Conditional Narrowing Modulo SMT Plus Axioms*

Luis Aguirre, Narciso Martí-Oliet, Miguel Palomino, and Isabel Pita

Technical Report 02/17

Departamento de Sistemas Informáticos y Computación
Facultad de Informática, Universidad Complutense de Madrid, Spain

August 2017

{luisagui, narciso, miguelpt, ipandreu}@ucm.es

Abstract. This work presents a narrowing calculus for reachability problems in order-sorted conditional rewrite theories whose underlying equational logic is composed of some theories solvable via a satisfiability modulo theories (SMT) solver plus some combination of associativity, commutativity, and identity axioms for the non-SMT part of the equational logic; the conditions of the rules can be either rewrite conditions or quantifier-free SMT formulas. For any normalized answer of a reachability problem, this calculus computes this answer, or a more general one that can be instantiated to it.

Keywords: Narrowing, reachability, rewriting logic, SMT, unification

1 Introduction

Rewriting logic is a computational logic that has been around for more than twenty years [Mes90]. The semantics of rewriting logic [BM06] has a precise mathematical meaning, allowing mathematical reasoning for proving properties, providing a flexible framework for the specification of concurrent systems; moreover, it can express both concurrent computation and logical deduction, allowing its application in many areas such as automated deduction, software and hardware specification and verification, security, etc. [MM02, Mes12]

A system is specified in rewriting logic as a rewrite theory $\mathcal{R} = (\Sigma, E, R)$, with (Σ, E) an underlying equational theory, which in this work will be *order-sorted equational logic*, where terms are given as an algebraic data type, and R a set of rules that specify how the deductive system can derive one term from another. *Many-sorted* and *unsorted* theories can be formulated as special cases of order-sorted (OS) theories.

Reachability problems have the form $\exists \bar{x}(t(\bar{x}) \to^* t'(\bar{x}))$, with t, t' terms with variables in $\bar{x}$, or a conjunction of several of these subgoals, $\exists \bar{x} \bigwedge_i (t_i(\bar{x}) \to^* t'_i(\bar{x}))$. Reachability problems can be solved by model-checking methods for finite state spaces. When the initial term t has no variables, i.e., it is a ground term, and under certain admissibility conditions, rewriting can be used in a breadth-first way to traverse the state space, trying to find a suitable matching of $t'(\bar{x})$ in each traversed node. In the general case where $t(\bar{x})$ is not a ground term, a technique known as *narrowing* [Fay79] that was first proposed as a method for solving equational goals (*unification*), has been extended to cover also reachability goals [MT07], leaving equational goals as a special case.

Such E-unification algorithm can itself make use of narrowing at another level for finding the solution to its equational goals. Specific E-unification algorithms exist for a small number

* Partially supported by MINECO Spanish projects TRACES (TIN2015-67522-C3-3-R) and StrongSoft (TIN2012-39391-C04-04), and Comunidad de Madrid program N-GREENS Software (S2013/ICE-2731).

of equational theories, but if the equational theory (Σ, E) can be decomposed as $E_0 \cup B$, where B is a set of axioms having a unification algorithm, and the equations E_0 can be turned into a set of rules $\overrightarrow{E_0}$, by orienting them, such that the rewrite theory $\overrightarrow{E} = (\Sigma, B, \overrightarrow{E_0})$ is admissible in the sense of the previous paragraph, then narrowing can be used on $\overrightarrow{E}$ to solve the E-unification goals generated by performing narrowing on $\mathcal{R}$. For these equational goals the idea of *variants of a term* has been applied in recent years to narrowing. A strategy known as *folding variant narrowing* [ESM12], which computes a complete set of variants of any term, has been developed by Escobar, Sasse, and Meseguer, allowing unification modulo a set of unconditional equations and axioms. The strategy terminates on any input term on those systems enjoying the *finite variant property*, and it is optimally terminating. It is being used for cryptographic protocol analysis [MT07], with tools like Maude-NPA [EMM09], termination algorithms modulo axioms [DLM+08], algorithms for checking confluence and coherence of rewrite theories modulo axioms [DM12], and infinite-state model checking [BM14]. Recent development in conditional narrowing has been made for order-sorted equational theories [CEM15] and also for rewriting with constraint solvers [RMM17].

Conditional narrowing without axioms for equational theories with an order-sorted type structure has been thoroughly studied for increasingly complex categories of term rewriting systems. A wide survey can be found in [MH94]. The literature is scarce when we allow for extra variables in conditions (e.g., [GM86], [Ham00]), conditional narrowing modulo axioms (e.g., [CEM15]), or conditional narrowing modulo a set of equations (e.g., [Boc93]).

Narrowing is a technique used to inspect complex concurrent and deductive systems. One of the weaknesses of narrowing is the state space explosion associated to any reachability problem where arithmetic equational theories are involved. *Satisfiability modulo theories* (SMT) solvers [dMB08] are an extension of *Boolean satisfiability* (SAT) solvers, that can handle a wide variety of equational theories, including integer and real numbers.

In this work we consider rewrite theories where the conditions that appear in their rules are either rewrite conditions or quantifier-free SMT formulas, with no restriction regarding the variables that appear in these rules or in the reachability problems. Rewrite theories always have an underlying equational theory. In our work, the underlying equational theory E of the admitted rewrite theories must be decomposable in $E = E_0 \cup B$ where E_0 is a subset of the theories handled by SMT solvers, and B is a set of axioms for the algebraic data types not handled by the SMT solvers. Abstracting the SMT subterms of the left hand side of the rules and adding compensating equations in the conditions, as already done in [RMM17], will play a significant role in our work.

This work extends the use of SMT solvers in rewriting from [RMM17], where neither rewrite conditions in the rules nor non-SMT variables in the reachability problems are admitted, to the narrowing environment, removing both restrictions.

The main contribution of this work is the development of a sound and weakly complete, i.e., complete with respect to idempotent normalized answers, narrowing calculus for conditional narrowing modulo $E_0 \cup B$ for the considered rewrite theories that has the property that just by having the access to an oracle for E_0, the SMT solver itself, it is possible to prove the soundness and weak completeness of the calculus. Usually the whole equational theory E is needed when performing this kind of proofs. To the best of our knowledge, a similar calculus does not exist in the literature.

The work is structured as follows: Section 2 presents basic definitions and properties for order-sorted equational deduction and unification, together with the concepts of built-in subtheories and abstraction. Section 3 presents rewriting modulo built-in subtheories and axioms (R/E), and the normal form $(\mathcal{R}^\circ)$ of a rewrite theory $\mathcal{R}$. Also a new relation, rewriting with normal forms and axioms (R°, B), is presented. This relation is closely related to the narrowing calculus

to be presented in Section 5 . In Section 4 the notions of B-extension and rewrite theory closed under B-extensions are presented. Then the equivalence of R/E-rewriting and R°, B-rewriting, for rewrite theories closed under B-extensions, is proved. In Section 5 the narrowing calculus for reachability is introduced. Then the soundness and weak completeness of the calculus are proved, as well as the completeness for some rewrite theories. Section 6 shows the calculus behavior in action with the running example. In Section 7, related work, conclusions, and future lines of investigation for this work are presented. The formulation of a related Corollary from [Mes17] and the proofs can be found in the appendices.

2 Preliminaries

Familiarity with term rewriting and rewriting logic [BM06] is assumed. Several definitions and results from [RMM17] are included in this section.

2.1 Running example

Example 1. Toast cooking will be used as running example. A toast is well-cooked if both sides of the toast have been cooked for exactly five seconds. No overcooking is allowed. Fresh toasts are taken from a toast bag, and they are cooked using a frying pan that can toast up to two toasts simultaneously, toasting one side of each toast. There is a tray, where fresh toasts are put when taken from the bag. A toast can be flipped directly over the pan, or returned to the tray. Finally, there is a dish where well-cooked toasts can be output.

A `toast` (abbreviated to `t`) can be a `realToast` (`rt`), represented as an ordered pair of natural numbers, each one with sort `integer` (`i`), storing the seconds that each side has already been toasted, or an `emptyToast` (`et`) which has a constant `zt`, representing the absence of `toasts`; a `pan` (`p`) is an unordered pair of `toasts`; a `kitchen` (`k`) has a timer, represented by a natural number, and a `pan`; a `tray` (`r`) is a multiset of `toasts`; the bag and the dish are represented by natural numbers, the number of `realToasts` in each one; the `system` (`s`) has a bag, a `tray`, a `kitchen`, and a dish. When a `realToast` is in the pan, the side being toasted is represented by the first integer of the ordered pair. There is one auxiliary function, `cook`. The rules for `toast` cooking are the following:

1. The function call `cook`(x, y) will return the `kitchen` obtained from `kitchen` x after y seconds, where y is a positive integer, only if no `realToast` in the `pan` gets overcooked.
2. A fresh `realToast` can pass from a non-empty bag to the `tray`.
3. A `realToast` can pass from the `tray` to the `pan` if there is room in the `pan`. The `realToast` cannot be flipped during this action.
4. A `kitchen` with at least one `realToast` in the `pan` can `cook` the `realToasts` that are laying on the pan any given integer number of seconds.
5. A `realToast` in the `pan` can be flipped over the `pan`.
6. A `realToast` in the `pan` can be returned to the `tray`, without getting flipped.
7. A well cooked `realToast` can be taken out to the dish. This operation takes one second, so if there is another `realToast` in the `pan`, it will get `cook`ed for one second.

2.2 Order-sorted equational logic

Definition 1 (Order-sorted signature). *An* order-sorted signature *is a tuple* $\Sigma = (S, \leq, F)$ *where:*

- $(S, \leq)$ *is a* kind complete *poset of sorts, i.e., its connected components are the equivalence classes corresponding to the least equivalence relation* $\equiv_{\leq}$ *containing* $\leq$*, and for each sort* s *in* S *its connected component has a top sort, denoted* $[s]$ *and called the* kind *of* s*.*
- $F = \{\Sigma_{s_1 \dots s_n, s}\}_{(s_1 \dots s_n, s) \in S^* \times S}$ *is an* $S^* \times S$*-indexed family of sets of* function symbols*, where for each function symbol* f *in* $\Sigma_{s_1 \dots s_n, s}$ *there is a function symbol* f *in* $\Sigma_{[s_1] \dots [s_n], [s]}$*.*
- Σ *is sensible, i.e., if* f *is a function symbol in* $\Sigma_{s_1 \dots s_n, s}$*,* f *is also a function symbol in* $\Sigma_{s'_1 \dots s'_n, s'}$*, and* $[s_i] = [s'_i]$ *for* $i = 1, \dots, n$ *then* $[s] = [s']$*.*

When each connected component of $(S, \leq)$ has exactly one sort, the signature is *many-sorted*.

Example 2. In the cooking example, omitting the implied kind for each connected component of S, $\Sigma = (S, \leq, F)$ is:
$S = \{\texttt{integer}, \texttt{realToast}, \texttt{emptyToast}, \texttt{toast}, \texttt{pan}, \texttt{kitchen}, \texttt{tray}, \texttt{system}\}$,
$\leq = \{(\texttt{realToast}, \texttt{toast}), (\texttt{emptyToast}, \texttt{toast}), (\texttt{toast}, \texttt{tray})\}$,
$F = \{\{[\_, \_]\}_{\texttt{i i,rt}}, \{\_\,\_\}_{\texttt{t t,p}}, \{\_;\_\}_{\texttt{r r,r}}, \{\_;\_\}_{\texttt{i p,k}}, \{\texttt{cook}\}_{\texttt{k i,[k]}}, \{\_/\_/\_/\_\}_{\texttt{i r k i,s}}, \{\texttt{zt}\}_{\texttt{et}}\}$.

The notation used in F has the following meaning: $\{[\_, \_]\}_{\texttt{i i,rt}}$ means that there is a mix-fix function symbol $[\_, \_]$ such that if i_1 and i_2 are terms with sort `integer` then $[i_1, i_2]$ is a term with sort `realToast`. It is possible to use functional notation for all function symbols, but mix-fix notation will be used in order to ease the reading.

The order $\leq$ on S is extended to S^* in the usual way: if $w = s_1 \dots s_n$ in S^n, $w' = s'_1 \dots s'_n$ in S^n, and $s_i \leq s'_i$ for $i = 1, \dots, n$ then $w \leq w'$. When $f \in \Sigma_{\epsilon, s}$, ϵ being the empty word, we call f a *constant* with type s and write $f \in \Sigma_s$ instead of $f \in \Sigma_{\epsilon, s}$.

A function symbol f in $\Sigma_{s_1 \dots s_n, s}$ is displayed as $f : s_1 \dots s_n \to s$, its *rank* declaration. Then f is said to have *arity* n and *end type* s. *Mix-fix* notation is allowed in Σ, where the symbol $\_$ is used to identify the position of each s_i in $s_1 \dots s_n$. If omitted, the usual functional notation $f(s_1, \dots, s_n)$, which is an admitted alternative notation for all functions, is assumed. An S-sorted set $\mathcal{X} = \{\mathcal{X}_s\}_{s \in S}$ of variables satisfies $s \neq s' \Rightarrow \mathcal{X}_s \cap \mathcal{X}'_s = \emptyset$, and the variables in $\mathcal{X}$ are disjoint from all the constants in Σ. Each variable in $\mathcal{X}$ has a subindex indicating its sort, i.e., x_s has sort s. A term that has no variables in it is said to be *ground*. A term where each variable occurs only once is said to be *linear*. For $S' \subseteq S$, a term is called S'*-linear* if no variable with sort in S' occurs in it twice.

The sets $\mathcal{T}_{\Sigma, s}$ and $\mathcal{T}_\Sigma(\mathcal{X})_s$ denote, respectively, the set of ground Σ-terms with sort s and the set of Σ-terms with sort s when the variables in $\mathcal{X}$ are added as extra constants. The notations $\mathcal{T}_\Sigma$ and $\mathcal{T}_\Sigma(\mathcal{X})$ are used as a shortcut for $\bigcup_{s \in S} \mathcal{T}_{\Sigma, s}$ and $\bigcup_{s \in S} \mathcal{T}_\Sigma(\mathcal{X})_s$ respectively. We write $vars(t)$ to denote the set of variables in a term t in $\mathcal{T}_\Sigma(\mathcal{X})$. This definition is extended in the usual way to other structures. It is also assumed that Σ has non-empty sorts, i.e., $\mathcal{T}_{\Sigma, s} \neq \emptyset$ for all sorts s in S.

Positions in a term t: when a term t is expressed in functional notation as $f(t_1, \dots, t_n)$, it can be pictured as a tree with root f and children t_i at position i, for $1 \leq i \leq n$. Then the root position of t is referred as ϵ and the other positions of t are referred as lists of nonzero natural numbers separated by dots, $i_1.i_2 \cdots i_m$, meaning the position $i_2 \cdots i_m$ of t_{i_1}, where $1 \leq i_1 \leq n$. The set of positions of a term is written $Pos(t)$. The set of nonvariable positions of a term is written $Pos_\Sigma(t)$. $t|_p$ is the subtree of t below position p. $t[u]_p$ is the replacement in t of the subterm at position p with a term u. As an example, if t is $f(g(a, b), c)$, then $t|_1$ is $g(a, b)$, $t|_{1.2}$ is b, and $t[d]_{1.2}$ is $f(g(a, d), c)$. For any position p define $p.\epsilon = p$. For positions p and q, we write $p \leq q$ if there is a position r such that $q = p.r$, and write $p < q$ if $q = p.r$ and $r \neq \epsilon$. Trivially $p \leq p$ because $p = p.\epsilon$.

Definition 2 (Preregularity). *Given an order-sorted signature* Σ*, for each natural number* n*, for every function symbol* f *in* Σ *with arity* n*, and for every tuple* $(s_1, \dots, s_n)$ *in* S^n*, let*

$S_{f,s_1\ldots,s_n}$ be the set containing all the sorts s' that appear in rank declarations in Σ of the form $f : s'_1 \ldots s'_n \to s'$ such that $s_i \leq s'_i$, for $1 \leq i \leq n$. If whenever $S_{f,s_1,\ldots,s_n}$ is not empty (so a term $f(t_1,\ldots,t_n)$ where t_i has type s_i for $1 \leq i \leq n$ would be a Σ-term), it is the case that $S_{f,s_1,\ldots,s_n}$ has a least sort, then Σ is said to be preregular.

Preregularity guarantees that every Σ-term t has a *least sort*, denoted $ls(t)$, among all the sorts that t has because of the different rank declarations that can be applied to t, which is the most accurate classification for t, i.e., for any rank declaration $f : s_1 \ldots s_n \to s$ that can be applied to t it is true that $ls(t) \leq s$.

A *substitution* $\sigma : \mathcal{X} \to \mathcal{R}$, where $\mathcal{R} \subseteq \mathcal{T}_\Sigma(\mathcal{X})$, is a function that matches the identity function in all $\mathcal{X}$ except for a finite set of variables called its *domain*, $dom(\sigma)$. If $\mathcal{R} \subseteq \mathcal{T}_\Sigma$ then the substitution is *ground*. A substitution σ is *well-formed* if $ls(y_s\sigma) \leq s$ for each variable y_s in $dom(\sigma)$. It is assumed throughout that all substitutions are well-formed. Substitutions are written as $\sigma = \{y^1_{s_1} \mapsto t_1, \cdots, y^n_{s_n} \mapsto t_n\}$ where $dom(\sigma)$ is $\{y^1_{s_1}, \ldots, y^n_{s_n}\}$ and the *range* of σ is $ran(\sigma) = \bigcup_{i=1}^n vars(t_i)$. We write $\sigma : \mathcal{D} \to \mathcal{R}$, where $\mathcal{D}$ is a finite set of variables, to imply that $dom(\sigma) = \mathcal{D}$. The identity substitution is displayed as id. A substitution σ where $dom(\sigma) = \{x^1_{s_1}, \ldots, x^n_{s_n}\}$ $(n \geq 0)$, $x^i_{s_i}\sigma = y^i_{s_i} \in \mathcal{X}$, for $1 \leq i \leq n$, and $y^i_{s_i} \neq y^j_{s_j}$ for $1 \leq i < j \leq n$ is called a *renaming*. Substitutions are homomorphically extended to terms in $\mathcal{T}_\Sigma(\mathcal{X})$ and also to the rest of syntactic structures to be introduced, such as equations, goals, etc. The restriction $\sigma_\mathcal{V}$ of σ to a set of variables $\mathcal{V}$ is defined as $x\sigma_\mathcal{V} = x\sigma$ if $x \in \mathcal{V}$ and $x\sigma_\mathcal{V} = x$ otherwise. Composition of two substitutions σ and σ' is denoted by $\sigma\sigma'$, with $x(\sigma\sigma') = (x\sigma)\sigma'$ (left associativity). For a substitution σ, if $\sigma\sigma = \sigma$ we say that σ is *idempotent*. It is also assumed throughout that all substitutions are idempotent, usually because $dom(\sigma) \cap ran(\sigma) = \emptyset$. For substitutions σ and σ', where $dom(\sigma) \cap dom(\sigma') = \emptyset$, we denote their union by $\sigma \cup \sigma'$. A *context* $\mathcal{C}$ is a λ-term of the form $\lambda x^1_{s_1} \cdots x^n_{s_n}.t$, with $t \in \mathcal{T}_\Sigma(\mathcal{X})$ and $\{x^1_{s_1}, \ldots, x^n_{s_n}\} \subseteq vars(t)$.

A *Σ-equation* is a binary predicate of the form $l = r$, where $l \in \mathcal{T}_\Sigma(\mathcal{X})_{s_l}$, $r \in \mathcal{T}_\Sigma(\mathcal{X})_{s_r}$, and $s_l \equiv_\leq s_r$. A *conditional Σ-equation* is a triple $l = r$ *if* C with $l = r$ a Σ-equation and C a conjunction of Σ-equations. We call a *Σ-equation* $l = r$: *regular* iff $vars(l) = vars(r)$; *sort-preserving* iff for each substitution σ, $l\sigma$ in $\mathcal{T}_\Sigma(\mathcal{X})_s$ implies $r\sigma$ in $\mathcal{T}_\Sigma(\mathcal{X})_s$ and vice versa; *left (or right) linear* iff l (resp. r) is linear; *linear* iff it is both left and right linear.

A set of equations E is said to be regular, or sort-preserving, or (left or right) linear, if each equation in it is so.

2.3 Built-ins and abstractions

Definition 3 (Signature with Built-ins [RMM17]). *An OS signature $\Sigma = (S, \leq, F)$, has* built-in subsignature *$\Sigma_0 = (S_0, \leq, F_0)$, iff:*

- *$\Sigma_0 \subseteq \Sigma$,*
- *Σ_0 is many-sorted,*
- *S_0 is a set of minimal elements in $(S, \leq)$, and*
- *if $f : w \to s \in F_1$, where $F_1 = F \setminus F_0$, then s is a sort not in S_0 and f has no other typing in Σ_0.*

We let $\mathcal{X}_0 = \{\mathcal{X}_s\}_{s \in S_0}$, $S_1 = S \setminus S_0$, $\Sigma_1 = (S, \leq, F_1)$, $\mathcal{H}_\Sigma(\mathcal{X}) = \mathcal{T}_\Sigma(\mathcal{X}) \setminus \mathcal{T}_{\Sigma_0}(\mathcal{X}_0)$, and $\mathcal{H}_\Sigma = \mathcal{T}_\Sigma \setminus \mathcal{T}_{\Sigma_0}$.

Definition 4 (Abstraction of built-in [RMM17]). *If $\Sigma \supseteq \Sigma_0$ is a signature with built-in subsignature, then an* abstraction of built-in *is a context $\mathcal{C} = \lambda x^1_{s_1} \cdots x^n_{s_n}.t^\circ$, with $n \geq 0$, such that $t^\circ \in \mathcal{T}_{\Sigma_1}(\mathcal{X})$ and $\{x^1_{s_1}, \ldots, x^n_{s_n}\} = vars(t^\circ) \cap \mathcal{X}_0$.*

Lemma 1 shows that there exists an abstraction that provides a canonical decomposition of any term in $\mathcal{H}_\Sigma(\mathcal{X})$.

Lemma 1 (Existence of a canonical abstraction [RMM17]). *Let Σ be a signature with built-in subsignature Σ_0. For each term t in $\mathcal{H}_\Sigma(\mathcal{X})$ there exists an abstraction of built-in $\lambda x^1_{s_1} \cdots x^n_{s_n}.t^\circ$ and a substitution $\theta^\circ : \mathcal{X}_0 \to \mathcal{T}_{\Sigma_0}(\mathcal{X}_0)$ such that (i) $t = t^\circ\theta^\circ$ and (ii) $dom(\theta^\circ) = \{x^1_{s_1}, \ldots, x^n_{s_n}\}$ are pairwise distinct and disjoint from $vars(t)$; moreover, (iii) t° can always be selected to be S_0-linear and with $\{x^1_{s_1}, \ldots, x^n_{s_n}\}$ disjoint from an arbitrarily chosen finite subset $\mathcal{Y}$ of $\mathcal{X}_0$.*

Now we present a function that will be needed several times in the definitions to come for rewriting and narrowing modulo built-ins.

