Variant Narrowing and Extreme Termination

Santiago Escobar[1], José Meseguer[2] and Ralf Sasse[2]

[1] Universidad Politécnica de Valencia, Spain. sescobar@dsic.upv.es
[2] University of Illinois at Urbana-Champaign, USA. {meseguer,rsasse}@cs.uiuc.edu

Abstract. For narrowing with a set of rules Δ modulo a set of axioms B almost nothing is known about terminating narrowing strategies, and basic narrowing is known to be incomplete for $B = AC$. In this work we ask and answer the question: *Is there such a thing as an extremely terminating narrowing strategy modulo B?* where we call a narrowing strategy S enjoying appropriate completeness properties *extremely terminating* iff whenever any other narrowing strategy S' enjoying the same completeness properties terminates on a term t, then S is guaranteed to terminate on t as well. We show that basic narrowing is *not* extremely terminating already for $B = \emptyset$, and provide a positive answer to the above question by means of a sequence of increasingly more restrictive *variant narrowing* strategies, called variant narrowing, variant narrowing with history, Δ, B–pattern narrowing with history, and Δ, B–pattern narrowing with history and folding, such that given a set Δ of confluent, terminating, and coherent rules modulo B: (i) Δ, B–pattern narrowing with history (and folding) are *strictly more restrictive* than basic narrowing; (ii) Δ, B–pattern narrowing with history and folding is an *extremely terminating* strategy modulo B, which *terminates* on a term t iff t has a finite, complete set of minimal variants; (iii) Δ, B–pattern narrowing with history and folding terminates on *all* terms *iff* $\Delta \cup B$ has the finite variant property; and (iv) Δ, B–pattern narrowing with history and folding yields a complete and minimal $\Delta \cup B$-unification algorithm, which is *finitary* when $\Delta \cup B$ has the finite variant property.

1 Introduction

Narrowing is a fundamental rewriting technique useful for many purposes, including equational unification [15], combinations of functional and logic programming [12,13], partial evaluation [2], and symbolic reachability analysis of rewrite theories understood as transition systems [21].

Narrowing with confluent and terminating equations E enjoys key completeness results, including the covering of all rewrite sequences of an instance of a term t by a normalized substitution as instances of narrowing sequences starting at t, and the generation of a complete set of E-unifiers [15]. However, full narrowing at all non-variable term positions can be quite inefficient both in space and time. Therefore, much work has been devoted to *narrowing strategies* that, while remaining complete, can have a much smaller search space. The *basic narrowing* strategy [15] was shown to be complete w.r.t. a complete set of E-unifiers for confluent and terminating equations E.

Termination aspects are another important potential benefit of narrowing strategies, since they can sometimes *terminate* —that is, generate a finite search tree when narrowing an input term t— while full narrowing may generate an infinite search tree on the same input term. For example, works such as [15,18,4,23,1] investigate conditions under which basic narrowing, one of the most fully studied strategies for termination purposes, terminates. Similarly, so-called lazy narrowing strategies also seek to both reduce the search space and to increase the chances of termination [5,10].

By decomposing an equational theory E into a set of rules Δ and a set of equational axioms B for which a B-unification algorithm exists, and imposing natural requirements such as confluence, termination and coherence of the rules Δ *modulo* B, narrowing can be generalized to narrowing *modulo* axioms B. As known since the original study [16], the good completeness properties of standard narrowing extend naturally to similar completeness properties for narrowing modulo B. However, except for [16,26], we are not aware of any studies about narrowing strategies in the modulo case. Furthermore, as work in [3,26] shows, narrowing modulo axioms such as associativity-commutativity (AC) can very easily lead to non-terminating behavior and, what is worse, as shown in the following example by Comon-Lundh and Delaune, basic narrowing modulo AC is *not* complete.

Example 1. [3] Consider the rewrite system $\mathcal{R} = \Delta \uplus B$ where Δ contains the following equations and B contains associativity and commutativity for $+$:

$$a + a = 0 \ (1) \qquad a + a + X = X \ (3) \qquad 0 + X = X \ (5)$$
$$b + b = 0 \ (2) \qquad b + b + X = X \ (4)$$

$\mathcal{R}$ is terminating, AC-convergent, and AC-coherent. The substitution $\sigma = \{x_1 \mapsto a + b; x_2 \mapsto a + b\}$ is a solution of the reachability problem $X_1 + X_2 \rightarrow^* 0$, whereas there is no basic AC-narrowing derivation yielding a more general solution, i.e., w.r.t. the extension of basic narrowing to AC where we just replace syntactic unification by AC-unification. The narrowing sequence corresponding to substitution σ consists of applying rule (3) with unifier $\rho_1 = \{X_1 \mapsto a + X', X_2 \mapsto a + X'', X \mapsto X' + X''\}$ and rule (2) with unifier $\rho_2 = \{X' \mapsto b, X'' \mapsto b\}$, or equivalently rule (4) and rule (1) with their corresponding unifiers. However, this sequence is not computed by basic AC-narrowing, as explained in Example 5 below. Furthermore, there is no other basic AC-narrowing sequence computing a substitution more general than σ.

Since there are many potential applications of narrowing modulo axioms to areas such as equational reasoning, combinations of functional and logic programming, partial evaluation, cryptographic protocol analysis, and reachability and model checking analysis of concurrent systems, the current almost complete absence of studies about narrowing strategies modulo axioms B and their related termination properties is a serious obstacle to the development of practical algorithms and tools supporting such applications, for which full narrowing modulo B, although complete in theory, appears hopeless in practice.

In our recent work we have presented some partial results in this direction, building upon the notion of variant proposed by Comon-Lundh and Delaune in [3]. Specifically, in [9] we developed a narrowing strategy called *variant narrowing*, that, given a theory E decomposed into axioms B for which a finitary unification algorithm exists and rules Δ that are confluent, terminating, and coherent modulo B, is complete, and generates a complete set of variants for any input term. Furthermore, when E has the finite variant property [3] it is possible to give a bound depending on the input term t, so that the strategy remains complete when the narrowing tree is restricted to narrowing sequences of depth up to the given bound; this bounded variant narrowing strategy also provides a finitary E-unification algorithm [9]. However, these results are not fully usable unless automated methods are given to check that the given theory E has the finite variant property; therefore in [8] we proposed one such method based on the dependency pairs technique for the modulo case [11].

For narrowing strategy termination purposes, what the results in [9] show is that *if* E has the finite variant property, then the variant narrowing strategy, although itself

non-terminating even under that assumption, can be made to terminate by cutting its search space with a depth bound dependent on the input term. Although useful for a number of purposes (for example for protocol analysis), these results are incomplete and unsatisfactory for the following reasons: (i) the finite variant property is quite a strong requirement; (ii) the bound is external to the strategy and can only be determined under such a property, so that no termination method exists in all other cases; and (iii) the bound is overly *conservative*, making the method rather crude and relatively inefficient.

In this work we ask and answer a more general and ambitious question:

Is there such a thing as an extremely terminating narrowing strategy?

where we call a narrowing strategy S enjoying appropriate completeness properties *extremely terminating* if and only if whenever any other narrowing strategy S' enjoying the same completeness properties terminates on a term t, then S is guaranteed to terminate on t as well. That is, no other strategy can remain complete and terminate on a term when S does not. To the best of our knowledge, the notion of extremely terminating narrowing strategy has not been formulated before. It clarifies important questions such as the following: is basic narrowing, perhaps the narrowing strategy for which the most termination results are known, extremely terminating? As we show in this paper, the answer is an emphatic *no*, even in the standard case ($B = \emptyset$).

Our contribution. Our answer to the above question assumes confluent, terminating, and coherent rules Δ modulo B (including the standard case $B = \emptyset$) and takes the form of a sequence of increasingly more restrictive variant narrowing strategies, called variant narrowing, variant narrowing with history, Δ, B–pattern narrowing with history, and Δ, B–pattern narrowing with history and folding, that are complete for reachability of instance terms in normal form and for unification purposes and such that:

1. from Δ, B–pattern narrowing with history on they are *strictly more restrictive* than basic narrowing, and therefore terminate strictly more often than basic narrowing does;
2. Δ, B–pattern narrowing with history and folding is an *extremely terminating* strategy; furthermore, the set of terms reached by Δ, B–pattern narrowing with history and folding provide a *minimal and complete set of variants* for the input term t, so that Δ, B–pattern narrowing with history and folding *terminates* on an input term t if and only if t has a finite, complete set of minimal variants;
3. Δ, B–pattern narrowing with history and folding terminates on *all* input terms *if and only if* the theory $\Delta \cup B$ has the finite variant property; since Δ, B–pattern narrowing with history and folding is extremely terminating, this shows that the finite variant property is the *weakest possible* condition for a narrowing strategy to terminate on all terms while keeping the above-mentioned completeness properties.
4. Δ, B–pattern narrowing with history and folding can be used to generate a complete and minimal set of $\Delta \cup B$-unifiers; furthermore, if $\Delta \cup B$ has the finite variant property, then Δ, B–pattern narrowing with history and folding provides a *finitary* $\Delta \cup B$-unification algorithm.

