E-unifiability via Narrowing *

Emanuele Viola

Dip. di Scienze dell'Informazione, Univ. di Roma "La Sapienza", V. Salaria 113, 00198 Roma, Italy
viola@dsi.uniroma1.it

Abstract. We formulate a narrowing-based decision procedure for E-unifiability. Termination is obtained requiring a *narrowing bound*: a bound on the length of narrowing sequences. We study general conditions under which the method guarantees that E-unifiability is in *NP*. The procedure is also extended to narrowing *modulo AC* (associativity and commutativity). As an application of our method, we prove NP-completeness of unifiability modulo bisimulation in process algebra with proper iteration, significantly extending a result in [8]. We also give (new) proofs, under a unified point of view, of NP-decidability of I, ACI, $ACI1$-unifiability and of unifiability in quasi-groups and central groupoids.

1 Introduction

E-unification is concerned with solving term equations modulo an *equational theory* E [11, 3]. It is a fundamental tool in theorem proving, logic programming and type assignment systems. *Narrowing* is a well-known technique that can be used as a *general* E-unification procedure in the presence of a *term rewriting system* (TRS) [2]. *Narrowing* a term is finding the minimal instantiation of it such that one rewrite step becomes applicable, and to apply it. If this process is applied to an equation and is iterated until finding an equation whose both terms are syntactically unifiable, then the composition of the *most general unifier* with all the substitutions computed during the narrowing sequence yields an *E-unifier* of the initial equation. The narrowing process that builds all the possible narrowing sequences starting from the equation to be solved, is an E-unification procedure that yields complete sets of unifiers, provided that E can be presented by a *convergent* (i.e. *confluent* and *terminating*) rewrite system [3]. However, in general this procedure does not terminate.

Hullot [9] gives sufficient conditions for this procedure to be terminating. His results also extend to equational narrowing. However, the TRS must satisfy strong requirements and no complexity analysis of the procedure is given. Furthermore, there is not much hope to find low complexity bounds, as long as we want complete sets of unifiers, since in simple cases their cardinality is unfeasible [14].

* Work carried out within the MURST project TOSCA (Theory of concurrency, higher order and types).

However, constraint approaches to theorem proving [15, 5] and logic programming [6], need the computation of finite complete sets of unifiers no longer for many applications. It is sufficient to decide solvability of the E-unification problems, namely *E-unifiability*.

Nieuwenhuis [18], using *basic paramodulation* techniques, shows that E-unifiability is in NP if E is *shallow* (i.e. variables at depth at most one). But there is no extension to equational paramodulation and being shallow is very restrictive.

Here we study E-unifiability via narrowing. This paper does not aim to define yet another refinement of the basic narrowing which does not destroy completeness (for a survey, see [3]). We show how optimal and new complexity results can be obtained considering a simple *bound on the length of the basic narrowing sequences*. Our method is *lazy*, in the sense that *we never compute unifiers*. Instead, we add equations to our unification problem, and only at the end we check the unifiability of all the equations we have created.

We show that if for every rule $l \to r$ in a convergent TRS we have that r is a subterm of l, then E-unifiability is in NP (where E is equivalent to the TRS). This is enough, for example, to give (new) proofs of NP-decidability of unifiability in quasi-groups, central groupoids and of I-unifiability (*idempotency*, i.e. $x + x \approx x$).

Of course not every theory can be presented as a convergent TRS. One of the main reasons is that some (sets of) axioms cannot be oriented into terminating (sets of) rewrite rules. Among these there is AC (*associativity*, i.e. $x + (y + z) \approx (x + y) + z$, and *commutativity*, i.e. $x + y \approx y + x$), satisfied by many common binary operations. Consequently, we extend our results to narrowing modulo AC. Being lazy is particularly important in this case, because the cardinality of a minimal complete set of AC-unifiers may be doubly-exponential [14, 17].

The most important application we consider here is in the field of *process algebra* [4]: NP-completeness of unifiability modulo bisimulation in minimal process algebra with proper iteration [7]. This is a significant extension of a result in [8].

Again, we get new proofs of classical results: NP-decidability of ACI, $ACI1$-unifiability (1 stands for *existence of unity*, i.e. $x + 1 \approx x$).