Definition 5 (Abstract function [RMM17]). *Given a term t in $\mathcal{T}_\Sigma(\mathcal{X})$, define $abstract_{\Sigma_1}(t, \mathcal{Y})$ as $\langle \lambda x^1_{s_1} \cdots x^n_{s_n}.t^\circ; \theta^\circ; \phi^\circ \rangle$ where the context $\lambda x^1_{s_1} \cdots x^n_{s_n}.t^\circ$ and the substitution θ° satisfy the properties (i)-(iii) in Lemma 1 and $\phi^\circ = \bigwedge_{i=1}^n (x^i_{s_i} = x^i_{s_i}\theta^\circ)$. If t in $\mathcal{T}_{\Sigma_1}(\mathcal{X} \backslash \mathcal{X}_0)$ then $abstract_{\Sigma_1}(t, \mathcal{Y}) = \langle \lambda.t; id; true \rangle$. We write $abstract_{\Sigma_1}(t)$ when $\mathcal{Y}$ is the set of all the variables that have already appeared in the current calculation, so each $x^i_{s_i}$ is a* fresh *variable.*

2.4 Order-sorted equational theories

Definition 6 (OS equational theory). *An* OS equational theory *is a pair (Σ, E), where Σ is an OS signature and E is a finite set of (possibly conditional) Σ-equations of the form $l = r$ if $\bigwedge_{i=1}^n l_i = r_i$. All the variables appearing in these Σ-equations are interpreted as universally quantified. We write $l = r$ if C as a shortcut.*

Example 3. The order-sorted theory for the cooking example has $\Sigma = (\Sigma, S, \leq)$ and E is the set E_0 of equations for integer arithmetic (not displayed), together with the equations:
$(x_{\mathtt{r}}; y_{\mathtt{r}}); z_{\mathtt{r}} = x_{\mathtt{r}}; (y_{\mathtt{r}}; z_{\mathtt{r}})$, $x_{\mathtt{r}}; y_{\mathtt{r}} = y_{\mathtt{r}}; x_{\mathtt{r}}$, $x_{\mathtt{r}}; \mathtt{zt} = x_{\mathtt{r}}$, $x_{\mathtt{t}} y_{\mathtt{t}} = y_{\mathtt{t}} x_{\mathtt{t}}$
stating that the `tray` is a multiset of `toasts` and that the position of the `toasts` in the `pan` is irrelevant.

Definition 7 (Equational deduction). *Given an OS equational theory (Σ, E) and a Σ-equation $l = r$, $E \vdash l = r$ denotes that $l = r$ can be deduced from E using the rules in Figure 1 [BM06, BM12]. We write $l =_E r$ iff $E \vdash l = r$.*

An OS equational theory $E = (\Sigma, E)$ has an *initial algebra* ($\mathcal{T}_{\Sigma/E}$ or $\mathcal{T}_E$), whose elements are the equivalence classes $[t]_E \subseteq \mathcal{T}_\Sigma$ of ground terms identified by the equations in E.

The deduction rules for OS equational logic specify a sound and complete calculus, i.e., for all Σ-equations $l = r$, $E \vdash l = r$ iff $l = r$ is a logical consequence of E (written $E \vDash l = r$) [Mes97].

$$\frac{t \in \mathcal{T}_\Sigma(\mathcal{X})}{t =_E t}\ \textsf{Reflexivity} \qquad \frac{l =_E r}{r =_E l}\ \textsf{Symmetry} \qquad \frac{l =_E t \quad t =_E r}{l =_E r}\ \textsf{Transitivity}$$

$$\frac{f \in \Sigma_{s_1 \cdots s_n, s} \quad l_i =_E r_i \quad l_i, r_i \in \mathcal{T}_\Sigma(\mathcal{X})_{s_i}, 1 \leq i \leq n}{f(l_1, \ldots, l_n) =_E f(r_1, \ldots, r_n)}\ \textsf{Congruence}$$

$$\frac{(l = r \text{ if } \bigwedge_{i=1}^n l_i = r_i) \in E \quad \sigma : \mathcal{X} \to \mathcal{T}_\Sigma(\mathcal{X}) \quad l_1\sigma =_E r_1\sigma \cdots l_n\sigma =_E r_n\sigma}{l\sigma =_E r\sigma}\ \textsf{Replacement}$$

Fig. 1. Deduction rules for OS equational logic.

Proposition 1 (Instance deduction). *Let (Σ, E) be an OS equational theory. For each Σ-equation $l = r$ in Σ and each substitution σ, if $E \vdash l = r$ then $E \vdash l\sigma = r\sigma$ using the same number of deduction steps.*

Proof. Immediate by induction.

A theory inclusion $(\Sigma, E) \subseteq (\Sigma', E')$ is called *protecting* iff the unique Σ-homomorphism $\mathcal{T}_{\Sigma/E} \longrightarrow \mathcal{T}_{\Sigma'/E'}|_\Sigma$ to the *Σ-reduct of the initial algebra* $\mathcal{T}_{\Sigma'/E'}$ is a Σ-isomorphism, written $\mathcal{T}_{\Sigma/E} \simeq \mathcal{T}_{\Sigma'/E'}|_\Sigma$.

2.5 Unification

Given an OS equational theory (Σ, E), the *E-subsumption* preorder $\ll_E$ on $\mathcal{T}_\Sigma(\mathcal{X})$ is defined by $t \ll_E t'$ if there is a substitution σ such that $t =_E t'\sigma$. For substitutions σ, ρ and a set of variables $\mathcal{V}$ we write $\rho_\mathcal{V} \ll_E \sigma_\mathcal{V}$ if there is a substitution η such that $\rho_\mathcal{V} =_E (\sigma\eta)_\mathcal{V}$. We say that σ is more general than ρ with respect to $\mathcal{V}$. When $\mathcal{V}$ is not specified, it is assumed that $dom(\sigma) \subseteq dom(\rho)$ and σ is said to be more general than ρ.

Given an OS equational theory (Σ, E), a *system of equations* F is a conjunction $\bigwedge_{i=1}^n l_i = r_i$ where, for $1 \leq i \leq n$, $l_i = r_i$ is a Σ-equation. An *E-unifier* for F is a substitution σ such that $l_i\sigma =_E r_i\sigma$, for $1 \leq i \leq n$. If id is an *E-unifier* for F then we say that F is *trivial*. The condition in a conditional equation is a system of equations.

Definition 8 (Complete set of unifiers). *For F a system of equations and $Var(F) \subseteq \mathcal{W}$, a set of substitutions $CSU_E^\mathcal{W}(F)$ is said to be a complete set of E-unifiers of F away from $\mathcal{W}$ iff each substitution σ in $CSU_E^\mathcal{W}(F)$ is an E-unifier of F, for any E-unifier ρ of F there is a substitution σ in $CSU_E^\mathcal{W}(F)$ such that $\rho_\mathcal{W} \ll_E \sigma_\mathcal{W}$, and for each substitution σ in $CSU_E^\mathcal{W}(F)$, $dom(\sigma) \subseteq Var(F)$ and $ran(\sigma) \cap \mathcal{W} = \emptyset$.*

The notation CSU_E is used when $\mathcal{W}$ is the set of all the variables that have already appeared in the current calculation, preventing the collision between new variables from the E-unifier and variables already used in the calculation. A substitution σ in $CSU_E(F)$ is always idempotent because $dom(\sigma) \cap ran(\sigma) = \emptyset$.

This notion was introduced by Plotkin [Plo72]. An E-unification algorithm is *complete* if for any given system of equations it generates a complete set of E-unifiers, which may not be finite. An E-unification algorithm is said to be *finitary* and complete if it terminates after generating a finite and complete set of solutions.

3 Conditional Rewriting modulo built-ins and axioms

This section introduces rewriting modulo built-ins and axioms, the normal form of a rewrite theory with built-ins, and the concept of R°, B-rewriting, which is one of the keys to the narrowing calculus presented in Section 5. Also the concept of one-step deduction for B, E_0, and E is presented. Using this concept, every deduction $t =_E t''$ can be seen as a mixed series of one-step deductions in B and E_0. The ultimate goal is to be able to put all the one-step deductions in B at the beginning of the deduction, so there exists a term t' such that $t =_B t' =_{E_0} t''$. A new concept of *topmost Σ_0-position* is presented in order to prove the interchangeability of one-step deductions in B end E_0 and find the desired term t'.

Definition 9 (B-preregularity). *Given a set of Σ-equations B used for deduction modulo B, a preregular OS signature Σ is called* B-preregular *iff for each equation $u = v$ in B and substitution σ, $ls(u\sigma) = ls(v\sigma)$.*

Definition 10 (Conditional rewrite theory with built-in subtheory and axioms). *A conditional rewrite theory $\mathcal{R} = (\Sigma, E, R)$ with built-in subtheory and axioms (Σ_0, E_0) consists of:*

1. *an OS equational theory (Σ, E) where:*
   - *$\Sigma = (\Sigma, S, \leq)$ is an OS signature with built-in subsignature $\Sigma_0 = (\Sigma_0, S_0)$,*
   - *$E = E_0 \uplus B$, where E_0 is the set of Σ_0-equations in E, the theory inclusion $(\Sigma_0, E_0) \subseteq (\Sigma, E)$ is protecting, B is a set of regular and linear equations, called* axioms, *each equation having only function symbols from $\Sigma \setminus \Sigma_0$,*
   - *there is a procedure that can compute $CSU_B^{\mathcal{W}}(F)$ for any system of equations F,*
   - *Σ is B-preregular, and*
2. *a finite set of (possibly conditional) rewrite rules R, each one with the form $l \to r$ if $\bigwedge_{i=1}^n l_i \to r_i \mid \phi$, we write $l \to r$ if C as a shortcut, where:*
   - *$l \in \mathcal{H}_\Sigma(\mathcal{X}) \setminus \mathcal{X}$, $r \in \mathcal{H}_\Sigma(\mathcal{X})$, $ls(l) \equiv_\leq ls(r)$,*
   - *for each pair l_i, r_i, $1 \leq i \leq n$, $l_i \in \mathcal{H}_\Sigma(\mathcal{X})$, $r_i \in \mathcal{H}_\Sigma(\mathcal{X})$, $ls(l_i) \equiv_\leq ls(r_i)$, and*
   - *$\phi \in QF(\mathcal{X}_0)$, the set of* quantifier free *formulas made up with terms in $\mathcal{T}_{\Sigma_0}(\mathcal{X}_0)$, the comparison function symbols $=$ and $\neq$, and the connectives $\vee$ and $\wedge$.*

   All the variables appearing in these rewrite rules are interpreted as universally quantified. Three particular cases of the general form are also admitted: $l \to r$ if $\bigwedge_{i=1}^n l_i \to r_i$, $l \to r$ if ϕ, and $l \to r$.

Proposition 2 (Relation between Σ-terms and abstractions in rewrite theories). *Let $\mathcal{R} = (\Sigma, E, R)$ be a rewrite theory with built-in subtheory (Σ_0, E_0), and t be a term in $\mathcal{H}_\Sigma(\mathcal{X})$, with $abstract_{\Sigma_1}(t) = \langle \lambda \bar{x}.t^\circ; \theta^\circ; \phi^\circ \rangle$. For any substitution σ such that $E_0 \vDash \phi^\circ\sigma$, it follows that $t^\circ\sigma =_E t\sigma$.*

The transitive (resp. transitive and reflexive) closure of the relation $\to_R^1$, inductively defined below, is denoted $\to_R^+$ (resp. $\to_R^*$).

Definition 11 (Rewrite step). *Given a rewrite theory $\mathcal{R} = (\Sigma, E_0 \cup B, R)$ with built-in subtheory (Σ_0, E_0), a term t in $\mathcal{H}_\Sigma$, a position p in $Pos(t)$, a rewrite rule $c = l \to r$ if $\bigwedge_{i=1}^n l_i \to r_i \mid \phi$ in R, and a substitution $\sigma : vars(c) \to \mathcal{T}_\Sigma$, the* one-step transition *$t \to_R^1 t[r\sigma]_p$ holds iff $t = t[l\sigma]_p$, $l_i\sigma \to_R^* r_i\sigma$, for $1 \leq i \leq n$, and $E_0 \vDash \phi\sigma$. We write $(t, u) \in \to_R^1$ when $t \to_R^1 u$. Given a rewrite theory $\mathcal{R}$, we call u reachable from t in $\to_R^1$ iff $t \to_R^* u$.*

For every rewrite step $t \to_R^1 t[r\sigma]_p$ there exists a closed proof tree witnessing it, in the sense of [LMM05].

Definition 12 (Reachability problem). *A* reachability problem *is an expression P with form $\bigwedge_{i=1}^n t_i \to v_i \mid \phi$, with t_i and v_i in $\mathcal{H}_\Sigma(\mathcal{X})$, for $1 \leq i \leq n$, and $\phi \in QF(\mathcal{X}_0)$. Each expression $t_i \to v_i$, $1 \leq i \leq n$, is a* subgoal *of P and ϕ is the* reachability formula *of P.*

Definition 13 (Solution of a reachability problem). *A substitution $\sigma : vars(P) \to \mathcal{T}_\Sigma$ is a solution of a reachability problem $P = \bigwedge_{i=1}^n t_i \to v_i \mid \phi$ in a rewrite relation iff $v_i\sigma$ is reachable from $t_i\sigma$, for $1 \leq i \leq n$, in that rewrite relation and $E_0 \vDash \phi\sigma$.*

The conditional part, C, of any rewrite rule $l \to r$ *if* C is a reachability problem. If a one-step transition is performed on a term using this rule and a substitution σ, then σ is a solution for C.

Example 4. In the cooking example, E_0 is the theory for integer arithmetic, B is the set of axioms in Example 3, and R is the following translation of the rules for cooking, shown in Example 2.1, where each rule is prefixed by a label that will be used in the following examples to distinguish the rule being used in each step and the abbreviations used for the subindices, as established

before, are $\mathtt{i} - \mathtt{integer}, \mathtt{rt} - \mathtt{realToast}, \mathtt{t} - \mathtt{toast}, \mathtt{k} - \mathtt{kitchen}, \mathtt{r} - \mathtt{tray}$:
$[r1a]: \mathtt{cook}(y_\mathtt{i}; \mathtt{zt}\ \mathtt{zt}, z_\mathtt{i}) \to y_\mathtt{i} + z_\mathtt{i}; \mathtt{zt}\ \mathtt{zt}$ *if* $z_\mathtt{i} > 0$
$[r1b]: \mathtt{cook}(y_\mathtt{i}; [a_\mathtt{i}, b_\mathtt{i}]\ \mathtt{zt}, z_\mathtt{i}) \to y_\mathtt{i} + z_\mathtt{i}; [a_\mathtt{i} + z_\mathtt{i}, b_\mathtt{i}]\ \mathtt{zt}$ *if* $z_\mathtt{i} > 0 \wedge a_\mathtt{i} + z_\mathtt{i} \leq 5$
$[r1c]: \mathtt{cook}(y_\mathtt{i}; [a_\mathtt{i}, b_\mathtt{i}]\ [c_\mathtt{i}, d_\mathtt{i}], z_\mathtt{i}) \to y_\mathtt{i} + z_\mathtt{i}; [a_\mathtt{i} + z_\mathtt{i}, b_\mathtt{i}]\ [c_\mathtt{i} + z_\mathtt{i}, d_\mathtt{i}]$
if $z_\mathtt{i} > 0 \wedge a_\mathtt{i} + z_\mathtt{i} \leq 5 \wedge c_\mathtt{i} + z_\mathtt{i} \leq 5$
$[r2]: n_\mathtt{i}/x_\mathtt{r}/g_\mathtt{k}/ok_\mathtt{i} \to (n_\mathtt{i} - 1)/[0,0]; x_\mathtt{r}/g_\mathtt{k}/ok_\mathtt{i}$ *if* $n_\mathtt{i} > 0$
$[r3]: n_\mathtt{i}/h_\mathtt{rt}; x_\mathtt{r}/y_\mathtt{i}; \mathtt{zt}\ v_\mathtt{t}/ok_\mathtt{i} \to n_\mathtt{i}/x_\mathtt{r}/y_\mathtt{i}; h_\mathtt{rt}\ v_\mathtt{t}\ /ok_\mathtt{i}$
$[r4]: y_\mathtt{i}; h_\mathtt{rt}\ v_\mathtt{t} \to \mathtt{cook}(y_\mathtt{i}; h_\mathtt{rt}\ v_\mathtt{t}, z_\mathtt{i})$
$[r5]: y_\mathtt{i}; [a_\mathtt{i}, b_\mathtt{i}]\ v_\mathtt{t} \to y_\mathtt{i}; [b_\mathtt{i}, a_\mathtt{i}]\ v_\mathtt{t}$
$[r6]: n_\mathtt{i}/x_\mathtt{r}/y_\mathtt{i}; [a_\mathtt{i}, b_\mathtt{i}]\ v_\mathtt{t}/ok_\mathtt{i} \to n_\mathtt{i}/[a_\mathtt{i}, b_\mathtt{i}]; x_\mathtt{r}/y_\mathtt{i}; \mathtt{zt}\ v_\mathtt{t}/ok_\mathtt{i}$
$[r7]: n_\mathtt{i}/x_\mathtt{r}/y_\mathtt{i}; [5,5]\ v_\mathtt{t}/ok_\mathtt{i} \to n_\mathtt{i}/x_\mathtt{r}/g_\mathtt{k}/ok_\mathtt{i} + 1$ *if* $\mathtt{cook}(y_\mathtt{i}; \mathtt{zt}\ v_\mathtt{t}, 1) \to g_\mathtt{k}$

The transitive closure of the relation $\to^1_{R/E}$, inductively defined below, is denoted $\to^+_{R/E}$. The relation $\to_{R/E}$ is defined as $\to_{R/E} = \to^+_{R/E} \cup =_E$ (or, equivalently, $\to^*_{R/E}; =_E$).

Definition 14 (Rewrite step modulo).
Given a rewrite theory $\mathcal{R} = (\Sigma, E, R)$ with built-in subtheory (Σ_0, E_0), and terms t, v in $\mathcal{H}_\Sigma$, a rewrite rule $c = l \to r$ if $\bigwedge_{i=1}^n l_i \to r_i \mid \phi$ in R specifies a one-step modulo transition $t \to^1_{R/E} v$ *iff there exist a term u in $\mathcal{H}_\Sigma$, a position p in $Pos(u)$, and a substitution $\sigma : vars(c) \to \mathcal{T}_\Sigma$ such that $t =_E u = u[l\sigma]_p$, $u[r\sigma]_p =_E v$, $l_i\sigma \to_{R/E} r_i\sigma$, for $1 \leq i \leq n$, and $E_0 \vDash \phi\sigma$.*

We call v *reachable* from t in $\to_{R/E}$ iff $t \to_{R/E} v$. A reachability problem $P = \bigwedge_{i=1}^n t_i \to v_i \mid \phi$ *holds* with substitution $\sigma : vars(P) \to \mathcal{T}_\Sigma$ in $\to_{R/E}$ iff $t_i\sigma \to_{R/E} t'_i\sigma$, for $1 \leq i \leq n$, and $E_0 \vDash \phi\sigma$.

Rewriting modulo is rewriting with the equivalence classes of the relation $=_E$. One rewrite step can be applied to a whole class $[t]_E$ iff it can be applied to any of its terms $u \in [t]_E$. The relation $\to^1_{R/E}$ on $\mathcal{T}_\Sigma$ corresponds to the relation $\to^1_R$ on $\mathcal{T}_{\Sigma/E}$, i.e., $t \to^1_{R/E} t'$ iff $[t]_E \to^1_R [t']_E$. A term t' is reachable from a term t in $\to_{R/E}$ iff $[t]_E \to^*_R [t']_E$, and that is what the definition of reachability modulo reflects, allowing to reason about sets of equivalent terms instead of about single terms, but maintaining the term notation.

Rewriting modulo is *more expressive* than rewriting ($\to^1_R \subsetneq \to^1_{R/E}$): from Definitions 11 and 14 it is clear that $\to^1_R \subseteq \to^1_{R/E}$; in the next example we prove that $\to^1_{R/E} \not\subseteq \to^1_R$.

Example 5. Let us assume a rewrite theory $\mathcal{R} = (\Sigma, E, R)$ with built-in subtheory (Σ_0, E_0), where $S_0 = \{n\}$, Σ_0 has constants 0, 1, 2, and a binary function symbol $\_ + \_ : n\ n \to n$; $E_0 = \{x + y = y + x\}$; f and g are function symbols in Σ_1; $B = \{f(x, y) = f(y, x)\}$; and the only rule in R is $c = f(2 + x, 0) \to g(x)$. Then $f(0, 1 + 2)$ cannot be rewritten in R because $f(0, 1 + 2) \neq f(2 + x, 0)\sigma$ for any substitution σ, but $f(0, 1 + 2) \to^1_{R/E} g(1)$ with $\sigma = \{x \mapsto 1\}$, because $1 + 2 =_{E_0} 2 + 1$, so $f(1 + 2, 0) =_E f(2 + 1, 0) = f(2 + x, 0)\sigma$.

Although rewriting modulo is more expressive than rewriting, whether a one-step modulo transition $t \to^1_{R/E} v$ holds is undecidable, in general, since E-congruence classes can be infinite. Two simpler relations, $\to^1_{R,B}$ and $\to_{R,B}$ [GK01], and the normal form $\mathcal{R}^\circ$ of a rewrite theory $\mathcal{R}$ are now defined. Under one additional assumption, see Theorem 1, rewriting with these new relations using the normal form of a rewrite theory will be equivalent to rewriting modulo E with the original theory, i.e., $\to^1_{R^\circ,B} = \to^1_{R/E}$ and $\to_{R^\circ,B} = \to_{R/E}$. The main difference between $\to^1_{R/E}$ and $\to^1_{R^\circ,B}$, apart from the possibly different set of rules, is that the first one uses matching modulo E and the second one uses matching modulo B, which is computable.

The transitive and reflexive closure of the relation $\to^1_{R,B}$, inductively defined below, is denoted $\to^*_{R,B}$. The relation $\to_{R,B}$ is defined as $\to_{R,B} = (\to^*_{R,B}; =_E)$.

Definition 15 (R,B rewriting). *Given a rewrite theory $\mathcal{R} = (\Sigma, E_0 \cup B, R)$ with built-in subtheory (Σ_0, E_0), and terms t, u in $\mathcal{H}_\Sigma$, a rewrite rule $c = l \to r$ if $\bigwedge_{i=1}^n l_i \to r_i \mid \phi$ specifies a* one-step transition in R, B $t \to^1_{R,B} u$ *iff there exist a position p in $Pos(t)$, and a substitution $\sigma : vars(c) \to \mathcal{T}_\Sigma$ such that $t|_p =_B l\sigma$, $u =_E t[r\sigma]_p$, $l_i\sigma \to_{R,B} r_i\sigma$, for $1 \le i \le n$, and $E_0 \vDash \phi\sigma$.*

We call *u reachable* from t in $\to_{R,B}$ if $t \to_{R,B} u$. A reachability problem $P = \bigwedge_{i=1}^n t_i \to u_i \mid \phi$ *holds* with substitution $\sigma : vars(P) \to \mathcal{T}_\Sigma$ in $\to_{R,B}$ iff $t_i\sigma \to_{R,B} u_i\sigma$, for $1 \le i \le n$, and $E_0 \vDash \phi\sigma$.

R, B-rewriting is more expressive than rewriting, as shown in the following example.

Example 6. Using the rewrite theory $\mathcal{R} = (\Sigma, E, R)$ from Example 5, $f(0, 2+1)$ cannot be rewritten in R because $f(0, 2+1) \neq f(2+x, 0)\sigma$ for any substitution σ, but $f(0, 2+1) \to^1_{R,B} g(1)$ with rule c and $\sigma = \{x \mapsto 1\}$, because $f(0, 2+1) =_B f(2+1, 0) = f(2+x, 0)\sigma$.

