Reviving Basic Narrowing Modulo

Dohan Kim[1], Christopher Lynch[1(✉)], and Paliath Narendran[2]

[1] Clarkson University, Potsdam, USA
{dohkim,clynch}@clarkson.edu
[2] University at Albany, SUNY, Albany, USA
pnarendran@albany.edu

Abstract. We define an inference rule called the Parallel rule. Given a rewrite system R and an equational theory E, where R is E-convergent modulo, we show that if R is saturated under the Parallel rule then Basic Narrowing modulo E is complete for R. If R is finitely saturated under both Parallel and Forward Overlap then Basic Narrowing, with right hand side abstracted, is complete and terminates, and thus it is a decision procedure for unification modulo $R \cup E$. We give examples, such as the theory of XOR, the theory of abelian groups and Associativity with a unit element. We also show that R has the finite variant property modulo E if and only if R can be finitely saturated under Parallel and Forward Overlap, provided that E unification is finitary.

Keywords: Basic Narrowing · E-unification · Finite Variant Property

1 Introduction

If an equational theory can be represented as a convergent rewrite system R, then rewriting with R decides the word problem. However, some equations cannot be oriented into rewrite rules, such as Associativity and Commutativity. Then we may be able to split the equational theory into a rewrite system R and a set of equations E where R is E-convergent, which also decides the word problem.

Narrowing lifts rewriting to solve unification problems. Narrowing with R modulo E produces a complete set of unifiers for the $R \cup E$ unification problem if R is E-convergent [10]. This is useful for applications such as Cryptographic Protocol Analysis [7,8]. Unfortunately, Narrowing modulo E rarely halts, so it is not practical to use. Basic Narrowing is a modification of Narrowing, where unification problems are stored as constraints, rather than solving them immediately. Narrowing may not take place inside a constraint, so Basic Narrowing is more likely to halt. Unfortunately, Basic Narrowing modulo E is non-terminating for many equational theories, and, even worse, it is not complete, i.e., it may not produce a complete set of unifiers [5]. Because of these flaws it has been mostly abandoned, in favor of other Narrowing methods such as Variant Narrowing [9].

This paper is our attempt to revive Basic Narrowing modulo. We create a new inference rule, called the Parallel rule. If R is saturated by the Parallel rule, we

A. Herzig and A. Popescu (Eds.): FroCoS 2019, LNAI 11715, pp. 313–329, 2019.
https://doi.org/10.1007/978-3-030-29007-8_18

show that Basic Narrowing modulo E is complete. We show that if R is finitely saturated under both Parallel and Forward Overlap then Basic Narrowing with Right Hand Side Abstracted (meaning that right hand sides of rewrite rules are assumed to be reduced) is both complete and terminating, which is necessary for applications. This gives a decision procedure for unification. These inference rules are practical, as we illustrate with examples such as the theory of Exclusive OR and the theory of Abelian groups, where the saturation under these inference rules produces very few additional rewrite rules. In fact we show that a rewrite system R can be finitely saturated by Parallel and Forward Overlap w.r.t. a finitary E if and only if R has the Finite Variant Property modulo E (see also [4] for a similar result in the empty theory).

Basic Narrowing modulo was shown to be incomplete [5] for the following AC-convergent rewrite system R_1:

1. $x + 0 \rightarrow x$
2. $a + a \rightarrow 0$
3. $b + b \rightarrow 0$
4. $a + a + x \rightarrow x$
5. $b + b + x \rightarrow x$

where $+$ is an AC symbol with an identity element 0, x is a variable, and a and b are constants. The $R_1 \cup AC$-unification problem $y + z \approx^?_{R_1 \cup AC} 0$ has a solution $\{y \mapsto a + b, z \mapsto a + b\}$, which cannot be found with Basic Narrowing. A Basic Narrowing step with the fourth rule gives $x \approx^?_{R_1 \cup AC} 0$, with a constraint of $y + z \approx_{AC} a + a + x$. One solution of this constraint is $x \mapsto u + v, y \mapsto a + u, z \mapsto a + v$. If we could Narrow into the constraint, corresponding to a Narrowing step at the variable position x, with $b + b \rightarrow 0$ then this problem would be solved, but Basic Narrowing does not allow that, and there is no other way to solve this problem. To solve this problem in this paper, we define an inference rule called Parallel (or E-Parallel and more specifically AC-Parallel). It combines the parallel steps from rules 4 and 3 into one rewrite rule $a + a + b + b \rightarrow 0$. It also creates the extension of this rule $a + a + b + b + x \rightarrow x$. (We sometimes leave out parentheses for AC formulas, when they are not important.) After adding these two additional rules, Basic Narrowing is complete.

To motivate the Forward Overlap rule, let $R_2 = \{h(x) * h(y) \rightarrow h(x * y)\}$. For the purposes of this example, it doesn't matter whether the $*$ and $+$ symbol are free or are associative and commutative. The forward Overlap rule combines two rewrite steps into one. An application of Forward Overlap gives a new rewrite rule $h(h(x)) * h(h(y)) \rightarrow h(h(x * y))$. This process can be repeated an infinite number of times in this particular example.

The Forward Overlap rule is not applicable for R_1. So a form of Narrowing called Basic Narrowing with Right Hand Side Abstracted (BNR) is complete for R_1. In R_1 it was only necessary to add two rewrite rules to make it complete for BNR. In other examples, such as R_2 it takes infinitely many new rewrite rules. But there are many practical examples like R_1 where very few rewrite rules are needed.

We give examples to show that saturation under Parallel and Forward Overlap can often be accomplished by adding just a few rules, in theories such as Exclusive OR and Abelian group theory. We also show that a theory can be finitely saturated by Parallel and Forward Overlap if and only if that theory has the Finite Variant Property, provided that the E unification problem is finitary.

