Constrained Narrowing for Conditional Equational Theories Modulo Axioms

Andrew Cholewa[1], Santiago Escobar[2], José Meseguer[1]

Abstract

For an unconditional equational theory (Σ, E) whose oriented equations $\vec{E}$ are confluent and terminating, narrowing provides an E-unification algorithm. This has been generalized by various authors in two directions: (i) by considering unconditional equational theories $(\Sigma, E \cup B)$ where the $\vec{E}$ are confluent, terminating and coherent modulo axioms B, and (ii) by considering conditional equational theories. Narrowing for a conditional theory $(\Sigma, E \cup B)$ has also been studied, but much less and with various restrictions. In this paper we extend these prior results by allowing conditional equations with extra variables in their conditions, provided the corresponding rewrite rules $\vec{E}$ are confluent, strictly coherent, operationally terminating modulo B and satisfy a natural *determinism* condition allowing incremental computation of matching substitutions for their extra variables. We also generalize the type structure of the types and operations in Σ to be order-sorted. The narrowing method we propose, called *constrained narrowing*, treats conditions as constraints whose solution is postponed. This can greatly reduce the search space of narrowing and allows notions such as *constrained variant* and *constrained unifier* that can cover symbolically possibly infinite sets of actual variants and unifiers. It also supports a *hierarchical* method of solving constraints. We give an inference system for hierarchical constrained narrowing modulo B and prove its soundness and completeness.

1. Introduction

Symbolic methods that describe infinite-state systems by means of constraints can be very useful in analyzing and verifying systems. Various kinds of symbolic techniques such as: (i) automata and grammars, e.g., [1, 15, 13, 14, 38, 66, 5, 4, 3, 33]; (ii) SMT and other forms of constraint solving, e.g., [6, 20, 35, 36, 64, 73, 75, 39, 11]; and (iii) narrowing [72, 30, 31, 9, 10], have been employed for this purpose. All are useful in their own way and can complement each other; and there is great interest in combining the power of these

Email addresses: acholew2@illinois.edu (Andrew Cholewa), sescobar@dsic.upv.es (Santiago Escobar), meseguer@illinois.edu (José Meseguer)

[1] University of Illinois at Urbana-Champaign, USA.

[2] DSIC-ELP, Universitat Politècnica de València, Spain.

different symbolic approaches to handle a wider range of applications [59, 60] (see, e.g., [70] and the survey [58] for combinations of this kind).

Narrowing, while generally less efficient that domain-specific approaches, is particulary attractive for system analysis because of its very wide applicability. Following the rewriting logic approach [56], a concurrent system can be naturally specified by a rewrite theory $\mathcal{R} = (\Sigma, E, R)$, where (Σ, E) is an equational theory specifying the distributed states as an algebraic data type, and R are rewrite rules specifying the system's concurrent transitions. Assuming that we have an E-unification algorithm, we can symbolically analyze by narrowing the behavior of our system, under reasonable assumptions on $\mathcal{R}$ [72], as follows. Instead of concrete system states, we can represent a possibly infinite set of such states by a *term* t with logical variables. We can then use narrowing modulo E to "symbolically execute" state transitions as narrowing steps $t \rightsquigarrow_{R,E} t'$, thus obtaining a useful form of symbolic reachability analysis and model checking with many applications [72, 30, 31, 9, 10] (see [58] for a survey of this work).

But where does the needed E-unification algorithm come from? Special-purpose narrowing algorithms only exist for specific, commonly occurring theories E; but the equations E of a system specification $\mathcal{R} = (\Sigma, E, R)$ can easily fall outside such specific theories. What we need is a *general-purpose* unification algorithm that will apply to a wide range of theories. And such a need is *answered by narrowing itself!* [44, 46]. That is, if the equations E in the theory (Σ, E) can be decomposed as $E = E_0 \uplus B$, where B is a set of equational axioms for which we do have a unification algorithm, and the equations E_0 can be oriented as rewrite rules $\vec{E}_0$ so that the rewrite theory $(\Sigma, B, \vec{E}_0)$ is convergent, then narrowing with $\vec{E}_0$ modulo B provides the desired E-unification algorithm [46]. Since the requirement that $(\Sigma, B, \vec{E}_0)$ is convergent is *de rigueur* for the equational part $E = E_0 \cup B$ of executable rewrite theories $\mathcal{R} = (\Sigma, E, R)$, this provides indeed a very general method of symbolic system analysis for $\mathcal{R}$. Note the interesting fact that narrowing then happens *at two levels*: at the *concurrent system* level as narrowing modulo E with a relation $t \rightsquigarrow_{R,E} t'$, and at the *equational level* to perform E-unification by narrowing with the relation $t \rightsquigarrow_{\vec{E}_0,B} t'$. Specifically, for narrowing at the equational level, *folding variant narrowing* [32] is the most effective method currently available, is supported by the Maude tool, and has been proved effective in the above-mentioned applications [30, 31, 9, 10].

However, as a generic unification method equational narrowing has two strong limitations: (i) unification may not be finitary and in general is only semi-decidable; and (ii) when a dedicated algorithm for the same theory exists, the dedicated algorithm is usually more efficient than the narrowing one. Variant unification modulo [32] has significantly improved this situation, since we currently have *four*, increasingly less efficient unification methods, and an associated way of gracefully trading off generality and efficiency, namely: (i) *dedicated, finitary* unification algorithms for specific theories or theory classes, which can be described by inference rules [45]; (ii) a *generic, finitary* unification algorithm based on folding variant narrowing [32] for any theory (Σ, E) decomposable as a convergent (including B-coherent) $(\Sigma, B, \vec{E}_0)$ if it has the finite variant property

[19] (FVP) and B-unification is finitary (see [29] for experiments comparing the performance of dedicated versus variant-based unification when E is FVP); (iii) a *generic, infinitary and semi-decidable* unification algorithm by folding variant narrowing for any equational theory as in (ii), but failing to be FVP (this can be seen as a greediest possible strategy supporting the approach in [46]); and (iv) when no confluence assumptions can be made on E, a *generic, infinitary and semi-decidable* unification algorithm by the inference rules in [34], which can be understood as a combination of (i) and [44] using a form of Knuth-Bendix completion. In general, of course, an equational theory may fall outside the "good" cases (i)-(ii). For example, in narrowing-based model checking applications, where we want to verify some temporal logic property of a rewrite theory $\mathcal{R} = (\Sigma, E, R)$ using the relation $t \rightsquigarrow_{R,E} t'$, as already mentioned, E *will* typically have a decomposition $(\Sigma, B, \vec{E}_0)$ falling within case (iii) above; but there may not be any way of pushing E into cases (i) or (ii). This is just a fact of life; actually, it can be viewed as an instance of the semi-decidability of general-purpose theorem proving. But, like for theorem proving, it does not prevent us from reasoning about our systems using complete methods.

There is, however, a further challenge, which we address in this paper. Even though in virtually all applications of interest the rewrite theory $(\Sigma, B, \vec{E}_0)$ associated to the equations E of a rewrite theory $\mathcal{R} = (\Sigma, E, R)$ is convergent, the equations $\vec{E}_0$ can often be *conditional* and, furthermore, the rules in $\vec{E}_0$ may have *extra variables* in their condition: the so-called strongly deterministic rules. Although there has been extensive work on conditional narrowing without axioms (i.e., $B = \emptyset$) (see, e.g., the survey of the literature in [63] and the discussion of related work in Section 9), much less is known about conditional narrowing modulo axioms B. This is further discussed in Section 9, but, for example, one of the few papers on the subject, by Bockmayr [12], assumes that there are no extra variables in the conditions of $\vec{E}_0$ and therefore leaves out many applications. Furthermore, since, as already mentioned, folding variant narrowing [32] seems at present the most effective approach for narrowing with unconditional equations $\vec{E}_0$ modulo axioms B, there are additional questions to be asked and answered, such as what a conditional notion of variant should look like, and how should such conditional variants be computed by narrowing. There is also a clear and present danger of *combinatorial explosion*, which can be extreme in the conditional case. For example, the approach presented in [12] and followed also by many other authors envisions narrowing not only on the terms being narrowed, but also on the *accumulated conditions* added after each narrowing step. After just a few steps this can lead to enormously big search spaces. Therefore, another key question to answer is: are there ways of *postponing* the evaluation of conditions so that we can obtain a much more manageable search space?

This paper studies conditional narrowing modulo axioms B for a very general class of convergent conditional rewrite theories $(\Sigma, B, \vec{E}_0)$ as a first, necessary step for applying the resulting variant and unification methods to the narrowing-based analysis of concurrent systems specified by rewrite theories of the form

$\mathcal{R} = (\Sigma, E_0 \cup B, R)$. And it addresses all the questions and challenges described above. Specifically, its main contributions can be summarized as follows:

1. A new notion of *constrained variant*, generalizing to the conditional case the notion of variant in [19, 32] and computed by a special type of constrained narrowing, is proposed. It shares constrained narrowing's economy of description and state-reduction advantages, so that a single constrained variant may symbolically encompass a huge, possibly infinite number of actual variants.

2. Likewise, a new notion of *constrained unifier*, also computed by a special type of constrained narrowing, is proposed. Again, a single constrained unifier may symbolically encompass a huge, possibly infinite number of actual unifiers.

3. A new hierarchical method, called *layered constrained narrowing*, to solve the accumulated conditions generated by constrained narrowing is also proposed and proved sound and complete. In particular this provides a method of extracting a complete set of actual variants (resp. actual unifiers) from a given constrained variant (resp. constrained unifier).

4. A new notion of *convergent conditional FPP rewrite theory* with particularly good executability properties, yet involving no real loss of generality (see Ex. 3), is also proposed. This notion is of interest not just for narrowing, but also for executable specification and equational programming.

5. Although an experimental evaluation of the narrowing algorithms developed in this work is beyond the scope of this paper, there are clear *a priori* reasons supporting the claim that these algorithms avoid as much as possible the danger of combinatorial explosion and should outperform those in previous approaches to conditional narrowing modulo. Specifically:

   - We follow the general constrained-based approach, e.g., [51, 18], to avoid evaluation of the accumulated conditions; this can yield a drastically smaller search space than standard approaches such as [12], where conditions are evaluated.

   - The use of *order-sorted* unification, e.g., [62, 42] is well-known to lead to search spaces that can be drastically smaller than those obtained by unsorted unification [76].

   - Even when after finding a constrained solution we wish to evaluate the constraint to extract actual solutions, our layered constraint narrowing method systematically exploits *frozen operators* [16] to drastically reduce both the amount of computation and the search space in condition evaluation.

   - In the unconditional case, *variant narrowing* [32] is the only practical complete strategy known at present to perform narrowing modulo axioms such as AC, and the greediest possible [32]. This work generalizes variant narrowing to the conditional case to make those advantages available for conditional narrowing.

- The narrowing paths are further restricted by imposing *irreducibility* conditions on the accumulated substitutions. This has been shown to be a key search space reduction technique in real applications such as cryptographic protocol analysis [28].

The rest of the paper is organized as follows. Preliminaries on order-sorted rewrite theories are presented in Section 2. Conditional rewriting modulo axioms and several proof systems for it are presented in Section 3. The key theories of current interest, namely, *convergent* rewrite theories are studied in Section 4. Section 5 contains core ideas such as: reachability problems and their solutions, constrained narrowing, and proofs of its soundness and completeness. Constrained variants and constrained unifiers are studied in Section 6. A useful theory transformation essential for layered constrained narrowing, and layered constrained narrowing itself are studied, respectively, in Sections 7 and 8. A discussion of related work and concluding remarks are gathered in Section 9.

2. Preliminaries on Order-Sorted Rewrite Theories

We follow the standard terminology and notation of term rewriting (see, e.g., [65, 7, 22, 71, 21]) order-sorted algebra [40, 57], and rewrite theories [56, 16]. Readers familiar with such terminology and notation can skip this section and proceed to Section 3. Recall the notions of order-sorted signature, term, substitution and equation. An order-sorted signature $(\Sigma, S, \leq)$ consists of a poset of sorts $(S, \leq)$ and an $S^* \times S$-indexed family of sets $\Sigma = \{\Sigma_{s_1 \ldots s_n, s}\}_{(s_1 \ldots s_n, s) \in S^* \times S}$ of function symbols. Throughout, Σ is assumed to be *preregular*, so that each term t has a least sort, denoted $ls(t)$ (see [40]). Σ is also assumed to be *kind-complete*, that is, for each sort $s \in S$ its connected component in the poset $(S, \leq)$ has a top sort, denoted $[s]$ and called the connected component's *kind*, and for each $f \in \Sigma_{s_1 \ldots s_n, s}$ there is also an $f \in \Sigma_{[s_1] \ldots [s_n], [s]}$. An order-sorted signature can always be extended to a kind-complete one. Maude automatically checks preregularity and adds a new "kind" sort $[s]$ at the top of the connected component of each sort $s \in S$ specified by the user, and automatically lifts each operator to the kind level. Finally, Σ is also assumed to be *sensible*, in the sense that for any two typings $f : s_1 \ldots s_s \longrightarrow s$ and $f : s'_1 \ldots s'_s \longrightarrow s'$ of an n-argument function symbol f, if s_i and s'_i are in the same connected component of $(S, \leq)$ for $1 \leq i \leq n$, then s and s' are also in the same connected component; this provides the right notion of *unambiguous* signature at the order-sorted level.

Given an S-sorted set $\mathcal{X} = \{\mathcal{X}_s\}_{s \in S}$ of *mutually disjoint* countably infinite sets of variables, $\mathcal{T}_\Sigma(\mathcal{X})_s$ denotes the set of Σ-terms of sort s with variables in $\mathcal{X}$, and $\mathcal{T}_\Sigma(\mathcal{X})$ denotes, ambiguously, both the S-sorted set of all Σ-terms with variables in $\mathcal{X}$, and the free Σ-algebra on those variables. Similarly, $\mathcal{T}_\Sigma$ denotes both the S-sorted set of all *ground* Σ-terms that have no variables, and the initial Σ-algebra. Σ is said to have *non-empty sorts* iff $\mathcal{T}_{\Sigma,s} \neq \emptyset$ for each sort s. $\mathcal{V}ar(t)$ denotes the set of variables appearing in term t.

A *substitution* is an S-sorted mapping $\sigma : \mathcal{X} \longrightarrow \mathcal{T}_\Sigma(\mathcal{X})$. We define its *domain*, denoted $Dom(\sigma)$, as the set $Dom(\sigma) = \{x \in \mathcal{X} \mid \sigma(x) \neq x\}$, and its *range*, denoted $Ran(\sigma)$, as the set $Ran(\sigma) = \{y \in \mathcal{X} \mid \exists x\ (x \in Dom(\sigma) \ \wedge\ y \in \mathcal{V}ar(\sigma(x)))\}$. σ can also be described more economically as the mapping $\sigma : Dom(\sigma) \longrightarrow \mathcal{T}_\Sigma(Ran(\sigma))$. Given a subset $\vec{x}$ of sorted variables in $\mathcal{X}$ and a substitution σ, $\sigma|_{\vec{x}}$, called the *restriction* of σ to $\vec{x}$, denotes the substitution mapping each $y \in \mathcal{X}$ to $\sigma(x)$ if $y \in \vec{x}$ and to y otherwise. Therefore, $Dom(\sigma|_{\vec{x}}) = Dom(\sigma) \cap \vec{x}$. The homomorphic extension $\sigma : \mathcal{T}_\Sigma(\mathcal{X}) \longrightarrow \mathcal{T}_\Sigma(\mathcal{X})$ is also denoted σ, and its application to a term t is denoted $t\sigma$. Composition of substitutions σ_1, σ_2 is denoted by juxtaposition, i.e., for any term t, $t(\sigma_1\sigma_2) = (t\sigma_1)\sigma_2$.

$Pos(t)$ denotes the set of positions (strings of naturals) of a Σ-term t, and t_p denotes the *subterm of t at position $p \in Pos(t)$*. Similarly, $Pos_\Sigma(t)$ denotes the *non-variable positions* of t, that is, those $p \in Pos(t)$ such that $t_p \notin \mathcal{V}ar(t)$. A term t with its subterm t_p replaced by the term t' is denoted $t[t']_p$.

For a Σ-equation $u = v$ to be well-formed, the sorts of u and v should be in the same connected component of $(S, \leq)$. A *conditional* Σ-equation is an implication $\bigwedge_{i=1,\ldots,n} u_i = v_i \Rightarrow l = r$ between Σ-equations, denoted from now on as: $l = r\ \mathit{if}\ \bigwedge_{i=1,\ldots,n} u_i = v_i$. A *conditional equational theory* is a pair (Σ, E) with Σ an order-sorted signature and E a set of conditional Σ-equations. An unconditional equation $u = v$ is the special case of a conditional equation with an empty condition $\top$. For E a set of conditional Σ-equations, $=_E$ denotes the provable E-equality relation [40, 57], and $[t]_E$ denotes the equivalence class of t modulo $=_E$.

Given a set E of Σ-equations, a substitution σ is an *E-unifier* of an equation $t = t'$ iff $t\sigma =_E t'\sigma$. Let $CSU_E(t, t')$ denote a complete set of most general E-unifiers of the equation $t = t'$, i.e., for any E-unifier ρ of $t = t'$, there is a substitution $\sigma \in CSU_E(t, t')$ and another substitution τ s.t. $\rho|_X =_E (\sigma\tau)|_X$ with $X = \mathcal{V}ar(t) \cup \mathcal{V}ar(t')$. Likewise, a substitution σ is an *E-match* from t to t' iff $t' =_E t\sigma$. Given two substitutions σ, τ, we call them *E-equal*, denoted $\sigma =_E \tau$, iff $\forall x \in \mathcal{X}\ \sigma(x) =_E \tau(x)$.

An unconditional equation $u = v$ is called *sort-preserving* iff for each well-sorted substitution θ we have $ls(u\theta) = ls(v\theta)$. Using substitutions that specialize variables to smaller sorts it can be easily checked whether an equation is sort-preserving (see [49]).

A *conditional order-sorted rewrite theory* is a triple $\mathcal{R} = (\Sigma, B, R)$, with Σ an order-sorted signature, B a set of unconditional Σ-equations, and R a set of conditional rewrite rules of the form $l \to r\ \mathit{if}\ \bigwedge_{i=1,\ldots,n} u_i \to v_i$, with *no restrictions* on the variables of l, r, or those of the u_i and v_i.

In general, the rewrite rules of a conditional rewrite theory $\mathcal{R}$ have a non-equational meaning as transition rules in a concurrent system [56, 58]. However, in this work we will focus for the most part on rewrite theories *with an equational interpretation*. That is, in the narrowing uses we study here, $\mathcal{R}$ will be of the form, $\mathcal{R} = (\Sigma, B, \vec{E})$, where $(\Sigma, E \cup B)$ is a conditional order-sorted equational theory, where the equations B are unconditional and the equations E are possibly conditional; and where $\vec{E}$ are conditional rewrite rules that interpret each conditional equation $l = r\ \mathit{if}\ \bigwedge_{i=1,\ldots,n} u_i = v_i$ as the conditional rewrite rule

$l \to r \ \mathit{if} \ \bigwedge_{i=1,\ldots,n} u_i \to v_i$. We call $\mathcal{R} = (\Sigma, B, \vec{E})$ the rewrite theory *associated* to the order-sorted conditional equational theory $(\Sigma, E \cup B)$ by choosing the equations B as axioms and *orienting* the conditional equations E as conditional rewrite rules.

Thererefore, rewriting with $\vec{E}$ is achieved *modulo* the unconditional equations B. Since the practical interest is in implementable uses of rewriting modulo B, we will assume that the provable B-equality relation $=_B$ is decidable and that B has a finitary B-matching algorithm; that is, an algorithm generating a complete finite set of B-matches from t to t', denoted $\mathit{Match}_B(t, t')$; that is, for any B-match σ there is a $\tau \in \mathit{Match}_B(t, t')$ such that for all $x \in \mathcal{V}ar(t)$ $\sigma(x) =_B \tau(x)$. For narrowing purposes we will also assume that B has a B-unification algorithm that can generate a set of most general B-unifiers $\mathit{CSU}_B(t, t')$ for each equation $t = t'$.

3. Proof Systems for Conditional Rewrite Theories

We present several proof systems for conditional rewriting modulo axioms. We also present basic notions and results from [61] on the strict coherence property for conditional rewrite rules that allows the rewrite relation $\to_{R/B}$ to be (bi-)simulated by the much simpler relation $\to_{R,B}$.

3.1. Standard Proof Systems

Given a rewrite theory $\mathcal{R} = (\Sigma, B, R)$, we follow closely the treatment in [61] to define the rewriting modulo B relation $\to_{R/B}$, and the easier to implement relation $\to_{R,B}$, by appropriate *inference systems.* The inference system[3] defining both $\to_{R/B}$ and $\to^\star_{R/B}$ when Σ has non-empty sorts is given as follows.

- **Reflexivity**. For each $t, t' \in \mathcal{T}_\Sigma(\mathcal{X})$ such that $t =_B t'$, $\dfrac{}{t \to^\star_{R/B} t'}$
- **Replacement**. For $l \to r \ \ \mathit{if} \ \ u_1 \to v_1 \wedge \ldots \wedge u_n \to v_n$ a rule in R, $t, u, v \in \mathcal{T}_\Sigma(\mathcal{X})$, $p \in \mathit{Pos}(t)$, and θ a substitution, such that $u =_B t[l\theta]_p$ and $v =_B t[r\theta]_p$,

$$\frac{u_1\theta \to^\star_{R/B} v_1\theta \quad \ldots \quad u_n\theta \to^\star_{R/B} v_n\theta}{u \to_{R/B} v}$$

[3] Modulo the fact that the relations $\to_{R/B}$ and $\to^\star_{R/B}$ are combined into a single relation, denoted $\to$, the inference system given here can easily be proved equivalent to the rewriting logic inference system in [56] (which works directly with B-equivalence classes) for the unsorted case, and to the generalized rewriting logic inference system in [16] when order-sorted equational logic is viewed as a sublogic of membership equational logic.

- **Transitivity** For $t_1, t_2, t_3 \in \mathcal{T}_\Sigma(\mathcal{X})$,

$$\frac{t_1 \rightarrow_{R/B} t_2 \qquad t_2 \rightarrow^{\star}_{R/B} t_3}{t_1 \rightarrow^{\star}_{R/B} t_3}$$

In general, the relation $u \rightarrow_{R/B} v$ may be undecidable, since checking whether $u \rightarrow_{R/B} v$ holds involves searching through the possibly infinite equivalence class $[u]_B$ to find a representative that can be rewritten with R and checking, furthermore, that the result u' of such rewriting belongs to the equivalence class $[v]_B$. For this reason, and for greater efficiency, a much simpler relation $\rightarrow_{R,B}$ is defined. The key idea about $\rightarrow_{R,B}$ is to replace general B-equalities of the form $u =_B t[l\theta]_p$ by a matching B-equality $t_p =_B l\theta$ with the subterm actually being rewritten. This completely eliminates any need for searching for a redex in the possibly infinite equivalence class $[u]_B$. Here is the inference system defining both $\rightarrow_{R,B}$ and $\rightarrow^{\star}_{R,B}$ when Σ has non-empty sorts.

- **Reflexivity**. For each $t, t' \in \mathcal{T}_\Sigma(\mathcal{X})$ such that $t =_B t'$, $\quad \dfrac{}{t \rightarrow^{\star}_{R,B} t'}$
- **Replacement**. For $l \rightarrow r \;\; \mathit{if} \;\; u_1 \rightarrow v_1 \wedge \ldots \wedge u_n \rightarrow v_n$ a rule in R, $t \in \mathcal{T}_\Sigma(\mathcal{X})$, $p \in \mathit{Pos}(t)$, and θ a substitution, such that $t_p =_B l\theta$,

$$\frac{u_1\theta \rightarrow^{\star}_{R,B} v_1\theta \;\; \ldots \;\; u_n\theta \rightarrow^{\star}_{R,B} v_n\theta}{t \rightarrow_{R,B} t[r\theta]_p}$$

- **Transitivity** For $t_1, t_2, t_3 \in \mathcal{T}_\Sigma(\mathcal{X})$,

$$\frac{t_1 \rightarrow_{R,B} t_2 \qquad t_2 \rightarrow^{\star}_{R,B} t_3}{t_1 \rightarrow^{\star}_{R,B} t_3}$$

For some applications, the above rewrite relation $\rightarrow_{R,B}$ can be restricted by a *frozenness map*[4] [16] $\phi : \Sigma \rightarrow \mathcal{P}(\mathbb{N})$, mapping each function symbol $f \in \Sigma$ with n arguments to a subset $\phi(f) \subseteq \{1, \ldots, n\}$ of the argument positions, below which rewriting is forbidden. For example, for *if* an if-then-else operator we may choose $\phi(\mathit{if}) = \{2, 3\}$ to forbid rewriting below the "then" and "else" branches and force instead evaluation by rewriting of the first argument (the Boolean condition). A frozenness map ϕ then defines the frozen positions of a Σ-term, where rewriting is forbidden, as follows:

Definition 1. *Let $\phi : \Sigma \rightarrow \mathcal{P}(\mathbb{N})$ be a frozenness map. Given a Σ-term t, a position $p \in Pos(t)$ is* frozen *by ϕ iff p can be decomposed as a string concatenation of the form $p = q \cdot i \cdot r$, with $t_q = f(u_1, \ldots, u_n)$ and $i \in \phi(f)$.*

[4] The notion of a frozenness map is *dual* to that of a restriction map $\mu : \Sigma \rightarrow \mathcal{P}(\mathbb{N})$ in *context-sensitive rewriting* (see, e.g., [52]): if f has n-arguments, $\{1, \ldots, n\} - \phi(f)$ defines an associated context-sensitive restriction map.

The above inference system for $\rightarrow_{R,B}$ and $\rightarrow^{\star}_{R,B}$ can be easily restricted to obtain an inference system for rewrite relations $\rightarrow_{R,B,\phi}$ and $\rightarrow^{\star}_{R,B,\phi}$ under frozenness restrictions ϕ, just by imposing to the **Replacement** rule the additional requirement that the position $p \in Pos(t)$ at which rewriting takes place is not frozen by ϕ. See Sections 1, 8, and 9, to appreciate the search space reduction uses of frozenness.

3.2. Strict Coherence of Conditional Rewrite Theories

Under suitable conditions of *strict coherence* on B and R explained below, the relations $\rightarrow^{\star}_{R/B}$ and $\rightarrow^{\star}_{R,B}$ coincide. This is very useful, since we can focus mostly on the much easier to implement rewrite relation $\rightarrow_{R,B}$. This will be exploited later to define constrained narrowing with R modulo B as a suitable generalization of the rewrite relation $\rightarrow_{R,B}$. In particular, the good properties of the constrained narrowing relation modulo B depend crucially on the strict coherence properties stated in Theorem 1 below.

Although the semantics of conditional ordered-sorted rewriting modulo B has been defined in Section 3.1 with no restrictions on B, when the equations B are non-linear and/or non-regular, the relations $\rightarrow_{R/B}$ and $\rightarrow_{R,B}$, although still relatable to each other under some conditions [47], lack a sufficiently good correspondence. As shown in [61], a considerably better correspondence between $\rightarrow_{R/B}$ and $\rightarrow_{R,B}$, called *strict coherence*, can be achieved for a conditional rewrite theory $\mathcal{R} = (\Sigma, B, R)$ if the axioms B are regular and linear and the conditional rules R are closed under so-called B-extensions, a notion going back to [67]. In this section we summarize some of the key notions and results from [61].

An equation $u = v$ is *regular* iff $\mathcal{V}ar(u) = \mathcal{V}ar(v)$, that is, both sides have the exact same variables. A term t is *linear* iff each of its variables occurs only once (at a single position) in t. An equation $u = v$ is *linear* iff both u and v are linear. The nilpotency equation $x * x = 0$ is neither regular nor linear.