This paper is organized as follows. In the next section we give some preliminaries. In Section 3 we define our narrowing-based decision procedure, study its complexity and compare our results with Hullot's and with Nieuwenhuis'. We also give some applications. In Section 4 we extend our results to AC-narrowing and detail an application in process algebra. We also discuss other applications. Section 5 is a conclusion.

2 Preliminaries

We assume that the reader is familiar with terms, equational theories, E-unification, term rewriting systems and related topics [2]. We denote by $Term(\sum \bigcup X)$ the set of *terms* generated by the *signature* $\sum$ and the set of *variable symbols* X. We denote the set of *positions* of a term s by $Pos(s)$. For

$p \in Pos(s)$, $s|_p$ is the *subterm of* s *at position* p, and $s[t]_p$ is the term obtained from s by *replacing the subterm at position* p *by the term* t. We denote by $\overline{Pos}(s)$ the set of non variable positions of s: $\{p : p \in Pos(s) \text{ and } s|_p \notin X\}$. The *size* of a term s is $|Pos(s)|$. We may write a *substitution* θ as $\{x_1 \leftarrow \theta x_1, ..., x_n \leftarrow \theta x_n\}$ if its *domain*, denoted by $Dom(\theta)$, is $\{x_1, ..., x_n\}$. Let E be an *equational theory.* It is convenient to see an *equation* over $\sum$ modulo E as a term with top symbol $=^?_E$ ($=^?_E \notin \sum$), i.e. $s =^?_E t$ where $s, t \in Term(\sum \cup X)$. We write $\theta \models s =^?_E t$ for $\theta s =_E \theta t$. An *E-unification problem* over $\sum$ is a *finite* set of equations modulo E. In this paper every E-unification problem is *general*, i.e. it may contain arbitrary function symbols not occurring in E. Let Π be an E-unification problem. The *size* of Π is $\sum_{e \in \Pi} size(e)$. Π is *E-unifiable* if there is a substitution θ such that for any $e \in \Pi$, $\theta \models e$. In this case we write $\theta \models \Pi$ and θ is said to be a *E-unifier.* If θ is a substitution, we write $\theta\Pi$ for $\{\theta e : e \in \Pi\}$.

A *term rewriting system* (TRS) T is a *finite* set of *identities*, called (*rewrite*) *rules* and written $l \to r$, such that for any $l \to r \in T$, $l \notin X$ and $var(l) \supseteq var(r)$ ($var(s)$ is the set of variables occurring in s). Let T be a TRS. We write $s \to_T t$ (s *reduces* to t) iff there are $l \to r \in T$, $p \in Pos(s)$ and a substitution θ such that $s|_p = \theta l$ and $t = s[\theta r]_p$. We write $s \to_{T/AC} t$ (s *reduces* modulo AC to t) iff there are terms s', t' such that $s =_{AC} s' \to_T t' =_{AC} t$. When considering $\to_{T/AC}$ we speak of an AC-TRS. Let T be an (AC-)TRS. If $s \to_{T(/AC)} t$ we speak of a *reduction step.* A term s is *reducible* if there is t such that $s \to_{T(/AC)} t$; otherwise, s is in *normal form.* A substitution θ is said to be *normalized* if for any $x \in Dom(\theta)$, θx is in normal form. T is *convergent* if it is *confluent* (modulo AC) and *terminating* (modulo AC).

3 Narrowing

We start with the case where E is equivalent to a convergent TRS T. A *system* is a couple $\Pi; K$ where Π is an E-unification problem and K a set of equations (modulo $\emptyset$). We define our narrowing relation $\rightsquigarrow$:

Definition 1. *Let* $\Pi \cup \{e\}; K$ *be a system,* $p \in \overline{Pos}(e)$ *and* $l \to r \in T$. *Then*

$$\Pi \cup \{e[u]_p\}; K \rightsquigarrow_T \Pi \cup \{e[r]_p\}; K \cup \{l =^? u\}$$

If $\Pi; K \rightsquigarrow_T \Pi'; K'$ then we say that $\Pi; K$ *narrows* in $\Pi'; K'$. We also speak of a (*narrowing*) *sequence* $\Pi_1; K_1 \rightsquigarrow_T ... \rightsquigarrow_T \Pi_n; K_n$, and we denote by $\rightsquigarrow^*_T$ the reflexive transitive closure of $\rightsquigarrow_T$. In the following we will occasionally slightly abuse this notation, narrowing systems where we have a term in place of the E-unification problem.

