R}_{\mathcal{F}_c} \ X\theta'_1 \ \mathcal{R}_{\mathcal{F}_c} \ X\theta'_2 \ \mathcal{R}_{\mathcal{F}_c} \ X\theta$. Hence, the result holds by denoting $\mathcal{C}_2 = \mathcal{C}_i$ and $(\sigma_2, \theta_2) = (\sigma, \theta)$.

Case of external rule: In such a case, the rule $\textsc{Rule}(\tilde{p})$ is applied on both $\mathcal{C}'_1$ and $\mathcal{C}'_2$. The only possible external rules are Cons, Axiom and Eq-ded-ded. By definition of an external application of the rule, we also know that if $\mathcal{C}$ is the right (resp. left) son of $\mathcal{C}_1$ then there exists a constraint system $\mathcal{C}'$ in $\mathcal{M}$ such that $\mathcal{C}'$ is the right (resp. left) son of $\mathcal{C}'_1$. We do a case analysis on the rule applied.

- Rule $\textsc{Cons}(X, \mathsf{f})$, left son: In such a case, $E_\Pi(\mathcal{C}_1) = E_\Pi(\mathcal{C}'_1) \wedge X =^? \mathsf{f}(X_1, \ldots, X_n)$, $E_\Pi(\mathcal{C}_2) = E_\Pi(\mathcal{C}'_2) \wedge X =^? \mathsf{f}(X_1, \ldots, X_n)$; and $E(\mathcal{C}_1) = E(\mathcal{C}'_1) \wedge X\delta^1(\mathcal{C}'_1) =^? \mathsf{f}(x_1, \ldots, x_n)$, $E(\mathcal{C}_2) = E(\mathcal{C}'_2) \wedge X\delta^1(\mathcal{C}'_2) =^? \mathsf{f}(y_1, \ldots, y_n)$ where X_i, x_i, y_i are fresh variables for all $i \in \{1, \ldots, n\}$ in $S_2(\mathcal{C}_1) = S_2(\mathcal{C}_2)$. Moreover, $X \in S_2(\mathcal{C}'_1) = S_2(\mathcal{C}'_2)$.

  By hypothesis, we know that $(\sigma_1, \theta_1) \in \mathsf{Sol}(\overline{\mathcal{C}_1})$, $\theta_1|_{vars^2(\mathcal{C}'_1)}$ and $(\sigma'_2, \theta'_2) \in \mathsf{Sol}(\overline{C'_2})$. Hence $\theta_1 \vDash E_\Pi(\mathcal{C}_1)$ implies that $\mathsf{root}(X\theta'_1) = \mathsf{f} \in \mathcal{F}_c$. But $X\theta'_1 \ \mathcal{R}_{\mathcal{F}_c} \ X\theta'_2$ thus we deduce that $\mathsf{root}(X\theta'_2) = \mathsf{f}$. We define $\theta_2 = \theta'_2 \cup \{X_1 \mapsto X\theta'_2|_1; \ldots X_n \mapsto X\theta'_2|_n\}$. We show that for all $i \in \{1, \ldots, n\}$, $X_i\theta_1 \ \mathcal{R}_{\mathcal{F}_c} \ X_i\theta_2$. $\mathsf{root}(X\theta'_2) = \mathsf{root}(X\theta'_1) =\in \mathcal{F}_c$ and $X\theta'_1 \ \mathcal{R}_{\mathcal{F}_c} \ X\theta'_2$ implies by definition of $\mathcal{R}_{\mathcal{F}_c}$ that $X\theta'_1 = \mathsf{f}(\xi_1, \ldots, \xi_n)$ and $X\theta'_2 = \mathsf{f}(\zeta_1, \ldots, \zeta_n)$ for some $\xi_1, \ldots, \xi_n, \zeta_1, \ldots, \zeta_n$, and for all $i \in \{1, \ldots, n\}$, $\xi_i \ \mathcal{R}_{\mathcal{F}_c} \ \zeta_i$. Since for all $i \in \{1, \ldots, n\}$, $X_i\theta_1 = \xi_i$ and $X_i\theta_2 = \zeta_i$, the result holds.

  Moreover, since for all $i \in \{1, \ldots, n\}$, $\mathsf{C}\lfloor\zeta_i\rfloor_{\Phi(\mathcal{C}_2)}$ is a subterm of $\mathsf{C}\lfloor X\theta'_2\rfloor_{\Phi(\mathcal{C}_2)}$, then hypothesis 4 implies property 4.

  It remains to build σ_2. Since $(\sigma'_2, \theta'_2) \in \mathsf{Sol}(\mathcal{C}'_2)$, we know that $X\theta'_2(\Phi(\mathcal{C}'_2)\sigma'_2)\downarrow = \mathsf{f}(u_1, \ldots, u_n)$ where for all $i \in \{1, \ldots, n\}$, $\zeta_i(\Phi(\mathcal{C}'_2)\sigma'_2)\downarrow = u_i$. Since $y_1, \ldots, y_n$ are fresh variables, we define $\sigma_2 = \sigma'_2 \cup \{y_1 \mapsto u_1, \ldots, y_n \mapsto u_n\}$. Hence $\sigma_2 \vDash X\delta^1(\mathcal{C}'_2) =^? \mathsf{f}(y_1, \ldots, y_n)$. Hence we conclude that $(\sigma_2, \theta_2) \in \mathsf{Sol}(\overline{\mathcal{C}_2})$.

- Rule $\textsc{Cons}(X, \mathsf{f})$, right son: In such a case, $E_\Pi(\mathcal{C}_1) = E_\Pi(\mathcal{C}'_1) \wedge \mathsf{root}(X) \neq^? \mathsf{f}$ and $E_\Pi(\mathcal{C}_2) = E_\Pi(\mathcal{C}'_2) \wedge \mathsf{root}(X) \neq \mathsf{f}$. By hypothesis, we know that $(\sigma_1, \theta_1) \in \mathsf{Sol}(\overline{\mathcal{C}_1})$, $\theta_1|_{vars^2(\mathcal{C}'_1)}$ and $(\sigma'_2, \theta'_2) \in \mathsf{Sol}(\overline{C'_2})$. Hence $\theta'_1 \vDash E_\Pi(\mathcal{C}_1)$ implies that $\mathsf{root}(X\theta'_1) \neq \mathsf{f} \in \mathcal{F}_c$. But $X\theta'_1 \ \mathcal{R}_{\mathcal{F}_c} \ X\theta'_2$ thus we deduce that $\mathsf{root}(X\theta'_2) \neq \mathsf{f}$. Hence the result holds with $(\sigma_2, \theta_2) = (\sigma'_2, \theta'_2)$. Moreover, hypothesis 4 trivially implies property 4.

- Rule $\textsc{Axiom}(X, \mathsf{path})$, left son: $E_\Pi(\mathcal{C}_1) = E_\Pi(\mathcal{C}'_1) \wedge X =^? \xi_1$, $E_\Pi(\mathcal{C}_2) = E_\Pi(\mathcal{C}'_2) \wedge X =^? \xi_2$, $E(\mathcal{C}_1) = E(\mathcal{C}'_1) \wedge X\delta^1(\mathcal{C}'_1) =^? \mathsf{path}(\xi_1)\delta^1(\mathcal{C}'_1)$ and $E(\mathcal{C}_2) = E(\mathcal{C}'_2) \wedge X\delta^1(\mathcal{C}'_2) =^? \mathsf{path}(\xi_2)\delta^1(\mathcal{C}'_2)$ where $\mathsf{path}(\xi_1) = \mathsf{path}(\xi_2)$.

  By hypothesis, we know that $(\sigma_1, \theta_1) \in \mathsf{Sol}(\overline{\mathcal{C}_1})$, $\theta_1|_{vars^2(\mathcal{C}'_1)}$ and $(\sigma'_2, \theta'_2) \in \mathsf{Sol}(\overline{C'_2})$. Hence $\theta_1 \vDash E_\Pi(\mathcal{C}_1)$ implies $X\theta'_1 = \xi_1\theta'_1$. But $X\theta'_1 \ \mathcal{R}_{\mathcal{F}_c} \ X\theta'_2$ hence since $\mathsf{path}(X\theta'_1$ exists, we deduce that $\mathsf{path}(X\theta'_2)$ exists and $\mathsf{path}(X\theta'_2) = \mathsf{path}(X\theta'_1)$. Moreover, $(\sigma'_2, \theta'_2) \in \mathsf{Sol}(\overline{C'_2})$ also implies that $X\theta'_2$ conforms with $\Phi(\mathcal{C}'_2)\theta'_2$ w.r.t. $\mathsf{NoUse}\theta'_2$. Hence since ξ_2 is a recipe of a frame element of $\Phi(\mathcal{C}'_2)$ such that $\mathsf{path}(\xi_2) = \mathsf{path}(\xi_1) = \mathsf{path}(X\theta'_2)$, we conclude that $X\theta'_2 = \xi_2\theta'_2$. Hence $\theta'_2 \vDash E_\Pi(\mathcal{C}_2)$. Moreover, hypothesis 4 trivially implies property 4.

  Since $(\sigma'_1, \theta'_1) \in \mathsf{Sol}(\overline{\mathcal{C}'_1})$, $(\sigma'_2, \theta'_2) \in \mathsf{Sol}(\overline{\mathcal{C}'_2})$ and $\sigma'_1|_{S_1(\mathcal{C}'_1)} = \sigma'_2|_{S_1\mathcal{C}'_2}$ then by Lemma 48, we have that $X\delta^1(\mathcal{C}'_2)\sigma'_2 = X\delta^1(\mathcal{C}'_1)\sigma'_1$ and $\mathsf{path}(\xi_1)\delta^1(\mathcal{C}'_1)\sigma'_1 = \mathsf{path}(\xi_2)\delta^1(\mathcal{C}'_2)\sigma'_2$. Hence, σ'_1 satisfies $X\delta^1(\mathcal{C}'_1) =^? Y\delta^1(\mathcal{C}'_1)$ implies that $\sigma'_2 \vDash X\delta^1(\mathcal{C}'_2) =^? \mathsf{path}(\xi_2)\delta^1(\mathcal{C}'_2)$. Hence $(\sigma'_2, \theta'_2) \in \mathsf{Sol}(\mathcal{C}_2)$.

- Rule $\textsc{Axiom}(X, \mathsf{path})$, right son: $E_\Pi(\mathcal{C}_1) = E_\Pi(\mathcal{C}'_1) \wedge X \neq^? \xi_1$, $E_\Pi(\mathcal{C}_2) = E_\Pi(\mathcal{C}'_2) \wedge X \neq^? \xi_2$. By hypothesis, we know that $(\sigma_1, \theta_1) \in \mathsf{Sol}(\overline{\mathcal{C}_1})$, $\theta_1|_{vars^2(\mathcal{C}'_1)}$ and $(\sigma'_2, \theta'_2) \in$

$\mathsf{Sol}(\overline{C'_2})$. Hence $\theta_1 \vDash E_\Pi(\mathcal{C}_1)$ implies $X\theta'_1 \neq^? \xi_1\theta'_1$. Since $X\theta'_1$ conforms with $\Phi(\mathcal{C}'_1)\theta'_1$ w.r.t. $\mathsf{NoUse}(\mathcal{C}'_1)\theta'_1$, it also implies that $\mathsf{path}(X\theta'_1) \neq^? \mathsf{path}(\xi_1)$. But $X\theta'_1 \mathcal{R}_{\mathcal{F}_c} X\theta'_2$ hence $\mathsf{path}(X\theta'_2) = \mathsf{path}(X\theta'_1)$ and so $\mathsf{path}(X\theta'_2) \neq \mathsf{path}(\xi_2)$. Thus, we deduce that $X\theta'_2 \neq \xi_2\theta'_2$ and so the result holds with $(\sigma_2, \theta_2) = (\sigma'_2, \theta'_2)$.

- Rule Eq-ded-ded(X, ξ), left son: $E_\Pi(\mathcal{C}_1) = E_\Pi(\mathcal{C}'_1) \wedge X =^? Y$, $E_\Pi(\mathcal{C}_2) = E_\Pi(\mathcal{C}'_2) \wedge X =^? Y$, $E(\mathcal{C}_1) = E(\mathcal{C}'_1) \wedge X\delta^1(\mathcal{C}'_1) =^? Y\delta^1(\mathcal{C}'_1)$ and $E(\mathcal{C}_2) = E(\mathcal{C}'_2) \wedge X\delta^1(\mathcal{C}'_2) =^? Y\delta^1(\mathcal{C}'_2)$. By hypothesis, we know that $(\sigma_1, \theta_1) \in \mathsf{Sol}(\overline{\mathcal{C}_1})$, $\theta_1|_{vars^2(\mathcal{C}'_1)}$ and $(\sigma'_2, \theta'_2) \in \mathsf{Sol}(\overline{C'_2})$. Hence $\theta_1 \vDash E_\Pi(\mathcal{C}_1)$ implies $X\theta'_1 = Y\theta'_1$. But $X\theta'_1 \mathcal{R}_{\mathcal{F}_c} X\theta'_2$ and $Y\theta'_1 \mathcal{R}_{\mathcal{F}_c} Y\theta'_2$. Hence, we deduce that $X\theta'_2 \mathcal{R}_{\mathcal{F}_c} Y\theta'_2$. Moreover, thanks to hypothesis 4, $X\theta'_2 \mathcal{R}_{\mathcal{F}_c} Y\theta'_2$ implies that $X\theta'_2 = Y\theta'_2$ and so $\theta'_2 \vDash E_\Pi(\mathcal{C}_2)$.

  Since $(\sigma'_1, \theta'_1) \in \mathsf{Sol}(\overline{\mathcal{C}'_1})$, $(\sigma'_2, \theta'_2) \in \mathsf{Sol}(\overline{\mathcal{C}'_2})$ and $\sigma'_1|_{S_1(\mathcal{C}'_1)} = \sigma'_2|_{S_1\mathcal{C}'_2}$ then by Lemma 48, we have that $X\delta^1(\mathcal{C}'_2)\sigma'_2 = X\delta^1(\mathcal{C}'_1)\sigma'_1$ and $Y\delta^1(\mathcal{C}'_1)\sigma'_1 = Y\delta^1(\mathcal{C}'_2)\sigma'_2$. Hence, σ'_1 satisfies $X\delta^1(\mathcal{C}'_1) =^? Y\delta^1(\mathcal{C}'_1)$ implies that $\sigma'_2 \vDash X\delta^1(\mathcal{C}'_2) =^? Y\delta^1(\mathcal{C}'_2)$. Hence $(\sigma'_2, \theta'_2) \in \mathsf{Sol}(\mathcal{C}_2)$. Thus the result holds with $(\sigma_2, \theta_2) = (\sigma'_2, \theta'_2)$.

- Rule Eq-ded-ded(X, ξ), right son: $E(\mathcal{C}_1) = E(\mathcal{C}'_1) \wedge X\delta^1(\mathcal{C}'_1) \neq^? Y\delta^1(\mathcal{C}'_1)$ and $E(\mathcal{C}_2) = E(\mathcal{C}'_2) \wedge X\delta^1(\mathcal{C}'_2) =^? Y\delta^1(\mathcal{C}'_2)$. Since $(\sigma'_1, \theta'_1) \in \mathsf{Sol}(\overline{\mathcal{C}'_1})$, $(\sigma'_2, \theta'_2) \in \mathsf{Sol}(\overline{\mathcal{C}'_2})$ and $\sigma'_1|_{S_1(\mathcal{C}'_1)} = \sigma'_2|_{S_1\mathcal{C}'_2}$ then by Lemma 48, we have that $X\delta^1(\mathcal{C}'_2)\sigma'_2 = X\delta^1(\mathcal{C}'_1)\sigma'_1$ and $Y\delta^1(\mathcal{C}'_1)\sigma'_1 = Y\delta^1(\mathcal{C}'_2)\sigma'_2$. Hence, σ'_1 satisfies $X\delta^1(\mathcal{C}'_1) \neq^? Y\delta^1(\mathcal{C}'_1)$ implies that $\sigma'_2 \vDash X\delta^1(\mathcal{C}'_2) \neq^? Y\delta^1(\mathcal{C}'_2)$. Hence $(\sigma'_2, \theta'_2) \in \mathsf{Sol}(\mathcal{C}_2)$. Thus the result holds with $(\sigma_2, \theta_2) = (\sigma'_2, \theta'_2)$. □

Appendix F.3. Existence of a solution

Lemma 54. *Let $\mathcal{M}$ be a matrix of constraint system obtained after applying Step e of Phase 1 of the strategy for some support s. Let $\mathcal{C}$ be a constraint system in $\mathcal{M}$. We have that $\mathsf{Sol}(\overline{\mathcal{C}}) = \mathsf{Sol}(\mathcal{C})$*

Proof. We prove this result by induction of the support s of the Step e. For the purpose of the induction, we assume that Step e of Phase 1 with support 0 corresponds to the initial matrix, i.e. the row matrix made of initial constaint systems. Note that an initial constraint system does not contain any deducibility constraint, and therefore the property trivially holds.

Base case $s = 0$: In such a case, we know that $\mathcal{M}$ is a row matrix of initial constraint systems. Hence, we trivially have that $\mathsf{Sol}(\mathcal{C}) = \mathsf{Sol}(\overline{\mathcal{C}})$ and so the result holds.

Inductive step $s > 0$: Let $(\sigma, \theta) \in \mathsf{Sol}(\overline{\mathcal{C}})$. Thanks to Lemma 51, we know that there exists θ' such that $(\sigma, \theta') \in \mathsf{Sol}(\overline{\mathcal{C}})$ and

1. for all $X \in vars^2(D(\mathcal{C}))$, for all position p of $\mathsf{C}\lfloor X\theta' \rfloor_{\Phi(\mathcal{C})}$, if $\mathsf{root}(\mathsf{C}\lfloor X\theta' \rfloor_{\Phi(\mathcal{C})}) \in \mathcal{F}_d$, then there is no recipe $\xi \in \Pi_r$ such that $\xi(\Phi(\mathcal{C})\sigma)\downarrow = X\theta'|_p(\Phi(\mathcal{C})\sigma)\downarrow$ and $\mathsf{param}_{\mathsf{max}}(\xi') < \mathsf{param}_{\mathsf{max}}(X\theta'|_p)$; and
2. for all $\xi, \xi' \in st(\{X\theta' \mid X \in vars^2(D(\mathcal{C}))\})$, $\mathsf{path}(\xi) = \mathsf{path}(\xi')$ implies $\xi = \xi'$.

Since $s > 0$, we also know that there exists a matrix $\mathcal{M}_1$ ancestor of $\mathcal{M}$ such that $\mathcal{M}_1$ is obtained at the end of Step a of the first phase with support s. Hence, there exists a constraint system $\mathcal{C}_1$ ancestor of $\mathcal{C}$ such that $\mathcal{C}_1$ is in $\mathcal{M}_1$.

By a simple induction on the number of rule applied between $\mathcal{M}_1$ and $\mathcal{M}$, we prove, thanks to Lemma 5, that there exists $(\sigma_1, \theta_1) \in \mathsf{Sol}(\overline{\mathcal{C}_1})$ such that $\sigma|_{vars^1(\mathcal{C}_1)} = \sigma_1$ and $\theta|_{vars^2(\mathcal{C}_2)} = \theta_1$.

Let $X \in vars^2(D(\mathcal{C}_1))$ and p a position of $\mathsf{C}\lfloor X\theta_1 \rfloor_{\Phi(\mathcal{C}_1)}$ such that $\mathsf{root}(\mathsf{C}\lfloor X\theta_1 \rfloor_{\Phi(\mathcal{C}_1)}|_p) \in \mathcal{F}_d$. We show that there exists $Y \in vars^2(D(\mathcal{C}))$ and p' a position of $\mathsf{C}\lfloor X\theta \rfloor_{\Phi(\mathcal{C})}$ such that $\mathsf{root}(\mathsf{C}\lfloor Y\theta \rfloor_{\Phi(\mathcal{C})}|_{p'}) \in \mathcal{F}_d$.

The rule DEST was never applied to obtained $\mathcal{M}$ from $\mathcal{M}_1$, thus $\theta|_{vars^2(\mathcal{C}_2)} = \theta_1$ implies that $\mathsf{root}(\mathsf{C}\lfloor X\theta_1 \rfloor_{\Phi(\mathcal{C}_1)}|_p) = \mathsf{root}(\mathsf{C}\lfloor X\theta \rfloor_{\Phi(\mathcal{C})}|_p) \in \mathcal{F}_d$, and so $\mathsf{root}(\mathsf{C}\lfloor X\theta_1 \rfloor_{\Phi(\mathcal{C}_1)}|_p) \in \mathcal{F}_d$ implies $\mathsf{root}(\mathsf{C}\lfloor X\theta \rfloor_{\Phi(\mathcal{C})}|_p) \in \mathcal{F}_d$. But thanks to Property 7 of a well formed constraint system, we know that $\mathsf{C}\lfloor X\mathsf{mgu}(E_\Pi(\mathcal{C})) \rfloor_{\Phi(\mathcal{C})} \in \mathcal{T}(\mathcal{F}_c \cup (\mathcal{F}_d^* \cdot \mathcal{AX}))$ and for all $Y \in vars^2(X\mathsf{mgu}(E_\Pi(\mathcal{C}))$, $Y \in vars^2(D(\mathcal{C}))$. Hence, $\mathsf{root}(\mathsf{C}\lfloor X\theta \rfloor_{\Phi(\mathcal{C})}|_p) \in \mathcal{F}_d$ implies that there exists $Y \in vars^2(D(\mathcal{C}))$ and a position p' such that $Y\theta|_{p'} = X\theta|_p$ and $\mathsf{root}(\mathsf{C}\lfloor Y\theta \rfloor_{\Phi(\mathcal{C})}|_{p'}) \in \mathcal{F}_d$.

Hence, we deduce that (σ_1, θ_1) satisfies:

1. for all $X \in vars^2(D(\mathcal{C}_1))$, for all position p of $\mathsf{C}\lfloor X\theta_1 \rfloor_{\Phi(\mathcal{C}_1)}$, if $\mathsf{root}(\mathsf{C}\lfloor X\theta_1 \rfloor_{\Phi(\mathcal{C})}) \in \mathcal{F}_d$, then there is no recipe $\xi \in \Pi_r$ such that $\xi(\Phi(\mathcal{C}_1)\sigma)\downarrow = X\theta_1|_p(\Phi(\mathcal{C}_1)\sigma)\downarrow$ and $\mathsf{param}_{\mathsf{max}}(\xi) < \mathsf{param}_{\mathsf{max}}(X\theta_1|_p)$; and
2. for all $\xi, \xi' \in st(\{X\theta_1 \mid X \in vars^2(D(\mathcal{C}_1))\})$, $\mathsf{path}(\xi) = \mathsf{path}(\xi')$ implies $\xi = \xi'$.

Moreover, let $\mathcal{M}_2$ be the matrix ancestor of $\mathcal{M}_1$ obtained from Step e with support $s-1$. Thanks to our inductive hypothesis, we know that for all constraint system $\mathcal{C}_0$ in $\mathcal{M}_2$, we have $\mathsf{Sol}(\overline{\mathcal{C}_0}) = \mathsf{Sol}(\mathcal{C}_0)$. Hence, we can apply Lemma 50 on $\mathcal{C}_1$ and (σ_1, θ_1) which implies that there exists a constraint system $\mathcal{C}_2$ in the same column of $\mathcal{C}_1$ and there exists $(\sigma_2, \theta_2) \in \mathsf{Sol}(\mathcal{C}_2)$ such that $\sigma_1|_{S_1(\mathcal{C}_1)} = \sigma_2|_{S_1\mathcal{C}_2}$ and for all $X \in S_2(\mathcal{C}_1)$, $X\theta_1 = X\theta_2$. $X\theta_1 = X\theta_2$ trivially implies that $X\theta_1 \mathcal{R}_{\mathcal{F}_c} X\theta_2$. Moreover, since $X\theta_1 = X\theta_2$ and for all $\xi, \xi' \in st(\{X\theta_1 \mid X \in vars^2(D(\mathcal{C}_1))\})$, $\mathsf{path}(\xi) = \mathsf{path}(\xi')$ implies $\xi = \xi'$, we deduce that for all $X, Y \in S_2(\mathcal{C}_2)$, for all $p \in \mathcal{P}os(\mathsf{C}\lfloor X\theta'_2 \rfloor_{\Phi(\mathcal{C}_2)})$, for all $p \in \mathcal{P}os(\mathsf{C}\lfloor Y\theta'_2 \rfloor_{\Phi(\mathcal{C}'_2)})$, if $\mathsf{path}(X\theta'_2|_p) = \mathsf{path}(X\theta'_2|_{p'})$ then $X\theta'_2|_p = X\theta'_2|_{p'}$.

Once again with a simple induction on the number of rule applied between $\mathcal{M}_1$ and $\mathcal{M}$, we use Lemma 53 to prove that there exists a constraint system $\mathcal{C}'$ in the column of $\mathcal{C}$ in $\mathcal{M}$ and $(\sigma'', \theta'') \in \mathsf{Sol}(\mathcal{C}')$ such that $\sigma''|_{S_1(\mathcal{C}')} = \sigma|_{S_1(\mathcal{C})}$ and for all $X \in S_2(\mathcal{C})$, $X\theta' = X\theta''$.

But thanks to Lemma 26, we know that the matrix $\mathcal{M}$ satisfies $\mathsf{InvMatrix}(s)$. Thus there exists a renaming ρ of first order variable such that:

- $\{x\rho \mid (X, i \vdash^? x) \in D(\mathcal{C}) \wedge i \leq s\} = \{x \mid (X, i \vdash^? x) \in D(\mathcal{C}') \wedge i \leq s\}$
- $\{u\rho \mid (\xi, i \rhd u) \in \Phi(\mathcal{C}) \wedge i \leq s\} = \{u \mid (\xi, i \rhd u) \in \Phi(\mathcal{C}') \wedge i \leq s\}$
- $ND(\mathcal{C})\rho = ND(\mathcal{C}')$

Moreover, $(\sigma, \theta') \in \mathsf{Sol}(\overline{\mathcal{C}})$, $(\sigma'', \theta'') \in \mathsf{Sol}(\mathcal{C}')$ and $\sigma|_{S_1(\mathcal{C})} = \sigma''|_{S_1(\mathcal{C}')}$. Hence by Lemma 48, we can deduce that for all $(X, i \vdash^? x) \in D(\mathcal{C}')$, with $i \leq s$, we have that $(X, i \vdash^? x\rho) \in D(\mathcal{C}')$ and $x\sigma'' = x\rho\sigma$. Thus with $ND(\mathcal{C})\rho = ND(\mathcal{C}')$ and $(\sigma'', \theta') \in \mathsf{Sol}(\mathcal{C}')$, we have that $\sigma'' \vDash ND(\mathcal{C}')$ which implies $\sigma'' \vDash ND(\mathcal{C})\rho$. Since for all $x \in vars^1(ND(\mathcal{C}))$, $\mathcal{L}^1_{\mathcal{C}}(x) \leq s$, we conclude that $\rho\sigma \vDash ND(\mathcal{C})\rho$ which implies that $\sigma \vDash ND(\mathcal{C})$ and so $(\sigma, \theta) \in \mathsf{Sol}(\mathcal{C})$. □

Lemma 55. *Let $(\mathcal{M}, \mathcal{M}')$ be a pair of matrix obtained at the end strategy. For all constraint system $\mathcal{C}$ in $\mathcal{M}$ or $\mathcal{M}'$, $\mathsf{Sol}(\mathcal{C}) = \mathsf{Sol}(\overline{\mathcal{C}})$.*

Proof. Let $(\sigma, \theta) \in \mathsf{Sol}(\overline{\mathcal{C}})$. Let $\mathcal{C}'$ be the constraint system ancestor of $\mathcal{C}$ such that $\mathcal{C}'$ is on the matrix obtained from the last Step e of Phase 1. With a simple induction on the number of rule applied from $\mathcal{C}'$ to $\mathcal{C}$, we use Lemma 5 to show that there exists $(\sigma', \theta') \in \mathsf{Sol}(\overline{\mathcal{C}'})$ with $\sigma|_{vars^1(\mathcal{C}')} = \sigma'$. But by Lemma 54, we know that $(\sigma', \theta') \in \mathsf{Sol}(\mathcal{C}')$. Furthermore, the rules applied on phase 2 of the strategy do not add new non-deducible constraint system hence we can deduce that $\sigma' \vDash ND(\mathcal{C}')$ and $\sigma|_{vars^1(\mathcal{C}')} = \sigma'$ implies that $\sigma \vDash ND(\mathcal{C})$ and so $(\sigma, \theta) \in \mathsf{Sol}(\mathcal{C})$. □

Using Lemma 55, we can now show that any constraint system on a leaf that is different from $\bot$ has at least one solution.

Lemma 56. *Let $(\mathcal{M}, \mathcal{M}')$ be a pair of matrix obtained at the end strategy. Let $\mathcal{C}$ be a constraint system in $\mathcal{M}$ or $\mathcal{M}'$ different from $\bot$. There exists $(\sigma, \theta) \in \mathsf{Sol}(\mathcal{C})$.*

Proof. Assume that $\mathcal{C} \neq \bot$. Thanks to Lemma 47, we know that $(\mathcal{M}, \mathcal{M}')$ is in solved form. Hence we deduce that $\mathcal{C}$ satisfies $\mathsf{InvVarConstraint}(\mathsf{s}_{max})$ and all right hand terms of deducible constraints are distinct variables. Therefore, for each deducibility constraint $(X, i \vdash^? x) \in D(\mathcal{C})$, we can define θ on $vars^2(D(\mathcal{C}))$ such that $X\theta \in \mathcal{T}(\mathcal{F}_c, \{ax_1\})$ for all $X \in vars^2(D(\mathcal{C}))$.

We show that for all u, $(ax_1, 1 \rhd u) \notin \mathsf{NoUse}(\mathcal{C})$. $(\mathcal{M}, \mathcal{M}')$ is in solved form implies that $\mathcal{C}$ is well-formed. Hence, if $(ax_1, 1 \rhd u) \in \mathsf{NoUse}(\mathcal{C})$ then by Definition 18, item 8, there exists $X \in vars^2(\mathcal{C})$ such that $\mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(X\mathsf{mgu}(E_\Pi(\mathcal{C}))) < 1$ which is impossible. Hence $(ax_1, 1 \rhd u) \notin \mathsf{NoUse}(\mathcal{C})$ and so for all $\xi \in \mathcal{T}(\mathcal{F}_c, \{ax_1\})$, for all θ, ξ conforms to $\Phi\theta$ w.r.t. $\mathsf{NoUse}\theta$.

Since the set $\mathcal{T}(\mathcal{F}_c, \{ax_1\})$ is infinite, we have an infinite set of pair of substitutions (σ, θ) where for all $(X, i \vdash^? x) \in D(\mathcal{C})$, $X\theta(\Phi\sigma)\downarrow = x\sigma$, $param(X\theta) = \{ax_1\} \subseteq \{ax_1, \ldots, ax_i\}$ and $X\theta$ conforms to $\Phi\theta$ w.r.t. $\mathsf{NoUse}\theta$. We extend each of (σ, θ) by (σ', θ') such that $\theta'|_{vars^2(D(\mathcal{C}))} = \theta$, $\sigma'|_{vars^1(D(\mathcal{C}))} = \sigma$, for all $X \in vars^2(\mathcal{C}) \backslash vars^2(D(\mathcal{C}))$, $X\theta' = X\mathsf{mgu}(E_\Pi)\theta$; and for all $x \in vars^1(\mathcal{C}) \setminus vars^1(\mathcal{C})$, $x\sigma' = x\mathsf{mgu}(E)\sigma$. Hence obtain an infinite set of pre-solution (σ, θ) of $\mathcal{C}$ such that $\sigma \vDash \mathsf{mgu}(E)$ and $\theta \vDash \mathsf{mgu}(E_\Pi)$. Moreover, we also know that for all $(X, i \vdash^? x) \in D(\mathcal{C})$, for all $\mathsf{f} \in \mathcal{F}_c$, $E_\Pi \nvDash \mathsf{root}(X) \neq^? \mathsf{f}$. At last, we also know that $E_\Pi \nvDash X \neq^? ax_1$. Hence, we deduce that $\theta \vDash E_\Pi$.

It remains to prove that there exists a pre-solution in this infinite set that satisfies the inequations in $E(\mathcal{C})$. Since each variable in the inequations are a variable of $vars^1(D(\mathcal{C}))$ and the set of possible values for each of these variable is infinite. Then, thanks to [36], we deduce that there exists at least one (σ_0, θ_0) of pre-solution such that $\sigma_0 \vDash E(\mathcal{C})$ and so $(\sigma_0, \theta_0) \in \mathsf{Sol}(\overline{\mathcal{C}})$. Therefore, thanks to Lemma 55, we deduce that $(\sigma_0, \theta_0) \in \mathsf{Sol}(\mathcal{C})$ and so the result holds. □

Lastly, we are interested in the symbolic equivalence of matrices of constraint systems. But in fact, when the matrices are in solved form, we can show that any constraint system on the same row of the matrices are symbolically equivalent.

Definition 23. *Let $\mathcal{C} = (S_1, S_2, \Phi, D, E, E_\Pi, ND)$ be a well formed solved constraint system. Let σ be a substitution mapping $vars^1(\mathcal{C})$ to ground messages. We define a new semantics on logic formula built upon elementary formulas using classical connectives.*

The semantics for the elementary formulas are given below and is extended as expected to general formulas. We have: for all $i \in \mathbb{N}$, for all $u, v \in \mathcal{T}(\mathcal{F}_c, \mathcal{N} \cup \mathcal{X}^1)$,

- $\sigma \vDash_{\leq i} u =^? v$ *if* $\sigma \vDash u =^? v$
- $\sigma \vDash_{\leq i} u \neq^? v$ *if* $\sigma \vDash u \neq^? v$ *or there exists* $x \in vars^1(u) \cup vars^1(v)$ *such that* $\mathcal{L}^1_{\mathcal{C}}(x) > i$

Lemma 57. *Let $\mathcal{C}$ be a well formed solved constraint system on a leaf. Let $n \in \mathbb{N}$. Let (σ, θ) such that:*

- $\sigma \vDash_{\leq n} E(\mathcal{C})$
- *for all* $(X, i \vdash^? u) \in D(\mathcal{C})$, $X\theta\Phi(\mathcal{C})\sigma{\downarrow} = u\sigma$ *and* $\mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(X\theta) \leq i$
- *for all* $(X, i \vdash^? u) \in D(\mathcal{C})$, $\mathsf{C}\lfloor X\theta \rfloor_{\Phi(\mathcal{C})} \in \mathcal{T}(\mathcal{F}_c \cup (\mathcal{F}_d^* \cdot \mathcal{A}\mathcal{X}))$ *and for* $(\xi, j \rhd v) \in \Phi(\mathcal{C})$, *if* $\mathsf{path}(\xi) \in st(\mathsf{C}\lfloor X\theta \rfloor_{\Phi(\mathcal{C})})$ *then* $j \leq i$.
- *for all* $X \in D(\mathcal{C})$, $X\theta$ *conforms to* $\Phi(\mathcal{C})\theta$ *w.r.t.* $\mathsf{NoUse}(\mathcal{C})\theta$

There exists $(\sigma', \theta') \in \mathsf{Sol}(\mathcal{C})$ *such that* $\sigma|_{\{x | \mathcal{L}^1_{\mathcal{C}}(x) \leq n\}} = \sigma'|_{\{x | \mathcal{L}^1_{\mathcal{C}}(x) \leq n\}}$

Proof. Since $\mathcal{C}$ is in solved formed, we know that it satisfies $\mathsf{InvVarConstraint}(\mathsf{s}_{max})$. Hence, we have that for all $(X, i \vdash^? u) \in D(\mathcal{C})$, u is a variable. Furthermore, all right hand variables of the deducibility constraints are distinct. Thus, for all $(X, i \vdash^? x) \in D(\mathcal{C})$, $\mathcal{L}^1_{\mathcal{C}}(x) = i$.

Let $\sigma_0 = \sigma_{\{} x | \mathcal{L}^1_{\mathcal{C}}(x) \leq n\}$. Let $D_0 = \{(X, i \vdash^? x) \in D(\mathcal{C}) \mid i > n\}$, $\Phi_0 = \mathsf{Init}(\Phi)\sigma_0$ and $E_0 = E(\mathcal{C})\sigma_0$. D_0, Φ_0 and E_0 represent a simplified version of $\mathcal{C}$ where we fixed the value of the variables in $\mathrm{dom}(\sigma_0)$.

Let $(ax_1, 1 \rhd u) \in \Phi_0$. Thanks to the origination property of a constraint system, we know that $vars^1(u) = \emptyset$. Furthermore, since $\mathcal{C}$ is a well formed constraint system, we also have that $(ax_1, 1 \rhd u) \notin \mathsf{NoUse}(\mathcal{C})$. Hence for all $\xi \in \mathcal{T}(\mathcal{F}_c \cup \{ax_1\})$, for all substitution λ, we have $\xi(\Phi_0\lambda){\downarrow} \in \mathcal{T}(\mathcal{F}_c, \mathcal{N})$. Thus for all $(X, i \vdash^? x) \in D_0$, x can be instantiated by any recipe $\xi \in \mathcal{T}(\mathcal{F}_c \cup \{ax_1\})$. But the set $\mathcal{T}(\mathcal{F}_c \cup \{ax_1\})$ is an infinite set and for all $x \in vars^1(E_0)$, $x \in vars^1(D_0)$. Therefore, thanks to [36], we deduce that there exists a substitution (σ_1, θ_1) such that $\mathrm{dom}(\theta_1) = vars^2(D_0)$, $\mathrm{dom}(\sigma_1) = vars^1(D_0)$ and:

- for all $(X, i \vdash^? x) \in D_0$, $X\theta_1 \in \mathcal{T}(\mathcal{F}_c \cup \{ax_1\})$ and $x\sigma_1 = X\theta_1(\Phi_0\sigma_1){\downarrow}$
- σ_1 satisfies the inequations of E_0.