To achieve the desired strict coherence property, from now on the equational axioms B in a rewrite theory $\mathcal{R} = (\Sigma, B, R)$ will always be regular, linear, sort-preserving, with $=_B$ decidable, have a finitary B-matching algorithm, and be *most general possible*, in the sense that for any $u = v \in B$, each $x \in \mathcal{V}ar(u = v)$ has a "kind" sort $[s]$ at the top of one the connected components in $(S, \leq)$. B being sort-preserving is extremely useful for performing *order-sorted* rewriting modulo B: when B-matching a subterm t_p against a rule's lefthand side to obtain a matching substitution σ, we need to check that σ is well-sorted, that is, that if a variable x has sort s, then some element in the B-equivalence class $[x\sigma]_B$ has also sort s. But since B is sort-preserving, this is equivalent to checking $ls(x\sigma) \leq s$. Of course, in the many-sorted and unsorted cases sort-preservation and greatest possible generality of the equations B are always satisfied, and all the assumptions on Σ boil down to Σ being unambiguous.

Strict coherence is the following property of the relation $\rightarrow_{R,B}$:

Definition 2. *[61] A rewrite theory $\mathcal{R} = (\Sigma, B, R)$ is called* strictly coherent *iff for any Σ-terms u, u', v if $u =_B u'$ and $u \rightarrow_{R,B} v$, then there exists a term*

v' such that $u' \to_{R,B} v'$ and $v =_B v'$. Adopting the convention of expressing existential quantifications by dotted lines, this property can be expressed by the diagram:

$$\begin{tikzcd} u \arrow[r, "R,B"'] \arrow[d, equal, "B"'] & v \arrow[d, dotted, dash, "B"] \\ u' \arrow[r, dotted, "R,B"'] & v' \end{tikzcd}$$

Under the above assumptions on B, $\mathcal{R} = (\Sigma, B, R)$ is strictly coherent if it is *closed under B-extensions*, in the following sense:

Definition 3. *[61] Let $\mathcal{R} = (\Sigma, B, R)$ be a conditional order-sorted rewrite theory, and let $l \to r$ if C be a rule in R, where C abbreviates the rule's condition. Without loss of generality we assume that $\mathcal{V}ar(B) \cap \mathcal{V}ar(l \to r \text{ if } C) = \emptyset$. If this is not the case,* only the variables of B *will be renamed; the variables of $l \to r$ if C will* never *be renamed. We then define the set of B-*extensions *of $l \to r$ if C as the set*[5]*:*

$$Ext_B(l \to r \text{ if } C) = \{u[l]_p \to u[r]_p \text{ if } C \mid u = v \in B \cup B^{-1} \wedge p \in Pos_\Sigma(u) - \{\epsilon\} \wedge CSU_B(l, u_p) \neq \emptyset\}$$

where, by definition, $B^{-1} = \{v = u \mid u = v \in B\}$.

Given two rules $l \to r$ if C and $l' \to r'$ if C with the same *condition C we say that $l \to r$ if C B-*subsumes[6] *$l' \to r'$ if C iff there is a substitution σ such that: (i) $Dom(\sigma) \cap \mathcal{V}ar(C) = \emptyset$, (ii) $l' =_B l\sigma$, and (iii) $r' =_B r\sigma$.*

We call $\mathcal{R} = (\Sigma, B, R)$ closed under B-extensions *iff for any rule $l \to r$ if C in R, each rule $l' \to r'$ if C in $Ext_B(l \to r \text{ if } C)$ is subsumed by some rule in R.*

A semi-algorithm to close a rewrite theory $\mathcal{R} = (\Sigma, B, R)$ under B-extensions under the above assumptions on B by computing for each rewrite rule $l \to r$ *if* C in R its extension closure $\overline{Ext}_B(l \to r \text{ if } C)$ is described in [61]. The main results about the strict coherence of rewrite theories closed under B-extensions can be summarized as follows:

Theorem 1. [61] *Let $\mathcal{R} = (\Sigma, B, R)$ satisfy all the above assumptions on B and Σ and be closed under B-extensions. Then $\mathcal{R}$ is* strictly coherent. *Furthermore:*

1. $\to^{\star}_{R/B} = \to^{\star}_{R,B}$

[5] Note that, because of the assumptions that Σ is kind-complete and that all $u = v \in B$ are most general possible and have variables whose sorts are tops of connected components in the sort poset $(S, \leq)$, the terms $u[l]_p$ and $u[r]_p$ are always well-formed Σ-terms.

[6] Note that for unconditional rules, since C is empty, we have $var(C) = \emptyset$, so that requirement (i) trivially holds for σ. Therefore, the conditional notion of subsumption yields the usual unconditional notion as a special case.

2. *if $u =_B u'$ and $u \to_{R,B} v$ at position p with a rule $l' \to r'$ if $C \in R$ and with substitution θ, then there exists a term v' such that $u' \to_{R,B} v'$ at some position q with a rule $l'' \to r''$ if $C \in R$ and with a substitution θ' such that: (i) $v =_B v'$, and (ii) for all $x \in \mathcal{V}ar(C)$ $x\theta = x\theta'$*

3. *Given any chain of $n \geq 0$ R,B-rewrite steps followed by a B-equality step of the form, $u \to_{R,B} u_1 \to_{R,B} u_2 \ldots u_{n-1} \to_{R,B} u_n =_B v$, where at each step a rule $l_i \to r_i$ if $C_i \in R$ has been applied with substitution θ_i, and given any term u' such that $u =_B u'$, there is another chain of $n \geq 0$ rewrite steps followed by a B-equality step of the form, $u' \to_{R,B} u'_1 \to_{R,B} u'_2 \ldots u'_{n-1} \to_{R,B} u'_n =_B v'$, such that: (i) $u_i =_B u'_i$, $1 \leq i \leq n$ and $v =_B v'$, where at each step a rule $l'_i \to r'_i$ if $C_i \in R$ has been applied with substitution θ'_i such that for all $x \in \mathcal{V}ar(C_i)$ $x\theta_i = x\theta'_i$, $1 \leq i \leq n$.* □

Remark 1. *In the above Theorem, (1) is an easy consequence of strict coherence because of the* **Reflexivity** *and* **Transitivity** *rules for $\to_{R,B}$. Note that (3) follows easily from (2). The key property for conditional narrowing, used crucially in the upcoming Lifting Lemma 4, is (2). It essentially means that if $u =_B u'$ and u can be rewritten to v with a conditional rule with a given substitution, then u' can also be rewritten to v' with $v =_B v'$ with the* same *rule and with the* same *substitution when we both substitutions are restricted to the variables in the condition. Because of the presence of extra variables in the condition, property (2) is non-trivial, yet essential.*

Not all frozenness maps ϕ are meaningful modulo a set of axioms B. The following definition imposes a simple requirement on ϕ to make it well-behaved when rewriting modulo axioms B:

Definition 4. *Given a strictly coherent theory $\mathcal{R} = (\Sigma, B, R)$ and a frozeness map $\phi : \Sigma \to \mathcal{P}(\mathbb{N})$, we say that ϕ is B-*stable *iff for any Σ-terms u, u', v if $u =_B u'$ and $u \to_{R,B,\phi} v$, then there exists a term v' such that $u' \to_{R,B,\phi} v'$ and $v =_B v'$. This property can be expressed by the diagram:*

$$\begin{tikzcd}
u \arrow[r, "{R,B,\phi}"'] \arrow[d, equal, "B"'] & v \arrow[d, dotted, dash, "B"] \\
u' \arrow[r, dotted, "{R,B,\phi}"'] & v'
\end{tikzcd}$$

For a simple example of a ϕ that is *not* B-stable, consider an unsorted theory with constants a, b and binary function symbol $+$, B the commutativity axiom $x + y = y + x$, and R the rule $a \to b$. This theory is closed under B-extensions (there are none) and therefore strictly coherent. The map ϕ with $\phi(+) = \{2\}$ is not B-stable, because $a + b \to_{R,B,\phi} b + b$, but $b + a$ *cannot* be rewriten with frozenness restrictions ϕ because position 2 is frozen.

3.3. Layered Proofs

For later uses in connection with narrowing, it will be useful to consider *layered proofs* of (conjunctions of) rewrites $u \to^{\star}_{R,B} v$ as an alternative inference system, yet equivalent to the proof system for $\to_{R,B}$ and $\to^{\star}_{R,B}$ in Section 3.1.

Given a conditional rewrite theory $\mathcal{R} = (\Sigma, B, R)$ we can be more general and consider as proof goals finite conjunctions of reachability goals

$$C = t_1 \to^{\star}_{R,B} t'_1 \wedge \cdots \wedge t_n \to^{\star}_{R,B} t'_n \tag{1}$$

We will use letters $C, D, C', D', \ldots$, for such conjunctions.

Proofs of the $\mathcal{R}$-reachability of such goals will be developed from left to right, trying to build an actual full trace for each $t_i \to^{\star}_{R,B} t'_i$ of the form:

$$t_i \to_{R,B} v_1 \to_{R,B} v_2 \to_{R,B} \cdots v_{n-1} \to_{R,B} v_n =_B t'_i \tag{2}$$

by applying rules in R modulo B. However, substitution instances of each rule's condition in each rewrite attempt will generate new reachability goals *one layer up*, which may, in turn, generate new such goals in a third layer, and so on. A proof is then *closed* when all such goals have been developed into full traces.

Example 1. *Let us consider a simple example with Σ having sorts* Nat*,* NeList*, and* List*, and subsort* NeList < List *(where* NeList *represents a non-empty list of natural numbers), a constructor list operator* $\mathtt{\_;\_}$: Nat List → NeList*, a list element* $\mathtt{nil}$.List*, and two defined operations* $\mathtt{head}$: NeList → Nat *and* $\mathtt{rest}$: NeList → List*. For the naturals, consider two constructor symbols* $\mathtt{0}$: Nat *and* $\mathtt{s}$: Nat → Nat*. Note that we implicitly assume all operators overloaded at the kind sorts, i.e.,* [List] *and* [Nat] *above* List *and* Nat*, respectively. There are no axioms in this example, i.e., $B = \emptyset$. The set of rules R is:*

$$\begin{aligned} \mathtt{first(L)} \to \mathtt{N} \text{ if } \mathtt{L} \to \mathtt{N\ ;\ L'} \\ \mathtt{rest(L)} \to \mathtt{L'} \text{ if } \mathtt{L} \to \mathtt{N\ ;\ L'} \end{aligned}$$

We then obtain the layered proof below for the reachability goal $\mathtt{first(rest(0;s(0);nil))} \to^{\star} \mathtt{s(0)}$ *where the reachability goals*

$$\begin{aligned} \mathtt{0\ ;\ s(0)\ ;\ nil} \to^{\star}_{R,B} \mathtt{0\ ;\ s(0)\ ;\ nil} \\ \mathtt{s(0)\ ;\ nil} \to^{\star}_{R,B} \mathtt{s(0)\ ;\ nil} \end{aligned}$$

generated by the first and second rewrite rules as conditions of the bottom trace can be proved just by reflexivity steps.

$$\dfrac{\dfrac{\top}{\mathtt{(0\ ;\ s(0)\ ;\ nil)} =_B \mathtt{(0\ ;\ s(0)\ ;\ nil)} \ \wedge\ \mathtt{(s(0)\ ;\ nil)} =_B \mathtt{(s(0)\ ;\ nil)}}}{\mathtt{first(rest(0\ ;\ s(0)\ ;\ nil))} \to^{\star}_{R,B} \mathtt{first(s(0)\ ;\ nil)} \to_{R,B} \mathtt{s(0)} = \mathtt{s(0)}} \tag{3}$$

Note the following about this example: (1) the fact that `first` *and* `rest` *are declared at the kind level —which is always understood as a sort for* undefined *or* error *expressions [57]— elegantly solves the problem that these functions are partial. For example,* `first(nil)` *has smallest sort* [List] *and is therefore undefined; (2) each layer contains the rewrite proofs of the conditions generated by the previous layer, but requires its upper layers to be proved as well; in our example the conditions of the rewrites for the bottom layer do not themselves generate conditions one level up, so we can close with the empty condition* $\top$*.*

Formally we represent layered proofs of this form as *lists of lists*, where each *list* has as elements reachability goals, perhaps partially (or fully) developed into traces. Each list is built with an associative binary conjunction operator $\_\wedge\_$ with identity $\top$ (we represent an unconditional rule $l \to r$ as the conditional rule $l \to r$ if $\top$). The associative operator building layers is denoted by $\_\uparrow\_$ with `nil` as its identity element. For example, the layered trace proof of Display (3) can be represented as the list of lists below, where we have added markers # at the beginning and end to emphasize the top and bottom:

$$\begin{aligned}
\#\texttt{first(rest(0 ; s(0) ; nil))} &\to_{R,B} \texttt{first(rest(s(0) ; nil))} \\
&\to_{R,B} \texttt{s(0)} =_B \texttt{s(0)} \uparrow \\
(\texttt{0 ; s(0) ; nil}) &=_B (\texttt{0 ; s(0) ; nil}) \wedge \\
(\texttt{s(0) ; nil}) &=_B (\texttt{s(0) ; nil}) \uparrow \top \qquad\qquad \#
\end{aligned}$$

The details of the inference system for developing layered proofs, as well as the proof of its equivalence with the standard inference system for conditional narrowing presented in Section 3.1, can be found in Appendix A.

4. Convergent Conditional Rewrite Theories

As mentioned in Section 2, in this work we focus for the most part on rewrite theories with an equational meaning, that is, theories whose rewrite rules have been obtained by *orienting* the equations of a conditional equational theory. Under suitable conditions on the rewrite rules, which we call *convergence* modulo B (because they generalize to the conditional and modulo case a similar notion of convergent rewrite rules), a very good correspondence exists between equational deduction and rewriting modulo B, namely, the *Church-Rosser* property. In particular, if $E = E_0 \cup B$, the Chuch-Rosser property is crucial to perform E-unification by constrained narrowing with $\vec{E_0}$ modulo B. Since not all confluent conditional rewite theories are Church-Rosser, suitable conditions have to be studied. Furthermore, for narrowing purposes one further condition, the *fresh pattern property* (FPP), is crucial.

We discuss below a series of conditions that, together, will give us the convergence property. Of course, to ensure that $\to^{\star}_{R/B} = \to^{\star}_{R,B}$, so that we can use the much easier to implement relation $\to_{R,B}$, the rewrite theory $\mathcal{R} = (\Sigma, B, R)$ should always be *closed under B-extensions*. However, this is not enough for implementation purposes.

We have so far not imposed any restrictions on the variables of a conditional rule. In particular, such rules may have *extra variables* in both their righthand side and their condition not appearing in its lefthand side. This can make the choice of substitution θ used in an application of the **Replacement** inference rule in Section 3.1 quite hard to implement, since, due to the extra variables in a rule's righthand side or condition, there can be an infinite number of possible choices for such a θ. This problem can be avoided, while still allowing extra variables in a rule's righthand side and condition, by requiring rewrite theories to be deterministic. When Σ is unsorted and $B = \emptyset$, this notion specializes to that of a *deterministic 3-CTRS* [65].

Definition 5 (Deterministic Rewrite Theory). *An order-sorted rewrite theory $\mathcal{R} = (\Sigma, B, R)$ is called* deterministic *iff for each rule $l \to r$ if $u_1 \to v_1 \wedge \ldots \wedge u_n \to v_n$ in R and for each i, $1 \leq i \leq n$, we have $\mathcal{V}ar(u_i) \subseteq \mathcal{V}ar(l) \cup \bigcup_{j=1}^{i-1} \mathcal{V}ar(v_j)$.*

In other words, variables are only introduced in the righthand terms of the condition, and the lefthand terms in the condition may only contain variables that appear either in the lefthand side of the rule, or in the previous righthand terms of the condition.

A deterministic rule $l \to r$ if $u_1 \to v_1 \wedge \ldots \wedge u_n \to v_n$ allows a simple algorithm for computing incrementally an expanded B-matching substitution for the extra variables in its condition from a B-matching substitution for l by solving the conditions one by one from left to right. Let t be the term to be rewritten at position p by $l \to r$ if $u_1 \to v_1 \wedge \ldots \wedge u_n \to v_n$. We first compute a B-match $\gamma_0 \in Match_B(l, t_p)$. Then, we instantiate u_1 with γ_0 and attempt to rewrite $u_1\gamma_0 \to^*_{R,B} w_1$ so that we can find a B-match (instantiating only the fresh variables in v_1) $\gamma_1 \in Match_B(v_1\gamma_0, w_1)$. Then, we instantiate u_2 with $\gamma_0 \cup \gamma_1$ and repeat this process, until the fresh variables of each v_i in the condition have an associated substitution γ_i. We then take $\gamma = \bigcup_{0 \leq i \leq n} \gamma_i$ as the *extended matching substitution* used to rewrite t.

Note that it is not necessary to rewrite $u_i\gamma$ to canonical form before attempting to match it against v_i. One may stop rewriting as soon as one achieves a match with v_i. As we shall see later, this can lead to problems when attempting to lift such rewrite sequences to narrowing. Furthermore, faithfully implementing this algorithm can be very inefficient. Therefore, we will further restrict our scope to *strongly deterministic rewrite theories*, and will present a much more efficient rewrite strategy. However, before we can define strongly deterministic rewrite theories, we need the notion of a *strongly irreducible term.*

Definition 6 (Irreducible and Strongly Irreducible). *Let (Σ, B, R) be a rewrite theory. A term t is* R, B-irreducible *iff there is no term u such that $t \to_{R,B} u$. A substitution θ is* R, B-irreducible *iff for each $x \in Dom(\theta)$ the term $x\theta$ is R, B-irreducible. A term t is* strongly R, B-irreducible *iff for every R, B-irreducible substitution σ, the term $t\sigma$ is R, B-irreducible.*

Definition 7 (Strongly Deterministic Rewrite Theory). *A deterministic rewrite theory* (Σ, B, R) *is called* strongly deterministic *iff for each rule* $l \to r \,\text{if}\, u_1 \to v_1 \wedge \ldots \wedge u_n \to v_n$ *in* R*, and for each* i*,* $1 \leq i \leq n$*,* v_i *is strongly* R, B*-irreducible.*

The next requirement on (Σ, B, R) is a termination requirement. Note, however, that for conditional theories the termination of the relation $\to_{R,B}$ is not enough, since looping can still happen when evaluating a rule's condition. The right notion for conditional theories is that of *operational termination* [24, 53]. The precise definition can be found in the just-cited papers, but the idea is intuitively quite simple, namely, *absence of infinite inference.* We can think of an interpreter, for example implementing R, B-rewriting for a strongly deterministic rewrite theory (Σ, B, R), as a *proof-building engine* that tries to build a proof tree using the inference system in Section 3.1 by trying to build proof trees from left to right for each of the subgoals generated by an application of an inference rule. At any intermediate point in the computation the interpreter will have only a partial proof, called a *well-formed* proof tree. Operational termination of (Σ, B, R) means that such an interpreter will never loop by trying to build an *infinite* well-formed proof tree, because there are none. That is, any proof attempt either succeeds in finite time, finding a proof, or fails in finite time for all attempts. For methods and tools to prove the operational termination of an order-sorted rewrite theory see, e.g., [24, 26, 25, 54].

The next requirement on (Σ, B, R) is *sort-decreasingness.* This requirement is always satisfied if Σ is a many-sorted or unsorted signature. Intuitively, it means that, as a term gets rewritten, more sort information becomes available. $\mathcal{R} = (\Sigma, B, R)$ is called *sort-decreasing* modulo B iff whenever $t \to_{R,B} t'$ we have $ls(t) \geq ls(t')$. A checkable sufficient condition for sort-decreasingness is that: (i) B is sort-preserving, and (ii) for all rules $l \to r$ *if* $\bigwedge_{i=1,\ldots,n} u_i \to v_i$ in R and all "sort specializations" ρ (i.e., sort-lowering substitutions ρ such that for all $x{:}s$ in $Dom(\rho)$ we have $\rho : x{:}s \mapsto x'{:}s'$ with $s \geq s'$) the property $ls(l\rho) \geq ls(r\rho)$ holds.

The last, yet most important, requirement is *confluence* modulo B, for which we need the auxiliary notion of *joinability* modulo B. For simplicity let us assume that $\mathcal{R} = (\Sigma, B, R)$ is closed under B-extensions, so that we can focus on the simpler and easier to implement R, B-rewrite relation. Two terms $u, v \in \mathcal{T}_\Sigma(\mathcal{X})$ are called R, B*-joinable*, denoted $u \downarrow_{R,B} v$ iff there exists $w \in \mathcal{T}_\Sigma(\mathcal{X})$ such that $u \to^\star_{R/B} w \;{}_{R/B}\!\overset{\star}{\leftarrow} v$. The relation $\to_{R,B}$ is called *confluent* modulo B iff for each $u, v, t \in \mathcal{T}_\Sigma(\mathcal{X})$, $u \;{}_{R,B}\!\overset{\star}{\leftarrow} t \to^\star_{R,B} v$ implies $u \downarrow_{R,B} v$. Checking of confluence modulo regular and linear axioms B with a finitary unification algorithm under the sort-decreasingness, operational termination and closure under B-extensions assumptions, and a tool supporting such checking for various combinations of associativity, commutativity and identity axioms have been documented in [27]. Indeed, such checking amounts to checking the confluence of *conditional critical pairs* modulo the axioms B (for the conditional notions of local confluence and critical pair see, e.g., [65, 27]).

We are now ready to define convergent theories.

Definition 8 (Convergent Rewrite Theory). *An order-sorted rewrite theory $\mathcal{R} = (\Sigma, B, R)$ is called* convergent *iff: (i) B satisfies all the requirements at the beginning of Section 3.2; (ii) R is closed under B-extensions; (iii) R is strongly deterministic; (iv) $\mathcal{R}$ is operationally terminating; (v) R is sort-decreasing, and (vi) R is confluent modulo B.*

An extremely useful property of convergent theories is that they satisfy the Church-Rosser property modulo B, that is, the equivalence between provable equality and joinability displayed in the following theorem:

Theorem 2 (Church Rosser modulo B with Decidable Equality). [61] *Let $\mathcal{R} = (\Sigma, B, \vec{E})$, associated to a conditional equational theory $(\Sigma, E \cup B)$, satisfy conditions (i)–(v) in Definition 8. Then $\mathcal{R}$ is confluent modulo B iff for any Σ-terms t, t' we have the equivalence:*

$$t =_{E \cup B} t' \Leftrightarrow t \downarrow_{\vec{E},B} t'.$$

Furthermore, for $\mathcal{R} = (\Sigma, B, \vec{E})$ convergent and therefore Church-Rosser modulo B, if E is finite the equality relation $t =_{E \cup B} t'$ is decidable by checking whether $t!_{\vec{E},B} =_B t'!_{\vec{E},B}$ holds, where $t!_{\vec{E},B}$ denotes the[7] *R, B-irreducible term $\rightarrow^{\star}_{\vec{E},B}$-reachable from t and called the $\vec{E}, B$-*canonical *(or $\vec{E}, B$-*normal*)* form *of t.*

Note that we can easily move back and forth between convergent rewrite theories and their corresponding equational theories. That is, given an equational theory $(\Sigma, E \cup B)$, if $(\Sigma, B, \vec{E})$ is convergent we have the above Church-Rosser theorem. But any convergent (Σ, B, R) is of the form $(\Sigma, B \cup \vec{E_R})$ for E_R the set of conditional equations

$$E_R = \{l = r \ if \bigwedge_{i=1,\ldots,n} u_i = v_i \mid (l \rightarrow r \ if \bigwedge_{i=1,\ldots,n} u_i \rightarrow v_i) \in R\}$$

so that (Σ, B, R) is the rewrite theory associated to the equational theory $(\Sigma, E_R \cup B)$.

To express that we can reach from a term t an R, B-irreducible term u we write $t \rightarrow^{!}_{R,B} u$. That is, $t \rightarrow^{!}_{R,B} u$ means that: (i) $t \rightarrow^{\star}_{R,B} u$, and (ii) u is R, B-irreducible. As mentioned above, if $\mathcal{R}$ is convergent, then the R, B-canonical form u is unique up to B-equality, is denoted $u = t!_{R,B}$, and is called the *normal form* of t. A term t is called *R,B-normalized* (or just normalized) iff $t =_B t!_{R,B}$. Likewise, if θ is a substitution and $\mathcal{R}$ is convergent, there is up to B-equality a unique R, B-irreducible substitution, denoted $\theta!_{R,B}$, where for each $x \in \mathit{Dom}(\theta)$, $\theta!_{R,B}(x) = \theta(x)!_{R,B}$. A substitution θ is called *R,B-normalized* (or just normalized) iff $\theta =_B \theta!_{R,B}$.

In a convergent rewrite theory (Σ, B, R) we can simplify and optimize the algorithm for computing the expanded matching substitution by rewriting each $u_i\gamma$ to its R, B-canonical form before attempting to match it against v_i.

[7] By confluence, $t'!_{\vec{E},B}$ is unique up to B-equality.

Such a simplified algorithm induces the following normalized-conditional rewriting (NC-rewriting) relation:

Definition 9 (NC-Rewriting). *Let (Σ, B, R) be a convergent order-sorted rewrite theory and t be a Σ-term. We say that t* rewrites with normalized condition *(NC) to $t[r\gamma]_p$ at position $p \in Pos(t)$ with rule $l \to r$* if *$u_1 \to v_1 \wedge \ldots \wedge u_n \to v_n$ and substitution γ, denoted $t \xrightarrow{NC}_{\gamma,R,B} t[r\gamma]_p$, iff $t_p =_B l\gamma$, and for all i, $1 \leq i \leq n$, $u_i\gamma \to^!_{R,B} v_i\gamma$.*

Unfortunately, the NC-rewrite strategy is in general not complete, even when $\mathcal{R}$ is convergent.

Example 2. *Consider the following unsorted signature Σ and strongly deterministic rules R:*

$$
\begin{array}{llll}
\Sigma : & & & \\
\quad S = \{s\} & & & \\
\quad a : \ \to s & b : \ \to s & c : \ \to s & d : \ \to s \\
\quad f : \ s \ s \to s & & & \\
\quad [\_,\_] : \ s \ s \to s & & & \\
R : & & & \\
\quad a \to b & & & \\
\quad c \to d & & & \\
\quad f(x,y) \to z \text{ if } [x,y] \to [x,z] & & &
\end{array}
$$

which do not have any critical pairs and are therefore locally confluent, and are also operationally terminating and therefore convergent. We can perform the rewrite $f(a,c) \to c$. However, $f(a,c)$ is irreducible by NC*-rewriting, because $[a,c]!_{R/B} = [b,d]$, which does not match the term $[a,z]$.*

We can make NC-rewriting complete by adopting a slightly more restrictive notion of strongly deterministic rewrite theory that we claim is the *right* notion for efficient executability purposes. Furthermore, as we explain below, this slight restriction involves no real loss of generality.

Definition 10 (Fresh Pattern Property). *We say that a strongly deterministic order-sorted rewrite theory (Σ, B, R) has the* fresh pattern property *(FPP) iff for each rule in R of the form $l \to r$* if *$u_1 \to v_1 \wedge \ldots \wedge u_n \to v_n$, and for each i, $1 \leq i \leq n$, $\mathcal{V}ar(v_i) \cap (\mathcal{V}ar(l) \cup \bigcup_{1 \leq j < i} \mathcal{V}ar(v_j)) = \emptyset$.*

In other words, if v_i has any variables, they are all *fresh* with respect to the variables in the lefthand side of the rule, and the variables appearing in the previous terms of the condition.

The fresh pattern property *involves no real loss of generality*, because we can easily transform any strongly deterministic theory that does not have the fresh pattern property into one that does. To do so, first, we add a new connected component, with a single fresh sort *Truth* to Σ. Then, for each top sort $[s]$ in every other connected component, we add the predicate $\_ \equiv \_ : [s]\ [s] \to \mathit{Truth}$. We also add a constant $\mathit{tt} :\to \mathit{Truth}$, and the rule $x \equiv x \to \mathit{tt}$. Then, for each conditional rule $l \to r$ if $\bigwedge_{1 \leq i \leq n} u_i \to v_i$, and each $i \in \{1, \ldots, n\}$ s.t. it has a variable $x \in \mathit{vars}(v_i) - (\mathit{vars}(l) \cup \bigcup_{1 \leq j < i} \mathit{vars}(v_j))$, we rename every occurrence of x in v_i by a fresh variable x' in a new term v_i', obtaining in this way a renamed condition $u_i \to v_i'$, and add the condition $x \equiv x' \to \mathit{tt}$ at the end of the conditional part of the rule. *NC*-rewriting then ensures that the substitution instance $u_i\gamma_{i-1}$ of u_i is normalized before being matched against v_i to obtain γ_i, and $x \equiv x' \to \mathit{tt}$ ensures that x' is properly bound to x. This is a standard procedure in functional logic programming where there are no reachability conditions but only equality conditions using a strict semantics, i.e., both terms of a strict equality are normalized into constructor terms and then checked for syntactic equality; see [41] and references therein.