Definition 16 (Normal form of a rewrite theory with built-in). *Let $\mathcal{R} = (\Sigma, E, R)$ be a rewrite theory with built-in subtheory (Σ_0, E_0). For every rewrite rule $c = l \to r$ if $\bigwedge_{i=1}^n l_i \to r_i \mid \phi$ in R, if $abstract_{\Sigma_1}(l) = \langle \lambda\bar{x}.l^\circ; \theta^\circ; \phi^\circ \rangle$ then the normal rewrite theory $\mathcal{R}^\circ = (\Sigma, E, R^\circ)$ has in R° a rewrite rule:*

$$c^\circ = l^\circ \to r \text{ if } \bigwedge_{i=1}^n l_i \to r_i \mid \phi \wedge \phi^\circ,$$

Example 7. The normal form R° for the cooking example has the same conditional rewrite rules in R, except the last one,
$[r7] : n_{\mathtt{i}}/x_{\mathtt{r}}/y_{\mathtt{i}}; [5,5]\, v_{\mathtt{t}}/ok_{\mathtt{i}} \to n_{\mathtt{i}}/x_{\mathtt{r}}/g_{\mathtt{k}}/ok_{\mathtt{i}} + 1$ *if* $\mathtt{cook}(y_{\mathtt{i}}; \mathtt{zt}\, v_{\mathtt{t}}, 1) \to g_{\mathtt{k}}$,
whose normal form is:
$[r7^\circ] : n_{\mathtt{i}}/x_{\mathtt{r}}/y_{\mathtt{i}}; [a_{\mathtt{i}}, b_{\mathtt{i}}]\, v_{\mathtt{t}}/ok_{\mathtt{i}} \to n_{\mathtt{i}}/x_{\mathtt{r}}/g_{\mathtt{k}}/ok_{\mathtt{i}} + 1$ *if* $\mathtt{cook}(y_{\mathtt{i}}; \mathtt{zt}\, v_{\mathtt{t}}, 1) \to g_{\mathtt{k}} \wedge a_{\mathtt{i}} = 5 \wedge b_{\mathtt{i}} = 5$.

Definition 17 (Normalized substitution). *Given a rewrite theory $\mathcal{R} = (\Sigma, E, R)$ with built-in subtheory (Σ_0, E_0) and its normal form $\mathcal{R}^\circ = (\Sigma, E_0 \cup B, R^\circ)$, a substitution σ is* R/E-normalized (resp. R°, B-normalized) *iff for each variable x in $dom(\sigma)$ there is no term t in $\mathcal{T}_\Sigma(\mathcal{X})$ such that $x\sigma \to^1_{R/E} t$ (resp. $x\sigma \to^1_{R^\circ,B} t$).*

Proposition 3 (Inclusion of $\to^1_{R,B}$ in $\to^1_{R^\circ,B}$). *Let $\mathcal{R} = (\Sigma, E_0 \cup B, R)$ be a rewrite theory with built-in subtheory (Σ_0, E_0) and $\mathcal{R}^\circ = (\Sigma, E_0 \cup B, R^\circ)$ be its normal rewrite theory. Then $\to^1_{R,B} \subseteq \to^1_{R^\circ,B}$.*

There exist rewrite theories where $\to^1_{R,B} \neq \to^1_{R^\circ,B}$.

Example 8. Using the rewrite theory $\mathcal{R} = (\Sigma, E, R)$ from Example 5, where $B = \{f(x,y) = f(y,x)\}$ and $R = \{f(2+x, 0) \to g(x)\}$, the only rule in R° is $c^\circ = f(y,z) \to g(x)$ *if* $nil \mid y = 2+x \wedge z = 0$. The term $f(0, 1+2)$ cannot be rewritten in R, B because as $1+2 \neq 2+1$ (syntactically speaking) then $f(0, 1+2) \neq_B f(2+x, 0)\sigma$ for any substitution σ. But $f(0, 1+2) \to^1_{R^\circ,B} g(1)$ with c° and $\sigma = \{x \mapsto 1, y \mapsto 1+2, z \mapsto 0\}$, because $E_0 \vDash 1+2 = 2+1 \wedge 0 = 0$ and $f(0, 1+2) =_B f(1+2, 0) = f(y,z)\sigma$, so in this example $\to^1_{R,B} \neq \to^1_{R^\circ,B}$.

Definition 18 (One-step B-deduction and E_0-deduction). *Let $\mathcal{R} = (\Sigma, E_0 \cup B, R)$ be a rewrite theory with built-in subtheory (Σ_0, E_0). Let $B^{-1} = \{v = w \mid w = v \in B\}$, then we write $l \leftrightarrow_B r$ iff there exists $v = w$ in $B \cup B^{-1}$, a position p in l and a substitution σ such that $l|_p = v\sigma$ and $r = l[w\sigma]_p$. Let $E_0^{-1} = \{v = w \text{ if } C \mid w = v \text{ if } C \in E_0\}$, then we write $l \leftrightarrow_{E_0} r$ iff there exists $v = w$ if C in $E_0 \cup E_0^{-1}$, a position p in l and a substitution σ such that $l|_p = v\sigma$, $r = l[w\sigma]_p$, and $E_0 \vdash C\sigma$. We define $\leftrightarrow_E = \leftrightarrow_B \cup \leftrightarrow_{E_0}$.*

Definition 19 (Set of topmost Σ_0-positions). *Let $\mathcal{R} = (\Sigma, E_0 \cup B, R)$ be a rewrite theory with built-in subtheory (Σ_0, E_0), and t a term in $\mathcal{H}_\Sigma(\mathcal{X})$. The set of topmost Σ_0 positions of t, $top_{\Sigma_0}(t)$, is $top_{\Sigma_0}(t) = \{p \mid p \in Pos(t) \wedge \exists i \in \mathbb{N}(p = q.i \wedge t|_q \in \mathcal{H}_\Sigma(\mathcal{X}) \wedge t|_p \in \mathcal{T}_{\Sigma_0}(\mathcal{X}_0))\}$.*

$top_{\Sigma_0}(t)$ characterizes the biggest $\mathcal{T}_{\Sigma_0}(\mathcal{X}_0)$-subterms of t. Obviously, if $p, q \in top_{\Sigma_0}(t)$ and $p \neq q$ then neither $p \leq q$ nor $q \leq p$.

Proposition 4 (Invariants of top_{Σ_0} under E_0-equality). *Let $\mathcal{R} = (\Sigma, E_0 \cup B, R)$ be a rewrite theory with built-in subtheory (Σ_0, E_0). If t and t' are two terms in $\mathcal{H}_\Sigma(\mathcal{X})$ such that $t =_{E_0} t'$ then:*

1. *$top_{\Sigma_0}(t) = top_{\Sigma_0}(t')$,*
2. *$ls(t|_q) = ls(t'|_q)$ and $t|_q =_{E_0} t'|_q$ for all positions q in $top_{\Sigma_0}(t)$,*
3. *$t|_{q'} =_{E_0} t'|_{q'}$ for all positions q' such that $t|_{q'} \in \mathcal{H}_\Sigma(\mathcal{X})$, and*
4. *if $top_{\Sigma_0}(t) = \{q_1, \ldots, q_n\}$ then $t' = t[t'|_{q_1}]_{q_1} \cdots [t'|_{q_n}]_{q_n}$.*

Proposition 5 (Relation between $abstract_{\Sigma_1}$ and top_{Σ_0}). *Let $\mathcal{R} = (\Sigma, E_0 \cup B, R)$ be a rewrite theory with built-in subtheory (Σ_0, E_0). If t is a term in $\mathcal{H}_\Sigma(\mathcal{X})$, $abstract_{\Sigma_1}(t, \mathcal{Y}) = \langle \lambda \bar{x}.t^\circ; \theta^\circ; \phi^\circ \rangle$, where $\bar{x} = \{x_1, \ldots, x_n\}$ and $t^\circ = t[x_1]_{q_1} \cdots [x_n]_{q_n}$, then (i) $top_{\Sigma_0}(t) = \{q_1, \ldots, q_n\}$, and (ii) for every substitution $\sigma : \bar{x} \to \mathcal{T}_{\Sigma_0}(\mathcal{X}_0)$ it holds that $top_{\Sigma_0}(t^\circ\sigma) = top_{\Sigma_0}(t)$.*

Using the previous results it is possible to prove that rewriting with $\to^1_{R^\circ, B}$ doesn't depend on the chosen representative for a class of terms modulo E_0.

Lemma 2 (Independence of R°, B-rewriting under E_0-equality). *Let $\mathcal{R} = (\Sigma, E_0 \cup B, R)$ be a rewrite theory with built-in subtheory (Σ_0, E_0) and $\mathcal{R}^\circ = (\Sigma, E_0 \cup B, R^\circ)$ its normal rewrite theory. If t, u, and v are terms in $\mathcal{H}_\Sigma$, $t =_{E_0} u$, and $u \to^1_{R^\circ, B} v$ then there exists a term w in $\mathcal{H}_\Sigma$ such that $t \to^1_{R^\circ, B} w$ and $w =_{E_0} v$.*

The interchangeability of $\leftrightarrow_B$ and $\leftrightarrow_{E_0}$ deduction is now proved, first for one step of each type, then for one $\leftrightarrow_B$ deduction step and several $\leftrightarrow_{E_0}$ steps, and finally for any combination of $\leftrightarrow_B$ and $\leftrightarrow_{E_0}$ deduction steps.

Proposition 6 (One-step transposition of B-deduction and E_0-deduction).
Let $\mathcal{R} = (\Sigma, E_0 \cup B, R)$ be a rewrite theory with built-in subtheory (Σ_0, E_0). If t_0, t_1, and t_2 are terms in $\mathcal{H}_\Sigma(\mathcal{X})$ such that $t_0 \leftrightarrow_{E_0} t_1 \leftrightarrow_B t_2$ then there exists a term t'_1 in $\mathcal{H}_\Sigma(\mathcal{X})$ such that $t_0 \leftrightarrow_B t'_1 \leftrightarrow_{E_0} t_2$.

Proposition 7 (transposition of B and E_0-deduction).
Let $\mathcal{R} = (\Sigma, E_0 \cup B, R)$ be a rewrite theory with built-in subtheory (Σ_0, E_0). If $\{t_0, \ldots, t_{n+1}\}$ is a set of terms in $\mathcal{H}_\Sigma(\mathcal{X})$ such that $t_0 \leftrightarrow_{E_0} t_1 \leftrightarrow_{E_0} \cdots \leftrightarrow_{E_0} t_{n-1} \leftrightarrow_B t_n$ then there exists a set of terms $\{t'_1, \ldots, t'_{n-1}\}$ in $\mathcal{H}_\Sigma(\mathcal{X})$ such that $t_0 \leftrightarrow_B t'_1 \leftrightarrow_{E_0} \cdots \leftrightarrow_{E_0} t'_{n-1} \leftrightarrow_{E_0} t_n$.

Proposition 7 can also be stated as: if $t_0 =_{E_0} t_{n-1} \leftrightarrow_B t_n$ then there exists t'_1 such that $t_0 \leftrightarrow_B t'_1 =_{E_0} t_n$.

Proposition 8 (Decomposition of E-equality in B-equality plus E_0-equality).
Let $\mathcal{R} = (\Sigma, E, R)$ be a rewrite theory with built-in subtheory (Σ_0, E_0), and $\mathcal{R}^\circ = (\Sigma, E_0 \cup B, R^\circ)$ its normal rewrite theory. If t and t'' are terms in $\mathcal{H}_\Sigma(\mathcal{X})$ and $t =_E t''$ then there exists a term t' in $\mathcal{H}_\Sigma(\mathcal{X})$ such that $t =_B t' =_{E_0} t''$.

4 Rewriting with B-extensions

In this section, the last elements needed for the narrowing calculus are presented: B-extensions and rewrite theories closed under B-extensions. These concepts and their properties have been studied by Giesl and Kapur [GK01], and also by Meseguer [Mes17]. Then the equivalence of R/E-rewriting and R°, B-rewriting, for rewrite theories closed under B-extensions, is proved. This equivalence is crucial for the weak completeness of the narrowing calculus, shown in the following section.

Consider a rewrite theory $\mathcal{R}$ with only one sort s, and whose only rule is $f(a,b) \to c$, where f is associative and commutative ($E_0 = \emptyset$). The term $f(f(a,a),b)$ is a normal form in $\to^1_{R,B}$, but $f(f(a,a),b) \to^1_{R/E} f(a,c)$, because $f(f(a,a),b) =_E f(a,f(a,b))$, so the relations are different. This problem would not happen if $\mathcal{R}$ had another rule $f(x_s, f(a,b)) \to f(x_s,c)$ that could be applied on top of the term $f(f(a,a),b)$ with matching $x_s \mapsto a$, modulo associativity and commutativity, leading to $f(f(a,a),b) \to^1_{R,B} f(a,c)$. Rewrite theories that include these rules, avoiding such problems, are called *closed under B-extensions*.

Definition 20 (Closure under B-extensions). *Let $\mathcal{R} = (\Sigma, E_0 \cup B, R)$ be a rewrite theory, and let $l \to r$ if C be a rule in R. Assume, without loss of generality, that $vars(B) \cap vars(l \to r \text{ if } C) = \emptyset$. 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 define the set of B-*extensions *as the set:*
$Ext_B(l \to r \text{ if } C) = \{u[l]_p \to u[r]_p \text{ if } C \mid u = v \in B \cup B^{-1} \wedge p \in Pos_\Sigma(u) - \{\epsilon\} \wedge CSU_B(l, u_p) \neq \emptyset\}$,
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, $l \to r$ if C B-*subsumes *$l' \to r'$ if C iff there is a substitution σ such that: (i) $dom(\sigma) \cap vars(C) = \emptyset$, (ii) $l' =_B l\sigma$, and (iii) $r' =_B r\sigma$.*

We say that $\mathcal{R} = (\Sigma, E \cup A, R)$ is 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.*

Corollary 2 in [Mes17] (see Appendix A) can be applied in a straightforward way to $\to^1_{R,B}$, yielding the following lemma.

Lemma 3 (Independence of R, B-rewriting modulo B for rewrite theories closed under B-extensions).

Let $\mathcal{R} = (\Sigma, E_0 \cup B, R)$ be a rewrite theory with built-in subtheory (Σ_0, E_0). If R is closed under B-extensions then $\to^1_{R,B}$ is strictly coherent, i.e., for all t_1, t_2, t_3 if $t_1 \to^1_{R,B} t_2$ and $t_1 =_B t_3$ then there exists t_4 such that $t_3 \to^1_{R,B} t_4$ and $t_2 =_B t_4$ (see Fig. 2).

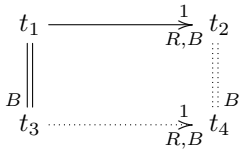

Fig. 2. strict coherence of $\to^1_{R,B}$

Example 9. In the cooking example, both R and R° are closed under B-extensions because the subterms of the equations in B have sorts `toast`, `tray`, or `pan`, and no head of any rule in R or R° has any of these sorts.

Theorem 1 (Equivalence of R/E and R°, B-rewriting for rewrite theories closed under B-extensions).
Let $\mathcal{R} = (\Sigma, E_0 \cup B, R)$ be a rewrite theory with built-in subtheory (Σ_0, E_0), and $\mathcal{R}^\circ = (\Sigma, E_0 \cup B, R^\circ)$ its normal rewrite theory. If $\mathcal{R}^\circ$ is closed under B-extensions then $\rightarrow^1_{R^\circ,B} = \rightarrow^1_{R/E}$ and $\rightarrow_{R^\circ,B} = \rightarrow_{R/E}$.

Corollary 1. *Let $\mathcal{R} = (\Sigma, E_0 \cup B, R)$ be a rewrite theory with built-in subtheory (Σ_0, E_0), and $\mathcal{R}^\circ$ its normal rewrite theory. If $\mathcal{R}^\circ$ is closed under B-extensions then any substitution is R/E-normalized iff it is R°, B-normalized.*

5 Reachability by conditional narrowing modulo SMT and axioms

In this section, the narrowing calculus for reachability is introduced, its soundness and weak completeness are proved, and completeness for *topmost* rewrite theories is also proved.

5.1 Narrowing, reachability goals and calculus

Some definitions and the calculus for reachability by conditional narrowing modulo SMT and axioms are presented now.

Narrowing is like R°, B-rewriting, where unification is used instead of matching, allowing the inspection of a set of initial states, namely the ground instances of the given symbolic initial state, which can have variables both in its SMT and non-SMT subterms, in contrast with [RMM17] whose initial states can only have variables in its SMT subterms.

Definition 21 (Narrowing). *Given a rewrite theory $\mathcal{R} = (\Sigma, E_0 \cup B, R)$ with built-in subtheory (Σ_0, E_0) and normal rewrite theory $\mathcal{R}^\circ = (\Sigma, E_0 \cup B, R^\circ)$, a reachability problem $P = \bigwedge_{i=1}^n t_i \rightarrow v_i \mid \psi$, and a rule $c^\circ = l \rightarrow r$ if $\bigwedge_{j=1}^m l_j \rightarrow r_j \mid \phi$ in R°, properly renamed so $vars(c^\circ) \cap vars(P) = \emptyset$, if there exists a term t_i, $1 \leq i \leq m$ (say 1 for simplicity), a non-variable position p in $Pos_\Sigma(t_1)$, and a substitution σ such that $t_1|_p\sigma =_B l\sigma$, $l_j\sigma \rightarrow_{R^\circ,B} r_j\sigma$, for $1 \leq j \leq m$, and $(\psi \wedge \phi)\sigma$ is satisfiable, then we write $P \rightsquigarrow_{1,p,c^\circ,\sigma} (t_1[r]_p \rightarrow v_1 \wedge \bigwedge_{i=2}^n t_i \rightarrow v_i)\sigma \mid (\psi \wedge \phi)\sigma$ and say that there is a* narrowing step *from P to $(t_1[r]_p \rightarrow v_1 \wedge \bigwedge_{i=2}^n t_i \rightarrow v_i)\sigma \mid (\psi \wedge \phi)\sigma$.*

In the expression $P \rightsquigarrow_{1,p,c^\circ,\sigma} P'$ it is admitted to omit any part of the subindex when it is not relevant to the matter discussed.

Consider a reachability problem $P = \bigwedge_{i=1}^n t_i \rightarrow v_i \mid \psi$. For simplicity of the explanation, let $n = 1$. A way to solve this problem using narrowing is to find a series of narrowing steps $t_1 \rightarrow v_1 \mid \psi \rightsquigarrow_{\sigma_1} \cdots \rightsquigarrow_{\sigma_{m-1}} t' \rightarrow v_1\sigma_1 \cdots \sigma_{m-1} \mid \phi$ and then find a substitution σ_m such that $t'\sigma_m =_E v_1\sigma_1 \cdots \sigma_m$ and $E_0 \vDash \phi\sigma_m$. It is immediate to show, using induction over the number of narrowing steps, that $\sigma = \sigma_1 \cdots \sigma_m$ is a solution for P.

In Definition 21, in order to perform a narrowing step from the term t_1 in P with rule c° it is required that $t_1|_p\sigma =_B l\sigma$, $l_j\sigma \rightarrow_{R^\circ,B} r_j\sigma$, for $1 \leq j \leq m$, and $E_0 \vDash (\psi \wedge \phi)\sigma$. This is not a trivial task. A method to achieve this task is to consider a position p in $Pos_\Sigma(t_1)$, and a B-unifier ρ_0 in $CSU_B(t_1|_p = l)$. Then $l_j\rho_0 \rightarrow r_j\rho_0$, for $1 \leq j \leq m$, is a set of reachability problems. Each problem $l_j\rho_0 \cdots \rho_{j-1} \rightarrow r_j\rho_0 \cdots \rho_{j-1}$, for $1 \leq j \leq m$, is solved recursively by narrowing, yielding the next substitution ρ_j as solution. We take $\sigma = \rho_0 \cdots \rho_m$. If $(\psi \wedge \phi)\sigma$ is satisfiable, then $P \rightsquigarrow_{1,p,c^\circ,\sigma} (t_1[r]_p \rightarrow v_1 \wedge \bigwedge_{i=2}^n t_i \rightarrow v_i)\sigma \mid (\psi \wedge \phi)\sigma$.

The method sketched in the previous paragraphs is the one used in the *calculus for reachability by conditional narrowing modulo SMT and axioms*, whose calculus rules are shown in Figure 3. This calculus handles an extension of reachability problems, called *reachability goals*.

Definition 22 (Reachability goal). *Given a rewrite theory $\mathcal{R} = (\Sigma, E_0 \cup B, R)$ with built-in subtheory (Σ_0, E_0), a reachability goal G is an expression with the form*

1. $\bigwedge_{i=1}^{n} u_i \to v_i \mid \phi$, *or*
2. $u_1 \to^1 x_k, u_2[x_k]_p \to v_2 \wedge \bigwedge_{i=3}^{n} u_i \to v_i \mid \phi$,

where $n \geq 0$, $u_i, v_i \in \mathcal{H}_\Sigma(\mathcal{X})$, for $1 \leq i \leq n$, $\phi \in QF(\mathcal{X}_0)$, $p \in Pos(u_2)$, $k = [ls(u_1)]$, the kind of the least sort of u_1, and x_k appears exactly twice in G in case (2). We say that x_k is the connecting variable *of the goal.*

Reachability problems are reachability goals with the first form; reachability goals with the second form are generated by the calculus rules; this second form prevents the repeated application of rule transitivity in a derivation, forcing the calculus of a narrowing step in the first subgoal of the reachability problem.

The notations $P \rightsquigarrow_{[r]} P'$, $P \rightsquigarrow_{[r],\sigma} P'$, or $P \rightsquigarrow_{[r],c^\circ,\sigma} P'$, will be used in the calculus to indicate that rule $[r]$ of the calculus has been applied (with substitution σ, if needed, and using rule c° from R° in the case that $[r]$ is the rewrite rule) to P, yielding P'.

We extend the definition of solution of a reachability problem in $\to_{R/E}$ and $\to_{R^\circ,B}$ to reachability goals with the second form.

Definition 23 (Solution of a reachability goal in $\to_{R/E}$). *Given a reachability goal $G = u_1 \to^1 x_k, u_2[x_k]_p \to v_2 \wedge \bigwedge_{i=3}^{n} u_i \to v_i \mid \phi$, a substitution $\sigma : vars(G) \to \mathcal{T}_\Sigma$ is a* solution *of G in $\to_{R/E}$ if $u_1\sigma \to^1_{R/E} x_k\sigma$, $u_2[x_k]_p\sigma \to_{R/E} v_2\sigma$, $u_i\sigma \to_{R/E} v_i\sigma$, for $3 \leq i \leq n$, and $E_0 \models \phi\sigma$.*

Definition 24 (Solution of a reachability goal in $\to_{R^\circ,B}$). *Given a reachability goal $G = u_1 \to^1 x_k, u_2[x_k]_p \to v_2 \wedge \bigwedge_{i=3}^{n} u_i \to v_i \mid \phi$, a substitution $\sigma : vars(G) \to \mathcal{T}_\Sigma$ is a* solution *of G in $\to_{R^\circ,B}$ if $u_1\sigma \to^1_{R^\circ,B} x_k\sigma$, $u_2[x_k]_p\sigma \to_{R^\circ,B} v_2\sigma$, $u_i\sigma \to_{R^\circ,B} v_i\sigma$, for $3 \leq i \leq n$, and $E_0 \models \phi\sigma$.*

We call *nil* $\mid \phi$, where ϕ is satisfiable, an *empty goal*. Given a rewrite theory $\mathcal{R} = (\Sigma, E, R)$ with built-in subtheory (Σ_0, E_0), whose normal rewrite theory $\mathcal{R}^\circ = (\Sigma, E_0 \cup B, R^\circ)$ is closed under B-extensions, a reachability problem P in $\to_{R/E}$ is solved by applying the calculus rules in Figure 3, starting with P and in a top-down manner, until an empty goal is obtained, generating a *narrowing path*.