In particular, we show that a rewrite system is saturated by Parallel if and only if every innermost redex can be reduced with an instance of a rule mapping all variables in the right hand side to terms in normal form (IRR). This implies that Basic Narrowing is complete. We also show that a rewrite system is saturated by Parallel and Forward Overlap if and only if every innermost redex can be reduced to normal form in one step (IR1). This implies that Basic Narrowing with Right Hand Side Abstracted is complete, which in turn implies a property we call the Finite Constraint Property, which is a generalization of the Finite Variant Property, to also handle equational theories with an infinitary unification problem, such as the theory of Associativity. If the unification problem is finitary, this is equivalent to the Finite Variant Property (FVP), which in turn implies IR1.

2 Preliminaries

We use standard notation of term rewriting [1,3,6,11] and equational unification [2]. We use the usual definition of substitution. If σ is a substitution and V is a set of variables, then $\sigma|_V$ is the restriction of σ to the variables of V. We say a substitution θ *extends* a substitution σ if $\theta|_{Dom(\sigma)} = \sigma$, where $Dom(\sigma) = \{x \mid x\sigma \neq x\}$. A *complete set of E-unifiers* of an E-unification problem Γ is a set of substitutions, denoted by $CSU_E(\Gamma)$, such that each element of $CSU_E(\Gamma)$ is an E-unifier of Γ and for each E-unifier θ of Γ, there exists some $\sigma \in CSU_E(\Gamma)$ such that $\sigma \leq_E^V \theta$, where V is the set of variables of Γ. An ordering has the *subterm property* no term t is greater than a proper subterm of t. A reduction ordering $>$ is E-compatible if $s' \approx_E s > t \approx_E t'$ implies $s' > t'$ for all s, s', t and t'.

Given a rewrite system R and a set of equations E, denoted by (R, E), the relation $\rightarrow_{R,E}$ on $T(\Sigma, V)$ is defined by $s \rightarrow_{R,E} t$ (or more specifically $s \xrightarrow{p}_{R,E} t$) iff there is a non-variable position $p \in \mathcal{FP}os(s)$, a rewrite rule $l \rightarrow r \in R$, and a substitution σ such that $s|_p \approx_E l\sigma$ and $t = s[r\sigma]_p$. The relation $\rightarrow_{R,E}$ is decidable whenever E-matching is decidable. The transitive and reflexive closure of $\rightarrow_{R,E}$ is denoted by $\xrightarrow{*}_{R,E}$. We say that a term t is R, E*-irreducible* (or in R, E-normal form) if there is no term t' such that $t \rightarrow_{R,E} t'$. If $s \xrightarrow{*}_{R,E} t$ and t is R, E-irreducible, we say that t is a *reduced form* of s (or a *normal form* of s), denoted by $t = s{\downarrow}_{R,E}$. E is *regular* if $Var(s) = Var(t)$ for all $s \approx t$ in E.

A substitution σ is called R, E*-reduced* if $x\sigma$ is R, E-irreducible for all $x \in V$. We say that a term t is an *innermost redex* of R, E iff t is R, E-reducible only at the top position. Let $s \rightarrow t$ be a rewrite rule. Let θ be a substitution. The instance $s\theta \rightarrow t\theta$ is a *right-reduced instance* if $x\theta$ is in normal form for all variables x in t. Note that $t\theta$ may or may not be reduced.

The rewrite system (R, E) is *Church-Rosser modulo E* if for all terms s and t with $s =_E t$, there are terms u and v such that $s \xrightarrow{*}_{R,E} u =_E v \xleftarrow{*}_{R,E} t$.

The rewrite system (R, E) is *convergent modulo E* if (R, E) is Church-Rosser modulo E and $\leftrightarrow_E \circ \rightarrow_R \circ \leftrightarrow_E$ is well-founded. In this paper, we simply say that the rewrite system R is *R, E-convergent* (or *E-convergent*) if the rewrite system (R, E) is *convergent modulo E.*

3 Inference Rules on the Rewrite System

Throughout the paper, we assume E is a regular equational theory, and R is an E-convergent rewrite theory, under an E-compatible reduction ordering with the subterm property, so we will not explicitly state this in the theorems.

We give an inference rule called Parallel (or E-Parallel) which is a key contribution of this paper. This is the rule that needs to be added to make Basic Narrowing complete modulo an equational theory. It can be viewed as a non-critical overlap below a variable position, but only in very specific cases. The example in the introduction gives an idea where the name comes from. The purpose of the rule is to ensure that every innermost redex can be reduced by an instance of a rewrite rule where substitutions to variables on the right hand side are reduced.

E-Parallel

$$\frac{s \rightarrow t \qquad l \rightarrow r \qquad v \approx u[l']}{v\sigma \rightarrow v'}$$

where

1. $s \rightarrow t \in R$
2. $l \rightarrow r \in R$
3. $v \approx u[l'] \in E$
4. l' is a strict subterm of u and is not a variable
5. $\sigma \in CSU_E(l \approx^?_E l',\ u \approx^?_E s)$
6. v' is some normal form of $v\sigma$
7. t contains a variable x, where $l'\sigma$ is E-equivalent to a subterm of $x\sigma$

Definition 1. The above Parallel inference rule is *redundant* if either

1. for all s' such that $s' \approx_E s\sigma$, a strict subterm of s' is R, E-reducible, or
2. $s\sigma$ is R, E-reducible by a right-reduced instance of a rule.

In the next section we will define Basic Narrowing, and later show that if R is saturated under Parallel, then Basic Narrowing is complete.

Next we define the Forward Overlap rule, which is like the Critical Pair rule, except it reduces an instance of the right side of a rule instead of the left side. It ensures that all innermost redexes can be reduced to normal form in one step.

ForwardOverlap

$$\frac{u \to v[s'] \qquad s \to t}{(u \to v[t])\theta}$$

where

1. $u \to v[s'] \in R$
2. $s \to t \in R$
3. s' is not a variable
4. $\theta \in CSU_E(s = s')$

Definition 2. The above Forward Overlap inference rule is *redundant* if, for all $u' \approx_E u\theta$, u' is R, E reducible by a right-reduced instance of a rule $l \to r$, with matching substitution σ, and either

1. $l\sigma < u\theta$ or
2. $l\sigma \approx_E u\theta$ and $r\sigma < v[s']\theta$.