Example 3. *We can easily transform the theory in Example 2 to make it FPP by just modifying the rule* $f(x, y) \to z$ if $[x, y] \to [x, z]$ *into the rule:* $f(x, y) \to z$ if $[x, y] \to [x', z] \wedge x \equiv x' \to \mathit{tt}$.

If $\mathcal{R}$ is convergent and FPP, then NC-rewriting is complete for reaching canonical forms, in the following sense:

Proposition 1 (Completeness of NC-Rewriting). *Let* $\mathcal{R} = (\Sigma, B, R)$ *be convergent and FPP. Then for each* Σ*-term* t*, if* $t \to^!_{R,B} v$*, then* $t \xrightarrow{NC}{}^!_{R,B}\ v$*, where* $t \xrightarrow{NC}{}^!_{R,B}\ v$ *denotes a sequence of* $n \geq 0$ *NC-rewriting steps followed by a step of* B*-equality.*

Proof. The case when $t =_B v$ is trivial. Suppose, therefore, that $t \to_{R,B} u \to^!_{R,B} v$. Since $\mathcal{R}$ is convergent, it is in particular operationally terminating, so that the relation $\to_{R,B}$ is well-founded. We can reason by well-founded induction on $\to_{R,B}$. But $t \to_{R,B} u$ means that there is a position $p \in \mathit{Pos}(t)$, a rule $l \to r$ if $u_1 \to v_1, \ldots, u_n \to v_n$ in R and a substitution σ such that $t_p =_B l\sigma$, $u_j\sigma \to^\star_{R,B} v_j\sigma$ for each $1 \leq j \leq n$, and $u = t[r\sigma]_p$. Since $\mathcal{R}$ is strongly deterministic, we have $u_j\sigma \to^\star_{R,B} v_j\sigma \to^!_{R,B} v_j(\sigma!_{R,B})$, and since it is FPP and confluent, $\sigma' = \sigma|_{\mathcal{V}ar(l)} \uplus (\sigma!_{R,B})|_{\mathcal{V}ar(v_1) \cup \cdots \mathcal{V}ar(v_n)}$ gives us an NC-rewrite step $t \xrightarrow{\text{NC}}_{R,B} t[r\sigma']_p$. By confluence and well-founded induction we then have $t[r\sigma']_p \xrightarrow{\text{NC}}{}^!_{R,B}\ v$, and therefore, $t \xrightarrow{\text{NC}}{}^!_{R,B}\ v$, as desired. □

Note that, if $\mathcal{R}$ is convergent and FPP, the above completeness result ensures that one can reach a canonical form using exclusively NC rewriting, both in each rewrite step, and in recursively evaluating the conditions of each such step to canonical form. This is of course much more time- and space-efficient than performing search when evaluating conditions.

5. Reachability Problems and Constrained Narrowing

Constrained terms are pairs $u \mid C$, with u a term and C a conjunction of reachability goals. Semantically, $u \mid C$ denotes the set of instances $u\theta$ (with θ a normalized substitution), such the $\mathcal{R} \vdash C\theta$. We say that $v \mid D$ is *$\mathcal{R}$-reachable* from $u \mid C$ if an instance of $u \mid C$ can be rewritten to an instance of $v \mid D$. We define *constrained narrowing* for convergent FPP theories, and prove it sound and complete to find NC-solutions to reachability problems between constrained terms.

5.1. Reachability Problems

Definition 11 (FPP Condition and Constrained Term). *Given a rewrite theory $\mathcal{R} = (\Sigma, B, R)$, a condition $u_1 \rightarrow^{\star}_{R,B} v_1 \wedge \cdots \wedge u_n \rightarrow^{\star}_{R,B} v_n$ is called an* FPP condition over $\vec{x}$ *iff:*

1. *all v_i are strongly R, B-irreducible.*
2. *$\mathcal{V}ar(u_1) \subseteq \vec{x}$*
3. *$\forall 1 < j \leq n$, $\mathcal{V}ar(u_j) \subseteq \vec{x} \cup (\bigcup_{1 \leq i < j} \mathcal{V}ar(v_i))$*
4. *$\forall 1 \leq j \leq n$, $\mathcal{V}ar(v_j) \cap (\vec{x} \cup (\bigcup_{1 \leq i < j} \mathcal{V}ar(v_i))) = \emptyset$.*

We call $\bigcup_{1 \leq i \leq n} \mathcal{V}ar(v_i)$ the fresh variables *of the FPP condition.*

A constrained Σ-term *is a pair $u \mid C$ where u is a Σ-term, and C is a conjunction of the form $u_1 \rightarrow^{\star}_{R,B} v_1 \wedge \cdots \wedge u_n \rightarrow^{\star}_{R,B} v_n$. A constrained term $u \mid C$ is called* FPP *iff $C = (u_1 \rightarrow^{\star}_{R,B} u'_1 \wedge \cdots \wedge u_n \rightarrow^{\star}_{R,B} u'_n)$ is FPP over $\mathcal{V}ar(u)$.*

Definition 12 (Reachability Problem and their Solutions). *Given a convergent FPP rewrite theory $\mathcal{R} = (\Sigma, B, R)$ and constrained terms $(u \mid C)$ and $(v \mid D)$, we call $(v \mid D)$* $\mathcal{R}$-reachable *from $(u \mid C)$ with solution σ iff there is a normalized substitution σ with $Dom(\sigma) \subseteq \mathcal{V}ar(u \mid C) \cup \mathcal{V}ar(v \mid D)$ such that:*

- *$\mathcal{R} \vdash C\sigma$ and $\mathcal{R} \vdash D\sigma$*
- *$u\sigma \rightarrow^{\star}_{R,B} v\sigma$.*

A solution σ is called an NC solution *iff there is an NC-rewrite sequence $u\sigma \rightarrow^{\star}_{R,B} v\sigma$.*

We call the problem of whether $v \mid D$ is reachable from $u \mid C$ an *$\mathcal{R}$-reachability problem*, denoted $u \mid C \rightsquigarrow^{\star} v \mid D$, and say that it is *solvable* (resp. *NC-solvable*) iff there is a solution (resp. NC-solution) σ reaching $v \mid D$ from $u \mid C$. If a solution σ exists, we then write $\mathcal{R} \vdash u \mid C \rightsquigarrow^{\star}_{\sigma} v \mid D$, or just $\mathcal{R} \vdash u \mid C \rightsquigarrow^{\star} v \mid D$.

The following lemma, showing that solutions exist up to B-equivalence is an easy consequence of Theorem 1; its proof is left to the reader.

Lemma 1. *Given a convergent FPP theory $\mathcal{R} = (\Sigma, B, R)$, constrained terms $u \mid C$ and $v \mid D$, and substitutions σ, τ with $\sigma =_B \tau$, then σ is a solution (resp. NC-solution) of the reachability problem $u \mid C \rightsquigarrow^\star v \mid D$ iff τ is so.* □

Example 4. *Note that some reachability problems may be solvable, but not NC-solvable. Consider, for example, the convergent FPP theory of Example 3, and the reachability problem $f(x, c) \mid \top \rightsquigarrow^\star c \mid \top$. This reachability problem is trivially solvable with solution the identity substitution id, since we have $f(x, c) \to c$. However, no NC-solution exists.*

The easy proof of the following lemma is left to the reader.

Lemma 2. *Let $\mathcal{R} = (\Sigma, B, R)$ be a convergent FPP theory, and $u \mid C \rightsquigarrow^\star v \mid D$ a reachability problem such that v is strongly R, B-irreducible. Then any solution σ of such a problem is an NC-solution.* □

In Definition 12 the set of shared variables $\vec{y} = \mathcal{V}ar(u \mid C) \cap \mathcal{V}ar(v \mid D)$ may be non-empty. However, by adding to $\mathcal{R}$ a tupling constructor we can easily reduce any $\mathcal{R}$-reachability problem to one where $\vec{y} = \emptyset$.

Lemma 3. *Let $\mathcal{R} = (\Sigma, B, R)$ be a convergent FPP rewrite theory, and $u \mid C \rightsquigarrow^\star v \mid D$ an $\mathcal{R}$-reachability problem with u and v of sort $[\mathsf{s}]$ and $\vec{y} = \mathcal{V}ar(u \mid C) \cap \mathcal{V}ar(v \mid D) = y_1{:}\mathsf{s_1}, \ldots, y_n{:}\mathsf{s_n}$ with $n \geq 0$.*

Extend $\mathcal{R}$ to $\mathcal{R}^{<>}$ by adding a new tupling constructor

$$\texttt{<\_,\ldots,\_>} : [\mathsf{s}]\ [\mathsf{s_1}]\ \cdots\ [\mathsf{s_k}] \to \mathsf{Tuple}.[\mathsf{s}].[\mathsf{s_1}].\ldots.[\mathsf{s_k}]$$

which does not appear in Σ and where the new sort $\mathsf{Tuple}.[\mathsf{s}].[\mathsf{s_1}].\ldots.[\mathsf{s_k}]$ is in a new connected component of the, thus extended, poset of sorts. Then:

1. *$\mathcal{R} \vdash (u \mid C) \rightsquigarrow^\star (v \mid D)$ iff*
2. *$\mathcal{R}^{<>} \vdash (< u, y_1, \ldots, y_n >\mid C) \rightsquigarrow^\star (< v\rho, y'_1, \ldots, y'_n >\mid D\rho)$, where $\vec{y'} = y'_1{:}\mathsf{s_1}, \ldots, y'_n{:}\mathsf{s_n}$, $Dom(\rho) = \vec{y}$, $Ran(\rho) = \vec{y'}$, $\rho(y_i) = y'_i$ for $1 \leq i \leq n$, and $\vec{y'} \cap (\mathcal{V}ar(u \mid C) \cup \mathcal{V}ar(v \mid D)) = \emptyset$.*

Furthermore, any solution θ of (1) extends to a solution $\overline{\theta}$ of (2) with $y'_i\overline{\theta} = y_i\theta$. Conversely, for any solution γ of (2), $\rho\gamma$ is a solution of (1).

Proof. Obviously, if $\mathcal{R} \vdash u \mid C \rightsquigarrow^\star_\theta v \mid D$, since $u\theta \to^*_{R,B} v\theta$, we also have $< u\theta, y_1\theta, \ldots, y_n\theta > \to^*_{R,B} < v\theta, y_1\theta, \ldots, y_n\theta >$, but extending θ to $\overline{\theta}$ by defining $y'_i\overline{\theta} = y_i\theta$, we have $< v\theta, y_1\theta, \ldots, y_n\theta >=< v\rho\overline{\theta}, y'_1\overline{\theta}, \ldots, y'_n\overline{\theta} >$, giving us a solution $\overline{\theta}$ of (2) as described.

Conversely, let γ be a solution of (2), so that we have $< u\gamma, y_1\gamma, \ldots, y_n\gamma > \to^\star_{R,B} < v\rho\gamma, y_1\rho\gamma, \ldots, y_n\rho\gamma >$. Since γ is R, B-irreducible and $< \_, \ldots, \_ >$ is a new constructor symbol, this forces: (i) $u\gamma \to^\star_{R,B} v\rho\gamma$, and (ii) $y_i\gamma =_B y_i\rho\gamma$, $1 \leq i \leq n$. But since ρ is a sort-preserving bijective renaming of variables,

(ii) then gives us $u\rho\gamma =_B u\gamma$ and $C\rho\gamma =_B C\gamma$, which by Theorem 1 gives us $u\rho\gamma \to^{\star}_{R,B} v\rho\gamma$ and $\mathcal{R} \vdash C\rho\gamma$, proving $\mathcal{R} \vdash u \mid C \leadsto^{\star}_{\rho\gamma} v \mid D$. □

Because of the above lemma, from now on without loss of generality we will assume that in all $\mathcal{R}$-reachability problems of the form $u \mid C \leadsto^{*} v \mid D$ we have $\mathcal{V}ar(u \mid C) \cap \mathcal{V}ar(v \mid D) = \emptyset$.

5.2. Constrained Narrowing

Given an $\mathcal{R}$-reachability problem, is there a *symbolic* method to find an NC-solution for it? As we shall see, when $\mathcal{R}$ is a convergent FPP theory, *constrained narrowing* provides such a method when the reachability goals do not share variables. Furthermore, we shall show that this symbolic method is sound (produces correct NC-solutions), and complete, in the sense that (up to B-equality) any NC-solution of a reachability problem is an *instance* of a symbolic solution found by constrained narrowing.

Given a convergent FPP theory $\mathcal{R} = (\Sigma, B, R)$, by a rule of R being *standardized apart*, denoted $(l' \to r' \text{ if } C') \ll R$, we mean that there is a variable renaming ρ and a rule $(l \to r \text{ if } C) \in R$ such that $(l' \to r' \text{ if } C') = (l \to r \text{ if } C)\rho$, and, furthermore, the variables $\mathcal{V}ar(l' \to r' \text{ if } C')$ are *disjoint* from all the variables previously met during any computation. In our case, the "computations" will be constrained narrowing sequences $u \mid C \leadsto_{\alpha_1} u_1 \mid C_1 \leadsto \cdots \leadsto_{\alpha_n} u_n \mid C_n =^{\gamma}_{B} v \mid D$, which are symbolic solutions of reachability goals $u \mid C \leadsto^{\star} v \mid D$, where the last step is a B-unification of u_n and v with B-unifier γ. Likewise, we say that a substitution θ is *standardized apart* if the variables in $Ran(\theta)$ are *disjoint* from all the variables previously met during any computation. Standardizing rules (resp. substitutions) apart allows all variables in such rules (resp. introduced by such substitutions) to always be fresh. Of course, over a computation, rules in R may have to be standardized apart many times.

Definition 13. *Let $u \mid C$ be a constrained term, and $\mathcal{R} = (\Sigma, B, R)$ a convergent FPP theory. A* constrained narrowing step *denoted*

$$u \mid C \leadsto_{\alpha,q,R,B} (u[r]_q \mid C \wedge D)\alpha$$

with rule $(l \to r \text{ if } D) \ll R$ at non-variable position $q \in Pos_{\Sigma}(u)$ and with substitution α is defined iff $\alpha \in CSU_B(u|_q, l)$ with $Dom(\alpha) = \mathcal{V}ar(u|_q) \uplus \mathcal{V}ar(l)$ and α standardized apart; in particular this implies that $Ran(\alpha) \cap (\mathcal{V}ar(u|C) \uplus \mathcal{V}ar(l \to r \text{ if } D)) = \emptyset$. When q, R and B are understood, we abbreviate a constrained narrowing step as: $u \mid C \leadsto_{\alpha} (u[r]_q \mid C \wedge D)\alpha$.

By a constrained narrowing sequence *of length $n \geq 0$ from $u \mid C$, we mean either the 0-step sequence $u \mid C$ or the $n > 0$ sequence of constrained narrowing steps*

$$u \mid C \leadsto_{\alpha_1} u_1 \mid C_1 \leadsto_{\alpha_2} u_2 \mid C_2 \leadsto \cdots \leadsto u_{n-1} \mid C_{n-1} \leadsto_{\alpha_n} u_n \mid C_n$$

with each α_i standardized apart, $1 \leq i \leq n$.

Like rewriting, narrowing can also be restricted by means of a frozenness map $\phi : \Sigma \to \mathcal{P}(\mathbb{N})$. We then obtain a relation $u \mid C \leadsto_{\alpha,q,R,B,\phi} (u[r]_q \mid C \wedge D)\alpha$ by imposing the extra condition that the position q is not frozen by ϕ.

The key result is the following *Lifting Lemma*, which shows that any NC-rewriting step can be lifted to a narrowing step of which it is an instance. Since unsorted unconditional rewriting is a special case of order-sorted conditional rewriting modulo axioms B (namely, for Σ unsorted and $B = \emptyset$), this generalizes well-known Lifting Lemmas for unsorted unconditional rewriting without axioms [44], and modulo axioms B [46]. The main differences with the proofs in the unsorted, unconditional case —making the proof details somewhat more delicate— are: (i) the presence of extra variables in conditions; (ii) only NC-rewriting steps can be lifted; and (iii) strict coherence properties are now essentially needed to keep track of B-equivalent versions of NC-rewriting steps and of their B-equivalent fully evaluated conditions.

Lemma 4 (Lifting Lemma). *Let $\mathcal{R} = (\Sigma, B, R)$ be a convergent FPP rewrite theory. Let $u \mid C$ be a Σ-constrained term, and β a R,B-normalized substitution with $Dom(\beta) \subseteq \mathcal{V}ar(u \mid C)$ such that $\mathcal{R} \vdash C\beta$. Let $u\beta \to_{R,B} u\beta[r\sigma]_q$ be an NC-rewrite step with rule*

$$l \to r \,\mathrm{if}\, u_1 \to v_1 \wedge \cdots \wedge u_n \to v_n \tag{4}$$

at position q with substitution σ. Then, there is a constrained narrowing step $u \mid C \rightsquigarrow_{\alpha,q,R,B} (u[r]_q \mid C \wedge u_1 \to^{\star}_{R,B} v_1 \wedge \cdots u_n \to^{\star}_{R,B} v_n)\alpha$ using (4) and a R,B-normalized substitution γ such that, assuming without loss of generality that (4) is standardized apart, and defining the mutually disjoint sets of variables: $\vec{x} = \mathcal{V}ar(u|_q)$, $\vec{y} = \mathcal{V}ar(u \mid C) \setminus \mathcal{V}ar(u|_q)$, $\vec{z} = \mathcal{V}ar(l)$, $\vec{z'} = \mathcal{V}ar(v_1) \cup \cdots \cup \mathcal{V}ar(v_n)$, and $\vec{z''} = Ran(\alpha)$, we have $Dom(\gamma) \subseteq \vec{y} \uplus \vec{z'} \uplus \vec{z''}$, and:

1. *$(\alpha\gamma)|_{\vec{x} \uplus \vec{y}} =_B \beta$,*

2. *$(\alpha\gamma)|_{\vec{z} \uplus \vec{z'}} =_B \sigma$,*

3. *There is an NC-rewrite $u\alpha\gamma \to_{R,B} u[r]_q\alpha\gamma$ with rule (4), substitution $(\alpha\gamma)|_{\vec{z} \uplus \vec{z'}}$, and provable condition $(u_1 \to^{\star}_{R,B} v_1 \wedge \cdots u_n \to^{\star}_{R,B} v_n)\alpha\gamma$ that coincides up to B-equality with the NC-rewrite step $u\beta \to_{R,B} u\beta[r\sigma]_q$ with same rule and provable condition $(u_1 \to^{\star}_{R,B} v_1 \wedge \cdots u_n \to^{\star}_{R,B} v_n)\sigma$, in the sense that:*

   - *$u\alpha\gamma =_B u\beta$ and $u\beta[r\sigma]_q =_B (u[r]_q)\alpha\gamma$, and*
   - *for $1 \leq i \leq n$, $u_i\alpha\gamma =_B u_i\sigma$, and $v_i\alpha\gamma =_B v_i\sigma$.*

4. *$\mathcal{R} \vdash (C \wedge u_1 \to^{\star}_{R,B} v_1 \wedge \cdots \wedge u_n \to^{\star}_{R,B} v_n)\alpha\gamma$.*

Proof. Since β is normalized we must have $q \in Pos_{\Sigma}(u)$; and since $u_q\beta =_B l\sigma$, there is a B-unifier $\alpha \in CSU_B(u_q, l)$ with domain $\vec{x} \uplus \vec{z}$ and a substitution γ_0 with domain $\vec{z''}$ such that $\beta|_{\vec{x}} =_B (\alpha\gamma_0)|_{\vec{x}}$ and $\sigma|_{\vec{z}} =_B (\alpha\gamma_0)|_{\vec{z}}$. Define γ as the following extension of γ_0:

$$\gamma = \beta|_{\vec{y}} \uplus \gamma_0 \uplus \sigma|_{\vec{z'}}$$

Note that γ is normalized since: (i) β is so, (ii) σ is the substitution associated to an NC-rewrite, which forces $\sigma|_{\vec{z'}}$ to be normalized, and, (iii) since B is regular and $u_q\alpha =_B l\alpha$, we have $\mathcal{V}ar(u_q\alpha) = \mathcal{V}ar(l\alpha) = Ran(\alpha) = \vec{z''}$, so that $\beta|_{\vec{x}} =_B (\alpha\gamma_0)|_{\vec{x}}$ and β normalized forces γ_0 to be normalized. Note that $(\alpha\gamma)|_{\vec{x}\uplus\vec{y}} = (\alpha\gamma)|_{\vec{x}} \uplus (\alpha\gamma)|_{\vec{y}} =_B \beta|_{\vec{x}} \uplus \gamma|_{\vec{y}} = \beta|_{\vec{x}} \uplus \beta|_{\vec{y}} = \beta$, which is point (1). We also have $(\alpha\gamma)|_{\vec{z}\uplus\vec{z'}} = (\alpha\gamma)|_{\vec{z}} \uplus (\alpha\gamma)|_{\vec{z'}} =_B \sigma|_{\vec{z}} \uplus \gamma|_{\vec{z'}} = \sigma|_{\vec{z}} \uplus \sigma|_{\vec{z'}} = \sigma$, which is point (2).

Since $u_q\beta =_B l\sigma$, $\beta|_{\vec{x}} =_B (\alpha\gamma_0)|_{\vec{x}} = (\alpha\gamma)|_{\vec{x}}$, and $\sigma|_{\vec{z}} =_B (\alpha\gamma_0)|_{\vec{z}} = (\alpha\gamma)|_{\vec{z}}$, we have $u_q\alpha\gamma =_B u_q\beta =_B l\sigma =_B l\alpha\gamma$. Furthermore, point (2) of Theorem 1, and the fact that for each $1 \leq i \leq n$ we have $u_i\sigma \rightarrow_{R,B} ! v_i\sigma$ gives us $u_i\alpha\gamma \rightarrow_{R,B} ! v_i\alpha\gamma$, which gives us the claimed NC-rewrite $u\alpha\gamma \rightarrow_{R,B} u[r]_q\alpha\gamma$, and the fact that $\alpha\gamma|_{\vec{z'}} = \gamma|_{\vec{z'}} = \sigma|_{\vec{z'}}$ gives us the actual identities $v_i\alpha\gamma = v_i\sigma$, which is (3).

Finally we have, $(C \wedge u_1 \rightarrow^{\star}_{R,B} v_1 \wedge \cdots \wedge u_n \rightarrow^{\star}_{R,B} v_n)\alpha\gamma = C\alpha\gamma \wedge (u_1 \rightarrow^{\star}_{R,B} v_1 \wedge \cdots \wedge u_n \rightarrow^{\star}_{R,B} v_n)\alpha\gamma =_B C\beta \wedge (u_1 \rightarrow^{\star}_{R,B} v_1 \wedge \cdots \wedge u_n \rightarrow^{\star}_{R,B} v_n)\alpha\gamma$. Since by hypothesis we have $\mathcal{R} \vdash C\beta$, and we have just shown that $\mathcal{R} \vdash (u_1 \rightarrow^{\star}_{R,B} v_1 \wedge \cdots \wedge u_n \rightarrow^{\star}_{R,B} v_n)\alpha\gamma$, again Theorem 1 gives (4), as desired. □

Remark 2. *For technical reasons that will become clear in Sections 7 and 8, we will be interested in using also the above Lifting Lemma when the convergent FPP rewrite theory comes with a B-stable frozenness map ϕ. If $\mathcal{R} = (\Sigma, B, R)$ is such a theory and ϕ is a frozenness map, we write $\mathcal{R}_\phi = (\Sigma, B, R, \phi)$ to denote $\mathcal{R}$ enriched with the extra frozenness information ϕ. As already mentioned in Section 3.1, the inference system defining the relation $\rightarrow_{R,B}$ can be naturally restricted to one defining the relation $\rightarrow_{R,B,\phi}$, where rules are only applied at non-frozen term positions. Of course, in $\mathcal{R}_\phi$ this frozenness restriction also applies to the evaluation of conditions by rewriting. However, in all the applications we will consider, $\mathcal{R}_\phi$ will have particularly good properties, namely, it will have: (i) a family of kinds $\{[s_i]\}_{i\in I}$ such that for each $i \in I$, any term t of kind $[s_i]$ has all its positions unfrozen; and (ii) for any rule $l \rightarrow r$ if D in R, all terms appearing in the lefthand or righthand side of a condition in D have their kind among the $\{[s_i]\}_{i\in I}$. We call $\mathcal{R}_\phi$ satisfying (i) and (ii) a theory with* unfrozen kinds $\{[s_i]\}_{i\in I}$ and unfrozen conditions.

The point, of couse, is that for terms t of kind $[s_i]$, the relations $\rightarrow_{R,B}$ and $\rightarrow_{R,B,\phi}$ coincide. *Therefore, notions such as normal form, normalized substitution, and so on, do not change at all for such terms by the introduction of the frozenness restrictions ϕ. Furthermore, for any term u whatsoever, which may have frozen positions, the notion of an NC*-rewrite $u \rightarrow_{R,B,\phi} v$ at a non-frozen position *makes perfect sense, since no frozenness restrictions can apply to the evaluation of conditions, so that the entire evaluation of the NC-step $u \rightarrow_{R,B,\phi} v$, including the evaluation of its condition, can be performed with $\mathcal{R}_\phi$.*

We leave for the reader to check that the above Lifting Lemma also applies to a theory $\mathcal{R}_\phi$ with ϕ B-stable and with unfrozen kinds $\{[s_i]\}_{i\in I}$ and unfrozen conditions provided: (i) the sorts of the variables $\mathcal{V}ar(u \mid C)$ are all below some unfrozen kind $[s_i]$, and (ii) the position q at which the rewrite takes place is non-frozen.

5.3. Solving Reachability Goals through Constrained Narrowing

Let $u \mid C$ and $v \mid D$ be constrained terms with $\mathcal{V}ar(u \mid C) \cap \mathcal{V}ar(v \mid D) = \emptyset$. We can use constrained narrowing as a symbolic method to find an NC-solution for the reachability problem $u \mid C \rightsquigarrow^{\star} v \mid D$ as follows.