We define θ' such that:

- for all $X \in vars^2(D(\mathcal{C})) \setminus vars^2(D_0)$, $X\theta' = X\theta$
- for all $X \in vars^2(D_0)$, $X\theta' = X\theta_1$
- for all $X \in vars^2(\mathcal{C}) \setminus vars^2(D(\mathcal{C}))$, $X\theta' = X\mathsf{mgu}(E_{\Pi}(\mathcal{C}))\theta'$.

Furthermore, we define σ' such that:

- $\sigma'|_{\{x | \mathcal{L}^1_{\mathcal{C}}(x) \leq n\}} = \sigma_0 = \sigma|_{\{x | \mathcal{L}^1_{\mathcal{C}}(x) \leq n\}}$
- $\sigma'|_{\{x | \mathcal{L}^1_{\mathcal{C}}(x) > n\}} = \sigma_1$

- for all $x \in vars^1(\mathcal{C}) \setminus vars^1(D(\mathcal{C}))$, $x\sigma' = x\mathsf{mgu}(E(\mathcal{C}))\sigma'$.

We verify that $(\sigma', \theta') \in \mathsf{Sol}(\overline{\mathcal{C}})$: For all $(X, i \vdash^? x) \in D(\mathcal{C})$, if $i \leq n$ then $X\theta' = X\theta$. But $\mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(X\theta) \leq i$ and $\sigma'|_{\{x|\mathcal{L}^1_{\mathcal{C}}(x)\leq n\}} = \sigma_0 = \sigma|_{\{x|\mathcal{L}^1_{\mathcal{C}}(x)\leq n\}}$. Thus we have that $X\theta'(\Phi(\mathcal{C})\sigma')\downarrow = X\theta(\Phi(\mathcal{C})\sigma)\downarrow = x\sigma = x\sigma'$.

Furthermore, since for all $(\xi, j \rhd v) \in \Phi(\mathcal{C})$, for all $Y \in vars^2(\xi)$, $\mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(Y) < j$, thanks to $\mathcal{C}$ being in solved form and so satisfying the invariant $\mathsf{InvVarFrame}(\mathsf{s}_{max})$. But for all $(X, i \vdash^? x) \in D(\mathcal{C})$, for all $(\xi, j \rhd v) \in \Phi(\mathcal{C})$, $\mathsf{path}(\xi) \in st(\mathsf{C}\lfloor X\theta \rfloor_{\Phi(\mathcal{C})})$ implies $j \leq i$ and so for all $Y \in vars^2(\mathsf{C}\lfloor X\theta \rfloor_{\Phi(\mathcal{C})}\delta^2(\mathcal{C}))$, $\mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(Y) < \mathsf{param}^{\mathcal{C}}_{\mathsf{max}}(X)$. Hence we deduce with a simple induction on i that for all $(X, i \vdash^? x) \in D(\mathcal{C})$, if $i \leq n$ then $X\theta$ conforms to $\Phi(\mathcal{C})\theta$ w.r.t. $\mathsf{NoUse}(\mathcal{C})\theta$ implies that $X\theta'$ conforms to $\Phi(\mathcal{C})\theta'$ w.r.t. $\mathsf{NoUse}(\mathcal{C})\theta'$.

Moreover, for all $(X, i \vdash^? x) \in D(\mathcal{C})$, if $i > n$ then $X\theta' \in \mathcal{T}(\mathcal{F}_c \cup \{ax_1\})$ and so $X\theta'$ trivially conforms to $\Phi(\mathcal{C})\theta'$ w.r.t. $\mathsf{NoUse}(\mathcal{C})\theta'$.

We already know that σ_1 satisfies the inequations of E_0 where $E_0 = E(\mathcal{C})\sigma_0$. Hence by definition of σ', we have that $\sigma' \vDash E(\mathcal{C})$.

At last, we know that for all $X \in vars^2(\mathcal{C}) \setminus vars^2(D(\mathcal{C}))$, $X\theta' = X\mathsf{mgu}(E_\Pi(\mathcal{C}))\theta'$. Furthermore, since $\mathcal{C}$ is in solved form, we have that for all $X \in vars^2(D(\mathcal{C}))$, for all $\mathsf{f} \in \mathcal{F}_c$, for all ξ recipe of $\Phi(\mathcal{C})$, $E_\Pi(\mathcal{C}) \not\vDash X \neq^? \xi$ and $E_\Pi(\mathcal{C}) \not\vDash \mathsf{root}(X) \neq^? \mathsf{f}$. Hence, we conclude that $\theta' \vDash E_\Pi(\mathcal{C})$.

To sum up, we have proved that $(\sigma', \theta') \in \mathsf{Sol}(\overline{\mathcal{C}})$. But since $\mathcal{C}$ is a constraint system on a leaf, then by Lemma 55, we know that $\mathsf{Sol}(\mathcal{C}) = \mathsf{Sol}(\overline{\mathcal{C}})$. Hence we conclude that $(\sigma', \theta') \in \mathsf{Sol}(\mathcal{C})$. □

Lemma 58. *Let $(\mathcal{M}, \mathcal{M}')$ be a pair of matrix obtained at the end strategy. Let $\mathcal{C}, \mathcal{C}'$ be two constraint systems on the same row in $(\mathcal{M}, \mathcal{M}')$ ($\mathcal{C}$ and $\mathcal{C}'$ may be part of the same matrix). If $\mathcal{C} \neq \bot$ and $\mathcal{C}' \neq \bot$ then $\mathcal{C} \approx_s \mathcal{C}'$.*

Proof. We show one side of the equivalence, the other side being done symmetrically. Let $(\sigma, \theta) \in \mathsf{Sol}(\mathcal{C})$. Thanks to Lemma 47, we know that $(\mathcal{M}, \mathcal{M}')$ are in solved form. We will show that there exists σ' such that:

1. (σ', θ) is a pre-solution of $\mathcal{C}'$ with $\sigma' \vDash \mathsf{mgu}(E(\mathcal{C}'))$ and $\theta \vDash E_\Pi(\mathcal{C}')$;
2. $\sigma' \vDash E(\mathcal{C}')$ and for all $\xi, \xi' \in \Pi_r$, if $\mathsf{C}\lfloor \xi \rfloor_{\Phi(\mathcal{C})}, \mathsf{C}\lfloor \xi' \rfloor_{\Phi(\mathcal{C})} \in \mathcal{T}(\mathcal{F}_c \cup (\mathcal{F}_d^* \cdot \mathcal{AX}))$ then
   - $\xi(\Phi(\mathcal{C})\sigma)\downarrow = \xi'(\Phi(\mathcal{C})\sigma)\downarrow$ is equivalent to $\xi(\Phi(\mathcal{C}')\sigma')\downarrow = \xi'(\Phi'(\mathcal{C}')\sigma')\downarrow$
   - $\xi(\Phi(\mathcal{C})\sigma)\downarrow \in \mathcal{T}(\mathcal{F}_c, \mathcal{N})$ is equivalent to $\xi(\Phi(\mathcal{C}')\sigma')\downarrow \in \mathcal{T}(\mathcal{F}_c, \mathcal{N})$
3. $\Phi(\mathcal{C})\sigma \sim \Phi(\mathcal{C}')\sigma'$ and $(\sigma', \theta) \in \mathsf{Sol}(\mathcal{C}')$

Property 1: Since $(\mathcal{M}, \mathcal{M}')$ are in solved form then $\mathcal{C}$ and $\mathcal{C}'$ also have the same structure. Hence, we deduce that $E_\Pi(\mathcal{C}) = E_\Pi(\mathcal{C}')$. But $(\sigma, \theta) \in \mathsf{Sol}(\mathcal{C})$, thus $\theta \vDash E_\Pi(\mathcal{C})$ and so $\theta \vDash E_\Pi(\mathcal{C}')$. Moreover, since $\mathcal{C}'$ is normalised, then $\mathsf{mgu}(E(\mathcal{C}'))$ exists and $vars^1(\Phi') \cup vars^1(D') = \mathrm{img}(\mathsf{mgu}(E')))$. Thus, we will first define σ' on the variables contain in Φ' and D'; and then for any variable $y \in vars^1(\mathcal{C}')$ we will have $y\sigma' = y\ \mathsf{mgu}(E')\sigma'$.

We define σ' recursively on the index of minimal constraint of a variable x:

Base case $\mathcal{L}^1_{\mathcal{C}'}(x) = 0$ *:* By definition of a constraint system, for all $(X, k \vdash^? u) \in D(\mathcal{C}')$, $k > 0$ which means that for all $x \in vars^1(D')$, $\mathcal{L}^1_{\mathcal{C}'}(x) > 0$. Thus, the result trivially holds.

Inductive step $\mathcal{L}^1_{\mathcal{C}'}(x) > 1$ *:* Let $(X, k \vdash^? x) \in D(\mathcal{C}')$ such that $k = \mathcal{L}^1_{\mathcal{C}'}(x)$. Since $\mathcal{C}$ and $\mathcal{C}'$ have same structure, we deduce that there exists $(X, k \vdash^? y) \in D(\mathcal{C})$ and $param(X\theta) \subseteq \{ax_1, \ldots, ax_k\}$. $\mathcal{C}$ being in solved form indicates that $\mathcal{C}$ satisfies $\mathsf{InvDest}(\mathsf{s}_{max})$. Hence thanks to Lemma 36, we have that $\mathsf{C}\lfloor X\theta \rfloor_{\Phi(\mathcal{C})} \in \mathcal{T}(\mathcal{F}_c \cup (\mathcal{F}_d^* \cdot \mathcal{AX}))$, which also means that $\mathsf{C}\lfloor X\theta \rfloor_{\Phi(\mathcal{C}')} \in \mathcal{T}(\mathcal{F}_c \cup (\mathcal{F}_d^* \cdot \mathcal{AX}))$.

$(\sigma, \theta) \in \mathsf{Sol}(\mathcal{C})$ implies that θ conforms to $\Phi(\mathcal{C})\theta$ w.r.t $\mathsf{NoUse}(\mathcal{C})\theta$. Once again, due to the same structure between $\mathcal{C}$ and $\mathcal{C}'$, we have $\{\xi, i \mid (\xi, i \rhd u) \in \mathsf{NoUse}(\mathcal{C})\} = \{\xi, i \mid (\xi, i \rhd u) \in \mathsf{NoUse}(\mathcal{C}')\}$. Thus, θ conforms to $\Phi(\mathcal{C})\theta$ w.r.t $\mathsf{NoUse}(\mathcal{C})\theta$ implies that θ conforms to $\Phi(\mathcal{C}')\theta$ w.r.t $\mathsf{NoUse}(\mathcal{C}')\theta$.

Let $\zeta \in st(X\theta)$ such that $\mathsf{C}\lfloor \zeta \rfloor_{\Phi(\mathcal{C}')} \in (\mathcal{F}_d^* \cdot \mathcal{AX})$. By definition of a context we know that there exists $(\xi, p \rhd v) \in \Phi(\mathcal{C}')$ such that $\mathsf{path}(\xi) = \mathsf{path}(\zeta)$. Furthermore, since θ conforms to $\Phi(\mathcal{C}')\theta$ w.r.t $\mathsf{NoUse}(\mathcal{C}')\theta$, we have that $\zeta = \xi\theta$. Since $\mathcal{C}'$ is in solved formed, $\mathcal{C}$ satisfies $\mathsf{InvVarFrame}(\mathsf{s}_{max})$ and so for all $Y \in vars^1\xi$, there exists $(Y, q \vdash^? y) \in D(\mathcal{C}')$ such that $q < p$. But we also know that the right hand term of the deducible constraints are distinct variables. Hence, we have that $\mathcal{L}^1_{\mathcal{C}'}(y) = q < p$. Moreover $(\sigma, \theta) \in \mathsf{Sol}(\mathcal{C})$ implies, thanks to $(\mathcal{M}, \mathcal{M}')$ satisfying $\mathsf{InvGeneral}$, that $param(\xi\theta) \subseteq \{ax_1, \ldots, ax_p\}$ and so $p \leq k$. Thus, we can deduce that $\mathcal{L}^1_{\mathcal{C}'}(y) < k$. By applying our inductive hypothesis on y, we know that $(Y\theta)(\Phi(\mathcal{C}')\sigma')\downarrow = y\sigma'$. By Property 5 of a well formed constraint system, we now can deduce $(\xi\theta)(\Phi(\mathcal{C}')\sigma')\downarrow = \zeta(\Phi(\mathcal{C}')\sigma')\downarrow = v\sigma' \in \mathcal{T}(\mathcal{F}_c, \mathcal{N})$.

Furthermore, we proved that $\mathsf{C}\lfloor X\theta \rfloor_{\Phi(\mathcal{C}')} \in \mathcal{T}(\mathcal{F}_c \cup (\mathcal{F}_d^* \cdot \mathcal{AX}))$ which allows us to conclude that $(X\theta)(\Phi(\mathcal{C}')\sigma')\downarrow \in \mathcal{T}(\mathcal{F}_c, \mathcal{N})$ and so we define $x\sigma'$ such that : $x\sigma' = (X\theta)(\Phi(\mathcal{C}')\sigma')\downarrow \in \mathcal{T}(\mathcal{F}_c, \mathcal{N})$.

Property 2: We first prove that for all $n \in \mathbb{N}$, $\sigma' \vDash_{\leq n} E(\mathcal{C}')$ implies that for all $\xi, \xi' \in \Pi_r$, if $\mathsf{C}\lfloor \xi \rfloor_{\Phi(\mathcal{C}')}, \mathsf{C}\lfloor \xi' \rfloor_{\Phi(\mathcal{C}')} \in \mathcal{T}(\mathcal{F}_c \cup (\mathcal{F}_d^* \cdot \mathcal{AX}))$, ξ and ξ' conforms to $\Phi(\mathcal{C}')\theta$, and for all $x \in vars^1(\mathsf{C}\lfloor \xi \rfloor_{\Phi(\mathcal{C}')}\delta^1(\mathcal{C}')) \cup vars^1(\mathsf{C}\lfloor \xi' \rfloor_{\Phi(\mathcal{C}')}\delta^1(\mathcal{C}'))$, $\mathcal{L}^1_{\mathcal{C}'}(x) \leq n$, then

- $\xi(\Phi(\mathcal{C}')\sigma')\downarrow \in \mathcal{T}(\mathcal{F}_c, \mathcal{N})$ implies $\xi(\Phi(\mathcal{C})\sigma)\downarrow \in \mathcal{T}(\mathcal{F}_c, \mathcal{N})$
- $\xi(\Phi(\mathcal{C}')\sigma')\downarrow = \xi'(\Phi(\mathcal{C}')\sigma')\downarrow \in \mathcal{T}(\mathcal{F}_c, \mathcal{N})$ implies $\xi(\Phi(\mathcal{C})\sigma)\downarrow = \xi'(\Phi(\mathcal{C})\sigma)\downarrow \in \mathcal{T}(\mathcal{F}_c, \mathcal{N})$

We prove this result by induction on $(|\xi(\Phi(\mathcal{C}')\sigma')\downarrow|, \mathsf{param}_{\mathsf{max}}(\xi) + \mathsf{param}_{\mathsf{max}}(\xi'))$:

Base case $(|\xi(\Phi(\mathcal{C}')\sigma')\downarrow|, \mathsf{param}_{\mathsf{max}}(\xi) + \mathsf{param}_{\mathsf{max}}(\xi')) = (0, 0)$*:* Such a case is impossible thus the result holds.

Inductive step $(|\xi(\Phi(\mathcal{C}')\sigma')\downarrow|, \mathsf{param}_{\mathsf{max}}(\xi) + \mathsf{param}_{\mathsf{max}}(\xi')) > (0, 0)$ *:* We prove the result by case analysis on the two recipes ξ and ξ' :

- $\mathsf{root}(\xi) = \mathsf{root}(\xi') \in \mathcal{F}_c$: In such a case, assume that $\xi = f(\xi_1, \ldots, \xi_n)$ and $\xi' = f(\xi'_1, \ldots, \xi'_n)$. Since $f \in \mathcal{F}_c$, $\xi(\Phi(\mathcal{C}')\sigma')\downarrow = \xi'(\Phi(\mathcal{C}')\sigma')\downarrow$ implies $\xi_k(\Phi(\mathcal{C}')\sigma')\downarrow = \xi'_k(\Phi(\mathcal{C}')\sigma')\downarrow$, for $k = 1 \ldots n$ and $|\xi_k(\Phi(\mathcal{C}')\sigma')\downarrow| < |\xi(\Phi(\mathcal{C}')\sigma')\downarrow|$, for k $= 1 \ldots n$. At last, since $vars^1(\mathsf{C}\lfloor \xi_k \rfloor_{\Phi(\mathcal{C}')}\delta^1(\mathcal{C}')) \subseteq vars^1(\mathsf{C}\lfloor \xi \rfloor_{\Phi(\mathcal{C}')}\delta^1(\mathcal{C}'))$, for $k = 1 \ldots n$, then we can apply our inductive hypothesis on ξ_k and ξ'_k which means that for all $k \in \{1, \ldots, n\}$,

$$\xi_k(\Phi(\mathcal{C})\sigma)\downarrow \in \mathcal{T}(\mathcal{F}_c, \mathcal{N}) \text{ and } \xi_k(\Phi(\mathcal{C})\sigma)\downarrow = \xi'_k(\Phi(\mathcal{C})\sigma)\downarrow$$

Thus, we deduce that $\xi(\Phi(\mathcal{C})\sigma)\downarrow \in \mathcal{T}(\mathcal{F}_c, \mathcal{N})$ and $\xi(\Phi(\mathcal{C})\sigma)\downarrow = \xi'(\Phi(\mathcal{C})\sigma)\downarrow$.

- $\mathsf{C}\lfloor\xi\rfloor_{\Phi(\mathcal{C}')} \in \mathcal{F}_d^* \cdot \mathcal{AX}$ and there exists $(\zeta, p \rhd u_1') \in \mathsf{NoUse}(\mathcal{C}')$ with $\zeta\theta = \xi$: First of all, $\mathsf{C}\lfloor\xi\rfloor_{\Phi(\mathcal{C}')} \in \mathcal{F}_d^* \cdot \mathcal{AX}$ and ξ conforms to $\Phi(\mathcal{C}')\theta$ implies that there exists $(\zeta, q \rhd u_1') \in \Phi(\mathcal{C}')$ such that $\zeta\theta = \xi$.

  $\mathcal{C}$ and $\mathcal{C}'$ being on the same line of a pair of matrices of constraint systems on the leaves, we deduce that $E_\Pi(\mathcal{C}) = E_\Pi(\mathcal{C}')$ and there exists $u_1' \in \mathcal{T}(\mathcal{F}_c, \mathcal{N} \cup \mathcal{X}^1)$ such that $(\zeta, p \rhd u_1') \in \Phi(\mathcal{C}) \cap \mathsf{NoUse}(\mathcal{C})$. Let's denote $\Theta = \mathsf{mgu}(E_\Pi(\mathcal{C}))$, we have $\Theta = \Theta'$.

  Since $\mathcal{C}$ is well-formed then by the property 5 of a well-formed constraint system, we deduce that $(\zeta\theta)\Phi(\mathcal{C})\sigma\downarrow = u_1\sigma \in \mathcal{T}(\mathcal{F}_c, \mathcal{N})$ and so $\xi(\Phi(\mathcal{C})\sigma\downarrow \in \mathcal{T}(\mathcal{F}_c, \mathcal{N})$. Secondly, by the property 8, we also know that there exists $X \in vars^2(\mathcal{C}') = vars^2(\mathcal{C})$ such that

  - $\mathsf{C}\lfloor X\Theta'\rfloor_{\Phi(\mathcal{C}')} \in \mathcal{T}(\mathcal{F}_c, \mathcal{F}_d^* \cdot \mathcal{AX} \cup \mathcal{X}^2)$
  - $\mathsf{C}\lfloor X\Theta'\rfloor_{\Phi(\mathcal{C}')}\delta^1(\mathcal{C}') = u_1'$ and $\mathsf{param}_{\mathsf{max}}^{\mathcal{C}'}(X\Theta) < p$

  where $\Theta' = \mathsf{mgu}(E_\Pi(\mathcal{C}')$.

  Furthermore, by hypothesis, we assumed for all $(Z, q \vdash^? z) \in D(\mathcal{C}')$, $\mathsf{C}\lfloor Z\theta\rfloor_{\Phi(\mathcal{C}')} \in \mathcal{T}(\mathcal{F}_c \cup (\mathcal{F}_d^* \cdot \mathcal{AX}))$, thus we have that $\mathsf{C}\lfloor X\theta\rfloor_{\Phi(\mathcal{C}')} \in \mathcal{T}(\mathcal{F}_c \cup (\mathcal{F}_d^* \cdot \mathcal{AX}))$. At last, by Property 5 of a well formed constraint system, we can also conclude that $(X\theta)\Phi(\mathcal{C}')\sigma'\downarrow = u_1'\sigma'\downarrow$.

  Furthermore, the equation $\mathsf{C}\lfloor X\Theta'\rfloor_{\Phi(\mathcal{C}')}\delta^1(\mathcal{C}') = u_1'$, due to the application of the rule Eq-frame-ded, implies that $\mathsf{C}\lfloor X\Theta\rfloor_{\Phi(\mathcal{C})}\delta^1(\mathcal{C}) = u_1$. Hence, with the same reasoning, we deduce that $(X\theta)\Phi(\mathcal{C})\sigma\downarrow = u_1\sigma\downarrow$. But $\mathsf{param}_{\mathsf{max}}(X\theta) < p$ therefore we can apply our inductive hypothesis on $(X\theta, \xi')$ which means that $\xi'\Phi(\mathcal{C})\sigma\downarrow = (X\theta)\Phi(\mathcal{C})\sigma\downarrow = u_1\sigma\downarrow = \xi(\Phi(\mathcal{C})\sigma)\downarrow$.

- $\mathsf{C}\lfloor\xi\rfloor_{\Phi(\mathcal{C}')}, \mathsf{C}\lfloor\xi'\rfloor_{\Phi(\mathcal{C}')} \in \mathcal{F}_d^* \cdot \mathcal{AX}$: In such a case, we know that there exists $(\zeta, p \rhd u_1'), (\zeta', p' \rhd u_2') \in \Phi(\mathcal{C}')$ such that $\zeta\theta = \xi$ and $\zeta'\theta = \xi'$. Furthermore, since $\mathcal{C}$ and $\mathcal{C}'$ have the same structure, there exists $u_1, u_2 \in \mathcal{T}(\mathcal{F}_c, \mathcal{N} \cup \mathcal{X}^1)$ such that $(\zeta, p \rhd u_1), (\zeta', p' \rhd u_2) \in \Phi(\mathcal{C})$.

  Since $\mathcal{C}$, $\mathcal{C}'$ are well-formed then by the property 5 of a well-formed constraint system, we deduce that $\xi(\Phi(\mathcal{C})\sigma)\downarrow = u_1\sigma$, $\xi'(\Phi(\mathcal{C})\sigma)\downarrow = u_2\sigma$, $\xi(\Phi(\mathcal{C}')\sigma')\downarrow = u_1'\sigma'$ and $\xi'(\Phi(\mathcal{C}')\sigma')\downarrow = u_2'\sigma'$.

  But $(\mathcal{M}, \mathcal{M}')$ is a leaf, then the rule Eq-frame-frame(ζ, ζ') is already applied on $(\mathcal{M}, \mathcal{M}')$. Thus,

  - either we have $E(\mathcal{C}) \vDash u_1 =^? u_2$ and $E(\mathcal{C}') \vDash u_1' =^? u_2'$: By the normalisation of a constraint system, we deduce that $u_1 = u_2$ and $u_1' = u_2'$. Thus, we trivially have that $\xi(\Phi(\mathcal{C})\sigma)\downarrow = \xi'(\Phi(\mathcal{C})\sigma)\downarrow$.
  - or $E(\mathcal{C}) \vDash u_1 \neq^? u_2$ and $E(\mathcal{C}') \vDash u_1' \neq^? u_2'$: $\xi(\Phi(\mathcal{C}')\sigma')\downarrow = \xi'(\Phi(\mathcal{C}')\sigma')\downarrow$ implies that $\sigma' \nvDash u_1' \neq^? u_2'$. But we know that for all $x \in vars^1(u_1') \cup vars^1(u_2')$, $\mathcal{L}^1_{\mathcal{C}'}(x) \leq n$, thus we have $\sigma' \nvDash u_1 \neq^? u_2$ implies that $\sigma' \nvDash_{\leq n} E(\mathcal{C}')$, which is in contradiction with our hypothesis.

- $\mathsf{C}\lfloor\xi\rfloor_{\Phi(\mathcal{C}')} \in \mathcal{F}_d^* \cdot \mathcal{AX}$ and $\mathsf{root}(\xi') \in \mathcal{F}_c$: By Lemma 57, we know that there exists $(\sigma'', \theta') \in \mathsf{Sol}(\mathcal{C}')$ such that $\sigma'|_{\{x|\mathcal{L}^1_{\mathcal{C}'}(x)\leq n\}} = \sigma''|_{\{x|\mathcal{L}^1_{\mathcal{C}'}(x)\leq n\}}$.

  Since $\mathsf{C}\lfloor\xi\rfloor_{\Phi(\mathcal{C}')} \in \mathcal{F}_d^* \cdot \mathcal{AX}$, then there exists $(\zeta, p \rhd u) \in \Phi(\mathcal{C})$ and $(\zeta, p \rhd u') \in \Phi(\mathcal{C}')$ such that $\zeta\theta = \xi$. Furthermore, since $\mathcal{C}$, $\mathcal{C}'$ are well-formed then by the property 5 of a well-formed constraint system, we deduce that $\xi(\Phi(\mathcal{C})\sigma)\downarrow = u\sigma$ and $\xi(\Phi(\mathcal{C}')\sigma')\downarrow = u'\sigma'$. Since $(\sigma'', \theta') \in \mathsf{Sol}(\mathcal{C}')$, we also have that $\zeta\theta'(\Phi(\mathcal{C}')\sigma'')\downarrow = u'\sigma''$.

  By hypothesis, we know that for all $x \in vars^1(\mathsf{C}\lfloor\xi\rfloor_{\Phi(\mathcal{C}')}\delta^1(\mathcal{C}'))$, $\mathcal{L}^1_{\mathcal{C}'}(x) \leq n$. Furthermore since $\sigma'|_{\{x|\mathcal{L}^1_{\mathcal{C}'}(x)\leq n\}} = \sigma''|_{\{x|\mathcal{L}^1_{\mathcal{C}'}(x)\leq n\}}$, we can deduce that $u'\sigma' = u'\sigma''$. Thus we have $\zeta\theta'(\Phi(\mathcal{C}')\sigma'')\downarrow = \xi(\Phi(\mathcal{C}')\sigma')\downarrow$.

  Similarly, we have that for all $x \in vars^1(\mathsf{C}\lfloor\xi'\rfloor_{\Phi(\mathcal{C}')}\delta^1(\mathcal{C}'))$, $\mathcal{L}^1_{\mathcal{C}'}(x) \leq n$. Since $\mathsf{C}\lfloor\xi'\rfloor_{\Phi(\mathcal{C}')} \in \mathcal{T}(\mathcal{F}_c \cup (\mathcal{F}_d^* \cdot \mathcal{AX}))$, we have $\mathsf{C}\lfloor\xi'\rfloor_{\Phi(\mathcal{C}')}\delta^1(\mathcal{C}')\sigma' = \mathsf{C}\lfloor\xi'\rfloor_{\Phi(\mathcal{C}')}\delta^1(\mathcal{C}')\sigma''$. Hence, $(\sigma'', \theta') \in \mathsf{Sol}(\mathcal{C}')$ implies that $\xi'(\Phi(\mathcal{C}')\sigma')\downarrow = \zeta'(\Phi(\mathcal{C}')\sigma'')\downarrow$ where $\zeta' = \mathsf{C}\lfloor\xi'\rfloor_{\Phi(\mathcal{C}')}\delta^2(\mathcal{C}')\theta'$.

  Thus, $\xi(\Phi(\mathcal{C}')\sigma')\downarrow = \xi'(\Phi(\mathcal{C}')\sigma')\downarrow$ implies that $\zeta\theta'(\Phi(\mathcal{C}')\sigma'')\downarrow = \zeta'(\Phi(\mathcal{C}')\sigma'')\downarrow$. But $(\sigma'', \theta') \in \mathsf{Sol}(\mathcal{C}')$ implies $\sigma'' \vDash ND(\mathcal{C}')$. Furthermore, since $\mathcal{C}'$ satisfies $\mathsf{InvDedsub}$ and since $\mathsf{root}(\xi') \in \mathcal{F}_c$ implies $\mathsf{root}(\zeta') \in \mathcal{F}_c$, we can deduce that there exists $X_1, \ldots, X_n \in vars^2(\mathcal{C}')$ such that $\mathsf{C}\lfloor\mathsf{f}(X_1, \ldots, X_n)\Theta'\rfloor_{\Phi(\mathcal{C}')}\delta^1(\mathcal{C}') = u'$, where $\Theta' = \mathsf{mgu}(E_\Pi(\mathcal{C}'))$. Furthermore, since $X_1, \ldots, X_n$ was obtained by the application of the rule DED-ST on the frame element $(\zeta, p \rhd u')$, we also have that $\mathsf{C}\lfloor\mathsf{f}(X_1, \ldots, X_n)\Theta\rfloor_{\Phi(\mathcal{C}')}\delta^1(\mathcal{C}') = u$, where $\Theta = \mathsf{mgu}(E_\Pi(\mathcal{C})) = \Theta'$.

  But thanks to $\mathcal{C}$ being well formed, we know for all $i \in \{1, \ldots, n\}$, $\mathsf{C}\lfloor X_i\Theta'\rfloor_{\Phi(\mathcal{C}')} \in \mathcal{T}(\mathcal{F}_c \cup (\mathcal{F}_d^* \cdot \mathcal{AX}))$. Hence we can deduce from Property 5 of a well-formed constraint system that $\mathsf{f}(X_1, \ldots, X_n)\theta(\Phi(\mathcal{C}')\sigma')\downarrow = u'\sigma'$. Similarly, we also have that $\mathsf{f}(X_1, \ldots, X_n)\theta(\Phi(\mathcal{C})\sigma)\downarrow = u\sigma$.

  At last, $\mathsf{root}(\xi') \in \mathcal{F}_c$ implies that there exists $\xi_1, \ldots, \xi_n$ such that $\xi' = \mathsf{f}(\xi_1, \ldots, \xi_n)$. Hence, by applying our inductive hypothesis on $(X_i\theta, \xi_i)$ since $|X_i\theta(\Phi(\mathcal{C}')\sigma'\downarrow| < |\xi\Phi(\mathcal{C}')\sigma'\downarrow|$, for $i = 1 \ldots n$. Hence we deduce that $\mathsf{f}(X_1, \ldots, X_n)\theta(\Phi(\mathcal{C})\sigma)\downarrow = \xi'(\Phi(\mathcal{C})\sigma)\downarrow$. Since we already proved $\mathsf{f}(X_1, \ldots, X_n)\theta(\Phi(\mathcal{C})\sigma)\downarrow = u\sigma = \xi(\Phi(\mathcal{C})\sigma)\downarrow$, we conclude that $\xi(\Phi\sigma)\downarrow = \xi'(\Phi\sigma)\downarrow$.

We continue the proof of Property 2 by proving that for all $n \in \mathbb{N}$, $\sigma' \vDash_{\leq n} E(\mathcal{C}')$. We prove this result by induction on n:

Base case $n = 0$*:* In such a case, we know that for all $u \neq^? v$ in $E(\mathcal{C}')$, for all $x \in vars^1(u) \cup vars^1(v)$, $\mathcal{L}^1_{\mathcal{C}'}(x) > 0$. Moreover, we know that $u, v \in \mathcal{T}(\mathcal{F}_c, \mathcal{X}^1)$ thanks to $\mathcal{C}'$ being in solved formed. Thus we can conclude that $\sigma' \vDash_{\leq 0} E(\mathcal{C}')$.

Inductive step $n > 0$ *:* Let $u \neq^? v$ in $E(\mathcal{C}')$ such that for all $x \in vars^1(u) \cup vars^1(v)$, $\mathcal{L}^1_{\mathcal{C}'}(x) \leq n$. But since $\mathcal{C}'$ is in solved form, we know that there is no name inside u and v. Thus, we can define two recipe ξ, ξ' such that $\xi = u\lambda$, $\xi' = v\lambda$ where λ is the substitution $\{x \to X\theta \mid X, p \vdash^? x \in D(\mathcal{C}')\}$ and $\xi\Phi(\mathcal{C}')\sigma'\downarrow = u\sigma'$, $\xi'\Phi(\mathcal{C}')\sigma'\downarrow = v\sigma'$. We know that for all $(X, p \vdash^? x) \in D(\mathcal{C}')$, $\mathsf{C}\lfloor X\theta\rfloor_{\Phi(\mathcal{C}')} \in \mathcal{T}(\mathcal{F}_c \cup (\mathcal{F}_d^* \cdot \mathcal{AX}))$ therefore we can deduce that $\mathsf{C}\lfloor\xi\rfloor_{\Phi(\mathcal{C}')}, \mathsf{C}\lfloor\xi'\rfloor_{\Phi(\mathcal{C}')} \in \mathcal{T}(\mathcal{F}_c \cup (\mathcal{F}_d^* \cdot \mathcal{AX}))$. Furthermore, for all $x \in vars^1(u, v)$, for all $w \in st(\mathsf{C}\lfloor x\lambda\rfloor_{\Phi(\mathcal{C}')}) \cap (\mathcal{F}_d^* \cdot \mathcal{AX}))$, if $(\zeta, q \rhd t) \in \Phi(\mathcal{C}')$ is the

frame element such that $w = \mathsf{path}(\zeta)$, then $q \leq \mathcal{L}^1_{\mathcal{C}'}(x) \leq n$ and we know that by the property of origination that for all $y \in vars^1(t)$, $\mathcal{L}^1_{\mathcal{C}'}(y) < q$. Thus we deduce that for all $y \in vars^1(\mathsf{C}\lfloor\xi\rfloor_{\Phi(\mathcal{C}')}\delta^1(\mathcal{C}')) \cup vars^1(\mathsf{C}\lfloor\xi'\rfloor_{\Phi(\mathcal{C}')}\delta^1(\mathcal{C}'))$, $\mathcal{L}^1_{\mathcal{C}'}(y) < n$.

Assume now that $u\sigma' = v\sigma'$. By our inductive hypothesis, we know that $\sigma' \vDash_{\leq n-1} E'$ and from the first result we showed in Property 2, we can deduce that $\xi\Phi(\mathcal{C}')\sigma'\downarrow = \xi'\Phi(\mathcal{C}')\sigma'\downarrow$ implies that $\xi\Phi(\mathcal{C})\sigma\downarrow = \xi'\Phi(\mathcal{C})\sigma\downarrow$. But thanks to $(\mathcal{M}, \mathcal{M}')$ being in solved form, we know that that there exists a renaming ρ such that $u\rho \neq^? v\rho$ in $E(\mathcal{C})$, $\xi\Phi(\mathcal{C})\sigma\downarrow = u\rho\sigma$ and $\xi'\Phi(\mathcal{C})\sigma\downarrow = v\rho\sigma$. Hence, it implies that $\sigma \nvDash E(\mathcal{C})$ which is incoherent with $(\sigma, \theta) \in \mathsf{Sol}(\mathcal{C})$. Our assumption is contradicted and so $u\sigma' \neq v\sigma'$. Hence the result holds.

By combining the first and second result of Property 2, we prove that $\sigma' \vDash E(\mathcal{C}')$ and for all $\xi, \xi' \in \Pi_r$, if $\mathsf{C}\lfloor\xi\rfloor_{\Phi(\mathcal{C}')}, \mathsf{C}\lfloor\xi'\rfloor_{\Phi(\mathcal{C}')} \in \mathcal{T}(\mathcal{F}_c \cup (\mathcal{F}_d^* \cdot \mathcal{AX}))$ and ξ, ξ' conforms to $\Phi(\mathcal{C}')\theta$ then

- $\xi(\Phi(\mathcal{C}')\sigma')\downarrow = \xi'(\Phi(\mathcal{C}')\sigma)\downarrow$ implies $\xi(\Phi(\mathcal{C})\sigma)\downarrow = \xi'(\Phi(\mathcal{C})\sigma)\downarrow$
- $\xi(\Phi(\mathcal{C}')\sigma')\downarrow \in \mathcal{T}(\mathcal{F}_c, \mathcal{N})$ implies $\xi(\Phi(\mathcal{C})\sigma)\downarrow \in \mathcal{T}(\mathcal{F}_c, \mathcal{N})$

By hypothesis, we know that $(\sigma, \theta) \in \mathsf{Sol}(\mathcal{C})$ and so $\sigma \vDash E(\mathcal{C})$. Thus, we can use the same reasoning as for the first result to prove that: for all $\xi, \xi' \in \Pi_r$, if $\mathsf{C}\lfloor\xi\rfloor_{\Phi(\mathcal{C})}, \mathsf{C}\lfloor\xi'\rfloor_{\Phi(\mathcal{C})} \in \mathcal{T}(\mathcal{F}_c \cup (\mathcal{F}_d^* \cdot \mathcal{AX}))$ and ξ, ξ' conforms to $\Phi(\mathcal{C})\theta$ then

- $\xi(\Phi(\mathcal{C})\sigma)\downarrow = \xi'(\Phi(\mathcal{C})\sigma)\downarrow$ implies $\xi(\Phi(\mathcal{C}')\sigma')\downarrow = \xi'(\Phi(\mathcal{C}')\sigma')\downarrow$
- $\xi(\Phi(\mathcal{C})\sigma)\downarrow \in \mathcal{T}(\mathcal{F}_c, \mathcal{N})$ implies $\xi(\Phi(\mathcal{C}')\sigma')\downarrow \in \mathcal{T}(\mathcal{F}_c, \mathcal{N})$

Thus, we conclude the proof of Property 2.