The notions of redundancy in this section are slightly different than the standard notions of redundancy. Instead of just requiring that redundant rules are implied by smaller instances of rules, this requires that redundant rules are implied by smaller instances of rules, where all substitutions to variables on the right hand sides of the rules are reduced. This will be necessary to make Basic Narrowing complete.

In the next section we will define Basic Narrowing with Right Hand Side Abstracted, and show that if R is saturated under the Parallel Rule and Forward Overlap then Basic Narrowing with Right Hand Side Abstracted is complete. Since we will see that Basic Narrowing with Right Hand Side Abstracted always terminates, this gives a decision procedure for unification.

We now give an example to illustrate the inference rules. There are also many interesting examples toward the end of the paper.

Example 1. $R_0 = \{f(x_1) \to g(x_1), k(x_2) \to q(x_2), b \to c\}$. Let $E = \{f(h(k(x))) \approx p(x), h(q(a)) \approx b\}$. There is a Parallel inference between $f(x_1) \to g(x_1)$ and $k(x_2) \to q(x_2)$ involving the equation $f(h(k(x))) \approx p(x)$. This is because $f(x_1)$ unifies with $f(h(k(x)))$, and $k(x_2)$ unifies with $k(x)$. Let $\sigma \in CSU_E(f(x_1) \approx_E^? f(h(k(x))), k(x_2) \approx_E^? k(x))$. So $\sigma = \{x_1 \mapsto h(k(x)), x_2 \mapsto x\}$. Since $k(x)$ is a subterm of $x_1\sigma$, the Parallel rule can be applied. The result is $p(x) \to g(h(q(x)))$. Let $R_1 = R_0 \cup \{p(x) \to g(h(q(x)))\}$. R_1 is saturated by Parallel, but it is not saturated by Forward Overlap. There is a Forward Overlap inference between $p(x) \to g(h(q(x)))$ and $b \to c$, because $h(q(x))$ is unifiable with b using the substitution $x \mapsto a$. The result of applying the Forward Overlap rule is $p(a) \to g(c)$. Let $R_2 = R_1 \cup \{p(a) \to g(c)\}$. Now R_2 is saturated by Parallel and Forward Overlap rule.

We define a set of inference rules to be *saturated* if all inferences are redundant, according to the definition of redundancy we give in each rule. An E-convergent rewrite system could be constructively saturated by applying the inferences exhaustively and adding new rewrite rules. The set of rewrite rules will still be E-convergent.

4 Inference Rules for Solving the Unification Problem

We introduce constrained terms, of the form $t|\varphi$, where t is a term and φ is a set of unification problems. Solutions and instances of constraints are defined as:

Definition 3. Let E be an equational theory. Let $t|\varphi$ be a constrained term. The *solutions of* φ are $Sol(\varphi) = \{\sigma \mid u\sigma \approx_E v\sigma$ for all $u \approx^?_E v \in \varphi\}$. The *irreducible instances of* $t|\varphi$ are $IInst(t|\varphi) = \{t\sigma \mid \sigma \in Sol(\varphi)$ and $x\sigma$ is in normal form for all $x \in Var(t)\}$.

Narrowing is a relation on constrained terms, with notation $t_1|\varphi_1 \rightsquigarrow t_2|\varphi_2$. Completeness is defined as follows:

Definition 4. A narrowing inference system is *complete* if given a term s and a reduced substitution σ, there is a sequence of narrowing steps $s \mid \top \overset{*}{\rightsquigarrow} t \mid \varphi$ and a substitution θ such that

1. σ can be extended to θ,
2. θ is a solution of φ, and
3. $t\theta$ is a normal form of $s\sigma$.

In this section we present two Narrowing rules. BN stands for Basic Narrowing, and BNR stands for Basic Narrowing with Right Hand Side Abstracted.

BN

$$\frac{u[s'] \mid \varphi \qquad s \rightarrow t}{u[t] \mid \varphi, s \approx^?_E s'}$$

where

1. $s \rightarrow t \in R$
2. s' is not a variable

Example 2. Consider the rewrite system R_0 from Example 1, and apply BN to $p(x)|\top$. The only reduction is with $f(x) \rightarrow g(x)$, which gives $g(x') \mid f(x') \approx^?_E p(x)$. (Note that $p(x) \approx_E f(h(k(x)))$.) All further BN steps have unsatisfiable constraints, but there are instances that are not reduced. This shows that BN is not complete for R_0. However, it can be checked that BN is complete for R_1.

Next we introduce the BNR inference rule, where the right hand side of the rewrite rule used for narrowing gets extracted into the constraint.

BNR

$$\frac{u[s']|\varphi \qquad s \rightarrow t}{u[x] \mid \varphi, s \approx^?_E s', x \approx^?_E t}$$

where

1. $s \rightarrow t \in R$
2. s' is not a variable
3. x is a fresh variable

Example 3. In Example 1, BNR is not complete for R_1. The term $p(a)$ cannot be reduced to its normal form $g(c)$ in one step. So, for example, a BNR from $p(a)$, using $p(x) \rightarrow g(h(q(x)))$ gives $y \mid p(a) \approx_E^? p(x), y \approx_E^? g(h(q(x)))$, which cannot be reduced further. It can be checked that BNR is complete for R_2.

BN and BNR are used, as usual, to find normal forms of every instance of a term. They can also be used to solve equational unification in $R \cup E$, in combination with an E-unification inference rule.

5 Optional Inference Rules

In this section we give some inference rules to augment the Basic Narrowing rules. These rules are not necessary for any of the results in this paper. But they are rules that are useful for designing an implementation that is efficient in practice. In these inference rules, as opposed to the earlier rules in the paper, the hypothesis is replaced by the conclusion.

The Concretization rule says that we can remove a constraint completely or partially remove a constraint, and apply a substitution satisfying the constraint directly to the unification problem.

Concretization

$$\frac{u|\varphi}{u\sigma|\varphi}$$

where σ is the most general unifier of φ.

The Split rule allows us to split a unification problem into two if the instances remain the same. Suppose a constraint has a finite number of solutions. We could split up a unification problem into one for each solution, and then apply Concretization to apply the substitutions.

Split

$$\frac{u|\varphi}{u|\varphi_1 \qquad u|\varphi_2}$$

where $IInst(u|\varphi) = IInst(u|\varphi_1) \cup IInst(u|\varphi_2)$.