Definition 14. *Given a convergent FPP rewrite theory $\mathcal{R}$ and constrained terms $u_0 \mid C_0$ and $v \mid D$ with $\mathcal{V}ar(u_0 \mid C_0) \cap \mathcal{V}ar(v \mid D) = \emptyset$, we call $v \mid D$* symbolically reachable by constrained narrowing *from $u_0 \mid C_0$* with symbolic NC-solution *$(\alpha_1 \ldots \alpha_n \delta)|_{\mathcal{V}ar(u_0|C_0)} \uplus \delta|_{\mathcal{V}ar(v|D)}$ iff there is a chain of constrained narrowing steps with $n \geq 0$ of the form:*

$$u_0 \mid C_0 \rightsquigarrow_{\alpha_1} u_1 \mid C_1 \rightsquigarrow_{\alpha_2} u_2 \mid C_2 \cdots u_{n-1} \mid C_{n-1} \rightsquigarrow_{\alpha_n} u_n \mid C_n$$

and a standardized apart unifier $\delta \in CSU_B(u_n, v)$ with $Dom(\delta) = \mathcal{V}ar(u_n) \uplus \mathcal{V}ar(v)$ such that:

1. *$(\alpha_1 \ldots \alpha_n \delta)|_{\mathcal{V}ar(u_0|C_0)}$ and δ are normalized*
2. *for each i, $1 \leq i < n$, $(\alpha_{i+1} \ldots \alpha_n \delta)|_{\mathcal{V}ar(u_i)}$ is normalized*
3. *for each i, $1 \leq i \leq n$, let $\vec{y_i}$ be the* fresh *variables of condition D_i of the rule $l_i \to r_i$ if D_i used in the narrowing step $u_{i-1} \mid C_{i-1} \rightsquigarrow_{\alpha_i} u_i \mid C_i$, then $(\alpha_i \ldots \alpha_n \delta)|_{\vec{y_i}}$ is normalized.*

We say that such a symbolic NC-solution $(\alpha_1 \ldots \alpha_n \delta)|_{\mathcal{V}ar(u_0|C_0)} \uplus \delta|_{\mathcal{V}ar(v|D)}$ has an actual NC-solution instance *$(\alpha_1 \ldots \alpha_n \delta\rho)|_{\mathcal{V}ar(u_0|C_0)} \uplus \delta\rho|_{\mathcal{V}ar(v|D)}$ iff there is a normalized substitution ρ with $Dom(\rho) \subseteq \mathcal{V}ar(u_0\alpha_1 \ldots \alpha_n\delta) \cup \mathcal{V}ar((v \mid C_n \wedge D)\delta)$ such that:*

1. *$\mathcal{R} \vdash (C_n \wedge D)\delta\rho$.*
2. *$(\alpha_1 \ldots \alpha_n \delta\rho)|_{\mathcal{V}ar(u_0|C_0)}$ and $\delta\rho$ are normalized*
3. *for each i, $1 \leq i < n$, $(\alpha_{i+1} \ldots \alpha_n \delta\rho)|_{\mathcal{V}ar(u_i)}$ is normalized*
4. *for each i, $1 \leq i \leq n$, $(\alpha_i \ldots \alpha_n \delta\rho)|_{\vec{y_i}}$ is normalized.*

Remark 3. *For the reasons given in Remark 2, Definition 14 can be easily adapted to a convergent FPP theory $\mathcal{R}_\phi$ with B-stable frozenness map ϕ that has a family of unfrozen kinds and with unfrozen conditions provided: (i) the kinds of the terms in each condition of $C_0 \wedge D$ have unfrozen kinds; (ii) the kinds of all variables in $\mathcal{V}ar(u_0 \mid C_0) \cup \mathcal{V}ar(v \mid B)$ have unfrozen kinds; and (iii) the positions at which narrowing takes place in the narrowing sequence are all unfrozen positions.*

The correctness of constrained narrowing as a symbolic method to solve reachability goals is expressed in the following theorem.

Theorem 3 (Soundness Theorem). *Given a convergent FPP rewrite theory $\mathcal{R} = (\Sigma, B, R)$ and constrained terms $u_0 \mid C_0$ and $v \mid D$ with $\mathcal{V}ar(u_0 \mid C_0) \cap \mathcal{V}ar(v \mid D) = \emptyset$, if $v \mid D$ is symbolically reachable by constrained narrowing from $u_0 \mid C_0$ with symbolic NC-solution $(\alpha_1 \ldots \alpha_n \delta)|_{\mathcal{V}ar(u|C)} \uplus \delta|_{\mathcal{V}ar(v|D)}$, any actual NC-solution instance $(\alpha_1 \ldots \alpha_n \delta\rho)|_{\mathcal{V}ar(u|C)} \uplus \delta\rho|_{\mathcal{V}ar(v|D)}$ is an NC-solution of the reachability goal $u_0 \mid C_0 \rightsquigarrow^\star v \mid D$.*

Proof. Suppose that $(\alpha_1 \ldots \alpha_n \delta\rho)|_{\mathcal{V}ar(u|C)} \uplus \delta\rho|_{\mathcal{V}ar(v|D)}$ is an actual NC-solution instance. This means that there are standardized apart rules $l_i \to r_i$ *if* D_i in R, and positions $p_i \in Pos(u_{i-1})$, $1 \leq i \leq n$ such that:

1. $\alpha_i \in CSU_B(l_i, (u_{i-1})_{p_i})$, $1 \leq i \leq n$
2. $u_i = u_{i-1}[r_i]_{p_i}\alpha_i$, $1 \leq i \leq n$
3. $C_i = (C_{i-1} \wedge D_i)\alpha_i$. $1 \leq i \leq n$.

But (3) implies that $\mathcal{R} \vdash (C_n \wedge D)\delta\rho$ exactly means that:

- $\mathcal{R} \vdash C_0\alpha_1 \ldots \alpha_n\delta\rho$
- $\mathcal{R} \vdash D_i\alpha_i \ldots \alpha_n\delta\rho$, $1 \leq i \leq n$, and
- $\mathcal{R} \vdash D\delta\rho$.

And since $(\alpha_i \ldots \alpha_n\delta\rho)|_{\vec{y}_i}$ is normalized and $\mathcal{R}$ is FPP, (1) and (2) then mean that there is an NC-rewrite step $u_{i-1}\alpha_i \ldots \alpha_n\delta\rho \to_{R,B} u_i\alpha_{i+1} \ldots \alpha_n\delta\rho$, $1 \leq i \leq n$. This, together with the fact that $u_n\delta\phi =_B v\delta\phi$, shows that there is an NC rewrite $u_0\alpha_1 \ldots \alpha_n\delta\rho \to^\star_{R,B} v\delta\phi$, and therefore that $(\alpha_1 \ldots \alpha_n\delta\rho)|_{\mathcal{V}ar(u|C)} \uplus \delta\rho|_{\mathcal{V}ar(v|D)}$ is an NC-solution of the reachability goal $u_0 \mid C_0 \rightsquigarrow^\star v \mid D$, as desired. □

Remark 4. *For the reasons given in Remarks 2–3, the above Soundness Theorem can be easily adapted to a convergent FPP theory $\mathcal{R}_\phi$ with B-stable frozenness map ϕ that has a family of unfrozen kinds and with unfrozen conditions provided: (i) the kinds of the terms in each condition of $C_0 \wedge D$ have unfrozen kinds; (ii) the kinds of all variables in $\mathcal{V}ar(u_0 \mid C_0) \cup \mathcal{V}ar(v \mid D)$ have unfrozen kinds; and (ii) the positions at which narrowing takes place in the narrowing sequence are all unfrozen positions.*

Note that Conditions (1)–(3) in Definition 14 can be very useful in weeding out useless narrowing paths early on, thus making the symbolic search for NC solutions more efficient. We already used this approach in [32] to drastically reduce the number of narrowing steps in the *variant narrowing* strategy.

Example 5. *Let Σ be an unsorted signature with constants a, b, binary associative-commutative operator $+$, and unary symbols f, h and $[\_]$, and with rules:*

1. $f(x) \to x + y$ *if* $h(x) \to [y]$

2. $z + a + a \to z + b$
3. $h(x) \to [x]$.

It is not hard to show that this theory is convergent, and it is clearly FPP. Consider the reachability problem

$$f(f(x_0)) \mid \top \rightsquigarrow^{\star} x'_0 + b \mid \top$$

We can find a symbolic NC-solution by constrained narrowing as follows: a first constrained narrowing step

$$f(f(x_0)) \mid \top \rightsquigarrow_{\alpha_1} f(x_1 + y) \mid h(x_1) \to^{\star} [y]$$

using rule (1) with substitution $\alpha_1 = \{x_0 \mapsto x_1, x \mapsto x_1\}$*; a second constrained narrowing step*

$$f(x_1 + y) \mid h(x_1) \to^{\star} [y] \rightsquigarrow_{\alpha_2} x'_1 + y'_1 + y' \mid h(x'_1) \to^{\star} [y'_1] \wedge h(x'_1 + y'_1) \to^{\star} [y']$$

using rule (1) standardized apart as $f(x') \to x' + y'$ *if* $h(x') \to [y']$ *with substitution* $\alpha_2 = \{x_1 \mapsto x'_1, y \mapsto y'_1, x' \mapsto x'_1 + y'_1\}$*; a third constrained narrowing step*

$$x'_1+y'_1+y' \mid h(x'_1) \to^{\star} [y'_1] \wedge h(x'_1+y'_1) \to^{\star} [y'] \rightsquigarrow_{\alpha_3} z'+b \mid h(a) \to^{\star} [a] \wedge h(a+a) \to^{\star} [z']$$

using rule (2) with substitution $\alpha_3 = \{z \mapsto x', y' \mapsto z', x'_1 \mapsto a, y'_1 \mapsto a\}$*; and a final substitution* $\delta = \{z' \mapsto x_2, x'_0 \mapsto x_2\}$ *unifying* $z' + b$ *and the term to be reached* $x'_0 + b$*.*

This symbolic solution has an actual NC-solution instance thanks to the substitution $\rho = \{x_2 \mapsto a + a\}$*, which instantiates the condition* $h(a) \to^{\star} [a] \wedge h(a + a) \to^{\star} [x_2]$ *to a provable one and yields the actual solution* $\{x_0 \mapsto a, x'_0 \mapsto a+a\}$*, for which we have the NC-rewrite sequence:*

$$f(f(a)) \to_{R,AC} f(a + a) \to_{R,AC} a + a + a + a \to_{R,AC} b + a + a.$$

Other narrowing sequences can be rejected early on because they fail to satisfy conditions (1)–(3) in Definition 14. For example, after the above first narrowing step, there is a second, alternative narrowing step

$$f(x_1 + y) \mid h(x_1) \to^{\star} [y] \rightsquigarrow_{\alpha'_2} f(z_1 + z_2 + b) \mid h(z_2) \to^{\star} [a + a + z_1]$$

using rule (2) with substitution $\alpha'_2 = \{x_1 \mapsto z_2, y \mapsto a + a + z_1, z \mapsto z_1 + z_2\}$*. This alternative path can be immediately rejected, because* α'_2 *maps the fresh variable* y *in the condition of rule (1) to a term reducible by rule (2), violating condition (3) in Definition 14.*

Is constrained narrowing a *complete* method to symbolically describe NC-solutions of reachability problems for $\mathcal{R}$ convergent and FPP? The positive answer is made precise in the following theorem.

Theorem 4 (Completeness of Constrained Narrowing). *Let $\mathcal{R}$ be convergent and FPP, $u_0 \mid C_0$ and $v \mid D$ two constrained terms with $\mathcal{V}ar(u_0 \mid C_0) \cap \mathcal{V}ar(v \mid D) = \emptyset$, and β, η normalized substitutions, with $Dom(\beta) \subseteq \mathcal{V}ar(u_0 \mid C_0)$ and $Dom(\eta) \subseteq \mathcal{V}ar(v \mid D)$, such that $\beta \uplus \eta$ is an NC-solution of the reachability problem $u_0 \mid C_0 \rightsquigarrow^{\star} v \mid D$ with an NC-rewrite sequence $u_0\beta \rightarrow_{R,B} w_1 \rightarrow_{R,B} w_2 \cdots w_{n-1} \rightarrow_{R,B} w_n =_B v\eta$. Then there is a symbolic NC-solution with constrained narrowing sequence $u_0 \mid C_0 \rightsquigarrow_{\alpha_1} u_1 \mid C_1 \rightsquigarrow_{\alpha_2} u_2 \mid C_2 \cdots u_{n-1} \mid C_{n-1} \rightsquigarrow_{\alpha_n} u_n \mid C_n$ and B-unifier $\delta \in CSU_B(u_n, v)$, and a substitution ρ with $Dom(\rho) \subseteq \mathcal{V}ar(u_0\alpha_1 \ldots \alpha_n\delta) \cup \mathcal{V}ar((v \mid C_n \wedge D)\delta)$ such that $(\alpha_1 \ldots \alpha_n\delta\rho)|_{\mathcal{V}ar(u_0|C_0)} \uplus \delta\rho|_{\mathcal{V}ar(v|D)}$ is an* actual NC-solution instance *and, furthermore:*

1. *$\beta =_B (\alpha_1 \ldots \alpha_n\delta\rho)|_{\mathcal{V}ar(u_0|C_0)}$ and $\eta =_B \delta\rho|_{\mathcal{V}ar(v|D)}$*

2. *the NC-rewrite sequence*

$$u_0\alpha_1 \ldots \alpha_n\delta\rho \rightarrow_{R,B} u_1\alpha_2 \ldots \alpha_n\delta\rho \ldots u_{n-1}\alpha_n\delta\rho \rightarrow_{R,B} u_n\delta\rho =_B v\delta\rho$$

ensured by the Soundness Theorem is such that: (i) $u_0\beta =_B u_0\alpha_1 \ldots \alpha_n\delta\rho$, (ii) for each i, $1 \leq i \leq n$, $w_i =_B u_i\alpha_{i+1} \ldots \alpha_n\delta\rho$, and (iii) $v\eta =_B v\delta\rho$.

Proof. The proof is by induction on the number n of NC-rewrite steps in the NC-rewrite sequence $u_0\beta \rightarrow_{R,B} w_1 \rightarrow_{R,B} w_2 \cdots w_{n-1} \rightarrow_{R,B} w_n =_B v\eta$. For $n = 0$ we have $u_0\beta =_B v\eta$ and, since $\mathcal{V}ar(u_0) \cap \mathcal{V}ar(v) = \emptyset$, there is a B-unifier $\delta \in CSU_B(u_n, v)$ and a substitution ρ_0 with $Dom(\rho_0) \subseteq Ran(\delta)$ such that $\beta|_{\mathcal{V}ar(u_0)} =_B \delta\rho_0|_{\mathcal{V}ar(u_0)}$, and $\eta|_{\mathcal{V}ar(v)} =_B \delta\rho_0|_{\mathcal{V}ar(v)}$. Extending ρ_0 to ρ by defining:

$$\rho = \beta|_{\mathcal{V}ar(C_0)-\mathcal{V}ar(u_0)} \uplus \rho_0 \uplus \eta|_{\mathcal{V}ar(D)-\mathcal{V}ar(v)}$$

gives us the desired NC-solution instance satisfying the requirements in the theorem.

Suppose that the theorem holds for any NC-solutions of reachability problems with associated NC-rewrite sequences of length less than n and let $\beta \uplus \eta$ be an NC-solution of the problem $u_0 \mid C_0 \rightsquigarrow^{\star} v \mid D$ with associated NC-rewrite sequence $u_0\beta \rightarrow_{R,B} w_1 \rightarrow_{R,B} w_2 \ldots w_{n-1} \rightarrow_{R,B} w_n =_B v\eta$. In particular, the NC-rewrite $u_0\beta \rightarrow_{R,B} w_1$ corresponds to a non-variable position p_1, a rule $l_1 \rightarrow r_1$ *if* D_1 and substitution σ such that $w_1 = u_0\beta[r_1\sigma]_{p_1}$ and, by the Lifting Lemma, there is a unifier α_1, a constrained narrowing step $u_0 \mid C_0 \rightsquigarrow_{\alpha_1} u_1 \mid C_1$ with $u_1 \mid C_1 = (u_0[r_1]_{p_1} \mid C_0 \wedge D_1)\alpha_1$, and a normalized substitution γ such that:

1. $(\alpha_1\gamma)|_{\mathcal{V}ar(u_0|C_0)} =_B \beta$

2. $(\alpha_1\gamma)|_{\mathcal{V}ar(l_1 \rightarrow r_1 \textit{ if } D_1)} =_B \sigma$

3. there is an NC-rewrite $u_0\alpha_1\gamma \rightarrow_{R,B} u_0[r_1]_{p_1}\alpha_1\gamma$ with $u_0\beta =_B u_0\alpha_1\gamma$, and $u_0[r_1]_{p_1}\alpha_1\gamma =_B w_1$

4. $\mathcal{R} \vdash (C_0 \wedge D_1)\alpha_1\gamma$.

Therefore, by Theorem 1 there is an NC-rewrite sequence

$$u_0\alpha_1\gamma \to_{R,B} u_0[r_1]_{p_1}\alpha_1\gamma \to_{R,B} w'_2 \ldots w'_{n-1} \to_{R,B} w'_n =_B v\eta$$

with $w_i =_B w'_i$, $2 \leq i \leq n$. This means that $\gamma|_{\mathcal{V}ar(u_1|C_1)} \uplus \eta$ is an NC-solution of the reachability problem $u_1 \mid C_1 \leadsto^\star v \mid D$ with $n-1$ NC-rewrite steps. Therefore, by the induction hypothesis there is a symbolic solution with narrowing sequence[8] $u_1 \mid C_1 \leadsto_{\alpha_2} u_2 \mid C_2 \cdots u_{n-1} \mid C_{n-1} \leadsto_{\alpha_n} n_n \mid C_n$ and B-unifier $\delta \in CSU_B(u_n, v)$, and a normalized substitution ρ_0 with $Dom(\rho_0) \subseteq \mathcal{V}ar(u_1\alpha_2\ldots\alpha_n\delta) \cup \mathcal{V}ar((v \mid C_n \wedge D)\delta)$ such that $(\alpha_2\ldots\alpha_n\delta\rho_0)|_{\mathcal{V}ar(u_1|C_1)} \uplus \delta\rho_0|_{\mathcal{V}ar(v|D)}$ is an actual NC-solution instance and, furthermore:

1. $\gamma|_{\mathcal{V}ar(u_1|C_1)} =_B (\alpha_2\ldots\alpha_n\delta\rho_0)|_{\mathcal{V}ar(u_1|C_1)}$ and $\eta =_B \delta\rho_0|_{\mathcal{V}ar(v|D)}$
2. the NC-rewrite sequence

   $$u_1\alpha_2\ldots\alpha_n\delta\rho_0 \to_{R,B} u_2\alpha_3\ldots\alpha_n\delta\rho_0 \ldots u_{n-1}\alpha_n\delta\rho \to_{R,B} u_n\delta\rho_0 =_B v\delta\rho_0$$

   is such that: (i) $u_1\gamma =_B u_1\alpha_2\ldots\alpha_n\delta\rho_0$, (ii) for each i, $2 \leq i \leq n$, $w'_i =_B u_i\alpha_{i+1}\ldots\alpha_n\delta\rho_0$, and (iii) $v\eta =_B v\delta\rho_0$.

Since by the assumptions in Footnote 8 we have a narrowing sequence $u_0 \mid C_0 \leadsto_{\alpha_1} u_1 \mid C_1 \leadsto_{\alpha_2} u_2 \mid C_2 \cdots u_{n-1} \mid C_{n-1} \leadsto_{\alpha_n} n_n \mid C_n$ and a B-unifier $\delta \in CSU_B(u_n, v)$, the natural candidate for the desired NC-solution instance would be $(\alpha_1\alpha_2\ldots\alpha_n\delta\rho_0)|_{\mathcal{V}ar(u_0|C_0)} \uplus \delta\rho_0|_{\mathcal{V}ar(v|D)}$. The problem, however, is that we need a normalized substitution ρ with $Dom(\rho) \subseteq \mathcal{V}ar(u_0\alpha_1\alpha_2\ldots\alpha_n\delta) \cup \mathcal{V}ar((v \mid C_n \wedge D)\delta)$, which may properly contain $Dom(\rho_0) \subseteq \mathcal{V}ar(u_1\alpha_2\ldots\alpha_n\delta) \cup \mathcal{V}ar((v \mid C_n \wedge D)\delta)$. This is because $u_1 = u_0[r_1]_{p_1}\alpha_1$, and the righthand side r_1 of the rule $l_1 \to r_1$ *if* D_1 may drop some of the variables of l_1. That is, the set $\vec{z_1} = Ran(\alpha_1) - \mathcal{V}ar(u_1)$ may be non-empty. But by the standardization apart assumptions in Footnote 8, $\vec{z_1} \cap Dom(\alpha_2\ldots\alpha_n\delta) = \emptyset$, so that $\vec{z_1}\alpha_2\ldots\alpha_n\delta = \vec{z_1}$, and our desired ρ has $Dom(\rho) \subseteq \mathcal{V}ar(u_0\alpha_1\alpha_2\ldots\alpha_n\delta) \cup \mathcal{V}ar((v \mid C_n \wedge D)\delta) = \vec{z_1} \uplus \mathcal{V}ar(u_1\alpha_2\ldots\alpha_n\delta) \cup \mathcal{V}ar((v \mid C_n \wedge D)\delta) = \vec{z_1} \uplus Dom(\rho_0)$. We can choose ρ as the normalized substitution extending ρ_0 as $\rho = \rho_0 \cup \gamma|_{\vec{z_1}}$. All we have left is to prove that ρ yields an actual NC-solution instance satisfying conditions (1)–(2) in the Theorem.

First of all note that, again, by the standardization apart, we have for each i, $1 \leq i < n$, $(\alpha_{i+1}\ldots\alpha_n\delta\rho)|_{\mathcal{V}ar(u_i)} = (\alpha_{i+1}\ldots\alpha_n\delta\rho_0)|_{\mathcal{V}ar(u_i)}$, which is normalized by the induction hypothesis, and for each i, $2 \leq i \leq n$, $\alpha_i\ldots\alpha_n\delta\rho|_{\vec{y_i}} = \alpha_i\ldots\alpha_n\delta\rho_0|_{\vec{y_i}}$, which again is normalized by the induction hypothesis. Likewise, $(C_n \wedge D)\delta\rho = (C_n \wedge D)\delta\rho_0$, so that $\mathcal{R} \vdash (C_n \wedge D)\delta\rho$. With respect to the fresh variables $\vec{y_1}$ of D_1, since $\vec{y_1}\alpha_1 = \vec{y_1}$ and $\vec{y_1} \subseteq \mathcal{V}ar(u_1 \mid C_1)$, the above equality

[8] Since we will later use the longer narrowing sequence $u_0 \mid C_0 \leadsto_{\alpha_1} u_1 \mid C_1 \leadsto_{\alpha_2} u_2 \mid C_2 \cdots u_{n-1} \mid C_{n-1} \leadsto_{\alpha_n} n_n \mid C_n$, we furthermore assume that the rules and unifiers in the subsequent steps are standardized apart with respect to the variables used in the initial step $u_0 \mid C_0 \leadsto_{\alpha_1} u_1 \mid C_1$.

$\gamma|_{\mathcal{V}ar(u_1|C_1)} =_B (\alpha_2 \ldots \alpha_n \delta\rho_0)|_{\mathcal{V}ar(u_1|C_1)}$ and γ normalized means, using again standardization apart, that $(\alpha_1\alpha_2 \ldots \alpha_n \delta\rho)|_{\vec{y}_1}$ is normalized. Also, $\delta\rho = \gamma|_{\vec{z_1}} \uplus \delta\rho_0$ and therefore is normalized. Furthermore, $(\delta\rho)|_{\mathcal{V}ar(v|D)} = \delta(\rho|_{\mathcal{V}ar((v|D)\delta)}) = \delta(\rho_0|_{\mathcal{V}ar((v|D)\delta)}) = (\delta\rho_0)|_{\mathcal{V}ar(v|D)} =_B \eta$, proving the second part of (1). So we just need to prove that $(\alpha_1\alpha_2 \ldots \alpha_n \delta\rho)|_{\mathcal{V}ar(u_0|C_0)}$ is normalized, so that we have an NC-solution, and that the first part of (1) and (2) hold. Since $\beta =_B (\alpha_1\gamma)|_{\mathcal{V}ar(u_0|C_0)}$, if we can prove $(\alpha_1\alpha_2 \ldots \alpha_n \delta\rho)|_{\mathcal{V}ar(u_0|C_0)} =_B (\alpha_1\gamma)|_{\mathcal{V}ar(u_0|C_0)}$, we will prove both the first part of (1) and $(\alpha_1\alpha_2 \ldots \alpha_n \delta\rho)|_{\mathcal{V}ar(u_0|C_0)}$ normalized. It is helpful to consider the following sets of variables: $\vec{x}_{p_1} = \mathcal{V}ar((u_0)_{p_1})$, $\vec{z}_0 = \mathcal{V}ar(u_0 \mid C_0) - \vec{x}_{p_1}$, $\vec{z}_2 = Ran(\alpha_1) - \vec{z}_1$, and to recall that $\vec{y}_1$ are the fresh variables of the FPP condition D_1. We then get the following partitions of variables: $\mathcal{V}ar(u_0 \mid C_0) = \vec{x}_{p_1} \uplus \vec{z}_0$, and $\mathcal{V}ar(u_1 \mid C_1) = \vec{z}_2 \uplus \vec{y}_1 \uplus \vec{z}_0$. Therefore, $(\alpha_1\alpha_2 \ldots \alpha_n \delta\rho)|_{\mathcal{V}ar(u_0|C_0)} = (\alpha_1\alpha_2 \ldots \alpha_n \delta\rho)|_{\vec{x}_{p_1}} \uplus (\alpha_1\alpha_2 \ldots \alpha_n \delta\rho)|_{\vec{z}_0}$. But, using standardization apart, the definition of ρ, and the equality $\gamma|_{\mathcal{V}ar(u_1|C_1)} =_B (\alpha_2 \ldots \alpha_n \delta\rho_0)|_{\mathcal{V}ar(u_1|C_1)}$, we get:

$$(\alpha_1\alpha_2 \ldots \alpha_n \delta\rho)|_{\vec{x}_{p_1}} = \alpha_1((\alpha_2 \ldots \alpha_n \delta\rho)|_{\vec{z}_1 \uplus \vec{z}_2}) =_B \alpha_1(\gamma|_{\vec{z}_1} \uplus \gamma|_{\vec{z}_2}) = (\alpha_1\gamma)|_{\vec{x}_{p_1}}.$$

Likewise, $(\alpha_1\alpha_2 \ldots \alpha_n \delta\rho)|_{\vec{z}_0} = (\alpha_2 \ldots \alpha_n \delta\rho)|_{\vec{z}_0} =_B \gamma|_{\vec{z}_0} = \alpha_1\gamma|_{\vec{z}_0}$, giving us $(\alpha_1\alpha_2 \ldots \alpha_n \delta\rho)|_{\mathcal{V}ar(u_0|C_0)} =_B (\alpha_1\gamma)|_{\mathcal{V}ar(u_0|C_0)}$ and therefore both the first part of (1) and its being normalized. For (2), note that: (i) $u_0\beta =_B u_0\alpha_1\gamma =_B u_0\alpha_1\alpha_2 \ldots \alpha_n\delta\rho$; (ii) for each i, $1 \leq i \leq n$, $w_i =_B w'_i = u_i\alpha_{i+1} \ldots \alpha_n\delta\rho$; and (iii) $u_n\delta\rho =_B v\delta\rho =_B v\eta$. □

Remark 5. *Using Remarks 2, 3 and 4, the above Completeness Theorem can be easily adapted to a convergent FPP theory $\mathcal{R}_\phi$ with B-stable frozenness map ϕ that has a family of unfrozen kinds and with unfrozen conditions provided: (i) the kinds of the terms in each condition of $C_0 \wedge D$ have unfrozen kinds; (ii) the kinds of all variables in $\mathcal{V}ar(u_0 \mid C_0) \cup \mathcal{V}ar(v \mid B)$ have unfrozen kinds; and (ii) the positions at which rewriting takes place in the NC-rewrite sequence $u_0\beta \to_{R,B} w_1 \to_{R,B} w_2 \cdots w_{n-1} \to_{R,B} w_n =_B v\eta$ are all unfrozen positions.*

The completeness of NC-rewriting immediately shows that, if v is strongly irreducible, constrained narrowing is a complete method to find as instances *all* solutions of a reachability problem $u_0 \mid C_0 \rightsquigarrow^\star v \mid D$, and not just NC-solutions.

Corollary 1. *If in Theorem 4 the term v is strongly irreducible, we can weaken the assumption on $\beta\uplus\eta$ to just be a solution of the reachability problem $u_0 \mid C_0 \rightsquigarrow^\star v \mid D$. Since $v\eta$ is normalized, the rewrite $u_0\beta \to^{!}_{R,B} v\eta$ has a description as an NC-rewrite sequence, so that $\beta \uplus \eta$ is an NC-solution.*

6. Constrained Variants and Constrained Unification

The completeness of constrained narrowing and Corollary 1 yield two useful symbolic methods, one for describing symbolically all $\mathcal{E}$-variants of a term in an equational theory $\mathcal{E} = (\Sigma, E \uplus B)$ by constrained narrowing with a convergent

FPP rewrite theory $(\Sigma, B, \vec{E})$, and another for describing symbolically all $E \uplus B$-unifiers of two terms by constrained narrowing with such a theory $(\Sigma, B, \vec{E})$.

The $\mathcal{E}$-variants of a term have only been defined for *unconditional* equational theories $\mathcal{E}$ [19, 32]. The following definition generalizes the variant notion to the conditional case.