Our narrowing relation is nothing but a *lazy* version of the *basic* narrowing relation introduced by Hullot [9]. Moving the subterm u in K enforces the *basic* restriction on future applications of the rule [3].

We are not interested in finding minimal complete set of E-unifiers [3], only in E-unifiability. So in our setting narrowing gives a *complete* semi-decision

$x * (x\backslash y) \to y$	$(x * y)/y \to x$
$(x/y) * y \to x$	$(x/y)\backslash x \to y$
$x\backslash(x * y) \to y$	$x/(y\backslash z) \to y$

Table 1. Rewrite rules for quasi-group theory.

procedure for E-unifiability. This means that, for every E-unification problem Π, the following two conditions are equivalent:

1. Π is E-unifiable.
2. $\Pi; \emptyset \leadsto_T^* \Pi'; K$ and $\Pi' \cup K$ is syntactically unifiable.

However, this does not give rise to a terminating decision procedure for E-unifiability. In fact some narrowing sequences may not terminate, and we don't know when we can stop following them.

Hullot [9] gives sufficient conditions for the narrowing to be a terminating decision procedure for E-unifiability. He proves that, given a TRS T, if for every $l \to r \in T$ every basic narrowing sequence starting from r terminates, then every narrowing sequence starting from every term terminates. Using this fact, one can give a decision procedure for I-unifiability. In fact the TRS $\{x + x \to x\}$ is convergent and equivalent to I, and moreover it satisfies the Hullot condition for termination, because there is no basic narrowing sequence starting from x. Similarly, Hullot gets decidability of unifiability in quasi-group theory, whose theory is equivalent to the convergent TRS reported in Table 1. Hullot's approach extends to narrowing modulo equational theories. But it gives no complexity analysis of the procedure and the TRS must satisfy a quite strong requirement.

Nieuwenhuis [18] shows that E-unifiability is in NP if E is *shallow* (i.e. variables at depth at most one). As a direct application one gets a new proof that I-unifiability is in NP, but one can not prove the same for quasi-group theory because it is not shallow. In fact being shallow is rather restrictive. In addition, this approach gives no extensions to deduction modulo equational theories.

Let's consider an easy case which is not covered by any of the above approaches. Let T be the TRS $\{f(f(x)) \to f(x)\}$ convergent and equivalent to $E := \{f(f(x)) \approx f(x)\}$. Intuitively, E-unifiability looks like an easy task. But we can't apply Nieuwenhuis' results because E is not shallow. Nor can we apply Hullot's results because there is a non-terminating narrowing sequence starting from $f(x)$, namely, using the non-lazy basic narrowing introduced by Hullot [9]:

$$f(x) \leadsto_{f(f(y)) \to f(y)} f(y) \leadsto_{f(f(z)) \to f(z)} f(z) \leadsto \ldots$$

However, suppose $t \in Term(\sum \bigcup X)$. If θ is normalized, how long can a reduction sequence starting from θt be? Clearly at most the number of occurrences of f in t, which is less than $size(t)$. So, if to every reduction sequence corresponds a narrowing sequence of the same length, in order to check the E-unifiability of an equation $s =_E^? t$ it is sufficient to consider narrowing sequences as long as $\max\{size(s), size(t)\}$.

In order to formalize this idea we introduce a useful notation. We write $s \to_{T,\theta} t$ to indicate the substitution θ involved in the reduction step. We write $s \mapsto_T t$ iff $s \to_{T,\theta} t$ and θ is normalized. Similarly, if Π and Π' are sets of equations, we write $\Pi \mapsto_T \Pi'$ iff $\Pi = \hat{\Pi} \cup \{e\}$, $\Pi' = \hat{\Pi} \cup \{e'\}$ and $e \mapsto_T e'$. We speak of an *inner reduction step*. Furthermore, we write $s\bar{\downarrow}_T^n$ ($\Pi\bar{\downarrow}_T^n$) if s (Π) reaches its normal form in at most n *inner* reduction steps, i.e. if there is no sequence $s \mapsto_T s_1 \mapsto_T ... \mapsto_T s_n \mapsto_T s_{n+1}$ ($\Pi \mapsto_T \Pi_1 \mapsto_T ... \mapsto_T \Pi_n \mapsto_T \Pi_{n+1}$).