Simplify is an important rule. Suppose a unification problem simplifies using a rewrite rule, then we are allowed to directly simplify it, without the nondeterminism that would come with a Basic Narrowing rule.

Simplify

$$\frac{u[s']|\varphi}{u[t\sigma]|\varphi}$$

where $s \rightarrow t \in R$ and $s\sigma \approx_E s'$.

A unification problem can be removed if all solutions of its constraint are reducible. This reduces the search space for narrowing.

ReducibleSubstitution

$$\frac{u|\varphi}{}$$

where σ is reducible over the variables of u for all $\sigma \in Sol(\varphi)$.

6 Completeness Proofs

In this section we prove the main completeness results of the paper. We show that if a set of rewrite rules R is saturated under our inference rules, then any minimal sequence of R, E rewrite steps, under an ordering we give below, can be lifted to a sequence of Basic Narrowing steps. This is a generalization of what can be done for Basic Narrowing in the empty theory, where any innermost sequence of R rewrite steps can be lifted to a Basic Narrowing sequence.

We first need an ordering to compare rewrite steps. We prefer smaller rewrite steps under this ordering. This means we prefer to use right-reduced instances of rules, because of the subterm property of our ordering. Our next preference is rules with smaller left hand sides, i.e., innermost reductions. Our last preference is rules with smaller right hand sides, i.e., to get to the normal form faster.

Definition 5. Let $s \rightarrow t$ and $u \rightarrow v$ be rewrite rules. Let θ_1 and θ_2 be substitutions. We define a relation on pairs of rewrite rules and substitutions.

- We say $(s \rightarrow t, \theta_1) \leq_N (u \rightarrow v, \theta_2)$ if $s\theta_1 \rightarrow t\theta_1$ is a right-reduced instance, or $u\theta_2 \rightarrow v\theta_2$ is not.
- We say $(s \rightarrow t, \theta_1) \leq_L (u \rightarrow v, \theta_2)$ if $s\theta_1 \leq u\theta_2$.
- We say $(s \rightarrow t, \theta_1) \leq_R (u \rightarrow v, \theta_2)$ if $t\theta_1 \leq v\theta_2$.
- Then define $\leq_B$ to be the lexicographic combination $(\leq_N, \leq_L, \leq_R)$.

We will show that saturation under Parallel is equivalent to the ability to reduce every innermost redex with a right-reduced instance of a rule, and closure under Parallel and Forward Overlap is equivalent to the ability to reduce every innermost redex to normal form in one step.

Definition 6. We say that R is IRR if every innermost redex is reducible by a right-reduced instance of R. We say that R is $IR1$ if every innermost redex is reducible to normal form in one step.

Theorem 1. *R is saturated by Parallel if and only if R is IRR.*

Proof. First the forward direction. Assume R is saturated by Parallel. Given an innermost redex s' and a reduction of s', let rule $s \to t$ and substitution θ be the smallest reduction of s' wrt $\leq_B$. We show that if $s\theta \to t\theta$ is not a right-reduced instance, then there is another reduction of s' which is smaller than $(s \to t, \theta)$.

Since $s\theta \to t\theta$ is not a right-reduced instance, there is a rewrite rule $l \to r$, a variable x in t and therefore also in s, and a substitution θ_1, extending θ, such that $l\theta_1$ is E-equivalent to a subterm of $x\theta$. Since s' is an innermost redex, we know that $l\theta_1$ is not a subterm of s'. Therefore, $s\theta$ is E-equivalent to s' but not identical. Therefore there must be some equation $u[l'] \approx v$ in E, and some substitution θ_2, extending θ_1 such that $l'\theta_2 \approx_E l\theta_1$, and l' is not a variable. Also, there must be some substitution θ_3, extending θ_2, such that $s\theta$ is E-equivalent to $u\theta_3$. θ_3 must be a unifier of $l \approx^? l'$ and $u \approx^? s$.

Therefore, the conditions of the Parallel rule are applicable. Let $\sigma \in CSU_E(l \approx^?_E l', u \approx^?_E s)$ such that $\sigma \leq_E \theta_3$ over the variables of the problem. The result of applying the Parallel rule is $v\sigma \to (v\sigma)\downarrow$. This rewrite rule can be used to reduce s'. The first component of the $\leq_B$ ordering either stays the same or gets smaller, since the right hand side was originally not a right-reduced instance. The second component stays the same, but the third one is smaller. Therefore the new rewrite step is smaller with respect to $\leq_B$.

This inference might be redundant. Suppose it is redundant because a strict subterm of every term E-equivalent to $s\sigma$ is reducible. Then there is a rewrite rule reducing a strict subterm of s', which is smaller in the $\leq_B$ ordering. Suppose that this inference is redundant because $s\sigma$ is reducible by a right-reduced instance of a rule. Then s' is also reducible by a right-reduced instance of a rule. A contradiction with the assumption has been obtained.

Now the reverse direction. Assume R is *IRR*. We need to show that all Parallel inferences are redundant. This is trivially true, because one one condition of the definition of redundancy for Parallel rules is that all innermost redexes can be reduced by a right-reduced instance of a rule. □

Theorem 2. *R is saturated by Parallel and Forward Overlap iff R is $IR1$.*

Proof. First the forward direction. Assume R is saturated by the Parallel and Forward Overlap rules. Once again we assume the smallest reduction to obtain a contradiction. Given an innermost redex s' and a reduction using rule $s \to t$ and substitution θ, we show that if $t\theta$ is not in normal form, then there is another reduction of s' which is smaller than $(s \to t, \theta)$ with respect to $\leq_B$.

Since $t\theta$ is not in normal form, there is a rewrite rule $l \to r$ and a substitution θ_1, extending θ, such that $l\theta_1$ is E-equivalent to a subterm of $t\theta$. By the previous theorem, and the fact that R is saturated by Parallel, we can assume that $s\theta \to t\theta$ is a right-reduced instance, therefore $l\theta_1$ is E-equivalent to a subterm of $t\theta$ at a non-variable position of t. Let l' be that subterm of t.