2 Preliminaries

We follow the classical notation and terminology from [25] for term rewriting and from [19,20] for rewriting logic and order-sorted notions. We assume an S-sorted family $\mathcal{X} = \{\mathcal{X}_\mathsf{s}\}_{\mathsf{s}\in\mathsf{S}}$ of disjoint variable sets with each $\mathcal{X}_\mathsf{s}$ countably infinite. $\mathcal{T}_\Sigma(\mathcal{X})_\mathsf{s}$ is the set of terms

of sort s, and $\mathcal{T}_{\Sigma,\mathsf{s}}$ is the set of ground terms of sort s. We write $\mathcal{T}_\Sigma(\mathcal{X})$ and $\mathcal{T}_\Sigma$ for the corresponding term algebras.

For a term t we write $Var(t)$ for the set of all variables in t. The set of positions of a term t is written $Pos(t)$, and the set of non-variable positions $Pos_\Sigma(t)$. The root position of a term is Λ. The subterm of t at position p is $t|_p$ and $t[u]_p$ is the term t where $t|_p$ is replaced by u. A *substitution* σ is a sorted mapping from a finite subset of $\mathcal{X}$, written $Dom(\sigma)$, to $\mathcal{T}_\Sigma(\mathcal{X})$. The set of variables introduced by σ is $Ran(\sigma)$. The identity substitution is *id*. Substitutions are homomorphically extended to $\mathcal{T}_\Sigma(\mathcal{X})$. The application of a substitution σ to a term t is denoted by $t\sigma$. The restriction of σ to a set of variables V is $\sigma|_V$. Composition of two substitutions is denoted by $\sigma\sigma'$. We call a substitution σ a *renaming* if there is another substitution σ^{-1} such that $\sigma\sigma^{-1}|_{Dom(\sigma)} = id$.

A *Σ-equation* is an unoriented pair $t = t'$, where $t, t' \in \mathcal{T}_\Sigma(\mathcal{X})_\mathsf{s}$ for some sort $\mathsf{s} \in \mathsf{S}$. Given Σ and a set E of Σ-equations such that $\mathcal{T}_{\Sigma,\mathsf{s}} \neq \emptyset$ for every sort s, order-sorted equational logic induces a congruence relation $=_E$ on terms $t, t' \in \mathcal{T}_\Sigma(\mathcal{X})$ (see [20]). Throughout this paper we assume that $\mathcal{T}_{\Sigma,\mathsf{s}} \neq \emptyset$ for every sort s. An *equational theory* (Σ, E) is a set of Σ-equations.

The *E-subsumption* preorder $\sqsubseteq_E$ (or $\sqsubseteq$ if E is understood) holds between $t, t' \in \mathcal{T}_\Sigma(\mathcal{X})$, denoted $t \sqsubseteq_E t'$ (meaning that t' is *more general* than t modulo E), if there is a substitution σ such that $t =_E t'\sigma$; such a substitution σ is said to be an *E-match* from t to t'. The E-renaming equivalence $t \approx_E t'$, holds if there is a renaming θ such that $t\theta =_E t'\theta$. For substitutions σ, ρ and a set of variables V we define $\sigma|_V =_E \rho|_V$ if $x\sigma =_E x\rho$ for all $x \in V$; and $\sigma|_V \sqsubseteq_E \rho|_V$ if there is a substitution η such that $\sigma|_V =_E (\rho\eta)|_V$.

An *E-unifier* for a Σ-equation $t = t'$ is a substitution σ such that $t\sigma =_E t'\sigma$. For $Var(t) \cup Var(t') \subseteq W$, a set of substitutions $CSU_E(t = t')$ is said to be a *complete* set of unifiers of the equation $t =_E t'$ away from W if: (i) each $\sigma \in CSU_E(t = t')$ is an E-unifier of $t =_E t'$; (ii) for any E-unifier ρ of $t =_E t'$ there is a $\sigma \in CSU_E(t = t')$ such that $\rho|_W \sqsubseteq_E \sigma|_W$; (iii) for all $\sigma \in CSU_E(t = t')$, $Dom(\sigma) \subseteq (Var(t) \cup Var(t'))$ and $Ran(\sigma) \cap W = \emptyset$. An E-unification algorithm is *complete* if for any equation $t = t'$ it generates a complete set of E-unifiers. Note that this set needs not be finite. A unification algorithm is said to be *finitary* and complete if it always terminates after generating a finite and complete set of solutions.

A *rewrite rule* is an oriented pair $l \to r$, where $l \notin \mathcal{X}$, and $l, r \in \mathcal{T}_\Sigma(\mathcal{X})_\mathsf{s}$ for some sort $\mathsf{s} \in \mathsf{S}$. An *(unconditional) order-sorted rewrite theory* is a triple $\mathcal{R} = (\Sigma, E, R)$ with Σ an order-sorted signature, E a set of Σ-equations, and R a set of rewrite rules. The rewriting relation on $\mathcal{T}_\Sigma(\mathcal{X})$, written $t \to_R t'$ or $t \to_{p,R} t'$ holds between t and t' iff there exist $p \in Pos_\Sigma(t)$, $l \to r \in R$ and a substitution σ, such that $t|_p = l\sigma$, and $t' = t[r\sigma]_p$. The relation $\to_{R/E}$ on $\mathcal{T}_\Sigma(\mathcal{X})$ is $=_E; \to_R; =_E$. Note that $\to_{R/E}$ on $\mathcal{T}_\Sigma(\mathcal{X})$ induces a relation $\to_{R/E}$ on the free (Σ, E)-algebra $\mathcal{T}_{\Sigma/E}(\mathcal{X})$ by $[t]_E \to_{R/E} [t']_E$ iff $t \to_{R/E} t'$. The transitive closure of $\to_{R/E}$ is denoted by $\to^+_{R/E}$ and the transitive and reflexive closure of $\to_{R/E}$ is denoted by $\to^*_{R/E}$. We say that a term t is $\to_{R/E}$-irreducible (or just R/E-irreducible) if there is no term t' such that $t \to_{R/E} t'$.

For substitutions σ, ρ and a set of variables V we define $\sigma|_V \to_{R/E} \rho|_V$ if there is $x \in V$ such that $x\sigma \to_{R/E} x\rho$ and for all other $y \in V$ we have $y\sigma =_E y\rho$. A substitution σ is called *R/E-normalized* (or normalized) if $x\sigma$ is R/E-irreducible for all $x \in V$.

We say that the relation $\to_{R/E}$ is *terminating* if there is no infinite sequence $t_1 \to_{R/E} t_2 \to_{R/E} \cdots t_n \to_{R/E} t_{n+1} \cdots$. We say that the relation $\to_{R/E}$ is *confluent* if whenever $t \to^*_{R/E} t'$ and $t \to^*_{R/E} t''$, there exists a term t''' such that $t' \to^*_{R/E} t'''$ and $t'' \to^*_{R/E} t'''$. An order-sorted rewrite theory $\mathcal{R} = (\Sigma, E, R)$ is confluent (resp. terminating) if the relation $\to_{R/E}$ is confluent (resp. terminating). In a confluent, terminating, order-sorted

rewrite theory, for each term $t \in \mathcal{T}_\Sigma(\mathcal{X})$, there is a unique (up to E-equivalence) R/E-irreducible term t' obtained from t by rewriting to canonical form, which is denoted by $t \to^!_{R/E} t'$ or $t{\downarrow_{R/E}}$ (when t' is not relevant).

3 Variant Semantics and Δ, B–pattern Rewriting

Since E-congruence classes can be infinite, $\to_{R/E}$-reducibility is undecidable in general. Therefore, R/E-rewriting is usually implemented [16] by R, E-rewriting. We assume the following properties on R and E:

1. E is *regular*, i.e., for each $t = t'$ in E, we have $Var(t) = Var(t')$, and *sort-preserving*, i.e., for each substitution σ, we have $t\sigma \in \mathcal{T}_\Sigma(\mathcal{X})_\mathsf{s}$ iff $t'\sigma \in \mathcal{T}_\Sigma(\mathcal{X})_\mathsf{s}$; furthermore all variables in $Var(t)$ have a top sort.
2. E has a finitary and complete unification algorithm.
3. For each $t \to t'$ in R we have $Var(t') \subseteq Var(t)$.
4. R is *sort-decreasing*, i.e., for each $t \to t'$ in R, each $\mathsf{s} \in \mathsf{S}$, and each substitution σ, $t'\sigma \in \mathcal{T}_\Sigma(\mathcal{X})_\mathsf{s}$ implies $t\sigma \in \mathcal{T}_\Sigma(\mathcal{X})_\mathsf{s}$.
5. The rewrite rules R are *confluent and terminating modulo* E, i.e., the relation $\to_{R/E}$ is confluent and terminating.