Definition 15 (Variants). *Let $\mathcal{E} = (\Sigma, E \uplus B)$ be an order-sorted conditional equational theory such that $\mathcal{R}_{\mathcal{E}} = (\Sigma, B, \vec{E})$ is a convergent FPP rewrite theory. Given a term t, an* $\mathcal{E}$-variant *of t is a pair (u, θ) with u a Σ-term and θ a substitution such that: (i) $Dom(\theta) \subseteq \mathcal{V}ar(t)$, (ii) $\theta = \theta!_{\vec{E},B}$, and (iii) $u =_B (t\theta)!_{\vec{E},B}$.*

Intuitively, we can think of the variants of a term t as the different *patterns* in $\vec{E}, B$-canonical form associated to instances of t.

As shown in [32], in the unconditional case the $\mathcal{E}$-variants of a term can be computed symbolically by *folding variant narrowing*. Can we have in the conditional case a constrained notion of variant as a symbolic way and method of describing all variants?

Definition 16 (Constrained Variant). *Let $\mathcal{E} = (\Sigma, E \uplus B)$ be an order-sorted conditional equational theory such that $\mathcal{R}_{\mathcal{E}} = (\Sigma, B, \vec{E})$ is a convergent FPP rewrite theory. A* constrained $\mathcal{E}$-variant *of a term t is a pair $(u_n\delta \mid C_n\delta, (\alpha_1 \cdots \alpha_n\delta)|_{\mathcal{V}ar(t)})$ such that the constrained narrowing sequence $t \mid \top \leadsto_{\alpha_1} u_1 \mid C_1 \leadsto \cdots \leadsto u_{n-1} \mid C_{n-1} \leadsto_{\alpha_n} u_n \mid C_n$, $n \geq 0$, together with the B-unifier $\delta \in CSU_B(u_n, x{:}\mathsf{s})$ is a symbolic NC-solution of the reachability problem $t \mid \top \leadsto^\star x{:}\mathsf{s} \mid \top$, where $s = ls(t)$, and x is a fresh variable not appearing in t.*

Note that conditions (1)–(2) in Definition 14, plus the fact that $u_n\delta =_B x{:}\mathsf{s}\delta$ ensure that: (i) $u_n\delta$ is normalized, and (ii) $\alpha_1 \cdots \alpha_n\delta|_{\mathcal{V}ar(t)}$ is a normalized substitution. In summary, therefore, a constrained variant of t is a pair $(v \mid C, \theta)$ obtained by constrained narrowing from $t \mid \top$ such that, if C were provable, (v, θ) would be an actual variant of t. As we show below, the key point about constrained variants is that they "cover" as instances all actual variants of t.

Note that $x{:}\mathsf{s}$ is a strongly irreducible term. Therefore, Corollary 1 applies, and we get as an immediate consequence of the Completeness Theorem for constrained narrowing the following completeness result, showing that constrained variants contain as instances *all* variantes up to B-equality.

Theorem 5 (Completeness of Constrained $\mathcal{E}$-Variants). *For $\mathcal{R}_{\mathcal{E}}$ as above, let t be a term and let (w, θ) be an $\mathcal{E}$-variant of t. Then there is a constrained $\mathcal{E}$-variant $(v \mid C, \gamma)$ and a normalized substitution ρ such that:*

1. *$v\rho =_B w$*

2. *$\theta =_B \gamma\rho$*

3. *$\mathcal{R}_{\mathcal{E}} \vdash C\rho$.*

Let $\mathcal{R}_{\mathcal{E}}$ be as above, and consider an $\mathcal{E}$-unification problem $u \overset{?}{=}_{E\cup B} v$. Note that, since $\mathcal{R}_{\mathcal{E}}$ is Church-Roser, θ is an $\mathcal{E}$-unifier iff $(u\theta)!_{\vec{E},B} =_B (v\theta)!_{\vec{E},B}$. Furthermore, without loss of generality we may assume $\theta = \theta!_{\vec{E},B}$. Note that, by assuming that for each top sort $[\mathsf{s}]$ in each connected component we add a fresh new sort $\mathsf{Pair}.[\mathsf{s}]$ in its own connected component and a pairing operator $< \_, \_ >$: $[\mathsf{s}]$ $[\mathsf{s}]$ $\to$ $\mathsf{Pair}.[\mathsf{s}]$, we can recast an $\mathcal{E}$-unification problem $u \overset{?}{=}_{E\cup B} v$ as a reachability problem $< u, v > \leadsto^{\star} < x, x >$ where x is a fresh variable not appearing in u and v and having the top sort $[\mathsf{s}]$ of the connected component of the sorts of u and v.

Definition 17 (Constrained $\mathcal{E}$-Unifier). *Let $\mathcal{R}_{\mathcal{E}}$ be as above. A* constrained $\mathcal{E}$-unifier *of a $\mathcal{E}$-unification problem $u \overset{?}{=}_{E\cup B} v$ is a pair of the form*

$$\alpha_1 \cdots \alpha_n \delta \mid C_n \gamma \delta$$

such that $< u, v > \leadsto_{\alpha_1} < u_1, v_1 > \leadsto \cdots \leadsto_{\alpha_n} < u_n, v_n >$ together with the B-unifier $\delta \in CSU_B(< u_n, v_n >, < x, x >)$ is a symbolic NC-solution of the reachability problem $< u, v > \mid \top \leadsto^{\star} < x, x > \mid \top$.

Note that conditions (1)–(2) in Definition 14, plus the fact that $< u_n, v_n > \delta =_B < x, x > \delta$ ensure that: (i) $\alpha_1 \cdots \alpha_n \delta|_{\mathcal{V}ar(<u,v>)}$ is a normalized substitution, and (ii) $u_n\delta$ and $v_n\delta$ are normalized.

Again, since $< x, x >$ is strongly irreducible, Corollary 1 applies, and we get as an immediate consequence of the Completeness Theorem for constrained narrowing the completeness of constrained unifiers to describe symbolically all (normalized) $\mathcal{E}$-unifiers up to B-equality.

Theorem 6 (Completeness of Constrained $\mathcal{E}$-unifiers). *Let $\mathcal{R}_{\mathcal{E}}$ be as above, and let $\theta = \theta!_{\vec{E},B}$ be a unifier of $u \overset{?}{=}_{E\cup B} v$. Then there is a constrained unifier $\gamma \mid D$ and a normalized substitution ρ such that:*

1. *$\gamma\rho =_B \theta$*
2. *$\mathcal{R}_{\mathcal{E}} \vdash D\rho$.*

Using a second tupling constructor, a simultaneous unification problem

$$u_1 \overset{?}{=}_{E\cup B} v_1 \wedge \cdots \wedge u_n \overset{?}{=}_{E\cup B} v_n$$

can be reduced to the single unification problem

$$< u_1, \ldots, u_n > \overset{?}{=}_{E\cup B} < v_1, \ldots, v_n >$$

and be symbolically described by its constrained unifiers.

There is of course the alternative, already described after Definition 10, of extending $\mathcal{R}_{\mathcal{E}}$ with a new sort *Truth*, with a constant tt $:\to$ *Truth*, in a new connected component, and adding for each top sort $[s]$ in each connected component of the sorts of $\mathcal{R}_{\mathcal{E}}$ the predicate $\_ \equiv \_ : [s]\ [s] \to \mathit{Truth}$ and the rule

$x \equiv x \to tt$. In this way we can, alternatively, *reduce* any $\mathcal{E}$-unification problem $u \overset{?}{=}_{E \cup B} v$ to the problem of computing the *variants* of the term $u \equiv v$ that have the form (tt, θ), which, by Theorem 5, can all be obtained as instances of constrained variants of the form $(tt \mid C, \gamma)$. However, since all constrained unifiers computed according to the treatment we have presented above are such that $u_n\delta$ and $v_n\delta$ are normalized, such a treatment may compute fewer constrained unifiers and may be more efficient. We leave a detailed comparison between both methods, including their experimental evaluation, as a subject for future research.

The advantage of constrained variants and constrained unifiers is that they can provide a more compact, yet complete, representation of, respectively, all $\mathcal{E}$-variants of a term and all $\mathcal{E}$-unifiers of a unification problem $u \overset{?}{=}_{E \cup B} v$. This can have many advantages, including the following two. First, in some cases there may be a finite set of constrained variants (resp. unifiers) when only an infinite set of variants (resp. unifiers) exists. This would allow achieving a finitely-braching search space instead of an infinitely-branching one, and postponing the possibly costly solution of the constrains until after some potential symbolic solution is found. Second, in conditional theories appearing in actual practice —particularly when sorts and subsorts are used— the set $\vec{E}_1$ of rules needed to solve the constraints generated by narrowing may be a proper subset of $\vec{E}$, and may even be unconditional and have the finite variant property. More generally, denoting $\vec{E} = \vec{E}_0$, we may have a sequence of increasingly simpler sets of equations $\vec{E}_0 \supset \vec{E}_1 \supset \ldots \vec{E}_k$, so that constraints generated using $\vec{E}_i$ can be handled with fewer and simpler rules in $\vec{E}_{i+1}$. This can make hierarchical, symbolic methods such as the computation of constrained variants and constrained unifiers quite effective. We illustrate these possibilities with an example.

Example 6. *As pointed out in the Introduction, a rewrite theory has often a non-equational meaning in which rules are viewed as transition rules in a concurrent system [56, 58]. We have developed, with K. Bae, a narrowing-based model checking method and implementation for such concurrent systems in [31, 9], called* logical model checking*, which allows rules to describe a concurrent system while the equational theory describes both system properties and state predicates. However, such logical model checking does not allow conditional transition rules or conditional equations. The work developed in this paper can clearly contribute to expanding the application of logical model checking by allowing conditional equations both for the system properties and the state predicates. Specifically, we are interested in performing model checking in a symbolic way with rewrite theories $(\Sigma, E \cup B, R)$ such that $(\Sigma, B, \vec{E})$ is a convergent FPP theory of the kind considered in this paper, and where the rules R may be conditional, but have only equational conditions that can be solved using the convergent FPP theory $(\Sigma, B, \vec{E})$.*

Let us consider a simple protocol example involving a data structure for messages exchanged between participants that is represented as a set. That is, we consider a sort Dataset *with a subsort* Data *and two operators, $\emptyset$ and an associative-commutative union operator & with equations $\emptyset$ & $y = y$, x & $x = x$*

and $y \mathbin{\&} x \mathbin{\&} x = y \mathbin{\&} x$ *using variables* $x, y{:}\mathsf{Dataset}$*. Assuming that communication channels may lose messages, the protocol repeats sending messages indefinitely, and thus channels may have repeated messages. Let us assume a very simple notion of state using symbol* $\_;\_;\_ : \mathsf{DataSet\ DataSet\ DataSet}$*, where the left component originally contains the initial data, the second component represents a unidirectional communication channel, and the third component will store the final data. For* S_0 *some specific data set to be sent, an initial configuration would be* $S_0; \emptyset; \emptyset$*, and the final configuration should be* $\emptyset; \emptyset; S_0$*.*

This protocol should satisfy an invariant asserting that all the information spread out among the communication channels is always the same, i.e., if there is an initial set of messages to be sent from sender participants to receiver participants, the set of messages scattered through all the channels is the same modulo repeated occurrences of messages. This is expressed with the following predicate $\textbf{\textit{inv}} : \mathsf{DataSet\ State} \to \mathsf{Bool}$ *which can be defined by the following conditional equation, oriented as the FPP rule:*

$$\textbf{\textit{inv}}(S_0, S_1; S_2; S_3) \to \textbf{\textit{true if}}\ S_1 \& S_2 \& S_3 \ \to S_4 \wedge \ S_0 \equiv S_4 \to tt. \qquad (5)$$

The equational theory $(\Sigma, B \uplus E_0 \uplus E_1)$ *associated to this example is a convergent FPP rewrite theory by orienting equations* E_1 *for symbol* & *and* E_0 *containing only Equation 5 into rules. Indeed, we have a hierarchical view of the equational theory, as explained above, where* $B \subset (E_1 \cup B) \subset (E_1 \cup E_0 \cup B)$*. The equational theory* $(\Sigma, B \cup E_1)$ *has the finite variant property and the latest version of the Maude tool can effectively generate variants and unifiers for it. Of course, the communication protocol is specified by a rewrite theory* $(\Sigma, B \uplus E_0 \uplus E_1, R)$ *where the rules* R *(not detailed here) specify the protocol transitions. We are in the desired, more general situation, since the underlying conditional equational theory* $(\Sigma, B \uplus E_0 \uplus E_1)$ *can be oriented as a convergent FPP rewrite theory* $(\Sigma, B, \vec{E}_0 \uplus \vec{E}_1)$*.*

In logical model checking, equational unification is performed every time a transition rule is applied by narrowing but this equational unification is restricted to the system properties, in this case properties of symbol &*. However, the generation of the logical state transition system requires instantiating every computed symbolic state in the transition system to a version where predicates can be evaluated to either* ***true*** *or* ***false****. Therefore, variants of symbolic states are generated using the equations for the state predicates. For example, given an initial data set* $m_0 \& m_1 \& m_2$ *and a state* $St = (m_1 \& X); m_1; (m_0 \& Y)$*, the variants of the term* $t = \textbf{\textit{inv}}(m_0 \& m_1 \& m_2, (m_1 \& X); m_1; (m_0 \& Y))$ *would be generated using constrained narrowing for the reachability goal* $t \mid \top \leadsto^\star x{:}\mathsf{s} \mid \top$*. In particular* *we get:*

$$\begin{array}{lr} \boldsymbol{inv}(m_0\&m_1\&m_2, (m_1\&X); m_1; (m_0\&Y)) \mid & \top \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\leadsto_{\alpha_1} & \\ \qquad\qquad\qquad\qquad\qquad\qquad\quad \boldsymbol{true} \mid & m_1\&X\&m_1\&m_0\&Y \to^\star S_4 \\ & \wedge \\ & S_4 \equiv m_0\&m_1\&m_2 \to^\star tt \end{array}$$

Finally, as explained before, the equational theory $(\Sigma, B, \vec{E_1})$ has the finite variant property and tools such as Maude can effectively solve the variant $E_1 \cup B$-unification problem

$$m_1\&X\&m_1\&m_0\&Y = m_0\&m_1\&m_2$$

whose more general solutions are $\sigma_1 = \{X \mapsto Z, Y \mapsto m_2\&Z\}$ and $\sigma_2 = \{X \mapsto m_2\&Z, Y \mapsto Z\}$.

An important issue left for future research is how to detect that a constrained variant (resp. constrained unifier) is *more general than* another (i.e., one subsumes another). Semantically, $(u \mid C, \alpha)$ is more general than $(v \mid D, \beta)$ iff there is a γ such that:

1. $u\gamma =_B v$, and
2. $\mathcal{R} \vdash (D \Rightarrow C\gamma)$ (i.e., for each substitution θ such that $\mathcal{R} \vdash D\theta$, we have that $\mathcal{R} \vdash C\gamma\theta$).

Likewise, $\alpha \mid C$ is semantically *more general* than $\beta \mid D$ (i.e., subsumes $\beta \mid D$) iff there is a substitution γ such that

1. $\alpha\gamma =_B \beta$, and
2. $\mathcal{R} \vdash (D \Rightarrow C\gamma)$

Of course, in both cases determining whether $\mathcal{R} \vdash (D \Rightarrow C\gamma)$ may in general be undecidable. However, either because we can use simpler equations $\vec{E_i}$ as described above, or by using a simple decidable condition, it may be possible to achieve checkable versions of subsumption for constrained variants and constrained unifiers.

Constrained variants and constrained unifiers seem appealing for symbolically and compactly representing all variants and unifiers of a conditional theory. But we can ask the question:

> *Given a constrained variant (resp. unifier) is there a systematic way to* extract *from it a complete family of the variants (resp. unifiers) that it represents?*

The answer, in the affirmative, is part of the more general method of *layered constrained narrowing* explained in Section 8.

7. A Useful Theory Transformation

Let $\mathcal{R}$ be a convergent, strongly deterministic FPP conditional order-sorted rewrite theory. In what follows it will be useful to bring to the object level certain meta-level constraints involving the operators $\_ \to^{\star} \_$ and $\_ \wedge \_$. This can be achieved by extending $\mathcal{R}$ (where S is its set of sorts) to a rewrite theory $\hat{\mathcal{R}}$ with the following new sorts:

- a sort Atom with a constant $\top$, and for each top sort $[\mathsf{s}]$ in S a new operator $\_ \to^{\star} \_ : [\mathsf{s}]\ [\mathsf{s}] \to \mathsf{Atom}$,
- a sort Cond with subsort $\mathsf{Atom} < \mathsf{Cond}$ and a binary operator $\_ \wedge \_ : \mathsf{Atom}\ \mathsf{Cond} \to \mathsf{Cond}$.

$\hat{\mathcal{R}}$ contains the axioms B and rules R of $\mathcal{R}$ plus the additional rules:

1. $(x \to^{\star} x) \to \top$, where x is a variable of the top sort $[\mathsf{s}]$ for each strongly connected component of S.
2. $(\top \wedge C) \to C$, where C is a variable of sort Cond

Since these rules are terminating and operate on a completely new connected component, it is not hard to show that, since $\mathcal{R}$ is operationally terminating, $\hat{\mathcal{R}}$ is also operationally terminating. By construction, the above rules cannot have any critical pairs with those in R, and do not themselves have any non-trivial critical pairs. Therefore $\hat{\mathcal{R}}$ is itself also a convergent FPP rewrite theory. In what follows, it will be useful to give to the new operators added to $\mathcal{R}$ in $\hat{\mathcal{R}}$ the following frozenness information using a mapping ϕ:

$$\phi(\_ \to^{\star} \_) = \{2\} \qquad\qquad \phi(\_ \wedge \_) = \{2\}$$

Instead, all operators f in $\mathcal{R}$ are unfrozen, i.e., $\phi(f) = \emptyset$. Since the only operators with frozenness restrictions obey no axioms, ϕ is clearly a B-stable map. It is easy to check that, if S is the set of sorts in $\mathcal{R}$, then $\hat{\mathcal{R}}_{\phi}$ is such that the kinds of S are unfrozen, with the conditions of the rules in $\hat{\mathcal{R}}$ also unfrozen.

What is the point of the transformation $\mathcal{R} \mapsto \mathcal{R}_{\phi}$? Why is it *useful*? The answer is: efficiency, efficiency, efficiency. What kind of efficiency? A massive reduction in the number of redexes where a conjunction of goals can be reduced: the frozenness requirement makes sure that only the *leftmost* term in the *leftmost* conjunct can be rewritten, as opposed to any possible redex in the conjunction. And why should we *care* about this kind of reduction? Because combinatorial explosion in narrowing search must be avoided like the plague, and in Section 8 we are going to *solve* the accumulated constrains obtained by constrained narrowing by a form of narrowing called *layered constrained narrowing* that will *use* $\mathcal{R}_{\phi}$ instead of $\mathcal{R}$ precisely to cut down the narrowing search space.

Note that the notion of a *layered proof* for a rewrite theory $\mathcal{R}$ (see Section 3.3) extends naturally to that of a layered proof for a theory $\mathcal{R}_{\phi}$, with frozenness information given by mapping ϕ, just by requiring that all rewrites take place at non-ϕ-frozen positions. In our case, since the conditions in the theory $\hat{\mathcal{R}}_\phi$ are unfrozen, the restrictions imposed by ϕ can apply at most to the first layer of such proofs: for all other layers the restrictions ϕ do not apply. A key point about the above extension is that we have the following equivalence, which ensures that the frozenness restrictions enforced in $\hat{\mathcal{R}}_\phi$, while massively reducing the possible redexes in a conjunction of goals, do not leave any condition unevaluated, that is, they can accomplish just the same final results as those obtained using the unrestricted theory $\hat{\mathcal{R}}$.

Theorem 7. *Let $u_1 \rightarrow^{\star}_{R,B} u'_1 \wedge \cdots \wedge u_n \rightarrow^{\star}_{R,B} u'_n$ be a conjunction of reachability goals, i.e., reachability problems, in $\mathcal{R}$. Then for each layered trace proof (resp. NC-proof[9]) $\#T \uparrow TS \uparrow \top\#$ in $\mathcal{R}$ of these reachability goals, there are:*

1. *a layered trace proof (resp. NC-proof) $\#T' \uparrow TS \uparrow \top\#$ of the following* transformed *sequence of reachability goals $(u_1 \rightarrow^{\star} v_1) \rightarrow^{\star} \top \wedge \cdots \wedge (u_n \rightarrow^{\star} v_n) \rightarrow^{\star} \top$ in $\hat{\mathcal{R}}_\phi$*

2. *a layered trace proof (resp. NC-proof) $\#T'' \uparrow TS \uparrow \top\#$ of the following* single *reachability goal $((u_1 \rightarrow^{\star} v_1) \wedge \cdots \wedge (u_n \rightarrow^{\star} v_n)) \rightarrow^{\star} \top$ in $\hat{\mathcal{R}}_\phi$*

Conversely, for any layered trace proofs (resp. NC-proofs) $\#T' \uparrow TS \uparrow \top\#$ and $\#T'' \uparrow TS \uparrow \top\#$ in $\hat{\mathcal{R}}_\phi$ of, respectively, the transformed reachability goals and the compact reachability goal above, there is a layered trace proof (resp. NC-proof) $\#T \uparrow TS \uparrow \top\#$ in $\mathcal{R}$.

Proof. We use throughout, without further mention, the fact that $\hat{\mathcal{R}}_\phi$ has unfrozen the kinds of $\mathcal{R}$ and unfrozen conditions. The layered trace proof $\#T \uparrow TS \uparrow \top\#$ of the given reachability goals in $\mathcal{R}$ is of the form:

$$\begin{array}{l} \#u_1 \rightarrow u_1^1 \rightarrow u_1^2 \rightarrow \cdots \rightarrow u_1^{k_1} =_B v_1 \wedge \cdots \wedge \\ \quad u_n \rightarrow u_n^1 \rightarrow u_n^2 \rightarrow \cdots \rightarrow u_n^{k_n} =_B v_n \uparrow TS \uparrow \top\# \end{array}$$

We can build a layered trace proof of the transformed reachability goals in $\hat{\mathcal{R}}_\phi$ of the form

$$\begin{array}{rl} \# & (u_1 \rightarrow^{\star} v_1) \rightarrow (u_1^1 \rightarrow^{\star} v_1) \rightarrow (u_1^2 \rightarrow^{\star} v_1) \rightarrow \cdots \rightarrow (u_1^{k_1} \rightarrow^{\star} v_1) \rightarrow \top =_B \top \\ & \hfill \wedge \cdots \wedge \\ & (u_n \rightarrow^{\star} v_n) \rightarrow (u_n^1 \rightarrow^{\star} v_n) \rightarrow (u_n^2 \rightarrow^{\star} v_n) \rightarrow \cdots \rightarrow (u_n^{k_1} \rightarrow^{\star} v_n) \rightarrow \top =_B \top \\ & \hfill \uparrow TS \uparrow \top\# \end{array}$$

[9] That is, a layered trace rewrite proof where *all* the rewrite steps (including those in evaluations of conditions) are NC-rewrites.

and likewise a layered trace proof of the compact reachability goal in $\hat{\mathcal{R}}_\phi$ of the form

$$\begin{array}{l}
\#((u_1 \rightarrow^\star v_1) \wedge \cdots (u_n \rightarrow^\star v_n)) \rightarrow^\star \top \\
\quad \rightarrow ((u_1^1 \rightarrow^\star v_1) \wedge \cdots (u_n \rightarrow^\star v_n)) \rightarrow^\star \top \\
\quad \rightarrow ((u_1^2 \rightarrow^\star v_1) \wedge \cdots (u_n \rightarrow^\star v_n)) \rightarrow^\star \top \\
\quad \vdots \\
\quad \rightarrow ((u_1^{k_1} \rightarrow^\star v_1) \wedge \cdots (u_n \rightarrow^\star v_n)) \rightarrow^\star \top \\
\quad \rightarrow (\top \wedge \cdots (u_n \rightarrow^\star v_n)) \rightarrow^\star \top \\
\quad \rightarrow ((u_2 \rightarrow^\star v_2) \wedge \cdots (u_n \rightarrow^\star v_n)) \rightarrow^\star \top \\
\quad \vdots \\
\quad \rightarrow ((u_2^{k_2} \rightarrow^\star v_2) \wedge \cdots (u_n \rightarrow^\star v_n)) \rightarrow^\star \top \\
\quad \rightarrow (\top \wedge \cdots (u_n \rightarrow^\star v_n)) \rightarrow^\star \top \\
\quad \rightarrow ((u_3 \rightarrow^\star v_3) \wedge \cdots (u_n \rightarrow^\star v_n)) \rightarrow^\star \top \\
\quad \vdots \\
\quad \rightarrow (u_n^{k_n} \rightarrow^\star v_n) \rightarrow^\star \top \\
\quad \rightarrow \top \rightarrow^\star \top \\
\quad \rightarrow \top =_B \top \uparrow TS \uparrow \top\#
\end{array}$$

The converse proof follows easily from the frozenness restrictions ϕ, which force the rewriting to be restricted to subterms of the form $u_1, u_1^1, \ldots, u_1^{k_1}, \ldots, u_n$, $u_n^1, \ldots, u_n^{k_n}$. Finally, since the levels TS of all proofs are the *same*, it is obvious by construction that NC rewriting proofs of the original reachability goals correspond to the NC rewriting proofs of both the transformed reachability goals and the compact reachability goal. □

Lemma 5. *Let $u_1 \rightarrow^\star_{R,B} u'_1 \wedge \cdots \wedge u_n \rightarrow^\star_{R,B} u'_n$ be such that for each i, $1 \leq i \leq n$, there is a strongly irreducible term v_i and a normalized substitution γ_i such that $u'_i =_B v_i\gamma_i$. Let θ be a substitution with $Dom(\theta) \subseteq \mathcal{V}ar(u_1 \rightarrow^\star_{R,B} u'_1 \wedge \cdots \wedge u_n \rightarrow^\star_{R,B} u'_n)$ and such that for each i, $1 \leq i \leq n$, $(\gamma_i\theta)|_{\mathcal{V}ar(v_i)}$ is normalized. Then if $(u_1 \rightarrow^\star_{R,B} u'_1 \wedge \cdots \wedge u_n \rightarrow^\star_{R,B} u'_n)\theta \rightarrow^* \top$ in $\hat{\mathcal{R}}$, there is an NC rewriting sequence for it satisfying the frozenness restrictions ϕ.*

Proof. First of all note that $u'_1\theta =_B v_1\gamma_1\theta, \ldots, u'_n\theta =_B v_n\gamma_n\theta$ are normalized, so no rewriting is possible for them. Second, it is easy to prove by induction on n that the above rewrite sequence is possible iff $u_1\theta!_{R,B} =_B v_1\gamma_1\theta, \ldots, u_n\theta!_{R,B} =_B v_n\gamma_n\theta$. Let $u_i\theta \rightarrow^* u_i\theta!_{R,B}$ be NC rewrite sequences, $1 \leq i \leq n$. We then obtain the following NC rewrite sequence satisfying the frozenness condition ϕ:

$$\begin{array}{l}
(u_1\theta \to^\star u'_1\theta \wedge \cdots \wedge u_n\theta \to^\star u'_n\theta) \\
\to^* (u_1\theta!_{R,B} \to^\star u'_1\theta \wedge u_2\theta \to^\star u'_2\theta \wedge \cdots \wedge u_n\theta \to^\star u'_n\theta) \\
\to (\top \wedge u_2\theta \to^\star u'_2\theta \wedge \cdots \wedge u_n\theta \to^\star u'_n\theta) \\
\to (u_2\theta \to^\star u'_2\theta \wedge \cdots \wedge u_n\theta \to^\star u'_n\theta) \\
\to^* (\top \wedge \cdots \wedge u_n\theta \to^\star u'_n\theta) \\
\qquad \vdots \\
\to (u_n\theta \to^\star u'_n\theta) \\
\to^* \top
\end{array}$$

□

8. Solving Constraints by Layered Constrained Narrowing

Constrained narrowing has an obvious advantage and an obvious limitation:

1. by not evaluating accumulated conditions and by the additional search space reduction techniques mentioned in the Introduction, it can drastically cut down the search space; but

2. it only yields *symbolic solutions*, whose accumulated constraint might be unsatisfiable; and how can we then *know* whether we have found an *actual* solution?