The previous considerations lead to the following definition:

Definition 2. *Let H be a computable function from the set of all E-unification problems into the positive integers. H is a* narrowing bound *for T if for any E-unification problem Π, if Π is unifiable then there is a unifier θ such that $\theta\Pi\bar{\downarrow}_T^{H(\Pi)}$.*

The reader might wonder about the rationale for considering inner reductions. In addition: why don't we use the well-known *innermost* reductions? There is a specific reason for this, explained at the end of Section 4.1.

We can now give our decision procedure for E-unifiability, when E is equivalent to a convergent TRS T and H is a narrowing bound for T. Let Π be an E-unification problem:

Decision Procedure

1. Guess $n \leq H(\Pi)$.
2. Guess a sequence $\Pi; \emptyset \rightsquigarrow_T \Pi_1; K_1 \rightsquigarrow_T ... \rightsquigarrow_T \Pi_n; K_n$.
3. Answer 'yes' iff $\Pi_n \cup K_n$ is syntactically unifiable.

The proof of the completeness of the above decision procedure should be substantially obvious [3, 23].

3.1 Complexity

Our approach allows us to say something more than just decidability of E-unifiability: we can prove it is in NP when there is a *polynomial* narrowing bound:

Definition 3. *A narrowing bound H is* polynomial *if it is polynomially computable and there is a polynomial q such that for every E-unification problem Π, $H(\Pi) \leq q(size(\Pi))$.*

In fact, if there is a polynomial narrowing bound for T, then we can restrict to considering only narrowing sequences whose length is bounded by a (fixed) polynomial in the size of the problem. Moreover, our lazy approach guarantees that if $\Pi; K \rightsquigarrow_T \Pi'; K'$ then $size(\Pi' \cup K') = O(size(\Pi \cup K))$. So the whole narrowing sequence is polynomial in the size of the problem, and can therefore be guessed in non-deterministic polynomial time. Noticing that general syntactic unifiability is in P [19, 3] concludes the proof of the following theorem.

Theorem 1. *Let E be an equational theory and T a convergent TRS equivalent to E. If there is a polynomial narrowing bound for T then E-unifiability is in NP.*

The point now is: how do we find a (polynomial) narrowing bound for a TRS? The following corollary establishes a rather general result:

Corollary 1. *Let E be an equational theory and T a convergent TRS equivalent to E. If for every $l \to r \in T$ we have that r is a subterm of l, then E-unifiability is in NP.*

Proof. We prove by induction that for every term t and for every normalized substitution θ, $\theta t \bar{\downarrow}_T^{size(t)}$. The result follows since for any $e \in \Pi$, $\theta e \bar{\downarrow}_T^{size(e)}$ and $size(\Pi) = \sum_{e \in \Pi} size(e)$, so we have $\theta \Pi \bar{\downarrow}_T^{size(\Pi)}$ and therefore we can consider $H(\Pi) := size(\Pi)$.

We proceed with the induction:

- If $t = x$ then θx is in normal form because θ is normalized.
- If $t = f(t_1, ..., t_n)$ for $n \geq 0$ then $\theta t = f(\theta t_1, ..., \theta t_n)$. By induction, one gets $\theta t_1 \bar{\downarrow}_T^{size(t_1)}, ..., \theta t_n \bar{\downarrow}_T^{size(t_n)}$. If $f(\theta t_1 \downarrow_T, ..., \theta t_n \downarrow_T) \to_T t'$ then t' is in normal form because it is a (proper) subterm of $f(\theta t_1 \downarrow_T, ..., \theta t_n \downarrow_T)$. So we perform at most $1 + \sum_{i=1}^{n} size(t_i)$ reduction steps, and we can conclude $\theta t \bar{\downarrow}_T^{size(t)}$.