Definition 25 (Computed answer). *Given a rewrite theory $\mathcal{R} = (\Sigma, E, R)$ with built-in subtheory (Σ_0, E_0), and a reachability goal G, if there is a narrowing path $G \rightsquigarrow_{\sigma_1} G_1 \rightsquigarrow_{\sigma_2} \cdots \rightsquigarrow_{\sigma_{n-1}} G_{n-1} \rightsquigarrow_{\sigma_n}$ nil $\mid \psi$, using the calculus rules in Figure 3, hence ψ is satisfiable, then we write $G \rightsquigarrow^*_\sigma$ nil $\mid \psi$, with $\sigma = \sigma_1 \cdots \sigma_n$, and we call $\sigma_{vars(G)} \mid \psi$ a* computed answer *for G. As the unifiers σ_i, $1 \leq i \leq n$, returned by CSU_B are idempotent and away from all the variables that have previously appeared in the computation, so $ran(\sigma_i) \cap \bigcup_{j=1}^{i-1} ran(\sigma_j) = \emptyset$, then σ is also idempotent.*

Rules unification and rewrite allow for simplifications in the reachability formulas obtained, i.e., $(\phi \wedge \phi^\circ)\theta$ can be replaced with another formula ψ under the assumptions stated in both rules. For instance $X - Y + Z > 0 \wedge X = Y$ can be replaced with $Z > 0$. It is always possible to obtain the same computed answer without using simplifications.

Proposition 9 (Canonical path). *Given a rewrite theory $\mathcal{R} = (\Sigma, E, R)$ with built-in subtheory (Σ_0, E_0), and a narrowing path from a reachability goal G, $G = \Delta_0 \mid \psi_0 \rightsquigarrow_{\sigma_1} \Delta_1 \mid \psi_1 \rightsquigarrow_{\sigma_2}$*

– $[u]$ unification

$$\frac{u \to v \ \wedge \ \Delta \mid \phi}{\Delta\theta \mid \psi}$$

where $abstract_{\Sigma_1}(v) = \langle \lambda\bar{x}.v^\circ; \theta^\circ; \phi^\circ \rangle$, θ in $CSU_B(u = v^\circ)$,
$vars(\psi) \subseteq vars((\phi \wedge \phi^\circ)\theta)$, $E_0 \vdash \psi \Leftrightarrow (\phi \wedge \phi^\circ)\theta$, and ψ is satisfiable

– $[t]$ transitivity

$$\frac{u \to v \ (\wedge \ \Delta) \mid \phi}{u \to^1 x_k, x_k \to v \ (\wedge \ \Delta) \mid \phi}$$

where $u \notin \mathcal{X}$, $k = [ls(u)]$, and x_k fresh variable

– $[c]$ congruence

$$\frac{u|_p \to^1 x_k, u[x_k]_p \to v \ (\wedge \ \Delta) \mid \phi}{u_i \to^1 y_{k'}, u[y_{k'}]_{p.i} \to v \ (\wedge \ \Delta) \mid \phi}$$

where $u|_p = f(u_1, \ldots, u_n)$, $u_i \notin \mathcal{X} \cup \mathcal{T}_{\Sigma_0}(\mathcal{X}_0)$,
$k' = [ls(u_i)]$, $1 \leq i \leq n$, and $y_{k'}$ fresh variable

– $[r]$ rewrite

$$\frac{u|_p \to^1 x_k, u[x_k]_p \to v \ (\wedge \ \Delta) \mid \phi}{(C \wedge u[r]_p \to v \ (\wedge \ \Delta))\theta \mid \psi}$$

where $u|_p \notin \mathcal{X}$, $l^\circ \to r$ *if* $C \mid \phi^\circ$ fresh rule in R°, θ in $CSU_B(u|_p = l^\circ)$,
$vars(\psi) \subseteq vars((\phi \wedge \phi^\circ)\theta)$, $E_0 \vdash \psi \Leftrightarrow (\phi \wedge \phi^\circ)\theta$, and ψ is satisfiable

Fig. 3. Inference rules for reachability by conditional narrowing modulo SMT and axioms.

$\cdots \Delta_{m-1} \mid \psi_{m-1} \rightsquigarrow_{\sigma_m} nil \mid \psi_m$, *there exists another narrowing path* $G = \Delta_0 \mid \psi_0 \rightsquigarrow_{\sigma_1} \Delta_1 \mid \chi_1 \rightsquigarrow_{\sigma_2} \cdots \Delta_{m-1} \mid \chi_{m-1} \rightsquigarrow_{\sigma_m} nil \mid \chi_m$, *where the same inference rule is applied at each step in both paths, there is no simplification of the reachability formula when rule* unification *or* rewrite *is applied on the second path, and* $E_0 \vdash \psi_i \Leftrightarrow \chi_i$, *for* $1 \leq i \leq m$.

The aim of this work is to solve reachability problems; it must be born in mind that a reachability goal with the second form comes from a reachability problem. Now it is proved that the calculus rules are a sound method for solving reachability goals in $\rightarrow_{R^\circ,B}$. A distinction is made depending on the form of the reachability goal. For goals of the second form it is necessary to be very careful with the connecting variable of the goal, since this variable does not appear in the original reachability problem.

5.2 Soundness and weak completeness of the calculus

Soundness and weak completeness, i.e., completeness with respect to R/E-normalized solutions, in $\rightarrow_{R/E}$ of the calculus for reachability problems are now proved.

Theorem 2 (Soundness in $\rightarrow_{R^\circ,B}$ of the Calculus for Reachability Goals). *Given a rewrite theory* $\mathcal{R} = (\Sigma, E_0 \cup B, R)$ *with built-in subtheory* (Σ_0, E_0), *where* $E = E_0 \cup B$, *and a narrowing path from a reachability goal* G, $G = \Delta_1 \mid \psi_1 \rightsquigarrow_{\sigma_1} \Delta_2 \mid \psi_2 \rightsquigarrow_{\sigma_2} \cdots \Delta_m \mid \psi_m \rightsquigarrow_{\sigma_m} nil \mid \psi$, *let* $\sigma = \sigma_1 \cdots \sigma_m$, *then:*

1. *if* $\Delta_1 = \bigwedge_{i=1}^n u_i \rightarrow v_i$ *and* $\rho : \mathcal{X} \rightarrow \mathcal{T}_\Sigma$ *is a substitution such that* $dom(\rho) = vars(G\sigma)$ *and* $\psi\rho$ *is satisfiable then* $(\sigma\rho)_{vars(G)}$ *is a solution for* G *in* $\rightarrow_{R^\circ,B}$, *and*
2. *if* $\Delta_1 = u_1|_p \rightarrow^1 x, u_1[x]_p \rightarrow v_1 \wedge \bigwedge_{i=2}^n u_i \rightarrow v_i \mid \psi_1$ *and* $\rho : \mathcal{X} \setminus \{x\} \rightarrow \mathcal{T}_\Sigma$ *is a substitution such that* $dom(\rho) = vars(G\sigma) \setminus \{x\}$ *and* $\psi\rho$ *is satisfiable then*
   (a) $(\sigma\rho)_{vars(G)\setminus\{x\}}$ *is a solution for* $\bigwedge_{i=1}^n u_i \rightarrow v_i \mid \psi_1$ *in* $\rightarrow_{R^\circ,B}$ *and*
   (b) *there exists a substitution* $\rho_x : \{x\} \rightarrow \mathcal{T}_\Sigma$ *such that* $(\sigma(\rho \cup \rho_x))_{vars(G)}$ *is a solution for* G *in* $\rightarrow_{R^\circ,B}$.

Proof. By structural induction over the length of the narrowing path and the first inference rule applied.

The soundness of the calculus rules with respect to the solutions of reachability problems in $\rightarrow_{R/E}$, for rewrite theories closed under B-extensions, is now a consequence of the soundness of the calculus rules in $\rightarrow_{R^\circ,B}$ and the fact that reachability problems are a special case of reachability goals.

Theorem 3 (Soundness in $\rightarrow_{R/E}$ of the Calculus for Reachability Problems). *Given a rewrite theory* $\mathcal{R} = (\Sigma, E_0 \cup B, R)$ *with built-in subtheory* (Σ_0, E_0), *where* $E = E_0 \cup B$, *whose normal rewrite theory* $\mathcal{R}^\circ = (\Sigma, E_0 \cup B, R^\circ)$ *is closed under* B*-extensions, and a narrowing path from a reachability problem* G, $G = \bigwedge_{i=1}^n u_i \rightarrow v_i \mid \psi_1 \rightsquigarrow_\sigma^* nil \mid \psi$, *if* $\rho : \mathcal{X} \rightarrow \mathcal{T}_\Sigma$ *is a substitution such that* $dom(\rho) = vars(G\sigma)$ *and* $\psi\rho$ *is satisfiable then* $(\sigma\rho)_{vars(G)}$ *is a solution for* G *in* $\rightarrow_{R/E}$.

Proof. By Theorem 2 (1), $(\sigma\rho)_{vars(G)}$ is a solution for G in $\rightarrow_{R^\circ,B}$. As $\mathcal{R}^\circ$ is closed under B-extensions, then, by Theorem 1, $(\sigma\rho)_{vars(G)}$ is also a solution for G in $\rightarrow_{R/E}$.

Finally, it is proved that any R/E-normalized solution of a reachability problem P is a satisfiable instance of a computed answer for P.

Theorem 4 (Weak Completeness in $\to_{R/E}$ of the Calculus for Reachability Problems). *Given a rewrite theory $\mathcal{R} = (\Sigma, E_0 \cup B, R)$ with built-in subtheory (Σ_0, E_0), where $E = E_0 \cup B$, whose normal rewrite theory $\mathcal{R}^\circ = (\Sigma, E_0 \cup B, R^\circ)$ is closed under B-extensions, and a reachability problem $P = \bigwedge_{i=1}^n u_i \to v_i \mid \phi$, if σ is an idempotent R/E-normalized solution for P in $\to_{R/E}$ then there exist a formula $\psi \in QF(\mathcal{X}_0)$, and substitutions γ and δ, such that $P \rightsquigarrow_\gamma^* nil \mid \psi$, $\sigma = (\gamma\delta)_{vars(P)}$, and $\psi\delta$ is satisfiable.*

Proof. By Theorem 1, $u_i\sigma \to_{R^\circ,B} v_i\sigma$, for $1 \leq i \leq n$. The proof is by induction over the number of R°, B-rewrite steps. No simplification is applied to the reachability formulas that appear in the generated path.

(i) Base case: zero rewrite steps. The proof is by induction over n, the size of the conjunction.

- Base case, $n = 1$: $P = u_1 \to v_1 \mid \phi$, $u_1\sigma =_E v_1\sigma$, and $E_0 \vDash \phi\sigma$. By Proposition 8, there exists a term w such that $u_1\sigma =_B w =_{E_0} v_1\sigma$. As σ is idempotent then also $u_1\sigma =_B w\sigma =_{E_0} v_1\sigma$. Let $abstract_{\Sigma_1}(v_1) = \langle \lambda\bar{x}.v_1^\circ; \theta^\circ; \phi^\circ \rangle$, with $\bar{x} = \{x_1, \ldots, x_n\}$, and let $top_{\Sigma_0}(v_1^\circ) = \{q_1, \ldots, q_n\}$. Let $\sigma^\circ = \sigma \cup \bigcup_{i=1}^n \{x_i \mapsto w|_{q_i}\sigma\}$. By Proposition 5, $top_{\Sigma_0}(v_1^\circ\sigma) = top_{\Sigma_0}(v_1)$. Then, by Proposition 4, $w\sigma = v_1\sigma[w|_{q_1}\sigma]_{q_1} \cdots [w|_{q_n}\sigma]_{q_n}$, where $w|_{q_i}\sigma =_{E_0} v_1|_{q_i}\sigma$, for $1 \leq i \leq n$. Let $\sigma^\circ = \sigma \cup \bigcup_{i=1}^n \{x_i \mapsto w|_{q_i}\sigma\}$. Then $v_1^\circ\sigma^\circ = (v_1[x_1]_{q_1} \cdots [x_n]_{q_n})\sigma^\circ = v_1\sigma[w|_{q_1}\sigma]_{q_1} \cdots [w|_{q_n}\sigma]_{q_n} = w\sigma =_B u_1\sigma = u_1\sigma^\circ$, because $vars(P) \cap \bar{x} = \emptyset$ implies $v_1\sigma^\circ = v_1\sigma$ and $u_1\sigma = u_1\sigma^\circ$. As $u_1\sigma^\circ =_B v_1^\circ\sigma^\circ$, there exist substitutions γ_1 and δ_1 such that $\gamma_1 \in CSU_B(u_1 = v_1^\circ)$ and $\sigma^\circ = \gamma_1\delta_1$, so $\sigma = (\gamma_1\delta_1)_{vars(P)}$.
  $vars(\phi) \cap \bar{x} = \emptyset$ implies $\phi\sigma^\circ = \phi\sigma$ so $E_0 \vDash \phi\sigma^\circ$, because $E_0 \vDash \phi\sigma$. Also, as $\phi^\circ\sigma^\circ = \bigwedge_{i=1}^n (w|_{q_i}\sigma = v_1|_{q_i}\sigma)$ because $vars(v) \cap \bar{x} = \emptyset$, $E_0 \vDash \phi^\circ\sigma^\circ$, so $E_0 \vDash (\phi \wedge \phi^\circ)\sigma^\circ$. Let $\psi = (\phi \wedge \phi^\circ)\gamma_1$. Then, as $\sigma^\circ = \gamma_1\delta_1$, ψ and $\psi\delta$ are satisfiable.
  As $\gamma_1 \in CSU_B(u = v^\circ)$ and ψ is satisfiable then $u_1 \to v_1 \mid \phi \rightsquigarrow_{[u],\gamma_1} nil \mid \psi$.
- Induction case, $n > 1$: $P = \bigwedge_{i=1}^n u_i \to v_i \mid \phi$, and $u_i\sigma =_E v_i\sigma$, for $1 \leq i \leq n$. Using the same proof of the base case $u_1 \to v_1 \wedge \bigwedge_{i=2}^n u_i \to v_i \mid \phi \rightsquigarrow_{[u],\gamma_1} \bigwedge_{i=2}^n u_i\gamma_1 \to v_i\gamma_1 \mid (\phi \wedge \phi^\circ)\gamma_1$ and $\sigma^\circ = \gamma_1\delta_1$. Let $G' = \bigwedge_{i=2}^n u_i\gamma_1 \to v_i\gamma_1 \mid \phi\gamma_1 \wedge \phi^\circ\gamma_1$. Then δ_1 is a solution of G' because $\sigma^\circ = \gamma_1\delta_1$, $E_0 \vDash (\phi \wedge \phi^\circ)\sigma^\circ$, and $u_i\sigma^\circ = u_i\sigma =_E v_i\sigma = v_i\sigma^\circ$, for $2 \leq i \leq n$. By induction hypothesis, there exist a formula $\psi \in QF(\mathcal{X}_0)$, and substitutions γ_2 and δ such that $G' \rightsquigarrow_{\gamma_2}^* nil \mid \psi$, $\delta_1 = (\gamma_2\delta)_{vars(G')}$, and $\psi\delta$ is satisfiable. Let $\gamma = \gamma_1\gamma_2$. Then $P \rightsquigarrow_{[u],\gamma_1} G' \rightsquigarrow_{\gamma_2}^* nil \mid \psi$, i.e., $P \rightsquigarrow_\gamma^* nil \mid \psi$, and $(\gamma\delta)_{vars(P)} = (\gamma_1\gamma_2\delta)_{vars(P)} = (\gamma_1\delta_1)_{vars(P)} = (\sigma^\circ)_{vars(P)} = \sigma$.

(ii) Induction case: at least there is one rewrite step. If there are not rewrite steps in $u_1\sigma \to_{R^\circ,B} v_1\sigma$ then reorder the reachability problem in a way that there is one rewrite step in the first subproblem. Let $\Delta = \bigwedge_{i=2}^n u_i \to v_i$. Then $P = u_1 \to v_1 \wedge \Delta \mid \phi$, $u_1\sigma \to_{R^\circ,B}^1 u' \to_{R^\circ,B} w =_E v_1\sigma$, $E_0 \vDash \phi\sigma$, and $u_i\sigma \to_{R^\circ,B} v_i\sigma$, for $2 \leq i \leq n$. As σ is idempotent then also $u_1\sigma \to_{R^\circ,B}^1 u'\sigma \to_{R^\circ,B} w\sigma =_E v_1\sigma$.

$u_1\sigma \to_{R^\circ,B}^1 u'\sigma$ with a rule $c^\circ = l^\circ \to r$ *if* $\bigwedge_{j=1}^m l_j \to r_j \wedge \phi^\circ$ in R° with some substitution δ at a position p in $Pos(u_1\sigma)$, because $u_1\sigma|_p =_B l^\circ\delta$, $E_0 \vDash \phi^\circ\delta$, $u' = u_1\sigma[r\delta]_p$, and $l_j\delta \to_{R^\circ,B} r_j\delta$, for $1 \leq j \leq m$. $p \in Pos_\Sigma(u_1)$ because otherwise there exists some integer k, $1 \leq k \leq m$, such that either $u_1|_p = y_k$ or the rewriting takes place at some position in a subterm of the form $y_k\sigma$. In both cases σ would be neither R°, B-normalized, nor R/E-normalized.

Then $u_1|_p\sigma = u_1\sigma|_p =_B l^\circ\delta$ and there exist idempotent substitutions α and β such that $\alpha \in CSU_B(u_1|_p = l^\circ)$ and $\sigma \cup \delta = \alpha\beta$, so $(\phi \wedge \phi^\circ)\alpha$ is satisfiable. Then $u_1 \to v_1 \wedge R \mid \phi \rightsquigarrow_{[t]} u_1 \to^1 x_\kappa, x_\kappa \to v_1 \wedge \Delta \mid \phi \rightsquigarrow_{[c]}^* u_1|_p \to^1 y_{\kappa'}, u_1[y_{\kappa'}]_p \to v_1 \wedge \Delta \mid \phi \rightsquigarrow_{[w],c^\circ,\alpha} \bigwedge_{j=1}^m l_j\alpha \to r_j\alpha \wedge u_1[r]_p\alpha \to v_1\alpha \wedge \Delta\alpha \mid (\phi \wedge \phi^\circ)\alpha$.

As $\sigma \cup \delta = \alpha\beta$ then:

1. $l_j\alpha\beta = l_j\delta \to_{R^\circ,B} r_j\delta = r_j\alpha\beta$, for $1 \leq j \leq m$,

2. $u_i\alpha\beta = u_i\delta \to_{R^\circ,B} v_i\delta = v_i\alpha\beta$, for $2 \leq i \leq n$,
3. $u_1[r]_p\alpha\beta = u_1\alpha\beta[r\alpha\beta]_p = u_1\sigma[r\delta]_p \to_{R^\circ,B} v_1\sigma = v_1\alpha\beta$, and
4. $(\phi \wedge \phi^\circ)\alpha\beta = (\phi \wedge \phi^\circ)\delta$ and $E_0 \vDash (\phi \wedge \phi^\circ)\delta$ implies $E_0 \vDash (\phi \wedge \phi^\circ)\alpha\beta$.

Then $\beta_{vars(G')}$ is a solution of the reachability problem $G' = \bigwedge_{i=1}^n l_i\alpha \to r_i\alpha \wedge u_1[r]_p\alpha \to v_1\alpha \wedge \Delta\alpha \mid (\phi \wedge \phi^\circ)\alpha$ that takes one less rewrite step than those taken to prove $P\sigma$ so, by induction hypothesis, there exist a formula $\psi \in QF(\mathcal{X}_0)$, and substitutions α' and δ' such that $G' \rightsquigarrow^*_{\alpha'} nil \mid \psi$, $\psi\delta'$ is satisfiable, and $\beta_{vars(G')} = (\alpha'\delta')_{vars(G')}$, so $P \rightsquigarrow_\alpha G' \rightsquigarrow^*_{\alpha'} nil \mid \psi$, i.e., $P \rightsquigarrow^*_{\alpha\alpha'} nil \mid \psi$. Let $\gamma = \alpha\alpha'$ and $\delta = \delta' \cup \{y \mapsto y\beta \mid y \in dom(\beta) \setminus vars(G')\}$.

For all variables x in $vars(P)$ and all variables y in $vars(x\alpha)$:

- if $y \in vars(G')$ then $y\alpha'\delta = y(\alpha'\delta')_{vars(G')} = y(\beta)_{vars(G')} = y\beta$, and
- if $y \notin vars(G')$ then $y\alpha' = y$. As $y \in vars(x\alpha)$ implies $y \in dom(\beta)$, then $y \in dom(\beta) \setminus vars(G')$, so $y\alpha'\delta = y\delta = y\beta$.

Then $x\gamma\delta = x\alpha\alpha'\delta = x\alpha\beta = x\sigma$, so $\sigma = (\gamma\delta)_{vars(P)}$. Also $vars(\psi) \cap (dom(\beta) \setminus vars(G')) = \emptyset$, because $vars(\psi)$ may only have variables in $vars(G')$ together with new fresh variables not in $vars(P)$, hence also not in $dom(\beta)$, so $\psi\delta = \psi\delta'$ and $\psi\delta$ is satisfiable.

5.3 Completeness in $\to_{R/E}$ of the calculus, for topmost rewrite theories

In the proof of weak completeness of the calculus for reachability, the only place where the hypothesis of σ being R/E-normalized is used is in the induction case, (ii), where it limits the positions where rewriting can happen at some proper subterm of $u_1\sigma$, an instance of the first term in the reachability problem P (u_1). It is immediate then to prove the *completeness of the calculus for topmost rewrite theories*, those rewrite theories $\mathcal{R} = (\Sigma, E, R)$ such that for some top sort `state`, no operator in Σ has `state` as argument sort and each rule $l \to r$ *if* $\bigwedge_{i=1}^n l_i \to r_i \mid \phi$ in R satisfies $l, r \in \mathcal{T}_\Sigma(\mathcal{X})_{\texttt{state}}$ and $l_i, r_i \in \mathcal{T}_\Sigma(\mathcal{X})_{\texttt{state}}$, for $1 \leq i \leq n$, since rewriting always happens at position ϵ of $u_1\sigma$, so the hypothesis of σ being R/E-normalized is not needed for this type of rewrite theories in the proof of completeness.