Therefore, the conditions of the Forward Overlap rule are applicable. There is a Forward Overlap among $s \to t[l']$ and $l \to r$. The result is $s\sigma \to t[r]\sigma$ for some $\sigma \in CSU_E(l \approx^? l')$. Then $s\sigma \to t[r]\sigma$ can reduce s'. It is smaller in the $\leq_B$ ordering, because it must be a right-reduced instance, the left hand sides are the same, and $t[r]\sigma\theta_1$ is smaller than $t[l]\theta_1$.

It is also possible that this inference is redundant because $s\sigma$ is reducible by a right-reduced instance of a rule smaller than $s\sigma \rightarrow t[l]\sigma$. This must be smaller with respect to $\leq_B$.

Now the reverse direction. Assume R is $IR1$. We need to show that all Parallel and Forward Overlap inferences are redundant. We have already showed that all Parallel rules are redundant in the last theorem. In order to show all Forward Overlap rules are redundant, consider a Forward Overlap of $u \rightarrow v[s']$ and $s \rightarrow t$, resulting in $u\theta \rightarrow v[t]\theta$. If $u\theta$ does not have an innermost redex, then this inference is redundant, because all equivalents of $u\theta$ have a reduction below the top. The smallest such reduction must be a right reduced instance. If $u\theta$ has an innermost redex, then there must be another rule reducing $u\theta$ to normal form in one step because R is $IR1$, and this rule must be a right reduced instance, so this inference is redundant. □

BN and BNR are clearly sound. We show that BN is complete for IRR theories, and BNR is complete for $IR1$ theories, with or without the optional rules. Since BNR halts, as long as Split is only applied finitely many times, BNR gives a decision procedure for unification in $IR1$ theories, and BN gives a complete procedure for unification in IRR theories.

Theorem 3. *If R is IRR then BN (with or without optional rules) is complete.*

Proof. We show that if $s\theta \in IInst(s \mid \varphi)$ and there exists t such that $s\theta \rightarrow t$ then there is a constrained term $t' \mid \varphi'$ and a sequence of one or more inference steps from $s \mid \varphi$ to $t' \mid \varphi'$ with $t \in IInst(t'|\varphi')$. That will show by induction that some rewrite sequence from $w\sigma$ to its normal form, where w is a term and σ is a reduced substitution, can be lifted to a narrowing sequence from $w \mid \top$.

Note that for Concretization, if $s\theta \in IInst(u \mid \varphi)$ then $s\theta \in IInst(u\sigma \mid \varphi)$. For Split, if $s\theta \in IInst(u \mid \varphi)$ then $s\theta \in IInst(u \mid \varphi_1)$ or $s\theta \in IInst(u \mid \varphi_2)$. So any sequence of those optional rules will preserve irreducibility. Also note that the ReducibleSubstitution rule is not applicable to $s \mid \varphi$. For Simplify, the conclusion $u[t\sigma] \mid \varphi$ has the same constraint and a subset of the variables of the hypothesis $u[s'] \mid \varphi$, so $u[t\sigma]\theta \in IInst(u[t\sigma] \mid \varphi)$ if $u[s']\theta \in IInst(u[s'] \mid \varphi)$.

If Simplify is not applied, and s is reducible, then, because R is IRR, s must be of the form $s[l']$ and there is some rule $l \rightarrow r$ such that $l'\theta =_E l\theta$ and $\theta|_{Var(r)}$ is irreducible. There is then a BN application from $s[l'] \mid \varphi$ to $s[r] \mid \varphi, l \approx_E^? l'$. Let $x \in Var(s[r])$. Then either $x \in Var(s[l'])$ or $x \in Var(r)$, and in both cases $x\theta$ is irreducible. So $s[r]\theta \in IInst(s[r] \mid \varphi, l \approx_E^? l')$. □

Theorem 4. *If R is $IR1$ then BNR, with or without optional rules, is complete.*

Proof. The proof is the same as the previous. Just redo the case where Simplify is not applied, and s is reducible, then, because R is $IR1$, s must be of the form $s[l']$ and there is some rule $l \rightarrow r$ such that $l'\theta \approx_E l\theta$ and $r\theta$ is irreducible. There is then a BNR application from $s[l'] \mid \varphi$ to $s[y] \mid \varphi, l \approx_E^? l', y \approx_E^? r$. Let $x \in Var(s[y])$. Then either $x \in Var(s[l'])$, in which case $x\theta$ is irreducible, or $x = y$, in which case again $x\theta$ is irreducible. So $s[r]\theta \in IInst(s[r] \mid \varphi, l \approx_E^? l', x \approx_E^? r)$. □

These theorems imply completeness of $R \cup E$ unification. We can decide the $R \cup E$ unification problem, and also find a complete set of $R \cup E$ unifiers if E unification is finitary. In the case of BNR it gives a complexity bound, since BNR narrowing branches nondeterministically but the length of a BNR sequence is at most linear in the size of the term. The size of the terms and constraints are linear in the size of the term. If E-unification is NP or better, then the complexity bound is NP. If E-unification is PSPACE or worse, then the complexity bound is the same as the complexity bound for unification modulo E.

We now give the definition of Finite Variant Property for rewrite systems R modulo E. We define R, E to have the FVP if a finite number of substitutions can be constructed, representing all normal forms of a given term. This requires that the E-unification problem is finitary. We generalize this to a Finite Constraint Property, which is also applicable to infinitary theories. R, E has the FCP if a finite number of constraints can be constructed, representing all normal forms of a given term. For finitary theories, this is the same as the Finite Variant Property. We show that if BNR is complete then R, E has the FCP. In the reverse direction, we show that if R, E has the FVP then R is $IR1$.

Definition 7. A term-substitution pair (t, θ) is an R, E *v*ariant of a term s if θ is normalized and $s\theta \approx_{R \cup E} t$. A *c*omplete set of R, E variants of s, denoted $[[s]]$, is a set of R, E variants of s such that:

1. for all $(t, \theta) \in [[s]]$, $s\theta \xrightarrow{*} t$ with t in normal form, and
2. For all reduced substitutions σ and reduced terms s' such that $s\sigma \xrightarrow{*} s'$, there exists a pair $(t, \theta) \in [[s]]$ and a substitution ρ such that $t\rho \approx_E s'$ and $\theta\rho \approx_E \sigma$.