Property 3: We have to show that $\Phi(\mathcal{C})\sigma \sim \Phi(\mathcal{C}')\sigma'$ and $(\sigma', \theta) \in \mathsf{Sol}(\mathcal{C}')$. From Property 2, we proved the static equivalence for any recipe $\xi, \xi' \in \Pi_r$ such that $\mathsf{C}\lfloor\xi\rfloor_{\Phi(\mathcal{C})}, \mathsf{C}\lfloor\xi'\rfloor_{\Phi(\mathcal{C})} \in \mathcal{T}(\mathcal{F}_c \cup (\mathcal{F}_d^* \cdot \mathcal{AX}))$ and ξ, ξ' conforms to the frame $\Phi(\mathcal{C})\theta$ (and so $\Phi(\mathcal{C}')\theta$).

Thanks to Property 2, we deduce that $\sigma' \vDash E(\mathcal{C}')$. Hence we have that $(\sigma', \theta) \in \mathsf{Sol}(\overline{\mathcal{C}'})$. But, thanks to Lemma 55, we know that $\mathsf{Sol}(\overline{\mathcal{C}'}) = \mathsf{Sol}(\mathcal{C}')$. Hence, we have that $(\sigma', \theta) \in \mathsf{Sol}(\mathcal{C}')$. Thus, by Lemma 36, we can deduce that for all $\xi \in \Pi_r$, $\xi(\Phi(\mathcal{C}')\sigma')\downarrow \in \mathcal{T}(\mathcal{F}_c, \mathcal{N})$ and ξ conforms to $\Phi(\mathcal{C}')\theta$ w.r.t. $\mathsf{NoUse}(\mathcal{C}')\theta$ implies that $\mathsf{C}\lfloor\xi\rfloor_{\Phi(\mathcal{C}')} \in \mathcal{T}(\mathcal{F}_c \cup (\mathcal{F}_d^* \cdot \mathcal{AX}))$.

Let $\xi, \xi' \in \Pi_r$. Let $\mathcal{M}(\xi, \xi')$ be the multiset of recipe ζ such that $\zeta \in st(\xi) \cup st(\xi')$ and ζ doesn't conforms to the frame $\Phi(\mathcal{C}')\theta$ w.r.t. $\mathsf{NoUse}(\mathcal{C}')\theta$. We prove our result by induction on the natural order on multiset.

Base case $\mathcal{M}(\xi, \xi') = \emptyset$: In such a case, we can deduce that ξ and ξ' conforms to the frame $\Phi(\mathcal{C}')\theta$ w.r.t. $\mathsf{NoUse}(\mathcal{C}')\theta$. Thus, thanks to Lemma 36, $\mathsf{C}\lfloor\xi\rfloor_{\Phi(\mathcal{C}')} \in \mathcal{T}(\mathcal{F}_c \cup (\mathcal{F}_d^* \cdot \mathcal{AX}))$ and $\mathsf{C}\lfloor\xi'\rfloor_{\Phi(\mathcal{C}')} \in \mathcal{T}(\mathcal{F}_c \cup (\mathcal{F}_d^* \cdot \mathcal{AX}))$. Thus we deduce by applying Property 2.

Inductive case $\mathcal{M}(\xi, \xi') \neq \emptyset$: Let $\zeta \in st(\xi) \cup st(\xi')$ the smallest recipe such that ζ doesn't conform to the frame $\Phi(\mathcal{C})\theta$. In such a case, we can deduce that $\mathsf{C}\lfloor\zeta\rfloor_{\Phi(\mathcal{C})} \in (\mathcal{F}_d^* \cdot \mathcal{AX})$ (if not, we would have $\zeta = f(\zeta_1, \ldots, \zeta_n)$ and there exists $i \in \{1 \ldots n\}$ such that ζ_i doesn't conforms to the frame $\Phi(\mathcal{C})\theta$ which contradict ζ being the smallest). Since $\mathsf{C}\lfloor\zeta\rfloor_{\Phi(\mathcal{C})} \in (\mathcal{F}_d^* \cdot \mathcal{AX})$, then there exists $(\beta, i \rhd u) \in \Phi(\mathcal{C})$ and $(\beta, i \rhd u') \in \Phi(\mathcal{C}')$ such that $\mathsf{path}(\beta) = \mathsf{path}(\zeta)$. We do a case analysis on $(\beta, i \rhd u)$:

Case $(\beta, i \rhd u) \notin \mathsf{NoUse}(\mathcal{C})$*:* In such a case, since ζ does not conforms with $\Phi(\mathcal{C})\theta$ w.r.t. $\mathsf{NoUse}\theta$, we deduce that $\zeta \neq \beta\theta$. Hence $\zeta = \mathsf{f}(\zeta_1, \ldots, \zeta_n)$ for some $\mathsf{f} \in \mathcal{F}_d$. Moreover, by minimality of ζ, for all $i \in \{1, \ldots, n\}$, we know that ζ_i conforms to $\Phi(\mathcal{C})\theta$ w.r.t. $\mathsf{NoUse}\theta$. Furthermore, $\mathsf{path}(\beta) = \mathsf{path}(\zeta)$ implies that $\beta = f(\beta_1, \ldots, \beta_n)$ and $\mathsf{path}(\beta_1) = \mathsf{path}(\zeta_1)$. Thus, ζ_1 conforms to $\Phi(\mathcal{C})\theta$ implies that $\zeta_1 = \beta_1\theta$. Furthermore, we know that $\zeta\Phi(\mathcal{C})\sigma\downarrow \in \mathcal{T}(\mathcal{F}_c, \mathcal{N})$ and $(\beta\theta)\Phi(\mathcal{C})\sigma\downarrow \in \mathcal{T}(\mathcal{F}_c, \mathcal{N})$, then by Lemma 32, we deduce that $\zeta_k\Phi(\mathcal{C})\sigma\downarrow \in \mathcal{T}(\mathcal{F}_c, \mathcal{N})$ and $(\beta_k\theta)\Phi(\mathcal{C})\sigma\downarrow \in \mathcal{T}(\mathcal{F}_c, \mathcal{N})$, for $k = 1 \ldots n$. At last, from the rewriting rule we consider and from $\zeta_1 = \beta_1\theta$, we can deduce that $(\beta_k\theta)\Phi(\mathcal{C})\sigma\downarrow = \zeta_k\Phi(\mathcal{C})\sigma\downarrow$. But all of $\beta_k\theta$ and ζ_k conform to $\Phi(\mathcal{C})\theta$, which means by Property 2 that $(\beta_k\theta)\Phi(\mathcal{C}')\sigma'\downarrow = \zeta_k\Phi(\mathcal{C}')\sigma'\downarrow$, for $k = 1 \ldots n$ and so $\zeta\Phi(\mathcal{C}')\sigma'\downarrow = (\beta\theta)\Phi(\mathcal{C}')\sigma'\downarrow$.

At last, since ζ is a subterm of ξ or ξ' (w.l.o.g. subterm of ξ), there exists a position p such that $\zeta = \xi_{|p}$. But $\mathcal{M}(\xi[\beta\theta]_p, \xi')$ is strictly smaller than $\mathcal{M}(\xi, \xi')$ since ζ doesn't conforms to $\Phi(\mathcal{C})\theta$ and $\beta\theta$ does. Thus we can apply our inductive hypothesis on $(\xi[\beta\theta]_p, \xi')$ and so:

- $\xi[\beta\theta]_p\Phi(\mathcal{C})\sigma\downarrow \in \mathcal{T}(\mathcal{F}_c, \mathcal{N})$ is equivalent to $\xi[\beta\theta]_p\Phi(\mathcal{C}')\sigma'\downarrow \in \mathcal{T}(\mathcal{F}_c, \mathcal{N})$
- if $\xi[\beta\theta]_p\Phi(\mathcal{C})\sigma\downarrow \in \mathcal{T}(\mathcal{F}_c, \mathcal{N})$ then $\xi[\beta\theta]_p\Phi(\mathcal{C})\sigma\downarrow = \xi'\Phi(\mathcal{C})\sigma\downarrow$ is equivalent to $\xi[\beta\theta]_p$ $\Phi(\mathcal{C}')\sigma'\downarrow = \xi'\Phi(\mathcal{C}')\sigma'\downarrow$.

But $\zeta\Phi(\mathcal{C})\sigma\downarrow = (\beta\theta)\Phi(\mathcal{C})\sigma\downarrow$ and $\zeta\Phi(\mathcal{C}')\sigma'\downarrow = (\beta\theta)\Phi(\mathcal{C}')\sigma'\downarrow$. Hence we deduce that:

- $\xi\Phi(\mathcal{C})\sigma\downarrow \in \mathcal{T}(\mathcal{F}_c, \mathcal{N})$ is equivalent to $\xi\Phi(\mathcal{C}')\sigma\downarrow \in \mathcal{T}(\mathcal{F}_c, \mathcal{N})$
- if $\xi\Phi(\mathcal{C})\downarrow \in \mathcal{T}(\mathcal{F}_c, \mathcal{N})$ then $\xi\Phi(\mathcal{C})\sigma\downarrow = \xi'\Phi(\mathcal{C})\sigma\downarrow$ is equivalent to $\xi\Phi(\mathcal{C}')\sigma'\downarrow = \xi'\Phi(\mathcal{C}')\sigma'\downarrow$.

Hence the result holds.

Case $(\beta, i \rhd u) \in \mathsf{NoUse}(\mathcal{C})$*:* Thanks to $\mathcal{C}$ being well-formed, we know that there exists $X \in vars^2(\mathcal{C})$ such that $X\theta \in \Pi_r$, $X\theta$ conforms to $\Phi(\mathcal{C})\theta$ w.r.t. $\mathsf{NoUse}(\mathcal{C})\theta$, and $X\theta(\Phi(\mathcal{C})\sigma)\downarrow = \beta\theta(\Phi(\mathcal{C})\sigma)\downarrow$. Moreover, similarly to the previous case, we can show that $\zeta\Phi(\mathcal{C})\sigma\downarrow = \beta\theta\Phi(\mathcal{C})\sigma\downarrow$ and $\zeta\Phi(\mathcal{C}')\sigma'\downarrow = \beta\theta\Phi(\mathcal{C}')\sigma'\downarrow$. Hence we would want to apply our inductive hypothesis on $\xi[X\theta]_p$ and ξ' where p is the position of ζ in ξ. However, $\xi[X\theta]_p$ is not necessary a recipe in Π_r. Thus we have to transform first this recipe so that we can apply our inductive hypothesis.

Subproperty: We show that for all recipe $\gamma \in \Pi_r$ conforms to $\Phi\theta$ w.r.t. $\mathsf{NoUse}\theta$, for all position p of ξ, if $\gamma \in \Pi_r$, $\gamma\Phi(\mathcal{C})\sigma\downarrow = \xi|_p\Phi(\mathcal{C})\sigma\downarrow$ and $\gamma\Phi(\mathcal{C}')\sigma'\downarrow = \xi|_p\Phi(\mathcal{C}')\sigma'\downarrow$ then that there exists a subterm γ' of γ and a position p' prefix of p such that $\xi[\gamma]_p(\Phi(\mathcal{C})\sigma)\downarrow = \xi[\gamma']_{p'}\Phi(\mathcal{C})\sigma\downarrow$, $\xi[\gamma]_p(\Phi(\mathcal{C}')\sigma')\downarrow = \xi[\gamma']_{p'}\Phi(\mathcal{C}')\sigma'\downarrow$ and $\xi[\zeta']_{p'} \in \Pi_r$. We prove this result by induction on the length $|p|$ of p.
Base case $|p| = 0$. In such a case we have that $p = \epsilon$. In such a case since $\gamma \in \Pi_r$, we deduce that $\xi[\gamma]_p \in \Pi_r$. Hence the result holds.

Inductive step $|p| > 1$*:* In such a case, we have that $p = p_1 \cdot r$ for some $r \in \mathbb{N}$ and some p_1 such that $|p_1| < |p|$. Assume that $\xi_{|p_1} = \mathsf{f}(\xi_1, \ldots, \xi_n)$. We have to distinguish two cases:

1. $r = 1$, $\mathsf{g} \in \mathcal{F}_d$ *and* $\mathsf{root}(\gamma) \in \mathcal{F}_c$*:* Since $\gamma\Phi(\mathcal{C})\sigma\downarrow = \xi|_p\Phi(\mathcal{C})\sigma\downarrow$ and $\xi\Phi(\mathcal{C})\sigma\downarrow \in \mathcal{T}(\mathcal{F}_c, \mathcal{N})$ then by Lemma 32, we deduce that g is reduced. We do a case analysis on f:

- $\mathsf{f} = \mathsf{sdec}$ with $\xi_{|p_1}[\gamma] = \mathsf{sdec}(\mathsf{senc}(\gamma_1, \gamma_2), \xi_2)$ and $\xi_2\Phi(\mathcal{C})\sigma\downarrow = \gamma_2\Phi(\mathcal{C})\sigma\downarrow$. But $\gamma_2 \in st(\gamma)$ and γ_2 conforms to $\Phi(\mathcal{C})\theta$ w.r.t. $\mathsf{NoUse}(\mathcal{C})\theta$. Moreover, $\xi_2 \in st(\xi)$ hence $\mathcal{M}(\xi, \xi') > \mathcal{M}(\gamma_2, \xi_2)$. Hence by our main inductive hypothesis, we deduce that $\gamma_2\Phi(\mathcal{C}')\sigma'\downarrow = \xi_2\Phi(\mathcal{C}')\sigma'\downarrow$ and so $\xi_{|p_1}[\gamma]\Phi(\mathcal{C}')\sigma'\downarrow = \gamma_1\Phi(\mathcal{C}')\sigma'\downarrow$. Thus, we apply our inductive hypothesis on $\gamma' = \gamma_1$ and p_1. Hence the result holds
- $\mathsf{f} \in \mathcal{F}_d \setminus \{\mathsf{sdec}\}$: The proof is similar to the case $\mathsf{f} = \mathsf{sdec}$.

2. *Otherwise:* By definition of Π_r, we have that $\xi[X\theta]_p \in \Pi_r$, and thus the result holds with $\zeta' = \zeta$ and $p' = p$.

Main proof: We already know that $X\theta(\Phi(\mathcal{C})\sigma)\downarrow = \beta\theta(\Phi(\mathcal{C})\sigma)\downarrow$. Since $X\theta$ and $\beta\theta$ conforms to $\overline{\Phi\theta}$ w.r.t. $\mathsf{NoUse}\theta$, we deduce that $X\theta(\Phi(\mathcal{C}')\sigma')\downarrow = \beta\theta(\Phi(\mathcal{C}')\sigma')\downarrow$. Furthermore, we proved that $\zeta\Phi(\mathcal{C})\sigma\downarrow = \beta\theta\Phi(\mathcal{C})\sigma\downarrow$ and $\zeta\Phi(\mathcal{C}')\sigma'\downarrow = \beta\theta\Phi(\mathcal{C}')\sigma'\downarrow$. Hence we deduce that $X\theta(\Phi(\mathcal{C})\sigma)\downarrow = \zeta\Phi(\mathcal{C})\sigma\downarrow$ and $X\theta(\Phi(\mathcal{C}')\sigma')\downarrow = \zeta\Phi(\mathcal{C}')\sigma'\downarrow$. Thanks to Subproperty, we deduce that there exists p' prefix of p and a subterm γ of $X\theta$ such that $\xi(\Phi(\mathcal{C})\sigma)\downarrow = \xi[\gamma]_{p'}\Phi(\mathcal{C})\sigma\downarrow$, $\xi(\Phi(\mathcal{C}')\sigma')\downarrow = \xi[\gamma]_{p'}\Phi(\mathcal{C}')\sigma'\downarrow$ and $\xi[\gamma]_{p'} \in \Pi_r$. But γ is a subterm of $X\theta$ hence is conforms to $\Phi(\mathcal{C})\theta$ w.r.t. $\mathsf{NoUse}(\mathcal{C})\theta$. Hence, since ζ do not conforms to $\Phi(\mathcal{C})\theta$ w.r.t. $\mathsf{NoUse}(\mathcal{C})\theta$, then $\mathcal{M}(\xi[\gamma]_{p'}, \xi') < \mathcal{M}(\xi, \xi')$. Hence we can apply our inductive hypothesis on $(\xi[\gamma]_{p'}, \xi')$.

$\xi\Phi(\mathcal{C})\sigma\downarrow \in \mathcal{T}(\mathcal{F}_c, \mathcal{N})$ implies $\xi[\gamma]_{p'}\Phi(\mathcal{C})\sigma\downarrow \in \mathcal{T}(\mathcal{F}_c, \mathcal{N})$ and so $\xi[\gamma]_{p'}\Phi(\mathcal{C}')\sigma'\downarrow \in \mathcal{T}(\mathcal{F}_c, \mathcal{N})$ which allows us to deduce that $\xi\Phi(\mathcal{C}')\sigma'\downarrow \in \mathcal{T}(\mathcal{F}_c, \mathcal{N})$. Similarly, if $\xi\Phi(\mathcal{C})\sigma\downarrow \in \mathcal{T}(\mathcal{F}_c, \mathcal{N})$ and $\xi\Phi(\mathcal{C})\sigma\downarrow = \xi'\Phi(\mathcal{C})\sigma\downarrow$ then $\xi[\gamma]_{p'}\Phi(\mathcal{C})\sigma\downarrow = \xi'\Phi(\mathcal{C})\sigma\downarrow$. Thus, thanks to our inductive hypothesis, $\xi[\gamma]_{p'}\Phi(\mathcal{C}')\sigma'\downarrow = \xi'\Phi(\mathcal{C}')\sigma'\downarrow$ and so $\xi\Phi(\mathcal{C}')\sigma'\downarrow = \xi'\Phi(\mathcal{C}')\sigma'\downarrow$. The other side of the equivalence can be done symmetrically. Hence the result holds. □

Using the previous lemma, we can finally prove that the pair of matrices on the leaves are symbolically equivalence if and only if they satisfy the final test.

Theorem 4. *Let $(\mathcal{M}_0, \mathcal{M}'_0)$ be a pair of sets of initial constraint systems and $(\mathcal{M}, \mathcal{M}')$ be a leaf of the tree whose root is labeled with $(\mathcal{M}_0, \mathcal{M}'_0)$ and which is obtained following the strategy $\mathcal{S}$. We have that $\mathcal{M} \approx_s \mathcal{M}'$ if, and only if, $\mathsf{LeafTest}(\mathcal{M}, \mathcal{M}') = \mathsf{true}$.*

Proof. Assume that $\mathcal{M}$ (resp. $\mathcal{M}'$) has n rows and m (resp. m') columns. We prove the two implications separately.

Left implication ($\Leftarrow$): Assume that $\mathsf{LeafTest}(\mathcal{M}, \mathcal{M}') = \mathsf{true}$. Let $i \in \{1, \ldots, n\}$ and $j \in \{1, \ldots, m\}$. Let $(\sigma, \theta) \in \mathsf{Sol}(\mathcal{M}_{i,j})$ where $\mathcal{M}_{i,j}$ represents the constraint system occurring at the ith row and jth column in $\mathcal{M}$. Since $\mathcal{M}_{i,j}$ has a solution, we deduce that $\mathcal{M}_{i,j} \neq \bot$. Hence, thanks to $\mathsf{LeafTest}(\mathcal{M}, \mathcal{M}') = \mathsf{true}$, there exists $j' \in \{1, \ldots, m'\}$ such that $\mathcal{M}'_{i,j'} \neq \bot$. By Lemma 58, we deduce that $\mathcal{M}_{i,j} \approx_s \mathcal{M}'_{i,j'}$. Thus, $(\sigma, \theta) \in \mathcal{M}_{i,j}$ implies that there exists σ' such that $(\sigma', \theta) \in \mathsf{Sol}(\mathcal{M}'_{i,j'})$ and $\Phi(\mathcal{M}_{i,j})\sigma \sim \Phi(\mathcal{M}'_{i,j'})\sigma'$. The other side of the equivalence is proved symmetrically. Therefore we deduce that $\mathcal{M} \approx_s \mathcal{M}'$.

Right implication ($\Rightarrow$): Assume that $\mathcal{M} \approx_s \mathcal{M}'$. We have to show that $\mathsf{LeafTest}(\mathcal{M}, \mathcal{M}') = \mathsf{true}$. Let $i \in \{1, \ldots, n\}$ and let $j \in \{1, \ldots, m\}$. Assume that $\mathcal{M}_{i,j} \neq \bot$. Thanks to Lemma 56, we deduce that there exists $(\sigma, \theta) \in \mathsf{Sol}(\mathcal{M}_{i,j})$. But $\mathcal{M} \approx_s \mathcal{M}'$, thus there

exists $j' \in \{1, \ldots, m'\}$ and σ' such that $(\sigma', \theta) \in \mathsf{Sol}(\mathcal{M}'_{i,j'})$ and $\Phi(\mathcal{M}_{i,j})\sigma \sim \Phi(\mathcal{M}'_{i,j'})\sigma'$. Since $\mathcal{M}'_{i,j'}$ contain at least a solution, we deduce that $\mathcal{M}'_{i,j'} \neq \bot$. The other side of the equivalence is proved symmetrically. Therefore, we deduce that $\mathsf{LeafTest}(\mathcal{M}, \mathcal{M}') = \mathsf{true}$. □

Appendix G. Termination

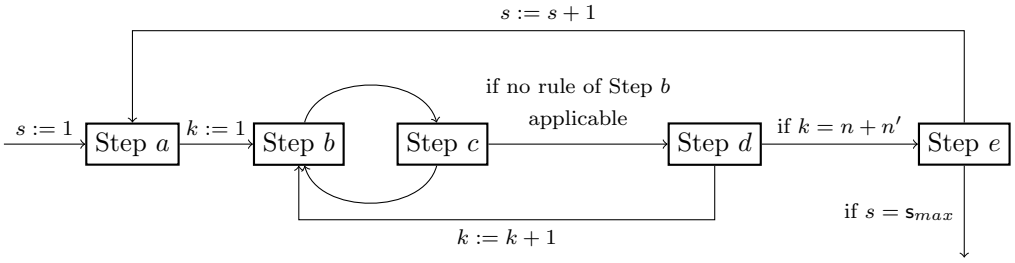
In this section, we show that the strategy $\mathcal{S}$ explained in Section 4 terminates by establishing the following theorem.

Theorem 5. *(termination) Applying the transformation rules on a pair of sets of initial constraint systems and following the strategy $\mathcal{S}$ always terminates.*

The strategy $\mathcal{S}$ is made of two phases (each phase is composed of several steps). We show termination of each phase separately. Termination of Phase 1 is proved in Proposition 1 whereas termination of Phase 2 is established in Proposition 2.

Appendix G.1. Phase 1: Taking care of deducibility constraints

The first phase of our strategy consists of applying transformation rules to put constraint systems in "pre-solved" form. As depicted below, this first phase is a cycle of several steps. The integer s indicates the *support of the rules* that are applied during the cycle.



We show termination of each step separately, and consider also the cycle Steps b/c.

Appendix G.1.1. Step a: frame analysis

During this step, we apply the rules Dest and Eq-frame-ded, with support equal to s, as long as possible with priority on the rule Eq-frame-ded. The application of those rules has to be a strong application for at least one constraint system that occurred in the row of the matrix on which we apply the rule.

Lexicographic measure $\mu_{1.a}(\mathcal{C})$ on a constraint system $\mathcal{C}$. When $\mathcal{C} \neq \bot$, the measure $\mu_{1.a}(\mathcal{C})$ is a 4-tuple defined as follows:

1. $|vars^1(D(\mathcal{C}))|$
2. the multiset $\{\{n \mid (\xi, i \rhd u) \in \Phi(\mathcal{C}) \wedge \textsc{Dest}(\xi, \ell \to r, s) \text{ not useless}\}\}$ where $n = |\{v \in st(u) \mid \mathsf{root}(v) \in \{\mathsf{aenc}, \mathsf{senc}, \langle\rangle, \mathsf{sign}\}\}|$
3. $|\Phi(\mathcal{C}) \setminus \mathsf{NoUse}(\mathcal{C})|$

4. $|\{(X,\xi) \mid (X, i \rhd u) \in D(\mathcal{C}) \wedge (\xi, j \rhd v) \in \Phi(\mathcal{C}) \smallsetminus \mathsf{NoUse}(\mathcal{C}) \wedge E(\mathcal{C}) \not\models u \neq^? v\}|$

We extend this measure to pairs of matrices. We have that

$$\mu^m_{1.a}(\mathcal{M}, \mathcal{M}') = \{\{\mu_{1.a}(\mathcal{C}) \mid \mathcal{C} \in \mathcal{M} \text{ or } \mathcal{C} \in \mathcal{M}'\}\}.$$

By convention, we have that $\mu_{1.a}(\bot) = (0, \emptyset, 0, 0)$.

Intuitively, the first item represents the number of first-order variables occurring in deducibility constraints. An application of Dest during Step a preserves this number while an application of Eq-frame-ded may decrease it strictly. The second item of this measure represents the subterms of the frame that may be deducible thanks to an application of the rule Dest. Typically when the application of $\textsc{Dest}(\xi, \ell \to r, s)$ is useless, then no new subterm u in $(\xi \rhd u)$ can be deduced thanks to Dest. The third item of the measure represents the number of frame elements that are not considered as useless. Lastly, the fourth item represents the possible parameters for which an application of Eq-frame-ded is not useless.

Lemma 59. *Let $(\mathcal{M}_0, \mathcal{M}'_0)$ be a pair of matrices obtained during Step a of Phase 1 (following the strategy $\mathcal{S}$). Let $\textsc{Rule}(\tilde{p})$ be an instance of Dest (resp. Eq-frame-ded) applicable on $(\mathcal{M}_0, \mathcal{M}'_0)$, and $(\mathcal{M}_1, \mathcal{M}'_1)$ be a resulting pair of matrices after the application of such a rule. We have that $\mu^m_{1.a}(\mathcal{M}_1, \mathcal{M}'_1) < \mu^m_{1.a}(\mathcal{M}_0, \mathcal{M}'_0)$.*

Proof. Let $\mathcal{C}$ be a constraint system occurring in $(\mathcal{M}_0, \mathcal{M}'_0)$, and $\mathcal{C}_1$, $\mathcal{C}_2$ be the two constraint systems obtained by applying an instance of Dest or Eq-frame-ded. We show, by case analysis on the rule, that:

$$\mu_{1.a}(\mathcal{C}_1) < \mu_{1.a}(\mathcal{C}) \quad \text{and} \quad \mu_{1.a}(\mathcal{C}_2) < \mu_{1.a}(\mathcal{C})$$

Case $\textsc{Eq-frame-ded}(X, \xi)$*:* The definition of Eq-frame-ded implies that there exists $(X, i \rhd u) \in D(\mathcal{C})$ and $(\xi, s \rhd v) \in \Phi(\mathcal{C})$ with $i < s$. Furthermore, we have that $D(\mathcal{C}_1) = D(\mathcal{C})\sigma$ and $\Phi(\mathcal{C}_1) = \Phi(\mathcal{C}_1)\sigma$ where $\sigma = \mathsf{mgu}(u, v)$. But thanks to the property of origination of a constraint system (Definition 3 - item 3), we know that $vars^1(v) \subseteq vars^1(D(\mathcal{C}))$.

Assume first that σ is different from the identity. In such a case, since $\mathcal{C}_1$ is normalised, we have that $\mathrm{dom}(\sigma) \cap vars^1(D(\mathcal{C}_1)) = \emptyset$ and so $|vars^1(D(\mathcal{C}_1))| < |vars^1(D(\mathcal{C}))|$. Hence we have that $\mu_{1.a}(\mathcal{C}_1) < \mu_{1.a}(\mathcal{C})$.

Assume now that σ is the identity. In such a case, we have that $\pi_1(\mu_{1.a}(\mathcal{C})) = \pi_1(\mu_{1.a}(\mathcal{C}_1))$ (the first component of the measure is left unchanged) and $\pi_2(\mu_{1.a}(\mathcal{C})) = \pi_2(\mu_{1.a}(\mathcal{C}_1)))$. Moreover, by the definition of the rule Eq-frame-ded, we know that $(\xi, s \rhd v) \in \mathsf{NoUse}(\mathcal{C}_1)$ while $(\xi, s \rhd v) \notin \mathsf{NoUse}(\mathcal{C})$. Hence we have that $|\Phi(\mathcal{C}_1)| - |\mathsf{NoUse}(\mathcal{C}_1)| < |\Phi(\mathcal{C})| - |\mathsf{NoUse}(\mathcal{C})|$ and so $\mu_{1.a}(\mathcal{C}_1) < \mu_{1.a}(\mathcal{C})$.

For the constraint system $\mathcal{C}_2$, since no substitution is applied on $\mathcal{C}$, then $\pi_1(\mu_{1.a}(\mathcal{C})) = \pi_1(\mu_{1.a}(\mathcal{C}_2))$ and $\pi_2(\mu_{1.a}(\mathcal{C})) = \pi_2(\mu_{1.a}(\mathcal{C}_2))$. Furthermore, we have that $\mathsf{NoUse}(\mathcal{C}) = \mathsf{NoUse}(\mathcal{C}_2)$ hence $\pi_3(\mu_{1.a}(\mathcal{C})) = \pi_3(\mu_{1.a}(\mathcal{C}_2))$. On the other hand, we have $E(\mathcal{C}_2) = E(\mathcal{C}) \wedge u \neq^? v$. Hence we deduce that $\pi_4(\mu_{1.a}(\mathcal{C}_2) < \pi_4(\mu_{1.a}(\mathcal{C}))$ and so $\mu_{1.a}(\mathcal{C}_2) < \mu_{1.a}(\mathcal{C})$.

Case $\textsc{Dest}(\xi, \ell \to r, s)$*:* By definition there exists i, u such that $(\xi, i \rhd u) \in \Phi(\mathcal{C})$. First of all, we deduce $u \notin \mathcal{X}^1$. Indeed, thanks to Lemma 27, we know that $(\mathcal{M}_0, \mathcal{M}'_0)$ satisfies Property $\mathsf{PP1Sa}(s)$. Hence if $u \in \mathcal{X}^1$, then either (a) $(\xi, i \rhd u) \in \mathsf{NoUse}(\mathcal{C}')$ if

$i < s$, or else (b) there exists $(X, j \vdash^? u) \in D(\mathcal{C})$. Case (a) is impossible since the rule $\textsc{Dest}(\xi, \ell \to r, s)$ would not be applicable, and case (b) is also impossible since it would imply that the rule $\textsc{Eq-frame-ded}(X, \xi)$ is applicable which contradict the strategy that imposes that the rule Eq-frame-ded are prioritised over the rule Dest.

According to Figure 1, $\Phi(\mathcal{C})\sigma \cup \{(\xi', s \rhd w\sigma)\} = \Phi(\mathcal{C}_1)$ and $D(\mathcal{C})\sigma \cup \{X_2, s \vdash^? u_2; \ldots; X_n, d \vdash^? u_n\} = D(\mathcal{C}_1)$ where $\mathsf{f}(u_1, \ldots, u_n) \to w$ is a fresh renaming of the rewrite rule $\ell \to r$ and $\sigma = \mathsf{mgu}(u_1 =^? u)$. But according to the definition of our rewrite rules, $u \notin \mathcal{X}^1$ implies that either $\sigma|_{vars^1(u)}$ is the identity or $\sigma|_{vars^1(u)} = \{x \mapsto \mathsf{pk}(z)\}$ where $x \in vars^1(u)$ and $z \in vars^1(u_1)$. Therefore, along with the fact that $vars^1(u_2, \ldots, u_n) \subseteq vars^1(u_1)$, we deduce that $|vars^1(D(\mathcal{C}_1))| = |vars^1(D(\mathcal{C})|$.

Furthermore, w is a strict subterm of u_1 hence $w\sigma$ is a strict subterm of $u\sigma$. For simplicity, let's denote $\mathcal{F}' = \{\mathsf{aenc}, \mathsf{senc}, \langle\rangle, \mathsf{sign}\}$. For all $(\zeta, p \rhd v) \in \Phi(\mathcal{C})$, since $\sigma|_{vars^1(D)}$ is either identity or $\sigma|_{vars^1(D)} = \{x \to \mathsf{pk}(y)\}$, then have that $|\{t \in st(v\sigma) \mid \mathsf{root}(t) \in \mathcal{F}'\}| = |\{t \in st(v) \mid \mathsf{root}(t) \in \mathcal{F}'\}|$. Furthermore, $w\sigma$ being a strict subterm of $u\sigma$ implies that $|\{t \in st(w\sigma) \mid \mathsf{root}(t) \in \mathcal{F}'\}|$ denoted n_1 is strictly inferior to $|\{t \in st(u\sigma) \mid \mathsf{root}(t) \in \mathcal{F}'\}|$, denoted n_2. At last, $\textsc{Dest}(\xi, \ell \to r, s)$ is useless on $\mathcal{C}_1$ hence there exists a multiset S such that $\pi_2(\mu_{1.a}(\mathcal{C}))) = S \cup \{\{n_2\}\}$ and $\pi_2(\mu_{1.a}(\mathcal{C}_1)) = S \cup \{\{n_1, n_1, n_1, n_1, n_1\}\}$ (there are five rewriting rules available). Thus, $n_1 < n_2$ implies that $\pi_2(\mu_{1.a}(\mathcal{C}_1)) < \pi_2(\mu_{1.a}(\mathcal{C}))$ and so $\mu_{1.a}(\mathcal{C}_1) < \mu_{1.a}(\mathcal{C})$.

For the case of the constraint system $\mathcal{C}_2$, since $\textsc{Dest}(\xi, \ell \to r, s)$ is useless on $\mathcal{C}_2$ and since only non-deducibility constraint are added, we trivially have that $|vars^1(D(\mathcal{C}_2))| = vars^1(D(\mathcal{C}))|$ and $\pi_2(\mu_{1.a}(\mathcal{C}_2)) < \pi_2(\mu_{1.a}(\mathcal{C}))$. Hence we have $\mu_{1.a}(\mathcal{C}_2) < \mu_{1.a}(\mathcal{C})$.

We finish the proof by showing that $\mu^m_{1.a}(\mathcal{M}_1, \mathcal{M}'_1) < \mu^m_{1.a}(\mathcal{M}_0, \mathcal{M}'_0)$. Each application of Dest or Eq-frame-ded is internal. Assume that $\mathcal{M}_0 = [R_1, \ldots R_n]$ and $\mathcal{M}'_0 = [R'_1, \ldots, R'_n]$ where R_i, R'_i are row matrices. Assume w.l.o.g. that the rule is applied on the first line. By definition of the application of an internal rule, we have $\mathcal{M}_1 = [W_1, W_2, R_2, \ldots, R_n]$ and $\mathcal{M}'_1 = [W'_1, W'_2, R'_2, \ldots, R'_n]$ where W_1, W_2 (resp. W'_1, W'_2) are the two row matrices obtained from R_1 (resp. R'_1).

Let $\mathcal{C}$ be constraint system in R_1 (resp. R'_1). Let $\mathcal{C}_1$ and $\mathcal{C}_2$ be the two sons of $\mathcal{C}$ by application of the rule. We know that $\mathcal{C}_1 \in W_1$ (resp. $\mathcal{C}_1 \in W'_1$) and $\mathcal{C}_2 \in W_2$ (resp. $\mathcal{C}_2 \in W'_2$). But since we proved that $\mu_{1.a}(\mathcal{C}_1) < \mu_{1.a}(\mathcal{C})$ and $\mu_{1.a}(\mathcal{C}_2) < \mu_{1.a}(\mathcal{C})$, we deduce that $\mu^m_{1.a}(\mathcal{M}_1, \mathcal{M}'_1) < \mu^m_{1.a}(\mathcal{M}_0, \mathcal{M}'_0)$. □

Appendix G.1.2. Steps b and c: dealing with internal deducibility constraints

As stated in Section 4, after Step a, the strategy alternates between Ste b and Step c. We first establish termination for each step separately (for any support s, and any column number k). Then, we will show termination of Steps b and c together.

Step b alone. We define a lexicographic measure $\mu_{1.b}(\mathcal{C})$ on constraint system $\mathcal{C}$ as follows (when $\mathcal{C} \neq \bot$, by convention, we have that $\mu_{1.b}(\mathcal{C}) = (\emptyset, 0, 0, 0, 0, 0, 0, 0, 0)$.):

1. The multiset $\{\{(X, \mathsf{f}) \mid E_\Pi \not\vdash \mathsf{root}(X) \neq^? \mathsf{f}, (X, i \vdash^? u) \in D, u \in \mathcal{X}^1, \mathsf{f} \in \mathcal{F}_c$ and there exists $\mathsf{g} \in \mathcal{F}_c$ such that $E_\Pi \vDash \mathsf{root}(X) \neq^? \mathsf{g}\}\}$.

2. The number of first-order variables occurring in deducibility constraints, i.e. $|vars^1(D)|$.

3. The number of frame elements on which DED-ST is not useless
4. The number of pair of frame elements on which EQ-FRAME-FRAME is not useless
5. The number of function symbols and names occurring in the right-hand side of a deducibility constraint.
6. The number of (X, f) such that $\mathsf{root}(X) \neq^? \mathsf{f}$ not in E_Π, $(X, i \vdash^? u) \in D$ and $\mathsf{f} \in \mathcal{F}_c$.
7. The number of (X, ξ) such that $(X, i \vdash^? u) \in D$, $(\xi, j \vdash^? v) \in \Phi$, $j \leq i$ and $X \neq \xi$ is not in E_Π.
8. The number of deducibility constraints, i.e. $|D|$.

Lemma 60. *Let $\mathcal{C}$ be a well-formed constraint system satisfying $\mathsf{InvVarFrame}(s)$, and $\text{RULE}(\tilde{p})$ be any instance of a rule (except DEST and EQ-FRAME-DED) with support inferior to s. Assume that $\text{RULE}(\tilde{p})$ is strongly applicable on $\mathcal{C}$, and let $\mathcal{C}_1$, $\mathcal{C}_2$ be the two constraint systems obtained by applying $\text{RULE}(\tilde{p})$ on $\mathcal{C}$. We have that:*

$$\mu_{1.b}(\mathcal{C}_1) < \mu_{1.b}(\mathcal{C}) \quad \wedge \quad \mu_{1.b}(\mathcal{C}_2) < \mu_{1.b}(\mathcal{C})$$

Proof. We prove the this result by case analysis on the rule $\text{RULE}(\tilde{p})$.