Definition 1 (Rewriting modulo). [27] *Let $\mathcal{R} = (\Sigma, E, R)$ be an order-sorted rewrite theory satisfying properties* (1)–(5)*. We define the relation $\to_{R,E}$ on $\mathcal{T}_\Sigma(\mathcal{X})$ by $t \to_{R,E} t'$ or $t \to_{p,R,E} t'$ iff there is a $p \in Pos_\Sigma(t)$, $l \to r$ in R and substitution σ such that $t|_p =_E l\sigma$ and $t' = t[r\sigma]_p$.*

Note that, since E-matching is decidable, $\to_{R,E}$ is decidable. Notions such as confluence, termination, irreducible terms, and normalized substitution, are defined in a straightforward manner for $\to_{R,E}$. Note that since R is confluent and terminating modulo E, the relation $\to^!_{R,E}$ is decidable, i.e., it terminates and produces a unique term (up to E-equivalence) for each initial term t, denoted by $t{\downarrow_{R,E}}$. Of course $t \to_{R,E} t'$ implies $t \to_{R/E} t'$, but the converse does not need to hold. To prove completeness of $\to_{R,E}$ w.r.t. $\to_{R/E}$ we need the following additional *coherence* assumption; we refer the reader to [24,11,27,17] for coherence completion algorithms.

6. $\to_{R,E}$ is *E-coherent* [16], i.e., $\forall t_1, t_2, t_3$ we have $t_1 \to_{R,E} t_2$ and $t_1 =_E t_3$ implies $\exists t_4, t_5$ such that $t_2 \to^*_{R,E} t_4$, $t_3 \to^+_{R,E} t_5$, and $t_4 =_E t_5$.

The following theorem in [16, Proposition 1] that generalizes ideas in [24] and has an easy extension to order-sorted theories, links $\to_{R/E}$ with $\to_{R,E}$.

Theorem 1 (Correspondence). [24,16] *Let $\mathcal{R} = (\Sigma, E, R)$ be an order-sorted rewrite theory satisfying properties* (1)–(6)*. Then $t_1 \to^!_{R/E} t_2$ iff $t_1 \to^!_{R,E} t_3$, where $t_2 =_E t_3$.*

Finally, we provide the notion of decomposition of an equational theory into rules and axioms.

Definition 2 (Decomposition). [9] *Let (Σ, E) be an order-sorted equational theory. We call (Σ, B, Δ) a* decomposition *of E if $E = \Delta \uplus B$ and (Σ, B, Δ) is an order-sorted rewrite theory satisfying properties* (1)–(6)*.*

In order to provide a suitable narrowing strategy in the next sections, we must first characterize a notion of completeness of a rewriting strategy and a new rewriting strategy.

3.1 The Variant Semantics $[\![t]\!]^{\star}_{\Delta,B}$ and $[\![t]\!]_{\Delta,B}$

Given an equational theory, and a term t, we can provide a notion of semantics of t based on the notion of *variant* from [3]. This semantics generalizes to decompositions of equational theories the syntactic notion where the semantics of t is the set of its substitution instances.

Definition 3 (Variant semantics). *Let $\mathcal{R} = (\Sigma, B, \Delta)$ be a decomposition of an equational theory and t be a term. We define the set of variants of t as $[\![t]\!]^{\star}_{\Delta,B} = \{(t', \theta) \mid t\theta \rightarrow^{!}_{\Delta,B} t'\}$.*

Definition 4 (Variant Preordering). *Let $\mathcal{R} = (\Sigma, B, \Delta)$ be a decomposition of an equational theory and t be a term. Given two variants $(t_1, \theta_1), (t_2, \theta_2) \in [\![t]\!]^{\star}_{\Delta,B}$, we write $(t_1, \theta_1) \sqsubseteq_{\Delta,B} (t_2, \theta_2)$ iff there is a substitution ρ such that $t_1 =_B t_2\rho$ and $\theta_1{\downarrow_{\Delta,B}} =_B \theta_2\rho$. We write $(t_1, \theta_1) \sqsubset_{\Delta,B} (t_2, \theta_2)$ if, furthermore, ρ is not a renaming. For $S_1, S_2 \subseteq [\![t]\!]^{\star}_{\Delta,B}$, $S_1 \sqsubseteq_{\Delta,B} S_2$ if for each $(t_1, \theta_1) \in S_1$, there exists $(t_2, \theta_2) \in S_2$ s.t. $(t_1, \theta_1) \sqsubseteq_{\Delta,B} (t_2, \theta_2)$. We write $S_1 \simeq_{\Delta,B} S_2$ if $S_1 \sqsubseteq_{\Delta,B} S_2$ and $S_2 \sqsubseteq_{\Delta,B} S_1$.*

For $(t_1, \theta_1), (t_2, \theta_2) \in [\![t]\!]^{\star}_{\Delta,B}$, we write $(t_1, \theta_1) \approx_B (t_2, \theta_2)$ if there is a renaming ρ such that $t_1\rho =_B t_2\rho$ and $\theta_1\rho =_B \theta_2\rho$. We write $S_1 \approx_B S_2$ if for each $(t_1, \theta_1) \in S_1$, there exists $(t_2, \theta_2) \in S_2$ s.t. $(t_1, \theta_1) \approx_B (t_2, \theta_2)$, and for each $(t_2, \theta_2) \in S_2$, there exists $(t_1, \theta_1) \in S_1$ s.t. $(t_2, \theta_2) \approx_B (t_1, \theta_1)$.

Definition 5 (Minimal and Complete Variant Semantics). *Let $\mathcal{R} = (\Sigma, B, \Delta)$ be a decomposition of an equational theory and t be a term. A* minimal and complete variant semantics *of t, denoted $[\![t]\!]_{\Delta,B}$, is a subset $S \subseteq [\![t]\!]^{\star}_{\Delta,B}$ such that, for each $(t_1, \theta_1) \in [\![t]\!]^{\star}_{\Delta,B}$, there is $(t_2, \theta_2) \in S$ s.t. (i) $(t_1, \theta_1) \sqsubseteq_{\Delta,B} (t_2, \theta_2)$, and (ii) there is no $(t_3, \theta_3) \in S$, (t_3, θ_3) different from (t_2, θ_2), s.t. $(t_2, \theta_2) \sqsubseteq_{\Delta,B} (t_3, \theta_3)$.*

Note that, for any term t, $[\![t]\!]^{\star}_{\Delta,B} \simeq_{\Delta,B} [\![t]\!]_{\Delta,B}$ but $[\![t]\!]^{\star}_{\Delta,B} \not\approx_B [\![t]\!]_{\Delta,B}$. Also, by definition, all the substitutions in $[\![t]\!]_{\Delta,B}$ are Δ, B-normalized. Moreover, if $(t', \theta) \in [\![t]\!]_{\Delta,B}$ then (t', θ) is unique up to $\approx_B$, other equivalent $(t'', \theta') \in [\![t]\!]_{\Delta,B}$ would destroy minimality. Therefore, $[\![t]\!]_{\Delta,B}$ is unique up to $\approx_B$ and provides a minimal description of $[\![t]\!]^{\star}_{\Delta,B}$.

Example 2. Let us consider the following equational theory for the exclusive or operator and the cancellation equations for public encryption/decryption. The exclusive or symbol $\oplus$ has associative and commutative (AC) properties with 0 as its unit. The symbol pk is used for public key encryption and the symbol sk for private key encryption. The equational theory (Σ, E) has a decomposition into Δ containing the following oriented equations and B containing associativity and commutativity for $\oplus$:

$$X \oplus 0 = X \quad (6) \qquad X \oplus X \oplus Y = Y \quad (8) \qquad pk(K, sk(K, M)) = M \quad (9)$$
$$X \oplus X = 0 \quad (7) \qquad\qquad\qquad\qquad sk(K, pk(K, M)) = M \quad (10)$$

Note that equations (6)–(7) are not AC-coherent, but adding equation (8) is sufficient to recover that property. For $t = M \oplus sk(K, pk(K, M))$ and $s = X \oplus sk(K, pk(K, Y))$, we have that $[\![t]\!]_{\Delta,B} = \{(0, id)\}$ and $[\![s]\!]_{\Delta,B}$ contains the following seven variants (i) $(X \oplus Y, id)$, (ii) $(Z, \{X \mapsto 0, Y \mapsto Z\})$, (iii) $(Z, \{X \mapsto Z, Y \mapsto 0\})$, (iv) $(Z, \{X \mapsto Z \oplus U, Y \mapsto U\})$, (v) $(Z, \{X \mapsto U, Y \mapsto Z \oplus U\})$, (vi) $(0, \{X \mapsto U, Y \mapsto U\})$, (vii) $(Z_1 \oplus Z_2, \{X \mapsto U \oplus Z_1, Y \mapsto U \oplus Z_2\})$. The minimality is easily checked as none of them subsumes another one.

3.2 The Δ, B–pattern Rewriting Strategy

The basic narrowing strategy [15,14] was shown to be complete for E-unification for a set E of confluent and terminating rules. Basic narrowing mimics innermost rewriting sequences, i.e., given a term t and an E-normalized substitution σ, every innermost rewriting sequence from $t\sigma$ can be lifted to a basic narrowing sequence from t computing a substitution more general then σ (see [22]). Intuitively, in an innermost rewriting sequence, the matching substitution of each step is E-normalized.

Similarly, when decomposing E into a set of rules Δ and a set of equational axioms B for which a B-unification algorithm exists, we need a rewriting and a narrowing strategy such that sequences of the former are lifted into sequences of the latter. However, innermost B-rewriting is not appropriate, since the innermost concept does not have an immediate extension to the modulo case, e.g. the term $(a + b) + (a + b)$ is a pattern, i.e., all strict subterms are normalized according to Example 1, but that does not hold for term $(a + a) + (b + b)$, which is equivalent modulo AC to the previous term. Note that this is related to the notion of B-coherence.