6 Example

An application of the calculus using the running example is shown. All the subindices for variables with sort `integer` are omitted for readability. Recall the rest of subindices: $\texttt{p} - \texttt{pan}, \texttt{rt} - \texttt{realToast}$, $\texttt{t} - \texttt{toast}, \texttt{k} - \texttt{kitchen}, \texttt{r} - \texttt{tray}, \texttt{s} - \texttt{system}$. Consider the reachability goal $G = n_1/\texttt{zt}/0; \texttt{ztzt}/0 \to m/x_\texttt{r}/t; y_\texttt{p}/1 \mid n_1 > 0 \wedge n_1 < 3 \wedge t < 12$, where from an initial `system` consisting of a bag containing one or two `realToast`s, an empty `tray`, an empty `kitchen` (with zero seconds of elapsed time), and no well-cooked `realToast`s, it is desired to reach a `system` with one well-cooked `realToast` in less than twelve seconds. Let $F = m/x_\texttt{r}/t; y_\texttt{p}/1$, $\phi_1 = n_1 > 0 \wedge n_1 < 3 \wedge t < 12$, and $\phi_2 = n_2 > 0 \wedge n_2 < 3 \wedge t < 12$. Then $abstract_{\Sigma_1}(F) = \langle \lambda ok.F^\circ; \theta^\circ; \phi^\circ \rangle$, with $F^\circ = m/x_\texttt{r}/t; y_\texttt{p}/ok$ and $\phi^\circ = (ok = 1)$. The labels of the rules used in each `rewrite` step are those in Example 4, with rule $r7^\circ$ instead of rule $r7$. Narrowing steps involving rules $[t]$ or $[c]$ have been joined in multiple narrowing steps, for instance $\rightsquigarrow^*_{[t],[c],[r]}$, after their first occurrences. The interaction between unification, SMT operations, and satisfiability is explained using the number of well-cooked `realToast`s, $0 + 1$, in step 15:

1. $n_1/\texttt{zt}/0; \texttt{zt zt}/0 \to F \mid \phi_1 \rightsquigarrow_{[t]}$
2. $n_1/\texttt{zt}/0; \texttt{zt zt}/0 \to^1 x1_{[\texttt{s}]}, x1_{[\texttt{s}]} \to F \mid \phi_1 \rightsquigarrow_{[r]r2,\sigma_2=\{n_1 \mapsto n_2\}}$
3. $n_2 - 1/[0,0]/0; \texttt{zt zt}/0 \to F \mid \phi_2 \rightsquigarrow_{[t]}$

4. $n_2 - 1/[0,0]/0; \mathtt{zt}\ \mathtt{zt}/0 \to^1 x2_{[\mathtt{s}]}, x2_{[\mathtt{s}]} \to F \mid \phi_2 \rightsquigarrow_{[r]r3}$
5. $n_2 - 1/\mathtt{zt}/0; [0,0]\ \mathtt{zt}/0 \to F \mid \phi_2 \rightsquigarrow^*_{[t]}$
6. $n_2 - 1/\mathtt{zt}/0; [0,0]\ \mathtt{zt}/0 \to^1 x3_{[\mathtt{s}]}, x3_{[\mathtt{s}]} \to F \mid \phi_2 \rightsquigarrow^*_{[c]}$
7. $0; [0,0]\ \mathtt{zt} \to^1 y2_{[\mathtt{k}]}, n_2 - 1/\mathtt{zt}/y2_{[\mathtt{k}]}/0 \to F \mid \phi_2 \rightsquigarrow_{[r]r4}$
8. $n_2 - 1/\mathtt{zt}/\mathtt{cook}(0; [0,0]\ \mathtt{zt}, z_1)/0 \to F \mid \phi_2 \wedge z_1 > 0 \rightsquigarrow^*_{[t],[c],[r]r1b}$
9. $n_2 - 1/\mathtt{zt}/z_1; [z_1,0]\ \mathtt{zt}/0 \to F \mid \phi_2 \wedge z_1 > 0 \wedge z_1 \leq 5 \rightsquigarrow^*_{[t],[c],[r]r5}$
10. $n_2 - 1/\mathtt{zt}/z_1; [0,z_1]\ \mathtt{zt}/0 \to F \mid \phi_2 \wedge z_1 > 0 \wedge z_1 \leq 5 \rightsquigarrow^*_{[t],[c],[r]r4}$
11. $n_2 - 1/\mathtt{zt}/\mathtt{cook}(z_1; [0,z_1]\ \mathtt{zt}, z_2)/0 \to F \mid \phi_2 \ \wedge\ z_1 > 0 \wedge z_1 \leq 5 \rightsquigarrow^*_{[t],[c],[r]r1b}$
12. $n_2 - 1/\mathtt{zt}/z_1 + z_2; [z_2,z_1]\ \mathtt{zt}/0 \to F \mid \phi_2 \ \wedge\ z_1 > 0 \wedge z_1 \leq 5 \wedge z_2 > 0 \wedge z_2 \leq 5 \rightsquigarrow_{[t]}$
13. $n_2 - 1/\mathtt{zt}/z_1 + z_2; [z_2,z_1]\ \mathtt{zt}/0 \to^1 x4_{[\mathtt{s}]}, x4_{[\mathtt{s}]} \to F \mid \phi_2 \ \wedge\ z_1 > 0 \wedge z_1 \leq 5 \wedge z_2 > 0 \wedge z_2 \leq 5 \rightsquigarrow_{[r]r7^\circ}$
14. $\mathtt{cook}(z_1 + z_2; \mathtt{zt}\ \mathtt{zt}, 1) \to y3_{[\mathtt{k}]} \wedge n_2 - 1/\mathtt{zt}/y3_{[\mathtt{k}]}/0 + 1 \to F \mid \phi_2 \ \wedge\ z_1 = 5 \wedge z_2 = 5 \rightsquigarrow^*_{[t],[c],[r]r1c}$
15. $n_2 - 1/\mathtt{zt}/1 + z_1 + z_2; \mathtt{zt}\ \mathtt{zt}/0 + 1 \to F \mid \ \wedge n_2 > 0 \wedge n_2 < 3 \wedge t < 12 \wedge z_1 = 5 \wedge z_2 = 5 \rightsquigarrow_{[u],F^\circ,\phi_0^\circ,\sigma_{15}}$
16. $nil \mid n_2 > 0 \wedge n_2 < 3 \wedge z_1 = 5 \wedge z_2 = 5$

The last narrowing step, the unification of $n_2 - 1/\mathtt{zt}/1 + z_1 + z_2; \mathtt{zt}\ \mathtt{zt}/0 + 1$ with F°, i.e., $m/x_{\mathtt{r}}/t; y_{\mathtt{p}}/ok$, is explained in detail. The unifier, indeed a matching, is $\sigma_{15} = \{m \mapsto n_2 - 1, x_{\mathtt{r}} \mapsto \mathtt{zt}, t \mapsto 1 + z_1 + z_2, y_{\mathtt{p}} \mapsto \mathtt{zt}\,\mathtt{zt}, ok \mapsto 0 + 1\}$. As there is a substitution $\sigma_2 = \{n_1 \mapsto n_2\}$ in step 2, then $\sigma_{vars(G)} = (\sigma_1 \cdots \sigma_{15})_{vars(G)} = \{n_1 \mapsto n_2, x_{\mathtt{r}} \mapsto \mathtt{zt}, t \mapsto 1 + z_1 + z_2, y_{\mathtt{p}} \mapsto \mathtt{zt}\,\mathtt{zt}, ok \mapsto 0 + 1\}$, where ok does not map to 1, but to $0 + 1$.

The new condition, including $\phi^\circ = (ok = 1)$, becomes $n_2 > 0 \wedge n_2 < 3 \wedge 1 + z_1 + z_2 < 12 \wedge z_1 = 5 \wedge z_2 = 5 \wedge 0 + 1 = 1$, which simplifies to $n_2 > 0 \wedge n_2 < 3 \wedge z_1 = 5 \wedge z_2 = 5$.

The computed answer for the reachability goal shows two different solutions, one with $n_2 = 1$ and another one with $n_2 = 2$. As $t = 1 + z_1 + z_2$, $z_1 = 5$, and $z_2 = 5$, then from a bag with one or two `realToast`s, it is possible to reach a `system` with one well-cooked `realToast` in $1 + 5 + 5$, i.e. 11, seconds, hence fulfilling all the requirements of the problem. The actions that lead to this answer correspond to one application of rule unification ($[u]$), that has already been explained, and with each application of rule rewrite ($[r]$):

- in step (2) a `realToast` is taken from the bag and put in the `tray`,
- in step (4) the `realToast` passes from the `tray` to the `kitchen`,
- in steps (7) and (8) one side of the `realToast` cooks for some time z_1 that is added to the timer,
- in step (9) the `realToast` is flipped,
- in steps (10) and (11) the other side of the `realToast` cooks for some time z_2 that is added to the timer,
- in steps (13) and (14) the `realToast` becomes a well-cooked `realToast`, forcing $z_1 = z_2 = 5$, and taken out to the dish; one second is added to the timer.

7 Related work, conclusions and future work

A classic reference in equational conditional narrowing modulo is the work of Bockmayr [Boc93]. The topic is addressed here for Church-Rosser equational conditional term rewriting systems with empty axioms, but non terminating axioms, like ACU, supported in the current work are not allowed. The intimate relationship between rewriting and reachability problems was shown by Hullot [Hul80], where he proved that any normalized solution to a reachability problem could be lifted to a narrowing derivation that computed a more general solution.

Narrowing modulo order-sorted equational logics is covered by Meseguer and Thati [MT07], being currently used for cryptographic protocol analysis, but neither conditions are allowed in the rules of the rewrite theories nor constraint solvers are considered in this work.

The idea of constraint solving by narrowing in combined algebraic domains was presented by H. Kirchner and Ringeissen [KR94], where the supported theories had unconstrained equalities and the rewrite rules had constraints from an algebraic built-in structure, but no reachability subgoals.

Escobar, Sasse, and Meseguer [ESM12] have developed the concepts of variant and folding variant narrowing, a narrowing strategy for order-sorted unconditional rewrite theories that terminates on those theories having the *finite variant property*, but it has no counterpart for conditional rewrite theories and it does not allow the use of constraint solvers.

Foundations for order-sorted conditional rewriting have been published by Meseguer [Mes17]. Cholewa, Escobar, and Meseguer [CEM15] have defined a new hierarchical method, called layered constraint narrowing, to solve narrowing problems in order-sorted conditional equational theories, an approach similar to ours, and given new theoretical results on that matter, including the definition of constrained variants for order-sorted conditional rewrite theories, but with no specific support for SMT solvers.

In previous work [AMPP14, AMPP15], the relationship between verifiable and computable answers for reachability problems in rewrite theories with an underlying membership equational logic has been studied, presenting two correct and weakly complete narrowing calculi, the second being a refinement of the first one. In this second calculus only normalized terms, in a similar way to the reduction phase of Fribourg in the language SLOG [Fri85], were considered in order to find an answer to a reachability problem.

Order-sorted conditional rewriting with constraint solvers has been addressed by Rocha et al. [RMM17], where the only admitted conditions in the rules are quantifier-free SMT formulas. Also the only non-ground terms admitted in the reachability problems in this work are those whose variables have sorts belonging to the SMT sorts supported.

This work extends the admitted conditions in [RMM17] by allowing reachability subgoals in the rewrite rules and also all reachability goals, without restrictions regarding the variables in them, and making use of narrowing instead of rewriting as the method to solve the reachability problems. A narrowing calculus for conditional narrowing modulo $E_0 \cup B$ when E_0 is a subset of the theories handled by SMT solvers, B are the axioms not related to the algebraic data types handled by the SMT solvers, and the conditions in the rules in R are either rewrite conditions or quantifier-free SMT formulas, with no restrictions regarding the variables that appear in these rules, has been presented. The soundness and weak completeness of the calculus, as well as the completeness of the calculus for topmost rewrite theories have been proved. To the best of our knowledge, a similar calculus did not previously exist in the literature. The rewriting language Maude [CDE+07], which allows the use of reflection and SMT solvers, is being used as a framework to develop the prototype for the calculus.

During the development of the running example for this work it became clear that the formulation of a reachability problem where the time taken to fulfill the actions was a parameter of the problem, instead of a constant fixed in advance, was not easy. To solve this problem, the immediate work will consist of the extension of this narrowing calculus to support parameterized SMT constants in the rewrite rules, modifying the SMT algebraic data types. On future work, the development of a narrowing calculus for $E_0 \cup (E_1 \cup B)$ unification, where $E_1 \cup B$ is a non-SMT equational theory, and, on a later step, the development of a narrowing calculus that can deal with $R/(E_0 \cup E_1 \cup B)$ reachability problems will be addressed.

Acknowledgments. We want to thank the anonymous referees for their precise comments and remarks that have helped us to improve this work so much.

References

[AMPP14] Luis Aguirre, Narciso Martí-Oliet, Miguel Palomino, and Isabel Pita. Conditional narrowing modulo in rewriting logic and Maude. In Escobar [Esc14], pages 80–96.

[AMPP15] Luis Aguirre, Narciso Martí-Oliet, Miguel Palomino, and Isabel Pita. Sentence-normalized conditional narrowing modulo in rewriting logic and maude. In Narciso Martí-Oliet, Peter Csaba Ölveczky, and Carolyn L. Talcott, editors, *Logic, Rewriting, and Concurrency - Essays dedicated to José Meseguer on the Occasion of His 65th Birthday*, volume 9200 of *Lecture Notes in Computer Science*, pages 48–71. Springer, 2015.

[BM06] Roberto Bruni and José Meseguer. Semantic foundations for generalized rewrite theories. *Theoretical Computer Science*, 360(1-3):386–414, 2006.

[BM12] Kyungmin Bae and José Meseguer. Model checking LTLR formulas under localized fairness. In Francisco Durán, editor, *Rewriting Logic and Its Applications - 9th International Workshop, WRLA 2012, Held as a Satellite Event of ETAPS, Tallinn, Estonia, March 24-25, 2012, Revised Selected Papers*, volume 7571 of *Lecture Notes in Computer Science*, pages 99–117. Springer, 2012.

[BM14] Kyungmin Bae and José Meseguer. Infinite-state model checking of LTLR formulas using narrowing. In Escobar [Esc14], pages 113–129.

[Boc93] Alexander Bockmayr. Conditional narrowing modulo a set of equations. *Applicable Algebra in Engineering, Communication and Computing*, 4:147–168, 1993.

[CDE+07] Manuel Clavel, Francisco Durán, Steven Eker, Patrick Lincoln, Narciso Martí-Oliet, José Meseguer, and Carolyn Talcott. *All About Maude - A High-Performance Logical Framework: How to Specify, Program, and Verify Systems in Rewriting Logic*, volume 4350 of *Lecture Notes in Computer Science*. Springer, 2007.

[CEM15] Andrew Cholewa, Santiago Escobar, and José Meseguer. Constrained narrowing for conditional equational theories modulo axioms. *Sci. Comput. Program.*, 112:24–57, 2015.

[DLM+08] Francisco Durán, Salvador Lucas, Claude Marché, José Meseguer, and Xavier Urbain. Proving operational termination of membership equational programs. *Higher-Order and Symbolic Computation*, 21(1-2):59–88, 2008.

[DM12] Francisco Durán and José Meseguer. On the Church-Rosser and coherence properties of conditional order-sorted rewrite theories. *The Journal of Logic and Algebraic Programming*, 81(7-8):816–850, 2012.

[dMB08] Leonardo de Moura and Nikolaj Bjørner. Z3: an efficient SMT solver. In C. R. Ramakrishnan and Jakob Rehof, editors, *Tools and Algorithms for the Construction and Analysis of Systems, 14th International Conference, TACAS 2008, Held as Part of the Joint European Conferences on Theory and Practice of Software, ETAPS 2008, Budapest, Hungary, March 29-April 6, 2008. Proceedings*, volume 4963 of *Lecture Notes in Computer Science*, pages 337–340. Springer, 2008.

[EMM09] Santiago Escobar, Catherine Meadows, and José Meseguer. Maude-NPA: Cryptographic protocol analysis modulo equational properties. In Alessandro Aldini, Gilles Barthe, and Roberto Gorrieri, editors, *Foundations of Security Analysis and Design V*, volume 5705 of *Lecture Notes in Computer Science*, pages 1–50. Springer, 2009.

[Esc14] Santiago Escobar, editor. *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*. Springer, 2014.

[ESM12] Santiago Escobar, Ralf Sasse, and José Meseguer. Folding variant narrowing and optimal variant termination. *The Journal of Logic and Algebraic Programming*, 81(7-8):898–928, 2012.

[Fay79] M. Fay. First-order unification in an equational theory. In *Proc. 4th Workshop on Automated Deduction*, pages 161–167, Austin, TX, USA, 1979. Academic Press.

[Fri85] Laurent Fribourg. SLOG: A logic programming language interpreter based on clausal superposition and rewriting. In *Proceedings of the 1985 Symposium on Logic Programming, Boston, Massachusetts, USA, July 15-18, 1985*, pages 172–184. IEEE-CS, 1985.

[GK01] Jürgen Giesl and Deepak Kapur. Dependency pairs for equational rewriting. In Aart Middeldorp, editor, *Rewriting Techniques and Applications, 12th International Conference, RTA 2001, Utrecht, The Netherlands, May 22-24, 2001, Proceedings*, volume 2051 of *Lecture Notes in Computer Science*, pages 93–108. Springer, 2001.

[GM86] Elio Giovannetti and Corrado Moiso. A completeness result for e-unification algorithms based on conditional narrowing. In Mauro Boscarol, Luigia Carlucci Aiello, and Giorgio Levi, editors, *Foundations of Logic and Functional Programming, Workshop, Trento, Italy, December 15-19, 1986, Proceedings*, volume 306 of *Lecture Notes in Computer Science*, pages 157–167. Springer, 1986.

[Ham00] Mohamed Hamada. Strong completeness of a narrowing calculus for conditional rewrite systems with extra variables. *Electronic Notes in Theoretical Computer Science*, 31:89–103, 2000.

[Hul80] Jean-Marie Hullot. Canonical forms and unification. In Wolfgang Bibel and Robert A. Kowalski, editors, *5th Conference on Automated Deduction, Les Arcs, France, July 8-11, 1980, Proceedings*, volume 87 of *Lecture Notes in Computer Science*, pages 318–334. Springer, 1980.

[KR94] Hélène Kirchner and Christophe Ringeissen. Constraint solving by narrowing in combined algebraic domains. In Pascal Van Hentenryck, editor, *Logic Programming, Proceedings of the Eleventh International Conference on Logic Programming, Santa Marherita Ligure, Italy, June 13-18, 1994*, pages 617–631. MIT Press, 1994.

[LMM05] Salvador Lucas, Claude Marché, and José Meseguer. Operational termination of conditional term rewriting systems. *Information Processing Letters*, 95(4):446–453, 2005.

[Mes90] José Meseguer. Rewriting as a unified model of concurrency. In J.C.M. Baeten and J.W. Klop, editors, *CONCUR '90 Theories of Concurrency: Unification and Extension*, volume 458 of *Lecture Notes in Computer Science*, pages 384–400. Springer, 1990.

[Mes97] José Meseguer. Membership algebra as a logical framework for equational specification. In Francesco Parisi-Presicce, editor, *Recent Trends in Algebraic Development Techniques, 12th International Workshop, WADT'97, Tarquinia, Italy, June 1997, Selected Papers*, volume 1376 of *Lecture Notes in Computer Science*, pages 18–61. Springer, 1997.

[Mes12] José Meseguer. Twenty years of rewriting logic. *Journal of Logic and Algebraic Programming*, 81(7-8):721–781, 2012.

[Mes17] José Meseguer. Strict coherence of conditional rewriting modulo axioms. *Theor. Comput. Sci.*, 672(C):1–35, April 2017.

[MH94] Aart Middeldorp and Erik Hamoen. Completeness results for basic narrowing. *Applicable Algebra in Engineering, Communication and Computing*, 5:213–253, 1994.

[MM02] Narciso Martí-Oliet and José Meseguer. Rewriting logic: roadmap and bibliography. *Theoretical Computer Science*, 285(2):121–154, 2002.

[MT07] José Meseguer and Prasanna Thati. Symbolic reachability analysis using narrowing and its application to verification of cryptographic protocols. *Higher-Order and Symbolic Computation*, 20(1-2):123–160, 2007.

[Plo72] Gordon Plotkin. Building in equational theories. *Machine Intelligence 7*, pages 73–90, 1972.

[RMM17] Camilo Rocha, José Meseguer, and César A. Muñoz. Rewriting modulo SMT and open system analysis. *J. Log. Algebr. Meth. Program.*, 86(1):269–297, 2017.

A Appendix

This appendix holds the formulation of Corollary 2 in [Mes17], related to Lemma 3.

Let $\mathcal{R} = (\Sigma, B, R)$ be a conditional order-sorted rewrite theory, where B satisfies the assumptions stated at the beginning of Section 4 and is closed under B-extensions. Then,

for each instance of **Replacement** of the form

$$\frac{l_1\theta \to_{R,B} r_1\theta \cdots l_n\theta \to_{R,B} r_n\theta}{l \to^1_{R,B} r}$$

and each B-equality proof $l =_B l'$ there is another instance of **Replacement** of the form

$$\frac{l_1\theta' \to_{R,B} r_1\theta' \cdots l_n\theta' \to_{R,B} r_n\theta'}{l' \to^1_{R,B} r'}$$

with $r =_B r'$ and $x\theta = x\theta'$ for each x in $vars(\{l_i \to r_i\}_{i=1}^n)$

B Appendix

This appendix holds the rest of the proofs of this work.

Proposition 2. Let $\mathcal{R} = (\Sigma, E, R)$ be a rewrite theory with built-in subtheory (Σ_0, E_0), and t be a term in $\mathcal{H}_\Sigma(\mathcal{X})$, with $abstract_{\Sigma_1}(t) = \langle \lambda\bar{x}.t^\circ; \theta^\circ; \phi^\circ \rangle$. For any substitution σ such that $E_0 \vDash \phi^\circ\sigma$, it follows that $t^\circ\sigma =_E t\sigma$.

Proof. By definition $\theta^\circ = \{x^1_{\kappa_1} \mapsto t_1, \ldots, x^n_{\kappa_n} \mapsto t_n\}$, $\phi^\circ = \bigwedge_{i=1}^n x^i_{\kappa_i} = t_i$, $t = t[t_1]_{p_1} \cdots [t_n]_{p_n}$, and $t^\circ = t[x^1_{\kappa_1}]_{p_1} \cdots [x^n_{\kappa_n}]_{p_n}$. Also, as $E_0 \vDash \phi^\circ\sigma$ then $x^i_{\kappa_i}\sigma =_{E_0} t_i\sigma$, for $1 \leq i \leq n$, so $t^\circ\sigma = (t[x^1_{\kappa_1}]_{p_1} \cdots [x^n_{\kappa_n}]_{p_n})\sigma = t\sigma[x^1_{\kappa_1}\sigma]_{p_1} \cdots [x^n_{\kappa_n}\sigma]_{p_n} =_{E_0} t\sigma[t_1\sigma]_{p_1} \cdots [t_n\sigma]_{p_n} = (t[t_1]_{p_1} \cdots [t_n]_{p_n})\sigma = t\sigma$.

As the theory inclusion is protecting then also $t^\circ\sigma =_E t\sigma$.

Proposition 3. Let $\mathcal{R} = (\Sigma, E_0 \cup B, R)$ be a rewrite theory with built-in subtheory (Σ_0, E_0) and $\mathcal{R}^\circ = (\Sigma, E_0 \cup B, R^\circ)$ be its normal rewrite theory. Then $\to^1_{R,B} \subseteq \to^1_{R^\circ,B}$.