Rule $\text{CONS}(X, \mathsf{f})$*:* Since we know that the rule is strongly applicable on $\mathcal{C}$, we know that there exists i, t such that $(X, i \vdash^? t) \in D(\mathcal{C})$ and $t \notin \mathcal{X}^1$ or $t \in \mathcal{X}^1$ and there exists $\mathsf{g} \in \mathcal{F}_c$ such that $\mathsf{root}(X) \neq^? \mathsf{g}$ is in $E_\Pi(\mathcal{C})$.

We first focus on $\mathcal{C}_1$. We know that $\mathcal{C}_1$ is normalised. Hence, the rule CONS adds in $D(\mathcal{C}_1)$ the deducibility constraints $(X_k, i \vdash^? x_k\sigma)$ where X_k, x_k are fresh, for $k = 1 \dots n$, and $\sigma = \mathsf{mgu}(t, \mathsf{f}(x_1, \dots, x_n))$.

But since X_k are fresh and $E_\Pi(\mathcal{C}_1) = E_\Pi(\mathcal{C}) \wedge X =^? \mathsf{f}(X_1, \dots, X_n)$, we deduce that $(X_k, \mathsf{g}) \notin \pi_1(\mu_{1.b}(\mathcal{C}_1))$, for all g, $k = 1 \dots n$. Furthermore, since for all $(Y, j \vdash^? v) \in D(\mathcal{C})$ other than $(X, i \vdash^? t)$, $(Y, j \vdash^? v\sigma) \in D(\mathcal{C}_1)$, then $(Y, \mathsf{g}) \in \pi_1(\mu_{1.b}(\mathcal{C}_1))$ implies $(Y, \mathsf{g}) \in \pi_1(\mu_{1.b}(\mathcal{C}_1))$. Hence we deduce that $\pi_1(\mu_{1.b}(\mathcal{C}_1)) \leq \pi_1(\mu_{1.b}(\mathcal{C}))$.

If $t \in \mathcal{X}^1$ then we have at least $(X, \mathsf{f}) \in \pi_1(\mathcal{C})$. But since $X \notin vars^2(D(\mathcal{C}_1))$, we deduce that $\pi_1(\mu_{1.b}(\mathcal{C}_1)) < \pi_1(\mu_{1.b}(\mathcal{C}))$. Thus, we conclude that $\mu_{1.b}(\mathcal{C}_1) < \mu_{1.b}(\mathcal{C})$.

Else $t \notin \mathcal{X}^1$: If $\mathsf{root}(t) \neq \mathsf{f}$, we have that $\mathcal{C}_1{\downarrow} = \bot$ hence the result trivially holds. Else $\mathsf{root}(t) = \mathsf{f}$ and so it implies that $\mathsf{root}(t) = \mathsf{f}$ and $\text{dom}(\sigma) = \{x_1, \dots, x_n\}$. Hence $x_k\sigma$ is a strict subterm of t, for $k = 1 \dots n$. Hence we have that $vars^1(D(\mathcal{C}_1)) = vars^1(D(\mathcal{C}))$ and so $\pi_2(\mu_{1.b}(\mathcal{C}_1)) = \pi_2(\mu_{1.b}(\mathcal{C}))$. $t \notin \mathcal{X}^1$ also implies that $\Phi(\mathcal{C}_1) = \Phi(\mathcal{C})$ and $ND(\mathcal{C}_1) = ND(\mathcal{C})$. Hence, since the application conditions of DED-ST and EQ-FRAME-FRAME only depends on these two elements, we deduce that $\pi_4(\mu_{1.b}(\mathcal{C}_1)) = \pi_4(\mu_{1.b}(\mathcal{C}))$ and $\pi_3(\mu_{1.b}(\mathcal{C}_1)) = \pi_3(\mu_{1.b}(\mathcal{C}))$. At last, since $\text{dom}(\sigma) = \{x_1, \dots, x_n\}$ and $x_k\sigma$ are strict subterms of t, we can deduce that $\pi_5(\mu_{1.b}(\mathcal{C}_1)) < \pi_5(\mu_{1.b}(\mathcal{C}))$. Thus, we conclude that $\mu_{1.b}(\mathcal{C}_1) < \mu_{1.b}(\mathcal{C})$.

We now focus on $\mathcal{C}_2$. In such a case, the only difference between $\mathcal{C}_2$ and $\mathcal{C}$ is that $E_\Pi(\mathcal{C}_2) = E_\Pi(\mathcal{C}) \wedge \mathsf{root}(X) \neq^? \mathsf{f}$. Hence we trivially have that $\pi_k(\mu_{1.b}(\mathcal{C}_2)) = \pi_k(\mu_{1.b}(\mathcal{C}))$, for $k = 2 \dots 5$. On the other hand, if $t \in \mathcal{X}^1$ then we have $\pi_1(\mu_{1.b}(\mathcal{C}_2)) < \pi_1(\mu_{1.b}(\mathcal{C}))$ else

we have that $\pi_1(\mu_{1.b}(\mathcal{C}_2)) = \pi_1(\mu_{1.b}(\mathcal{C}))$ and $\pi_6(\mu_{1.b}(\mathcal{C}_2)) < \pi_6(\mu_{1.b}(\mathcal{C}))$. Hence, in both cases, we can conclude that $\mu_{1.b}(\mathcal{C}_2) < \mu_{1.b}(\mathcal{C})$.

Rule AXIOM(X, ξ)*:* Since the rule is strongly applicable on $\mathcal{C}$, we know that there exists $(X, i \vdash^? u) \in D(\mathcal{C})$, $(\xi, j \rhd v) \in \Phi(\mathcal{C})$ such that $j \leq i$ and either $u \notin \mathcal{X}^1$ or $t \in \mathcal{X}^1$ and there exists $\mathsf{g} \in \mathcal{F}_c$ such that $E_\Pi(\mathcal{C}) \vDash \mathsf{root}(X) \neq^? \mathsf{g}$.

We first focus on $\mathcal{C}_1$. We know that $\mathcal{C}_1$ is normalised. Hence, we have that $D(\mathcal{C}_1) = D(\mathcal{C})\sigma \setminus \{X, i \vdash^? u\sigma\}$ where $\sigma = \mathsf{mgu}(u, v)$. Furthermore, we have $E_\Pi(\mathcal{C}_1) = E_\Pi(\mathcal{C}) \wedge X =^? \xi$. Thus, we have that $\pi_1(\mu_{1.b}(\mathcal{C}_1)) \leq \pi_1(\mu_{1.b}(\mathcal{C}))$. We now do a case analysis on the terms u and v:

- *Case* $u \in \mathcal{X}^1$: In such a case we have that there exist f such that $(X, \mathsf{f}) \in \pi_1(\mu_{1.b}(\mathcal{C}))$. Since $D(\mathcal{C}_1) = D(\mathcal{C})\sigma \setminus \{X, i \vdash^? u\sigma\}$, we can deduce that $\pi_1(\mu_{1.b}(\mathcal{C}_1)) < \pi_1(\mu_{1.b}(\mathcal{C}))$. Thus we conclude that $\mu_{1.b}(\mathcal{C}_1) < \mu_{1.b}(\mathcal{C})$.

- *Case* $u \notin \mathcal{X}^1$ *and* σ *is the identity:* σ being the identity implies that $u = v$ and so thanks to the origination property of constraint system, we have that $|vars^1(D(\mathcal{C}_1))| = |vars^1(D(\mathcal{C}))|$. Furthermore since $\Phi(\mathcal{C}_1) = \Phi(\mathcal{C})$, we trivially have that $\pi_4(\mu_{1.b}(\mathcal{C}_1)) = \pi_4(\mu_{1.b}(\mathcal{C}))$ and $\pi_3(\mu_{1.b}(\mathcal{C}_1)) = \pi_3(\mu_{1.b}(\mathcal{C}))$. At last, $u \notin \mathcal{X}^1$ implies that u is either a name or $\mathsf{root}(u) \in \mathcal{F}_c$. Thus $D(\mathcal{C}_1) = D(\mathcal{C}) \setminus \{X, i \vdash^? u\}$ implies that $\pi_5(\mu_{1.b}(\mathcal{C}_1)) < \pi_5(\mu_{1.b}(\mathcal{C}))$. Thus we conclude that $\mu_{1.b}(\mathcal{C}_1) < \mu_{1.b}(\mathcal{C})$.

- *Case* $u \notin \mathcal{X}^1$ *and* σ *is not the identity:*. By the property of origination of a constraint system, we know that $vars^1(v) \subseteq vars^1(D(\mathcal{C}))$. Hence we have that $|vars^1(D(\mathcal{C})\sigma)| < |vars^1(D(\mathcal{C}))|$. We proved that $D(\mathcal{C}_1) \subseteq D(\mathcal{C})\sigma$, therefore we can deduce that $\pi_2(\mu_{1.b}(\mathcal{C}_1)) < \pi_2(\mu_{1.b}(\mathcal{C}_1))$. Thus we conclude that $\mu_{1.b}(\mathcal{C}_1) < \mu_{1.b}(\mathcal{C})$.

We now focus on $\mathcal{C}_2$. In such a case, the only difference between $\mathcal{C}_2$ and $\mathcal{C}$ is that $E_\Pi(\mathcal{C}_2) = E_\Pi(\mathcal{C}) \wedge X \neq^? \xi$. Hence we trivially have that $\pi_k(\mu_{1.b}(\mathcal{C}_2)) = \pi_k(\mu_{1.b}(\mathcal{C}))$, for $k = 1 \ldots 6$. Moreover, $E_\Pi(\mathcal{C}_2) = E_\Pi(\mathcal{C}) \wedge X \neq^? \xi$ also implies that $\pi_7(\mu_{1.b}(\mathcal{C}_2)) < \pi_7(\mu_{1.b}(\mathcal{C}))$. Thus we conclude that $\mu_{1.b}(\mathcal{C}_2) < \mu_{1.b}(\mathcal{C})$.

Rule EQ-FRAME-FRAME(ξ_1, ξ_2)*:* Since the rule is (strongly) applicable on $\mathcal{C}$ (for Phase 1), we know that there exists $(\xi_1, i_1 \vdash^? u_1) \in \Phi(\mathcal{C})$, $(\xi_2, u_2 \rhd u_2) \in \Phi(\mathcal{C})$.

We first focus on $\mathcal{C}_1$. We know that $\mathcal{C}_1$ is normalised. Hence, we have that $D(\mathcal{C}_1) = D(\mathcal{C})\sigma$ where $\sigma = \mathsf{mgu}(u_1, u_2)$. Thus, we have that $\pi_1(\mu_{1.b}(\mathcal{C}_1)) \leq \pi_1(\mu_{1.b}(\mathcal{C}))$.

By the origination property of a constraint system, we know that $vars^1(u_1, u_2) \subseteq vars^1(D(\mathcal{C}))$. Hence we deduce that $vars^1(D(\mathcal{C}_1)) \subseteq vars^1(D(\mathcal{C}))$. In case σ is not the identity we have that $|vars^1(D(\mathcal{C}_1))| < |vars^1(D(\mathcal{C}))|$. Thus we deduce that $\mu_{1.b}(\mathcal{C}_1) < \mu_{1.b}(\mathcal{C})$.

Otherwise, we have that σ is the identity, and we have that $vars^1(D(\mathcal{C}_1)) = vars^1(D(\mathcal{C}))$ and so $\pi_2(\mu_{1.b}(\mathcal{C}_1)) \leq \pi_2(\mu_{1.b}(\mathcal{C}))$. Furthermore, σ being the identity also implies that $\Phi(\mathcal{C}_1) = \Phi(\mathcal{C})$. Thus we deduce that $\pi_3(\mu_{1.b}(\mathcal{C}_1)) = \pi_3(\mu_{1.b}(\mathcal{C}))$. At last, since we consider an application of the rule EQ-FRAME-FRAME, we trivially have that $\pi_4(\mu_{1.b}(\mathcal{C}_1)) < \pi_4(\mu_{1.b}(\mathcal{C}))$. Thus, we conclude that $\mu_{1.b}(\mathcal{C}_1) < \mu_{1.b}(\mathcal{C})$.

Rule EQ-DED-DED(X, Y)*:* Since the rule is strongly applicable on $\mathcal{C}$, we know that there exists $(X, i \vdash^? u) \in D(\mathcal{C})$ and $(Y, j \vdash^? v) \in D(\mathcal{C})$ such that $u = v \in \mathcal{X}^1$. In such a case, we first have that $\mathcal{C}_2 = \bot$ since $E_\Pi(\mathcal{C}_2) \vDash u \neq^? u$ yields $\bot$ by normalisation. Thus we deduce that $\mu_{1.b}(\mathcal{C}_2) < \mu_{1.b}(\mathcal{C})$.

We know focus on $\mathcal{C}_1$. We have that $D(\mathcal{C}_1) = D(\mathcal{C}) \setminus \{Xi \vdash^? u\}$. Hence we deduce that $\pi_k(\mu_{1.b}(\mathcal{C}_1)) \leq \pi_k(\mu_{1.b}(\mathcal{C}))$, for $k = 1, 6, 7$ and that $\pi_8(\mu_{1.b}(\mathcal{C}_1)) < \pi_8(\mu_{1.b}(\mathcal{C}))$. Furthermore, since $\Phi(\mathcal{C}_1) = \Phi(\mathcal{C})$, we deduce that $\pi_k(\mu_{1.b}(\mathcal{C}_1)) = \pi_k(\mu_{1.b}(\mathcal{C}))$, for $k = 2, 3, 4, 5$. Thus we conclude that $\mu_{1.b}(\mathcal{C}_1) < \mu_{1.b}(\mathcal{C})$.

Rule DED-ST(ξ, f, i)*:* Since the rule is (strongly) applicable on $\mathcal{C}$, we know that there exists $(\xi, i \rhd u) \in \Phi(\mathcal{C})$ such that $(\xi, i \rhd u) \notin \mathsf{NoUse}(\mathcal{C})$. We know that $\mathcal{C}$ satisfies the invariant $\mathsf{InvVarFrame}(s)$ hence we deduce that $u \notin \mathcal{X}^1$.

We first focus on $\mathcal{C}_1$. In case $\mathsf{root}(u) \neq \mathsf{f}$, we have that $\mathcal{C}_1 = \bot$ since $\mathcal{C}_1$ is normalised (otherwise, we would have $E(\mathcal{C}_1) = E(\mathcal{C}) \wedge u =^? \mathsf{f}(x_1, \ldots, x_n)$ which is reduced into $\bot$ by the normalisation rule (Nins1)). Thus we deduce that $\mu_{1.b}(\mathcal{C}_1) < \mu_{1.b}(\mathcal{C})$.

Otherwise, we have that $\mathsf{root}(u) = \mathsf{f}$. In such a case, we have $E_\Pi(\mathcal{C}_1) = E_\Pi(\mathcal{C})$, $\Phi(\mathcal{C}_1) = \Phi(\mathcal{C})$ and $D(\mathcal{C}_1) = D(\mathcal{C}) \cup \{X_k, i \vdash^? x_k\sigma\}_{k=1\ldots n}$ such that $x_k\sigma$ is a strict subterm of u and X_k are fresh, for $k = 1 \ldots n$ and $\sigma = \mathsf{mgu}(u =^? \mathsf{f}(x_1, \ldots, x_n))$. X_k being fresh implies that there do not exist $\mathsf{g} \in \mathcal{F}_c$ such that $E_\Pi(\mathcal{C}_1) \vDash \mathsf{root}(X) \neq^? \mathsf{g}$. Hence we deduce that $\pi_1(\mu_{1.b}(\mathcal{C}_1)) = \pi_1(\mu_{1.b}(\mathcal{C}))$. Furthermore, thanks to the origination property of a constraint system, we know that $vars^1(u) \subseteq vars^1(D(\mathcal{C}))$, thus thanks to $x_k\sigma$ being strict subterm of u, we deduce that $\pi_2(\mu_{1.b}(\mathcal{C}_1)) \leq \pi_2(\mu_{1.b}(\mathcal{C}))$. At last, we are focused on the case of the application of the rule DED-ST, therefore we trivially have that $\pi_3(\mu_{1.b}(\mathcal{C}_1)) < \pi_3(\mu_{1.b}(\mathcal{C}))$. Thus we conclude that $\mu_{1.b}(\mathcal{C}_1) < \mu_{1.b}(\mathcal{C})$.

We now focus on $\mathcal{C}_2$. In such a case, we have that $E_\Pi(\mathcal{C}_2) = E_\Pi(\mathcal{C})$, $\Phi(\mathcal{C}_2) = \Phi(\mathcal{C})$ and $D(\mathcal{C}_2) = D(\mathcal{C})$. Hence we trivially have that $\pi_k(\mu_{1.b}(\mathcal{C}_2)) \leq \pi_k(\mu_{1.b}(\mathcal{C}))$, for $k = 1, 2$. At last, since we consider an application of the rule DED-ST, we trivially have that $\pi_3(\mu_{1.b}(\mathcal{C}_2)) < \pi_3(\mu_{1.b}(\mathcal{C}))$ and so we conclude that $\mu_{1.b}(\mathcal{C}_2) < \mu_{1.b}(\mathcal{C})$. □

During Step b with parameter s and k where k is the index of the column of $(\mathcal{M}, \mathcal{M}')$, an internal rule is applied on the i^{th} line of the matrices $(\mathcal{M}, \mathcal{M}')$ only if this rule is strongly applicable on constraint system on the i^{th} line and k^{th} column of $(\mathcal{M}, \mathcal{M}')$. Hence, for a pair of matrices of constraint system, we define a measure from $\mu_{1.b}(\cdot)$, denoted $\mu^k_{1.b}()$, which is the following multiset:

$$\mu^k_{1.b}(\mathcal{M}, \mathcal{M}') = \{\{\mu_{1.b}(\mathcal{C}) \mid i \in \mathbb{N} \text{ and } \mathcal{C} \text{ is on the } i^{\text{th}} \text{ line and } k^{\text{th}} \text{ column of } (\mathcal{M}, \mathcal{M}')\}\}$$

Hence thanks to Lemma 60, we can deduce the following corollary.

Corollary 3. *Let $(\mathcal{M}_0, \mathcal{M}'_0)$ be a pair of matrices of constraint systems obtained during Step b of Phase 1 with parameters s and k, and following the strategy $\mathcal{S}$. Let* RULE$(\tilde{p})$ *be an instance of an internal rule applicable at this stage, and $(\mathcal{M}_1, \mathcal{M}'_1)$ be the resulting pair of matrices. We have that: $\mu^k_{1.b}(\mathcal{M}_1, \mathcal{M}'_1) < \mu^k_{1.b}(\mathcal{M}_0, \mathcal{M}'_0)$*

Step c alone. The purpose of this step is to definitely remove internal deducibility constraints. During this step, an application can be either an internal one or an external one, and this last case may imply some modifications in the whole matrix. The application condition of a rule during this step of the strategy heavily depends on the subset $\mathsf{X}^1(\mathcal{C})$ which collects all the first-order variables of the deducibility constraints whose recipe variable is not in $S_2(\mathcal{C})$. Hence, the measure that we use to show the termination of this step also depends on this set.

Let $\mathcal{C} = (S_1; S_2; \Phi; D; E; E_\Pi; ND; \mathsf{NoUse})$ be a constraint system, we define a lexicographic measure on $\mathcal{C}$, denoted $\mu_{1.c}(\mathcal{C})$, which is composed by :

1. The multiset $\{\{(j,p) \mid (X, i \vdash^? u) \in D(\mathcal{C}), u|_p \in \mathsf{X}^1(\mathcal{C}), \mathcal{L}^1_{\mathcal{C}}(u|_p) = j \text{ and } X \in S_2\}\}$.
2. The multiset $\{\{X, Y \mid (X, s \vdash^? u) \in D(\mathcal{C}), (Y, s \vdash^? v) \in D(\mathcal{C}), X, Y \notin S_2(\mathcal{C}) \text{ and } u = v \in \mathcal{X}^1\}\}$.
3. The number of (X, f) such that $E_\Pi \not\Vdash \mathsf{root}(X) \neq^? \mathsf{f}$, $(X, i \vdash^? u) \in D$, $X \in S_2$, $\mathsf{f} \in \mathcal{F}_c$ and $vars(u) \cap \mathsf{X}^1(\mathcal{C}) \neq \emptyset$.
4. The number of (X, ξ) such that $(X, i \vdash^? u) \in D$, $(\xi, j \rhd v) \in \Phi$, $j \leq i$, $E_\Pi \not\Vdash X \neq^? \xi$, $X \in S_2$ and $vars(u) \cap \mathsf{X}^1(\mathcal{C}) \neq \emptyset$.

By convention, we have that $\mu_{1.c}(\mathcal{C}) = (\emptyset, \emptyset, 0, 0)$ when $\mathcal{C} = \bot$.

Furthermore, we extend this measure to a pair $(\mathcal{M}, \mathcal{M}')$ of matrices as follows:

$$\mu^k_{1.c}(\mathcal{M}, \mathcal{M}') = \{\{\mu_{1.c}(\mathcal{C}) \mid i \in \mathbb{N} \text{ and } \mathcal{C} \text{ is on the } i^{\text{th}} \text{ line and } k^{\text{th}} \text{ column of } (\mathcal{M}, \mathcal{M}')\}\}$$

Thanks to this measure, we are now able to show that the Step c of Phase 1 of the strategy terminates for parameters s and k.

Lemma 61. *Let $(\mathcal{M}, \mathcal{M}')$ be a pair of matrices obtained during the Step c of Phase 1 of the the strategy with parameters s and k, and assume w.l.o.g. that k is less or equal to the number of columns in $\mathcal{M}$. Assume that the rule* Cons(X_0, f) *can be applied externally on $(\mathcal{M}, \mathcal{M}')$ such that $(X_0, j_0 \vdash^? u_0) \in D(\mathcal{M}_{i_0,k})$, $i_0 \in \{1, \ldots, n\}$ and*

$$\mathcal{L}^1_{\mathcal{M}_{i_0,k}}(X_0, j_0 \vdash^? u_0) = \min \left\{ \mathcal{L}^1_{\mathcal{M}_{i,k}}(Z, \ell \vdash^? v) \;\middle|\; \begin{array}{l} i \in \{1, \ldots, n\}, (Z, \ell \vdash^? v) \in D(\mathcal{M}_{i,k}), \\ vars(v) \cap \mathsf{X}^1(\mathcal{M}_{i,k}) \neq \emptyset, Z \in S_2 \end{array} \right\}$$

For all term u, for all $i \in \{1, \ldots, n\}$, if $(X_0, j_0 \vdash^? u) \in D(\mathcal{M}_{i,k})$ and $u \in \mathcal{X}^1$ then $u \notin \mathsf{X}^1(\mathcal{M}_{i,k})$.

Proof. For simplicity, we will denote $\mathcal{C} = \mathcal{M}_{i_0,k}$ and $\mathcal{C}' = \mathcal{M}_{i,k}$. We know $(X_0, j_0 \vdash^? u_0) \in D(\mathcal{C})$. Let $(X_0, j_0 \vdash^? u) \in D(\mathcal{C}')$ such that $u \in \mathcal{X}^1$. Assume that $u \in \mathsf{X}^1(\mathcal{C}')$. In such a case, we have that $\mathcal{L}^1_{\mathcal{C}'}(X_0, j_0 \vdash^? u) = (j_0, \epsilon)$. But we know that $(X_0, j_0 \vdash^? u_0) \in D(\mathcal{C})$ and by the minimality of $\mathcal{L}^1_{\mathcal{C}}(X_0, j_0 \vdash^? u_0)$, we deduce that $\mathcal{L}^1_{\mathcal{C}}(X_0, j_0 \vdash^? u_0) \leq (j_0, \epsilon)$. Hence we deduce that $u_0 \in \mathcal{X}^1$ and $u_0 \in \mathsf{X}^1(\mathcal{C})$.

But $u_0 \in \mathsf{X}^1(\mathcal{C})$ also implies that there exists $(Y, j \vdash^? u_0) \in D(\mathcal{C})$ such that $Y \notin S_2$. Moreover, the minimality of $\mathcal{L}^1_{\mathcal{C}}(X_0, j_0 \vdash^? u_0)$ also implies that there is no deducibility constraint $(Y', j' \vdash^? v) \in D(\mathcal{C})$ such that $u_0 \in vars^1(v)$ and $j' < j_0$. Hence, thanks to $\mathcal{C}$ being well-formed (Definition 18, item 10) we deduce that $j_0 < j$. Consider the pair of matrices of constraint system system $(\mathcal{M}_1, \mathcal{M}'_1)$ ancestor of $(\mathcal{M}, \mathcal{M}')$ such that $(\mathcal{M}_1, \mathcal{M}'_1)$ is obtained at the end of Step b with parameters s and k. Thanks to Lemma 27, we know that $(\mathcal{M}_1, \mathcal{M}'_1)$ satisfies $\mathsf{PP1SbE}(s, k)$. Let $\mathcal{C}_1$ be the constraint system in $\mathcal{M}_1$ ancestor of $\mathcal{C}$. Since no internal rule are applied other than Eq-ded-ded during step c, we deduce that $(Y', j' \vdash^? v') \in D(\mathcal{C}_1)$ for some v' and so thanks to Property $\mathsf{PP1SbE}(s, k)$, we deduce that for all $\mathsf{f} \in \mathcal{F}_c$, $E_\Pi(\mathcal{C}_1) \not\Vdash \mathsf{root}(Y) \neq^? \mathsf{f}$. Once again thanks to the fact that no internal rule are applied other than Eq-ded-ded during step c, we can easily show that for all $\mathsf{f} \in \mathcal{F}_c$, $E_\Pi(\mathcal{C}) \not\Vdash \mathsf{root}(Y) \neq^? \mathsf{f}$.

Furthermore, Property $\mathsf{PP1SbE}(s, k)$ indicates that for all $X \in vars^2(D(\mathcal{C}_1))$, for all $\mathsf{f} \in \mathcal{F}_c$, $E_\Pi(\mathcal{C}_1) \not\Vdash \mathsf{root}(X) \neq^? \mathsf{f}$. Hence, if if there exists $\mathsf{f} \in \mathcal{F}_c$ such that $E_\Pi(\mathcal{C}) \vDash \mathsf{root}(X_0) \neq^? \mathsf{f}$, it would implies that there exists $\mathcal{C}''$ such that $\mathcal{C}_1 \to^* \mathcal{C}'' \to^* \mathcal{C}$, $\mathcal{C}''$ is

obtained during step c, $(X_0, j_0 \vdash^? u_0) \in D(\mathcal{C}'')$, $(Y, j \vdash^? u_0) \in D(\mathcal{C}'')$ and for all $\mathsf{f} \in \mathcal{F}_c$, $E_\Pi(\mathcal{C}) \not\vDash \mathsf{root}(X_0) \neq^? \mathsf{f}$. But in such a case, the rule Eq-ded-ded should have been applied according to the strategy and so we would have that $(Y, j \vdash^? x_0) \notin D(\mathcal{C})$ which is a contradiction. Hence we conclude that $u \notin \mathsf{X}^1(\mathcal{C}')$. □

Lemma 62. *Let $(\mathcal{M}, \mathcal{M}')$ be a pair of matrices obtained during the Step c of Phase 1 with parameters s and k. Let* Rule$(\tilde{p})$ *be an instance of a rule which is applicable according to Step c of the strategy and let $(\mathcal{M}_1, \mathcal{M}'_1)$ and $(\mathcal{M}_2, \mathcal{M}'_2)$ be the two pairs of matrices of constraint systems obtained by application of* Rule$(\tilde{p})$ *on $(\mathcal{M}, \mathcal{M}')$ (in case* Rule$(\tilde{p})$ *is* Eq-ded-ded*, there is only one resulting pairsince* Eq-ded-ded *is applied internally). We have that:*

$$\mu^k_{1.c}(\mathcal{M}_1, \mathcal{M}'_1) < \mu^k_{1.c}(\mathcal{M}, \mathcal{M}') \quad \wedge \quad \mu^k_{1.c}(\mathcal{M}_2, \mathcal{M}'_2) < \mu^k_{1.c}(\mathcal{M}, \mathcal{M}')$$

Proof. We prove the result by case analysis on the rule Rule$(\tilde{p})$:

Rule Eq-ded-ded(X, Y)*:* Since this rule is applied internally, there exists $\mathcal{C}$ in the k^{th} column of $(\mathcal{M}, \mathcal{M}')$ such that Eq-ded-ded(X, Y) is strongly applicable on $\mathcal{C}$. Furthermore, we deduce that $X \notin S_2(\mathcal{C})$ and $Y \in S_2(\mathcal{C})$. Assume that $(X, i \vdash^? x) \in D(\mathcal{C})$ and $(Y, j \vdash^? x) \in D(\mathcal{C})$. According to the strong application condition of Eq-ded-ded(X, Y) in case of internal rule for phase 1, we have that $j < i$.

By normalisation, we have that $\mathcal{C}_2 = \bot$ and so we trivially have that $\mu_{1.c}(\mathcal{C}_2) < \mu_{1.c}(\mathcal{C})$.

We focus on $\mathcal{C}_1$: Since $Y \in S_2(\mathcal{C})$ and $x \in \mathcal{X}^1$, we can deduce that $\mathcal{L}^1_{\mathcal{C}}(Y, j \vdash^? x) = (j, 0)$. But $D(\mathcal{C}_1) = D(\mathcal{C}) \setminus \{X, i \vdash^? x\}$.

If there is no $(Z, \ell \vdash^? x) \in D(\mathcal{C})$ such that $Z \neq X$ and $Z \notin S_2(\mathcal{C})$, we have that $x \notin \mathsf{X}^1(\mathcal{C}_1)$. Hence, we can deduce that $\mathcal{L}^1_{\mathcal{C}_1}(Y, j \vdash^? x)$ is not defined and so $\pi_1(\mu_{1.c}(\mathcal{C}_1)) < \pi_1(\mu_{1.c}(\mathcal{C}))$. Thus we deduce that $\mu_{1.c}(\mathcal{C}_1) < \mu_{1.c}(\mathcal{C})$

Else there exists $(Z, \ell \vdash^? x) \in D(\mathcal{C})$ such that $Z \neq X$ and $Z \notin S_2(\mathcal{C})$. Thus $\mathsf{X}^1(\mathcal{C}_1) = \mathsf{X}^1(\mathcal{C})$. Thus, with $D(\mathcal{C}_1) = D(\mathcal{C}) \setminus \{X, i \vdash^? x\}$, we deduce that $\pi_1(\mu_{1.c}(\mathcal{C}_1)) = \pi_1(\mu_{1.c}(\mathcal{C}))$. Furthermore, we $(X, Z) \in \pi_2(\mu_{1.c}(\mathcal{C}))$ while $(X, Z) \notin \pi_2(\mu_{1.c}(\mathcal{C}_1))$. Hence we easily deduce that $\pi_2(\mu_{1.c}(\mathcal{C}_1)) < \pi_2(\mu_{1.c}(\mathcal{C}))$ and so that $\mu_{1.c}(\mathcal{C}_1) < \mu_{1.c}(\mathcal{C})$.

Since we proved that $\mu_{1.c}(\mathcal{C}_1) < \mu_{1.c}(\mathcal{C})$ and $\mu_{1.c}(\mathcal{C}_2) < \mu_{1.c}(\mathcal{C})$ and since the rule is applied internally, we deduce that $\mu^k_{1.c}(\mathcal{M}_1, \mathcal{M}'_1) < \mu^k_{1.c}(\mathcal{M}, \mathcal{M}')$.

Rue Cons(X, f)*:* The rule is applied externally. Hence we will show that for all constraint system $\mathcal{C}$ in the k^{th} column, we have that $\mu_{1.c}(\mathcal{C}_1) \leq \mu_{1.c}(\mathcal{C})$ and $\mu_{1.c}(\mathcal{C}_2) \leq \mu_{1.c}(\mathcal{C})$ where $\mathcal{C}_1$ and $\mathcal{C}_2$ are the constraint systems obtained by applying the rule on $\mathcal{C}$. Furthermore, by the definition of the strategy, we know that there exists $\mathcal{C}_0$ such that $\mathcal{L}^1_{\mathcal{C}_0}(X, i_0 \vdash^? u_0)$ is minimal. Thus, we will show that in the case of $\mathcal{C}_0$, $\mu_{1.c}(\mathcal{C}_1) < \mu_{1.c}(\mathcal{C}_0)$ and $\mu_{1.c}(\mathcal{C}_2) < \mu_{1.c}(\mathcal{C}_0)$, where $\mathcal{C}_1$ and $\mathcal{C}_2$ are the constraint systems obtained by applying the rule on $\mathcal{C}_0$.

We first focus on $\mathcal{C}_1$. Thanks to Lemma 61, we know that for all $\mathcal{C}$ in the k^{th} column, for all $i \in \mathbb{N}$, for all term u, $(X, i_0 \vdash^? u) \in D(\mathcal{C})$ and $u \in \mathcal{X}^1$ implies $u \notin \mathsf{X}^1(\mathcal{C})$. We distinguish several cases:

- *Case $u \in \mathcal{X}^1$:* By normalisation, $D(\mathcal{C}_1) = (D(\mathcal{C})\{X, i_0 \vdash^? u\})\sigma \cup \{X_j, i_0 \vdash^? x_j\}_{j=1\ldots n}$ where $\sigma = \{u \to \mathsf{f}(x_1, \ldots, x_n)\}$ and x_j are fresh variables and $u \notin \mathsf{X}^1(\mathcal{C})$. Hence we deduce that for all $(Y, j \vdash^? v) \in D(\mathcal{C}_1)$, for all p, if $v|_p \in \mathsf{X}^1(\mathcal{C}_1)$ then $v|_p \in \mathcal{X}^1$, $v|_p = v|_p\sigma$ and $(Y, j \vdash^? v) \in D(\mathcal{C})$. Thus we deduce that $v|_p \in \mathsf{X}^1(\mathcal{C})$ and so

$\pi_1(\mu_{1.c}(\mathcal{C}_1)) = \pi_1(\mu_{1.c}(\mathcal{C}))$. Since $X_j \in S_2(\mathcal{C}_1)$, for $j = 1 \dots n$, we deduce that $\pi_2(\mu_{1.c}(\mathcal{C}_1)) = \pi_2(\mu_{1.c}(\mathcal{C}))$. At last, $x_j \notin \mathsf{X}^1(\mathcal{C}_1)$, for $j = 1 \dots n$ also implies that $\pi_i(\mu_{1.c}(\mathcal{C}_1)) = \pi_i(\mu_{1.c}(\mathcal{C}))$, for $i = 3, 4$ and so we deduce that $\mu_{1.c}(\mathcal{C}_1) = \mu_{1.c}(\mathcal{C})$.

- *Case $u \notin \mathcal{X}^1$ and $vars^1(u) \cap \mathsf{X}^1(\mathcal{C}) = \emptyset$:* In such a case, we have that $D(\mathcal{C}_1) = (D(\mathcal{C}) \setminus \{X, i_0 \vdash^? u\}) \cup \{X_j, i_0 \vdash^? x_j\sigma\}_{j=1\dots n}$ where $x_j\sigma$ is a strict subterm of u, for $j = 1 \dots n$ and $\sigma = \mathsf{mgu}(u =^? \mathsf{f}(x_1, \dots, x_n))$. Thus, $vars^1(u) \cap \mathsf{X}^1(\mathcal{C}) = \emptyset$ implies that $vars^1(x_j\sigma) \cap \mathsf{X}^1(\mathcal{C}) = \emptyset$ for $j = 1 \dots n$. Therefore, we have that $\mathcal{L}^1_{\mathcal{C}_1}(X_j, i_0 \vdash^? x_j\sigma)$ does not exist, for $j = 1 \dots n$ which implies that $\pi_j(\mu_{1.c}(\mathcal{C}_1)) = \pi_j(\mu_{1.c}(\mathcal{C}))$ for $j = 1, 3, 4$. At last, since $X_j \in S_2(\mathcal{C}_1)$, for $j = 1 \dots n$, we deduce that $\pi_2(\mu_{1.c}(\mathcal{C}_1)) = \pi_2(\mu_{1.c}(\mathcal{C}))$ and so we conclude that $\mu_{1.c}(\mathcal{C}_1) = \mu_{1.c}(\mathcal{C})$.

- *Case $u \notin \mathcal{X}^1$ and $vars^1(u) \cap \mathsf{X}^1(\mathcal{C}) \neq \emptyset$:* In such a case, we still have that $D(\mathcal{C}_1) = (D(\mathcal{C}) \setminus \{X, i_0 \vdash^? u\}) \cup \{X_j, i_0 \vdash^? x_j\sigma\}_{j=1\dots n}$ where $\sigma = \mathsf{mgu}(u, \mathsf{f}(x_1, \dots, x_n))$. Since $u \notin \mathcal{X}^1$, we can deduce that for all $j \in \{1, \dots, n\}$, for all p, if $x_j\sigma|_p \in \mathsf{X}^1(\mathcal{C}_1)$ then $u|_{j \cdot p} = x_j\sigma|_p \in \mathsf{X}^1(\mathcal{C})$. With the fact that $\mathcal{L}^1_{\mathcal{C}}(x) = \mathcal{L}^1_{\mathcal{C}_1}(x)$ for all $x \in vars^1(D(\mathcal{C}))$, we can deduce that $(\mathcal{L}^1_{\mathcal{C}_1}(x_j\sigma|_p), p) < (\mathcal{L}^1_{\mathcal{C}}(x_j\sigma|_p), j \cdot p)$, for all $j \in \{1, \dots, n\}$. Thus we can deduce that $\pi_1(\mu_{1.c}(\mathcal{C}_1)) < \pi_1(\mu_{1.c}(\mathcal{C}))$ and so $\mu_{1.c}(\mathcal{C}_1) < \mu_{1.c}(\mathcal{C})$.