In [8], we developed a notion of Δ, B–pattern that is suitable for this purpose. Unlike innermost rewriting, we do not require a pattern nor a normalized matching substitution, but a term that *has* a pattern within its equivalence class.

Definition 6 (Δ, B–pattern). *[8] Let $\mathcal{R} = (\Sigma, B, \Delta)$ be a decomposition of an equational theory. We call a term $f(t_1, \ldots, t_n)$ a* Δ, B–pattern *if all subterms $t_1, \ldots, t_n$ are $\rightarrow_{\Delta,B}$-irreducible. We say that a term t* has *a Δ, B–pattern if there is a Δ, B–pattern t' s.t. $t' =_B t$.*

It is worth pointing out that whether a term has a Δ, B–pattern is *decidable*: given a term t, t has a Δ, B–pattern t' iff there is a symbol $f \in \Sigma$ with arity k and different variables $X_1, \ldots, X_k$ of the appropriate top sorts and there is a substitution θ s.t. $t =_B f(X_1, \ldots, X_k)\theta$ and θ is Δ, B-normalized, where $t' = f(X_1, \ldots, X_k)\theta$. In the case of a term t rooted by a free symbol, t has a Δ, B–pattern if it is already a Δ, B–pattern, i.e., every argument of the root symbol must be irreducible. And, in the case of a term t rooted by an AC symbol, we only have to consider in the previous algorithm the same AC symbol at the root of t, instead of every symbol.

Definition 7 (Δ, B–pattern rewriting strategy). *Let $\mathcal{R} = (\Sigma, B, \Delta)$ be a decomposition of an equational theory. A rewrite sequence $t_0 \overset{p_0}{\rightarrow}_{\Delta,B} t_1 \ldots \overset{p_n}{\rightarrow}_{\Delta,B} t_{n+1}$ is called a* Δ, B–pattern sequence *if each redex term $t_i|_{p_i}$ has a Δ, B–pattern. Given a term t, the* Δ, B–pattern rewriting strategy *produces only Δ, B–pattern rewriting sequences from t.*

As we are only considering decompositions of equational theories, any rewriting strategy is complete for normalization purposes.

Corollary 1. *Let $\mathcal{R} = (\Sigma, B, \Delta)$ be a decomposition of an equational theory. If $t \rightarrow^!_{\Delta,B} t'$, there is a Δ, B–pattern sequence $t \rightarrow^*_{\Delta,B} t''$ s.t. $t'' =_B t'$.*

4 Δ, B-Narrowing

Narrowing generalizes rewriting by performing unification at non-variable positions instead of the usual matching. The essential idea behind narrowing is to *symbolically* represent the rewriting relation between terms as a narrowing relation between more general terms.

Definition 8 (Narrowing modulo). *(see, e.g.,* [16,21]*) Let $\mathcal{R} = (\Sigma, B, \Delta)$ be a decomposition of an equational theory. Let $CSU_B(u = u')$ provide a finitary, and complete set of unifiers for any pair of terms u, u' with the same top sort. The Δ, B-narrowing relation on $\mathcal{T}_\Sigma(\mathcal{X})$ is defined as $t \rightsquigarrow_{p,\sigma,\Delta,B} t'$ (or $\rightsquigarrow_\sigma$ if p, Δ, B are understood) if there is $p \in Pos_\Sigma(t)$, a (possibly renamed) rule $l \to r$ in Δ, and $\sigma \in CSU_B(t|_p = l)$ such that $t' = (t[r]_p)\sigma$.*

The transitive closure of $\rightsquigarrow_\sigma$ is denoted by $\rightsquigarrow_\sigma^+$ and the transitive and reflexive closure by $\rightsquigarrow_\sigma^*$, i.e., $t \rightsquigarrow_\sigma^* t'$ if there are $s_1, \ldots, s_{k-1}$ and substitutions $\rho_1, \ldots, \rho_k$ such that $t \rightsquigarrow_{\rho_1} s_1 \cdots s_{k-1} \rightsquigarrow_{\rho_k} t'$, $k \geq 0$, and $\sigma = \rho_1 \cdots \rho_k$. We may write the concrete number of steps instead of $+$ or $*$.

Several notions of completeness of narrowing w.r.t. rewriting have been given in the literature [15,16,21,5]. In this paper we are interested in a slightly different but pertinent notion of completeness. First, we extend the variant semantics to narrowing and consider only narrowing sequences to normalized terms.

Definition 9 (Variant narrowing semantics). *Let $\mathcal{R} = (\Sigma, B, \Delta)$ be a decomposition of an equational theory and t be a term. We define the set of* narrowing variants *of t as $[\![t]\!]^{\rightsquigarrow}_{\Delta,B} = \{(t', \theta) \mid t \rightsquigarrow^*_{\theta,\Delta,B} t' \text{ and } t' = t'{\downarrow_{\Delta,B}}\}$.*

Theorem 2 (Completeness). [16] *Let $\mathcal{R} = (\Sigma, B, \Delta)$ be a decomposition of an equational theory. Let t be a term. Then, $[\![t]\!]_{\Delta,B} \simeq_{\Delta,B} [\![t]\!]^{\rightsquigarrow}_{\Delta,B}$.*

Example 3. Following Example 2, as $t \to^!_{\Delta,B} 0$ we have $t \overset{id}{\rightsquigarrow}^!_{\Delta,B} 0$ and, therefore, $[\![t]\!]_{\Delta,B} = \{(0, id)\}$. For $s = X \oplus sk(K, pk(K, Y))$ we get that the variants are generated by the following narrowing sequences (we indicate the number of steps as a super-index): (i) $s \rightsquigarrow_{id,\Delta,B} X \oplus Y$, (ii) $s \rightsquigarrow^2_{\{X \mapsto 0, Y \mapsto Z\},\Delta,B} Z$, (iii) $s \rightsquigarrow^2_{\{X \mapsto Z, Y \mapsto 0\},\Delta,B} Z$, (iv) $s \rightsquigarrow^2_{\{X \mapsto Z \oplus U, Y \mapsto U\},\Delta,B} Z$, (v) $s \rightsquigarrow^2_{\{X \mapsto U, Y \mapsto Z \oplus U\},\Delta,B} Z$, (vi) $s \rightsquigarrow^2_{\{X \mapsto U, Y \mapsto U\},\Delta,B} 0$, (vii) $s \rightsquigarrow^2_{\{X \mapsto U \oplus Z_1, Y \mapsto U \oplus Z_2\},\Delta,B} Z_1 \oplus Z_2$.

The narrowing relation $\rightsquigarrow_{\Delta,B}$ is known to give a sound and complete $\Delta \uplus B$-unification procedure [16] that we now relate to the variant semantics.

Proposition 1 (Minimal and Complete E-unification Procedure). *Let $\mathcal{R} = (\Sigma, B, \Delta)$ be a decomposition of an equational theory (Σ, E). Let t, t' be two terms. Then, $S = \{\theta \mid (\mathtt{tt}, \theta) \in [\![\mathtt{eq}(t, t')]\!]^{\rightsquigarrow}_{\widehat{\Delta},B}\}$ is a minimal and complete set of E-unifiers for $t = t'$, where $\mathtt{eq}$ and $\mathtt{tt}$ are new symbols[3] and $\widehat{\Delta} = \Delta \cup \{\mathtt{eq}(X, X) \to \mathtt{tt}\}$.*

5 Narrowing Strategies and Extreme Termination

First, we present a slight reformulationa of the variant narrowing of [9]. Next, we introduce our three refinements, giving rise to variant narrowing with history, Δ, B–pattern narrowing with history, and Δ, B–pattern narrowing with history and folding.

For our running example, we show that: (i) variant narrowing, (ii) variant narrowing with history, and (iii) Δ, B–pattern narrowing with history may be non-terminating whenever Δ, B–pattern narrowing with history and folding does terminate.

[3] That is, we extend Σ to $\widehat{\Sigma}$ by adding a new sort Truth, not related to any sort in Σ, with constant $\mathtt{tt}$, and for each top sort of a connected component [s], an operator $\mathtt{eq} : [s] \times [s] \to$ Truth.

5.1 Variant Narrowing

We have modified the variant narrowing of [9] and give its new definition here.