R, E has the *Finite Variant Property (FVP)* if a finite $[[s]]$ can be constructed for all s.

Definition 8. A term/constraint pair (t, φ) is an R, E *constraint variant* of term s if $s\theta \approx_{R \cup E} t$ for all solutions θ of φ. A *c*omplete set of R, E constraint variants of s, denoted $[[s]]_c$, is a set of R, E constraint variants of s such that:

1. for all $(t, \varphi) \in [[s]]_c$ and $\theta \in Sol(\varphi)$, $s\theta \xrightarrow{*} t$ with t in normal form, and
2. For all reduced substitutions σ and reduced terms s' such that $s\sigma \xrightarrow{*} s'$, there exists a pair $(t, \varphi) \in [[s]]_c$ and a substitution $\theta \in Sol(\varphi)$ such that σ can be extended to θ and $t\theta \approx_E s'$.

R, E has the *Finite Constraint Property* (FCP) if a finite $[[s]]_c$ can be constructed for all s.

Theorem 5. *If BNR is complete for R then R, E has the FCP.*

Proof. Saturate a term s under BNR. Then $[[s]]_c$ is the set of all pairs $(t \mid \varphi)$ such that BNR produces $t \mid \varphi$. □

The inverse of the above theorem is not necessarily true. But the inverse of the below corollary is true, as shown by the results of this paper.

Corollary 1. *Let R be a finite rewrite system. If BNR is complete for R, and unification modulo E is finitary, then R, E has the FVP.*

Theorem 6. *Let R be a finite equational rewrite system. If R, E has the FVP then R has a finite saturation under Parallel and Forward Overlap.*

Proof. We definite a rewrite system V_R as follows:

$$V_R = \{s\theta \rightarrow s' \mid s \rightarrow t \in R, (s', \theta) \in [[s]] \text{ and } s\theta \text{ is an innermost redex}\}$$

Since R, E has the finite variant property, V_R is finite.

Let R^* be a (possibly infinite) saturation of R. Then R^* is $IR1$. This means that every innermost redex can be reduced to normal form in one step in R^*. Consider some $s\theta \rightarrow s'$ in V_R. Then $s\theta$ is reducible to its normal form s' in one step in R^*. So there is a $u \rightarrow v \in R^*$ and a substitution ρ such that $u\rho \approx_E s\theta$ and $v\rho \approx_E s'$. This means there is a finite set $V'_R \subseteq R^*$ such that all members of V_R are subsumed by some member of V'_R, and therefore every innermost redex can be rewritten to normal form in one step by a member of V'_R. So V'_R is $IR1$. By definition, terms have the same normal form in V'_R as they do in R.

Since V'_R is finite, all rules from V'_R will appear in finite time in the saturation of R. At that time, the set of rules will be $IR1$, so saturated under Parallel and Forward Overlap. □

7 Examples of Equational Theories

In this section, we consider a few examples of equational theories, and show how the E-Parallel rule is adapted for those theories.

First, consider the empty theory. Since the E-Parallel rule requires an equational axiom, it does not apply to the empty theory. Therefore, if R is convergent modulo E then BN is complete for R, and BNR is complete for R if R is saturated under Forward Overlap.

Now we consider AC, the theory of Associativity and Commutativity. When we instantiate the E-Parallel rule to AC, we get the following inference rule.

AC-Parallel

$$\frac{u_2 + x \rightarrow w \qquad p + s \rightarrow r}{(u_2 + x)\sigma \rightarrow (w\sigma)\downarrow}$$

where

1. $u_2 + x \rightarrow w$ or $x + u_2 \rightarrow w$ is in R
2. $p + s \rightarrow r \in R$
3. x is a variable which appears in w
4. $\sigma = [x \mapsto p + s]$ or $[x \mapsto p + s + y]$ for a fresh variable y

We show that this inference rule is correct.

Theorem 7. *AC-Parallel is an instance of E-Parallel for AC.*

Proof. Using the notation of the E-Parallel rule, we know that since l appears on the left hand side of a rewrite rule, it cannot be a variable. So it must be the sum of two terms, since it must unify with a nonvariable position of one side of an equation from AC. This justifies $p + s \to r$ as the right premise of the AC-Parallel inference rule. Since $p + s$ must unify with a strict subterm of an AC equation, we can assume wlog that $p + s$ unifies with $x_1 + y_1$ of the equation $(x_1 + y_1) + z_1 \approx x_1 + (y_1 + z_1)$.

The left hand side of the left premise of the inference rule must be of the form $u_2 + x$ since it is not a variable, it is unifiable with one side of an equation from AC, and it must contain the variable x, since t and therefore s contains the variable x. So $u_2 + x$ unifies with $(x_1 + y_1) + z_1$. Let $\sigma \in CSU_{AC}(p + s \approx^?_{AC} x_1 + y_1, u_2 + x \approx^?_{AC} (x_1 + y_1) + z_1)$.

$(p + s)\sigma$ must be AC-equivalent to a subterm of $x\sigma$ by Condition 6 of the E-Parallel rule. If $(p + s)\sigma$ is AC-equivalent to a strict subterm of $x\sigma$ then $x\sigma = (p + s + y)\sigma$ for some fresh variable y. Since $(p + s)\sigma \approx_{AC} (x_1 + y_1)\sigma$, this implies that $u_2\sigma + y\sigma = z_1\sigma$. Then $(u_2 + x)\sigma \approx_{AC} ((x_1 + y_1) + z_1)\sigma \approx_{AC} ((p + s)\sigma + u_2\sigma + y\sigma)$.

A similar, but slightly simpler argument holds if $x\sigma =_{AC} (p + s)\sigma$. □

In practice, AC-Parallel inferences are usually redundant if u_2 is not a sum.

We now give an A-Parallel rule for the theory of Associativity.