  Note that by the application condition of the rule $\textsc{Cons}(X, \mathsf{f})$ for Step c, we can deduce that $u_0 \notin \mathcal{X}^1$ and $vars^1(u_0) \cap \mathsf{X}^1(\mathcal{C}_0) \neq \emptyset$. Thus we have $\mu_{1.c}(\mathcal{C}_1) < \mu_{1.c}(\mathcal{C}_0)$

We now focus on $\mathcal{C}_2$. In such a case we have that $D(\mathcal{C}_2) = D(\mathcal{C})$. Hence, we trivially have that $\pi_i(\mu_{1.c}(\mathcal{C}_2)) = \pi_i(\mu_{1.c}(\mathcal{C}))$, for $i = 1, 2$. On the other hand, since $E_\Pi(\mathcal{C}_2) = E_\Pi(\mathcal{C}) \wedge \mathsf{root}(X) \neq^? \mathsf{f}$, we have that $\pi_3(\mu_{1.c}(\mathcal{C}_2)) \leq \pi_3(\mu_{1.c}(\mathcal{C}))$ which allows us to conclude that $\mu_{1.c}(\mathcal{C}_2) \leq \mu_{1.c}(\mathcal{C})$.

Note that by the application condition of the rule $\textsc{Cons}(X, \mathsf{f})$ for Step c, we can deduce that $u_0 \notin \mathcal{X}^1$ and $vars^1(u_0) \cap \mathsf{X}^1(\mathcal{C}_0) \neq \emptyset$. Thus we have $\pi_3(\mu_{1.c}(\mathcal{C}_2)) < \pi_3(\mu_{1.c}(\mathcal{C}_0))$ which allows us to conclude that $\mu_{1.c}(\mathcal{C}_2) < \mu_{1.c}(\mathcal{C}_0)$.

Rue $\textsc{Axiom}(X, \mathsf{path})$*:* The rule is applied externally. Hence, similarly to the case of the rule Cons, we will show that for all constraint system $\mathcal{C}$ in the k^{th} column, we have that $\mu_{1.c}(\mathcal{C}_1) \leq \mu_{1.c}(\mathcal{C})$ and $\mu_{1.c}(\mathcal{C}_2) \leq \mu_{1.c}(\mathcal{C})$ where $\mathcal{C}_1$ and $\mathcal{C}_2$ are the constraint systems obtained by applying the rule on $\mathcal{C}$. Furthermore, we will show that in the case of $\mathcal{C}_0$, $\mu_{1.c}(\mathcal{C}_1) < \mu_{1.c}(\mathcal{C}_0)$ and $\mu_{1.c}(\mathcal{C}_2) < \mu_{1.c}(\mathcal{C}_0)$, where $\mathcal{C}_1$ and $\mathcal{C}_2$ are the constraint systems obtained by applying the rule on $\mathcal{C}_0$.

By definition of the rule, we know that there exists $(X, i \vdash^? u) \in D(\mathcal{C})$ and $(\xi, j \vdash^? v) \in \Phi(\mathcal{C})$ such that $j \leq i$.

We first focus on $\mathcal{C}_1$. By definition of the rule, we have that $D(\mathcal{C}_1) = D(\mathcal{C})\sigma \setminus \{X, i \vdash^? u\sigma\}$ where $\sigma = \mathsf{mgu}(u, v)$. Furthermore, we have that $\Phi(\mathcal{C}_1) = \Phi(\mathcal{C})\sigma$.

Let $x \in vars^1(v)$. By the property of origination of a constraint system, we deduce that $\mathcal{L}^1_{\mathcal{C}}(x) < i$. Let $(Y, \ell \vdash^? t) \in D(\mathcal{C})$ such that $x \in vars^1 t$ and $\mathcal{L}^1_{\mathcal{C}}(x) = \ell$. By the minimality of $\mathcal{L}^1_{\mathcal{C}_0}(X, i \vdash^? u_0)$, we deduce that $x \notin \mathsf{X}^1(\mathcal{C})$.

Let $x \in \mathsf{X}^1(\mathcal{C}) \cap vars^1(u)$. If $x \in \mathrm{img}(\sigma)$ then we have that $x \in vars^1(v\sigma)$. But by the property of origination of a constraint system, we deduce that there exists $(Y, \ell \vdash^? t) \in D(\mathcal{C}_1)$ such that $\ell < j \leq i$ and $x \in vars^1(t)$. Moreover, $x \in \mathsf{X}^1(\mathcal{C})$ implies that for all $(Z, m \vdash^? w) \in D(\mathcal{C})$, $x \in vars^1(w)$ implies that $\mathcal{L}^1_{\mathcal{C}}(Z, m \vdash^? w)$ exists. But by minimality

of $\mathcal{L}^1_{\mathcal{C}_0}(X, i \vdash^? u_0)$, we deduce that $i \leq m$. Hence, we deduce that $\mathcal{L}^1_{\mathcal{C}}(x) = i$. Since we already show that $\mathcal{L}^1_{\mathcal{C}_1}(x) \leq \ell < j \leq i$, we deduce that $\mathcal{L}^1_{\mathcal{C}_1}(x) < \mathcal{L}^1_{\mathcal{C}}(x)$.

Let $(Y, \ell \vdash^? t\sigma) \in D(\mathcal{C}_1)$, let p a position such that $t\sigma|_p \in \mathsf{X}^1(\mathcal{C}_1)$. We distinguish two cases:

- *Case* 1, $t|_p = t\sigma|_p$ *and* $t|_p \notin vars^1(\sigma)$*:* In such a case, it implies that $t|_p \in \mathsf{X}^1(\mathcal{C})$. Furthermore, we deduce that $(\mathcal{L}^1_{\mathcal{C}}(t|_p) = \mathcal{L}^1_{\mathcal{C}_1}(t|_p)$. Hence we have that $\{\{(\mathcal{L}^1_{\mathcal{C}_1}(t|_p), p') \mid (Z, \ell' \vdash^? t') \in D(\mathcal{C}_1) \wedge t'|_{p'} = t|_p\}\} = \{\{(\mathcal{L}^1_{\mathcal{C}}(t|_p), p') \mid (Z, \ell' \vdash^? t') \in D(\mathcal{C}) \wedge t'|_{p'} = t|_p\}\}$
- *Case* 2, $t\sigma|_p \in \mathrm{img}(\sigma)$*:* We have shown that in such a case, $\mathcal{L}^1_{\mathcal{C}_1}(t\sigma|_p) < \mathcal{L}^1_{\mathcal{C}}(t\sigma|_p)$. Since $t\sigma|_p \in vars^1(u)$, we deduce that $\{\{(\mathcal{L}^1_{\mathcal{C}_1}(t\sigma|_p), p') \mid (Z, \ell' \vdash^? t') \in D(\mathcal{C}_1) \wedge t'|_{p'} = t\sigma|_p\}\} < \{\{(\mathcal{L}^1_{\mathcal{C}}(t\sigma|_p), p') \mid (Z, \ell' \vdash^? t') \in D(\mathcal{C}) \wedge t'|_{p'} = t\sigma|_p\}\}$.

Hence we deduce that $\pi_1(\mu_{1.c}(\mathcal{C}_1)) \leq \pi_1(\mu_{1.c}(\mathcal{C}))$ and if $vars^1(u) \cap \mathsf{X}^1(\mathcal{C}) \neq \emptyset$ then $\pi_1(\mu_{1.c}(\mathcal{C}_1)) < \pi_1(\mu_{1.c}(\mathcal{C}))$.

At last, since $D(\mathcal{C}_1) = D(\mathcal{C})\sigma \setminus \{X, i \vdash^? u\sigma\}$ and $E_\Pi(\mathcal{C}_1) = E_\Pi(\mathcal{C}) \wedge X =^? \xi$, we deduce that $\pi_i(\mu_{1.c}(\mathcal{C}_1)) \leq \pi_i(\mu_{1.c}(\mathcal{C}))$, for $i = 2, 3, 4$. Thus we conclude that $\mu_{1.c}(\mathcal{C}_1) \leq \mu_{1.c}(\mathcal{C})$.

Note that $vars^1(u_0) \cap \mathsf{X}^1(\mathcal{C}_0) \neq \emptyset$. Hence we have that $\pi_1(\mu_{1.c}(\mathcal{C}_1)) < \pi_1(\mu_{1.c}(\mathcal{C}_0))$ and so $\mu_{1.c}(\mathcal{C}_1) < \mu_{1.c}(\mathcal{C}_0)$.

We now focus on $\mathcal{C}_2$. In such a case, we have that $D(\mathcal{C}_2) = D(\mathcal{C})$ and $E_\Pi(\mathcal{C}_2) = E_\Pi(\mathcal{C}) \wedge X \neq^? \xi$. Hence we trivially have that $\pi_i(\mu_{1.c}(\mathcal{C}_2)) = \pi_i(\mu_{1.c}(\mathcal{C}))$, for $i = 1, 2, 3$. Furthermore, we also have that $\pi_4(\mu_{1.c}(\mathcal{C}_2)) = \pi_4(\mu_{1.c}(\mathcal{C}))$ if $vars^1(u) \cap \mathsf{X}^1(\mathcal{C}) = \emptyset$, else $\pi_4(\mu_{1.c}(\mathcal{C}_2)) < \pi_4(\mu_{1.c}(\mathcal{C}))$.

We conclude that $\mu_{1.c}(\mathcal{C}_2) \leq \mu_{1.c}(\mathcal{C})$ and since $vars^1(u_0) \cap \mathsf{X}^1(\mathcal{C}_0) \neq \emptyset$, we also conclude that $\mu_{1.c}(\mathcal{C}_2) < \mu_{1.c}(\mathcal{C}_0)$. □

Lemma 63. *Let $(\mathcal{M}, \mathcal{M}')$ be a pair of matrices obtained during the Step c of Phase 1 with parameters s and k. Let* Rule$(\tilde{p})$ *be an instance of a rule which is applicable according to Step c of the strategy and let $(\mathcal{M}_1, \mathcal{M}'_1)$ and $(\mathcal{M}_2, \mathcal{M}'_2)$ be the two pairs of matrices of constraint systems obtained by application of* Rule$(\tilde{p})$ *on $(\mathcal{M}, \mathcal{M}')$ (in case* Rule$(\tilde{p})$ *is* Eq-ded-ded*, there is only one resulting pairsince* Eq-ded-ded *is applied internally). We have that:*

$$\mu^k_{1.c}(\mathcal{M}_1, \mathcal{M}'_1) < \mu^k_{1.c}(\mathcal{M}, \mathcal{M}') \quad \wedge \quad \mu^k_{1.c}(\mathcal{M}_2, \mathcal{M}'_2) < \mu^k_{1.c}(\mathcal{M}, \mathcal{M}')$$

Proof. We prove the result by case analysis on the rule Rule$(\tilde{p})$:

Rule Eq-ded-ded(X, Y)*:* Since this rule is applied internally, there exists $\mathcal{C}$ in the k^{th} column of $(\mathcal{M}, \mathcal{M}')$ such that Eq-ded-ded(X, Y) is strongly applicable on $\mathcal{C}$. Furthermore, we deduce that $X \notin S_2(\mathcal{C})$ and $Y \in S_2(\mathcal{C})$. Assume that $(X, i \vdash^? x) \in D(\mathcal{C})$ and $(Y, j \vdash^? x) \in D(\mathcal{C})$. According to the strong application condition of Eq-ded-ded(X, Y) in case of internal rule for phase 1, we have that $j < i$.

By normalisation, we have that $\mathcal{C}_2 = \bot$ and so we trivially have that $\mu_{1.c}(\mathcal{C}_2) < \mu_{1.c}(\mathcal{C})$.

We focus on $\mathcal{C}_1$: Since $Y \in S_2(\mathcal{C})$ and $x \in \mathcal{X}^1$, we can deduce that $\mathcal{L}^1_{\mathcal{C}}(Y, j \vdash^? x) = (j, 0)$. But $D(\mathcal{C}_1) = D(\mathcal{C}) \setminus \{X, i \vdash^? x\}$.

If there is no $(Z, \ell \vdash^? x) \in D(\mathcal{C})$ such that $Z \neq X$ and $Z \notin S_2(\mathcal{C})$, we have that $x \notin \mathsf{X}^1(\mathcal{C}_1)$. Hence, we can deduce that $\mathcal{L}^1_{\mathcal{C}_1}(Y, j \vdash^? x)$ is not defined and so $\pi_1(\mu_{1.c}(\mathcal{C}_1)) < \pi_1(\mu_{1.c}(\mathcal{C}))$. Thus we deduce that $\mu_{1.c}(\mathcal{C}_1) < \mu_{1.c}(\mathcal{C})$

Else there exists $(Z, \ell \vdash^? x) \in D(\mathcal{C})$ such that $Z \neq X$ and $Z \notin S_2(\mathcal{C})$. Thus $\mathsf{X}^1(\mathcal{C}_1) = \mathsf{X}^1(\mathcal{C})$. Thus, with $D(\mathcal{C}_1) = D(\mathcal{C}) \setminus \{X, i \vdash^? x\}$, we deduce that $\pi_1(\mu_{1.c}(\mathcal{C}_1)) = \pi_1(\mu_{1.c}(\mathcal{C}))$. Furthermore, we $(X, Z) \in \pi_2(\mu_{1.c}(\mathcal{C}))$ while $(X, Z) \notin \pi_2(\mu_{1.c}(\mathcal{C}_1))$. Hence we easily deduce that $\pi_2(\mu_{1.c}(\mathcal{C}_1)) < \pi_2(\mu_{1.c}(\mathcal{C}))$ and so that $\mu_{1.c}(\mathcal{C}_1) < \mu_{1.c}(\mathcal{C})$.

Since we proved that $\mu_{1.c}(\mathcal{C}_1) < \mu_{1.c}(\mathcal{C})$ and $\mu_{1.c}(\mathcal{C}_2) < \mu_{1.c}(\mathcal{C})$ and since the rule is applied internally, we deduce that $\mu^k_{1.c}(\mathcal{M}_1, \mathcal{M}'_1) < \mu^k_{1.c}(\mathcal{M}, \mathcal{M}')$.

Rue $\textsc{Cons}(X, \mathsf{f})$*:* The rule is applied externally. Hence we will show that for all constraint system $\mathcal{C}$ in the k^{th} column, we have that $\mu_{1.c}(\mathcal{C}_1) \leq \mu_{1.c}(\mathcal{C})$ and $\mu_{1.c}(\mathcal{C}_2) \leq \mu_{1.c}(\mathcal{C})$ where $\mathcal{C}_1$ and $\mathcal{C}_2$ are the constraint systems obtained by applying the rule on $\mathcal{C}$. Furthermore, by the definition of the strategy, we know that there exists $\mathcal{C}_0$ such that $\mathcal{L}^1_{\mathcal{C}_0}(X, i_0 \vdash^? u_0)$ is minimal. Thus, we will show that in the case of $\mathcal{C}_0$, $\mu_{1.c}(\mathcal{C}_1) < \mu_{1.c}(\mathcal{C}_0)$ and $\mu_{1.c}(\mathcal{C}_2) < \mu_{1.c}(\mathcal{C}_0)$, where $\mathcal{C}_1$ and $\mathcal{C}_2$ are the constraint systems obtained by applying the rule on $\mathcal{C}_0$.

We first focus on $\mathcal{C}_1$. Thanks to Lemma 61, we know that for all $\mathcal{C}$ in the k^{th} column, for all $i \in \mathbb{N}$, for all term u, $(X, i_0 \vdash^? u) \in D(\mathcal{C})$ and $u \in \mathcal{X}^1$ implies $u \notin \mathsf{X}^1(\mathcal{C})$. We distinguish several cases:

- *Case* $u \in \mathcal{X}^1$*:* By normalisation, $D(\mathcal{C}_1) = (D(\mathcal{C})\{X, i_0 \vdash^? u\})\sigma \cup \{X_j, i_0 \vdash^? x_j\}_{j=1\ldots n}$ where $\sigma = \{u \to \mathsf{f}(x_1, \ldots, x_n)\}$ and x_j are fresh variables and $u \notin \mathsf{X}^1(\mathcal{C})$. Hence we deduce that for all $(Y, j \vdash^? v) \in D(\mathcal{C}_1)$, for all p, if $v|_p \in \mathsf{X}^1(\mathcal{C}_1)$ then $v|_p \in \mathcal{X}^1$, $v|_p = v|_p\sigma$ and $(Y, j \vdash^? v) \in D(\mathcal{C})$. Thus we deduce that $v|_p \in \mathsf{X}^1(\mathcal{C})$ and so $\pi_1(\mu_{1.c}(\mathcal{C}_1)) = \pi_1(\mu_{1.c}(\mathcal{C}))$. Since $X_j \in S_2(\mathcal{C}_1)$, for $j = 1 \ldots n$, we deduce that $\pi_2(\mu_{1.c}(\mathcal{C}_1)) = \pi_2(\mu_{1.c}(\mathcal{C}))$. At last, $x_j \notin \mathsf{X}^1(\mathcal{C}_1)$, for $j = 1 \ldots n$ also implies that $\pi_i(\mu_{1.c}(\mathcal{C}_1)) = \pi_i(\mu_{1.c}(\mathcal{C}))$, for $i = 3, 4$ and so we deduce that $\mu_{1.c}(\mathcal{C}_1) = \mu_{1.c}(\mathcal{C})$.

- *Case* $u \notin \mathcal{X}^1$ *and* $vars^1(u) \cap \mathsf{X}^1(\mathcal{C}) = \emptyset$*:* In such a case, we have that $D(\mathcal{C}_1) = (D(\mathcal{C}) \setminus \{X, i_0 \vdash^? u\}) \cup \{X_j, i_0 \vdash^? x_j\sigma\}_{j=1\ldots n}$ where $x_j\sigma$ is a strict subterm of u, for $j = 1 \ldots n$ and $\sigma = \mathsf{mgu}(u =^? \mathsf{f}(x_1, \ldots, x_n))$. Thus, $vars^1(u) \cap \mathsf{X}^1(\mathcal{C}) = \emptyset$ implies that $vars^1(x_j\sigma) \cap \mathsf{X}^1(\mathcal{C}) = \emptyset$ for $j = 1 \ldots n$. Therefore, we have that $\mathcal{L}^1_{\mathcal{C}_1}(X_j, i_0 \vdash^? x_j\sigma)$ does not exist, for $j = 1 \ldots n$ which implies that $\pi_j(\mu_{1.c}(\mathcal{C}_1)) = \pi_j(\mu_{1.c}(\mathcal{C}))$ for $j = 1, 3, 4$. At last, since $X_j \in S_2(\mathcal{C}_1)$, for $j = 1 \ldots n$, we deduce that $\pi_2(\mu_{1.c}(\mathcal{C}_1)) = \pi_2(\mu_{1.c}(\mathcal{C}))$ and so we conclude that $\mu_{1.c}(\mathcal{C}_1) = \mu_{1.c}(\mathcal{C})$.

- *Case* $u \notin \mathcal{X}^1$ *and* $vars^1(u) \cap \mathsf{X}^1(\mathcal{C}) \neq \emptyset$*:* In such a case, we still have that $D(\mathcal{C}_1) = (D(\mathcal{C}) \setminus \{X, i_0 \vdash^? u\}) \cup \{X_j, i_0 \vdash^? x_j\sigma\}_{j=1\ldots n}$ where $\sigma = \mathsf{mgu}(u, \mathsf{f}(x_1, \ldots, x_n))$. Since $u \notin \mathcal{X}^1$, we can deduce that for all $j \in \{1, \ldots, n\}$, for all p, if $x_j\sigma|_p \in \mathsf{X}^1(\mathcal{C}_1)$ then $u|_{j \cdot p} = x_j\sigma|_p \in \mathsf{X}^1(\mathcal{C})$. With the fact that $\mathcal{L}^1_{\mathcal{C}}(x) = \mathcal{L}^1_{\mathcal{C}_1}(x)$ for all $x \in vars^1(D(\mathcal{C}))$, we can deduce that $(\mathcal{L}^1_{\mathcal{C}_1}(x_j\sigma|_p), p) < (\mathcal{L}^1_{\mathcal{C}}(x_j\sigma|_p), j \cdot p)$, for all $j \in \{1, \ldots, n\}$. Thus we can deduce that $\pi_1(\mu_{1.c}(\mathcal{C}_1)) < \pi_1(\mu_{1.c}(\mathcal{C}))$ and so $\mu_{1.c}(\mathcal{C}_1) < \mu_{1.c}(\mathcal{C})$.

  Note that by the application condition of the rule $\textsc{Cons}(X, \mathsf{f})$ for Step c, we can deduce that $u_0 \notin \mathcal{X}^1$ and $vars^1(u_0) \cap \mathsf{X}^1(\mathcal{C}_0) \neq \emptyset$. Thus we have $\mu_{1.c}(\mathcal{C}_1) < \mu_{1.c}(\mathcal{C}_0)$

We now focus on $\mathcal{C}_2$. In such a case we have that $D(\mathcal{C}_2) = D(\mathcal{C})$. Hence, we trivially have that $\pi_i(\mu_{1.c}(\mathcal{C}_2)) = \pi_i(\mu_{1.c}(\mathcal{C}))$, for $i = 1, 2$. On the other hand, since $E_\Pi(\mathcal{C}_2) = E_\Pi(\mathcal{C}) \wedge \mathsf{root}(X) \neq^? \mathsf{f}$, we have that $\pi_3(\mu_{1.c}(\mathcal{C}_2)) \leq \pi_3(\mu_{1.c}(\mathcal{C}))$ which allows us to conclude that $\mu_{1.c}(\mathcal{C}_2) \leq \mu_{1.c}(\mathcal{C})$.

Note that by the application condition of the rule $\textsc{Cons}(X, \mathsf{f})$ for Step c, we can deduce that $u_0 \notin \mathcal{X}^1$ and $vars^1(u_0) \cap \mathsf{X}^1(\mathcal{C}_0) \neq \emptyset$. Thus we have $\pi_3(\mu_{1.c}(\mathcal{C}_2)) < \pi_3(\mu_{1.c}(\mathcal{C}_0))$ which allows us to conclude that $\mu_{1.c}(\mathcal{C}_2) < \mu_{1.c}(\mathcal{C}_0)$.

Rue $\textsc{Axiom}(X, \mathsf{path})$*:* The rule is applied externally. Hence, similarly to the case of the rule Cons, we will show that for all constraint system $\mathcal{C}$ in the k^{th} column, we have that $\mu_{1.c}(\mathcal{C}_1) \leq \mu_{1.c}(\mathcal{C})$ and $\mu_{1.c}(\mathcal{C}_2) \leq \mu_{1.c}(\mathcal{C})$ where $\mathcal{C}_1$ and $\mathcal{C}_2$ are the constraint systems obtained by applying the rule on $\mathcal{C}$. Furthermore, we will show that in the case of $\mathcal{C}_0$, $\mu_{1.c}(\mathcal{C}_1) < \mu_{1.c}(\mathcal{C}_0)$ and $\mu_{1.c}(\mathcal{C}_2) < \mu_{1.c}(\mathcal{C}_0)$, where $\mathcal{C}_1$ and $\mathcal{C}_2$ are the constraint systems obtained by applying the rule on $\mathcal{C}_0$.

By definition of the rule, we know that there exists $(X, i \vdash^? u) \in D(\mathcal{C})$ and $(\xi, j \vdash^? v) \in \Phi(\mathcal{C})$ such that $j \leq i$.

We first focus on $\mathcal{C}_1$. By definition of the rule, we have that $D(\mathcal{C}_1) = D(\mathcal{C})\sigma \setminus \{X, i \vdash^? u\sigma\}$ where $\sigma = \mathsf{mgu}(u, v)$. Furthermore, we have that $\Phi(\mathcal{C}_1) = \Phi(\mathcal{C})\sigma$.

Let $x \in vars^1(v)$. By the property of origination of a constraint system, we deduce that $\mathcal{L}^1_{\mathcal{C}}(x) < i$. Let $(Y, \ell \vdash^? t) \in D(\mathcal{C})$ such that $x \in vars^1 t$ and $\mathcal{L}^1_{\mathcal{C}}(x) = \ell$. By the minimality of $\mathcal{L}^1_{\mathcal{C}_0}(X, i \vdash^? u_0)$, we deduce that $x \notin \mathsf{X}^1(\mathcal{C})$.

Let $x \in \mathsf{X}^1(\mathcal{C}) \cap vars^1(u)$. If $x \in \mathrm{img}(\sigma)$ then we have that $x \in vars^1(v\sigma)$. But by the property of origination of a constraint system, we deduce that there exists $(Y, \ell \vdash^? t) \in D(\mathcal{C}_1)$ such that $\ell < j \leq i$ and $x \in vars^1(t)$. Moreover, $x \in \mathsf{X}^1(\mathcal{C})$ implies that for all $(Z, m \vdash^? w) \in D(\mathcal{C})$, $x \in vars^1(w)$ implies that $\mathcal{L}^1_{\mathcal{C}}(Z, m \vdash^? w)$ exists. But by minimality of $\mathcal{L}^1_{\mathcal{C}_0}(X, i \vdash^? u_0)$, we deduce that $i \leq m$. Hence, we deduce that $\mathcal{L}^1_{\mathcal{C}}(x) = i$. Since we already show that $\mathcal{L}^1_{\mathcal{C}_1}(x) \leq \ell < j \leq i$, we deduce that $\mathcal{L}^1_{\mathcal{C}_1}(x) < \mathcal{L}^1_{\mathcal{C}}(x)$.

Let $(Y, \ell \vdash^? t\sigma) \in D(\mathcal{C}_1)$, let p a position such that $t\sigma|_p \in \mathsf{X}^1(\mathcal{C}_1)$. We distinguish two cases:

- *Case* 1, $t|_p = t\sigma|_p$ *and* $t|_p \notin vars^1(\sigma)$*:* In such a case, it implies that $t|_p \in \mathsf{X}^1(\mathcal{C})$. Furthermore, we deduce that $(\mathcal{L}^1_{\mathcal{C}}(t|_p) = \mathcal{L}^1_{\mathcal{C}_1}(t|_p)$. Hence we have that $\{\{(\mathcal{L}^1_{\mathcal{C}_1}(t|_p), p') \mid (Z, \ell' \vdash^? t') \in D(\mathcal{C}_1) \wedge t'|_{p'} = t|_p\}\} = \{\{(\mathcal{L}^1_{\mathcal{C}}(t|_p), p') \mid (Z, \ell' \vdash^? t') \in D(\mathcal{C}) \wedge t'|_{p'} = t|_p\}\}$
- *Case* 2, $t\sigma|_p \in \mathrm{img}(\sigma)$*:* We have shown that in such a case, $\mathcal{L}^1_{\mathcal{C}_1}(t\sigma|_p) < \mathcal{L}^1_{\mathcal{C}}(t\sigma|_p)$. Since $t\sigma|_p \in vars^1(u)$, we deduce that $\{\{(\mathcal{L}^1_{\mathcal{C}_1}(t\sigma|_p), p') \mid (Z, \ell' \vdash^? t') \in D(\mathcal{C}_1) \wedge t'|_{p'} = t\sigma|_p\}\} < \{\{(\mathcal{L}^1_{\mathcal{C}}(t\sigma|_p), p') \mid (Z, \ell' \vdash^? t') \in D(\mathcal{C}) \wedge t'|_{p'} = t\sigma|_p\}\}$.

Hence we deduce that $\pi_1(\mu_{1.c}(\mathcal{C}_1)) \leq \pi_1(\mu_{1.c}(\mathcal{C}))$ and if $vars^1(u) \cap \mathsf{X}^1(\mathcal{C}) \neq \emptyset$ then $\pi_1(\mu_{1.c}(\mathcal{C}_1)) < \pi_1(\mu_{1.c}(\mathcal{C}))$.

At last, since $D(\mathcal{C}_1) = D(\mathcal{C})\sigma \setminus \{X, i \vdash^? u\sigma\}$ and $E_\Pi(\mathcal{C}_1) = E_\Pi(\mathcal{C}) \wedge X =^? \xi$, we deduce that $\pi_i(\mu_{1.c}(\mathcal{C}_1)) \leq \pi_i(\mu_{1.c}(\mathcal{C}))$, for $i = 2, 3, 4$. Thus we conclude that $\mu_{1.c}(\mathcal{C}_1) \leq \mu_{1.c}(\mathcal{C})$.

Note that $vars^1(u_0) \cap \mathsf{X}^1(\mathcal{C}_0) \neq \emptyset$. Hence we have that $\pi_1(\mu_{1.c}(\mathcal{C}_1)) < \pi_1(\mu_{1.c}(\mathcal{C}_0))$ and so $\mu_{1.c}(\mathcal{C}_1) < \mu_{1.c}(\mathcal{C}_0)$.

We now focus on $\mathcal{C}_2$. In such a case, we have that $D(\mathcal{C}_2) = D(\mathcal{C})$ and $E_\Pi(\mathcal{C}_2) = E_\Pi(\mathcal{C}) \wedge X \neq^? \xi$. Hence we trivially have that $\pi_i(\mu_{1.c}(\mathcal{C}_2)) = \pi_i(\mu_{1.c}(\mathcal{C}))$, for $i = 1, 2, 3$. Furthermore, we also have that $\pi_4(\mu_{1.c}(\mathcal{C}_2)) = \pi_4(\mu_{1.c}(\mathcal{C}))$ if $vars^1(u) \cap \mathsf{X}^1(\mathcal{C}) = \emptyset$, else $\pi_4(\mu_{1.c}(\mathcal{C}_2)) < \pi_4(\mu_{1.c}(\mathcal{C}))$.

We conclude that $\mu_{1.c}(\mathcal{C}_2) \leq \mu_{1.c}(\mathcal{C})$ and since $vars^1(u_0) \cap \mathsf{X}^1(\mathcal{C}_0) \neq \emptyset$, we also conclude that $\mu_{1.c}(\mathcal{C}_2) < \mu_{1.c}(\mathcal{C}_0)$. □

Lemma 64. *Let $(\mathcal{M}, \mathcal{M}')$ be a pair of matrices obtained during the Step c of Phase 1 with parameters s and k. Let* Rule$(\tilde{p})$ *be an instance of a rule which is applicable according to Step c of the strategy and let $(\mathcal{M}_1, \mathcal{M}'_1)$ and $(\mathcal{M}_2, \mathcal{M}'_2)$ be the two pairs of matrices of constraint systems obtained by application of* Rule$(\tilde{p})$ *on $(\mathcal{M}, \mathcal{M}')$ (in case* Rule$(\tilde{p})$ *is* Eq-ded-ded*, there is only one resulting pairsince* Eq-ded-ded *is applied internally). We have that:*

$$\mu^k_{1.c}(\mathcal{M}_1, \mathcal{M}'_1) < \mu^k_{1.c}(\mathcal{M}, \mathcal{M}') \quad \wedge \quad \mu^k_{1.c}(\mathcal{M}_2, \mathcal{M}'_2) < \mu^k_{1.c}(\mathcal{M}, \mathcal{M}')$$

Proof. We prove the result by case analysis on the rule Rule$(\tilde{p})$:

Rule Eq-ded-ded(X, Y)*:* Since this rule is applied internally, there exists $\mathcal{C}$ in the k^{th} column of $(\mathcal{M}, \mathcal{M}')$ such that Eq-ded-ded(X, Y) is strongly applicable on $\mathcal{C}$. Furthermore, we deduce that $X \notin S_2(\mathcal{C})$ and $Y \in S_2(\mathcal{C})$. Assume that $(X, i \vdash^? x) \in D(\mathcal{C})$ and $(Y, j \vdash^? x) \in D(\mathcal{C})$. According to the strong application condition of Eq-ded-ded(X, Y) in case of internal rule for phase 1, we have that $j < i$.

By normalisation, we have that $\mathcal{C}_2 = \bot$ and so we trivially have that $\mu_{1.c}(\mathcal{C}_2) < \mu_{1.c}(\mathcal{C})$.

We focus on $\mathcal{C}_1$: Since $Y \in S_2(\mathcal{C})$ and $x \in \mathcal{X}^1$, we can deduce that $\mathcal{L}^1_{\mathcal{C}}(Y, j \vdash^? x) = (j, 0)$. But $D(\mathcal{C}_1) = D(\mathcal{C}) \setminus \{X, i \vdash^? x\}$.

If there is no $(Z, \ell \vdash^? x) \in D(\mathcal{C})$ such that $Z \neq X$ and $Z \notin S_2(\mathcal{C})$, we have that $x \notin \mathsf{X}^1(\mathcal{C}_1)$. Hence, we can deduce that $\mathcal{L}^1_{\mathcal{C}_1}(Y, j \vdash^? x)$ is not defined and so $\pi_1(\mu_{1.c}(\mathcal{C}_1)) < \pi_1(\mu_{1.c}(\mathcal{C}))$. Thus we deduce that $\mu_{1.c}(\mathcal{C}_1) < \mu_{1.c}(\mathcal{C})$

Else there exists $(Z, \ell \vdash^? x) \in D(\mathcal{C})$ such that $Z \neq X$ and $Z \notin S_2(\mathcal{C})$. Thus $\mathsf{X}^1(\mathcal{C}_1) = \mathsf{X}^1(\mathcal{C})$. Thus, with $D(\mathcal{C}_1) = D(\mathcal{C}) \setminus \{X, i \vdash^? x\}$, we deduce that $\pi_1(\mu_{1.c}(\mathcal{C}_1)) = \pi_1(\mu_{1.c}(\mathcal{C}))$. Furthermore, we $(X, Z) \in \pi_2(\mu_{1.c}(\mathcal{C}))$ while $(X, Z) \notin \pi_2(\mu_{1.c}(\mathcal{C}_1))$. Hence we easily deduce that $\pi_2(\mu_{1.c}(\mathcal{C}_1)) < \pi_2(\mu_{1.c}(\mathcal{C}))$ and so that $\mu_{1.c}(\mathcal{C}_1) < \mu_{1.c}(\mathcal{C})$.

Since we proved that $\mu_{1.c}(\mathcal{C}_1) < \mu_{1.c}(\mathcal{C})$ and $\mu_{1.c}(\mathcal{C}_2) < \mu_{1.c}(\mathcal{C})$ and since the rule is applied internally, we deduce that $\mu^k_{1.c}(\mathcal{M}_1, \mathcal{M}'_1) < \mu^k_{1.c}(\mathcal{M}, \mathcal{M}')$.

Rue Cons(X, f)*:* The rule is applied externally. Hence we will show that for all constraint system $\mathcal{C}$ in the k^{th} column, we have that $\mu_{1.c}(\mathcal{C}_1) \leq \mu_{1.c}(\mathcal{C})$ and $\mu_{1.c}(\mathcal{C}_2) \leq \mu_{1.c}(\mathcal{C})$ where $\mathcal{C}_1$ and $\mathcal{C}_2$ are the constraint systems obtained by applying the rule on $\mathcal{C}$. Furthermore, by the definition of the strategy, we know that there exists $\mathcal{C}_0$ such that $\mathcal{L}^1_{\mathcal{C}_0}(X, i_0 \vdash^? u_0)$ is minimal. Thus, we will show that in the case of $\mathcal{C}_0$, $\mu_{1.c}(\mathcal{C}_1) < \mu_{1.c}(\mathcal{C}_0)$ and $\mu_{1.c}(\mathcal{C}_2) < \mu_{1.c}(\mathcal{C}_0)$, where $\mathcal{C}_1$ and $\mathcal{C}_2$ are the constraint systems obtained by applying the rule on $\mathcal{C}_0$.

We first focus on $\mathcal{C}_1$. Thanks to Lemma 61, we know that for all $\mathcal{C}$ in the k^{th} column, for all $i \in \mathbb{N}$, for all term u, $(X, i_0 \vdash^? u) \in D(\mathcal{C})$ and $u \in \mathcal{X}^1$ implies $u \notin \mathsf{X}^1(\mathcal{C})$. We distinguish several cases:

- *Case $u \in \mathcal{X}^1$:* By normalisation, $D(\mathcal{C}_1) = (D(\mathcal{C})\{X, i_0 \vdash^? u\})\sigma \cup \{X_j, i_0 \vdash^? x_j\}_{j=1\ldots n}$ where $\sigma = \{u \to \mathsf{f}(x_1, \ldots, x_n)\}$ and x_j are fresh variables and $u \notin \mathsf{X}^1(\mathcal{C})$. Hence we deduce that for all $(Y, j \vdash^? v) \in D(\mathcal{C}_1)$, for all p, if $v|_p \in \mathsf{X}^1(\mathcal{C}_1)$ then $v|_p \in \mathcal{X}^1$, $v|_p = v|_p\sigma$ and $(Y, j \vdash^? v) \in D(\mathcal{C})$. Thus we deduce that $v|_p \in \mathsf{X}^1(\mathcal{C})$ and so $\pi_1(\mu_{1.c}(\mathcal{C}_1)) = \pi_1(\mu_{1.c}(\mathcal{C}))$. Since $X_j \in S_2(\mathcal{C}_1)$, for $j = 1 \ldots n$, we deduce that $\pi_2(\mu_{1.c}(\mathcal{C}_1)) = \pi_2(\mu_{1.c}(\mathcal{C}))$. At last, $x_j \notin \mathsf{X}^1(\mathcal{C}_1)$, for $j = 1 \ldots n$ also implies that $\pi_i(\mu_{1.c}(\mathcal{C}_1)) = \pi_i(\mu_{1.c}(\mathcal{C}))$, for $i = 3, 4$ and so we deduce that $\mu_{1.c}(\mathcal{C}_1) = \mu_{1.c}(\mathcal{C})$.