The good news about point (1) is that we can postpone condition evaluation until a symbolic solution has been found, thus avoiding wasteful searches that can easily go nowhere. But how can we solve the limitation involved in point (2)? That is, how can we pass from: (i) a complete set of *symbolic NC-solutions* to a reachability problem $u \mid C \rightsquigarrow^\star v \mid D$ with $u \mid C$ and $v \mid D$ constrained terms, and $\mathcal{V}ar(u \mid C) \cap \mathcal{V}ar(v \mid D) = \emptyset$ —that is, symbolic solutions that "cover" or "lift" all actual NC-solution $\beta \uplus \eta$— to (ii) a set of *most general actual NC-solutions* $\{\beta_i \uplus \eta_i\}_{i \in \mathcal{I}}$ to the same reachability problem?

The answer is: continue doing constrained narrowing, but now on the accumultated condition regarded as a *term.* Technically, key idea making this answer possible and search-efficient is to exploit the theory transformation in Section 7 that allows us to recast the solution of a conjunction of reachability goals in $\mathcal{R}$

$$u_1 \to^\star_{R,B} {u'}_1 \wedge \cdots \wedge u_n \to^\star_{R,B} {u'}_n$$

as a single reachability goal

$$(u_1 \to^\star_{R,B} {u'}_1 \wedge \cdots \wedge u_n \to^\star_{R,B} {u'}_n) \to^\star \top$$

in $\hat{\mathcal{R}}_\phi$. We can apply this idea to *solve by constrained narrowing* the accumulated condition $(C_n \wedge D)\delta$ computed by constrained narrowing when symbolically solving a goal $u \mid C \rightsquigarrow^{\star} v \mid D$. Indeed, we can do so by symbolically solving the reachability goal $(C_n \wedge D)\delta \mid \top \rightsquigarrow^{\star} \top \mid \top$ by constrained narrowing in $\hat{\mathcal{R}}_{\phi}$. Solving this goal will generate another accumulated condition goal, and so on. Repeated application of this method then gives us a *sound and complete* method to compute a set of most general NC-solutions $\{\beta_i \uplus \eta_i\}_{i \in \mathcal{I}}$ of a reachability goal $u \mid C \rightsquigarrow^{\star} v \mid D$, provided $u \mid C$ and $v \mid D$ are FPP.

The method can be expressed by an inference system for *layered constrained narrowing* which is analogous to the one in Appendix A based on layered traces: here we have layered constrained narrowing traces. But, since we can gather all conjunction into a single term in $\hat{\mathcal{R}}$, the inference system is simpler, since it solves a single reachability goal in each layer.

Layered traces will be of the form:

$$\#T_1 \uparrow T_2 \uparrow \cdots \uparrow T_n \mid G \mid \top\#$$

with $n \geq 0$, the T_i fully expanded narrowing traces, and G a possibly partially expanded reachability goal. A *closed proof* will have the form

$$\#T_1 \uparrow T_2 \uparrow \cdots \uparrow T_n \uparrow \top\#$$

so that fully expanded constrained narrowing proofs of all layers have been developed and no more inference steps are possible.

Initially, we start with a reachability goal in $\mathcal{R}$,

$$\#u \mid C \rightsquigarrow^{\star} v \mid D \uparrow \top\#$$

with $\mathcal{V}ar(u \mid C) \cap \mathcal{V}ar(v \mid D) = \emptyset$ (but see below for a more general possibility). By a *fully expanded* narrowing trace T of a goal $u_0 \mid C_0 \rightsquigarrow^{\star} v_0 \mid D_0$, where all the variables of the goal, and each of the terms in the conditions C_0 or D_0, belong to sorts in $\mathcal{R}$, we mean a symbolic NC-solution of it in $\widehat{\mathcal{R}}_{\phi}$, represented as a sequence of normalized substitutions followed by the actual symbolic trace as follows:

$$[\gamma, \delta, \vec{\mu}, \vec{\nu}] : u \mid C \rightsquigarrow_{\alpha_1,\phi} u_1 \mid C_1 \rightsquigarrow \cdots \rightsquigarrow u_{n-1} \mid C_{n-1} \rightsquigarrow_{\alpha_n,\phi} u_n \mid C_n =_B^{\delta} v \mid D$$

where $\gamma = \alpha_1 \ldots \alpha_n \delta|_{\mathcal{V}ar(u|C)} \uplus \delta|_{\mathcal{V}ar(v|D)}$ is the symbolic NC-solution, which, as δ, is normalized by definition; $\vec{\mu} = \{\alpha_{i+1} \ldots \alpha_n \delta|_{\mathcal{V}ar(u_i)}\}_{1 \leq i < n}$ is the family of substitutions also normalized by definition; and $\vec{\nu} = \{\alpha_i \ldots \alpha_n \delta|_{\vec{y_i}}\}_{1 \leq i \leq n}$ is the family of substitutions, normalized by definition, where $\vec{y_i}$ are the fresh variables of the condition D_i in the rule $l_i \to r_i$ *if* D_i used in narrowing step $u_{i-1} \mid C_{i-1} \rightsquigarrow_{\alpha_i,\phi} u_i \mid C_i$. Note that, since all the sorts of $\mathcal{R}$ and all conditions in its rules are unfrozen in $\widehat{\mathcal{R}}_{\phi}$, we can trivially view each trace of a goal $u \mid C \rightsquigarrow^{\star} v \mid D$ in $\mathcal{R}$ as a trace of a goal in $\widehat{\mathcal{R}}_{\phi}$. This suggests widening our inference system to deal not just with initial reachability goals in $\mathcal{R}$, but with initial reachability goals $u \mid C \rightsquigarrow^{\star} v \mid D$ in $\widehat{\mathcal{R}}_{\phi}$ such that: (i) $\mathcal{V}ar(u \mid C) \cap \mathcal{V}ar(v \mid D) = \emptyset$, and (ii) all the variables of the goal and each of the terms in the conditions C or D have sorts in $\mathcal{R}$.

$TS, TS', \ldots$, etc., will range over sequences $T_1 \uparrow T_2 \uparrow \cdots \uparrow T_n$ of such fully-expanded narrowing traces (called *trace stacks*), where $n \geq 0$, i.e., TS can also be the empty trace stack, denoted *nil*. The inference system for layered constrained narrowing is quite simple. It is very similar to the layered proof system in Section 3.3 and has just three inference rules, expressed as meta-level rewrite rules that expand reachability goals:

Narrowing

$$\# \; TS \uparrow (u_0 \mid C_0) \rightsquigarrow_{\alpha_1,\phi} (u_1 \mid C_1) \rightsquigarrow \cdots \rightsquigarrow (u_n \mid C_n) \rightsquigarrow^{\star}_{R,B} (v \mid D) \uparrow \top \; \#$$
$$\rightarrow$$
$$\# \; TS \uparrow (u_0 \mid C_0) \rightsquigarrow_{\alpha_1,\phi} (u_1 \mid C_1) \rightsquigarrow \cdots \rightsquigarrow (u_n \mid C_n) \rightsquigarrow_{\alpha_{n+1},\phi} (u_{n+1} \mid C_{n+1}) \rightsquigarrow^{\star}_{R,B} (v \mid D) \uparrow \top \; \#$$

where $n \geq 0$ and $u_n | C_n \rightsquigarrow_{\alpha_{n+1},\phi} u_{n+1} | C_{n+1}$ is a constrained narrowing step in $\hat{\mathcal{R}}_\phi$

Unification

$$\# \; TS \uparrow (u_0 \mid C_0) \rightsquigarrow_{\alpha_1} (u_1 \mid C_1) \rightsquigarrow \cdots \rightsquigarrow (u_n \mid C_n) \rightsquigarrow^{\star}_{R,B} (v \mid D) \uparrow \top \; \#$$
$$\rightarrow$$
$$\# \; TS \uparrow [\gamma, \delta, \vec{\mu}, \vec{\nu}] : (u_0 \mid C_0) \rightsquigarrow_{\alpha_1} (u_1 \mid C_1) \rightsquigarrow \cdots \rightsquigarrow (u_n \mid C_n) =^{\delta}_{B} (v \mid D) \uparrow \top \; \#$$

if:

1. $n \geq 0$, and $\delta \in CSU_B(u_n = v)$
2. the above trace is a symbolic solution of the reachability goal $u_0 \mid C_0 \rightsquigarrow^{\star}_{R,B} v \mid D$ with $[\gamma, \delta, \vec{\mu}, \vec{\nu}]$ its associated sequence or normalized substitutions, and
3. if $TS = [\gamma_1, \delta_1, \vec{\mu_1}, \vec{\nu_1}] : S_1 \uparrow \ldots \uparrow [\gamma_k, \delta_k, \vec{\mu_k}, \vec{\nu_k}] : S_k$, $k \geq 0$, with the S_j the actual narrowing sequences followed by their last unification step, then, for each j, $1 \leq j \leq k$, the substitutions
$$[\gamma_j \gamma_{j+1} \ldots \gamma_k \gamma, \delta_j \gamma_{j+1} \ldots \gamma_k \gamma, \vec{\mu}_j \gamma_{j+1} \ldots \gamma_k \gamma, \vec{\nu}_j \gamma_{j+1} \ldots \gamma_k \gamma]$$
are all normalized.

Shift

$$\# \; TS \uparrow [\gamma, \delta, \vec{\mu}, \vec{\nu}] : (u \mid C) \rightsquigarrow_{\alpha_1,\phi} (u_1 \mid C_1) \rightsquigarrow \cdots \rightsquigarrow (u_n \mid C_n) =^{\delta}_{B} (v \mid D) \uparrow \top \; \#$$
$$\rightarrow$$
$$\# \; TS \uparrow [\gamma, \delta, \vec{\mu}, \vec{\nu}] : (u \mid C) \rightsquigarrow_{\alpha_1,\phi} (u_1 \mid C_1) \rightsquigarrow \cdots \rightsquigarrow (u_n \mid C_n) =^{\delta}_{B} (v \mid D) \uparrow ((C_n \wedge D)\delta \mid \top) \rightsquigarrow^{\star}_{R,B} (\top \mid \top) \uparrow \top \; \#$$

if $C_n \neq \top$ or $D \neq \top$.

Note that, because of condition (3) in the **Unification** rule, the normalization conditions on the substitutions $[\gamma, \delta, \vec{\mu}, \vec{\nu}]$ associated to a symbolic NC-solution at one layer according to Definition 14 are now *inherited by previous* *layers by composition.* This can make the above inference system quite effective, since many layered proofs will not even be developed when failure of normalization is detected in the composed substitutions. In an actual implementation it is of course not necessary to wait until a **Unification** step is taken to check normalization of composed substitutions. As already pointed out in Example 5, this can (and should) also be done after each step of **Narrowing**, to weed out useless narrowing sequences at each layer.

The use of this inference system can be best illustrated with an example.

Example 7. *Recall the reachability problem*

$$f(f(x_0)) \mid \top \rightsquigarrow^{\star} x_0' + b \mid \top$$

in Example 5. In the present inference system this becomes the initial goal

$$\#f(f(x_0)) \mid \top \rightsquigarrow^{\star} x_0' + b \mid \top \uparrow \top\#$$

Three applications of the above **Narrowing** *inference rule, with the rewrite rules, positions, and substitutions in Example 5, give us:*

$$\begin{aligned}\#f(f(x_0)) \mid \top &\rightsquigarrow_{\alpha_1} f(x_1 + y) \mid h(x_1) \to^{\star} [y]\\ &\rightsquigarrow_{\alpha_2} x_1' + y_1' + y' \mid h(x_1') \to^{\star} [y_1'] \wedge h(x_1' + y_1') \to^{\star} [y']\\ &\rightsquigarrow_{\alpha_3} z' + b \mid h(a) \to^{\star} [a] \wedge h(a + a) \to^{\star} [z']\\ &\rightsquigarrow^{\star} x_0' + b \mid \top \uparrow \top\#\end{aligned}$$

And then the unifier $\delta = \{z' \mapsto x_2, x_0' \mapsto x_2\}$ *allows us to apply the* **Unify** *rule, yielding:*

$$\begin{aligned}\#[\gamma, \delta, \vec{\mu}, \vec{\nu}] : f(f(x_0)) \mid \top &\rightsquigarrow_{\alpha_1} f(x_1 + y) \mid h(x_1) \to^{\star} [y]\\ &\rightsquigarrow_{\alpha_2} x_1' + y_1' + y' \mid h(x_1') \to^{\star} [y_1'] \wedge h(x_1' + y_1') \to^{\star} [y']\\ &\rightsquigarrow_{\alpha_3} z' + b \mid h(a) \to^{\star} [a] \wedge h(a + a) \to^{\star} [z']\\ &=_{AC}^{\delta} x_0' + b \mid \top \uparrow \top\#\end{aligned}$$

We can now apply the **Shift** *rule, getting:*

$$\begin{aligned}\#[\gamma, \delta, \vec{\mu}, \vec{\nu}] : f(f(x_0)) \mid \top &\rightsquigarrow_{\alpha_1} f(x_1 + y) \mid h(x_1) \to^{\star} [y]\\ &\rightsquigarrow_{\alpha_2} x_1' + y_1' + y' \mid h(x_1') \to^{\star} [y_1'] \wedge h(x_1' + y_1') \to^{\star} [y']\\ &\rightsquigarrow_{\alpha_3} z' + b \mid h(a) \to^{\star} [a] \wedge h(a + a) \to^{\star} [z']\\ &=_{AC}^{\delta} x_0' + b \mid \top\\ &\uparrow h(a) \to^{\star} [a] \wedge h(a + a) \to^{\star} [x_2] \mid \top \rightsquigarrow^{\star} \top \mid \top \uparrow \top\#\end{aligned}$$

Using rule (3) standardized apart as $h(x_3) \to [x_3]$ *we can apply the* **Narrowing** *inference rule with substitution* $\alpha_4 = \{x_3 \mapsto a\}$ *at non-frozen position 1.1 to get:*

$$\begin{aligned}
\#[\gamma,\delta,\vec{\mu},\vec{\nu}] : f(f(x_0)) \mid \top &\rightsquigarrow_{\alpha_1} f(x_1+y) \mid h(x_1) \to^{\star} [y] \\
&\rightsquigarrow_{\alpha_2} x'_1 + y'_1 + y' \mid h(x'_1) \to^{\star} [y'_1] \wedge h(x'_1+y'_1) \to^{\star} [y'] \\
&\rightsquigarrow_{\alpha_3} z' + b \mid h(a) \to^{\star} [a] \wedge h(a+a) \to^{\star} [z'] \\
&=^{\delta}_{AC} x'_0 + b \mid \top \\
&\uparrow h(a) \to^{\star} [a] \wedge h(a+a) \to^{\star} [x_2] \mid \top \\
&\rightsquigarrow_{\alpha_4} [a] \to^{\star} [a] \wedge h(a+a) \to^{\star} [x_2] \mid \top \rightsquigarrow^{\star} \top \mid \top \uparrow \top\#
\end{aligned}$$

We can now apply **Narrowing** *with standarized apart rule $x_4 \to^{\star} x_4 \to \top$ at non-frozen position 1 with subsitution $\alpha_5 = \{x_4 \mapsto a\}$ to get:*

$$\begin{aligned}
\#[\gamma,\delta,\vec{\mu},\vec{\nu}] : f(f(x_0)) \mid \top &\rightsquigarrow_{\alpha_1} f(x_1+y) \mid h(x_1) \to^{\star} [y] \\
&\rightsquigarrow_{\alpha_2} x'_1 + y'_1 + y' \mid h(x'_1) \to^{\star} [y'_1] \wedge h(x'_1+y'_1) \to^{\star} [y'] \\
&\rightsquigarrow_{\alpha_3} z' + b \mid h(a) \to^{\star} [a] \wedge h(a+a) \to^{\star} [z'] \\
&=^{\delta}_{AC} x'_0 + b \mid \top \\
&\uparrow h(a) \to^{\star} [a] \wedge h(a+a) \to^{\star} [x_2] \mid \top \\
&\rightsquigarrow_{\alpha_4} [a] \to^{\star} [a] \wedge h(a+a) \to^{\star} [x_2] \mid \top \\
&\rightsquigarrow_{\alpha_5} \top \wedge h(a+a) \to^{\star} [x_2] \mid \top \rightsquigarrow^{\star} \top \mid \top \uparrow \top\#
\end{aligned}$$

Applying **Narrowing** *again with rule $\top \wedge C \to C$ at non-frozen position ϵ with subsitution $\alpha_6 = \{C \mapsto h(a+a) \to^{\star} [x_2]\}$ we get:*

$$\begin{aligned}
\#[\gamma,\delta,\vec{\mu},\vec{\nu}] : f(f(x_0)) \mid \top &\rightsquigarrow_{\alpha_1} f(x_1+y) \mid h(x_1) \to^{\star} [y] \\
&\rightsquigarrow_{\alpha_2} x'_1 + y'_1 + y' \mid h(x'_1) \to^{\star} [y'_1] \wedge h(x'_1+y'_1) \to^{\star} [y'] \\
&\rightsquigarrow_{\alpha_3} z' + b \mid h(a) \to^{\star} [a] \wedge h(a+a) \to^{\star} [z'] \\
&=^{\delta}_{AC} x'_0 + b \mid \top \\
&\uparrow h(a) \to^{\star} [a] \wedge h(a+a) \to^{\star} [x_2] \mid \top \\
&\rightsquigarrow_{\alpha_4} [a] \to^{\star} [a] \wedge h(a+a) \to^{\star} [x_2] \mid \top \\
&\rightsquigarrow_{\alpha_5} \top \wedge h(a+a) \to^{\star} [x_2] \mid \top \\
&\rightsquigarrow_{\alpha_6} h(a+a) \to^{\star} [x_2] \mid \top \rightsquigarrow^{\star} \top \mid \top \uparrow \top\#
\end{aligned}$$

Applying **Narrowing** *with standarized apart rule $h(x_5) \to [x_5]$ and substitution $\alpha_7 = \{x_5 \mapsto a+a\}$ at non-frozen position 1 we then get:*

$$\begin{aligned}
\#[\gamma,\delta,\vec{\mu},\vec{\nu}] : f(f(x_0)) \mid \top &\rightsquigarrow_{\alpha_1} f(x_1+y) \mid h(x_1) \to^{\star} [y] \\
&\rightsquigarrow_{\alpha_2} x'_1 + y'_1 + y' \mid h(x'_1) \to^{\star} [y'_1] \wedge h(x'_1+y'_1) \to^{\star} [y'] \\
&\rightsquigarrow_{\alpha_3} z' + b \mid h(a) \to^{\star} [a] \wedge h(a+a) \to^{\star} [z'] \\
&=^{\delta}_{AC} x'_0 + b \mid \top \\
&\uparrow h(a) \to^{\star} [a] \wedge h(a+a) \to^{\star} [x_2] \mid \top \\
&\rightsquigarrow_{\alpha_4} [a] \to^{\star} [a] \wedge h(a+a) \to^{\star} [x_2] \mid \top \\
&\rightsquigarrow_{\alpha_5} \top \wedge h(a+a) \to^{\star} [x_2] \mid \top \\
&\rightsquigarrow_{\alpha_6} h(a+a) \to^{\star} [x_2] \mid \top \\
&\rightsquigarrow_{\alpha_7} [a+a] \to^{\star} [x_2] \mid \top \rightsquigarrow^{\star} \top \mid \top \uparrow \top\#
\end{aligned}$$

Applying **Narrowing** *with standarized apart rule $x_6 \rightarrow^\star x_6 \rightarrow \top$ at non-frozen position ϵ with subsitution $\alpha_8 = \{x_6 \mapsto a + a, x_2 \mapsto a + a\}$ we then get:*

$$\begin{aligned}
\#[\gamma, \delta, \vec{\mu}, \vec{\nu}] : f(f(x_0)) \mid \top &\rightsquigarrow_{\alpha_1} f(x_1 + y) \mid h(x_1) \rightarrow^\star [y] \\
&\rightsquigarrow_{\alpha_2} x_1' + y_1' + y' \mid h(x_1') \rightarrow^\star [y_1'] \wedge h(x_1' + y_1') \rightarrow^\star [y'] \\
&\rightsquigarrow_{\alpha_3} z' + b \mid h(a) \rightarrow^\star [a] \wedge h(a + a) \rightarrow^\star [z'] \\
&=^{\delta}_{AC} x_0' + b \mid \top \\
&\uparrow h(a) \rightarrow^\star [a] \wedge h(a + a) \rightarrow^\star [x_2] \mid \top \\
&\rightsquigarrow_{\alpha_4} [a] \rightarrow^\star [a] \wedge h(a + a) \rightarrow^\star [x_2] \mid \top \\
&\rightsquigarrow_{\alpha_5} \top \wedge h(a + a) \rightarrow^\star [x_2] \mid \top \\
&\rightsquigarrow_{\alpha_6} h(a + a) \rightarrow^\star [x_2] \mid \top \\
&\rightsquigarrow_{\alpha_7} [a + a] \rightarrow^\star [x_2] \mid \top \\
&\rightsquigarrow_{\alpha_8} \top \mid \top \rightsquigarrow^\star \top \mid \top \uparrow \top\#
\end{aligned}$$

A final application of the **Unification** *inference rule with identity substitution id gives us the closed proof:*

$$\begin{aligned}
\#[\gamma, \delta, \vec{\mu}, \vec{\nu}] : f(f(x_0)) \mid \top &\rightsquigarrow_{\alpha_1} f(x_1 + y) \mid h(x_1) \rightarrow^\star [y] \\
&\rightsquigarrow_{\alpha_2} x_1' + y_1' + y' \mid h(x_1') \rightarrow^\star [y_1'] \wedge h(x_1' + y_1') \rightarrow^\star [y'] \\
&\rightsquigarrow_{\alpha_3} z' + b \mid h(a) \rightarrow^\star [a] \wedge h(a + a) \rightarrow^\star [z'] \\
&=^{\delta}_{AC} x_0' + b \mid \top \\
&\uparrow [\gamma', \delta', \vec{\mu'}, \vec{\nu'}] : h(a) \rightarrow^\star [a] \wedge h(a + a) \rightarrow^\star [x_2] \mid \top \\
&\rightsquigarrow_{\alpha_4} [a] \rightarrow^\star [a] \wedge h(a + a) \rightarrow^\star [x_2] \mid \top \\
&\rightsquigarrow_{\alpha_5} \top \wedge h(a + a) \rightarrow^\star [x_2] \mid \top \\
&\rightsquigarrow_{\alpha_6} h(a + a) \rightarrow^\star [x_2] \mid \top \\
&\rightsquigarrow_{\alpha_7} [a + a] \rightarrow^\star [x_2] \mid \top \\
&\rightsquigarrow_{\alpha_8} \top \mid \top \\
&=^{id}_{AC} \top \mid \top \uparrow \top\#
\end{aligned}$$

The crucial point is that we can obtain from this closed proof an NC-solution $\gamma\gamma'|_{\{x_0, x_0'\}}$ of our original goal $f(f(x_0)) \mid \top \rightsquigarrow^\star x_0' + b \mid \top$. Indeed, $\gamma\gamma'(x_0) = a$, and $\gamma\gamma'(x_0') = a + a$, which gives us the NC-solution with NC-rewrite sequence:

$$f(f(a)) \rightarrow_{R,AC} f(a + a) \rightarrow_{R,AC} a + a + a + a \rightarrow_{R,AC} a + a + b.$$

The two main theorems about this inference system for layered constrained narrowing state its soundness and completeness for computing NC-solutions of reachability goals.

Theorem 8 (Soundness of Layered Constrained Narrowing). *Consider a reachability goal $u \mid C \rightsquigarrow^\star v \mid D$ in $\widehat{\mathcal{R}}_\phi$ such that $\mathcal{V}ar(u \mid C) \cap \mathcal{V}ar(v \mid D) = \emptyset$ and all the variables of the goal, and each of the terms in the conditions C or*

D belong to sorts in $\mathcal{R}$. If we can use the inference system for layered constrained narrowing to rewrite the initial goal $\#u \mid C \rightsquigarrow^{\star} v \mid D \uparrow \top\#$ to a closed proof of the form $\#[\gamma_0, \delta_0, \vec{\mu_0}, \vec{\nu_0}] : S_0 \uparrow \ldots \uparrow [\gamma_n, \delta_n, \vec{\mu_n}, \vec{\nu_n}] : S_n \uparrow \top\#$, then $(\gamma_0 \ldots \gamma_n)|_{\mathcal{V}ar(u|C) \uplus \mathcal{V}ar(v|D)}$ is an NC-solution of such a goal in $\widehat{\mathcal{R}}_{\phi}$.

Proof. First of all, note that the inference rules for layered constrained narrowing will never produce from such a goal any constrained term $w \mid Q$ where the sorts of either the variables or of the terms in its condition Q will not be in $\mathcal{R}$. Clearly, neither **Unification** nor **Shift** can violate this invariant. And **Narrowing** cannot either, for the following reasons: (i) the added condition in a narrowing step has all terms having sorts in $\mathcal{R}$, because all conditional rules of $\widehat{\mathcal{R}}_{\phi}$ are rules in $\mathcal{R}$; (ii) the only rule in $\widehat{\mathcal{R}}_{\phi}$ which has a variable whose sort is not in $\mathcal{R}$ is rule $(\top \wedge C) \to C$. But if we apply it to narrow a constrained term $w \mid Q$ where the sorts of the variables are in $\mathcal{R}$, the unifier α must map C to a term whose variables are all in $\mathcal{R}$. Therefore, the narrowing step $w \mid Q \rightsquigarrow_{\alpha,\phi} (w[C]_p \mid Q)\alpha$ yields a new constrained term where the sorts of the variables and of the terms in its condition $Q\alpha$ are all in $\mathcal{R}$.

We prove the theorem by induction on n. If $n = 0$, the closed proof must necessarily be of the form $\#[\gamma_0, \delta_0, \vec{\mu_0}, \vec{\nu_0}] : u|\top \rightsquigarrow_{\alpha_1,\phi} \ldots \rightsquigarrow u_k \mid \top =_B^{\delta_0} v \mid \top \uparrow \top\#$. But this means that $\rho = id$ provides an actual NC-solution instance $\gamma_0 = \gamma_0 id$, which by the Soundness Theorem is an NC-solution of the goal, as desired.

Suppose $n > 0$ and assume the theorem is true for $n - 1$. Then we must have a closed proof of the form

$$\#[\gamma_0, \delta_0, \vec{\mu_0}, \vec{\nu_0}] : u|C \rightsquigarrow_{\alpha_1,\phi} \ldots \rightsquigarrow u_k|C_k =_B^{\delta_0} v \mid D \uparrow$$

$$[\gamma_1, id, \vec{\mu_1}, \vec{\nu_1}] : ((C_k \wedge D) \mid \top)\delta_0 \rightsquigarrow_{\alpha_{k+1},\phi} \ldots \rightsquigarrow \top|C_{k+h} =_B^{id} \top \mid \top \uparrow$$

$$\ldots \uparrow [\gamma_n, id, \vec{\mu_n}, \vec{\nu_n}] : S_n \uparrow \top\#$$

But this means that

$$\#[\gamma_1, id, \vec{\mu_1}, \vec{\nu_1}] : ((C_k \wedge D) \mid \top)\delta_0 \rightsquigarrow_{\alpha_{k+1},\phi} \ldots \rightsquigarrow \top|C_{k+h} =_B^{id} \top \mid \top \uparrow$$

$$\ldots \uparrow [\gamma_n, id, \vec{\mu_n}, \vec{\nu_n}] : S_n \uparrow \top\#$$

is a closed proof for the goal $\#((C_k \wedge D) \mid \top)\delta_0 \rightsquigarrow^{\star} \top \mid \top \uparrow \top\#$. By the induction hypothesis, $(\gamma_1 \ldots \gamma_n)|_{\mathcal{V}ar((C_k \wedge D)\delta_0)}$ is then an NC-solution of $((C_k \wedge D) \mid \top)\delta_0 \rightsquigarrow^{\star} \top \mid \top$ in $\widehat{\mathcal{R}}_{\phi}$. But by Theorem 7, plus the layered irreducibility conditions forced by the repeaded applications of the **Unification** inference rule, this means that $\mathcal{R} \vdash (C_k \wedge D)\delta_0\gamma_1 \ldots \gamma_n$ (and of course $\widehat{\mathcal{R}} \vdash (C_k \wedge D)\delta_0\gamma_1 \ldots \gamma_n$), and that $(\gamma_0 \ldots \gamma_n)|_{\mathcal{V}ar(u|C) \uplus \mathcal{V}ar(v|D)}$ is an NC-solution of the goal $u \mid C \rightsquigarrow^{\star} v \mid D$ in $\widehat{\mathcal{R}}_{\phi}$, as desired. □

The completeness of layered constrained narrowing depends crucially on our ability to turn the accumulated condition $(C_n \wedge D)\delta$ at the end of one layer of narrowing into a reachability goal $((C_n \wedge D)\delta \mid \top) \rightsquigarrow^{\star}_{R,B} (\top \mid \top)$ one layer up and solving it by constrained narrowing. But this, in turn, requires that if the reachability goal $((C_n \wedge D)\delta \mid \top) \rightsquigarrow^\star_{R,B} (\top \mid \top)$ is solvable, then it has an *NC-solution*. In general, however, this may not be the case.