Proof. Let t be a term in $\mathcal{H}_\Sigma$, and $c = l \to r \ if \ \bigwedge_{i=1}^n l_i \to r_i \mid \phi$ be a rule in R such that $t \to^1_{R,B} t[r\sigma]_p$ using rule c at position p with substitution σ, so $t|_p = l\sigma$, $l_i\sigma \to_{R,B} r_i\sigma$, for $1 \leq i \leq n$, and $E_0 \vDash \phi\sigma$. R° has a rule $c^\circ = l^\circ \to r \ if \ \bigwedge_{i=1}^n l_i \to r_i \mid \phi \wedge \phi^\circ$, where $dom(\theta^\circ) \cap vars(c) = \emptyset$, $l = l^\circ\theta^\circ$, and $\phi^\circ\theta^\circ = \bigwedge_{j=1}^m (x_j\theta^\circ = x_j\theta^\circ)$.

The proof uses induction in the total number of $\to^1_{R,B}$ rewrite steps in the proof tree.

1. $t|_p = l\sigma = l^\circ\theta^\circ\sigma$. As $dom(\theta^\circ) \cap vars(c) = \emptyset$, then $l_i\theta^\circ = l_i$ and $r_i\theta^\circ = r_i$, for $1 \leq i \leq n$,
2. – Zero rewrite steps:
   for $1 \leq i \leq n$, $l_i\sigma \to_{R,B} r_i\sigma$ in zero rewrite steps, so $l_i\sigma =_E r_i\sigma$. Then $l_i\theta^\circ\sigma = l_i\sigma =_E r_i\sigma = r_i\theta^\circ\sigma$, i.e., $l_i\theta^\circ\sigma \to_{R^\circ,B} r_i\theta^\circ\sigma$.
   – Several rewrite steps:
   if $l_i\sigma \to_{R,B} r_i\sigma$ in zero rewrite steps then $l_i\theta^\circ\sigma \to_{R^\circ,B} r_i\theta^\circ\sigma$, as proved in the previous subcase, else $l_i\theta^\circ\sigma = l_i\sigma \to^1_{R,B} t_1 \to^1_{R,B} \cdots \to^1_{R,B} t_n =_E r_i\sigma = r_i\theta^\circ\sigma$. Then, by I.H., $l_i\theta^\circ\sigma \to^1_{R^\circ,B} t_1 \to^1_{R^\circ,B} \cdots \to^1_{R^\circ,B} t_n =_E r_i\theta^\circ\sigma$, i.e., $l_i\theta^\circ\sigma \to_{R^\circ,B} r_i\theta^\circ\sigma$.
3. $\phi\theta^\circ = \phi$, because $dom(\theta^\circ) \cap vars(c) = \emptyset$. As $E_0 \vDash \phi\sigma$ then $E_0 \vDash \phi\theta^\circ\sigma$, and
4. $\phi_i^\circ\theta^\circ\sigma = \bigwedge_{j=1}^{m_j}(x_i^j\theta_i^\circ\sigma = x_i^j\theta^\circ\sigma) = \bigwedge_{j=1}^{m_j}(x_i^j\theta^\circ\sigma = x_i^j\theta^\circ\sigma)$, for $0 \leq i \leq n$, so trivially $E_0 \vDash \phi_i^\circ\theta^\circ\sigma$. As also $E_0 \vDash \phi\theta^\circ\sigma$ then $E_0 \vDash (\phi \wedge \bigwedge_{i=0}^n \phi_i^\circ)\theta^\circ\sigma$.

Then $t \to^1_{R^\circ,B} t[r\theta^\circ\sigma]_p$ and, as $r\theta^\circ\sigma = r\sigma$ because $dom(\theta^\circ) \cap vars(c) = \emptyset$, also $t \to^1_{R^\circ,B} t[r\sigma]_p$, so $\to^1_{R,B} \subseteq \to^1_{R^\circ,B}$.

Proposition 4. Let $\mathcal{R} = (\Sigma, E_0 \cup B, R)$ be a rewrite theory with built-in subtheory (Σ_0, E_0). If t and t' are two terms in $\mathcal{H}_\Sigma(\mathcal{X})$ such that $t =_{E_0} t'$ then:

1. $top_{\Sigma_0}(t) = top_{\Sigma_0}(t')$,
2. $ls(t|_q) = ls(t'|_q)$ and $t|_q =_{E_0} t'|_q$ for all positions q in $top_{\Sigma_0}(t)$,
3. $t|_{q'} =_{E_0} t'|_{q'}$ for all positions q' such that $t|_{q'} \in \mathcal{H}_\Sigma(\mathcal{X})$, and
4. if $top_{\Sigma_0}(t) = \{q_1, \ldots, q_n\}$ then $t' = t[t'|_{q_1}]_{q_1} \cdots [t'|_{q_n}]_{q_n}$.

Proof. Immediate since either $t = t'$ and all invariants follow trivially, or induction can be used in combination with Proposition 10 below, since $t =_{E_0} t'$ can be seen as a series of one-step deductions $t \leftrightarrow_{E_0} t_1 \cdots \leftrightarrow_{E_0} t_n \cdots \leftrightarrow_{E_0} t'$ for suitable t_i, $1 \leq i \leq n$.

Proposition 10 (Invariants of top_{Σ_0} under E_0-deduction). *Let $\mathcal{R} = (\Sigma, E_0 \cup B, R)$ be a rewrite theory with built-in subtheory (Σ_0, E_0). If t and t' are two terms in $\mathcal{H}_\Sigma(\mathcal{X})$ such that $t \leftrightarrow_{E_0} t'$ then:*

1. *$top_{\Sigma_0}(t) = top_{\Sigma_0}(t')$,*
2. *$ls(t|_q) = ls(t'|_q)$ and $t|_q =_{E_0} t'|_q$ for all positions q in $top_{\Sigma_0}(t)$,*
3. *$t|_{q'} =_{E_0} t'|_{q'}$ for all positions q' such that $t|_{q'} \in \mathcal{H}_\Sigma(\mathcal{X})$, and*
4. *if $top_{\Sigma_0}(t) = \{q_1, \ldots, q_n\}$ then $t' = t[t'|_{q_1}]_{q_1} \cdots [t'|_{q_n}]_{q_n}$.*

Proof. As $t \in \mathcal{H}_\Sigma(\mathcal{X})$ and $t|_p \in \mathcal{T}_{\Sigma_0}(\mathcal{X}_0)$, there must exist a position p' in $top_{\Sigma_0}(t)$ such that $p' \leq p$, so $p = p'.r$ for suitable r. The first two points are proved simultaneously.

1. and (2) As p' in $top_{\Sigma_0}(t)$, then $p' = p''.i$ for suitable position p'' and natural number i, and $t|_{p''} \in \mathcal{H}_\Sigma(\mathcal{X})$, so $t' = t[w\sigma]_{p'.r} = t[w\sigma]_{p''.i.r}$. If q in $top_{\Sigma_0}(t)$ and $q \neq p'$ then neither $q \leq p'$ nor $p' \leq q$, so $t|_q$ is unaffected by the E_0-deduction step. Then $t|_q = t'|_q$, hence $ls(t|_q) = ls(t'|_q)$ and $t|_q =_{E_0} t'|_q$, so q in $top_{\Sigma_0}(t')$.
   For $top_{\Sigma_0}(t)$ and $top_{\Sigma_0}(t')$ to be equal it must be proved that $p' \in top_{\Sigma_0}(t')$. As (Σ_0, E_0) is many-sorted then $ls(v\sigma) = ls(w\sigma)$, so we are replacing in $t|_{p'}$ the subterm $t|_{p'.r}$, having the value $v\sigma$, with the subterm $w\sigma$ both of them with the same sort, so also $t|_{p'}$ and $t|_{p'}[w\sigma]_r$ have the same sort in S_0. As $t|_{p''} = (t[v\sigma]_{p''.i.r})|_{p''} \in \mathcal{H}_\Sigma(\mathcal{X})$, and $v\sigma$ and $w\sigma$ have the same sort then also $(t[w\sigma]_{p''.i.r})|_{p''} \in \mathcal{H}_\Sigma(\mathcal{X})$, so $p' \in top_{\Sigma_0}(t')$. As $t \leftrightarrow_{E_0} t[w\sigma]_p = t'$ and $p = p'.r$, then $t'|_{p'} = t|_{p'}[w\sigma]_r$ and $t|_{p'} \leftrightarrow_{E_0} t|_{p'}[w\sigma]_r = t'|_{p'}$, so $t|_{p'} =_{E_0} t'|_{p'}$.
3. If q' is a position such that $t|_{q'} \in \mathcal{H}_\Sigma(\mathcal{X})$ then:
   - $p' \not\leq q'$, because as p' in $top_{\Sigma_0}(t)$ if $p' \leq q'$ then $t|_{q'} \in \mathcal{T}_{\Sigma_0}(\mathcal{X}_0)$, in contradiction with $t|_{q'} \in \mathcal{H}_\Sigma(\mathcal{X})$,
   - if $q' = p'$ then $t|_{q'} = t'|_{q'}$, so $t|_{q'} =_{E_0} t'|_{q'}$, and
   - if $q' < p'$ then $p' = q'.r'$, for suitable position r', so $p = p'.r = q'.r'.r$. As $t' = t[w\sigma]_p$ then $t'|_{q'} = t|_{q'}[w\sigma]_{r'.r}$, and as $t|_p = t|_{q'.r'.r} = v\sigma$, then $t|_{q'} = t|_{q'}[v\sigma]_{r'.r}$, so $t|_{q'} \leftrightarrow_{E_0} t'|_{q'}$ with the same equation c and substitution σ at position $r'.r$, and $t|_{q'} =_{E_0} t'|_{q'}$.
4. As p' in $top_{\Sigma_0}(t)$, without loss of generality take $p' = q_1$, so $t'|_{q_j} = t|_{q_j}$, for $2 \leq j \leq n$. $t' = t[w\sigma]_{p'.r} = t[w\sigma]_{q_1.r} = t[t|_{q_1}[w\sigma]_r]_{q_1}$. As $t'|_{q_1.r} = w\sigma$ then $t'|_{q_1} = t|_{q_1}[w\sigma]_r$, so $t' = t[t'|_{q_1}]_{q_1}$. As $t = t[t|_{q_1}]_{q_1}[t|_{q_2}]_{q_2} \cdots [t|_{q_n}]_{q_n} = t[t|_{q_1}]_{q_1}[t'|_{q_2}]_{q_2} \cdots [t'|_{q_n}]_{q_n}$ and $t' = t[t'|_{q_1}]_{q_1}$, then $t' = (t[t|_{q_1}]_{q_1}[t'|_{q_2}]_{q_2} \cdots [t'|_{q_n}]_{q_n})[t'|_{q_1}]_{q_1} = t[t'|_{q_1}]_{q_1}[t'|_{q_2}]_{q_2} \cdots [t'|_{q_n}]_{q_n}$.

Proposition 5. Let $\mathcal{R} = (\Sigma, E_0 \cup B, R)$ be a rewrite theory with built-in subtheory (Σ_0, E_0). If t is a term in $\mathcal{H}_\Sigma(\mathcal{X})$, $abstract_{\Sigma_1}(t, \mathcal{Y}) = \langle \lambda \bar{x}.t^\circ; \theta^\circ; \phi^\circ \rangle$, where $\bar{x} = \{x_1, \ldots, x_n\}$ and $t^\circ = t[x_1]_{q_1} \cdots [x_n]_{q_n}$, then (i) $top_{\Sigma_0}(t) = \{q_1, , q_n\}$, and (ii) for every substitution $\sigma : \bar{x} \to \mathcal{T}_{\Sigma_0}(\mathcal{X}_0)$ it holds that $top_{\Sigma_0}(t^\circ\sigma) = top_{\Sigma_0}(t)$.

Proof. By definition of $abstract_{\Sigma_1}$, $t^\circ\theta^\circ = t$, $vars(t^\circ) \cap \mathcal{X}_0 = \bar{x}$, t° in$\mathcal{T}_{\Sigma_1}(\mathcal{X})$, $t|_{q_i}$ in $\mathcal{T}_{\Sigma_0}(\mathcal{X}_0)$, and $x_i\theta^\circ = t|_{q_i}$, for $1 \leq i \leq n$. (i) - $top_{\Sigma_0}(t) = \{q_1, \ldots, q_n\}$.

1. $\{q_1, \ldots, q_n\} \subseteq top_{\Sigma_0}(t)$.
   For $1 \leq i \leq n$, as t in $\mathcal{H}_\Sigma(\mathcal{X})$ and $t|_{q_i}$ in $\mathcal{T}_{\Sigma_0}(\mathcal{X}_0)$, then $q_i \neq \epsilon$, so $q_i = q_i'.j_i$, for suitable position q_i' and integer j_i. As $t^\circ = t[x_1]_{q_1} \cdots [x_n]_{q_n} \in \mathcal{T}_{\Sigma_1}(\mathcal{X})$ and $q_i' < q_i$, then $t^\circ|_{q_i'}$ is a term in $\mathcal{T}_{\Sigma_1}(\mathcal{X})$. Now, as $\theta^\circ : \bar{x} \to \mathcal{T}_{\Sigma_0}(\mathcal{X}_0)$ then $t^\circ|_{q_i'}\theta^\circ$ is a term in $\mathcal{H}_\Sigma(\mathcal{X})$. But $t^\circ|_{q_i'}\theta^\circ = t^\circ\theta^\circ|_{q_i'} = t|_{q_i'}$, so $t|_{q_i'}$ in $\mathcal{H}_\Sigma(\mathcal{X})$, and q_i in $top_{\Sigma_0}(t)$.
2. $top_{\Sigma_0}(t) \subseteq \{q_1, \ldots, q_n\}$.
   Let p be a position in $top_{\Sigma_0}(t)$. By definition $t|_p$ in $\mathcal{T}_{\Sigma_0}(\mathcal{X}_0)$ and $t = t[t|_p]_p$.
   (a) If for $1 \leq i \leq n$, $p \not\leq q_i$ and $q_i \not\leq p$ then $t^\circ = t[x_1]_{q_1} \cdots [x_n]_{q_n} = t[t|_p]_p[x_1]_{q_1} \cdots [x_n]_{q_n}$. As $t|_p$ in $\mathcal{T}_{\Sigma_0}(\mathcal{X}_0)$ then either t° is not a term in $\mathcal{T}_{\Sigma_1}(\mathcal{X})$ or $vars(t^\circ) \cap \mathcal{X}_0 \neq \bar{x}$, both in contradiction with t° being an abstraction.
   (b) If $q_i < p$ for some $1 \leq i \leq n$, then $p = q_i.q_i'.j_i$ for suitable (possibly empty) position q_i' and integer j_i. As $x_i\theta^\circ = t|_{q_i} \in \mathcal{T}_{\Sigma_0}(\mathcal{X}_0)$ then $t|_{q_i.q_i'} \in \mathcal{T}_{\Sigma_0}(\mathcal{X}_0)$ so $p = q_i.q_i'.j_i$ is not a position in $top_{\Sigma_0}(t)$.
   (c) If $Q = \{q_i \mid q_i \in \{q_1, \ldots, q_n\} \wedge p < q_i\}$ is non-empty, so $Q = \{q_{i_1}, \ldots, q_{i_m}\}$, then $q_{i_j} = p.q_{i_j}'$, for suitable $q_{i_j}' \neq \epsilon$, for $1 \leq j \leq m$. As $t|_p$ in $\mathcal{T}_{\Sigma_0}(\mathcal{X}_0)$ then $t^\circ|_p = t|_p[x_{i_1}]_{q_{i_1}'} \cdots [x_{i_m}]_{q_{i_m}}$ is a term in $\mathcal{T}_{\Sigma_0}(\mathcal{X}_0) \setminus \mathcal{X}_0$, so t° is not a term in $\mathcal{T}_{\Sigma_1}(\mathcal{X})$.
   The only possibility left is $p = q_i$ for some $1 \leq i \leq n$, so $p \in \{q_1, \ldots, q_n\}$.

(*ii*) - If $\sigma : \bar{x} \to \mathcal{T}_{\Sigma_0}(\mathcal{X}_0)$ then $top_{\Sigma_0}(t^\circ\sigma) = top_{\Sigma_0}(t)$.

1. $top_{\Sigma_0}(t^\circ\sigma) \subseteq top_{\Sigma_0}(t)$
   For $1 \leq i \leq n$, $x_i\sigma \in \mathcal{T}_{\Sigma_0}(\mathcal{X}_0)$. As $vars(t^\circ) \cap \mathcal{X}_0 = \bar{x}$ and $t^\circ|_p \in \mathcal{T}_{\Sigma_1}(\mathcal{X}) \setminus \mathcal{X}_0$ if $p \in Pos(t^\circ) \setminus \{q_1, \ldots, q_n\}$, then if $q \in top_{\Sigma_0}(t^\circ\sigma)$ there must exist some i, with $1 \leq i \leq n$, such that $q_i \leq q$. But as $t^\circ\sigma|_{q_i} = x_i\sigma \in \mathcal{T}_{\Sigma_0}(\mathcal{X}_0)$ then $q_i \not< q$, so $q_i = q$ and $q \in top_{\Sigma_0}(t)$.
2. $top_{\Sigma_0}(t) \subseteq top_{\Sigma_0}(t^\circ\sigma)$
   $top_{\Sigma_0}(t) = \{q_i\}_{i=1}^n$. For $1 \leq i \leq n$ there exists a position q_i' and an integer j_i such that $q_i = q_i'.j_i$; also as $x_i\sigma \in \mathcal{T}_{\Sigma_0}(\mathcal{X}_0)$ then $(t^\circ\sigma)|_{q_i} = x_i\sigma \in \mathcal{T}_{\Sigma_0}(\mathcal{X}_0)$. Let $\{q_{i_1}, \ldots, q_{i_m}\} = \{q_j \mid q_i' < q_j, 1 \leq j \leq n\}$. Then $q_{i_k} = q_i'.p_{i_k}$ for suitable $p_{i_k} \neq \epsilon$, for $1 \leq k \leq m$, so $t|_{q_i'} = t|_{q_i'}[t|_{q_{i_1}}]_{p_{i_1}} \cdots [t|_{q_{i_m}}]_{p_{i_m}}$ and, as $t^\circ|_{q_i'} = t|_{q_i'}[x_{i_1}]_{p_{i_1}} \cdots [x_{i_m}]_{p_{i_m}}$, then $t^\circ\sigma|_{q_i'} = t|_{q_i'}[x_{i_1}\sigma]_{p_{i_1}} \cdots [x_{i_m}\sigma]_{p_{i_m}}$. Σ_0 is many sorted, σ is well-formed, and $ls(x_{i_k}) = ls(t|_{q_{i_k}})$ by definition of $abstract_{\Sigma_1}$, so $ls(x_{i_k}\sigma) = ls(x_{i_k}) = ls(t|_{q_{i_k}})$, for $1 \leq k \leq m$. Then $ls(t|_{q_i'}) = ls(t^\circ\sigma|_{q_i'})$, so $t^\circ\sigma|_{q_i'} \in \mathcal{T}_{\Sigma_1}(\mathcal{X})$ and $q_i \in top_{\Sigma_0}(t^\circ\sigma)$.

Lemma 2. Let $\mathcal{R} = (\Sigma, E_0 \cup B, R)$ be a rewrite theory with built-in subtheory (Σ_0, E_0) and $\mathcal{R}^\circ = (\Sigma, E_0 \cup B, R^\circ)$ its normal rewrite theory. If t, u, and v are terms in $\mathcal{H}_\Sigma$, $t =_{E_0} u$, and $u \to^1_{R^\circ,B} v$ then there exists a term w in $\mathcal{H}_\Sigma$ such that $t \to^1_{R^\circ,B} w$ and $w =_{E_0} v$.

Proof. As $u \to^1_{R^\circ,B} v$, there are rules $c = l \to r$ *if* $\bigwedge_{i=1}^m l_i \to r_i \mid \phi$ in R and $c^\circ = l^\circ \to r$ *if* $\bigwedge_{i=1}^m l_i \to r_i \mid \phi \wedge \phi^\circ$ in R°, a position p in $Pos(u)$, and a substitution $\sigma : vars(c^\circ) \to \mathcal{T}_\Sigma$ such that $u|_p = l^\circ\sigma$, $l_i\sigma \to_{R,B} r_i\sigma$, for $1 \leq i \leq m$, and $E_0 \vDash (\phi \wedge \phi^\circ)\sigma$, so $v = u[r\sigma]_p$. Also $u|_p$ in $\mathcal{H}_\Sigma$ because l° in $\mathcal{T}_{\Sigma_1}(\mathcal{X})$ so, by Proposition 4, $t|_p =_{E_0} u|_p = l^\circ\sigma$. Let $w = t[r\sigma]_p$.

$u|_p = l^\circ\sigma$ has the form $l\sigma[x_1\sigma]_{q_1} \cdots [x_n\sigma]_{q_n}$ so, by Proposition 5, $top_{\Sigma_0}(u|_p) = top_{\Sigma_0}(l^\circ\sigma) = \{q_1, \ldots, q_n\}$. As $t|_p =_{E_0} u|_p$ then, again by Proposition 4, $top_{\Sigma_0}(t|_p) = \{q_1, \ldots, q_n\}$, $t|_p = u[t|_{p.q_1}]_{q_1} \cdots [t|_{p.q_n}]_{q_n}$, and $t|_{p.q_i} =_{E_0} u|_{p.q_i}$, for $1 \leq i \leq n$. Let $\bar{x} = \{x_1, \ldots, x_n\}$ and let $\sigma' = \sigma_{dom(\sigma) \setminus \bar{x}} \cup \bigcup_{j=1}^n \{x_j \mapsto t|_{p.q_j}\}$.

As $u|_p = l^\circ\sigma = l\sigma[x_1\sigma]_{q_1} \cdots [x_n\sigma]_{q_n}$, then it holds that $l^\circ\sigma' = l\sigma[x_1\sigma']_{q_1} \cdots [x_n\sigma']_{q_n} = u|_p[t|_{p.q_1}]_{q_1} \cdots [t|_{p.q_n}]_{q_n} = t|_p$. Also, as $vars(c) \cap \bar{x} = \emptyset$, $r\sigma' = r\sigma$, $l_i\sigma' = l_i\sigma$, $r_i\sigma' = r_i\sigma$, for $1 \leq i \leq m$, and $\phi\sigma' = \phi\sigma$, then $l_i\sigma' = l_i\sigma \to_{R,B} r_i\sigma = r_i\sigma'$, for $1 \leq i \leq m$, and $E_0 \vDash \phi\sigma'$.

$E_0 \vDash \phi^\circ\sigma$, where $\phi^\circ\sigma = \bigwedge_{j=1}^n ((x_j\sigma = l|_{q_j}\sigma) = \bigwedge_{j=1}^n ((u|_{p.q_j}\sigma = l|_{q_j}\sigma)$. As $\phi^\circ\sigma' = \bigwedge_{j=1}^n ((x_j\sigma' = l|_{q_j}\sigma') = \bigwedge_{j=1}^n (t|_{p.q_j} = l|_{q_j}\sigma)$ and $t|_{p.q_i} =_{E_0} u|_{p.q_i}$, for $1 \leq i \leq n$, then $E_0 \vDash \phi^\circ\sigma'$, so $E_0 \vDash (\phi \wedge \phi^\circ)\sigma'$ and $t \to^1_{R^\circ,B} t[r\sigma]_p = w$. As $t =_{E_0} u$ then $t[r\sigma]_p =_{E_0} u[r\sigma]_p$, i.e., $v =_{E_0} w$.

Proposition 6. Let $\mathcal{R} = (\Sigma, E_0 \cup B, R)$ be a rewrite theory with built-in subtheory (Σ_0, E_0). If t_0, t_1, and t_2 are terms in $\mathcal{H}_\Sigma(\mathcal{X})$ such that $t_0 \leftrightarrow_{E_0} t_1 \leftrightarrow_B t_2$ then there exists a term t_1' in $\mathcal{H}_\Sigma(\mathcal{X})$ such that $t_0 \leftrightarrow_B t_1' \leftrightarrow_{E_0} t_2$.