- *Case $u \notin \mathcal{X}^1$ and $vars^1(u) \cap \mathsf{X}^1(\mathcal{C}) = \emptyset$:* In such a case, we have that $D(\mathcal{C}_1) = (D(\mathcal{C}) \setminus \{X, i_0 \vdash^? u\}) \cup \{X_j, i_0 \vdash^? x_j\sigma\}_{j=1\ldots n}$ where $x_j\sigma$ is a strict subterm of u, for $j = 1 \ldots n$ and $\sigma = \mathsf{mgu}(u =^? \mathsf{f}(x_1, \ldots, x_n))$. Thus, $vars^1(u) \cap \mathsf{X}^1(\mathcal{C}) = \emptyset$ implies that $vars^1(x_j\sigma) \cap \mathsf{X}^1(\mathcal{C}) = \emptyset$ for $j = 1 \ldots n$. Therefore, we have that $\mathcal{L}^1_{\mathcal{C}_1}(X_j, i_0 \vdash^? x_j\sigma)$ does not exist, for $j = 1 \ldots n$ which implies that $\pi_j(\mu_{1.c}(\mathcal{C}_1)) = \pi_j(\mu_{1.c}(\mathcal{C}))$ for $j = 1, 3, 4$. At last, since $X_j \in S_2(\mathcal{C}_1)$, for $j = 1 \ldots n$, we deduce that $\pi_2(\mu_{1.c}(\mathcal{C}_1)) = \pi_2(\mu_{1.c}(\mathcal{C}))$ and so we conclude that $\mu_{1.c}(\mathcal{C}_1) = \mu_{1.c}(\mathcal{C})$.

- *Case $u \notin \mathcal{X}^1$ and $vars^1(u) \cap \mathsf{X}^1(\mathcal{C}) \neq \emptyset$:* In such a case, we still have that $D(\mathcal{C}_1) = (D(\mathcal{C}) \setminus \{X, i_0 \vdash^? u\}) \cup \{X_j, i_0 \vdash^? x_j\sigma\}_{j=1\ldots n}$ where $\sigma = \mathsf{mgu}(u, \mathsf{f}(x_1, \ldots, x_n))$. Since $u \notin \mathcal{X}^1$, we can deduce that for all $j \in \{1, \ldots, n\}$, for all p, if $x_j\sigma|_p \in \mathsf{X}^1(\mathcal{C}_1)$ then $u|_{j \cdot p} = x_j\sigma|_p \in \mathsf{X}^1(\mathcal{C})$. With the fact that $\mathcal{L}^1_{\mathcal{C}}(x) = \mathcal{L}^1_{\mathcal{C}_1}(x)$ for all $x \in vars^1(D(\mathcal{C}))$, we can deduce that $(\mathcal{L}^1_{\mathcal{C}_1}(x_j\sigma|_p), p) < (\mathcal{L}^1_{\mathcal{C}}(x_j\sigma|_p), j \cdot p)$, for all $j \in \{1, \ldots, n\}$. Thus we can deduce that $\pi_1(\mu_{1.c}(\mathcal{C}_1)) < \pi_1(\mu_{1.c}(\mathcal{C}))$ and so $\mu_{1.c}(\mathcal{C}_1) < \mu_{1.c}(\mathcal{C})$.

  Note that by the application condition of the rule $\textsc{Cons}(X, \mathsf{f})$ for Step c, we can deduce that $u_0 \notin \mathcal{X}^1$ and $vars^1(u_0) \cap \mathsf{X}^1(\mathcal{C}_0) \neq \emptyset$. Thus we have $\mu_{1.c}(\mathcal{C}_1) < \mu_{1.c}(\mathcal{C}_0)$

We now focus on $\mathcal{C}_2$. In such a case we have that $D(\mathcal{C}_2) = D(\mathcal{C})$. Hence, we trivially have that $\pi_i(\mu_{1.c}(\mathcal{C}_2)) = \pi_i(\mu_{1.c}(\mathcal{C}))$, for $i = 1, 2$. On the other hand, since $E_\Pi(\mathcal{C}_2) = E_\Pi(\mathcal{C}) \wedge \mathsf{root}(X) \neq^? \mathsf{f}$, we have that $\pi_3(\mu_{1.c}(\mathcal{C}_2)) \leq \pi_3(\mu_{1.c}(\mathcal{C}))$ which allows us to conclude that $\mu_{1.c}(\mathcal{C}_2) \leq \mu_{1.c}(\mathcal{C})$.

Note that by the application condition of the rule $\textsc{Cons}(X, \mathsf{f})$ for Step c, we can deduce that $u_0 \notin \mathcal{X}^1$ and $vars^1(u_0) \cap \mathsf{X}^1(\mathcal{C}_0) \neq \emptyset$. Thus we have $\pi_3(\mu_{1.c}(\mathcal{C}_2)) < \pi_3(\mu_{1.c}(\mathcal{C}_0))$ which allows us to conclude that $\mu_{1.c}(\mathcal{C}_2) < \mu_{1.c}(\mathcal{C}_0)$.

Rue $\textsc{Axiom}(X, \mathsf{path})$*:* The rule is applied externally. Hence, similarly to the case of the rule Cons, we will show that for all constraint system $\mathcal{C}$ in the k^{th} column, we have that $\mu_{1.c}(\mathcal{C}_1) \leq \mu_{1.c}(\mathcal{C})$ and $\mu_{1.c}(\mathcal{C}_2) \leq \mu_{1.c}(\mathcal{C})$ where $\mathcal{C}_1$ and $\mathcal{C}_2$ are the constraint systems obtained by applying the rule on $\mathcal{C}$. Furthermore, we will show that in the case of $\mathcal{C}_0$, $\mu_{1.c}(\mathcal{C}_1) < \mu_{1.c}(\mathcal{C}_0)$ and $\mu_{1.c}(\mathcal{C}_2) < \mu_{1.c}(\mathcal{C}_0)$, where $\mathcal{C}_1$ and $\mathcal{C}_2$ are the constraint systems obtained by applying the rule on $\mathcal{C}_0$.

By definition of the rule, we know that there exists $(X, i \vdash^? u) \in D(\mathcal{C})$ and $(\xi, j \vdash^? v) \in \Phi(\mathcal{C})$ such that $j \leq i$.

We first focus on $\mathcal{C}_1$. By definition of the rule, we have that $D(\mathcal{C}_1) = D(\mathcal{C})\sigma \setminus \{X, i \vdash^? u\sigma\}$ where $\sigma = \mathsf{mgu}(u, v)$. Furthermore, we have that $\Phi(\mathcal{C}_1) = \Phi(\mathcal{C})\sigma$.

Let $x \in vars^1(v)$. By the property of origination of a constraint system, we deduce that $\mathcal{L}^1_{\mathcal{C}}(x) < i$. Let $(Y, \ell \vdash^? t) \in D(\mathcal{C})$ such that $x \in vars^1 t$ and $\mathcal{L}^1_{\mathcal{C}}(x) = \ell$. By the minimality of $\mathcal{L}^1_{\mathcal{C}_0}(X, i \vdash^? u_0)$, we deduce that $x \notin \mathsf{X}^1(\mathcal{C})$.

Let $x \in \mathsf{X}^1(\mathcal{C}) \cap vars^1(u)$. If $x \in \mathrm{img}(\sigma)$ then we have that $x \in vars^1(v\sigma)$. But by the property of origination of a constraint system, we deduce that there exists $(Y, \ell \vdash^? t) \in D(\mathcal{C}_1)$ such that $\ell < j \leq i$ and $x \in vars^1(t)$. Moreover, $x \in \mathsf{X}^1(\mathcal{C})$ implies that for all $(Z, m \vdash^? w) \in D(\mathcal{C})$, $x \in vars^1(w)$ implies that $\mathcal{L}^1_{\mathcal{C}}(Z, m \vdash^? w)$ exists. But by minimality of $\mathcal{L}^1_{\mathcal{C}_0}(X, i \vdash^? u_0)$, we deduce that $i \leq m$. Hence, we deduce that $\mathcal{L}^1_{\mathcal{C}}(x) = i$. Since we already show that $\mathcal{L}^1_{\mathcal{C}_1}(x) \leq \ell < j \leq i$, we deduce that $\mathcal{L}^1_{\mathcal{C}_1}(x) < \mathcal{L}^1_{\mathcal{C}}(x)$.

Let $(Y, \ell \vdash^? t\sigma) \in D(\mathcal{C}_1)$, let p a position such that $t\sigma|_p \in \mathsf{X}^1(\mathcal{C}_1)$. We distinguish two cases:

- *Case* 1, $t|_p = t\sigma|_p$ *and* $t|_p \notin vars^1(\sigma)$*:* In such a case, it implies that $t|_p \in \mathsf{X}^1(\mathcal{C})$. Furthermore, we deduce that $(\mathcal{L}^1_{\mathcal{C}}(t|_p) = \mathcal{L}^1_{\mathcal{C}_1}(t|_p)$. Hence we have that $\{\{(\mathcal{L}^1_{\mathcal{C}_1}(t|_p), p') \mid (Z, \ell' \vdash^? t') \in D(\mathcal{C}_1) \wedge t'|_{p'} = t|_p\}\} = \{\{(\mathcal{L}^1_{\mathcal{C}}(t|_p), p') \mid (Z, \ell' \vdash^? t') \in D(\mathcal{C}) \wedge t'|_{p'} = t|_p\}\}$
- *Case* 2, $t\sigma|_p \in \mathrm{img}(\sigma)$*:* We have shown that in such a case, $\mathcal{L}^1_{\mathcal{C}_1}(t\sigma|_p) < \mathcal{L}^1_{\mathcal{C}}(t\sigma|_p)$. Since $t\sigma|_p \in vars^1(u)$, we deduce that $\{\{(\mathcal{L}^1_{\mathcal{C}_1}(t\sigma|_p), p') \mid (Z, \ell' \vdash^? t') \in D(\mathcal{C}_1) \wedge t'|_{p'} = t\sigma|_p\}\} < \{\{(\mathcal{L}^1_{\mathcal{C}}(t\sigma|_p), p') \mid (Z, \ell' \vdash^? t') \in D(\mathcal{C}) \wedge t'|_{p'} = t\sigma|_p\}\}$.

Hence we deduce that $\pi_1(\mu_{1.c}(\mathcal{C}_1)) \leq \pi_1(\mu_{1.c}(\mathcal{C}))$ and if $vars^1(u) \cap \mathsf{X}^1(\mathcal{C}) \neq \emptyset$ then $\pi_1(\mu_{1.c}(\mathcal{C}_1)) < \pi_1(\mu_{1.c}(\mathcal{C}))$.

At last, since $D(\mathcal{C}_1) = D(\mathcal{C})\sigma \setminus \{X, i \vdash^? u\sigma\}$ and $E_\Pi(\mathcal{C}_1) = E_\Pi(\mathcal{C}) \wedge X =^? \xi$, we deduce that $\pi_i(\mu_{1.c}(\mathcal{C}_1)) \leq \pi_i(\mu_{1.c}(\mathcal{C}))$, for $i = 2, 3, 4$. Thus we conclude that $\mu_{1.c}(\mathcal{C}_1) \leq \mu_{1.c}(\mathcal{C})$.

Note that $vars^1(u_0) \cap \mathsf{X}^1(\mathcal{C}_0) \neq \emptyset$. Hence we have that $\pi_1(\mu_{1.c}(\mathcal{C}_1)) < \pi_1(\mu_{1.c}(\mathcal{C}_0))$ and so $\mu_{1.c}(\mathcal{C}_1) < \mu_{1.c}(\mathcal{C}_0)$.

We now focus on $\mathcal{C}_2$. In such a case, we have that $D(\mathcal{C}_2) = D(\mathcal{C})$ and $E_\Pi(\mathcal{C}_2) = E_\Pi(\mathcal{C}) \wedge X \neq^? \xi$. Hence we trivially have that $\pi_i(\mu_{1.c}(\mathcal{C}_2)) = \pi_i(\mu_{1.c}(\mathcal{C}))$, for $i = 1, 2, 3$. Furthermore, we also have that $\pi_4(\mu_{1.c}(\mathcal{C}_2)) = \pi_4(\mu_{1.c}(\mathcal{C}))$ if $vars^1(u) \cap \mathsf{X}^1(\mathcal{C}) = \emptyset$, else $\pi_4(\mu_{1.c}(\mathcal{C}_2)) < \pi_4(\mu_{1.c}(\mathcal{C}))$.

We conclude that $\mu_{1.c}(\mathcal{C}_2) \leq \mu_{1.c}(\mathcal{C})$ and since $vars^1(u_0) \cap \mathsf{X}^1(\mathcal{C}_0) \neq \emptyset$, we also conclude that $\mu_{1.c}(\mathcal{C}_2) < \mu_{1.c}(\mathcal{C}_0)$. □

Steps b and c together. We have already shown that Step b and Step c terminate. We now have to establish termination of Steps b and c together. For this purpose, we define a measure on pair of matrices using $\mathcal{L}^1_{\mathcal{C}}(\cdot)$. Let $(\mathcal{M}, \mathcal{M}')$ be a pair of matrices of constraint systems. Assume w.l.o.g. that the parameter k corresponds to a column oin $\mathcal{M}$. We define a measure, denoted $\mu^k_{1.b+c}(\mathcal{M}, \mathcal{M}')$, such that:

$$\mu^k_{1.b+c}(\mathcal{M}, \mathcal{M}') = \max \left\{ \mathcal{L}^1_{\mathcal{C}}(u) \;\middle|\; \begin{array}{l} i \in \mathbb{N}, X \notin S_2, (X, j \vdash^? u) \in D(\mathcal{C}) \text{ and } \mathcal{C} \text{ is} \\ \text{on the } i^{\text{th}} \text{ line and } k^{\text{th}} \text{ column of } (\mathcal{M}, \mathcal{M}') \end{array} \right\}$$

We will first show that $\mu^k_{1.b+c}(\mathcal{M}, \mathcal{M}')$ can not increase during Step b and Step c.Moreover, the strategy of Step c will allow us to show that between the beginning of Step c and the end of Step c, the measure strictly decreases. Indeed, at the beginning of Step c, every internal deducibility constraints contain only variable as right hand term. Furthermore, we know that these deducibility constraints can either be removed thanks to Eq-ded-ded or either be instantiated by the application of Axiom. But the choice of the rule and its parameters are determined by minimizing $\mathcal{L}^1_{\cdot}(\cdot)$. Hence, in the case of the rule Axiom, we always instantiate a variable x by a term that can only contain variables appearing strictly at an earlier stage in the constraint system.

Lemma 65. *Let $\mathcal{C}$ be a well-formed constraint system. Let* Rule($\tilde{p}$) *be an instance of one of the following rule :* Cons, Axiom *or* Eq-ded-ded*. Let $\mathcal{C}_1, \mathcal{C}_2$ be the two constraint systems obtained by application of* Rule($\tilde{p}$) *on $\mathcal{C}$. For all $i \in \{1, 2\}$, for all $u \in \mathcal{T}(\mathcal{F}_c, \mathcal{N} \cup \mathcal{X}^1)$, if $vars^1(u) \subseteq vars^1(D(\mathcal{C}))$ then $\mathcal{L}^1_{\mathcal{C}_i}(u\sigma_i) \leq \mathcal{L}^1_{\mathcal{C}}(u)$ where $\sigma_i = \mathsf{mgu}(E(\mathcal{C}_i))$.*

Proof. We do a case analysis on the rule. Note that, according to the definition of the rule in Figures 1 and 2, we have that $\mathsf{mgu}(E(\mathcal{C}_2)) = \mathsf{mgu}(E(\mathcal{C}))$ and $D(\mathcal{C}_2) = D(\mathcal{C})$ for all the rules that we will consider here. Hence, we have that $u\sigma_2 = u$ and $\mathcal{L}^1_{\mathcal{C}_2}(u) = \mathcal{L}^1_{\mathcal{C}}(u)$. Thus the result holds for $i = 2$.

Rule Cons(X, f)*:* Let $(X, i \vdash^? t) \in D(\mathcal{C})$. According to Figure 1, we have that $D(\mathcal{C}_1) = (D(\mathcal{C})\sigma \setminus \{X, i \vdash^? t\sigma\}) \cup \{X_k, i \vdash^? x_k\}_{k=1..n}$, where x_k, X_k are fresh variables for $k = 1 \dots n$ and $\sigma = \mathsf{mgu}(t, \mathsf{f}(x_1, \dots, x_n))$.

In case $t \notin \mathcal{X}^1$, we have that $\mathrm{dom}(\sigma) = \{x_1, \dots, x_n\}$, $D(\mathcal{C})\sigma = D(\mathcal{C})$ and $vars^1(D(\mathcal{C})) = vars^1(D(\mathcal{C}_1))$. Hence we deduce that $u\sigma_1 = u$ and $\mathcal{L}^1_{\mathcal{C}_1}(u) = \mathcal{L}^1_{\mathcal{C}}(u)$ and so $\mathcal{L}^1_{\mathcal{C}_1}(u\sigma_1) = \mathcal{L}^1_{\mathcal{C}}(u)$.

Otherwise, we have that $t \in \mathcal{X}^1$. In such a case, $\sigma = \{t \mapsto \mathsf{f}(x_1, \dots, x_n)\}$. For all $x \in vars^1(D(C_1)) \setminus \{x_1, \dots, x_n\}$, $\mathcal{L}^1_{\mathcal{C}_1}(x) = \mathcal{L}^1_{\mathcal{C}}(x)$. Assume now that $\mathcal{L}^1_{\mathcal{C}}(t) < i$ thus there exists $(Y, j \vdash^? v) \in D(\mathcal{C})$ such that $t \in vars^1(v)$ and $\mathcal{L}^1_{\mathcal{C}}(t) = j$. But it implies that $(Y, j \vdash^? v\sigma) \in D(\mathcal{C}_1)$. On the other hand, if $\mathcal{L}^1_{\mathcal{C}}(t) = i$ we know that $\{X_k, i \vdash^? x_k\}_{k=1..n} \subseteq D(\mathcal{C}_1)$. Hence we deduce that for all $k \in \{1, \dots, n\}$, $\mathcal{L}^1_{\mathcal{C}_1}(x_k) = \mathcal{L}^1_{\mathcal{C}}(t)$.

Since $\mathcal{L}^1_{\mathcal{C}}(u) = \max\{\mathcal{L}^1_{\mathcal{C}}(x) \mid x \in vars^1(u)\}$, we deduce that $\mathcal{L}^1_{\mathcal{C}}(u) = \mathcal{L}^1_{\mathcal{C}_1}(u\sigma_1)$. Thus the result holds.

Rule Axiom(X, path)*:* Let $(X, i \vdash^? t) \in D(\mathcal{C})$ and $(\xi, j \rhd v) \in \Phi(\mathcal{C})$ such that $\mathsf{path}(\xi) = \mathsf{path}$. According to Figure 1, we have that $D(\mathcal{C}_1) = (D(\mathcal{C})\sigma \setminus \{X, i \vdash^? t\sigma\})$ were $\sigma = \mathsf{mgu}(t, v)$.

For all $x \notin vars^1(t, v)$, we have that $x\sigma = x$ and since $D(\mathcal{C}_1) = (D(\mathcal{C})\sigma \setminus \{X, i \vdash^? t\sigma\})$, we can deduce that $\mathcal{L}^1_{\mathcal{C}_1}(x) = \mathcal{L}^1_{\mathcal{C}}(x)$.

Let $x \in \mathrm{dom}(\sigma)$. We show that for all $y \in vars^1(x\sigma)$, $\mathcal{L}^1_{\mathcal{C}_1}(y) \leq \mathcal{L}^1_{\mathcal{C}}(x)$. If $\mathcal{L}^1_{\mathcal{C}}(x) = \ell$ then it implies that there exists $(Y, \ell \vdash^? w) \in D(\mathcal{C})$ such that $x \in vars^1(w)$. If $X \neq Y$ then we have that $(Y, \ell \vdash^? w\sigma) \in D(\mathcal{C}_1)$ and since $y \in vars^1(w\sigma)$, we can deduce that $\mathcal{L}^1_{\mathcal{C}_1}(y) \leq \mathcal{L}^1_{\mathcal{C}}(x)$. Else if $X = Y$ then it implies that $x \in vars^1(t)$. But $\Phi(\mathcal{C}_1) = \Phi(\mathcal{C})$ which implies that $(\xi, j \rhd v\sigma) \in \Phi(\mathcal{C}_1)$. Thus, by the origination property of a constraint system, we can deduce that $y \in vars^1(v\sigma)$ implies that there exists $(Z, p \vdash^? w') \in D(\mathcal{C}_1)$ such that $p < j$ and $y \in vars^1(w')$. Hence we deduce that $\mathcal{L}^1_{\mathcal{C}_1}(y) \leq p < j \leq \mathcal{L}^1_{\mathcal{C}}(x)$. Hence the result holds.

Let $x \in vars^1(\mathrm{img}(\sigma))$. If $\mathcal{L}^1_{\mathcal{C}}(x) < i$ then since $D(\mathcal{C}_1) = (D(\mathcal{C})\sigma \setminus \{X, i \vdash^? t\sigma\})$, we deduce that $\mathcal{L}^1_{\mathcal{C}_1}(x) \leq \mathcal{L}^1_{\mathcal{C}}(x)$. Else $\mathcal{L}^1_{\mathcal{C}}(x) = i$. But since $x \in vars^1(v\sigma)$, the by the properties of origination, we deduce that $\mathcal{L}^1_{\mathcal{C}_1}(x) < \mathcal{L}^1_{\mathcal{C}}(x)$.

We proved that for all $x \in vars^1(u)$, we have that $\mathcal{L}^1_{\mathcal{C}_1}(x\sigma) \leq \mathcal{L}^1_{\mathcal{C}}(x)$. Thus we conclude that $\mathcal{L}^1_{\mathcal{C}_1}(u\sigma) \leq \mathcal{L}^1_{\mathcal{C}}(u)$.

Rule Eq-ded-ded(X, Y)*:* Let $(X, i_1 \vdash^? v_1) \in D(\mathcal{C})$ and $(Y, i_2 \vdash^? v_2) \in D(\mathcal{C})$ such that $i_1 \geq i_2$. According to Figure 2, we have that $D(\mathcal{C}_1) = (D(\mathcal{C})\sigma \setminus \{X, i_1 \vdash^? v_1\sigma\})$ where $\sigma = \mathsf{mgu}(v_1, v_2)$.

For all $x \notin vars^1(v_1, v_2)$, we have that $x\sigma = x$ thus we can deduce that $\mathcal{L}^1_{\mathcal{C}_1}(x) = \mathcal{L}^1_{\mathcal{C}}(x)$.

Let $x \in \mathrm{dom}(\sigma)$. Let $y \in vars^1(x\sigma)$. If $\mathcal{L}^1_{\mathcal{C}}(x) = \ell$ then it implies that there exists $(Z, \ell \vdash^? w) \in D(\mathcal{C})$ such that $x \in vars^1(w)$. If $X \neq Z$ then we have that $(Z, \ell \vdash^? w\sigma) \in D(\mathcal{C}_1)$ and since $y \in vars^1(w\sigma)$, we can deduce that $\mathcal{L}^1_{\mathcal{C}_1}(y) \leq \mathcal{L}^1_{\mathcal{C}}(x)$. Else if $X = Z$ then it implies that $x \in vars^1(v_1)$. But $(Y, i_2 \vdash^? v_2\sigma) \in D(\mathcal{C}_1)$ and $y \in vars^1(v_2\sigma)$. Hence we have that $\mathcal{L}^1_{\mathcal{C}_1}(y) \leq i_2 \leq i_1 = \mathcal{L}^1_{\mathcal{C}}(x)$.

Let $x \in vars^1(\mathrm{img}(\sigma))$. If $\mathcal{L}^1_{\mathcal{C}}(x) < i_1$ then since $D(\mathcal{C}_1) = (D(\mathcal{C})\sigma \setminus \{X, i_1 \vdash^? v_1\sigma\})$, we deduce that $\mathcal{L}^1_{\mathcal{C}_1}(x) \leq \mathcal{L}^1_{\mathcal{C}}(x)$. Else $\mathcal{L}^1_{\mathcal{C}}(x) = i_1$. But since $x \in vars^1(v_2\sigma)$ and $(Y, i_2 \vdash^? v_2\sigma) \in D(\mathcal{C}_1)$, we deduce that $\mathcal{L}^1_{\mathcal{C}_1}(x) \leq i_2 \leq i_1 = \mathcal{L}^1_{\mathcal{C}}(x)$.

We proved that for all $x \in vars^1(u)$, we have that $\mathcal{L}^1_{\mathcal{C}_1}(x\sigma) \leq \mathcal{L}^1_{\mathcal{C}}(x)$. Thus we conclude that $\mathcal{L}^1_{\mathcal{C}_1}(u\sigma) \leq \mathcal{L}^1_{\mathcal{C}}(u)$. □

Lemma 66. *Let $(\mathcal{M}, \mathcal{M}')$ be a pair of matrices obtained at the end of the Step c of Phase 1 of the strategy with parameters s and k. Let $(\mathcal{M}_1, \mathcal{M}'_1)$ be a pair of matrices obtained by application on $(\mathcal{M}, \mathcal{M}')$ of Steps b and c with the same parameters. $\mu^k_{1.b+c}(\mathcal{M}_1, \mathcal{M}'_1) < \mu^k_{1.b+c}(\mathcal{M}, \mathcal{M}')$.*

Proof. Since $(\mathcal{M}, \mathcal{M}')$ and $(\mathcal{M}_1, \mathcal{M}'_1)$ are both obtained at two consecutive end of step c of phase 1, there exists $(\mathcal{M}_2, \mathcal{M}'_2)$ such that $(\mathcal{M}, \mathcal{M}') \to^* (\mathcal{M}_2, \mathcal{M}'_2) \to^* (\mathcal{M}_1, \mathcal{M}'_1)$ and $(\mathcal{M}_2, \mathcal{M}'_2)$ is obtained at the end of Step b of Phase 1. The proof of this result is divided in two parts. We first show that $\mu^k_{1.b+c}(\mathcal{M}_2, \mathcal{M}'_2) \leq \mu^k_{1.b+c}(\mathcal{M}, \mathcal{M}')$. Secondly we show that $\mu^k_{1.b+c}(\mathcal{M}_1, \mathcal{M}'_1) < \mu^k_{1.b+c}(\mathcal{M}_2, \mathcal{M}'_2)$.

First part, $\mu^k_{1.b+c}(\mathcal{M}_2, \mathcal{M}'_2) \leq \mu^k_{1.b+c}(\mathcal{M}, \mathcal{M}')$: All the rules applied during Step b are internal rules. Furthermore, we know that $(\mathcal{M}, \mathcal{M}')$ was obtained at the end of step c which means that we already apply at leaf one Step b before obtaining $(\mathcal{M}, \mathcal{M}')$. Hence, the rules Ded-st and Eq-frame-frame are useless on $(\mathcal{M}, \mathcal{M}')$ for the support s and the column k. Thus the only rules that are applied between $(\mathcal{M}, \mathcal{M}')$ and $(\mathcal{M}_2, \mathcal{M}'_2)$ are Cons, Eq-ded-ded and Axiom.

Consider two pair of matrices $(\mathcal{M}_3, \mathcal{M}'_3)$ and $(\mathcal{M}_4, \mathcal{M}'_4)$ such that $(\mathcal{M}, \mathcal{M}') \to^* (\mathcal{M}_4, \mathcal{M}'_4) \to (\mathcal{M}_3, \mathcal{M}'_3) \to^* (\mathcal{M}_2, \mathcal{M}'_2)$ and assume that $\textsc{Rule}(\tilde{p})$ is the rule applied on $(\mathcal{M}_4, \mathcal{M}'_4)$. Let $\mathcal{C}$ be a constraint system in the k^{th} column of $(\mathcal{M}_4, \mathcal{M}'_4)$. If the rule $\textsc{Rule}(\tilde{p})$ was not applied on $\mathcal{C}$ then $\mathcal{C}$ is in the k^{th} column on $(\mathcal{M}_3, \mathcal{M}'_3)$. If the rule $\textsc{Rule}(\tilde{p})$ was applied on $\mathcal{C}$ then there exists $\mathcal{C}_1$ and $\mathcal{C}_2$ such that $\mathcal{C}_1$ and $\mathcal{C}_2$ both in the k^{th} column of $(\mathcal{M}_3, \mathcal{M}'_3)$ and they are the two constraint systems obtained by applying $\textsc{Rule}(\tilde{p})$ on $\mathcal{C}$.

According to Figure 1 and 2, and the normalisation rules 3, for all $i \in \{1, 2\}$, for all $(X, i \vdash^? u) \in D(\mathcal{C}_i)$, there exists $(Y, i \vdash^? v) \in D(\mathcal{C})$ and $v' \in st(v)$ such that $v'\mathsf{mgu}(E(\mathcal{C}_i)) = u$. But thanks to Lemma 65, $\mathcal{L}^1_{\mathcal{C}_i}(v'\mathsf{mgu}(E(\mathcal{C}_i))) \leq \mathcal{L}^1_{\mathcal{C}}(v')$ and so $\mathcal{L}^1_{\mathcal{C}_i}(u) \leq \mathcal{L}^1_{\mathcal{C}}(v')$. Since $v' \in st(v)$, we deduce that $\mathcal{L}^1_{\mathcal{C}_i}(u) \leq \mathcal{L}^1_{\mathcal{C}}(v)$. This allows us to deduce that $\max\{\mathcal{L}^1_{\mathcal{C}_i}(u) \mid X \notin S_2(\mathcal{C}_i), (X, j \vdash^? u) \in D(\mathcal{C}_i)\} \leq \max\{\mathcal{L}^1_{\mathcal{C}}(u) \mid X \notin S_2(\mathcal{C}), (X, j \vdash^? u) \in D(\mathcal{C})\}$. Hence we deduce that $\mu^k_{1.b+c}(\mathcal{M}_3, \mathcal{M}'_3) \leq \mu^k_{1.b+c}(\mathcal{M}_4, \mathcal{M}'_4)$. With a simple induction, we can conclude that $\mu^k_{1.b+c}(\mathcal{M}_2, \mathcal{M}'_2) \leq \mu^k_{1.b+c}(\mathcal{M}, \mathcal{M}')$.

Second part, $\mu^k_{1.b+c}(\mathcal{M}_1, \mathcal{M}'_1) < \mu^k_{1.b+c}(\mathcal{M}_2, \mathcal{M}'_2)$: Let $\mathcal{C}_1$ be a constraint system in the k^{th} column of $(\mathcal{M}_1, \mathcal{M}'_1)$. Let $\mathcal{C}_2$ be the constraint system ancestor of $\mathcal{C}_1$ such that $\mathcal{C}_2$ is in $(\mathcal{M}_2, \mathcal{M}'_2)$.

Thanks to Lemma 27, we know that $(\mathcal{M}_1, \mathcal{M}'_1)$ satisfies $\mathsf{PP1ScE}(s, k)$, and $(\mathcal{M}_2, \mathcal{M}'_2)$ satisfies $\mathsf{PP1SbE}(s, k)$. Thus we deduce that for all $(X, i \vdash^? u) \in D(\mathcal{C}_1)$, if $X \notin S_2(\mathcal{C}_1)$, then $u \notin \mathcal{X}^1$ and $i = s$. Furthermore, we deduce that for all $(X, i \vdash^? u) \in D(\mathcal{C}_2)$, if $X \notin S_2(\mathcal{C}_2)$, then $u \in \mathcal{X}^1$ and $i = s$. But the rules applied during step c either remove internal deducibility constraint by Eq-ded-ded or instantiate them by Axiom or Cons. Thus, for all $(X, s \vdash^? t_1) \in D(\mathcal{C}_1)$, if $X \notin S_2(\mathcal{C}_1)$, then there exists t_2 such that $(X, s \vdash^? t_2) \in D(\mathcal{C}_2)$.

Let $\mathcal{C}_3$ be a constraint system such that $\mathcal{C}_2 \to^* \mathcal{C}_3 \to^* \mathcal{C}_1$. Let $(X, s \vdash^? t_3) \in D(\mathcal{C}_3)$. Thanks to Lemma 65, we know that $\mathcal{L}^1_{\mathcal{C}_1}(t_1) \leq \mathcal{L}^1_{\mathcal{C}_3}(t_3) \leq \mathcal{L}^1_{\mathcal{C}_2}(t_2)$. We will show that that there exists $\mathcal{C}_4$ and $\mathcal{C}_3$ such that $\mathcal{C}_2 \to^* \mathcal{C}_3 \to \mathcal{C}_4 \to^* \mathcal{C}_1$, $(X, s \vdash^? t_4) \in D(\mathcal{C}_4)$, $(X, s \vdash^? t_3) \in D(\mathcal{C}_3)$ and $\mathcal{L}^1_{\mathcal{C}_4}(t_4) < \mathcal{L}^1_{\mathcal{C}_3}(t_3)$, which will imply that $\mathcal{L}^1_{\mathcal{C}_1}(t_1) < \mathcal{L}^1_{\mathcal{C}_2}(t_2)$.

Let $\mathcal{C}_3$ and $\mathcal{C}_4$ be the constraint systems such that $(X, s \vdash^? t_3) \in D(\mathcal{C}_3)$, $(X, s \vdash^? t_4) \in D(\mathcal{C}_4)$, $t_2 = t_3$, $t_3 \neq t_4$ and $\mathcal{C}_2 \to^* \mathcal{C}_3 \to \mathcal{C}_4 \to^* \mathcal{C}_1$. Those two constraints systems exist since we know that $t_1 \neq t_2$. Let $\text{RULE}(\tilde{p})$ be the rule applied on $\mathcal{C}_3$ to obtained $\mathcal{C}_4$. Since $t_2 = t_3$, we deduce that $t_3 \in \mathcal{X}^1$ and so $t_3 \in \mathsf{X}^1(\mathcal{C}_3)$. Thanks to Lemma 61 and $t_3 \in \mathsf{X}^1(\mathcal{C}_3)$, we deduce that $\text{RULE}(\tilde{p})$ is not an instance of CONS. Furthermore, since EQ-DED-DED is applied internally we also deduce that $\text{RULE}(\tilde{p})$ is not an instance of EQ-DED-DED. Hence we conclude that $\text{RULE}(\tilde{p})$ is an instance of AXIOM.

Assume that $\text{RULE}(\tilde{p}) = \text{AXIOM}(X_0, \mathsf{path})$. By definition, of the rule, there exists $(X_0, i_0 \vdash^? u_0) \in D(\mathcal{C}_3)$ and $(\xi, j_0 \rhd v_0) \in \Phi(\mathcal{C}_3)$ such that $j_0 \leq i_0$. Furthermore, we have $D(\mathcal{C}_4) = D(\mathcal{C}_3)\sigma \setminus \{X_0, i_0 \vdash^? u_0\sigma\}$, $t = v\sigma$ and $\Phi(\mathcal{C}_4) = \Phi(\mathcal{C}_3)\sigma$ where $\sigma = \mathsf{mgu}(u_0, v_0)$. Since by hypothesis $(X, s \vdash^? t_4) \in D(\mathcal{C}_4)$ and $t_4 \neq t_3$, we have that $t_3 \in \text{dom}(\sigma)$ and $t_3 \in \mathit{vars}^1(u_0, v_0)$. But the rule AXIOM is applied on the deducibility constraint minimal for $\mathcal{L}^1()$. Hence we deduce that $t_3 \in \mathit{vars}^1(u_0)$ and $\mathcal{L}^1_{\mathcal{C}_3}(t_3) = i_0$. But for all $x \in \mathit{vars}^1(t_3\sigma)$, we have that $x \in \mathit{vars}^1(v_0\sigma)$ and $\Phi(\mathcal{C}_4) = \Phi(\mathcal{C}_3)\sigma$. Thus, by the property of origination of a constraint system, we know that there exists $(Y, p \vdash^? w) \in D(\mathcal{C}_4)$ such that $x \in \mathit{vars}^1(w)$ and $p < j_0 \leq i_0$. Thus, we have that $\mathcal{L}^1_{\mathcal{C}_4}(x) < i_0$ and so for all $x \in \mathit{vars}^1(t_3\sigma))$, $\mathcal{L}^1_{\mathcal{C}_4}(x) < \mathcal{L}^1_{\mathcal{C}_3}(t_3)$. Since $t_3\sigma = t_4$, we conclude that $\mathcal{L}^1_{\mathcal{C}_4}(t_4) < \mathcal{L}^1_{\mathcal{C}_3}(t_3)$.

We have shown that for all $(X, s \vdash^? u) \in D(\mathcal{C}_1)$, if $X \notin S_2(\mathcal{C}_1)$ there exists v such that $(X, s \vdash^? v) \in D(\mathcal{C}_2)$ and $\mathcal{L}^1_{\mathcal{C}_1}(u) < \mathcal{L}^1_{\mathcal{C}_2}(v)$. Thus we can conclude that $\mu^k_{1.b+c}(\mathcal{M}_1, \mathcal{M}'_1) < \mu^k_{1.b+c}(\mathcal{M}_2, \mathcal{M}'_2)$. □

Appendix G.1.3. Step d: dealing with external deducibility constraints

During this step, we simplify the external deducibility constraints to obtain decubility constraint with a variable as a right-hand term. To achieve this, we apply the external rules EQ-DED-DED, CONS and AXIOM as long as they are strongly applicable on $\mathcal{M}_{i,k}$ by increasing order on the index of the line i (if we assume that k corresponds to an index of the matrix $\mathcal{M}$ in the pair $(\mathcal{M}, \mathcal{M}')$).

To prove the termination of this step, we will use the measure $\mu_{1.b}()$ defined on constraint system to establish termination of Step b. Thanks to Lemma 60, we know that the measure $\mu_{1.b}()$ strictly decreases for a rule strongly applicable on a constraint system. Assume that n is the number of lines in $\mathcal{M}$ and $\mathcal{M}'$, we define a lexicographic measure on $(\mathcal{M}, \mathcal{M}')$, denoted $\mu^k_{1.d}(\mathcal{M}, \mathcal{M}')$, as follows:

1. The number $n - i_0$ where i_0 is the maximal index of the line such that for all $i \leq i_0$, $\mathcal{M}_{i_0,k} = \bot$ or $\mathcal{M}_{i,k}$ satisfies the invariant $\mathsf{InvVarConstraint}(s)$
2. $\mu_{1.b}(\mathcal{M}_{i_0+1,k})$
3. The number of (X, path) such that $(X, i \vdash^? u) \in D(\mathcal{M}_{\ell,k})$, $(\xi, j \rhd v) \in \Phi(\mathcal{M}_{\ell,k})$, $j \leq i$, $X \neq^? \xi$ is not in $E_\Pi(\mathcal{M}_{\ell,k})$, $X \in S_2$, $\mathsf{path}(\xi) = \mathsf{path}$, $\ell \in \{1, \ldots, n\}$ and there exist $\mathsf{f} \in \mathcal{F}_c$ such that $\mathsf{root}(X) \neq^? \mathsf{f}$ in $E_\Pi(\mathcal{M}_{\ell,k})$

We will assume for this measure that $\mathcal{M}_{n',k} = \bot$ when $n' > n$.