Example 8. *Consider the convergent FPP theory of Example 3, and recall from Example 4 that the reachability problem $f(x,c) \mid \top \rightsquigarrow^\star c \mid \top$ is solvable but has no NC-solution in this theory. Consider now the following reachability problem:*

$$f(x_0,c) \mid f(x_0,c) \to^\star_{R,B} c \rightsquigarrow^\star d \mid \top$$

We can easily find a symbolic NC-solution for it as follows:

$$f(x_0,c) \mid f(x_0,c) \to^\star c \rightsquigarrow_\alpha z \mid f(x'',c) \to^\star c \wedge [x'',c] \to^\star [x',z] \wedge x'' \equiv x' \to^\star tt =^\delta_B d \mid \top$$

where we have narrowed with the conditional rule in Example 3 with unifier $\alpha = \{x_0 \mapsto x'', x \mapsto x', y \mapsto c\}$, and δ is the unifier $\delta = \{z \mapsto d\}$. This symbolic NC-solution has *an actual NC-solution instance, namely by taking $\rho = \{x'' \mapsto x''', x' \mapsto x'''\}$, so that we get the NC-rewrite $f(x''',c) \to d$. And of course ρ solves the accumulated condition $f(x'',c) \to^\star c \wedge [x'',c] \to^\star [x',d] \wedge x'' \equiv x' \to^\star tt$, which becomes the true condition $f(x''',c) \to^\star c \wedge [x''',c] \to^\star [x''',d] \wedge x''' \equiv x''' \to^\star tt$. However, the accumulated condition is* not *NC-solvable, because there is no NC-rewrite $f(x'',c) \to^\star_R c$ for x'' or any of its instances, although we have $f(x'',c) \to_R c$.*

The moral of this story is that, although constrained narrowing is a complete *method for symbolically describing* all *NC-solutions, layered constrained narrowing is* not complete *in general, since we cannot find an NC-solution for the reachability goal*

$$f(x'',c) \to^\star_{R,B} c \wedge [x'',c] \to^\star_{R,B} [x',d] \wedge x'' \equiv x' \to^\star_{R,B} tt \mid \top \rightsquigarrow^\star \top \mid \top$$

that layered narrowing would generate one level up.

What restrictions should we place on a reachability goal $(u \mid C) \rightsquigarrow^\star (v \mid D)$ to make layered narrowing complete? A very simple and natural one, already mentioned earlier, suffices, namely, requiring that $(u \mid C)$ and $(v \mid D)$ are FPP. The restriction is not a strong one, since FPP conditions are the most attractive and easy-to-compute way to place additional restrictions on a term. That is, if $(u \mid C)$ is FPP and θ is a normalized substitution for the variables of u, we can use the exact same incremental method to test the FPP condition C of a rewrite rule before a rewrite step to similarly test whether $\mathcal{R} \vdash C\theta'$ holds, where θ' is a normalized substitution extending θ and obtained incrementally in the usual way. For example, the reachability goal in Example 8 can be easily transformed into the following one satisfying the FPP requirement:

$$f(x_0,c) \mid f(x_0,c) \equiv c \to^\star tt \rightsquigarrow^\star d \mid \top$$

and this transformed goal *is* solvable by layered constrained narrowing.

The key reason why the FPP requirement allows layered constrained narrowing, and in particular the **Shift** rule, to be effective in solving accumulated conditions can be summarized as follows:

Lemma 6. *Let $(u \mid C) \rightsquigarrow^\star (v \mid D)$ be a goal in $\widehat{\mathcal{R}}_\phi$ satisfying the requirements in Theorem 8 and such that $(u \mid C)$ and $(v \mid D)$ are FPP. Then, if $(C_n \wedge D)\delta$ is the accumulated condition of a symbolic NC-solution γ found by constrained narrowing with $\widehat{\mathcal{R}}_\phi$, and $\gamma\rho$ is an actual NC-solution instance, then there is an NC-rewrite sequence $(C_n \wedge D)\delta\rho \to^\star \top$ in $\widehat{\mathcal{R}}_\phi$.*

Proof. This follows by direct application of Lemma 5. All we need to do is to make this obvious by "unpacking" $(C_n \wedge D)\delta$. But this we have already done in the proof of Theorem 3, namely,

$$(C_n \wedge D)\delta = C_0\alpha_1 \dots \alpha_n\delta \wedge D_1\alpha_1 \dots \alpha_n\delta \wedge \dots \wedge D_n\alpha_n\delta \wedge D\delta.$$

Then, conditions (1)–(3) on an actual NC-solution in Definition 14, plus the assumption that $(u \mid C)$ and $(v \mid D)$ are FPP, ensure that ρ, which plays the role of θ in Lemma 5, satisfies the requirements for θ in that lemma, thus yielding the claimed result. □

Another key observation is that if the original reachability goal $(u \mid C) \rightsquigarrow^\star (v \mid D)$ satisfies the requirements in Lemma 6 above, and has a closed proof by layered trace narrowing with NC-solution $\gamma_0\gamma_1\gamma_n$, then the existence of an NC-rewrite sequence $(C_n \wedge D)\delta_0\gamma_1 \dots \gamma_n \to^\star \top$ in $\widehat{\mathcal{R}}_\phi$ ensured Lemma 6 holds also for the accumulated conditions $(C'_{n'} \wedge \top)\delta_i$ at upper layers $(i \geq 1)$. That is, there is an NC-rewrite sequence $(C'_{n'} \wedge \top)\delta_i\gamma_{i+1} \dots \gamma_n \to^\star \top$ in $\widehat{\mathcal{R}}_\phi$. This is because the accumulated condition $C'_{n'}\delta_i$ is precisely a conjunction of conditions of the form $D_j\alpha_j \dots \alpha_{n'}\delta_i$, with D_j the FPP condition of a rewrite rule in $\mathcal{R}$, and then the irreducibility conditions imposed on substitutions by the inference system of layered constrained narrowing ensure that $(C'_{n'} \wedge \top)\delta_i\gamma_{i+1} \dots \gamma_n$ satisfies the requirements in Lemma 5.

We are now ready to state and prove the key theorem about layered constrained narrowing, namely, its completeness.

Theorem 9 (Completeness of Layered Constrained Narrowing). *Let $(u_0 \mid C_0) \rightsquigarrow^\star (v \mid D)$ be a reachability goal in $\hat{\mathcal{R}}_\phi$ satisfying the requirements in Theorem 8 and such that $(u_0 \mid C_0)$ and $(v \mid D)$ are FPP, and let σ be an NC solution of this goal in $\hat{\mathcal{R}}_\phi$. Then there exists a closed proof of the goal by layered constrained narrowing of the form $\#[\gamma_0, \delta_0, \vec{\mu_0}, \vec{\nu_0}] : S_0 \uparrow \dots \uparrow [\gamma_n, \delta_n, \vec{\mu_n}, \vec{\nu_n}] : S_n \uparrow \top\#$, and a normalized substitution θ such that $\sigma =_B (\gamma_0 \dots \gamma_n\theta)|_{\mathcal{V}ar(u|C) \uplus \mathcal{V}ar(v|D)}$.*

Proof. The proof of the theorem will be by strong induction on $h(\sigma, P) - 1$, where $h(\sigma, P)$ is the *height* of a pair (σ, P), with σ an NC-solution of a goal $(u_0 \mid C_0) \rightsquigarrow^\star (v \mid D)$, and P a partially developed layered proof of an NC-rewrite trace

$$T = u_0\sigma \to_{R,B} w_1 \to_{R,B} \cdots w_{n-1} \to_{R,B} w_n =_B v\sigma \qquad (6)$$

having the form $\#T \uparrow D_1\sigma_1 \wedge \dots D_n\sigma_n\#$, where each D_i is the condition of the rule used in the i-th rewrite step of T. $h(\sigma, P)$ is defined in detail below. Define first the *height* of a layered trace (rewrite) proof $\#T_1 \uparrow T_2 \uparrow \cdots \uparrow T_n \uparrow \top\#$ to be n. The height of the empty conjunction $\top$ of rewrite goals is 0 by convention. Define then the *height* $h(\sigma, P)$ for a solution σ of goal $(u_0 \mid C_0) \rightsquigarrow^\star (v \mid D)$ as $h(\sigma) = h_{C_0} + h_P + h_D$, where h_{C_0} (resp. h_D) is the smallest height of a layered NC-proof of $C_0\sigma$ (resp. $D\sigma$) in $\mathcal{R}$, and h_P is the smallest height of a layered NC-proof obtained by repeated application of inference rules to the partial proof P of the trace T in 6.

Since by Lemma 1 solutions are closed under B-equivalence, we can use the Completeness Theorem for constrained narrowing (Theorem 4) to assume, without real loss of generality, that σ is an actual NC-solution instance of a symbolic NC-solution of our goal by constrained narrowing. That is, there is a symbolic NC-solution $\gamma_0 = (\alpha_1 \ldots \alpha_n \delta_0)|_{\mathcal{V}ar(u_0|C_0)} \uplus \delta_0|_{\mathcal{V}ar(v|D)}$ in $\hat{\mathcal{R}}_\phi$ with constrained narrowing proof

$$u_0 \mid C_0 \rightsquigarrow_{\alpha_1} u_1 \mid C_1 \rightsquigarrow_{\alpha_2} u_2 \mid C_2 \cdots u_{n-1} \mid C_{n-1} \rightsquigarrow_{\alpha_n} u_n \mid C_n =_B^{\delta_0} v \mid D$$

and a normalized substitition ρ with $Dom(\rho) \subseteq \mathcal{V}ar(u_0\alpha_1 \ldots \alpha_n\delta_0) \cup \mathcal{V}ar((v \mid C_n \wedge D)\delta_0)$ such that $\sigma = (\alpha_1 \ldots \alpha_n \delta_0 \rho)|_{\mathcal{V}ar(u_0|C_0)} \uplus \delta_0\rho|_{\mathcal{V}ar(v|D)}$.

In our definition of $h(\sigma, P)$ for the above σ, the chosen trace T will be the NC-rewrite sequence

$$T = u_0\alpha_1 \ldots \alpha_n\delta\rho \rightarrow_{R,B} u_1\alpha_2 \ldots \alpha_n\delta\rho \ldots u_{n-1}\alpha_n\delta\rho \rightarrow_{R,B} u_n\delta\rho =_B v\delta\rho$$

in $\hat{\mathcal{R}}_\phi$, and P will then be the partial layered trace proof $\#T \uparrow D_1\alpha_1 \ldots \alpha_n\delta_0\rho \wedge \ldots \wedge D_n\alpha_n\delta_0\rho\#$, where D_i is the condition of the rule used in the i-th step of the narrowing sequence of which T is an instance.

Suppose that $h(\sigma, P) - 1 = 0$. This can only happen if $C_0 = D = \top$ and all the rules applied in the above narrowing sequence are unconditional, so that $C_1 = \ldots = C_n = \top$. But then $\#[\gamma_0, \delta_0, \vec{\mu_0}, \vec{\nu_0}] : u_0 \mid \top \rightsquigarrow_{\alpha_1} u_1 \mid \top \rightsquigarrow_{\alpha_2} u_2 \mid \top \cdots u_{n-1} \mid \top \rightsquigarrow_{\alpha_n} u_n \mid \top =_B^{\delta_0} v \mid \top \uparrow \top\#$ is a layered constrained narrowing proof of the goal, and choosing $\theta = \rho$ we are done.

Suppose instead that $h(\sigma, P) > 1$. Since $\mathcal{R} \vdash (C_n \wedge D)\delta_0\rho$, the fact the $u_0 \mid C_0$ and $v \mid D$ are FPP and Lemma 6 ensure that there is an NC-rewrite sequence $(C_n \wedge D)\delta_0\rho \rightarrow^\star \top$ in $\widehat{\mathcal{R}}_\phi$. But this exactly means that $\rho|_{\mathcal{V}ar((C_n \wedge D)\delta_0)}$ is an NC-solution of the reachability goal $(C_n \wedge D)\delta_0 \mid \top \rightsquigarrow^\star \top \mid \top$ in $\widehat{\mathcal{R}}_\phi$. Let now h be the smallest possible height of a layered trace NC-proof of $(C_n \wedge D)\delta_0\rho \rightarrow^\star \top$. Using Theorem 7, h is also the smallest possible height of a layered trace NC-proof of $C_0\alpha_1 \ldots \alpha_n\delta_0\rho \wedge D_1\alpha_1 \ldots \alpha_n\delta_0\rho \wedge \ldots \wedge D_n\alpha_n\delta_0\rho \wedge D\delta_0\rho$. That is, of $C_0\sigma \wedge D_1\alpha_1 \ldots \alpha_n\delta_0\rho \wedge \ldots \wedge D_n\alpha_n\delta_0\rho \wedge D\sigma$. But if $h(\sigma, P) = h_{C_0} + h_P + h_D$, with corresponding layered trace NC-proofs $\#TS_{C_0}\#$, $\#T \uparrow TS\#$, $\#TS_D\#$, then, by Lemma 8, $\#TS_{C_0}\# \parallel \#TS\# \parallel \#TS_D\#$ is a layered NC-proof of $C_0\sigma \wedge D_1\alpha_1 \ldots \alpha_n\delta_0\rho \wedge \ldots \wedge D_n\alpha_n\delta_0\rho \wedge D\sigma$, which has height $max(h_{C_0}, (h_R - 1), h_D)$, so that $h \leq max(h_{C_0}, (h_R - 1), h_D) < h(\sigma, P)$; and by Theorem 7 this is also the height of a layered NC-proof of $(C_n \wedge D)\delta_0\rho \rightarrow^\star \top$. Since the conditions of the goal $(C_n \wedge D)\delta_0 \mid \top \rightsquigarrow^\star \top \mid \top$ in $\widehat{\mathcal{R}}_\phi$ are both $\top$, this means that we can choose P' so that $h = h(\rho|_{\mathcal{V}ar((C_n \wedge D)\delta_0)}, P') < h(\sigma, P)$, so that the strong induction hypothesis applies.

Therefore, there exists a closed proof of the goal $(C_n \wedge D)\delta_0 \mid \top \rightsquigarrow^\star \top \mid \top$ by layered constrained narrowing of the form $\#[\gamma_1, \delta_1, \vec{\mu_1}, \vec{\nu_1}] : S_1 \uparrow \ldots \uparrow [\gamma_n, \delta_n, \vec{\mu_n}, \vec{\nu_n}] : S_n \uparrow \top\#$, and a normalized substitution θ_0 such that $\rho|_{\mathcal{V}ar((C_n \wedge D)\delta_0)} =_B (\gamma_1 \ldots \gamma_n \theta_0)|_{\mathcal{V}ar((C_n \wedge D)\delta_0)}$. Define $\vec{z} = \mathcal{V}ar(u_0\alpha_1 \ldots \alpha_n\delta_0) - \mathcal{V}ar((C_n \wedge D)\delta_0)$, and extend θ_0 to $\theta = \theta_0 \uplus \rho|_{\vec{z}}$. This means that $\rho =_B \rho|_{\vec{z}} \uplus (\gamma_1 \ldots \gamma_n\theta)|_{\mathcal{V}ar((C_n \wedge D)\delta_0)}$. But by the standardized apart assumption, we have $\rho|_{\vec{z}} = (\gamma_1 \ldots \gamma_n\theta)|_{\vec{z}}$, which shows that $\rho =_B (\gamma_1 \ldots \gamma_n\theta)|_{\mathcal{V}ar(u_0\alpha_1 \ldots \alpha_n\delta_0) \cup \mathcal{V}ar((C_n \wedge D)\delta_0)}$. Therefore, $\sigma = (\alpha_1 \ldots \alpha_n\delta_0\rho)|_{\mathcal{V}ar(u_0|C_0)} \uplus \delta_0\rho|_{\mathcal{V}ar(v|D)} = (\gamma_0\rho)|_{\mathcal{V}ar(u_0|C_0) \cup \mathcal{V}ar(v|D)} =_B (\gamma_0\gamma_1 \ldots \gamma_n\theta)|_{\mathcal{V}ar(u_0|C_0) \cup \mathcal{V}ar(v|D)}$ is also an actual NC-solution instance of the symbolic solution γ_0 solving our original goal $(u_0 \mid C_0) \rightsquigarrow^\star (v \mid D)$ and is B-equal to σ. Furthermore, it is easy to check that conditions (1)–(3) for an actual NC-solution instance in Definition 14 ensure that $\#[\gamma_0, \delta_0, \vec{\mu_0}, \vec{\nu_0}] : S_0 \uparrow \ldots \uparrow [\gamma_n, \delta_n, \vec{\mu_n}, \vec{\nu_n}] : S_n \uparrow \top\#$ is a closed proof of the goal by layered constrained narrowing. This finishes the proof of the theorem. $\square$

In complete analogy to Corollary 1 we then obtain:

Corollary 2. *If in Theorem 9 the term v is strongly irreducible, we can weaken the assumption on σ to just be a solution of the reachability problem $u_0 \mid C_0 \rightsquigarrow^\star v \mid D$. Since $v\sigma$ is normalized, the rewrite $u_0\sigma \to^!_{R,B} v\sigma$ has a description as an NC-rewrite sequence, so that σ is an NC-solution.*

This corollary has two important consequences:

1. Layered constrained narrowing gives us a method to extract from a constrained variant of a term a complete set of actual variant instances. More generally, it gives us a method to generate a complete set of variants for any term.

2. Layered constrained narrowing gives us a method to extract from a constrained unifier of an equation a complete set of actual unifier instances. More generally, it gives us a method to generate a complete set of unifiers for an equation, or set of equations.

9. Related Work and Conclusions

A good overview of (conditional) narrowing and its different completeness results can be found in [63]. This work does not study narrowing modulo axioms, which is the main focus of this paper. It is remarkable that it has identified several problems and wrong proofs in previous works on (conditional) narrowing. The main results are restricted to 1-CTRS and 2-CTRS but the results in this paper apply to convergent FPP theories, which fall into the 3-CTRS characterization (for a detailed taxonomy classifying CTRSs into 1-, 2-, 3-, and 4-CTRSs see [65]). [63] provides a completeness result for conditional narrowing in *level-complete* 3-CTRS, where the notion of *level-confluence* (used by the notion of level-completeness) defines confluence separately for each theory in the hierarchy of theories into which a theory is split. Level-complete theories and convergent FPP theories are different, since FPP theories do not impose any hierarchy. Furthermore, our work is within the more general context of order-sorted rewriting modulo axioms. Indeed, the definition of convergent FPP theories is an important contribution of our paper compared to previous work. Also, most approaches for conditional narrowing rely on a set of equality constraints whose evaluation order is not stated. However, as pointed out in Section 4 and elsewhere in the paper, by adding an explicit equality predicate $\_ \equiv \_$ and rules $x \equiv x \to tt$ for each kind, such unoriented conditions can be viewed as a special case of our oriented conditional approach, which is the appropriate one for strongly deterministic theories.

Unconditional narrowing modulo axioms B goes back to [46], which the current work generalizes from an untyped and unconditional to an order-sorted and conditional setting. However, nothing was known about terminating narrowing strategies modulo axioms B until folding variant narrowing was introduced in [32]. By proposing the notion of constrained variant, this work is a first step in generalizing the ideas in [32] to the conditional case.

In [12], Bockmayr considered conditional rewriting modulo B with the R,B-relation, but without requiring B-extensions, and only under the assumptions of no extra variables in a rule's condition (called 1-CTRS) and of the simplifying termination [65] of R modulo B. Our work extends Bockmayr's in several ways: first by considering convergent FPP theories, which are 3-CTRS, second by considering operational termination modulo axioms, and third by incorporating B-extensions. Bockmayr's work also relies on a set of equality constraints, instead of our approach of a list of reachability constraints. Another important difference between Bockmayr's work and ours is that ours is hierarchical (i.e., layered), and based on the systematic use of constraints, irreducibility conditions and frozenness restrictions that, as argueed in the Introduction, should drastically reduce the search space. Furthermore, notions like constrained variant and constrained unifier, which are important contributions of our work, cannot be expressed in Bockmayr's framework.

In [41], conditional narrowing is considered for a set of rules without axioms. The rules do not have any restriction on the conditional part (are 4-CTRS) and they do not restrict to convergent theories (and clearly, since no axioms B are involved there are no B-extensions). However, this approach studies lazy narrowing with non-determinism in the computations and with a call-time choice semantics (in order to ensure all occurrences of a variable in the right-hand side of a rule have the same actual term). In our work, we restrict ourselves to convergent FPP theories and argue that this is actually the most useful definition for conditional rewriting in a convergent theory, since there is an intuitive notion of deterministic functional computation that, when lifted to narrowing, is easily expressible and useful in practice. Another interesting aspect of [41] is the definition of conditions using strict equality, which normalizes terms to a constructor term and performs checks for syntactic equality. We have reachability conditions instead of equality conditions and have somehow incorporated this aspect of strict equality by requiring strongly irreducible terms in the destination term of each reachability condition. This enjoys better properties for lifting conditional rewriting to narrowing.

The work in [2] provides a calculus for conditional narrowing modulo axioms in rewriting logic. They consider convergent 4-CTRS equational order-sorted theories, with similar assumptions on operational termination and B-coherence to ours. They provide weak-completeness and soundness results of conditional narrowing for unification in these theories. An important difference is that that work provides results for the relation $\rightarrow_{E/B}$ instead of $\rightarrow_{E,B}$. Their work considers membership equational logic, whereas ours does not consider membership conditions. Their approach is based on a set of reachability constraints with no order of evaluation of the constraints, while ours relies on the deterministic evaluation features of a list of reachability constraints.

In [48], conditional narrowing modulo axioms is defined as a set of inference rules for a set of conditional equality constraints, i.e., each equality constraint may have its own set of conditions to be solved. This provides a very general form of conditional narrowing for convergent theories, where a simplification ordering is required for termination, confluence modulo axioms is also required, and a notion of B-extension is also considered. They also consider an approach similar in spirit to our constrained narrowing, where conditions are not solved but checked for solvability. However, the focus of that work is the generation of a saturated set of conditional equality constraints in order to be able to prove properties in such a finitely saturated set. Besides [48], other related work on constrained deduction and constrained narrowing includes, e.g., [51, 18, 50]. In particular, from a theorem proving perspective, constrained conditional narrowing modulo is closely related to paramodulation [68], superposition modulo [8], and superposition with constraints [37, 43].

Furthermore, since rewriting logic is not only a semantic framework for concurrent systems, but also a logical framework [55], logical deduction in a logic $\mathcal{L}$ can be both represented and implemented as deduction in an associated rewrite theory $\mathcal{R}_{\mathcal{L}} = (\Sigma, E_0 \cup B, R)$. What the distinction between the, in general nonconfluent and therefore non-deterministic, rules R modeling deduction in $\mathcal{L}$ and the, convergent modulo B, oriented equations $\vec{E_0}$ captures is the enormously useful difference between *computation* with $\vec{E_0}$ modulo B, which can be performed very efficiently by normalization to canonical form, and *deduction* with R modulo $E_0 \cup B$, which requires search and is more costly. This difference can be exploited to make theorem proving much more efficient and has been described by some authors by the name of *theorem proving modulo* [23, 17]. Since [74], it has been clearly understood that theorem proving modulo in a logic $\mathcal{L}$ is just deduction in a rewrite theory $\mathcal{R}_{\mathcal{L}} = (\Sigma, E_0 \cup B, R)$ (see also the more recent [69]). Therefore, the present work has connections with the theorem proving modulo work in several ways. Firstly, it supports symbolic deduction in a logic $\mathcal{L}$ represented as $\mathcal{R}_{\mathcal{L}} = (\Sigma, E_0 \cup B, R)$ such that its "computation rules" $\vec{E_0}$ can be conditional. Second, it also opens up the possibility of having "deduction rules" R which can have equational conditions solvable by constrained conditional narrowing with $\vec{E_0}$ modulo B.

In conclusion, the work presented here provides new concepts such as those of: (i) convergent FPP conditional theory, which, while being very general, allows very efficient implementation of conditional rewriting (by NC-rewriting), because it avoids any need for search when evaluating a rule's condition; (ii) constrained narrowing, which allows symbolic solutions while postponing solving the constraints and, as argued in the Introduction, should drastically reduce the search space; (iii) constrained variant and constrained unifier, which allow a simpler and more economic symbolic, yet complete description of all variants and unifiers; and (iv) layered constrained narrowing, a new, hierarchical way of performing conditional narrowing. It also provides soundness and completeness results for constrained narrowing and layered constrained narrowing.

As pointed out in the Introduction, although no experimental evaluation is yet available, there are good *a priori* reasons to expect the algorithms presented here to outperform previous conditional narrowing modulo algorithms, because of the combined seach space reduction effects of using: (i) constraints; (ii) order-sorted unification; (iii) frozen operators; (iv) variants; and (v) irreducibility conditions.

Much work remains ahead, particularly: (i) on implementing our approach, for which we plan to rely on, and extend, the existing Maude infrastucture for narrowing, variants, and unification (we have developed a preliminary design of an implementation that relies on such a planned extensions of the Core Maude infrastructure); (ii) on extending it from the equational case to, as mentioned in the Introduction and in Section 6, the model checking analysis of concurrent systems specified as conditional rewrite theories; (iii) on experimentally evaluating the effectiveness and performance of our approach, and comparing it with other approaches using such an implementation; and (iv) on developing a substantial body of case studies demonstrating the usefulness and effectiveness of our approach: at the purely equational level, case studies showing how *finite* complete sets of constrained variants and constrained unifiers can represent infinite sets of actual variants and actual unifiers would be particularly appealing; at the model checking level mentioned in (ii) above, case studies showing how infinite-state systems specified with conditional equations and rules can be model cheked in a way that generalizes the current unconditional narrowing-based model checking in [9, 10] would be very useful. All this will be the focus of our work in the near future.

Acknowledgments. We thank the anonymous referees for their constructive criticism and their very detailed and helpful suggestions for improving an earlier version of this work. We also thank Luis Aguirre for kindly giving us additional suggestions to improve the text. This work has been partially supported by NSF Grant CNS 13-19109 and by the EU (FEDER) and the Spanish MINECO under grant TIN 2013-45732-C4-1-P, and by Generalitat Valenciana PROMETEOII/2015/013.

References

[1] P. A. Abdulla, B. Jonsson, P. Mahata, and J. d'Orso. Regular tree model checking. In *Computer Aided Verification, 14th International Conference,*

CAV 2002,Copenhagen, Denmark, July 27-31, 2002, Proceedings, volume 2404 of *Lecture Notes in Computer Science*, pages 555–568. Springer, 2002.

[2] L. Aguirre, N. Martí-Oliet, M. Palomino, and I. Pita. Conditional narrowing modulo in rewriting logic and maude. In *Rewriting Logic and Its Applications - 10th International Workshop, WRLA 2014, Held as a Satellite Event of ETAPS, Grenoble, France, April 5-6, 2014, Revised Selected Papers*, volume 8663 of *Lecture Notes in Computer Science*, pages 80–96. Springer, 2014.