Definition 10 (Preorder and equivalence of narrowing steps). *[9] Let $\mathcal{R} = (\Sigma, B, \Delta)$ be a decomposition of an equational theory. Let us consider two narrowing steps $\alpha_1 : t \rightsquigarrow_{\sigma_1,\Delta,B} s_1$ and $\alpha_2 : t \rightsquigarrow_{\sigma_2,\Delta,B} s_2$. We write $\alpha_1 \sqsubseteq_B \alpha_2$ if $\sigma_1|_{Var(t)} \sqsubseteq_B \sigma_2|_{Var(t)}$ and $\alpha_1 \sqsubset_B \alpha_2$ if $\sigma_1|_{Var(t)} \sqsubset_B \sigma_2|_{Var(t)}$ (i.e., σ_2 is strictly more general than σ_1). We write $\alpha_1 \approx_B \alpha_2$ if $\sigma_1|_{Var(t)} \approx_B \sigma_2|_{Var(t)}$. The relation $\alpha_1 \approx_B \alpha_2$ between two narrowing steps from t defines a set of equivalence classes between such narrowing steps. In what follows we will choose a unique representation $\underline{\alpha} \in [\alpha]_{\approx_B}$ in each equivalence class of narrowing steps from t. Therefore, $\underline{\alpha}$ will always denote a chosen unique representative $\underline{\alpha} \in [\alpha]_{\approx_B}$.*

Definition 11 (Variant Narrowing). *Let $\mathcal{R} = (\Sigma, B, \Delta)$ be a decomposition of an equational theory. We define $t \overset{vn}{\rightsquigarrow}_{p,\theta,\Delta,B} t'$ as $\underline{\alpha} : t \rightsquigarrow_{p,\theta,\Delta,B} t'$ such that $(t\theta)|_p$ has a Δ, B–pattern, $\underline{\alpha}$ is maximal w.r.t. the order $\sqsubseteq_B$, and $\underline{\alpha}$ is a chosen unique representative of its $\approx_B$-equivalence class.*

Note that the substitution θ at each variant narrowing step $t \overset{vn}{\rightsquigarrow}_{p,\theta,\Delta,B} t'$ is Δ, B-normalized, since $(t\theta)|_p$ has a Δ, B–pattern.

Variant narrowing is obviously sound, as any step $t \overset{vn}{\rightsquigarrow}_\sigma t'$ can be performed by rewriting, i.e., $t\sigma \to t'$. Completeness follows from the fact that any Δ, B-pattern rewriting sequence can be lifted to a narrowing sequence by Theorem 2 and such narrowing sequence is generated by variant narrowing.

Theorem 3 (Completeness of Variant Narrowing). *Let $\mathcal{R} = (\Sigma, B, \Delta)$ be a decomposition of an equational theory. Let $[\![t]\!]^{\overset{vn}{\rightsquigarrow}}_{\Delta,B} = \{(t', \theta) \mid t \overset{vn*}{\rightsquigarrow}_{\theta,\Delta,B} t' \text{ and } t' = t'{\downarrow_{\Delta,B}}\}$. Then $[\![t]\!]_{\Delta,B} \simeq_{\Delta,B} [\![t]\!]^{\overset{vn}{\rightsquigarrow}}_{\Delta,B}$.*

Example 4. Using the theory from our running example, Example 2, for $t = X \oplus Y$ we get the following steps with variant narrowing: (i) $t \overset{vn}{\rightsquigarrow}_{\phi_1} Z$, with $\phi_1 = \{X \mapsto 0, Y \mapsto Z\}$, (ii) $t \overset{vn}{\rightsquigarrow}_{\phi_2} Z$, with $\phi_2 = \{X \mapsto Z, Y \mapsto 0\}$, (iii) $t \overset{vn}{\rightsquigarrow}_{\phi_3} Z$, with $\phi_3 = \{X \mapsto Z \oplus U, Y \mapsto U\}$, (iv) $t \overset{vn}{\rightsquigarrow}_{\phi_4} Z$, with $\phi_4 = \{X \mapsto U, Y \mapsto Z \oplus U\}$, (v) $t \overset{vn}{\rightsquigarrow}_{\phi_5} 0$, with $\phi_5 = \{X \mapsto U, Y \mapsto U\}$, (vi) $t \overset{vn}{\rightsquigarrow}_{\phi_6} Z_1 \oplus Z_2$, with $\phi_6 = \{X \mapsto U \oplus Z_1, Y \mapsto U \oplus Z_2\}$. There are no further steps possible from (i)-(v) as any instantiation of Z for which a narrowing step is possible would mean that the substitution is not normalized. On the other hand, with the result of (vi), $Z_1 \oplus Z_2$, we are back at the beginning and can repeat all of the steps possible for t. Obviously variant narrowing does not terminate for term t.

5.2 Variant Narrowing vs. Basic narrowing

In this section we show that variant narrowing and basic narrowing are incomparable, that is, it is not the case that one of them subsumes the other.

Definition 12 (Basic narrowing). *[14] Let $\mathcal{R} = (\Sigma, \emptyset, R)$ be an order-sorted rewrite theory. Given a term $t \in \mathcal{T}_\Sigma(\mathcal{X})$ and a substitution ρ, a basic narrowing step for $\langle t, \rho\rangle$ is defined by $\langle t, \rho\rangle \overset{b}{\rightsquigarrow}_{p,\theta,\mathcal{R}} \langle t', \rho'\rangle$ if there exist $p \in Pos_\Sigma(t)$, a (possibly renamed) rule $l \to r$ in Δ, and substitution θ such that $\theta = mgu(t|_p\rho, l)$, $t' = (t[r]_p)$, and $\rho' = \rho\theta$.*

Example 5. The narrowing sequence shown in Example 1 is not a basic AC-narrowing sequence, i.e., w.r.t. the extension of basic narrowing to AC where we just replace syntactic unification by AC-unification, as after the first step it results in $\langle x, \rho_1 \rangle$ and no further basic AC-narrowing step is possible.

The following example shows that basic narrowing may be non-terminating in cases when variant narrowing does terminate.

Example 6. Consider the rewrite theory $(\Sigma, \emptyset, \Delta)$, the set of convergent rules $\Delta = \{f(x) \to x, f(f(x)) \to f(x)\}$, and the term $t = f(x)$. Basic narrowing performs the following two narrowing steps (i) $f(x) \overset{b}{\leadsto}_{id,\Delta} x$ and (ii) $f(x) \overset{b}{\leadsto}_{\sigma,\Delta} f(x')$ with $\sigma = \{x/f(x')\}$. However, the second narrowing step leads to the following non-terminating basic narrowing sequence

$$f(x) \overset{b}{\leadsto}_{\{x/f(x')\},\Delta} f(x') \overset{b}{\leadsto}_{\{x'/f(x'')\},\Delta} f(x'') \cdots$$

Variant narrowing will perform only the narrowing step (i), since the narrowing step (ii) contains a non-normalized substitution, and thus variant narrowing does not produce the non-terminating narrowing sequence.

However, since the variant narrowing strategy does not carry any history of computed terms or substitutions, it is not able to avoid some useless narrowing sequences, whereas basic narrowing will avoid any of those sequences from the very beginning by avoiding narrowing inside the substitutions. The following example shows that variant narrowing may be non-terminating in cases when basic narrowing does terminate.

Example 7. Now, consider the rewrite theory $(\Sigma, \emptyset, \Delta)$, the set of convergent rules $\Delta = \{f(f(x)) \to x\}$, and the term $t = c(f(x), x)$ where $c \in \Sigma$. Basic narrowing performs only $c(f(x), x) \overset{b}{\leadsto}_{\sigma,\Delta} c(x', f(x'))$ with $\sigma = \{x/f(x')\}$ and it stops, since the term $f(x')$ is introduced by a substitution. However, variant narrowing will perform the following non-terminating narrowing sequence

$$c(f(x), x) \overset{vn}{\leadsto}_{\theta_1,\Delta} c(x_1, f(x_1)) \overset{vn}{\leadsto}_{\theta_2,\Delta} c(f(x_2), x_2) \cdots$$

with $\theta_1 = \{x/f(x_1)\}$, $\theta_{i+1} = \{x_i/f(x_{i+1})\}$, since every of the individual unifiers is normalized, though the composition $\theta_1 \cdots \theta_{i+1}$ is non-normalized.

5.3 Variant Narrowing with History

The problem of variant narrowing is that it performs some narrowing sequences that are not a lifting of some concrete Δ, B–pattern sequence because variant narrowing does not keep a history of the substitution computed so far, as basic narrowing does. We improve on variant narrowing in this section, by making it history-sensitive, as basic narrowing is.

Definition 13 (Variant Narrowing with History). *Let $\mathcal{R} = (\Sigma, B, \Delta)$ be a decomposition of an equational theory. We say $\langle t \mid \rho \rangle \overset{vnh}{\leadsto}_{p,\theta,\Delta,B} \langle t' \mid \rho' \rangle$ iff (i) $t \overset{vn}{\leadsto}_{p,\theta,\Delta,B} t'$, (ii) $\rho' = \rho(\theta|_{Var(t)})$, and (iii) ρ' is $\to_{\Delta,B}$-normalized.*

Soundness of variant narrowing with history is obvious as it is just a further restriction of variant narrowing. The proof of completeness is identical to the proof of Theorem 3, since we just simply remove narrowing sequences that do not correspond to Δ, B–pattern sequences.