Lemma 67. *Let $(\mathcal{M}, \mathcal{M}')$ be a pair of matrices obtained during Step d of Phase 1 with parameters s and k. Let* Rule$(\tilde{p})$ *be a rule applicable according to Step d of the strategy and let $(\mathcal{M}_1, \mathcal{M}'_1)$ and $(\mathcal{M}_2, \mathcal{M}'_2)$ be the two resulting pairs of matrices obtained by application of this rule on $(\mathcal{M}, \mathcal{M}')$. We have that:*

$$\mu^k_{1.d}(\mathcal{M}_1, \mathcal{M}'_1) < \mu^k_{1.d}(\mathcal{M}, \mathcal{M}') \quad \wedge \quad \mu^k_{1.d}(\mathcal{M}_2, \mathcal{M}'_2) < \mu^k_{1.d}(\mathcal{M}, \mathcal{M}')$$

Proof. Assume w.l.o.g. that the k^{th} column of $(\mathcal{M}, \mathcal{M}')$ is the k^{th} column of $\mathcal{M}$. We know that the only rules that can be applied in Step d are Cons, Eq-ded-ded and Axiom. Furthermore, the external application of those rules implies that $\mathcal{M}_{i,k} \to \mathcal{M}_{1\,i,k}$ and $\mathcal{M}_{i,k} \to \mathcal{M}_{2\,i,k}$, for all $i \in \{1, \ldots, n\}$. But thanks to Lemma 9, we know that if $\mathcal{M}_{i,k}$ satisfies $\mathsf{InvVarConstraint}(s)$ then $\mathcal{M}_{1\,i,k}$ and $\mathcal{M}_{2\,i,k}$ also satisfy $\mathsf{InvVarConstraint}(s)$ or are equal to $\bot$. Thus, we deduce that $\pi_1(\mu^k_{1.d}(\mathcal{M}_1, \mathcal{M}'_1)) \leq \pi_1(\mu^k_{1.d}(\mathcal{M}, \mathcal{M}'))$ and $\pi_1(\mu^k_{1.d}(\mathcal{M}_2, \mathcal{M}'_2)) \leq \pi_1(\mu^k_{1.d}(\mathcal{M}, \mathcal{M}'))$.

Let i_0 be the index of the line such that for all $i \leq i_0$, $\mathcal{M}_{i_0,k} = \bot$ or $\mathcal{M}_{i,k}$ satisfies the invariant $\mathsf{InvVarConstraint}(s)$. Let Rule$(\tilde{p})$ be an instance of a rule that is strongly applicable on $\mathcal{M}_{j_0,k}$. We do a case analysis on j_0.

Case $j_0 \leq i_0 + 1$ and Rule$(\tilde{p})$ *strongly applicable on $\mathcal{M}_{i_0+1,k}$:* In such a case, by applying Lemma 60, we obtained that $\mu_{1.b}(\mathcal{M}_{1\,i_0+1,k}) < \mu_{1.b}(\mathcal{M}_{i_0+1,k})$ and $\mu_{1.b}(\mathcal{M}_{2\,i_0+1,k}) < \mu_{1.b}(\mathcal{M}_{i_0+1,k})$. It implies that $\pi_2(\mu^k_{1.d}(\mathcal{M}_1, \mathcal{M}'_1)) < \pi_2(\mu^k_{1.d}(\mathcal{M}, \mathcal{M}'))$ and $\pi_2(\mu^k_{1.d}(\mathcal{M}_2, \mathcal{M}'_2)) < \pi_2(\mu^k_{1.d}(\mathcal{M}, \mathcal{M}'))$. Hence the result holds.

Case $j_0 \leq i_0 + 1$ and Rule$(\tilde{p})$ *not strongly applicable on $\mathcal{M}_{i_0+1,k}$:* Rule$(\tilde{p})$ is strongly applicable on $\mathcal{M}_{j_0,k}$, and therefore we have that $\mathcal{M}_{j_0,k} \neq \bot$ and $j_0 \neq i_0 + 1$. Hence by definition of i_0, we deduce that $\mathcal{M}_{j_0,k}$ satisfies the invariant $\mathsf{InvVarConstraint}(s)$. Hence Rule$(\tilde{p})$ strongly applicable on $\mathcal{M}_{j_0,k}$ implies that:

- Rule$(\tilde{p})$ = Cons(X, f) with $(X, i \vdash^? x) \in D(\mathcal{M}_{j_0,k})$, $x \in \mathcal{X}^1$ and there exists $\mathsf{g} \in \mathcal{F}_c$ such that $E_\Pi(\mathcal{M}_{j_0,k}) \vDash \mathsf{root}(X) \neq^? \mathsf{g}$. But thanks to Lemma 28, $(\mathcal{M}, \mathcal{M}')$ satisfies $\mathsf{InvGeneral}$ and more specifically Property 6 of the invariant $\mathsf{InvGeneral}$ which means that $E_\Pi(\mathcal{M}_{i_0+1,k}) \vDash \mathsf{root}(X) \neq^? \mathsf{g}$. Thus, we deduce that Rule$(\tilde{p})$ is also strongly applicable on $\mathcal{M}_{i_0+1,k}$ which is a contradiction with our hypothesis.

- Rule$(\tilde{p})$ = Axiom(X, path) with $(X, i \vdash^? x) \in D(\mathcal{M}_{j_0,k})$, $x \in \mathcal{X}^1$ and there exists $\mathsf{g} \in \mathcal{F}_c$ such that $E_\Pi(\mathcal{M}_{j_0,k}) \vDash \mathsf{root}(X) \neq^? \mathsf{g}$. Once again, thanks to Property 6 of the invariant $\mathsf{InvGeneral}$, we deduce that $E_\Pi(\mathcal{M}_{i_0+1,k}) \vDash \mathsf{root}(X) \neq^? \mathsf{g}$. However Rule$(\tilde{p})$ is not strongly applicable on $\mathcal{M}_{i_0+1,k}$ which means that if there exists a frame element $(\xi, i \vdash^? u) \in \Phi(\mathcal{M}_{i_0+1,k})$ such that $\mathsf{path}(\xi) = \mathsf{path}$ then $E_\Pi(\mathcal{M}_{i_0+1,k}) \vDash X \neq^? \xi$. But thanks to Property 7 and the fact that Axiom(X, path) is strongly applicable on $\mathcal{M}_{j_0,k}$, we deduce that there is no frame element $(\xi, i \vdash^? u) \in \Phi(\mathcal{M}_{i_0+1,k})$ such that $\mathsf{path}(\xi) = \mathsf{path}$. Thus, we have that $\mathcal{M}_{1\,i_0+1,k} = \bot$ and $\mathcal{M}_{2\,i_0+1,k} = \mathcal{M}_{i_0+1,k}$.

  Therefore, we deduce that $\pi_1(\mu^k_{1.d}(\mathcal{M}_1, \mathcal{M}'_1)) < \pi_1(\mu^k_{1.d}(\mathcal{M}, \mathcal{M}'))$ and $\pi_2(\mu^k_{1.d}(\mathcal{M}_2, \mathcal{M}'_2)) = \pi_2(\mu^k_{1.d}(\mathcal{M}, \mathcal{M}'))$. Furthermore, we have that $E_\Pi(\mathcal{M}_{2\,j_0,k}) = E_\Pi(\mathcal{M}_{j_0,k}) \wedge X \neq^? \xi$ where $\mathsf{path}(\xi) = \mathsf{path}$ and $(\xi, i \vdash^? u) \in \Phi(\mathcal{M}_{j_0,k})$. Hence we deduce that $\pi_3(\mu^k_{1.d}(\mathcal{M}_2, \mathcal{M}'_2)) < \pi_3(\mu^k_{1.d}(\mathcal{M}, \mathcal{M}'))$. Thus we conclude that $\mu^k_{1.d}(\mathcal{M}_1, \mathcal{M}'_1) < \mu^k_{1.d}(\mathcal{M}, \mathcal{M}')$ and $\mu^k_{1.d}(\mathcal{M}_2, \mathcal{M}'_2) < \mu^k_{1.d}(\mathcal{M}, \mathcal{M}')$.

Case $j_0 > i_0 + 1$: In such a case, it implies that no instance of the rule Cons, Axiom and Eq-ded-ded can be strongly applied on $\mathcal{M}_{i_0+1,k}$ with support inferior of equal to s. Thus, we can first deduce that for all $(X, i \vdash^? u) \in D(\mathcal{M}_{i_0+1,k})$, if $i \leq s$ then $u \in \mathcal{X}^1$ and for all $\mathsf{f} \in \mathcal{F}_c$, $E_\Pi(\mathcal{M}_{i_0+1,k}) \nvDash \mathsf{root}(X) \neq^? \mathsf{f}$. Indeed, assume that $u \notin \mathcal{X}^1$.

- if there exists $(\xi, j \rhd v) \in \Phi(\mathcal{M}_{i_0+1,k})$ such that $j \leq i$ and $E_\Pi(\mathcal{M}_{i_0+1,k}) \nvDash X \neq^? \xi$, then $\textsc{Axiom}(X, \mathsf{path}(\xi))$ would be strongly applicable on $\mathcal{M}_{i_0,k}$ which contradicts our hypothesis
- if there exists $\mathsf{f} \in \mathcal{F}_c$ such that $E_\Pi(\mathcal{M}_{i_0+1,k}) \nvDash \mathsf{root}(X) \neq^? \mathsf{f}$, then $\textsc{Cons}(X, \mathsf{f})$ would be strongly applicable on $\mathcal{M}_{i_0+1,k}$ which contradicts our hypothesis.
- Else we would have that for all $(\xi, j \rhd v) \in \Phi(\mathcal{M}_{i_0+1,k})$, $j \leq i$ implies $E_\Pi(\mathcal{M}_{i_0+1,k}) \vDash X \neq^? \xi$ and for all $\mathsf{f} \in \mathcal{F}_c$, $E_\Pi(\mathcal{M}_{i_0+1,k}) \vDash \mathsf{root}(X) \neq^? \mathsf{f}$. But in such a case, the normalisation of the constraint system would implies that $\mathcal{M}_{i_0+1,k} = \bot$ witch contradicts the definition of i_0.

We now prove that in fact the case $j_0 > i_0 + 1$ is impossible. Assume that $(X, i \vdash^? x)$ and $(Y, j \vdash^? y)$ in $D(\mathcal{M}_{i_0+1,k})$ such that $x = y$. In such a case, since we proved that for all $\mathsf{f} \in \mathcal{F}_c$, $E_\Pi(\mathcal{M}_{i_0+1,k}) \nvDash \mathsf{root}(X) \neq^? \mathsf{f}$ and $E_\Pi(\mathcal{M}_{i_0+1,k}) \nvDash \mathsf{root}(Y) \neq^? \mathsf{f}$, we can deduce that the rule Eq-ded-ded(X, Y) is strongly applicable on $\mathcal{M}_{i_0+1,k}$ which is a contradiction on our hypothesis. Hence we can deduce that $\mathcal{M}_{i_0+1,k}$ satisfies the invariant $\mathsf{InvVarConstraint}(s)$ which is also a contradiction on the definition of i_0. Hence the case $j_0 > i_0 + 1$ is impossible. □

Appendix G.1.4. Step e: solving non-deducibility constraints

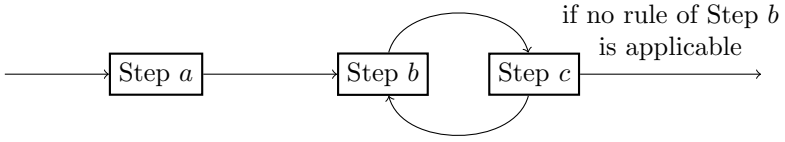
This step only consists of replacing some constraint systems by $\bot$, and its termination is ensured.

Proposition 1. *Applying the transformation rules on a pair of sets of initial constraint systems following the Phase 1 of the strategy terminates.*

Proof. According to Section 4, Phase 1 of the strategy depends on two parameters s and k that are respectively bounded by the size of the frames in the initial matrices of constraint systems and by the sum of the number of columns of the two matrices. Hence, the proof termination of Phase 1 follows directly from the proof of termination of the different step given parameters s and k. Lemma 59 ensures the termination of Step a. Corollary 3 ensures the individual termination of Step b. Lemma 64 ensures the individual termination of Step c. Lemma 66 ensures the termination of the cycle of steps b and c. Finally, Lemma 67 ensures termination of Step d. □

Appendix G.2. Phase 2: Taking care of disequations

During the second phase of our strategy $\mathcal{S}$, the only rules that can be applied are Cons, Axiom and Eq-ded-ded. Furthermore these rules will always be applied as external rules. As already explained, the purpose of this phase is to take care of the disequations. For this, we need to match them, and ensure that the same disequations occur in each constraint system. As depicted below, this second phase is made up of three steps.



We show termination of each step separately, and we consider also the cycle Steps b/c.

Appendix G.2.1. Step a: getting rid of universally quantified variables

This step of the strategy consists of getting rid of the universal variable. In order to show that this step terminates, we introduce a measure on the formulas E that considers the positions of all the universal variables. Let $(\mathcal{M}, \mathcal{M}')$ be a pair of matrices, we define a lexicographic measure, denoted $\mu_{2.a}(\mathcal{M}, \mathcal{M}')$, which is composed of :

1. The multiset of the positions of any occurrence of universal variables in $E(\mathcal{C})$, for any constraint system $\mathcal{C}$ in $\mathcal{M}$ and $\mathcal{M}'$, i.e. $\{\{p \mid E(\mathcal{C}) = E' \wedge [\forall \tilde{y}.\forall x.E'' \vee u \neq^? v]$ and $u_{|p} = x$ and $\mathcal{C}$ in $(\mathcal{M}, \mathcal{M}')\}\}$
2. The number of (X, f) such that $\mathsf{root}(X) \neq \mathsf{f}$ not in E_Π, $X, i \vdash^? u \in D(\mathcal{C})$, $\mathsf{f} \in \mathcal{F}_c$ and $\mathcal{C}$ in $(\mathcal{M}, \mathcal{M}')$.
3. The number of (X, ξ) such that $X, i \vdash^? u \in D$, $\xi, j \vdash^? v \in \Phi$, $j \leq i$, $X \neq \xi$ is not in $E_\Pi(\mathcal{C})$ and $\mathcal{C}$ in $(\mathcal{M}, \mathcal{M}')$.

Thanks to this measure we are able to prove the termination of Step a.

Lemma 68. *Let $(\mathcal{M}, \mathcal{M}')$ be a pair of matrices obtained during Step a of Phase 2 of the strategy. Let* Rule$(\tilde{p})$ *be an instance of the rule* Axiom *or* Cons *such that* Rule$(\tilde{p})$ *is strongly applicable on at least one constraint system in $\mathcal{M}$ or $\mathcal{M}'$, and let $(\mathcal{M}_1, \mathcal{M}'_1)$ and $(\mathcal{M}_2, \mathcal{M}'_2)$ be the two resulting pairs of matrices. We have that:*

$$\mu_{2.a}(\mathcal{M}_1, \mathcal{M}'_1) < \mu_{2.a}(\mathcal{M}, \mathcal{M}') \quad \wedge \quad \mu_{2.a}(\mathcal{M}_2, \mathcal{M}'_2) < \mu_{2.a}(\mathcal{M}, \mathcal{M}')$$

Proof. Thanks to the normalisation, we know that for all constraint system $\mathcal{C}$ in $\mathcal{M}$, the disjunctions of inequations in $E(\mathcal{C})$ are of the form $\forall \tilde{y}. \bigvee_i x_i \neq^? u_i$ where $\tilde{y}$ is a set of universal variable and x_i are not universal for any i. Assume that $(X, i \vdash^? x) \in D(\mathcal{C})$ and a rule is applied on this deducibility constraint, i.e. Cons(X, f) or Axiom(X, path). Let's denote $\mathcal{C}_1$ and $\mathcal{C}_2$ the two constraint systems obtained by applying the rule on $\mathcal{C}$, i.e. $\mathcal{C}_1$ is in $(\mathcal{M}_1, \mathcal{M}'_1)$ and $\mathcal{C}_2$ is in $(\mathcal{M}_2, \mathcal{M}'_2)$.

We first focus on $(\mathcal{M}_1, \mathcal{M}'_1)$. In the case of rule Cons, since $\mathcal{C}$ satisfies the invariant $\overline{\mathsf{InvVarConstraint}(\mathsf{s}_{max})}$, we deduce that x will be instantiated in $\mathcal{C}_1$ by $\mathsf{f}(x_1, \ldots, x_n)$ where x_k are not universal, for all $k \in \{1, \ldots, n\}$. In the case of rule Axiom, since $\mathcal{C}$ satisfies the invariant $\mathsf{InvNoUse}(\mathsf{s}_{max})$, we know that $(\xi, j \rhd u) \in \Phi(\mathcal{C})$ with $\mathsf{path}(\xi) = \mathsf{path}(\xi)$ implies that $u \notin \mathcal{X}^1$ (otherwise we would have $(\xi, j \rhd u) \in \mathsf{NoUse}(\mathcal{C})$ and so the rule Axiom(X, path) would not be applicable).

Hence we have shown that x is necessary instantiated by a term different from a variable. We denote σ the substitution that instantiates x. Let's now look at the possible atomic statement that contains x:

1. Case $E(\mathcal{C}) = E' \wedge [\forall \tilde{y}.z.E'' \vee x \neq^? v]$ and $z \in vars^1(v)$: In such a case, we have that $E(\mathcal{C}_1) = E'\sigma\downarrow \wedge [\forall \tilde{y}.z.E''\sigma \vee x\sigma \neq^? v\sigma]\downarrow$. By hypothesis, we know that $E(\mathcal{C})$ is normalised. Hence we have that $v \neq z$ which means that $\mathsf{root}(v) \in \mathcal{F}_c$. Let's denote $v = \mathsf{g}(v_1, \ldots, v_n)$. Since $x \in vars^1(v)$, there exists k and a position p such that $z \in vars^1(v_k)$ and $v_k|_p = z$. This implies that $(k \cdot p) \in \pi_1(\mu_{2.a}(\mathcal{M}, \mathcal{M}'))$. Furthermore, we proved that $x\sigma \notin \mathcal{X}^1$, thus we can denote $x\sigma = \mathsf{f}(u_1, \ldots, u_m)$.

   If $\mathsf{g} = \mathsf{f}$ then $n = m$ and we have that $(x\sigma \neq^? v\sigma)\downarrow = u_1 \vee v_1 \vee \ldots \vee u_n \vee v_n$. Hence in such a case, we deduce that the same occurrence of z have the position $p \in \pi_1(\mu_{2.a}(\mathcal{M}_1, \mathcal{M}'_1))$.

   Else $\mathsf{g} \neq \mathsf{f}$. In such a case, we deduce that $E'\sigma\downarrow \wedge [\forall \tilde{y}.z.E''\sigma \vee x\sigma \neq^? v\sigma]\downarrow = E'\sigma\downarrow$. Thus, this specific occurrence of z in $E(\mathcal{C})$ is no longer in $E(\mathcal{C}_1)$.

2. Case $E(\mathcal{C}) = E' \wedge [\forall \tilde{y}.z.E'' \vee x' \neq^? v]$, $x' \neq x$ and $z \in vars^1(v)$: We already proved that $x\sigma$ do not contain an universal variable and $x \neq^? x'$ which implies that $x' \neq^? v\sigma)\downarrow = x' \neq^? v\sigma$. Hence if p is a position such that $v\sigma|_p = z$ then we also have that $v|_p = z$ which means that $p \in \pi_1(\mu_{2.a}(\mathcal{M}, \mathcal{M}'))$ and $p \in \pi_1(\mu_{2.a}(\mathcal{M}_1, \mathcal{M}'_1))$.

3. Case $E(\mathcal{C}) = E' \wedge [\forall \tilde{y}.E'' \vee x' \neq^? v]$ and $vars^1(v) \cap \tilde{y} = \emptyset$: Once again, we already proved that $x\sigma$ do not contain an universal variable hence $vars^1(v) \cap \tilde{y} = \emptyset$ implies that $vars^1(v\sigma) \cap \tilde{y} = \emptyset$

We have shown that the position of an occurrence of an universal variable either stays the same or decrease. More specifically, we have shown that in Case 1, the position necessary decreases or the occurrence is no longer in $E(\mathcal{C}_1)$. Since Case 1 corresponds to the application condition of the rule Axiom and Cons, we deduce that $\mu_{2.a}(\mathcal{M}_1, \mathcal{M}'_1) < \mu_{2.a}(\mathcal{M}, \mathcal{M}')$.

We now focus on $(\mathcal{M}_2, \mathcal{M}'_2)$. By definition of the rule Axiom and Cons, we know that the only difference between $\mathcal{C}$ and $\mathcal{C}_2$ is the second order formula E_Π, i.e. $E_\Pi(\mathcal{C}_2) = E_\Pi(\mathcal{C}) \wedge \mathsf{root}(X) \neq^? \mathsf{f}$ in the case of the rule Cons(X, f); and $E_\Pi(\mathcal{C}_2) = E_\Pi(\mathcal{C}) \wedge X \neq^? \xi$ in the case of the rule Axiom(X, path) with $\mathsf{path}(\xi) = \mathsf{path}$ and $(\xi, j \rhd u) \in \Phi(\mathcal{C})$. Hence we trivially have that $\pi_k(\mu_{2.a}(\mathcal{M}_2, \mathcal{M}'_2)) = \pi_k(\mu_{2.a}(\mathcal{M}, \mathcal{M}'))$ with $k = 1, 2$ and $\pi_3(\mu_{2.a}(\mathcal{M}_2, \mathcal{M}'_2)) < \pi_3(\mu_{2.a}(\mathcal{M}, \mathcal{M}'))$ in the case of the rule Axiom; whereas we have $\pi_1(\mu_{2.a}(\mathcal{M}_2, \mathcal{M}'_2)) = \pi_1(\mu_{2.a}(\mathcal{M}, \mathcal{M}'))$ and $\pi_2(\mu_{2.a}(\mathcal{M}_2, \mathcal{M}'_2)) < \pi_2(\mu_{2.a}(\mathcal{M}, \mathcal{M}'))$ in the case of the rule Cons. We conclude that $\mu_{2.a}(\mathcal{M}_2, \mathcal{M}'_2) < \mu_{2.a}(\mathcal{M}, \mathcal{M}')$. □

Appendix G.2.2. Steps b and c: matching disequations

Step b alone. This step consists of applying, as long as we can, either an instance of the rule Cons or an instance of the rule Eq-ded-ded due to the presence of a disequation $x \neq^? u$ in a constraint system $\mathcal{C}$. Moreover, we consider an application where $\mathcal{L}^1_{\mathcal{C}}(x \neq^? u)$ is maximum.

$$\mathcal{L}^1_{\mathcal{C}}(u) = max\left(\{i \mid (X, i \vdash^? x) \in D(\mathcal{C}) \wedge x \in vars(u)\} \cup \{0\}\right).$$

The idea behind the measure that we will use to prove termination of this step is to over-approximate the number of possible applications of these two rules (Cons and Eq-ded-ded) along a branch. This can be achieved by looking at the depth at which names and "faulty" variables occur in disequations for the Cons rule, and by simply

counting the number of distinct variables for the Eq-ded-ded rule. Actually, we need to be more precise and to take into account the support at which the rule is applied.

Consider a matrix $\mathcal{M}$ and let n be the size of the frames in $\mathcal{M}$. For all $i \in \{1, \ldots, n\}$, we denote by $\mu^i_{cons}(\mathcal{M})$ the measure characterizing how many times the rule Cons will need to be applied with a recipe variables of support i as parameter, and we define it as follows:

$$\mu^i_{cons}(\mathcal{M}) = \left\{\!\!\left\{ h \;\middle|\; \begin{array}{l} \mathcal{C} \text{ is in } \mathcal{M},\ E(\mathcal{C}) = E \wedge (D \vee x \neq^? v), \\ (X, i \vdash^? x) \in D(\mathcal{C}),\ \mathsf{root}(v) \in \mathcal{F}_c, \\ E_\Pi(\mathcal{C}) \not\models \mathsf{root}(X) \neq^? \mathsf{root}(v), \\ \text{either } st(v) \cap \mathcal{N} \neq \emptyset \text{ or } i < \mathcal{L}^1_{\mathcal{C}}(v), \\ h = \max\{|p| \;\mid\; v|_p \in \mathcal{N} \vee (v|_p \in \mathcal{X}^1 \wedge i < \mathcal{L}^1_{\mathcal{C}}(v|_p))\} \end{array} \right\}\!\!\right\}$$

Recall that at this point of the strategy, all the constraint systems in the matrix are in pre-solved form and in particular all deducibility constraints have a variable as right hand term. At each disequation $x \neq^? v$ of any constraint system of the two matrices where the rule Cons is applicable (given by $E_\Pi(\mathcal{C}) \not\models \mathsf{root}(X) \neq^? \mathsf{root}(v)$ and either $st(v) \cap \mathcal{N} \neq \emptyset$ or $i < \mathcal{L}^1_{\mathcal{C}}(v)$), we associate an integer that corresponds to the maximal depth at which either a name or a variable with a support greater than the support of x occurs in v. A high value for $\mu^i_{cons}(\mathcal{M})$ indicates a possible high number of application of the rule Cons at support i.

For example, assume that we consider the disequation $x \neq \mathsf{f}(\mathsf{g}(a), y)$ where x and y have the same support i. This disequation will contribute to the measure $\mu^i_{cons}(\mathcal{M})$ by adding 2 (the depth of the name a in this disequation). As long as the name a is not on the root of the disequation, an application of the rule Cons will be possible:

$$\begin{array}{cc} x \neq \mathsf{f}(\mathsf{g}(a), y) & \\ \downarrow & \text{Cons on } x \\ x_1 \neq \mathsf{g}(a) \vee x_2 \neq^? y & \\ \downarrow & \text{Cons on } x_1 \\ x_3 \neq a \vee x_2 \neq^? y & \text{No more Cons} \end{array}$$

The $\mu^i_{cons}(\mathcal{M})$ is an over-approximation of the number of applications of the rule Cons on the matrix $\mathcal{M}$ along a branch. It differs from the number of possible applications of Cons on $\mathcal{M}$ that we denote by $\mu^{App}_{cons}(\mathcal{M})$.

We need also to take into account the number of possible applications of the rule Eq-ded-ded along a branch, denoted by $\mu^i_{eqrr}(\mathcal{M})$. First $\mu^i_{eqrr}(\mathcal{M}) = 0$ in case $\mathcal{M}$ only contains constraint systems that are reduced to $\bot$. Otherwise, let $\mathcal{C}_\mathcal{M}$ be a non $\bot$ constraint system in $\mathcal{M}$, $\mu^i_{eqrr}(\mathcal{M}) = |\{x \in vars^1(\mathcal{C}_\mathcal{M}) \mid \mathcal{L}^1_{\mathcal{C}_\mathcal{M}}(x) = i\}|$. Note that since all the constraint systems in $\mathcal{M}$ have the same shape, this measure does not depend of the choice of the representant $\mathcal{C}_\mathcal{M}$ in $\mathcal{M}$. The measure $\mu^i_{eqrr}(\mathcal{M})$ only calculates how many variable of index i there are in a constraint system. Once again, this measure differs from the actual number of possible applications of Eq-ded-ded on $(\mathcal{M}, \mathcal{M}')$, that we denote by $\mu^{App}_{eqrr}(\mathcal{M})$.

We can combine these measures as follows:

$$\mu_{2.b}(\mathcal{M}) = (\mu^n_{cons}(\mathcal{M}), \mu^n_{eqrr}(\mathcal{M}), \ldots, \mu^1_{cons}(\mathcal{M}), \mu^1_{eqrr}(\mathcal{M}), \mu^{App}_{cons}(\mathcal{M}), \mu^{App}_{eqrr}(\mathcal{M}))$$

Lemma 69. *Let $(\mathcal{M}, \mathcal{M}')$ be a pair of matrices obtained during Step b of the second phase. Let* Rule$(\tilde{p})$ *be an applicable rule and let $(\mathcal{M}_1, \mathcal{M}'_1)$ and $(\mathcal{M}_2, \mathcal{M}'_2)$ the two resulting pairs of matrices obtained by appluing* Rule$(\tilde{p})$ *on $(\mathcal{M}, \mathcal{M}')$. We have that:*

$$\mu_{2.b}(\mathcal{M}_1, \mathcal{M}'_1) <_{\mathsf{lex}} \mu_{2.b}(\mathcal{M}, \mathcal{M}') \quad \textit{and} \quad \mu_{2.b}(\mathcal{M}_2, \mathcal{M}'_2) <_{\mathsf{lex}} \mu_{2.b}(\mathcal{M}, \mathcal{M}')$$

Proof. First, at this stage, all the constraint systems of the matrix are in pre-solved form and do not contain universal variable. Hence, the application conditions of the rules Cons and Eq-ded-ded only depend on E and E_Π. Moreover, we consider w.l.o.g. that $(\mathcal{M}_1, \mathcal{M}'_1)$ (resp. $(\mathcal{M}_2, \mathcal{M}'_2)$) is the pair of matrices on which the guess of the rule is satisfied (resp. not satisfied).

Case of the branch $(\mathcal{M}_1, \mathcal{M}'_1)$. Consider $\mathcal{C}$ in $(\mathcal{M}, \mathcal{M}')$ and let us denote by $\mathcal{C}_1$ the result in $(\mathcal{M}_1, \mathcal{M}'_1)$ by application of the rule Cons or Eq-ded-ded on $\mathcal{C}$. For both rules, a substitution $\sigma = \{x \to u\}$ was applied on $E(\mathcal{C})$ to obtain $E(\mathcal{C}_1)$, that is $E(\mathcal{C}_1) = E(\mathcal{C})\sigma\downarrow$. In the case of the rule Cons, $u = \mathsf{f}(x_1, \ldots, x_n)$ where $x_1, \ldots, x_n$ are some fresh variables and in the case of the rule Eq-ded-ded, u is a term without any name. Moreover, in both cases, we have $\mathcal{L}^1_{\mathcal{C}}(u) \leq \mathcal{L}^1_{\mathcal{C}}(x)$.

Let us assume $E(\mathcal{C}) = E \wedge (D \vee y \neq^? v)$ for some E, D, y and v; and let us observe the influence of the application of σ on the computation of $\mu^i_{cons}(\mathcal{M}_1, \mathcal{M}'_1)$ for all $i \geq \mathcal{L}^1_{\mathcal{C}}(x)$. Let us assume first that the disequation $y \neq^? v$ induces an integer h in the multiset $\mu^i_{cons}(\mathcal{M}, \mathcal{M}')$ for some $i \geq \mathcal{L}^1_{\mathcal{C}}(x)$.

If $x \notin vars(v)$ and $x \neq y$ then the disequation $(y \neq^? v)$ is left unchanged by application of σ. If $x \in vars(v)$ then $(y \neq^? v)\sigma\downarrow$ is in fact the disequation $y \neq^? v\sigma$. But, $y \neq^? v$ inducing the integer h in the multiset $\mu^i_{cons}(\mathcal{M}, \mathcal{M}')$ implies that $i = \mathcal{L}^1_{\mathcal{C}}(y)$. With the fact that u does not contain any name, $i \geq \mathcal{L}^1_{\mathcal{C}}(x)$ and $\mathcal{L}^1_{\mathcal{C}}(u) \leq \mathcal{L}^1_{\mathcal{C}}(x)$, we deduce that the heights of names in v and the heights of the variables with strictly bigger support than y is left unchanged after application of the substitution σ, that is:

$$\begin{gathered}\max\{\mathsf{h}(p) \mid v|_p \in \mathcal{N} \vee (v|_p \in \mathcal{X}^1 \wedge i < \mathcal{L}^1_{\mathcal{C}}(v|_p))\} \\ = \\ \max\{\mathsf{h}(p) \mid v\sigma|_p \in \mathcal{N} \vee (v\sigma|_p \in \mathcal{X}^1 \wedge i < \mathcal{L}^1_{\mathcal{C}}(v\sigma|_p))\}\end{gathered}$$

This allows us to deduce that $y \neq^? v$ and $(y \neq^? v)\sigma\downarrow$ produces respectively the same integer in $\mu^i_{cons}(\mathcal{M}, \mathcal{M}')$ and $\mu^i_{cons}(\mathcal{M}_1, \mathcal{M}'_1)$.

Let us now consider the last case, that is $y = x$, meaning that $i = \mathcal{L}^1_{\mathcal{C}}(x)$. In such a case $(y \neq^? v)\sigma$ is either reduced after normalisation to (a) true; or to (b) $z \neq^? v$ when u is a variable (that we rename z for the occasion); or to (c) a disjunction of disequation $\vee^m_{k=1} u_k \neq^? v_k$ where u_k and v_k are respectively strict subterm of u and v (the fact that u_i and v_i are strict subterm comes from our knowledge that $y \neq^? v$ induces h in $\mu^i_{cons}(\mathcal{M}, \mathcal{M}')$ and so that v is neither a variable nor a name).

In case (b), since $\mathcal{L}^1_{\mathcal{C}}(z) \leq \mathcal{L}^1_{\mathcal{C}}(x)$, the disequation $z \neq^? v$ either induces the same integer as $x \neq^? v$ in the multiset $\mu^i_{cons}(\mathcal{M}_1, \mathcal{M}'_1)$ when $\mathcal{L}^1_{\mathcal{C}}(z) = \mathcal{L}^1_{\mathcal{C}}(x)$ or else induces an integer in the multiset $\mu^j_{cons}(\mathcal{M}_1, \mathcal{M}'_1)$ with $j < \mathcal{L}^1_{\mathcal{C}}(x)$.

In case (c), by normalisation, we know that for all $k \in \{1, \ldots, m\}$, either u_k or v_k is a variable. When u_k is a variable, the facts that u_k is a subterm of u and $\mathcal{L}^1_{\mathcal{C}}(u) \leq \mathcal{L}^1_{\mathcal{C}}(x)$ imply that if $u_k \neq^? v_k$ induces an integer in a multiset $\mu^j_{cons}(\mathcal{M}_1, \mathcal{M}'_1)$ then $j \leq i$.

Moreover, because v_k is a strict subterm of v, then the induced integer is strictly smaller than the integer h induced by $y \neq^? v$ in the multiset $\mu^i_{cons}(\mathcal{M}, \mathcal{M}')$. On the other hand, when v_k is a variable, since u does not contain any name and $\mathcal{L}^1_{\mathcal{C}}(u) \leq \mathcal{L}^1_{\mathcal{C}}(x)$ then $u_k \neq^? v_k$ can only induces an integer in a multiset $\mu^j_{cons}(\mathcal{M}_1, \mathcal{M}'_1)$ where $j < i$.

To summarize the different cases, we showed that the application of σ on $y \neq^? v$ where $\mathcal{L}^1_{\mathcal{C}}(y) = i$ induces either the same integer h in $\mu^i_{cons}(\mathcal{M}_1, \mathcal{M}'_1)$ or; induces several integers in $\mu^i_{cons}(\mathcal{M}_1, \mathcal{M}'_1)$, all of them strictly smaller than h; or else induces some integers in $\mu^j_{cons}(\mathcal{M}_1, \mathcal{M}'_1)$ with $j < \mathcal{L}^1_{\mathcal{C}}(x)$. This allows us to deduce that for all $k \geq \mathcal{L}^1_{\mathcal{C}}(x)$, $\mu^k_{cons}(\mathcal{M}_1, \mathcal{M}'_1) \leq \mu^k_{cons}(\mathcal{M}, \mathcal{M}')$.

For the rule Cons, we can be more specific by showing that for $k = \mathcal{L}^1_{\mathcal{C}}(x)$, $\mu^k_{cons}(\mathcal{M}_1, \mathcal{M}'_1) < \mu^k_{cons}(\mathcal{M}, \mathcal{M}')$. Indeed, the application conditions of the rule imply the existence of at least one disequation $x \neq^? v$ with names or variables in v with bigger index than x, meaning that $x \neq^? v$ induces an integer h in $\mu^k_{cons}(\mathcal{M}, \mathcal{M}')$. But the integers induced by $(u \neq^? v)\downarrow$ in $\mu^k_{cons}(\mathcal{M}_1, \mathcal{M}'_1)$ are all strictly smaller than h. Therefore, $\mu^k_{cons}(\mathcal{M}_1, \mathcal{M}'_1) < \mu^k_{cons}(\mathcal{M}, \mathcal{M}')$.

Lastly, we trivially have $\mu^k_{eqrr}(\mathcal{M}_1, \mathcal{M}'_1) = \mu^k_{eqrr}(\mathcal{M}, \mathcal{M}')$ for all $k > \mathcal{L}^1_{\mathcal{C}}(x)$, and in the case of the rule Eq-ded-ded, we also have that $\mu^k_{eqrr}(\mathcal{M}_1, \mathcal{M}'_1) < \mu^k_{eqrr}(\mathcal{M}, \mathcal{M}')$ for $k = \mathcal{L}^1_{\mathcal{C}}(x)$. This allows us to conclude that $\mu_{2.b}(\mathcal{M}_1, \mathcal{M}'_1) < \mu_{2.b}(\mathcal{M}, \mathcal{M}')$.

Case of the branch $(\mathcal{M}_2, \mathcal{M}'_2)$. Consider $\mathcal{C}$ in $(\mathcal{M}, \mathcal{M}')$ and let us denote by $\mathcal{C}_2$ the result in $(\mathcal{M}_2, \mathcal{M}'_2)$ of the application of the rule Cons or Eq-ded-ded on $\mathcal{C}$.