A-Parallel

$$\frac{u_1 + x + u_2 \to w \qquad p + s \to r}{(u_1 + x + u_2)\sigma \to (w\sigma)\downarrow}$$

where

1. $u_1 + x + u_2 \to w \in R$
2. $p + s \to r \in R$
3. x is a variable which appears in w
4. $\sigma = [x \mapsto p + s]$ or $[x \mapsto p + s + y]$ for a fresh variable y

Theorem 8. *A-Parallel is an instance of E-Parallel for Associativity.*

Proof. As in the AC case, using the notation from the E-Parallel rule, we know that since l appears on the left hand side of a rewrite rule, it cannot be a variable. So it must be the sum of two terms, since it must unify with a a nonvariable position of one side of an equation from A. This justifies $p + s \to r$ as the right premise of the A-Parallel inference rule. Since $p + s$ must unify with a strict subterm of an A equation, we can assume that $p + s$ either unifies with $y_1 + z_1$ of the equation $x_1 + (y_1 + z_1) \approx (x_1 + y_1) + z_1$.

Let $s \to t$ be the left premise of if the inference rule. s is not a variable but must contain a variable x, and it is unifiable with one side of an equation from A. So s unifies with $x_1 + (y_1 + z_1)$. Let $\sigma \in CSU_A(p + s \approx^?_A y_1 + z_1, s \approx^?_A x_1 + (y_1 + z_1))$.

Suppose s is of the form u_2+x. $(p+s)\sigma$ must be A-equivalent to a subterm of $x\sigma$. Suppose that $x\sigma =_A (p+s)\sigma$. Since $(p+s)\sigma{\approx_A}(y_1+z_1)\sigma$, then $u_2\sigma = x_1\sigma$. Then $(u_2+x)\sigma{\approx_A}(x_1+(y_1+z_1))\sigma{\approx_A}u_2\sigma+(p+s)\sigma$, which is of the form t_1+t_2. If t_2 contains $p\sigma + s\sigma$ as part of its sum, then t_2 is reducible, and $t_1 + t_2$ is reducible below the root. Suppose t_2 does not contain $p\sigma + s\sigma$. Then t_1 must contain $u_2\sigma$. But since R is convergent modulo A, $p\sigma+s\sigma+t_3$ must be reducible for any term t_3. Therefore t_1 is reducible and t_1+t_2 is again reducible below the root. In either case, the inference is redundant. If $(p+s)\sigma$ is A-equivalent to a strict subterm of $x\sigma$, the argument is identical. It is also an identical argument if s is of the form $x + u_2$.

Now suppose s is of the form $u_1 + x + u_2$. The argument here is the same as the argument for the AC case. □

8 Examples of Rewrite Systems

In this section we apply our results to some rewrite systems that are convergent modulo AC or A or modulo two AC operators.

Example 4. Consider the example from the introduction. If we apply Parallel to this theory, we create two new rules: $a+a+b+b \to 0$ and $a+a+b+b+x \to x$. All other Parallel inferences are redundant, and Forward Overlap cannot be applied. So this rewrite system is now saturated by Parallel and Forward Overlap, and BNR is complete and terminating.

Example 5. Let $R = \{a+b \to c, a+b+x \to c+x\}$ where $+$ is AC. This cannot be finitely saturated under Parallel. It creates all possible rules of the following forms: $\{a^n + b^n \to c^n, a^n + b^n + x \to c^n + x\}$. We use a^n as an abbreviation for a sum of n occurrences of a.

None of these rules are redundant. Since this rewrite system cannot be finitely saturated under Parallel, it does not have the Finite Variant Property. It is interesting that such simple rewrite systems do not have the finite variant property, but much more complicated rewrite systems sometimes do.

Example 6. The theory of Exclusive OR satisfies Associativity, Commutativity, Unit and Nilpotence. It consists of the following rewrite rules, modulo AC of $+$.

1. $x+x \to 0$ 2. $x+0 \to x$ 3. $x+x+y \to y$

Every application of Parallel is redundant in this theory. For example, a Parallel inference between Rule 3 and Rule 2 gives $x+x+x'+0 \to x'$. Every AC-equivalent of $x+x+x'+0$ is reducible below the root. A Parallel inference between Rule 3 and Rule 1 results in $x+x+x'+x' \to 0$. Every AC-equivalent of $x+x+x'+x'$ is reducible below the root, except for $(x+x')+(x+x')$, which is reducible at the root by a right reducible instance of $x+x \to 0$. Similarly for all applications of Parallel. There are no instances of Forward Overlap.

Example 7. Consider the rewrite presentation of Abelian Groups from Lankford, given in the Comon/Delaune paper [5], where $*$ is an AC operator.

1. $x * 1 \to x$
2. $(x^{-1})^{-1} \to x$
3. $1^{-1} \to 1$
4. $(x^{-1} * y)^{-1} \to y^{-1} * x$
5. $x * x^{-1} \to 1$
6. $x * (x^{-1} * y) \to y$
7. $x^{-1} * y^{-1} \to (x * y)^{-1}$
8. $x^{-1} * (y^{-1} * z) \to (y * x)^{-1} * z$
9. $(x * y)^{-1} * x \to y^{-1}$
10. $(x * y)^{-1} * (y * z) \to x^{-1} * z$

All applications of Parallel are redundant and there are two applications of Forward Overlap that are not redundant. A Forward Overlap between Rule 10 and Rule 7 gives $(x * y)^{-1} * (y * z^{-1}) \to (z * x)^{-1}$. A Forward Overlap between Rule 10 and Rule 8 gives $(x * y)^{-1} * (y * z^{-1}) * w \to (z * x)^{-1} * w$.

It can be checked that when these two new rules are added, the rewrite system is saturated under Parallel and Forward Overlap.

Example 8. Here we consider a homomorphism from an AC operator to another AC operator. Notice this is not an endomorphism as is often considered, because the binary operator on the left hand side is not the same as the binary operator on the right hand side. Let $R = \{h(x)*h(y) \to h(x+y), h(x)*h(y)*z \to h(x+y)*z\}$ where $+$ and $*$ are both AC symbols.