Theorem 4 (Completeness of Variant Narrowing with History). *Let $\mathcal{R} = (\Sigma, B, \Delta)$ be a decomposition of an equational theory. Let $[\![t]\!]^{\overset{vnh}{\rightsquigarrow}}_{\Delta,B} = \{(t', \theta) \mid \langle t \mid id\rangle \overset{vnh}{\rightsquigarrow}^*_{\theta,\Delta,B} \langle t' \mid \theta\rangle$ and $t' = t'{\downarrow_{\Delta,B}}\}$. Then $[\![t]\!]_{\Delta,B} \simeq_{\Delta,B} [\![t]\!]^{\overset{vnh}{\rightsquigarrow}}_{\Delta,B}$.*

Example 8. Using the theory from our running example, Example 2, and the substitutions ϕ_i from Example 4, for $t = X \oplus Y$ we get the following steps with variant narrowing with history, starting from $\langle t \mid id\rangle$: (i) $\langle t \mid id\rangle \overset{vnh}{\rightsquigarrow}_{\phi_1} \langle Z \mid \phi_1\rangle$, (ii) $\langle t \mid id\rangle \overset{vnh}{\rightsquigarrow}_{\phi_2} \langle Z \mid \phi_2\rangle$, (iii) $\langle t \mid id\rangle \overset{vnh}{\rightsquigarrow}_{\phi_3} \langle Z \mid \phi_3\rangle$, (iv) $\langle t \mid id\rangle \overset{vnh}{\rightsquigarrow}_{\phi_4} \langle Z \mid \phi_4\rangle$, (v) $\langle t \mid id\rangle \overset{vnh}{\rightsquigarrow}_{\phi_5} \langle 0 \mid \phi_5\rangle$, (vi) $\langle t \mid id\rangle \overset{vnh}{\rightsquigarrow}_{\phi_6} \langle Z_1 \oplus Z_2 \mid \phi_6\rangle$. There are no further steps possible from (i)-(v) as any instantiation of Z for which a narrowing step is possible would mean that the substitution is not normalized. On the other hand, with the result of (vi), $\langle Z_1 \oplus Z_2 \mid \phi_6\rangle$, we are not quite back at the start as we cannot do the steps similar to (i), (ii), and (v) again, but we can repeat the steps (up to renamings with larger substitutions) similar to (iii), (iv), and (vi). Obviously variant narrowing with history does not terminate for term t either.

As variant narrowing with history does not terminate even though the theory has the finite variant property, as shown in [8], we will continue to improve on the termination properties of our variant narrowing by applying further restrictions in Section 5.5.

5.4 Variant Narrowing with History vs. Basic Narrowing

In this section, we first argue that variant narrowing with history does indeed subsume basic narrowing. We also see, using Example 6, that variant narrowing with history is able to terminate in some cases where basic narrowing does not.

The following example shows that variant narrowing may be non-terminating in cases when basic narrowing does terminate but variant narrowing with history does indeed terminate, whenever basic narrowing does.

Example 9. Consider the rewrite theory $(\Sigma, \emptyset, \Delta)$, and the term $t = c(f(x), x)$ of Example 7. Basic narrowing performs only $c(f(x), x) \overset{b}{\rightsquigarrow}_{\sigma,\Delta} c(x', f(x'))$ with $\sigma = \{x \mapsto f(x')\}$ and it stops, since the term $f(x')$ is introduced by a substitution. Variant narrowing with history will similarly only perform the first step,

$$\langle c(f(x), x) \mid id\rangle \overset{vnh}{\rightsquigarrow}_{\sigma,\Delta} \langle c(x_1, f(x_1)) \mid \sigma\rangle$$

since the second step would result in the substitution $\{x \mapsto f(f(x''))\}$ which is not normalized and thus variant narrowing with history will not perform that step.

Essentially, variant narrowing with history is a subrelation of basic narrowing.

Proposition 2 (Sub-relation). *Let $\mathcal{R} = (\Sigma, \emptyset, R)$ be an order-sorted rewrite theory. Then, $\langle t\phi \mid \phi\rangle \overset{vnh}{\rightsquigarrow}_\theta \langle t'\phi' \mid \phi'\rangle$ implies $\exists u, \rho$ s.t. $\langle t, \phi\rangle \overset{b}{\rightsquigarrow}_\theta \langle u, \rho\rangle$, $\phi' = \rho|_{Var(t)}$, and $u\rho =_B t'\phi'$.*

Proof. By contradiction. Let us assume that $\langle t\phi \mid \phi\rangle \overset{vnh}{\rightsquigarrow}_{p,\theta} \langle t'\phi' \mid \phi'\rangle$ but there are no u, ρ s.t. $\langle t, \phi\rangle \overset{b}{\rightsquigarrow}_\theta \langle u, \rho\rangle$, $\phi' = \rho|_{Var(t)}$, and $u\rho =_B t'\phi'$. Since ϕ and ϕ' are Δ, B-normalized by definition of variant narrowing with history, then there is a unifier of $t|_p$ and lhs l which is available also for basic narrowing. Then, the conclusion follows. □

However, not all the narrowing sequences of variant narrowing with history are basic narrowing sequences, since basic narrowing simulates only innermost rewriting sequences and variant narrowing with history does not. Therefore, we improve the variant narrowing with history strategy in the following section.

5.5 Δ, B–pattern Narrowing with History

Definition 14 (Δ, B–pattern Narrowing with history). *Given a decomposition $\mathcal{R} = (\Sigma, B, \Delta)$ of an equational theory. Let t be a term, ϕ a substitution and L a sequence of terms, with nil being the empty sequence. We write $\langle t \mid \rho \mid L\rangle \overset{vph}{\rightsquigarrow}_{p,\theta,\Delta,B} \langle t' \mid \rho' \mid (L, t|_p)\theta\rangle$ iff (i) $\langle t \mid \rho\rangle \overset{vnh}{\rightsquigarrow}_{p,\theta,\Delta,B} \langle t' \mid \rho'\rangle$, and (ii) each term in $(L, t|_p)\theta$ has a Δ, B–pattern.*

Δ, B–pattern narrowing with history is sound as it is a further restriction of variant narrowing with history.

Again, the proof of completeness is identical to the proof of Theorem 4, since we just simply remove narrowing sequences that do not correspond to Δ, B–pattern sequences.

Theorem 5 (Completeness of Δ, B–pattern Narrowing with history). *Let $\mathcal{R} = (\Sigma, B, \Delta)$ be a decomposition of an equational theory. Let $[\![t]\!]^{\overset{vph}{\rightsquigarrow}}_{\Delta,B} = \{(t', \theta) \mid \langle t \mid id \mid nil\rangle \overset{vph*}{\rightsquigarrow}_{\theta,\Delta,B} \langle t' \mid \theta \mid L\rangle$ and $t' = t'{\downarrow_{\Delta,B}}\}$. Then $[\![t]\!]_{\Delta,B} \simeq_{\Delta,B} [\![t]\!]^{\overset{vph}{\rightsquigarrow}}_{\Delta,B}$.*

Example 10. Using the theory from our running example, Example 2, and the substitutions ϕ_i from Example 8, for $t = X \oplus Y$ we get the following steps with Δ, B–pattern narrowing with history, starting from $\langle t \mid id \mid nil\rangle$: (i) $\langle t \mid id \mid nil\rangle \overset{vph}{\rightsquigarrow}_{\phi_1} \langle Z \mid \phi_1 \mid t\phi_1\rangle$, (ii) $\langle t \mid id \mid nil\rangle \overset{vph}{\rightsquigarrow}_{\phi_2} \langle Z \mid \phi_2 \mid t\phi_2\rangle$, (iii) $\langle t \mid id \mid nil\rangle \overset{vph}{\rightsquigarrow}_{\phi_3} \langle Z \mid \phi_3 \mid t\phi_3\rangle$, (iv) $\langle t \mid id \mid nil\rangle \overset{vph}{\rightsquigarrow}_{\phi_4} \langle Z \mid \phi_4 \mid t\phi_4\rangle$, (v) $\langle t \mid id \mid nil\rangle \overset{vph}{\rightsquigarrow}_{\phi_5} \langle 0 \mid \phi_5 \mid t\phi_5\rangle$, (vi) $\langle t \mid id \mid nil\rangle \overset{vph}{\rightsquigarrow}_{\phi_6} \langle Z_1 \oplus Z_2 \mid \phi_6 \mid t\phi_6\rangle$. There are no further steps possible from (i)-(v) as any instantiation of Z for which a narrowing step is possible would mean that the substitution is not normalized. On the other hand, with the result of (vi), $\langle Z_1 \oplus Z_2 \mid \phi_6 \mid t\phi_6\rangle$, we are not quite back at the beginning as we cannot do the steps similar to (i), (ii), and (v) again, but we can repeat the steps (up to renamings with larger substitution) similar to (iii), (iv), and (vi):

- (iii'): $\langle Z_1 \oplus Z_2 \mid \phi_6 \mid t\phi_6\rangle \overset{vph}{\rightsquigarrow}_{\tau_3} \langle Z \mid \phi_6\tau_3 \mid (t\phi_6\tau_3, (Z_1 \oplus Z_2)\tau_3)\rangle$ with $\tau_3 = \{Z_1 \mapsto Z \oplus U', Z_2 \mapsto U'\}$, where obviously $t\phi_6\tau_3$ and $(Z_1 \oplus Z_2)\tau_3$ have a Δ, B–pattern.
- Similar for (iv').
- (vi'): $\langle Z_1 \oplus Z_2 \mid \phi_6 \mid t\phi_6\rangle \overset{vph}{\rightsquigarrow}_{\tau_6} \langle Z_1' \oplus Z_2' \mid \phi_6\tau_6 \mid (t\phi_6\tau_6, (Z_1 \oplus Z_2)\tau_6\rangle)$ with $\tau_6 = \{Z_1 \mapsto U' \oplus Z_1', Z_2 \mapsto U' \oplus Z_2'\}$, and this step can be repeated infinitely often. Note that $t\phi_6\tau_6$ as well as $(Z_1 \oplus Z_2)\tau_6$ have a Δ, B–pattern, and actually all further such instantiations and added terms in that list will have Δ, B–patterns.