For the rule Cons with parameter X and f, the only difference between $\mathcal{C}$ and $\mathcal{C}_2$ is the addition of $\mathsf{root}(X) \neq^? \mathsf{f}$ in $E_\Pi(\mathcal{C}_2)$ which reduces by one the number of application of Cons. Indeed, the application of Cons with once again X and f would be useless. Therefore, $\mu^{App}_{cons}(\mathcal{M}_2, \mathcal{M}'_2) < \mu^{App}_{cons}(\mathcal{M}, \mathcal{M}')$ and so $\mu_{2.b}(\mathcal{M}_2, \mathcal{M}'_2) < \mu_{2.b}(\mathcal{M}, \mathcal{M}')$.

For the rule Eq-ded-ded, a disequation may have been added to $\mathcal{C}$ to obtain $\mathcal{C}_2$. However, we know that this disequation is of the form $x' \neq^? u'$ where u' does not contain name and $\mathcal{L}^1_{\mathcal{C}}(x) \geq \mathcal{L}^1_{\mathcal{C}}(u')$. Thus, $x' \neq^? u'$ does not induces an integer in any multiset $\mu^k_{cons}(\mathcal{M}_2, \mathcal{M}'_2)$, for all k, and it also does not trigger the application of an instance of the rule Cons. Lastly, once the rule Eq-ded-ded is applied with some parameters, the same instance of the rule becomes useless on $(\mathcal{M}_2, \mathcal{M}'_2)$. Hence $\mu^{App}_{eqrr}(\mathcal{M}_2, \mathcal{M}'_2) < \mu^{App}_{eqrr}(\mathcal{M}, \mathcal{M}')$ and so we conclude that $\mu_{2.b}(\mathcal{M}_2, \mathcal{M}'_2) < \mu_{2.b}(\mathcal{M}, \mathcal{M}')$. □

Step c alone. The measure used to prove termination of Step c is very simple. Indeed, during Step c, we only apply the rule Axiom which either decreases the number of deducibility constraints or adds a disequation between recipes. Let $(\mathcal{M}, \mathcal{M}')$ be a pair of matrices, let $\mathcal{C}_0$ be a constraint system in $\mathcal{M}$ or $\mathcal{M}'$ such that $\mathcal{C}_0 \neq \bot$, we define the lexicographic measure $\mu_{2.c}(\mathcal{M}, \mathcal{M}')$, as follows:

1. The number of deducibility constraints, i.e. $|D(\mathcal{C}_0)|$
2. The number of pair (X, ξ) such that $(X, i \vdash^? x) \in D(\mathcal{C}_0)$, $(\xi, j \rhd u) \in \Phi(\mathcal{C}_0)$ and $E_\Pi(\mathcal{C}_0) \nvdash X \neq^? \xi$.

Thanks to this measure, we can now state the termination lemma.

Lemma 70. *Let $(\mathcal{M}, \mathcal{M}')$ be a pair of matrices obtained during Step c of the second phase. Let* Axiom$(\tilde{p})$ *be an applicable rule and let $(\mathcal{M}_1, \mathcal{M}'_1)$ and $(\mathcal{M}_2, \mathcal{M}'_2)$ the two*

resulting pairs of matrices obtained by application of AXIOM($\tilde{p}$) *on* $(\mathcal{M}, \mathcal{M}')$. *We have that:*

$$\mu_{2.c}(\mathcal{M}_1, \mathcal{M}'_1) < \mu_{2.c}(\mathcal{M}, \mathcal{M}') \quad \textit{and} \quad \mu_{2.c}(\mathcal{M}_2, \mathcal{M}'_2) < \mu_{2.c}(\mathcal{M}, \mathcal{M}')$$

Proof. Direct from the definition of the rule AXIOM. □

Steps b and c together. We now describe the main measure that will necessarily strictly decrease after one cycle Step $b + c$. For a constraint system $\mathcal{C}$ of the matrix, the application of any of the three rules AXIOM, CONS and EQ-DED-DED, transforms $E(\mathcal{C})$ by either adding a disequation (case of EQ-DED-DED when the guess is not satisfied) or by applying a substitution $\sigma = \{x \to u\}$ where $\mathcal{L}^1_{\mathcal{C}}(x) \geq \mathcal{L}^1_{\mathcal{C}}(u)$ (all the other cases). Thus, we will consider the measure defined in Section 4.2 that characterizes a disequation by the indexes of its variables, that is $\mathcal{L}^1_{\mathcal{C}}(u \neq^? v)$. We also extend this measure to disjunction of disequations as follows:

$$\mathcal{L}^1_{\mathcal{C}}(\bigvee_i^n u_i \neq^? v_i) = \max\{\mathcal{L}^1_{\mathcal{C}}(u_i \neq^? v_i) \mid i = 1 \dots n\}$$

We use the lexicographic order $>_{\mathsf{lex}}$ to compare pairs of integers, i.e. $(i_1, i_2) >_{\mathsf{lex}} (j_1, j_2)$ if

- either $max(i_1, i_2) > max(j_1, j_2)$;
- or $max(i_1, i_2) = max(j_1, j_2)$ and $min(i_1, i_2) > min(j_1, j_2)$

Intuitively, the idea would be to measure all the values $\mathcal{L}^1_{\mathcal{C}}(D)$ for all disjunctions D in all constraint system $\mathcal{C}$ of the matrix. However, even if this measure will never increase on a single disjunction of disequations after application of any rule, it is not enough to ensure termination. Indeed, the rule EQ-DED-DED adds new disjunctions of disequations in all constraint systems of the matrix when the guess done by the rule is not satisfied. However, these disequations are all the same up to renaming of first order variables. Thus, we establish a measure that will avoid counting these particular disequations several times. For that we will rely on the recipes that were used in parameters of the rule EQ-DED-DED as follows.

Let us first define the measure $\mathcal{L}^2_{\mathcal{C}}(\beta)$ where β is a context of recipes:

$$\mathcal{L}^2_{\mathcal{C}}(\beta) = \max\{i \mid (w \cdot ax_i) \in st(\beta) \text{ or } (X, i \vdash^? x) \in D(\mathcal{C}) \text{ with } X \in st(\beta)\}$$

Note that at this stage of the strategy, our matrix contains constraint systems having the same shapre, and thus the same deducibility constraints up to a renaming of the first order variables. Hence, given a matrix $\mathcal{M}$ containing at least one constraint system $\mathcal{C}$ different from bottom, we denote $\mathcal{L}^2_{\mathcal{M}}(\beta) = \mathcal{L}^2_{\mathcal{C}}(\beta)$. We can now define our measure similar to $\mathcal{L}^1_{\mathcal{C}}()$ but specific to disequations of context of recipes, denoted $\mathcal{L}^2_{\mathcal{M}}()$ and defined as follows: $\mathcal{L}^2_{\mathcal{M}}(\xi \neq^? \beta) = (\mathcal{L}^2_{\mathcal{M}}(\xi); \mathcal{L}^2_{\mathcal{M}}(\beta))$. We use the same lexicographic order $>_{\mathsf{lex}}$ to compare pairs of integers. Lastly, we also extend this notion to disjunction of disequations such that:

$$\mathcal{L}^2_{\mathcal{M}}(\bigvee_i^n \beta_i \neq^? \beta'_i) = \max\{\mathcal{L}^2_{\mathcal{M}}(\beta_i \neq^? \beta'_i) \mid i = 1 \dots n\}$$

Even though we defined a measure for any disequations of context of recipes, we do not want to consider all of them. Remember that these disequations should represent the disequations between messages that appear into the matrices we consider. In particular, if D is a disjunction of context of recipes representing the disjunction D in $\mathcal{C}$ then we want that $\mathcal{L}^2_{\mathcal{M}}(\mathsf{D}) = \mathcal{L}^1_{\mathcal{C}}(D)$. Therefore, we define a set of disjunction of disequations of contexts, denoted $\mathcal{D}_\Pi(\mathcal{M})$, that satisfy this identity:

$$\mathcal{D}_\Pi(\mathcal{M}) = \left\{ \begin{array}{l|l} (\bigvee_{i=1}^n \beta_i \neq^? \beta'_i)\}\!\!\downarrow & \exists j \in \{1,\ldots,n\}. X \in vars^2(\beta_j), X' \in vars^2(\beta'_j) \text{ s.t.} \\ & \mathcal{L}^2_{\mathcal{M}}(\bigvee_{i=1}^n \beta_i \neq^? \beta'_i) = \mathcal{L}^2_{\mathcal{M}}(\beta_j \neq^? \beta'_j), \\ & \mathcal{L}^2_{\mathcal{M}}(\beta_j) = \mathcal{L}^2_{\mathcal{M}}(X) \text{ and } \mathcal{L}^2_{\mathcal{M}}(\beta'_j) = \mathcal{L}^2_{\mathcal{M}}(X') \end{array} \right\}$$

Note that the normalisation of disjunction of disequations of context of recipes, denoted by $\mathsf{D}\}\!\!\downarrow$, is formally defined by the rule:

$$\mathsf{D} \vee \mathsf{f}(\xi_1,\ldots,\xi_n) \neq^? \mathsf{f}(\beta_1,\ldots,\beta_n) \rightsquigarrow \mathsf{D} \vee \xi_1 \neq^? \beta_1 \vee \ldots \vee \xi_n \neq^? \beta_n$$

Given a constraint system $\mathcal{C}$ and a disjunction $\mathsf{D} = \bigvee_{i=1}^n \beta_i \neq^? \beta'_i$, we denote $F_{\mathcal{C}}(\mathsf{D}) = \left(\bigvee_i^n \beta_i \delta^1(\mathcal{C}) \neq^? \beta'_i \delta^1(\mathcal{C})\right)\!\!\downarrow$. Thanks to the origination property satisfied by our constraint systems, we can easily prove that for all constraint system $\mathcal{C}$ in $\mathcal{M}$, for all $\mathsf{D} \in \mathcal{D}_\Pi(\mathcal{M})$, $\mathcal{L}^2_{\mathcal{M}}(\mathsf{D}) = \mathcal{L}^1_{\mathcal{C}}(D)$. Moreover, for any disjunction of disequations of context of recipes D, if $\mathsf{D} \notin \mathcal{D}_\Pi(\mathcal{M})$ then $\mathcal{L}^2_{\mathcal{M}}(\mathsf{D}) > \mathcal{L}^1_{\mathcal{C}}(D)$ where $D = \mathsf{D}\delta^1(\mathcal{C})\!\!\downarrow$.

We define *the general measure on matrices*, denoted $\mu_{gen}()$, as follows. Let $(\mathcal{M}, \mathcal{M}')$ be a pair of matrices of constraint systems. W.l.o.g. let us assume that $\mathcal{M}$ contains at least one constraint system different from bottom. Let $S = \{\mathcal{C} \text{ in } \mathcal{M} \text{ or } \mathcal{M}'\}$. We have:

$$\mu^1_{gen}(\mathcal{M}, \mathcal{M}') = \left\{\!\!\left\{ \mathcal{L}^1_{\mathcal{C}}(D) \;\middle|\; \begin{array}{l} \mathcal{C} \in S,\, E(\mathcal{C}) = E \wedge D \\ \text{for some } E \text{ and some disjunction } D \\ \forall D' \in \mathcal{D}_\Pi(\mathcal{C}), F_{\mathcal{C}}(D') \neq D \end{array} \right\}\!\!\right\}$$

$$\mu^2_{gen}(\mathcal{M}, \mathcal{M}') = \left\{\!\!\left\{ \mathcal{L}^2_{\mathcal{M}}(\mathsf{D}) \;\middle|\; \begin{array}{l} \mathsf{D} \in \mathcal{D}_\Pi(\mathcal{M}) \text{ and } \exists \mathcal{C} \text{ in } \mathcal{M} \text{ or } \mathcal{M}' \text{ s.t.} \\ E(\mathcal{C}) = E \wedge D \text{ for some } E \text{ and} \\ F_{\mathcal{C}}(\mathsf{D}) = D \end{array} \right\}\!\!\right\}$$

$$\mu_{gen}(\mathcal{M}, \mathcal{M}') = \mu^1_{gen}(\mathcal{M}, \mathcal{M}') \cup \mu^2_{gen}(\mathcal{M}, \mathcal{M}')$$

Intuitively, $\mu^1_{gen}(\mathcal{M}, \mathcal{M}')$ represents the measure for the inequations that are not matched by the Eq-ded-ded rule yet. On the other hand, $\mu^2_{gen}(\mathcal{M}, \mathcal{M}')$ represents the measure for the inequation that were matched at one point in the strategy by the rule Eq-ded-ded.

Lemma 71. *Let $(\mathcal{M}, \mathcal{M}')$ be a pair of matrices obtained during Step b of the second phase. Assume that there exists $(\mathcal{M}_{bc}, \mathcal{M}'_{bc})$, different from $(\mathcal{M}, \mathcal{M}')$ obtained at the end of Step c of the second phase such that $(\mathcal{M}, \mathcal{M}') \rightarrow^* (\mathcal{M}_{bc}, \mathcal{M}'_{bc})$. In such a case, $\mu_{gen}(\mathcal{M}_{bc}, \mathcal{M}'_{bc}) < \mu_{gen}(\mathcal{M}, \mathcal{M}')$.*

Proof. Since $(\mathcal{M}_{bc}, \mathcal{M}'_{bc})$ is different from $(\mathcal{M}, \mathcal{M}')$, we can deduce that there exists at least one instance of a rule Eq-ded-ded, Cons or Axiom that is applied on $(\mathcal{M}, \mathcal{M}')$. Let us denote $(\mathcal{M}_1, \mathcal{M}'_1)$ be the pair of matrices obtained by application of such instance

of rule on $(\mathcal{M}, \mathcal{M}')$ and such that $(\mathcal{M}, \mathcal{M}') \to (\mathcal{M}_1, \mathcal{M}'_1) \to^* (\mathcal{M}_{bc}, \mathcal{M}'_{bc})$. Note that $(\mathcal{M}_1, \mathcal{M}'_1)$ may correspond to the case where the guess of the rule is satisfied, as well as the case where the guess is not satisfied.

The proof of this result will first consist of proving that in general the measure $\mu_{gen}(\mathcal{M}, \mathcal{M}')$ never increases. In particular:

1. If the rule applied is Cons or Axiom then $\mu_{gen}(\mathcal{M}_1, \mathcal{M}'_1) \leq \mu_{gen}(\mathcal{M}, \mathcal{M}')$;
2. If the rule applied is Eq-ded-ded and $(\mathcal{M}_1, \mathcal{M}'_1)$ corresponds to the case where the guess of the rule is satisfied then $\mu_{gen}(\mathcal{M}_1, \mathcal{M}'_1) \leq \mu_{gen}(\mathcal{M}, \mathcal{M}')$

Thus, one can note that we never show that the measure strictly decrease and the case of the rule Eq-ded-ded with a guess not satisfied is not covered. In fact, following these two properties, we will show that since $(\mathcal{M}_{bc}, \mathcal{M}'_{bc})$ is at the end of Step c (*i.e.* no more rule Axiom applicable), then

3. If the rule applied is Axiom and $(\mathcal{M}, \mathcal{M}')$ is at the beginning of Step c then $\mu_{gen}(\mathcal{M}_{bc}, \mathcal{M}'_{bc}) < \mu_{gen}(\mathcal{M}, \mathcal{M}')$;
4. If the rule applied is Eq-ded-ded and $(\mathcal{M}_1, \mathcal{M}'_1)$ corresponds to the case where the guess of the rule is not satisfied, then either $\mu_{gen}(\mathcal{M}_1, \mathcal{M}'_1) \leq \mu_{gen}(\mathcal{M}, \mathcal{M}')$ or else $\mu_{gen}(\mathcal{M}_{bc}, \mathcal{M}'_{bc}) < \mu_{gen}(\mathcal{M}, \mathcal{M}')$.

The last property is probably the most technical. Indeed, we will show that in some particular cases, the application of Eq-ded-ded will increase the measure (*i.e.* $\mu_{gen}(\mathcal{M}_1, \mathcal{M}'_1) > \mu_{gen}(\mathcal{M}, \mathcal{M}')$) but in the long run (*i.e.* at the end of the cycle) the measure will still strictly decrease (*i.e.* $\mu_{gen}(\mathcal{M}_{bc}, \mathcal{M}'_{bc}) < \mu_{gen}(\mathcal{M}, \mathcal{M}')$).

Therefore, by Properties 1,2 and 4, we can apply a simple induction on the length of derivation $(\mathcal{M}, \mathcal{M}') \to^* (\mathcal{M}_{bc}, \mathcal{M}'_{bc})$ proving that $\mu_{gen}(\mathcal{M}_{bc}, \mathcal{M}'_{bc}) \leq \mu_{gen}(\mathcal{M}, \mathcal{M}')$. Moreover, if no rule Axiom was applied in the derivation then it means $(\mathcal{M}_{bc}, \mathcal{M}'_{bc})$ is in solved form or else by Property 3 we have that $\mu_{gen}(\mathcal{M}_{bc}, \mathcal{M}'_{bc}) < \mu_{gen}(\mathcal{M}, \mathcal{M}')$.

We first focus on the evolution of $\mu_{gen}(\mathcal{M}, \mathcal{M}')$ by application of an instance of a rule Cons, Eq-ded-ded or Axiom when the guess is satisfied.

Let us consider a disequation that induces an element in $\mu^1_{gen}(\mathcal{M}, \mathcal{M}')$. Hence, w.l.o.g., consider $\mathcal{C} \in \mathcal{M}$ such that $E(\mathcal{C}) = E \wedge D$ for some E and some disjunction D and such that for all $\mathsf{D} \in \mathcal{D}_\Pi(\mathcal{M})$, $F_{\mathcal{C}}(\mathsf{D}) \neq D$. Moreover, let us denote $\mathcal{C}_1$ the constraint systems obtained from $\mathcal{C}$ after application of the rule and assume that $\mathcal{C}_1$ is the constraint system. For any instance of any of these rules, a substitution $\sigma = \{x \to u\}$ is applied on $\mathcal{C}$ to obtain $\mathcal{C}_1$ where $\mathcal{L}^1_{\mathcal{C}}(x) \geq \mathcal{L}^1_{\mathcal{C}}(u)$. Thus, we obtain that $\mathcal{L}^1_{\mathcal{C}}(D) \geq \mathcal{L}^1_{\mathcal{C}}(D\sigma\downarrow)$. Hence, if $D\sigma\downarrow$ induces an element in $\mu^1_{gen}(\mathcal{M}_1, \mathcal{M}'_1)$, then it is smaller than the element induced by D in $\mu^1_{gen}(\mathcal{M}, \mathcal{M}')$. Moreover, since we know that for all $\mathsf{D} \in \mathcal{D}_\Pi(\mathcal{M})$, $\mathcal{L}^2_{\mathcal{M}}(\mathsf{D}) = \mathcal{L}^1_{\mathcal{C}}(F_{\mathcal{C}}(\mathsf{D}))$, then even if $D\sigma\downarrow$ induces an element in $\mu^2_{gen}(\mathcal{M}_1, \mathcal{M}'_1)$ through some disjunction $\mathsf{D} \in \mathcal{D}_\Pi(\mathcal{M})$, this element would still be smaller than the one induced by D in $\mu^1_{gen}(\mathcal{M}, \mathcal{M}')$.

Let us now consider a disequation that induces an element in $\mu^2_{gen}(\mathcal{M}, \mathcal{M}')$. In such a case, there exists $\mathsf{D} \in \mathcal{D}_\Pi(\mathcal{M})$ and some constraint systems $\mathcal{C}_1, \ldots, \mathcal{C}_n$ in $\mathcal{M}$ or $\mathcal{M}'$, and disjunctions $D_1, \ldots, D_n$ such that for all $i \in \{1, \ldots, n\}$, $F_{\mathcal{C}_i}(\mathsf{D}) = D_i$ and $E(\mathcal{C}_i) = E_i \wedge D_i$ for some E_i. Moreover, let us denote $\mathcal{C}'_1, \ldots, C'_n$ the constraint systems

in $(\mathcal{M}_1, \mathcal{M}'_1)$ resulting of the application of the rule on respectively $\mathcal{C}_1, \ldots, C_n$. As we already mentioned, for any instance of the rules Cons, Eq-ded-ded or Axiom, for all $i \in \{1, \ldots, n\}$, a substitution $\sigma_i = \{x_i \to u_i\}$ is applied on $E(\mathcal{C}_i)$. We will show that either (a) there exists θ such that $\mathsf{D}\theta\downarrow \in \mathcal{D}_\Pi(\mathcal{M}_1)$, $\mathcal{L}^2_{\mathcal{M}_1}(\mathsf{D}\theta\downarrow) \leq \mathcal{L}^2_{\mathcal{M}}(\mathsf{D})$ and $D_i\sigma\downarrow = F_{\mathcal{C}'_i}(\mathsf{D}\theta\downarrow)$ for all $i = 1 \ldots n$; or else (b) $\mathcal{L}^1_{\mathcal{C}'_i}(D_i\sigma\downarrow) < \mathcal{L}^2_{\mathcal{M}}(\mathsf{D})$ for all $i = 1 \ldots n$.

By definition of the rule Cons, Eq-ded-ded and Axiom, we know that there exists $X \in \mathcal{X}^2$ such that $(X, k \vdash^? x_i) \in D(\mathcal{C}_i)$ for all $i \in \{1, \ldots, n\}$. Moreover, there also exists a context of recipes β such that for all $i \in \{1, \ldots, n\}$, $u_i = \beta\delta^1(\mathcal{C}_i)$ and $\mathcal{L}^2_{\mathcal{M}_1}(\beta) \leq \mathcal{L}^2_{\mathcal{M}}(X)$. Typically, when the rule is Axiom with path as parameter, then β is path; when the rule is Cons with f as parameter, then β is $\mathsf{f}(Y_1, \ldots, Y_m)$ with $Y_1, \ldots, Y_m$ the fresh recipe variables created by the rule; and when the rule $Eqrr$ is applied with parameter ξ then $\beta = \xi$. Therefore, we can easily deduce that $\mathcal{L}^2_{\mathcal{M}_1}(\mathsf{D}\theta\downarrow) \leq \mathcal{L}^2_{\mathcal{M}}(\mathsf{D})$ and for all $i \in \{1, \ldots, n\}$, $D_i\sigma\downarrow = F_{\mathcal{M}_1}(\mathsf{D}\theta\downarrow)$.

If $\mathsf{D}\theta\downarrow \in \mathcal{D}_\Pi(\mathcal{M}_1)$ then we satisfy point (a). Else let us assume that $\mathsf{D}\theta\downarrow \notin \mathcal{D}_\Pi(\mathcal{M}_1)$. But in such a case, we know that $\mathcal{L}^1_{\mathcal{M}_1}(F_{\mathcal{M}_1}(\mathsf{D}\theta\downarrow)) < \mathcal{L}^2_{\mathcal{M}_1}(\mathsf{D}\theta\downarrow)$. Hence we can deduce that for all $i \in \{1, \ldots, n\}$, $\mathcal{L}^1_{\mathcal{C}'_i}(D_i\sigma\downarrow) < \mathcal{L}^2_{\mathcal{M}}(\mathsf{D})$ hence we satisfy point (b).

Let us now focus on the evolution of $\mu_{gen}(\mathcal{M}, \mathcal{M}')$ by application of a rule Cons or Axiom when the guess is not satisfied. When these rules are applied, the disequations are either not modified by the rule or some of them are removed by normalisation. Thus, in such a case, we trivially have that $\mu_{gen}(\mathcal{M}_1, \mathcal{M}'_1) \leq \mu_{gen}(\mathcal{M}, \mathcal{M}')$. This allows us to conclude that Properties 1 and 2 hold.

We now focus on Property 3 hence we assume that the rule Axiom is applied on $(\mathcal{M}, \mathcal{M}')$. Let us observer the state of any disjunction $D = \vee_{i=1}^n x_i \neq^? u_i$ in any constraint system $\mathcal{C}$ in $\mathcal{M}$ or $\mathcal{M}'$: Either D is in fact a unique disequation $D = x_1 \neq^? u_1$ where u_1 does not contain names and $\mathcal{L}^1_{\mathcal{C}}(u_1) \leq \mathcal{L}^1_{\mathcal{C}}(x_1)$; or else for all $i \in \{1, \ldots, n\}$, one of the following properties holds:

- $u_i \in \mathcal{N}$.
- $u_i \in \mathcal{X}$, $E_\Pi(\mathcal{C}) \vDash \mathsf{root}(X_i) \neq^? \mathsf{f}$ and $E_\Pi(\mathcal{C}) \nvDash \mathsf{root}(Y_i) \neq^? \mathsf{g}$ for all $\mathsf{f}, \mathsf{g} \in \mathcal{F}_c$ where $X_i\delta^1(\mathcal{C}) = x_i$ and $Y_i\delta^1(\mathcal{C}) = u_i$.
- $\mathsf{root}(u_i) \in \mathcal{F}_c$ and for all $\mathsf{f} \in \mathcal{F}_c$, $E_\Pi(\mathcal{C}) \vDash \mathsf{root}(X_i) \neq^? \mathsf{f}$ where $X\delta^1(\mathcal{C}) = x_i$.

These properties are consequences of the rules Cons and Eq-ded-ded not being applicable anymore. Note that these properties are given by Lemma 30.

One can notice that either u_i is a name or $E_\Pi(\mathcal{C})$ satisfies the disequations $\mathsf{root}(X_i) \neq^? \mathsf{f}$ where $X_i\delta^1(\mathcal{C}) = x_i$. This means that the rule Axiom will be applied with all the variables $X_1, \ldots, X_n$ unless D becomes trivially true or false by normalisation. Let us denote σ the substitution corresponding to the different applications of the rules Axiom from $(\mathcal{M}, \mathcal{M}')$ to $(\mathcal{M}_{bc}, \mathcal{M}'_{bc})$, meaning that either $D\sigma\downarrow$ is either true, or false, or is in $E(\mathcal{C}_{bc})$. But in the latter case, the origination property satisfied by all the constraint systems ensures us that $\mathcal{L}^1_{\mathcal{C}_{bc}}(x_i\sigma) < \mathcal{L}^1_{\mathcal{C}}(x_i)$ for all $i \in \{1, \ldots, n\}$. Hence, we deduce that $\mathcal{L}^1_{\mathcal{C}_{bc}}(D\sigma\downarrow) < \mathcal{L}^1_{\mathcal{C}}(D)$. Also note that even if D was inducing an element in $\mu^2_{gen}(\mathcal{M}, \mathcal{M}')$ through a disjunction D, since we know that $\mathcal{L}^1_{\mathcal{C}}(D) = \mathcal{L}^2_{\mathcal{M}}(\mathsf{D})$, we have that $\mathcal{L}^1_{\mathcal{C}_{bc}}(D\sigma\downarrow) < \mathcal{L}^2_{\mathcal{M}}(\mathsf{D})$. Moreover, since the same reasonning can be applied on all disjunction D' in any other constraint system $\mathcal{C}'$ such that $D' = F_{\mathcal{C}'}(\mathsf{D})$, we deduce that

the element $\mathcal{L}^2_{\mathcal{M}}(\mathsf{D})$ in $\mu_{gen}(\mathcal{M}, \mathcal{M}')$ is in fact replaced by several strictly smaller elements in $\mu_{gen}(\mathcal{M}_{bc}, \mathcal{M}'_{bc})$. This allows us to conclude that $\mu_{gen}(\mathcal{M}_{bc}, \mathcal{M}'_{bc}) < \mu_{gen}(\mathcal{M}, \mathcal{M}')$.

Let us now focus on the last property, that is when the rule Eq-ded-ded is applied and the guess is not satisfied. Once again, we do a case analysis on the disequation that triggered the application of the rule Eq-ded-ded.

Assume first that the disequation induces an element in $\mu^1_{gen}(\mathcal{M}, \mathcal{M}')$. Hence, w.l.o.g., consider $\mathcal{C} \in \mathcal{M}$ such that $E(\mathcal{C}) = E \wedge D$ for some E and some disjunction D and such that for all $\mathsf{D} \in \mathcal{D}_\Pi(\mathcal{M})$, $F_{\mathcal{C}}(\mathsf{D}) \neq D$. Moreover, assume that $D = D' \vee x \neq^? u$ for some disjunction D' and for some terms x, u such that $x \neq^? u$ triggers the application of Eq-ded-ded with parameters X and ξ. By definition of the rule Eq-ded-ded, we know that $X\delta^1(\mathcal{C}) = x$ and $\xi\delta^1(\mathcal{C}) = u$. Moreover, the application of the rule on $\mathcal{C}$ will add the disequation $x \neq^? u$ in $E(\mathcal{C})$ but will also remove the disjunction D by normalisation ($x \neq^? u$ implies $D' \vee x \neq^? u$). Hence, $E(\mathcal{C}_1) = E \wedge x \neq^? u$ and so the element $\mathcal{L}^1_{\mathcal{C}}(D)$ in $\mu^1_{gen}(\mathcal{M}, \mathcal{M}')$ is replaced by $\mathcal{L}^2_{\mathcal{M}_1}(X \neq^? \xi)$ in $\mu^2_{gen}(\mathcal{M}_1, \mathcal{M}'_1)$. Note that since in any other constraint systems $\mathcal{C}'$ of the matrices, only the disequation $X\delta^1(\mathcal{C}') \neq^? \xi\delta^1(\mathcal{C}')$ is added. Hence they are captured by the element $\mathcal{L}^2_{\mathcal{M}_1}(X \neq^? \xi)$ in $\mu^2_{gen}(\mathcal{M}_1, \mathcal{M}'_1)$. But $\mathcal{L}^1_{\mathcal{C}}(D) \geq \mathcal{L}^1_{\mathcal{C}}(x \neq^? u) = \mathcal{L}^2_{\mathcal{M}_1}(X \neq^? \xi)$ hence we deduce that $\mu_{gen}(\mathcal{M}_1, \mathcal{M}'_1) \leq \mu_{gen}(\mathcal{M}, \mathcal{M}')$.

Assume now that the disequation induces an element in $\mu^2_{gen}(\mathcal{M}, \mathcal{M}')$. In such a case, there exists $\mathsf{D} \in \mathcal{D}_\Pi(\mathcal{M})$ and constraint systems $\mathcal{C}_1, \ldots, \mathcal{C}_n$ in $\mathcal{M}$ or $\mathcal{M}'$, and disjunctions $D_1, \ldots, D_n$ such that for all $i \in \{1, \ldots, n\}$, $F_{\mathcal{C}_i}(\mathsf{D}) = D_i$ and $E(\mathcal{C}_i) = E_i \wedge D_i$ for some E_i. Moreover, w.l.o.g we can assume that $D_1 = D'_1 \vee x \neq^? u$ where $x \neq^? u$ triggered the application of the rule Eq-ded-ded. We have to consider whether or not $\mathsf{D} = \mathsf{D}' \vee X \neq^? \xi$ such that $X\delta^1(\mathcal{C}_1) = x$ and $\xi\delta^1(\mathcal{C}_1) = u$.

When such decomposition of D exists, then it implies that for all $i \in \{1, \ldots, n\}$ there exists D'_i such that $D_i = D'_i \vee (X\delta^1(\mathcal{C}_i) \neq^? \xi\delta^1(\mathcal{C}_i))$. Thus, the application of the rule Eq-ded-ded on $\mathcal{C}_i$ will add the disequation $X\delta^1(\mathcal{C}_i) \neq^? \xi\delta^1(\mathcal{C}_i)$ but also remove the disjunction D_i by normalisation. Hence, the element $\mathcal{L}^2_{\mathcal{M}}(\mathsf{D})$ in $\mu^2_{gen}(\mathcal{M}, \mathcal{M}')$ will be replaced by the element $\mathcal{L}^2_{\mathcal{M}_1}(X \neq^? \xi)$ in $\mu^2_{gen}(\mathcal{M}_1, \mathcal{M}'_1)$. Since $\mathsf{D} = \mathsf{D}' \vee X \neq^? \xi$ and so $\mathcal{L}^2_{\mathcal{M}_1}(X \neq^? \xi) \leq \mathcal{L}^2_{\mathcal{M}}(\mathsf{D})$, we deduce that $\mu_{gen}(\mathcal{M}_1, \mathcal{M}'_1) \leq \mu_{gen}(\mathcal{M}, \mathcal{M}')$.

Now let us assume that such decomposition of D does not exist. It implies in fact that the disequation $x \neq^? u$ is derived from a disequation of context of recipe of the form $\mathsf{path} \neq^? \xi$, meaning that $(\mathsf{path}\,\delta^1(\mathcal{C}) \neq^? \xi\delta^1(\mathcal{C}))\downarrow = D''_1 \vee x \neq^? u$ for some D''_1. Intuitively, it indicates that the disequation $x \neq^? u$ was generated by the application of a rule Axiom during the previous cycle. Thanks to the origination property satisfied by constraint systems, we can also deduce that $\mathcal{L}^2_{\mathcal{M}}(\mathsf{path} \neq^? \xi) > \mathcal{L}^1_{\mathcal{C}_1}(x \neq u)$. In summary, we have that $\mathsf{D} = \mathsf{D}' \vee \mathsf{path} \neq^? \xi$ and $D_1 = D'_1 \vee x \neq^? u$ such that $\mathcal{L}^2_{\mathcal{M}}(\mathsf{path} \neq^? \xi) > \mathcal{L}^1_{\mathcal{C}_1}(x \neq u)$. Moreover, the application of Eq-ded-ded will add the disequation $x \neq^? u$ and remove the disjunction D_1 due to the normalisation in $\mathcal{C}_1$.

The main difficulty here is that in all the other constraint system $\mathcal{C}_2, \ldots, \mathcal{C}_n$, the normalisation will not necessarily remove the disjunctions $D_2, \ldots, D_n$. Hence, $\mathcal{L}^2_{\mathcal{M}}(\mathsf{D})$ will continue to be in $\mu^2_{gen}(\mathcal{M}_1, \mathcal{M}'_1)$ and we also added the element $\mathcal{L}^2_{\mathcal{M}}(X \neq^? \xi)$ in $\mu^2_{gen}(\mathcal{M}_1, \mathcal{M}'_1)$, all of that implying that $\mu_{gen}(\mathcal{M}_1, \mathcal{M}'_1) > \mu_{gen}(\mathcal{M}, \mathcal{M}')$ meaning that the measure does not decrease at this step and even increase. In fact, we can show that even if the measure increases after application of the rule Eq-ded-ded, the measure will strictly decrease at end of Step *c*, *i.e.,* after applying the different instances of the rules

AXIOM.

Indeed, by definition of $\mathsf{D} \in \mathcal{D}_\Pi(\mathcal{M})$, we know that there exists $Y \neq^? \beta$ such that $\mathsf{D} = \mathsf{D}'' \vee \mathsf{path} \neq^? \xi \vee Y \neq^? \beta$ for some D'' and such that $\mathcal{L}^2_{\mathcal{M}}(\mathsf{path} \neq^? \xi) \leq \mathcal{L}^2_{\mathcal{M}}(Y \neq^? \beta)$. But we also know that we only apply the rules EQ-DED-DED and CONS on the disequations with the biggest value $\mathcal{L}^1_{\mathcal{M}}()$ first. Therefore, since the application of EQ-DED-DED was possible on $x \neq^? u$ where $\mathcal{L}^1_{\mathcal{C}_1}(Y\delta^1(\mathcal{C}_1) \neq^? \beta\delta^1(\mathcal{C}_1)) > \mathcal{L}^1_{\mathcal{C}_1}(x \neq u)$, we can deduce that neither CONS or EQ-DED-DED were applicable on $Y\delta^1(\mathcal{C}_1) \neq^? \beta\delta^1(\mathcal{C}_1)$. By definition of the two rules, it implies that the disequation $\mathsf{root}(Y) \neq^? \mathsf{f}$ for all $\mathsf{f} \in \mathcal{F}_c$ are in $E_\Pi(\mathcal{C}_1)$. Thus, during Step c, either the disjunction $D_2, \ldots, D_n$ will all have become trivially true, or trivially false, or else the presence of $\mathsf{root}(Y) \neq^? \mathsf{f}$ will trigger the application of the rule AXIOM on Y. As we previously shown during the proof of Property 3, triggering applications of the rule AXIOM implies that the disjunctions D_i^{bc} in $(\mathcal{M}_{bc}, \mathcal{M}'_{bc})$ obtained from D_i in $(\mathcal{M}, \mathcal{M}')$ satisfy $\mathcal{L}^1_{\mathcal{C}_i^{bc}}(D_i^{bc}) < \mathcal{L}^1_{\mathcal{C}_i}(D_i)$ for all $i \in \{2, \ldots, n\}$ and where $\mathcal{C}_i^{bc}$ is the resulting constraint system by the successive applications of rules on $\mathcal{C}_i$. This allows us to conclude that the element $\mathcal{L}^2_{\mathcal{M}}(\mathsf{D})$ in $\mu^2_{gen}(\mathcal{M}, \mathcal{M}')$ was replaced by several strictly smaller elements $\mathcal{L}^1_{\mathcal{C}_i^{bc}}(D_i^{bc})$ in $\mu^1_{gen}(\mathcal{M}_{bc}, \mathcal{M}'_{bc})$, and so that $\mu_{gen}(\mathcal{M}_c, \mathcal{M}'_c) < \mu_{gen}(\mathcal{M}, \mathcal{M}')$. □

Proposition 2. *Let $(\mathcal{M}_1, \mathcal{M}'_1)$ be a pair of matrices obtained at the end of Phase 1 from a pair of sets of initial constraint systems (by following the strategy $\mathcal{S}$). Applying the transformation rules on $(\mathcal{M}_1, \mathcal{M}'_1)$ following strategy $\mathcal{S}$ as defined in Phase 2 terminates.*

Proof. The proof of termination of Phase 2 of the strategy is directly given by Lemmas 68, 69, 70 and 71 which respectively prove the termination of Step a, Step b, Step c and finally termination of the cycle Steps b/c. □