□

Clearly, the existence of a polynomial narrowing bound for a TRS T does not imply that r is a subterm of l for every rule $l \to r \in T$. For example, the trivial TRS $\{a \to b\}$ has a polynomial narrowing bound. We are currently working on generalizations of the above corollary. However, it already gives interesting results, which we detail in the next section.

3.2 Applications

We immediately get a new narrowing-based proof of the following well-known result.

Theorem 2. *I-unifiability is in NP.*

Proof. The TRS $\{x + x \to x\}$ is convergent and equivalent to I. The result follows because of Corollary 1. □

Notice that this last result is optimal: I-unifiability is NP-complete [13]. As we noted before, I-unifiability can be showed to be in NP using the results in [18]. However, our technique applies to non-shallow theories as well. We give a couple of examples:

Theorem 3. *Unifiability in quasi-group theory is in NP.*

Proof. A convergent TRS equivalent to quasi-group theory is reported in Table 1. The result follows because of Corollary 1. $\square$

The theory $\{(x * y) * (y * z) \approx y\}$ defines *central groupoids* [2].

Theorem 4. *Unifiability in central groupoids is in NP.*

Proof. The following is a convergent TRS equivalent to $\{(x * y) * (y * z) \approx y\}$ [2]:

$$\begin{array}{c}(x * y) * (y * z) \to y\\ x * ((x * y) * z) \to x * y\\ (x * (y * z)) * z \to y * z\end{array}$$

The result follows because of Corollary 1. $\square$

4 AC-Narrowing

In this section we extend our results to narrowing modulo AC. A special attention has always been devoted to this case [9, 17], as A and C are well-suited for being built-in due to their permutative nature and they often occur in practical specifications (we will give an example in Section 4.2).

For simplicity, we assume that $+$ is the only AC-symbol, i.e. interpreted as an operator satisfying AC. Cases where there are several AC-symbols can be treated analogously.

We extend our narrowing relation in a way which parallels inner equational rewriting. One extends inner rewriting to inner AC-rewriting defining

$$s \mapsto_{T/AC} t \quad \text{iff} \quad s =_{AC} s' \mapsto_T t' =_{AC} t$$

for some s', t'. We might then define our AC-narrowing relation in the following way:

$$\Pi \cup \{e\}; K \rightsquigarrow_{T/AC} \Pi'; K' \quad \text{iff} \quad e' =_{AC} e \text{ and } \Pi \cup \{e'\}; K \rightsquigarrow_T \Pi'; K'$$

This would lead to a decision procedure for E-unifiability as in Section 3, where the final system is checked for AC-unifiability instead of syntactic unifiability (now K is a set of equations modulo AC).

However, the completeness is lost. In fact, the completeness of our narrowing for E-unifiability rests on a variant of the *Hullot property* [9, 11]:

Definition 4. ***(Hullot property)*** *For every normalized substitution θ:*

$$\textit{if} \quad \theta e \mapsto_{T/AC} e' \quad \textit{then} \quad e; \emptyset \rightsquigarrow_{T/AC} e''; K$$

and there is a normalized substitution $\theta' \supseteq \theta$ such that $\theta' e'' =_{AC} e'$ and $\theta' \models K$.

We now show that the introduced narrowing relation does *not* satisfy the Hullot property. For readability we write $\bar{x}_n$ for $x_1 + ... + x_n$ and $\bar{a}_n$ for $a + ... + a$ (where there are n a's).

Example 1. Let $T := \{x + x \to c\}$ and $E := AC \cup \{x + x \approx c\}$. For every even $n > 1$ consider the equation $\bar{x}_n =^?_E c$. The substitution $\theta := \{x_1 \leftarrow a + b, ..., x_n \leftarrow a + b\}$ is normalized and we get:

$$\theta(\bar{x}_n =^?_E c) \mapsto_{T/AC} c + \bar{b}_n =^?_E c$$

The system $\bar{x}_n =^?_E c; \emptyset$ could narrow in $c =^?_E c; \bar{x}_n =^?_{AC} z + z$ but now $c \neq c + \bar{b}_n$. So the Hullot property is not satisfied.

Other narrowing sequences lead to similar results.