Proof. By Proposition 10, $top_{\Sigma_0}(t_0) = top_{\Sigma_0}(t_1)$. The one-step E_0-deduction $t_0 \leftrightarrow_{E_0} t_1$ is performed at some position p of the term t_0 with a Σ_0-sentence $v_0 = w_0$ *if* C in $E_0 \cup E_0^{-1}$, and substitution σ_0, so $t_0|_p$ in $\mathcal{T}_{\Sigma_0}$. Let $q = top_{\Sigma_0}(t_0, p)$. Then $p = q.q'$, for suitable q', $t_0 = t_0[v_0\sigma_0]_{q.q'}$, and $t_1 = t_0[w_0\sigma_0]_{q.q'}$.

The one-step B-deduction $t_1 \leftrightarrow_B t_2$ uses a regular Σ_1-equation $v = w$ and a substitution σ at some position r of t_1, so $t_1|_r$ in $\mathcal{H}_\Sigma(\mathcal{X})$ and $t_1|_r = v\sigma$. Let $vars(v) \cap \mathcal{X}_0 = \{x_1, \ldots, x_m\}$. As B is regular then $vars(w) \cap \mathcal{X}_0 = vars(v) \cap \mathcal{X}_0$. For $0 \leq i \leq m$, as B is linear, let r_i be the position of the variable x_i in v and let s_i be the position of the variable x_i in w. As v in $\mathcal{T}_{\Sigma_1}(\mathcal{X})$, so there are no function symbols from Σ_0, then there exists a position r_i' and a natural number j_i such that $r_i = r_i'.j_i$, $v|_{r_i}$ in $\mathcal{X}_0 \subseteq \mathcal{T}_{\Sigma_0}(\mathcal{X}_0)$, and $v|_{r_i'}$ in $\mathcal{H}_\Sigma(\mathcal{X})$, so r_i in $top_{\Sigma_0}(v)$.

As all Σ_0-subterms of $t_1|_r$ must be matched with the term v through the variables $\{x_1, \ldots, x_m\}$, then $top_{\Sigma_0}(t_1|_r) = \{r_1, \ldots, r_m\}$, and $v\sigma|_{r_i} = t_1|_{r.r_i}$ is a topmost Σ_0-subterm of t_1, that is moved to position $r.s_i$ in t_2.

There are three cases to consider regarding the relative position of p and r:

1. $p \not\leq r$ because:
   (a) if $p = r$ then $t_1|_p$ is both a term in $\mathcal{T}_{\Sigma_0}$ and in $\mathcal{H}_\Sigma$, a contradiction, and
   (b) if $p < r$ then $r = p.p'$, for suitable $p' \neq \epsilon$, and $t_1|_p$ is a term in $\mathcal{T}_{\Sigma_0}$ that has a subterm in $\mathcal{H}_\Sigma$ at position p', in contradiction with (Σ_0, E_0) being a subsignature of (Σ, E).
2. If $p \not\leq r$ and $r \not\leq p$ then both one-step deductions are independent and $t_2 = (t_0[w_0\sigma_0]_p)[w\sigma]_r = (t_0[w\sigma]_r)[w_0\sigma_0]_p$. Applying the one-step B-deduction before the one-step E_0-deduction yields $t_1' = t_0[w\sigma]_r$.
3. If $r < p$, as $p = q.q'$ and $top_{\Sigma_0}(t_0) = top_{\Sigma_0}(t_1)$, then $t_1|_q \in \mathcal{T}_{\Sigma_0}$, $t_0|_r \in \mathcal{T}_{\Sigma_1}$, and (Σ_0, E_0) is a subsignature of (Σ, E), then $q < r$, so $q = r.r_l$, for some $r_l \in top_{\Sigma_0}(t_0|_r)$, because q is a topmost E_0-position of t_0 and t_1, and $t_0 = t_0[v_0\sigma_0]_{r.r_l.q'}$. As both one-step deductions take place below position r, let $t_0|_r = t'$ for simplicity of notation. Then $t' = t'[v_0\sigma_0]_{r_l.q'} \leftrightarrow_{E_0} t'[w_0\sigma_0]_{r_l.q'} = t'[t'|_{r_l}[w_0\sigma_0]_{q'}]_{r_l} = v\sigma \leftrightarrow_B w\sigma = w\sigma[t'|_{r_l}[w_0\sigma_0]_{q'}]_{s_l}$, where $v|_{r_l} = x_l$ and $x_l\sigma = t'|_{r_l}[w_0\sigma_0]_{q'}$, so $t_2 = t_0[w\sigma[t'|_{r_l}[w_0\sigma_0]_{q'}]_{s_l}]_r$.
   Let $\sigma' = \sigma_{dom(\sigma)\setminus x_l \cup \{x_l \mapsto t'|_{r_l}\}}$. As v is linear and $r_l \leq r_l.q'$ then $v\sigma' = (t'[w_0\sigma_0]_{r_l.q'})[t'|_{r_l}]_{r_l} = t'$. But $t' = t'[v_0\sigma_0]_{r_l.q'}$, so $t'[v_0\sigma_0]_{r_l.q'} = t' = v\sigma' \leftrightarrow_B w\sigma' = w\sigma[t'|_{r_l}]_{s_l} = w\sigma[t_0|_{r.r_l}]_{s_l}$. As $(w\sigma[t'|_{r_l}]_{s_l})|_{s_l.q'} = t'|_{r_l.q'}$ then $w\sigma[t'|_{r_l}]_{s_l} \leftrightarrow_{E_0} (w\sigma[t'|_{r_l}]_{s_l})[w_0\sigma_0]_{s_l.q'} = w\sigma[t'|_{r_l}[w_0\sigma_0]_{q'}]_{s_l}$. In conclusion, $t' \leftrightarrow_B w\sigma[t'|_{r_l}]_{s_l} \leftrightarrow_{E_0} w\sigma[t'|_{r_l}[w_0\sigma_0]_{q'}]_{s_l}$. Then, take $t_1' = t_0[w\sigma[t'|_{r_l}]_{s_l}]_r = t_0[w\sigma[t_0|_{r.r_l}]_{s_l}]_r$, so $t_0 = t_0[t']_r \leftrightarrow_B t_0[w\sigma[t'|_{r_l}]_{s_l}]_r = t_1' \leftrightarrow_{E_0} t_0[w\sigma[t'|_{r_l}[w_0\sigma_0]_{q'}]_{s_l}]_r = t_2$.

Proposition 7. Let $\mathcal{R} = (\Sigma, E_0 \cup B, R)$ be a rewrite theory with built-in subtheory (Σ_0, E_0). If $\{t_0, \ldots, t_{n+1}\}$ is a set of terms in $\mathcal{H}_\Sigma(\mathcal{X})$ such that $t_0 \leftrightarrow_{E_0} t_1 \leftrightarrow_{E_0} \cdots \leftrightarrow_{E_0} t_{n-1} \leftrightarrow_B t_n$ then there exists a set of terms $\{t_1', \ldots, t_{n-1}'\}$ in $\mathcal{H}_\Sigma(\mathcal{X})$ such that $t_0 \leftrightarrow_B t_1' \leftrightarrow_{E_0} \cdots \leftrightarrow_{E_0} t_{n-1}' \leftrightarrow_{E_0} t_n$.

Proof. By induction in n.

- Base case, $n = 2$. $t_0 \leftrightarrow_{E_0} t_1 \leftrightarrow_B t_2$, so by Proposition 6 there exists a term t_1' in $\mathcal{H}_\Sigma(\mathcal{X})$ such that $t_0 \leftrightarrow_B t_1' \leftrightarrow_{E_0} t_2$.
- Induction case. As $t_1 \leftrightarrow_{E_0} \cdots \leftrightarrow_{E_0} t_{n-1} \leftrightarrow_B t_n$, by I.H., there exists a set of terms $\{t_2', \ldots, t_{n-1}'\}$ in $\mathcal{H}_\Sigma(\mathcal{X})$ such that $t_1 \leftrightarrow_B t_2' \leftrightarrow_{E_0} \cdots \leftrightarrow_{E_0} t_{n-1}' \leftrightarrow_{E_0} t_n$, so $t_0 \leftrightarrow_{E_0} t_1 \leftrightarrow_B t_2' \leftrightarrow_{E_0} \cdots \leftrightarrow_{E_0} t_{n-1}' \leftrightarrow_{E_0} t_n$. By Proposition 6, as $t_0 \leftrightarrow_{E_0} t_1 \leftrightarrow_B t_2'$, there exists t_1' in $\mathcal{H}_\Sigma(\mathcal{X})$ such that $t_0 \leftrightarrow_B t_1' \leftrightarrow_{E_0} t_2'$, and $t_0 \leftrightarrow_B t_1' \leftrightarrow_{E_0} \cdots \leftrightarrow_{E_0} t_{n-1}' \leftrightarrow_{E_0} t_n$.

Proposition 8. Let $\mathcal{R} = (\Sigma, E, R)$ be a rewrite theory with built-in subtheory (Σ_0, E_0), and $\mathcal{R}^\circ = (\Sigma, E_0 \cup B, R^\circ)$ its normal rewrite theory. If t and t'' are terms in $\mathcal{H}_\Sigma(\mathcal{X})$ and $t =_E t''$ then there exists a term t' in $\mathcal{H}_\Sigma(\mathcal{X})$ such that $t =_B t' =_{E_0} t''$.

Proof. By induction in the number of applications of axioms in B.

- Base case: zero B-axioms. Then $t =_{E_0} t''$. Take $t' = t$, so $t =_B t' =_{E_0} t''$.
- Induction case. There are two cases to consider depending on the position of the first $\leftrightarrow_B$ step.
  - If $t \leftrightarrow_B t_1 \leftrightarrow_E \cdots \leftrightarrow_E t''$, by I.H., there exists a term t' in $\mathcal{H}_\Sigma(\mathcal{X})$ such that $t_1 =_B t' =_{E_0} t''$, so $t \leftrightarrow_B t_1 =_B t' =_{E_0} t''$, i.e., $t =_B t' =_{E_0} t''$.
  - $t \leftrightarrow_{E_0} \cdots \leftrightarrow_{E_0} t_{j-1} \leftrightarrow_B t_j \leftrightarrow_E \cdots \leftrightarrow_E t''$. By Proposition 7, as $t \leftrightarrow_{E_0} \cdots \leftrightarrow_{E_0} t_{j-1} \leftrightarrow_B t_j$, there exists a set $\{t'_1, \ldots, t'_{j-1}\}$ in $\mathcal{H}_\Sigma(\mathcal{X})$ such that $t \leftrightarrow_B t'_1 \leftrightarrow_{E_0} \cdots \leftrightarrow_{E_0} t'_{j-1} \leftrightarrow_{E_0} t_j$. Then, by I.H., in $t'_1 \leftrightarrow_{E_0} \cdots \leftrightarrow_{E_0} t'_{j-1} \leftrightarrow_{E_0} t_j \cdots \leftrightarrow_E t_n \cdots \leftrightarrow_E t''$, there exists a term t' in $\mathcal{H}_\Sigma(\mathcal{X})$ such that $t'_1 =_B t' =_{E_0} t''$, so $t \leftrightarrow_B t'_1 =_B t' =_{E_0} t''$, i.e., $t =_B t' =_{E_0} t''$.

Theorem 1. Let $\mathcal{R} = (\Sigma, E_0 \cup B, R)$ be a rewrite theory with built-in subtheory (Σ_0, E_0), and $\mathcal{R}^\circ = (\Sigma, E_0 \cup B, R^\circ)$ its normal rewrite theory. If $\mathcal{R}^\circ$ is closed under B-extensions then $\rightarrow^1_{R^\circ,B} = \rightarrow^1_{R/E}$ and $\rightarrow_{R^\circ,B} = \rightarrow_{R/E}$.

Proof. There is a special case to consider when there are no rewrite steps involved in the deductions.
(i) $\rightarrow^1_{R^\circ,B} \subseteq \rightarrow^1_{R/E}$ and $\rightarrow_{R^\circ,B} \subseteq \rightarrow_{R/E}$.

In the special case, $t \rightarrow_{R^\circ,B} v$ with no rewrite steps. As $\rightarrow_{R^\circ,B} = (\rightarrow^*_{R^\circ,B}; =_E)$ then $t =_E v$, so $t \rightarrow_{R/E} v$. The other cases are proved using induction in the total number of $\rightarrow^1_{R^\circ,B}$ rewrite steps in the proof tree.

- Base case:
  $t \rightarrow^1_{R^\circ,B} w =_E v$ with only one $\rightarrow^1_{R^\circ,B}$ rewrite step in the proof tree, so there are rules $c = l \rightarrow r$ *if* $\bigwedge_{i=1}^m l_i \rightarrow r_i \mid \phi$ in R and $c^\circ = l^\circ \rightarrow r$ *if* $\bigwedge_{i=1}^m l_i \rightarrow r_i \mid \phi \wedge \phi^\circ$ in R°, a position p in $Pos(t)$, and a substitution σ such that $t|_p =_B l^\circ\sigma$, $l_i\sigma =_E r_i\sigma$, for $1 \leq i \leq m$, and $E_0 \vDash (\phi \wedge \phi^\circ)\sigma$, so $w = t[r\sigma]_p$. l° has the form $l[x_1]_{q_1} \cdots [x_n]_{q_n}$, and $t|_p[t|_{p.q_1}]_{q_1} \cdots [t|_{p.q_n}]_{q_n} = t|_p =_B l^\circ\sigma = l\sigma[x_1\sigma]_{q_1} \cdots [x_n\sigma]_{q_n}$.
  As $\phi^\circ = \bigwedge_{j=1}^n (x_j = l|_{q_j})$ and $E_0 \vDash \phi^\circ\sigma$ then $x_j\sigma =_E l\sigma|_{q_j}$, for $1 \leq j \leq n$, so $l\sigma = l\sigma[l\sigma|_{q_1}]_{q_1} \cdots [\sigma_{q_n}]_{q_n} =_E l\sigma[x_1\sigma]_{q_1} \cdots [x_n\sigma]_{q_n} =_B t|_p$. As $=_B \subseteq =_E$, then $l\sigma =_E t|_p$.
  As $t|_p =_E l\sigma$ and $l_i\sigma =_E r_i\sigma$, for $1 \leq i \leq m$, then $t = t[t|_p]_p =_E t[l\sigma]_p \rightarrow^1_R t[r\sigma]_p = w =_E v$ with rule c in R, that is, $t \rightarrow^1_{R/E} v$, so $t \rightarrow_{R/E} v$.
- Induction case:
  there are two subcases to consider:
  1. $t \rightarrow^1_{R^\circ,B} w =_E v$ with several $\rightarrow^1_{R^\circ,B}$ rewrite steps in the derivation. As in the base case, there are rules $c = l \rightarrow r$ *if* $\bigwedge_{i=1}^m l_i \rightarrow r_i \mid \phi$ in R and $c^\circ = l^\circ \rightarrow r$ *if* $\bigwedge_{i=1}^m l_i \rightarrow r_i \mid \phi \wedge \phi^\circ$ in R°, a position p in $Pos(t)$, and a substitution σ such that $t|_p = l^\circ\sigma$, $l_i\sigma \rightarrow_{R^\circ,B} r_i\sigma$, for $1 \leq i \leq m$, and $E_0 \vDash (\phi \wedge \bigwedge_{i=0}^m \phi_i^\circ)\sigma$, so $w = t[r\sigma]_p$.
     By induction hypothesis $l_i\sigma \rightarrow_{R/E} r_i\sigma$, for $1 \leq i \leq m$. As in the base case, $E_0 \vDash \phi\sigma$ and $t|_p =_E l\sigma$, so $t = t[t|_p]_p =_E t[l\sigma]_p \rightarrow^1_R t[r\sigma]_p = w =_E v$, i.e., $t \rightarrow^1_{R/E} v$ and, also, $t \rightarrow^1_{R/E} w =_E v$, i.e., $t \rightarrow_{R/E} v$.
  2. $t \rightarrow^1_{R^\circ,B} u \rightarrow^+_{R^\circ,B} w =_E v$. By the previous subcase $t \rightarrow^1_{R/E} u \rightarrow^+_{R^\circ,B} w =_E v$, and, by I.H., $t \rightarrow^1_{R/E} u \rightarrow^+_{R/E} w =_E v$, i.e., $t \rightarrow^*_{R/E} w =_E v$, or $t \rightarrow_{R/E} v$.

(*ii*) $\rightarrow^1_{R/E} \subseteq \rightarrow^1_{R^\circ,B}$ and $\rightarrow_{R/E} \subseteq \rightarrow_{R^\circ,B}$.

In the special case, $t \rightarrow_{R/E} v$ with no rewrite steps because $t =_E v$. As $\rightarrow_{R^\circ,B} = (\rightarrow^*_{R^\circ,B}; =_E)$ then $t \rightarrow_{R^\circ,B} v$. The other cases are proved using induction in the number n in the derivation $t = t_0 \rightarrow_{R/E} t_1 \cdots \rightarrow_{R/E} t_n = v$.

- Base case: $t =_E t'' \rightarrow^1_R u =_E v$. By Proposition 8 there exists a term t' in $\mathcal{H}_\Sigma$ such that $t =_B t' =_{E_0} t'' \rightarrow^1_R u =_E v$ so, by Proposition 3, $t =_B t' =_{E_0} t'' \rightarrow^1_{R^\circ,B} u =_E v$. Then, by Lemma 2, there exists a term u_1 in $\mathcal{H}_\Sigma$ such that $t =_B t' \rightarrow^1_{R^\circ,B} u_1 =_{E_0} u =_E v$ and, by Lemma 3, there exists a term w such that $t' =_B t \rightarrow^1_{R^\circ,B} w =_B u_1 =_{E_0} u =_E v$, i.e., $t \rightarrow^1_{R^\circ,B} v$.
- Induction case: $t \rightarrow^1_{R/E} u \rightarrow^+_{R/E} v$. By the previous subcase there exists a term u' such that $t \rightarrow^1_{R^\circ,B} u' =_E u \rightarrow^+_{R/E} v$, i.e., $t \rightarrow^1_{R^\circ,B} u' \rightarrow^+_{R/E} v$. Then, by I.H., there exists a term w such that $t \rightarrow^1_{R^\circ,B} u' \rightarrow^+_{R^\circ,B} w =_E v$, so $t \rightarrow_{R^\circ,B} v$.

Proposition 9. Given a rewrite theory $\mathcal{R} = (\Sigma, E, R)$ with built-in subtheory (Σ_0, E_0), and a narrowing path from a reachability goal G, $G = \Delta_0 \mid \psi_0 \rightsquigarrow_{\sigma_1} \Delta_1 \mid \psi_1 \rightsquigarrow_{\sigma_2} \cdots \Delta_{m-1} \mid \psi_{m-1} \rightsquigarrow_{\sigma_m} \mathit{nil} \mid \psi_m$, there exists another narrowing path $G = \Delta_0 \mid \psi_0 \rightsquigarrow_{\sigma_1} \Delta_1 \mid \chi_1 \rightsquigarrow_{\sigma_2} \cdots \Delta_{m-1} \mid \chi_{m-1} \rightsquigarrow_{\sigma_m} \mathit{nil} \mid \chi_m$, where if one rule is applied at step i in one path then the same rule is applied at step i in the other path, for $1 \leq i \leq m$, there is no simplification of the reachability formula when rule unification or rewrite is applied, and $E_0 \vdash \psi_i \Leftrightarrow \chi_i$, for $1 \leq i \leq m$.

Proof. As the applied rule at each step i only depends on Δ_{i-1} which is the same on both paths, as long as ψ_i and χ_i are satisfiable, all that it has to be proved is $E_0 \vdash \psi_i \Leftrightarrow \chi_i$. Then as ψ_i is satisfiable so is χ_i.

Let $\chi_0 = \psi_0$, so $E_0 \vdash \psi_0 \Leftrightarrow \chi_0$. Then $E_0 \vdash \psi_{i-1} \Leftrightarrow \chi_{i-1}$ implies $E_0 \vdash \psi_i \Leftrightarrow \chi_i$, for $1 \leq i \leq m$. The proof for rules transitivity and congruence is trivial, since $\psi_i = \psi_{i-1}$, $\chi_i = \chi_{i-1}$, and $E_0 \vdash \psi_{i-1} \Leftrightarrow \chi_{i-1}$, and it is also trivial for rules unification and rewrite since $\chi_i = (\chi_{i-1} \wedge \phi^\circ)\sigma_i$ and $E_0 \vdash \psi_i \Leftrightarrow (\chi_{i-1} \wedge \phi^\circ)\sigma_i$. As $E_0 \vdash \psi_0 \Leftrightarrow \chi_0$ then $E_0 \vdash \psi_i \Leftrightarrow \chi_i$, for $1 \leq i \leq m$.

Theorem 2. Given a rewrite theory $\mathcal{R} = (\Sigma, E_0 \cup B, R)$ with built-in subtheory (Σ_0, E_0), where $E = E_0 \cup B$, and a narrowing path from a reachability goal G, $G = \Delta_1 \mid \psi_1 \rightsquigarrow_{\sigma_1} \Delta_2 \mid \psi_2 \rightsquigarrow_{\sigma_2} \cdots \Delta_m \mid \psi_m \rightsquigarrow_{\sigma_m} \mathit{nil} \mid \psi$, let $\sigma = \sigma_1 \cdots \sigma_m$, then:

1. if $\Delta_1 = \bigwedge_{i=1}^n u_i \rightarrow v_i$ and $\rho : \mathcal{X} \rightarrow \mathcal{T}_\Sigma$ is a substitution such that $dom(\rho) = vars(G\sigma)$ and $\psi\rho$ is satisfiable then $(\sigma\rho)_{vars(G)}$ is a solution for G in $\rightarrow_{R^\circ,B}$, and
2. if $\Delta_1 = u_1|_p \rightarrow^1 x, u_1[x]_p \rightarrow v_1 \wedge \bigwedge_{i=2}^n u_i \rightarrow v_i \mid \psi_1$ and $\rho : \mathcal{X} \setminus \{x\} \rightarrow \mathcal{T}_\Sigma$ is a substitution such that $dom(\rho) = vars(G\sigma) \setminus \{x\}$ and $\psi\rho$ is satisfiable then
   (a) $(\sigma\rho)_{vars(G)\setminus\{x\}}$ is a solution for $\bigwedge_{i=1}^n u_i \rightarrow v_i \mid \psi_1$ in $\rightarrow_{R^\circ,B}$ and
   (b) there exists a substitution $\rho_x : \{x\} \rightarrow \mathcal{T}_\Sigma$ such that $(\sigma(\rho \cup \rho_x))_{vars(G)}$ is a solution for G in $\rightarrow_{R^\circ,B}$.

Proof. By structural induction over the length of the narrowing path and the first inference rule applied.