Obviously Δ, B–pattern narrowing with history does not terminate for term t either.

This motivates adding a further restriction to Δ, B–pattern narrowing with history in Section 5.7, under which it will actually terminate for a range of theories as wide as possible, in particular also for this example.

5.6 Δ, B–pattern Narrowing with History vs. Basic Narrowing

For $B = \emptyset$, variant narrowing with history is a sub-relation of basic narrowing but the same result does not apply for sequences. Δ, B–pattern narrowing with history rectifies this issue.

Proposition 3 (Inclusion of narrowing sequences). *Let $\mathcal{R} = (\Sigma, \emptyset, R)$ be an order-sorted rewrite theory. Let t be a term and V be a set of variables such that $Var(t) \subseteq V$. Then, $\langle t \mid id \mid nil\rangle \overset{vph}{\rightsquigarrow}{}^{*}_{\theta} \langle t'\phi \mid \phi \mid L\rangle$ implies $\langle t, id\rangle \overset{b}{\rightsquigarrow}{}^{*}_{\theta} \langle t', \rho\rangle$ and $\phi = \theta|_V = \rho|_V$.*

Proof. By Proposition 2 and the fact that the rewrite sequence $t\phi \rightarrow^{*} t'\phi$ associated to the narrowing sequence computed by Δ, B–pattern with history corresponds to an innermost rewriting sequence and, thus, is lifted by a valid basic narrowing sequence. □

5.7 Δ, B–pattern Narrowing with History and Folding

As we have seen in Example 10, infinite sequences may be due to looping by narrowing that always computes the same variant, independently of the length. We have developed in [7] a way of detecting such useless loops that we reuse in this paper.

Definition 15 (Transition System). *[7] A* transition system *is written $\mathcal{A} = (A, \rightarrow)$, where A is a set of states, and $\rightarrow$ is a transition relation between states, i.e., $\rightarrow \subseteq A \times A$. We write $\mathcal{A} = (A, \rightarrow, I)$ when $I \subseteq A$ is a set of initial states.*

Definition 16 (Folding Reachable Transition Subsystem). *[7] Given $\mathcal{A} = (A, \rightarrow, I)$ and a relation $G \subseteq A \times A$, the reachable subsystem from I in A with folding G is written $\mathcal{R}each^{G}_{\mathcal{A}}(I) = (Reach^{G}_{\rightarrow}(I), \rightarrow^{G}, I)$, where*

$$
\begin{array}{l}
Reach^{G}_{\rightarrow}(I) = \bigcup_{n\in\mathbb{N}} Frontier^{G}_{\rightarrow}(I)_n,\\
Frontier^{G}_{\rightarrow}(I)_0 = I,\\
Frontier^{G}_{\rightarrow}(I)_{n+1} = \{y \in A \mid (\exists z \in Frontier^{G}_{\rightarrow}(I)_n : z \rightarrow y) \wedge \\
\qquad\qquad\qquad\qquad (\nexists k \leq n, w \in Frontier^{G}_{\rightarrow}(I)_k : y\ G\ w)\},\\
\rightarrow^{G} = \bigcup_{n\in\mathbb{N}} \rightarrow^{G}_{n+1},\\
x \rightarrow^{G}_{n+1} y \begin{cases} \text{if } x \in Frontier^{G}_{\rightarrow}(I)_n, y \in Frontier^{G}_{\rightarrow}(I)_{n+1}, x \rightarrow y; \text{ or} \\ \text{if } x \in Frontier^{G}_{\rightarrow}(I)_n, y \notin Frontier^{G}_{\rightarrow}(I)_{n+1}, \\ \quad \exists k \leq n : y \in Frontier^{G}_{\rightarrow}(I)_k, \exists w : (x \rightarrow w \wedge w\ G\ y) \end{cases}
\end{array}
$$

Note that, the more general the relation G, the greater the chances of $\mathcal{R}each^{G}_{\mathcal{A}}(I)$ being a finite transition system.

Definition 17 (Subsumption relation for pairs). *For terms $t, t' \in \mathcal{T}_{\Sigma}(\mathcal{X})$, substitutions ρ, ρ', and sequences L, L' of terms we write $\langle t \mid \rho \mid L\rangle \sqsubseteq_{\Delta,B} \langle t' \mid \rho' \mid L'\rangle$ iff $(t, \rho) \sqsubseteq_{\Delta,B} (t', \rho')$.*

Definition 18 (Δ, B–pattern Narrowing with History and Folding). *Let $\mathcal{R} = (\Sigma, B, \Delta)$ be a decomposition of an equational theory. Let t be a term, ρ a substitution, and L a sequence of terms, with nil being the empty sequence. We define $\langle t \mid \rho \mid L\rangle \overset{vpf}{\rightsquigarrow}{}^{k}_{\theta,\Delta,B} \langle t' \mid \rho' \mid L'\rangle$ if $\langle t \mid \rho \mid L\rangle \overset{vph}{\rightsquigarrow}{}^{k}_{\theta,\Delta,B} \langle t' \mid \rho' \mid L'\rangle$ and $\langle t' \mid \rho' \mid L'\rangle \in Frontier^{\sqsubseteq_{\Delta,B}}_{\overset{vph}{\rightsquigarrow}}(I)_n$ for the initial state $I = \{\langle t \mid \rho \mid L\rangle\}$.*

Note that by the use of the folding definition we only get the shortest paths to each possible term (depending on the substitution) as the longer paths are simply subsumed. Δ, B–pattern narrowing with history and folding is sound as it is a further restriction of Δ, B–pattern narrowing with history.

Theorem 6 (Completeness of Δ, B–pattern Narrowing with History and Folding). *Let $\mathcal{R} = (\Sigma, B, \Delta)$ be a decomposition of an equational theory. Let $[\![t]\!]^{vpf}_{\Delta,B} = \{(t', \theta) \mid \langle t \mid id \mid nil\rangle \overset{vpf}{\rightsquigarrow}{}^{*}_{\theta,\Delta,B} \langle t' \mid \theta \mid L\rangle$ and $t' = t'{\downarrow_{\Delta,B}}\}$. Then $[\![t]\!]_{\Delta,B} \simeq_{\Delta,B} [\![t]\!]^{vpf}_{\Delta,B}$.*

Combining Proposition 1 and Theorem 6 gives us a minimal and complete E-unification procedure that has a smaller search space, based on the Δ, B–pattern narrowing with history and folding strategy.

Example 11. Using the theory from our running example, Example 2, and the substitutions introduced in Examples 4 and 8, for $t = X \oplus Y$ we get the following steps with Δ, B–pattern narrowing with history and folding, starting from $\langle t \mid id \mid nil\rangle$: (i) $\langle t \mid id \mid nil\rangle \overset{vpf}{\rightsquigarrow}_{\phi_1} \langle Z \mid \phi_1 \mid t\phi_1\rangle$, (ii) $\langle t \mid id \mid nil\rangle \overset{vpf}{\rightsquigarrow}_{\phi_2} \langle Z \mid \phi_2 \mid t\phi_2\rangle$, (iii) $\langle t \mid id \mid nil\rangle \overset{vpf}{\rightsquigarrow}_{\phi_3} \langle Z \mid \phi_3 \mid t\phi_3\rangle$, (iv) $\langle t \mid id \mid nil\rangle \overset{vpf}{\rightsquigarrow}_{\phi_4} \langle Z \mid \phi_4 \mid t\phi_4\rangle$, (v) $\langle t \mid id \mid nil\rangle \overset{vpf}{\rightsquigarrow}_{\phi_5} \langle 0 \mid \phi_5 \mid t\phi_5\rangle$, (vi) $\langle t \mid id \mid nil\rangle \overset{vpf}{\rightsquigarrow}_{\phi_6} \langle Z_1 \oplus Z_2 \mid \phi_6 \mid t\phi_6\rangle$. There are no further steps possible from (i)-(v) as any instantiation of Z for which a narrowing step is possible would mean that the substitution is not normalized, as for variant narrowing with history. On the other hand, with the result of (vi), $\langle Z_1 \oplus Z_2 \mid \phi_6 \mid t\phi_6\rangle$, we cannot do the steps for (i), (ii), and (v) again, but we can look at the steps possible by Δ, B–pattern narrowing with history to (iii), (iv), and (vi) itself.

- (iii'): $\langle Z_1 \oplus Z_2 \mid \phi_6 \mid t\phi_6\rangle \overset{vpf}{\rightsquigarrow}_{\tau_3} \langle Z \mid \phi_6\tau_3 \mid t\phi_6\tau_3, (Z_1 \oplus Z_2)\tau_3\rangle$ but this step is actually subsumed for Δ, B–pattern narrowing with history and folding by (iii) with $\xi_3 = \{U \mapsto U \oplus U'\}$.
- (iv'): Similarly to (iii').
- (vi'): $\langle Z_1 \oplus Z_2 \mid \phi_6 \mid t\phi_6\rangle \overset{vpf}{\rightsquigarrow}_{\tau_6} \langle Z_1' \oplus Z_2' \mid \phi_6\tau_6 \mid t\phi_6\tau_6, (Z_1 \oplus Z_2)\tau_6\rangle$. But again, this is subsumed for Δ, B–pattern narrowing with history and folding, by (vi) itself this time, with $\xi_6 = \{U \mapsto U \oplus U', Z_1 \mapsto Z_1', Z_2 \mapsto Z_2'\}$.