There are many applications of Parallel, and Forward Overlap. One of the applications of Parallel gives $h(x) * h(y) * h(u) * h(v) \to h(x + y + u + v)$. Every equivalent instance can be rewritten below the root. Similarly, the other applications of Parallel and the applications of Forward Overlap derive rules where all equivalent instances of the left hand side can be rewritten below the root. So all Parallel and Forward Overlap rules are redundant. Therefore the two rules above are saturated under Parallel and Forward Overlap.

Example 9. Consider the homomorphism theory over AC, where the binary operator is the same on both sides. Let $R = \{h(x) * h(y) \to h(x * y), h(x) * h(y) * z \to h(x*y) * z\}$. R is saturated under Parallel, for the same reason as the other homomorphism theory. But it cannot be finitely saturated under Forward Overlap. Therefore, BN is complete for this theory, but BNR cannot be made complete.

We could flip the order of the rules in this example. We would get $R = \{h(x * y) \to h(x) * h(y)\}$. Since the top symbol on the left hand side is not AC, there are no extensions or Parallel inferences. So BN is complete. But this theory also cannot be saturated by Forward Overlap.

Even though Associative Unification is infinitary, we can still represent them with a constraint. Even when we cannot list out all the unifiers we can still give a constraint representing them. Associative constraints are decidable, so we can decide unification in theories that are closed under Parallel and Forward Overlap. This is an advantage over the Finite Variant Property, which does not allow infinitary theories, so it does not cover Associativity.

Example 10. Consider the theory AU of an associative operator with a unit, as given by $R = \{x + 0 \to x, 0 + x \to x\}$. There are no applications of Parallel and Forward Overlap. So it is saturated under Parallel and Forward Overlap.

9 Conclusion

Basic Narrowing modulo an equational theory is known to be incomplete for E-convergent rewrite systems R [5]. We defined an inference rule called Parallel, and showed that if R is saturated by Parallel then Basic Narrowing is complete. If R is also saturated by Forward Overlap, then BNR, a restricted form of Basic Narrowing, is complete. Since BNR always terminates, this gives a decision procedure for $R \cup E$ unification, which runs in NP time if E-unification is decidable in NP. If E-unification is finitary, we can also produce a complete set of unifiers.

Since Basic Narrowing was shown to be incomplete, recent research on narrowing modulo E has focused on Variant Narrowing [9], which works if R, E has the Finite Variant Property. We show that R has the Finite Variant Property modulo E if and only if R can be finitely saturated by Parallel and Forward Overlap wrt E, and the finite saturation of R makes BNR complete modulo E.

The work on the Finite Variant Property may deal with many sorted/order sorted theories [12]. We see no issues in extending our work to cover order sorted theories, but that is left for future work. On the other hand, we allow theories where E-unification is infinitary such as Associativity, while the Finite Variant Property does not cover that. We have generalized the Finite Variant Property to something called the Finite Constraint Property, which we believe would also allow Variant Narrowing to deal with infinitary equational theories. If E is infinitary, it may not be possible to saturate R; but it can be saturated in cases that do not require infinitary unification. We give the example of Associativity with a unit in this paper.

For future work, we will extend BNR to handle sorts. We also think there would not be a problem to extend our results to unfailing completion and full first order theorem proving. We have given some examples in this paper, like Exclusive OR and Abelian groups. We would like to find other interesting and practical theories where BNR gives a decision procedure.

References

1. Baader, F., Nipkow, T.: Term Rewriting and All That. Cambridge University Press, Cambridge (1998)
2. Baader, F., Snyder, W.: Unification theory. In: Robinson, A., Voronkov, A. (eds.) Handbook of Automated Reasoning, chap. 8, vol. 1, pp. 445–532. Elsevier Science, Amsterdam (2001)
3. Bachmair, L., Dershowitz, N.: Completion for rewriting modulo a congruence. Theor. Comput. Sci. **67**(2), 173–201 (1989)
4. Bouchard, C., Gero, K.A., Lynch, C., Narendran, P.: On forward closure and the finite variant property. In: Fontaine, P., Ringeissen, C., Schmidt, R.A. (eds.) FroCoS 2013. LNCS (LNAI), vol. 8152, pp. 327–342. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-40885-4_23
5. Comon-Lundh, H., Delaune, S.: The finite variant property: how to get rid of some algebraic properties. In: Giesl, J. (ed.) RTA 2005. LNCS, vol. 3467, pp. 294–307. Springer, Heidelberg (2005). https://doi.org/10.1007/978-3-540-32033-3_22

6. Dershowitz, N., Plaisted, D.A.: Rewriting. In: Robinson, A., Voronkov, A. (eds.) Handbook of Automated Reasoning, chap. 9, vol. 1, pp. 535–610. Elsevier Science, Amsterdam (2001)
7. Erbatur, S., et al.: Effective symbolic protocol analysis via equational irreducibility conditions. In: Foresti, S., Yung, M., Martinelli, F. (eds.) ESORICS 2012. LNCS, vol. 7459, pp. 73–90. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-33167-1_5
8. Escobar, S., Meadows, C., Meseguer, J.: Maude-NPA: cryptographic protocol analysis modulo equational properties. In: Aldini, A., Barthe, G., Gorrieri, R. (eds.) FOSAD 2007-2009. LNCS, vol. 5705, pp. 1–50. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-642-03829-7_1
9. Escobar, S., Sasse, R., Meseguer, J.: Folding variant narrowing and optimal variant termination. J. Logic Algebraic Program. **81**(7), 898–928 (2012)
10. Hullot, J.-M.: Canonical forms and unification. In: Bibel, W., Kowalski, R. (eds.) CADE 1980. LNCS, vol. 87, pp. 318–334. Springer, Heidelberg (1980). https://doi.org/10.1007/3-540-10009-1_25
11. Kirchner, H.: Some extensions of rewriting. In: Comon, H., Jounnaud, J.-P. (eds.) TCS School 1993. LNCS, vol. 909, pp. 54–73. Springer, Heidelberg (1995). https://doi.org/10.1007/3-540-59340-3_5
12. Meseguer, J.: Strict coherence of conditional rewriting modulo axioms. Theor. Comput. Sci. **672**, 1–35 (2017). https://doi.org/10.1016/j.tcs.2016.12.026