(*i*) Base case

$G = u_1 \rightarrow v_1 \mid \psi_1 \rightsquigarrow_{[u],\sigma} \mathit{nil} \mid \psi$, where $\mathit{abstract}_{\Sigma_1}(v_1) = \langle \lambda\bar{x}.v_1^\circ; \theta^\circ; \phi^\circ \rangle$, $vars(\psi) \subseteq vars((\psi_1 \wedge \phi^\circ)\sigma)$, $E_0 \vdash \psi \Leftrightarrow (\psi_1 \wedge \phi^\circ)\sigma$, $\bar{x} = \{x_1, \ldots, x_l\}$, $v_1^\circ = v_1[x_1]_{q_1} \cdots [x_l]_{q_l}$, $\phi^\circ = \bigwedge_{i=1}^l x_i = v_1|_{q_i}$, σ in $CSU_B(u_1 = v_1^\circ)$, so $u_1\sigma =_B v_1^\circ\sigma$, and ψ is satisfiable. As ρ is a substitution such that $dom(\rho) = vars(G\sigma)$ and $\psi\rho$ is satisfiable, so $(\psi_1 \wedge \phi^\circ)\sigma\rho$ is also satisfiable, then $\psi_1\sigma\rho \in \mathcal{T}_{\Sigma_0}$, so $E_0 \vDash \psi_1\sigma\rho$, and $\phi^\circ\sigma\rho = \bigwedge_{i=1}^l x_i\sigma\rho = v_1|_{q_i}\sigma\rho$ is satisfiable, where $v_1|_{q_i}\sigma\rho \in \mathcal{T}_\Sigma$, for $1 \leq i \leq l$, so

there exists a substitution $\rho' : \bigcup_{i=1}^{l} vars(x_i\sigma\rho) \to \mathcal{T}_\Sigma$ such that $x_i\sigma\rho\rho' =_{E_0} v_1|_{q_i}\sigma\rho\rho' = v_1|_{q_i}\sigma\rho$, for $1 \leq i \leq l$. Let $\gamma = \sigma\rho\rho'$.

As $u_1\sigma\rho$ and $v_1\sigma\rho$ in $\mathcal{T}_\Sigma$, the theory inclusion $(\Sigma_0, E_0) \subseteq (\Sigma, E)$ is protecting, and $u_1\sigma\rho =_B v_1^\circ\sigma\rho$, then $u_1\sigma\rho = u_1\gamma =_B v_1^\circ\gamma = v_1\gamma[x_1\gamma]_{q_1} \cdots [x_l\gamma]_{q_l} = v_1\sigma\rho[x_1\gamma]_{q_1} \cdots [x_l\gamma]_{q_l} =_{E_0}$ $v_1\sigma\rho[v_1|_{q_1}\sigma\rho]_{q_1} \cdots [v_1|_{q_l}\sigma\rho]_{q_l} = v_1\sigma\rho$, so $u_1\sigma\rho =_E v_1\sigma\rho$, and $u_1\sigma\rho \to_{R^\circ,B} v_1\sigma\rho$. Also as $vars(\{u_1, v_1, \psi_1\})$ is a subset of $vars(G)$ then $u_1(\sigma\rho)_{vars(G)} \to_{R^\circ,B} v_1(\sigma\rho)_{vars(G)}$ and $E_0 \vDash \psi_1(\sigma\rho)_{vars(G)}$.

(*ii*) Induction case

$G = \bigwedge_{i=1}^{n} u_i \to v_i \mid \psi_1$ or $G = u_1|_p \to^1 x, u_1[x]_p \to v_1 \wedge \bigwedge_{i=2}^{n} u_i \to v_i \mid \psi_1$. Let $\Delta = \bigwedge_{i=2}^{n} u_i \to v_i$. There is one case for each inference rule.

1. Rule transitivity: $G = u_1 \to v_1 \wedge \Delta \mid \psi_1 \rightsquigarrow_{[t]} u_1 \to^1 x, x \to v_1 \wedge \Delta \mid \psi_1 \rightsquigarrow_\sigma^* nil \mid \psi$, so $\sigma_{vars(G)} \mid \psi$ is a computed answer for G. Let $G_1 = u_1 \to^1 x, x \to v_1 \wedge \Delta \mid \psi_1$. As $dom(\rho) = vars(G_1\sigma)$ and $vars(G_1) = vars(G) \cup \{x\}$ then $dom(\rho) = vars(G_1\sigma) \setminus \{x\}$ so, by I.H., $(\sigma\rho)_{vars(G)}$ is a solution for G in $\to_{R^\circ,B}$.
2. Rule congruence: $G = u_1|_p \to^1 x, u_1[x]_p \to v_1 \wedge \Delta \mid \psi_1 \rightsquigarrow_{[c]} u_1|_{p.i} \to^1 y, u_1[y]_{p.i} \to v_1 \wedge \Delta \mid \psi_1 \rightsquigarrow_\sigma^* nil \mid \psi$, where each one of x and y appears exactly twice in the narrowing path. Let $G' = u_1|_{p.i} \to^1 y, u_1[y]_{p.i} \to v_1 \wedge \Delta \mid \psi_1$. As $vars(u_1|_p, u_1[x]_p) = vars(u_1) \cup \{x\}$ and $vars(u_1|_{p.i}, u_1[y]_{p.i}) = vars(u_1) \cup \{y\}$ then $vars(G') = (vars(G) \cup \{y\}) \setminus \{x\}$. Then $dom(\rho) = vars(G\sigma) \setminus \{x\} = vars(G\sigma) \setminus \{y\}$ so, by I.H., $(\sigma\rho)_{vars(G)}$ is a solution for $\bigwedge_{i=1}^{n} u_i \to v_i \mid \psi_1$ in $\to_{R/E}$ and there exists a substitution $\rho_y : \{y\} \to \mathcal{T}_\Sigma$ such that $(\rho \cup \rho_y)_{vars(G')}$ is a solution for G' in $\to_{R^\circ,B}$ so, as $(\rho \cup \rho_y)_{vars(G')} = (\rho \cup \rho_y)$ when applied to any term in G', $u_1(\rho \cup \rho_y)|_{p.i} \to^1_{R^\circ,B} y(\rho \cup \rho_y)$, $u_1(\rho \cup \rho_y)[y(\rho \cup \rho_y)]_{p.i} \to_{R^\circ,B} v_1(\rho \cup \rho_y)$ and $u_i(\rho \cup \rho_y) \to v_i(\rho \cup \rho_y)$, for $i \leq 2 \leq n$. As y appears exactly twice in G', this is equivalent to: $u_1\rho|_{p.i} \to^1_{R^\circ,B} y\rho_y$, $u_1\rho[y\rho_y]_{p.i} \to_{R^\circ,B} v_1\rho$ and $u_i\rho \to v_i\rho$, for $i \leq 2 \leq n$. Let $\rho_x = \{x \mapsto (u_1\rho[y\rho_y]_{p.i})|_p\}$. Then:
   (a) as $u_1\rho|_{p.i} \to^1_{R^\circ,B} y\rho_y$ then $u_1\rho|_p \to^1_{R^\circ,B} (u_1\rho[y\rho_y]_{p.i})|_p$, i.e. $u_1\rho|_p \to^1_{R^\circ,B} x\rho_x$, and
   (b) as $u_1\rho[y\rho_y]_{p.i} \to_{R^\circ,B} v_1\rho$ then $x\rho_x \to_{R^\circ,B} v_1\rho$.
   As x appears exactly twice in G, this is equivalent to $u_1(\rho \cup \rho_x)|_p \to^1_{R^\circ,B} x(\rho \cup \rho_x)$, $x(\rho \cup \rho_x) \to_{R^\circ,B} v_1(\rho \cup \rho_x)$, and $u_i(\rho \cup \rho_x) \to v_i(\rho \cup \rho_x)$, for $i \leq 2 \leq n$, so $(\rho \cup \rho_x)_{vars(G)}$ is a solution for G in $\to_{R^\circ,B}$.
3. Rule unification: $G = u_1 \to v_1 \wedge \Delta \mid \psi_1 \rightsquigarrow_{[u],\sigma_1} \Delta\sigma_1 \mid \psi_2 \rightsquigarrow_\beta^* nil \mid \psi$, where $\beta = \sigma_2 \cdots \sigma_m$ and $\sigma = \sigma_1\beta$. Consider the canonical path $G = u_1 \to v_1 \wedge \Delta \mid \chi_1 \rightsquigarrow_{[u],\sigma_1} \Delta\sigma_1 \mid \chi_2 \rightsquigarrow_\beta^* nil \mid \chi$, where $\chi_1 = \psi_1$. By Proposition 9, $E_0 \vdash \psi \Leftrightarrow \chi$ so, as ρ is a substitution such that $\psi\rho$ is satisfiable then $\chi\rho$ is also satisfiable. As $dom(\rho) = vars(G\sigma)$ then the proof can be done over the canonical path. The first narrowing step is as in the base case, with $\chi_2 = (\chi_1 \wedge \phi^\circ)\sigma_1$. Let $G' = \Delta \mid \chi_1 \wedge \phi^\circ$. As in the base case $\phi^\circ = (\bigwedge_{i=1}^{l} x_i = v_1|_{q_i})$, and σ_1 in $CSU_B(u_1 = v_1^\circ)$, so $u_1\sigma_1 =_B v_1^\circ\sigma_1$.
   Let $\rho = \rho_1 \cup \rho_2$, with $\rho_1 = \rho_{vars(G\sigma) \cap vars(G'\sigma)}$ and $\rho_2 = \rho_{vars(G\sigma) \setminus vars(G'\sigma)}$. As ρ is a substitution such that $\chi\rho$ is satisfiable, then $\chi\rho_1$, a more general formula, is also satisfiable, so there exists a substitution $\rho' : (vars(\chi) \setminus vars(G\sigma)) \cap vars(G'\sigma) \to \mathcal{T}_{\Sigma_0}$ such that $\chi(\rho_1 \cup \rho')$ is satisfiable. Let δ be a substitution $\delta : vars(G'\sigma(\rho_1 \cup \rho')) \to \mathcal{T}_\Sigma$, which must exist because all signatures have non-empty sorts, and let $\gamma = \rho_1 \cup \rho' \cup \delta$. Then $dom(\gamma) = vars(G'\sigma)$, $ran(\gamma) = \emptyset$ and $\chi\gamma$, equal to $\chi(\rho_1 \cup \rho')$, is satisfiable.
   $G'\sigma_1 \rightsquigarrow_\beta^* nil \mid \chi$, $\beta = \sigma_2 \cdots \sigma_m$, $dom(\gamma) = vars(G'\sigma) = vars((G'\sigma_1)\beta)$, and $\chi\gamma$ is satisfiable so, by I.H., $(\beta\gamma)_{vars(G'\sigma_1)}$ is a solution for $G'\sigma_1$ in $\to_{R^\circ,B}$.
   As, trivially, $(\beta\gamma)_{vars(G'\sigma_1)} = \beta\gamma$ when applied to $G'\sigma_1$, then $u_i\sigma_1\beta\gamma \to_{R^\circ,B} v_i\sigma_1\beta\gamma$, for $2 \leq i \leq n$, and $E_0 \vDash (\chi_1 \wedge \phi^\circ)\sigma_1\beta\gamma$. Now, as $\sigma_1\beta = \sigma$ then $u_i\sigma\gamma \to_{R^\circ,B} v_i\sigma\gamma$, for $2 \leq i \leq n$, and $E_0 \vDash (\chi_1 \wedge \phi^\circ)\sigma\gamma$, so also $E_0 \vDash \chi_1\sigma\gamma$ and $E_0 \vDash \phi^\circ\sigma\gamma$, ground formulas.
   As $dom(\rho_2) = vars(G\sigma) \setminus vars(G'\sigma)$ and $dom(\gamma) = vars(G'\sigma)$, then $dom(\rho_2 \cup \gamma) = vars(G\sigma) \cup vars(G'\sigma)$. But $\rho_2 \cup \gamma = \rho_2 \cup \rho_1 \cup \rho' \cup \delta = \rho \cup \rho' \cup \delta$, where $dom(\rho \cup \rho' \cup \delta) = vars(G\sigma) \cup$

$vars(G'\sigma)$, so $u_i\sigma(\rho_2 \cup \gamma) \to_{R^\circ,B} v_i\sigma(\rho_2 \cup \gamma)$, for $2 \leq i \leq n$, $E_0 \vDash \chi_1\sigma(\rho_2 \cup \gamma)$, and $E_0 \vDash \phi^\circ\sigma(\rho_2 \cup \gamma)$, i.e., $u_i\sigma(\rho \cup \rho' \cup \delta) \to_{R^\circ,B} v_i\sigma(\rho \cup \rho' \cup \delta)$, for $2 \leq i \leq n$, $E_0 \vDash \chi_1\sigma(\rho \cup \rho' \cup \delta)$, and $E_0 \vDash \phi^\circ\sigma(\rho \cup \rho' \cup \delta)$. Then, as $vars(\chi_1\sigma) \cup \bigcup_{i=1}^n vars(u_i) \cup \bigcup_{i=1}^n vars(v_i) \subseteq vars(G\sigma) = dom(\rho)$, $u_i\sigma\rho \to_{R^\circ,B} v_i\sigma\rho$, for $2 \leq i \leq n$, and $E_0 \vDash \chi_1\sigma\rho$.
As $\phi^\circ = (\bigwedge_{i=1}^l x_i = v_1|_{q_i})$ and $E_0 \vDash \phi^\circ\sigma(\rho \cup \rho' \cup \delta)$ then $E_0 \vDash \bigwedge_{i=1}^l x_i\sigma(\rho \cup \rho' \cup \delta) = v_1|_{q_i}\sigma(\rho \cup \rho' \cup \delta)$, but $vars(v_1\sigma) \subseteq vars(G\sigma) = dom(\rho)$, so $E_0 \vDash \bigwedge_{i=1}^l x_i\sigma(\rho \cup \rho' \cup \delta) = v_1|_{q_i}\sigma\rho$.
As $u_1\sigma_1 =_B v_1^\circ\sigma_1$ and $\sigma = \sigma_1\beta$ then also $u_1\sigma(\rho \cup \rho' \cup \delta) =_B v_1^\circ\sigma(\rho \cup \rho' \cup \delta)$. Now, as $v_1^\circ = v_1[x_1]_{q_1} \cdots [x_l]_{q_l}$ and $vars(u_1\sigma) \subseteq vars(G\sigma) = dom(\rho)$, then $u_1\sigma\rho = u_1\sigma(\rho \cup \rho' \cup \delta) =_B v_1^\circ\sigma(\rho \cup \rho' \cup \delta) = (v_1[x_1]_{q_1} \cdots [x_l]_{q_l})\sigma(\rho \cup \rho' \cup \delta) = v_1\sigma\rho[x_1\sigma(\rho \cup \rho' \cup \delta)]_{q_1} \cdots [x_l\sigma(\rho \cup \rho' \cup \delta)]_{q_l}) =_{E_0} (v_1\sigma\rho[v_1|_{q_1}\sigma\rho]_{q_1} \cdots [v_1|_{q_l}\sigma\rho]_{q_l}) = v_1\sigma\rho$, i.e., $u_1\sigma\rho =_E v_1\sigma\rho$, so $u_1\sigma\rho \to_{R^\circ,B} v_1\sigma\rho$ and $(\sigma\rho)_{vars(G)}$ is a solution for G in $\to_{R^\circ,B}$.

4. Rule rewrite: $G = u_1|_p \to^1 x, u_1[x]_p \to v_1 \wedge \Delta \mid \psi_1 \rightsquigarrow_{[r],\sigma_1} \Delta_2 \mid \psi_2 \rightsquigarrow_\beta^* nil \mid \psi$, where $\beta = \sigma_2 \cdots \sigma_m$ and $\sigma = \sigma_1\beta$. Consider the canonical path $G = u_1|_p \to^1 x, u_1[x]_p \to v_1 \wedge \Delta \mid \chi_1 \rightsquigarrow_{[u],\sigma_1} \Delta_2 \mid \chi_2 \rightsquigarrow_\beta^* nil \mid \chi$, where $\chi_1 = \psi_1$, as in the previous case. The first narrowing step uses a rule $c^\circ = l^\circ \to r$ *if* $\bigwedge_{i=1}^k l_i \to r_i \mid \phi$ in R°. This narrowing step has the form: $u_1|_p \to^1 x, u_1[x]_p \to v_1 \wedge \Delta \mid \psi_1 \rightsquigarrow_{[r],\sigma_1} (\bigwedge_{i=1}^k l_i \to r_i \wedge u_1[r]_p \to v_1 \wedge \Delta)\sigma_1 \mid (\chi_1 \wedge \phi)\sigma_1$, where σ_1 in $CSU_B(u_1|_p = l^\circ)$, so $u_1|_p\sigma_1 =_B l^\circ\sigma_1$. As x appears exactly twice in G and $ran(\sigma)$ is away from all the variables that have appeared before in the narrowing path, then $dom(\sigma) \cap \{x\} = \emptyset$ and $ran(\sigma) \cap \{x\} = \emptyset$. Let $G' = \bigwedge_{i=1}^k l_i \to r_i \wedge u_1[r]_p \to v_1 \wedge \Delta \mid \chi_1 \wedge \phi$.
Let $\rho = \rho_1 \cup \rho_2$, with $\rho_1 = \rho_{(vars(G\sigma)\setminus\{x\}) \cap vars(G'\sigma)}$ and $\rho_2 = \rho_{(vars(G\sigma)\setminus\{x\})\setminus vars(G'\sigma)}$. As ρ is a substitution such that $\chi\rho$ is satisfiable, then $\chi\rho_1$, a more general formula, is also satisfiable, so there exists a substitution $\rho' : (vars(\chi) \setminus (vars(G\sigma) \setminus \{x\})) \cap vars(G'\sigma) \to \mathcal{T}_{\Sigma_0}$ such that $\chi(\rho_1 \cup \rho')$ is satisfiable. Let δ be a substitution $\delta : vars(G'\sigma(\rho_1 \cup \rho')) \to \mathcal{T}_\Sigma$, which must exist because all signatures have non-empty sorts, and let $\gamma = \rho_1 \cup \rho' \cup \delta$. As ρ and ρ_1 are ground substitutions then $dom(\gamma) = vars(G'\sigma)$ and $ran(\gamma) = \emptyset$. Also, as $vars(\chi) \cap vars(G'\sigma) \subseteq dom(\rho_1 \cup \rho)$ then $\chi\gamma = \chi(\rho_1 \cup \rho')$, so $\chi\gamma$ is satisfiable.
$G'\sigma_1 \rightsquigarrow_\beta^* nil \mid \chi$, $\beta = \sigma_2 \cdots \sigma_m$, $dom(\gamma) = vars(G'\sigma) = vars((G'\sigma_1)\beta)$, and $\chi\gamma$ is satisfiable so, by I.H., $(\beta\gamma)_{vars(G'\sigma_1)}$ is a solution for $G'\sigma_1$ in $\to_{R^\circ,B}$. As $(\beta\gamma)_{vars(G'\sigma_1)} = \beta\gamma$ when applied to $G'\sigma_1$ then $l_i\sigma\gamma \to_{R^\circ,B} r_i\sigma\gamma$, for $1 \leq i \leq k$, $u_j\sigma\gamma \to_{R^\circ,B} v_j\sigma\gamma$, for $2 \leq j \leq n$, $u_1[r]_p\sigma\gamma \to_{R^\circ,B} v_1\sigma\gamma$, and $E_0 \vDash (\chi_1 \wedge \phi)\sigma\gamma$, so also $E_0 \vDash \chi_1\sigma\gamma$ and $E_0 \vDash \phi\sigma\gamma$, ground formulas.
In the same way that has been proven for rule unification, as $\rho_2 \cup \gamma = \rho \cup \rho' \cup \delta$, then $u_j\sigma\rho \to_{R^\circ,B} v_j\sigma\rho$, for $2 \leq j \leq n$, and $E_0 \vDash \chi_1\sigma\rho$.
As $u_1[r]_p\sigma\gamma \to_{R^\circ,B} v_1\sigma\gamma$, both ground terms, and $vars(v_1\sigma) \subseteq (vars(G\sigma) \setminus \{x\}) = dom(\rho)$ then $u_1[r]_p\sigma(\rho_2 \cup \gamma) = u_1[r]_p\sigma\gamma \to_{R^\circ,B} v_1\sigma\gamma = v_1\sigma(\rho_2 \cup \gamma)$, i.e., $u_1[r]_p\sigma(\rho \cup \rho' \cup \delta) \to_{R^\circ,B} v_1\sigma(\rho \cup \rho' \cup \delta) = v_1\sigma\rho$.
As $u_1|_p\sigma_1 =_B l^\circ\sigma_1$ then $u_1|_p\sigma(\rho \cup \rho' \cup \delta) =_B l^\circ\sigma(\rho \cup \rho' \cup \delta)$. Also as $l_i\sigma\gamma \to_{R^\circ,B} r_i\sigma\gamma$ then $l_i\sigma(\rho \cup \rho' \cup \delta) \to_{R^\circ,B} r_i\sigma(\rho \cup \rho' \cup \delta)$, for $1 \leq i \leq k$, and as $E_0 \vDash \phi\sigma\gamma$ then $E_0 \vDash \phi\sigma(\rho \cup \rho' \cup \delta)$, so $u_1|_p\sigma(\rho \cup \rho' \cup \delta) \to^1_{R^\circ,B} r\sigma(\rho \cup \rho' \cup \delta)$, with rule c°. In consequence, $u_1\sigma(\rho \cup \rho' \cup \delta) \to^1_{R^\circ,B} u_1[r]_p\sigma(\rho \cup \rho' \cup \delta)$ so, as $vars(u_1\sigma) \subseteq (vars(G\sigma) \setminus \{x\}) = dom(\rho)$, $u_1\sigma\rho = u_1\sigma(\rho \cup \rho' \cup \delta) \to^1_{R^\circ,B} u_1[r]_p\sigma(\rho \cup \rho' \cup \delta)$.
As $u_1\sigma\rho \to^1_{R^\circ,B} u_1[r]_p\sigma(\rho \cup \rho' \cup \delta)$ and $u_1[r]_p\sigma(\rho \cup \rho' \cup \delta) \to_{R^\circ,B} v_1\sigma\rho$ then $u_1\sigma\rho \to_{R^\circ,B} v_1\sigma\rho$, so $(\sigma\rho)_{vars(G)\setminus\{x\}}$ is a solution for $\bigwedge_{i=1}^n u_i \to v_i \mid \psi_1$ in $\to_{R^\circ,B}$.
Take $\rho_x = \{x \mapsto r\sigma(\rho \cup \rho' \cup \delta)\}$. As $dom(\sigma) \cap \{x\} = \emptyset$ and $ran(\sigma) \cap \{x\} = \emptyset$, then $u_1|_p\sigma(\rho \cup \rho_x) = u_1|_p\sigma\rho = u_1|_p\sigma(\rho \cup \rho' \cup \delta) \to^1_{R^\circ,B} r\sigma(\rho \cup \rho' \cup \delta) = x\rho_x = x\sigma\rho_x = x\sigma(\rho \cup \rho_x)$. Also, as $vars(u_1\sigma, v1\sigma) \subseteq (vars(G\sigma) \setminus \{x\}) = dom(\rho)$ and $ran(\rho) = \emptyset$, $u_1[x]_p\sigma(\rho \cup \rho_x) = u_1\sigma\rho[r\sigma(\rho \cup \rho' \cup \delta)]_p = u_1\sigma(\rho \cup \rho' \cup \delta)[r\sigma(\rho \cup \rho' \cup \delta)]_p = u_1[r]_p\sigma(\rho \cup \rho' \cup \delta) \to_{R^\circ,B} v_1\sigma\rho = v_1\sigma(\rho \cup \rho_x)$. Then, as $vars(\Delta) \cap dom(\rho_x) = \emptyset$, $(\sigma(\rho \cup \rho_x))_{vars(G)}$ is a solution for G in $\to_{R^\circ,B}$.