[3] R. Alur, C. Courcoubetis, T. A. Henzinger, and P.-H. Ho. Hybrid automata: an algorithmic approach to the specification and verification of hybrid systems. In R. Grossman, A. Nerode, A. Ravn, and H. Rischel, editors, *Workshop on Theory of Hybrid Systems*, pages 209–229. Springer LNCS 739, 1993.

[4] R. Alur and D. L. Dill. A theory of timed automata. *Theoretical Computer Science*, 126(2):183–235, 1994.

[5] R. Alur and P. Madhusudan. Adding nesting structure to words. *J. ACM*, 56(3), 2009.

[6] A. Armando, J. Mantovani, and L. Platania. Bounded model checking of software using SMT solvers instead of SAT solvers. *Model Checking Software*, pages 146–162, 2006.

[7] F. Baader and T. Nipkow. *Term Rewriting and All That.* Cambridge University Press, 1998.

[8] L. Bachmair and H. Ganzinger. Associative-commutative superposition. In N. Dershowitz and N. Lindenstrauss, editors, *CTRS*, volume 968 of *Lecture Notes in Computer Science*, pages 1–14. Springer, 1994.

[9] K. Bae and J. Meseguer. Abstract Logical Model Checking of Infinite-State Systems Using Narrowing. In *Rewriting Techniques and Applications (RTA'13)*, volume 21 of *LIPIcs*, pages 81–96. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, 2013.

[10] K. Bae and J. Meseguer. Infinite-state model checking of LTLR formulas using narrowing. In *Rewriting Logic and Its Applications - 10th International Workshop, WRLA 2014, Held as a Satellite Event of ETAPS, Grenoble, France, April 5-6, 2014, Revised Selected Papers*, volume 8663 of *Lecture Notes in Computer Science*, pages 113–129. Springer, 2014.

[11] T. A. Beyene, M. Brockschmidt, and A. Rybalchenko. CTL+FO verification as constraint solving. In *Proc. 2014 International Symposium on Model Checking of Software, SPIN 2014*, pages 101–104. ACM, 2014.

[12] A. Bockmayr. Conditional narrowing modulo of set of equations. *Appl. Algebra Eng. Commun. Comput.*, 4:147–168, 1993.

[13] A. Bouajjani. Languages, rewriting systems, and verification of infinite-state systems. *Automata, Languages and Programming*, pages 24–39, 2001.

[14] A. Bouajjani and J. Esparza. Rewriting models of boolean programs. *Term Rewriting and Applications*, pages 136–150, 2006.

[15] A. Bouajjani, B. Jonsson, M. Nilsson, and T. Touili. Regular model checking. In *Computer Aided Verification*, pages 403–418. Springer, 2000.

[16] R. Bruni and J. Meseguer. Semantic foundations for generalized rewrite theories. *Theor. Comput. Sci.*, 360(1-3):386–414, 2006.

[17] G. Burel. Embedding deduction modulo into a prover. In *Proc. Computer Science Logic, 24th International Workshop, CSL*, volume 6247 of *Lecture Notes in Computer Science*, pages 155–169. Springer, 2010.

[18] H. Comon, C. Marché, and R. Treinen, editors. *Constraints in Computational Logics: Theory and Applications, International Summer School, CCL'99 Gif-sur-Yvette, France, September 5-8, 1999, Revised Lectures*, volume 2002 of *Lecture Notes in Computer Science*. Springer, 2001.

[19] H. Comon-Lundth and S. Delaune. The finite variant property: how to get rid of some algebraic properties. In Proc *RTA'05*, Springer LNCS 3467, 294–307, 2005.

[20] L. Cordeiro, B. Fischer, and J. Marques-Silva. SMT-based bounded model checking for embedded ansi-c software. In *ASE*, pages 137–148. IEEE, 2009.

[21] N. Dershowitz and J.-P. Jouannaud. Rewrite systems. In J. van Leeuwen, editor, *Handbook of Theoretical Computer Science*, volume Formal Models and Sematics (B), pages 244–320. Elsevier, 1990.

[22] N. Dershowitz and D. Plaisted. Rewriting. In A. Robinson and A. Voronkov, editors, *Handbook of Automated Reasoning*, volume I, chapter 9, pages 535–610. Elsevier, 2001.

[23] G. Dowek, T. Hardin, and C. Kirchner. Theorem proving modulo. *J. Autom. Reasoning*, 31(1):33–72, 2003.

[24] F. Durán, S. Lucas, C. Marché, J. Meseguer, and X. Urbain. Proving operational termination of membership equational programs. *Higher-Order and Symbolic Computation*, 21(1-2):59–88, 2008.

[25] F. Durán, S. Lucas, and J. Meseguer. Methods for proving termination of rewriting-based programming languages by transformation. *Electr. Notes Theor. Comput. Sci.*, 248:93–113, 2009.

[26] F. Durán, S. Lucas, and J. Meseguer. Termination modulo combinations of equational theories. In *Frontiers of Combining Systems, 7th International Symposium, FroCoS 2009, Trento, Italy, September 16-18, 2009. Proceedings*, volume 5749 of *Lecture Notes in Computer Science*, pages 246–262. Springer, 2009.

[27] F. Durán and J. Meseguer. On the Church-Rosser and coherence properties of conditional order-sorted rewrite theories. *J. Algebraic and Logic Programming*, 81:816–850, 2012.

[28] S. Erbatur, S. Escobar, D. Kapur, Z. Liu, C. Lynch, C. Meadows, J. Meseguer, P. Narendran, S. Santiago, and R. Sasse. Effective symbolic protocol analysis via equational irreducibility conditions. In S. Foresti, M. Yung, and F. Martinelli, editors, *ESORICS*, volume 7459 of *Lecture Notes in Computer Science*, pages 73–90. Springer, 2012.

[29] S. Erbatur, S. Escobar, D. Kapur, Z. Liu, C. Lynch, C. Meadows, J. Meseguer, P. Narendran, S. Santiago, and R. Sasse. Asymmetric unification: A new unification paradigm for cryptographic protocol analysis. In M. P. Bonacina, editor, *CADE*, volume 7898 of *Lecture Notes in Computer Science*, pages 231–248. Springer, 2013.

[30] S. Escobar, C. Meadows, and J. Meseguer. Maude-NPA: Cryptographic protocol analysis modulo equational properties. In *Foundations of Security Analysis and Design V, FOSAD 2007/2008/2009 Tutorial Lectures*, volume 5705 of *Lecture Notes in Computer Science*, pages 1–50. Springer, 2009.

[31] S. Escobar and J. Meseguer. Symbolic model checking of infinite-state systems using narrowing. In *RTA*, volume 4533 of *Lecture Notes in Computer Science*, pages 153–168, 2007.

[32] S. Escobar, R. Sasse, and J. Meseguer. Folding variant narrowing and optimal variant termination. *J. Algebraic and Logic Programming*, 81:898–928, 2012.

[33] A. Farzan, M. Heizmann, J. Hoenicke, Z. Kincaid, and A. Podelski. Automated program verification. In *Language and Automata Theory and Applications - 9th International Conference, LATA 2015, Nice, France, March 2-6, 2015, Proceedings*, volume 8977 of *Lecture Notes in Computer Science*, pages 25–46. Springer, 2015.

[34] J. H. Gallier and W. Snyder. Complete sets of transformations for general E-unification. *Theor. Comput. Sci.*, 67(2&3):203–260, 1989.

[35] M. Ganai and A. Gupta. Accelerating high-level bounded model checking. In *ICCAD*, pages 794–801. ACM, 2006.

[36] M. Ganai and A. Gupta. Completeness in SMT-based BMC for software programs. In *DATE*, pages 831–836. IEEE, 2008.

[37] H. Ganzinger and R. Nieuwenhuis. Constraints and theorem proving. In Comon et al. [18], pages 159–201.

[38] T. Genet and V. Tong. Reachability analysis of term rewriting systems with timbuk. In *Logic for Programming, Artificial Intelligence, and Reasoning*, pages 695–706. Springer, 2001.

[39] S. Ghilardi and S. Ranise. MCMT: A model checker modulo theories. In *Proc. Automated Reasoning, 5th International Joint Conference, IJCAR 2010*, volume 6173 of *Lecture Notes in Computer Science*, pages 22–29. Springer, 2010.

[40] J. Goguen and J. Meseguer. Order-sorted algebra I: Equational deduction for multiple inheritance, overloading, exceptions and partial operations. *Theoretical Computer Science*, 105:217–273, 1992.

[41] J. C. González-Moreno, M. T. Hortalá-González, F. J. López-Fraguas, and M. Rodríguez-Artalejo. An approach to declarative programming based on a rewriting logic. *Journal of Logic Programming*, 40:47–87, 1999.

[42] J. Hendrix and J. Meseguer. Order-sorted equational unification revisited. *Electr. Notes Theor. Comput. Sci.*, 290:37–50, 2012.

[43] M. Horbach and V. Sofronie-Stokkermans. Locality transfer: From constrained axiomatizations to reachability predicates. In *Proc. Automated Reasoning - 7th International Joint Conference, IJCAR 2014*, volume 8562 of *Lecture Notes in Computer Science*, pages 192–207. Springer, 2014.

[44] J.-M. Hullot. Canonical forms and unification. In W. Bibel and R. Kowalski, editors, *Proceedings, Fifth Conference on Automated Deduction*, pages 318–334. Springer-Verlag, 1980. LNCS, Volume 87.

[45] J.-P. Jouannaud and C. Kirchner. Solving equations in abstract algebras: A rule-based survey of unification. In *Computational Logic - Essays in Honor of Alan Robinson*, pages 257–321. MIT Press, 1991.

[46] J.-P. Jouannaud, C. Kirchner, and H. Kirchner. Incremental construction of unification algorithms in equational theories. In *Proc. ICALP'83*, pages 361–373. Springer LNCS 154, 1983.

[47] J.-P. Jouannaud and H. Kirchner. Completion of a set of rules modulo a set of equations. *SIAM Journal of Computing*, 15:1155–1194, November 1986.

[48] C. Kirchner and H. Kirchner. Rewriting Solving Proving. Technical report, 2006. Available at `http://www.loria.fr/~ckirchne/=rsp/rsp.pdf`.

[49] C. Kirchner, H. Kirchner, and J. Meseguer. Operational semantics of OBJ3. In T. Lepistö and A. Salomaa, editors, *Proceedings, 15th Intl. Coll. on Automata, Languages and Programming, Tampere, Finland, July 11-15, 1988*, pages 287–301. Springer LNCS 317, 1988.

[50] H. Kirchner and C. Ringeissen. Constraint solving by narrowing in combined algebraic domains. In *Logic Programming, Proceedings of the Eleventh International Conference on Logic Programming*, pages 617–631. MIT Press, 1994.

[51] K. Kirchner, H. Kirchner, and M. Rusinowitch. Deduction with symbolic constraints. *Revue d'intelligence artificielle*, 4(3):9–52, 1990.

[52] S. Lucas. Context-sensitive computations in functional and functional logic programs. *J. Functl. and Log. Progr.*, 1(4):446–453, 1998.

[53] S. Lucas, C. Marché, and J. Meseguer. Operational termination of conditional term rewriting systems. *Information Processing Letters*, 95(4):446–453, 2005.

[54] S. Lucas and J. Meseguer. Strong and weak operational termination of order-sorted rewrite theories. In *Proc. WRLA 2014*, volume 8663, pages 178–194. Springer LNCS, 2014.

[55] N. Martí-Oliet and J. Meseguer. General logics and logical frameworks. In D. Gabbay, editor, *What is a Logical System?*, pages 355–392. Oxford University Press, 1994.

[56] J. Meseguer. Conditional rewriting logic as a unified model of concurrency. *Theoretical Computer Science*, 96(1):73–155, 1992.

[57] J. Meseguer. Membership algebra as a logical framework for equational specification. In F. Parisi-Presicce, editor, *Proc. WADT'97*, pages 18–61. Springer LNCS 1376, 1998.

[58] J. Meseguer. Twenty years of rewriting logic. *J. Algebraic and Logic Programming*, 81:721–781, 2012.

[59] J. Meseguer. Symbolic formal methods: Combining the power of rewriting, narrowing, SMT solving and model checking. In F. Arbab and M. Sirjani, editors, *Fundamentals of Software Engineering – 5th International Conference, FSEN 2013, Tehran, Iran, April 24-26, 2013*, volume 8161. Springer LNCS, 2013.

[60] J. Meseguer. Extensible symbolic system analysis. In *Proc. Unification Workshop (UNIF 2014)*. Workshop papers available at: http://www.loria.fr/ ringeiss/UNIF2014/UNIF2014-papers.html, 2014.

[61] J. Meseguer. Strict coherence of conditional rewriting modulo axioms. Technical Report http://hdl.handle.net/2142/50288, C.S. Department, University of Illinois at Urbana-Champaign, August 2014.

[62] J. Meseguer, J. Goguen, and G. Smolka. Order-sorted unification. *J. Symbolic Computation*, 8:383–413, 1989.

[63] A. Middeldorp and E. Hamoen. Completeness results for basic narrowing. *Appl. Algebra Eng. Commun. Comput.*, 5:213–253, 1994.

[64] A. Milicevic and H. Kugler. Model checking using SMT and theory of lists. *NASA Formal Methods*, pages 282–297, 2011.

[65] E. Ohlebusch. *Advanced Topics in Term Rewriting.* Springer Verlag, 2002.

[66] H. Ohsaki, H. Seki, and T. Takai. Recognizing boolean closed a-tree languages with membership conditional rewriting mechanism. In *Rewriting Techniques and Applications*, pages 483–498. Springer, 2003.

[67] G. E. Peterson and M. E. Stickel. Complete sets of reductions for some equational theories. *Journal of the Association Computing Machinery*, 28(2):233–264, 1981.

[68] G. A. Robinson and L. T. Wos. Paramodulation and theorem proving in first order theories with equality. In *Machine Intelligence*, volume 4, pages 133–150. American Elsevier, 1969.

[69] C. Rocha and J. Meseguer. Theorem proving modulo based on boolean equational procedures. In *Proc. RelMiCS 2008*, volume 4988, pages 337–351. Springer LNCS, 2008.

[70] C. Rocha, J. Meseguer, and C. A. Muñoz. Rewriting modulo SMT and open system analysis. In *Proc. Rewriting Logic and Its Applications - 10th International Workshop, WRLA 2014*, pages 247–262, 2014.

[71] TeReSe. *Term Rewriting Systems.* Cambridge University Press, 2003.

[72] P. Thati and J. Meseguer. Symbolic reachability analysis using narrowing and its application to the verification of cryptographic protocols. *J. Higher-Order and Symbolic Computation*, 20(1–2):123–160, 2007.

[73] M. Veanes, N. Bjørner, and A. Raschke. An SMT approach to bounded reachability analysis of model programs. In *FORTE*, pages 53–68. Springer, 2008.

[74] P. Viry. Adventures in sequent calculus modulo equations. *Electr. Notes Theor. Comput. Sci.*, 15:21–32, 1998.

[75] D. Walter, S. Little, and C. Myers. Bounded model checking of analog and mixed-signal circuits using an SMT solver. *Automated Technology for Verification and Analysis*, pages 66–81, 2007.

[76] C. Walther. A mechanical solution of Schubert's steamroller by many-sorted resolution. *Artif. Intell.*, 26(2):217–224, 1985.

Appendix A. Layered Proofs Inference System

Recall the list-of-lists representation of layered proofs already explained in Section 3.3. Each *list* has as elements reachability goals, perhaps partially (or fully) developed into traces. Each list is built with an associative binary conjunction operator $\_ \wedge \_$ with identity $\top$ (we represent an unconditional rule

Replacement

$\# \; TS \uparrow T \wedge w \rightarrow_{R,B} w_1 \rightarrow_{R,B} \cdots \rightarrow_{R,B} w_{n-1} \rightarrow_{R,B} w_n \rightarrow^{\star}_{R,B} v \wedge C \uparrow D \; \#$

$\rightarrow$

$\# \; TS \uparrow T \wedge w \rightarrow_{R,B} w_1 \rightarrow_{R,B} \cdots \rightarrow_{R,B} w_n \rightarrow_{R,B} w_n[r\theta]_p \rightarrow^{\star}_{R,B} v \wedge C \uparrow$

$D \wedge u_1\theta \rightarrow^{\star}_{R,B} v_1\theta \wedge \cdots \wedge u_k\theta \rightarrow^{\star}_{R,B} v_k\theta \; \#$

where $n \geq 0, (l \rightarrow r \,\text{if}\, u_1 \rightarrow v_1 \wedge \cdots \wedge u_k \rightarrow v_k) \in R,$ and θ s.t. $l\theta =_B (w_n)_p$.

Reflexivity

$\# \; TS \uparrow T \wedge w \rightarrow_{R,B} w_1 \rightarrow_{R,B} \cdots \rightarrow_{R,B} w_{n-1} \rightarrow_{R,B} w_n \rightarrow^{\star}_{R,B} v \wedge C \uparrow D \; \#$

$\rightarrow$

$\# \; TS \uparrow T \wedge w \rightarrow_{R,B} w_1 \rightarrow_{R,B} \cdots \rightarrow_{R,B} w_{n-1} \rightarrow_{R,B} w_n =_B v \wedge C \uparrow D \; \#$

if $w_n =_B v$ (with $n \geq 0$)

Shift

$\#TS \uparrow D\# \rightarrow \#TS \uparrow D \uparrow \top\#$ if $D \neq \top$

Figure A.1: Inference rules for layered trace proofs

$l \rightarrow r$ as the conditional rule $l \rightarrow r \,\text{if}\, \top$). The associative operator building layers is denoted by $\_ \uparrow \_$ with `nil` as its identity element.

Initially, any goal of the form:

$$C = t_1 \rightarrow^{\star}_{R,B} t'_1 \wedge \cdots \wedge t_n \rightarrow^{\star}_{R,B} t'_n \tag{A.1}$$

is represented as:

$$\# \; t_1 \rightarrow^{\star}_{R,B} t'_1 \wedge \cdots \wedge t_n \rightarrow^{\star}_{R,B} t'_n \uparrow \top \; \#$$

and a layered trace proof is built by application of the three inference rules in Figure A.1, applied as meta-level rewrite rules to try to build a full proof. Such inference rules perform, respectively: (i) one step of R, B-rewriting in $\mathcal{R} = (\Sigma, B, R)$; (ii) one B-equality step; and (iii) shift one level up in the proof. These inference rules are order-sorted, in the sense that any sequence of the form in Display (A.1) has sort GoalSequence, represented with variables $C, D, C', D', \ldots$, whereas any sequence which is a conjunction of full traces of the form:

$$t_i \rightarrow_{R,B} v_1 \rightarrow_{R,B} v_2 \rightarrow_{R,B} \cdots v_{n-1} \rightarrow_{R,B} v_n =_B t'_i \tag{A.2}$$

has sort FullTraceSequence, represented with variables $T, T', \ldots$.

We call a sequence of full trace sequences of the form $T_1 \uparrow T_2 \uparrow \cdots \uparrow T_n$ a *trace stack*, and represent such stacks with variables $TS, TS', \ldots$. Note that in Figure A.1, no R, B-rewrite step can be performed in a trace stack TS.

$$\# \, \texttt{first(rest(0;s(0);nil))} \rightarrow^{\star}_{R,\emptyset} \texttt{s(0)} \uparrow \top \#$$

$$\longrightarrow_{\text{Replacement}}$$

$$\begin{aligned}
\# \, \texttt{first(rest(0;s(0);nil))} \rightarrow_{R,\emptyset} \; & \texttt{first(s(0);nil)} \rightarrow^{\star}_{R,\emptyset} \texttt{s(0)} \\
& \uparrow \texttt{0;s(0);nil} \rightarrow^{\star}_{R,\emptyset} \texttt{0;s(0);nil} \#
\end{aligned}$$

$$\longrightarrow_{\text{Replacement}}$$

$$\begin{aligned}
\# \, \texttt{first(rest(0;s(0);nil))} \rightarrow_{R,\emptyset} \; & \texttt{first(s(0);nil)} \rightarrow_{R,\emptyset} \texttt{s(0)} \rightarrow^{\star}_{R,\emptyset} \texttt{s(0)} \\
& \uparrow \texttt{0;s(0);nil} \rightarrow^{\star}_{R,\emptyset} \texttt{0;s(0);nil} \\
& \quad \wedge \texttt{s(0);nil} \rightarrow^{\star}_{R,\emptyset} \texttt{s(0);nil} \#
\end{aligned}$$

$$\longrightarrow_{\text{Reflexivity}}$$

$$\begin{aligned}
\# \, \texttt{first(rest(0;s(0);nil))} \rightarrow_{R,\emptyset} \; & \texttt{first(s(0);nil)} \rightarrow_{R,\emptyset} \texttt{s(0)} = \texttt{s(0)} \\
& \uparrow \texttt{0;s(0);nil} \rightarrow^{\star}_{R,\emptyset} \texttt{0;s(0);nil} \\
& \quad \wedge \texttt{s(0);nil} \rightarrow^{\star}_{R,\emptyset} \texttt{s(0);nil} \#
\end{aligned}$$

$$\longrightarrow_{\text{Shift}}$$

$$\begin{aligned}
\# \, \texttt{first(rest(0;s(0);nil))} \rightarrow_{R,\emptyset} \; & \texttt{first(s(0);nil)} \rightarrow_{R,\emptyset} \texttt{s(0)} = \texttt{s(0)} \\
& \uparrow \texttt{0;s(0);nil} \rightarrow^{\star}_{R,\emptyset} \texttt{0;s(0);nil} \\
& \quad \wedge \texttt{s(0);nil} \rightarrow^{\star}_{R,\emptyset} \texttt{s(0);nil} \uparrow \top \#
\end{aligned}$$

$$\longrightarrow_{\text{Reflexivity}}$$

$$\begin{aligned}
\# \, \texttt{first(rest(0;s(0);nil))} \rightarrow_{R,\emptyset} \; & \texttt{first(s(0);nil)} \rightarrow_{R,\emptyset} \texttt{s(0)} = \texttt{s(0)} \\
& \uparrow \texttt{0;s(0);nil} = \texttt{0;s(0);nil} \\
& \quad \wedge \texttt{s(0);nil} \rightarrow^{\star}_{R,\emptyset} \texttt{s(0);nil} \uparrow \top \#
\end{aligned}$$

$$\longrightarrow_{\text{Reflexivity}}$$

$$\begin{aligned}
\# \, \texttt{first(rest(0;s(0);nil))} \rightarrow_{R,\emptyset} \; & \texttt{first(s(0);nil)} \rightarrow_{R,\emptyset} \texttt{s(0)} = \texttt{s(0)} \\
& \uparrow \texttt{0;s(0);nil} = \texttt{0;s(0);nil} \\
& \quad \wedge \texttt{s(0);nil} = \texttt{s(0);nil} \uparrow \top \#
\end{aligned}$$

Figure A.2: Inference steps for Example 1 in Section 3.3

For example, the proof of our running example is obtained by the inference steps of Figure A.2.

A *layered trace proof* of a goal is an (obviously *irreducible* by the inference rules) trace stack of the form: $\#TS \uparrow \top\#$, obtained by repeated application of the **Replacement**, **Reflexivity**, and **Shift** inference rules from the initial goal. That is, we obtain $\#TS \uparrow \top\#$ by a sequence of inference steps from an initial goal as the rewrite inference sequence:

$$\#t_1 \rightarrow^{\star}_{R,B} t'_1 \wedge \cdots \wedge t_n \rightarrow^{\star}_{R,B} t'_n \uparrow \top\# \longrightarrow^{*} \#TS \uparrow \top\#$$

We then write $\mathcal{R} \vdash_{LT} t_1 \rightarrow^{\star}_{R,B} t'_1 \wedge \cdots \wedge t_n \rightarrow^{\star}_{R,B} t'_n$, and call such a goal *provable* with layered proof $\#TS \uparrow \top\#$. For example, the last step in the sequence of rewrites of Figure A.2 give us a layered trace proof for the goal

$$\texttt{first(rest(0;s(0);nil))} \rightarrow^{\star}_{R} \texttt{s(0)}$$

Of course, some initial goals may not be provable at all, so that such a fully developed trace stack can never be reached.

The usefulness of layered trace proofs is that they are the natural proof object to consider when analyzing layered constrained conditional narrowing proofs and greatly help in reasoning about them. They are of course equivalent to the standard proof system in the following sense:

Proposition 2. *Denoting by* $\mathcal{R} \vdash t_1 \rightarrow^{\star}_{R,B} t'_1 \wedge \cdots \wedge t_n \rightarrow^{\star}_{R,B} t'_n$ *the conjunction* $\mathcal{R} \vdash t_1 \rightarrow^{\star}_{R,B} t'_1 \wedge \cdots \wedge \mathcal{R} \vdash t_n \rightarrow^{\star}_{R,B} t'_n$*, with* $\vdash$ *the proof system for* $\rightarrow_{R,B}$ *and* $\rightarrow^{\star}_{R,B}$ *in Section 3.1, we have the equivalence:*

$$\mathcal{R} \vdash t_1 \rightarrow^{\star}_{R,B} t'_1 \wedge \cdots \wedge t_n \rightarrow^{\star}_{R,B} t'_n \iff \mathcal{R} \vdash_{LT} t_1 \rightarrow^{\star}_{R,B} t'_1 \wedge \cdots \wedge t_n \rightarrow^{\star}_{R,B} t'_n$$

A useful fact about layered trace proofs that follows immediately from Theorem 1 is the following.

Lemma 7. *Let* $\mathcal{R} = (\Sigma, B, R)$ *be closed under* B*-extensions and let* $\#T \uparrow TS \uparrow \top\#$ *be a layered trace proof of the goal* $t_1 \rightarrow^{\star}_{R,B} t'_1 \wedge \cdots \wedge t_n \rightarrow^{\star}_{R,B} t'_n$*, and* $u_1 \rightarrow^{\star}_{R,B} u'_1 \wedge \cdots \wedge u_n \rightarrow^{\star}_{R,B} u'_n$ *be such that* $t_i =_B u_i$ *and* $t'_i =_B u'_i$, $1 \leq i \leq n$*. Then there exists a full trace sequence* T' *such that* $\#T' \uparrow TS \uparrow \top\#$ *is a layered trace proof of the goal* $u_1 \rightarrow^{\star}_{R,B} u'_1 \wedge \cdots \wedge u_n \rightarrow^{\star}_{R,B} u'_n$*.*

Another useful property of layered trace proofs is that they can be *composed in parallel* in a very easy and natural way. We give below the definition and state the obvious lemma, whose easy proof is left to the reader.

Definition 18. *Let* $LTP = \#T_1 \uparrow T_2 \uparrow \cdots \uparrow T_n \uparrow \top\#$ *and* $LTP' = \#T'_1 \uparrow T'_2 \uparrow \cdots \uparrow T'_m \uparrow \top\#$ *be two layered trace proofs. Then their* parallel composition*, denoted* $LTP \parallel LTP'$ *is constructed as follows:*

- *If* $n > m$, $LTP \parallel LTP' = \#T_1 \wedge T'_1 \uparrow \cdots T_m \wedge T'_m \uparrow T_{m+1} \uparrow \cdots \uparrow T_n \uparrow \top\#$
- *If* $n \leq m$, $LTP \parallel LTP' = \#T_1 \wedge T'_1 \uparrow \cdots T_n \wedge T'_n \uparrow T'_{n+1} \uparrow \cdots \uparrow T'_m \uparrow \top\#$.

Lemma 8. *Let LTP be a layered trace proof of the goal* $t_1 \rightarrow^{\star}_{R,B} t'_1 \wedge \cdots \wedge t_n \rightarrow^{\star}_{R,B} t'_n$*, and* LTP' *a layered trace proof of the goal* $u_1 \rightarrow^{\star}_{R,B} u'_1 \wedge \cdots \wedge u_m \rightarrow^{\star}_{R,B} u'_m$*. Then* $LTP \parallel LTP'$ *is a layered trace proof of the goal* $t_1 \rightarrow^{\star}_{R,B} t'_1 \wedge \cdots \wedge t_n \rightarrow^{\star}_{R,B} t'_n \wedge u_1 \rightarrow^{\star}_{R,B} u'_1 \wedge \cdots \wedge u_m \rightarrow^{\star}_{R,B} u'_m$*.*