Thus, Δ, B–pattern narrowing with history and folding *terminates* for t in the given rewrite theory, whereas variant narrowing, variant narrowing with history and Δ, B–pattern narrowing with history do not.

Our very final but the most interesting result follows from Theorem 2.

Corollary 2 (Variant Equivalence). *Let $\mathcal{R} = (\Sigma, B, \Delta)$ be a decomposition of an equational theory. Let t be a Δ, B-normalized term. Then $[\![t]\!]_{\Delta,B} \approx_B [\![t]\!]^{vpf}_{\Delta,B}$.*

This result triggers the idea of a narrowing strategy being *extremely terminating*, i.e., a narrowing strategy S enjoying completeness w.r.t. our variant semantics is extremely terminating iff whenever any other narrowing strategy S' enjoying the same completeness w.r.t. our variant semantics terminates on a term t, then S is guaranteed to terminate on t as well. Clearly, if strategy S satisfies $[\![t]\!]_{\Delta,B} \approx_B [\![t]\!]^{S}_{\Delta,B}$, then it is extremely terminating.

To the best of our knowledge, the notion of extremely terminating narrowing strategy has not been formulated before. It clarifies important questions such as the following: is basic narrowing, perhaps the narrowing strategy for which the most termination results are known, extremely terminating? As we show in Example 6, the answer is an emphatic *no* in the standard case $B = \emptyset$ where basic narrowing is complete.

Also, note that whenever $[\![t]\!]_{\Delta,B}$ is finite, Δ, B–pattern narrowing with history and folding *terminates* for t. Therefore, the notion of the finite variant property of a theory,

defined in [3], which essentially states that $[\![t]\!]_{\Delta,B}$ is finite for all terms, is also related to Δ, B–pattern narrowing with history and folding. Specifically, a theory has the finite variant property *if and only if* Δ, B–pattern narrowing with history and folding terminates on all input terms.

In a previous paper [8] we have given a sufficient condition to effectively check whether a theory has the finite variant property. Obviously this immediately translates into a method to prove termination of Δ, B–pattern narrowing with history and folding. However, a reformulation of the technique of [8] for the termination of Δ, B–pattern narrowing with history and folding is left for future work.

6 Conclusions

Narrowing modulo axioms B generalizes standard narrowing and greatly widens the range of applications of narrowing. But without good narrowing strategies many such applications easily become unfeasible. We have introduced the notion of an extremely terminating narrowing strategy, which terminates more often than any other equally complete strategy. And we have shown that Δ, B-pattern narrowing with history and folding is extremely terminating. We have also shown that the finite variant property is the weakest condition on a theory decomposition under which this strategy terminates on all input terms. Much work remains ahead, particularly at the implementation level. A cruder and much less search-space-efficient version of variant narrowing based on bounds has already been used quite effectively in the Maude-NPA tool [6] to analyze cryptographic protocols modulo nontrivial theories. We plan to implement the new Δ, B-pattern narrowing with history and folding strategy in the near future, which should clearly have a much smaller search space. Of course, extra computation will have to be done; but since it is based mainly on *B-matching* for the extra features such as Δ, B-patterns and folding, we expect the substantial gains in search space size to amply compensate for this extra computational cost.

References

1. M. Alpuente, S. Escobar, and J. Iborra. Modular termination of basic narrowing. In A. Voronkov, editor, *Rewriting Techniques and Applications, 19th International Conference, RTA 2008, Hagenberg, Austria, July 15-17, 2008, Proceedings*, volume 5117 of *Lecture Notes in Computer Science*, pages 1–16. Springer, 2008.
2. M. Alpuente, M. Falaschi, and G. Vidal. Partial Evaluation of Functional Logic Programs. *ACM Transactions on Programming Languages and Systems*, 20(4):768–844, 1998.
3. H. Comon-Lundh and S. Delaune. The finite variant property: How to get rid of some algebraic properties. In J. Giesl, editor, *Term Rewriting and Applications, 16th International Conference, RTA 2005, Nara, Japan, April 19-21, 2005, Proceedings*, volume 3467 of *Lecture Notes in Computer Science*, pages 294–307. Springer, 2005.
4. N. Dershowitz, S. Mitra, and G. Sivakumar. Decidable matching for convergent systems (preliminary version). In D. Kapur, editor, *CADE*, volume 607 of *Lecture Notes in Computer Science*, pages 589–602. Springer, 1992.
5. S. Escobar. Implementing natural rewriting and narrowing efficiently. In Y. Kameyama and P. J. Stuckey, editors, *7th International Symposium on Functional and Logic Programming (FLOPS 2004)*, volume 2998 of *Lecture Notes in Computer Science*, pages 147–162. Springer, 2004.
6. S. Escobar, C. Meadows, and J. Meseguer. A rewriting-based inference system for the NRL protocol analyzer and its meta-logical properties. *Theor. Comput. Sci.*, 367(1-2):162–202, 2006.

7. S. Escobar and J. Meseguer. Symbolic model checking of infinite-state systems using narrowing. In F. Baader, editor, *RTA*, volume 4533 of *Lecture Notes in Computer Science*, pages 153–168. Springer, 2007.
8. S. Escobar, J. Meseguer, and R. Sasse. Effectively checking the finite variant property. In A. Voronkov, editor, *RTA*, volume 5117 of *Lecture Notes in Computer Science*, pages 79–93. Springer, 2008.
9. S. Escobar, J. Meseguer, and R. Sasse. Variant narrowing and equational unification. In *Accepted at: 7th International Workshop on Rewriting Logic and its Applications*, 2008.
10. S. Escobar, J. Meseguer, and P. Thati. Natural narrowing for general term rewriting systems. In J. Giesl, editor, *Term Rewriting and Applications, 16th International Conference, RTA 2005, Nara, Japan, April 19-21, 2005, Proceedings*, volume 3467 of *Lecture Notes in Computer Science*, pages 279–293. Springer, 2005.
11. J. Giesl and D. Kapur. Dependency pairs for equational rewriting. In A. Middeldorp, editor, *RTA*, volume 2051 of *Lecture Notes in Computer Science*, pages 93–108. Springer, 2001.
12. J. A. Goguen and J. Meseguer. Equality, types, modules, and (why not ?) generics for logic programming. *J. Log. Program.*, 1(2):179–210, 1984.
13. M. Hanus. The Integration of Functions into Logic Programming: From Theory to Practice. *Journal of Logic Programming*, 19&20:583–628, 1994.
14. S. Hölldobler. *Foundations of Equational Logic Programming*, volume 353 of *Lecture Notes in Artificial Intelligence*. Springer-Verlag, Berlin, 1989.
15. J.-M. Hullot. Canonical forms and unification. In W. Bibel and R. A. Kowalski, editors, *CADE*, volume 87 of *Lecture Notes in Computer Science*, pages 318–334. Springer, 1980.
16. J.-P. Jouannaud, C. Kirchner, and H. Kirchner. Incremental construction of unification algorithms in equational theories. In J. Díaz, editor, *ICALP*, volume 154 of *Lecture Notes in Computer Science*, pages 361–373. Springer, 1983.
17. J.-P. Jouannaud and H. Kirchner. Completion of a set of rules modulo a set of equations. *SIAM J. Comput.*, 15(4):1155–1194, 1986.
18. D. Kapur and P. Narendran. Matching, Unification and Complexity. *ACM SIGSAM Bulletin*, 21(4):6–9, 1987.
19. J. Meseguer. Conditional rewriting logic as a united model of concurrency. *Theor. Comput. Sci.*, 96(1):73–155, 1992.
20. J. Meseguer. Membership algebra as a logical framework for equational specification. In F. Parisi-Presicce, editor, *WADT*, volume 1376 of *Lecture Notes in Computer Science*, pages 18–61. Springer, 1997.
21. J. Meseguer and P. 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.
22. A. Middeldorp and E. Hamoen. Completness results for basic narrowing. *Journal of Applicable Algebra in Engineering, Communication, and Computing*, 5:213–253, 1994.
23. S. Mitra. *Semantic Unification for Convergent Rewrite Systems*. PhD thesis, University Illinois at Urbana-Champaign, 1994.
24. G. E. Peterson and M. E. Stickel. Complete sets of reductions for some equational theories. *J. ACM*, 28(2):233–264, 1981.
25. TeReSe, editor. *Term Rewriting Systems*. Cambridge University Press, Cambridge, 2003.
26. E. Viola. E-unifiability via narrowing. In A. Restivo, S. R. D. Rocca, and L. Roversi, editors, *ICTCS*, volume 2202 of *Lecture Notes in Computer Science*, pages 426–438. Springer, 2001.
27. P. Viry. Equational rules for rewriting logic. *Theor. Comput. Sci.*, 285(2):487–517, 2002.