The point is that every θx_i in the above example is only *partially* involved in the reduction step. I.e. $\theta x_i =_{AC} u_i + v_i$ where u_i is *not* involved in the reduction step.

To overcome the incompleteness, we consider *extensions* of the equations. We use them *implicitly*, that is coding them in the narrowing relation. This idea first appeared in [21]. The reader may consult [22] for a comparison between implicit and explicit [20] extensions, and for another example showing that AC-paramodulation is incomplete without extensions. In many cases, it is sufficient to consider single-variable extensions, i.e. given an equation $s = t$ one considers $s + x = t + x$ where x is a new variable [20, 17]. But in our framework this is not sufficient. We will return to this later.

Recall we assume $+$ is the only AC-symbol in $\sum$. We denote by $UngPos(s)$ the set of *variable* positions *unguarded* in s, i.e. $\{p : p \in Pos(s),\ s|_p \in X$ and if $p = qq'$ with $|q'| > 0$ then $s|_q = t + t'\}$ [4].

Our AC-narrowing relation is then:

Definition 5. *Let $\Pi \cup \{e\}; K$ be a system, $e =_{AC} e'$, $p \in \overline{Pos}(e')$, $l \to r \in T$ and $y_0, ..., y_{n-1}$ new variables where $n \leq |UngPos(e'|_p)|$. Then*

$$\Pi \cup \{e\}; K \rightsquigarrow_{T/AC} \Pi \cup \{e'[r + \bar{y}_n]_p\}; K \cup \{l + \bar{y}_n =^?_{AC} e'|_p\}.$$

Using this relation, AC-narrowing is complete. For instance, in the previous example we get:

$$\bar{x}_n =^?_E c; \emptyset \rightsquigarrow_{T/AC} c + \bar{y}_n =^?_E c; z + z + \bar{y}_n =^?_{AC} \bar{x}_n$$

now considering $\theta' := \theta \cup \{z \longleftarrow \bar{a}_{n/2}, y_1 \longleftarrow b, ..., y_n \longleftarrow b\}$ we see that the Hullot property is satisfied.

This example also explains the inequality $n \leq |UngPos(e'|_p)|$: the Hullot property would not be satisfied using less than n new variables.

The notion of narrowing bound translates to the AC-case simply considering inner reductions modulo AC. Let E be equivalent to a convergent AC-TRS T and let H be a narrowing bound for T. Given an E-unification problem Π, the following procedure decides its E-unifiability:

Decision Procedure (AC case)
1. Guess $n \leq H(\Pi)$.
2. Guess a sequence $\Pi; \emptyset \rightsquigarrow_{T/AC} \Pi_1; K_1 \rightsquigarrow_{T/AC} \ldots \rightsquigarrow_{T/AC} \Pi_n; K_n$.
3. Answer 'yes' iff $\Pi_n \cup K_n$ is AC-unifiable.

Again, the proof of the completeness should be substantially obvious, but it requires some technical notations to deal with AC-symbols [23].

4.1 Complexity

Implicit extensions do not affect the complexity of our decision procedure: all we have to do is to guess the number of new variables, which is bounded by the size of the term being considered. In addition, given a term s we can guess in non-deterministic polynomial time any term s' such that $s =_{AC} s'$. Noticing that AC-unifiability is in NP [12] gives the following:

Theorem 5. *Let E be an equational theory and T a convergent AC-TRS equivalent to E. If there is a polynomial narrowing bound for T then E-unifiability is in NP.*

Polynomial narrowing bounds exist for significant AC-TRS, as we shall see in the next section. However, we can't hope in a result as Corollary 1. To see this, consider $E := AC \cup \{a + b \approx b\}$ and $T := \{a + b \to b\}$. The point is: if a term s is in normal form, how many reductions do we need to take $s + b$ to its normal form? This clearly depends on the number of a's in s, which might be exponential in the size of the unification problem. More precisely, using an argument similar to one in [19], we define for every $n \geq 1$ the unification problem $\Pi_n :=$

$$\begin{aligned} x + b &=^?_E b \\ x &=^?_E x_1 + x_1 \\ x_1 &=^?_E x_2 + x_2 \\ &\ldots \\ x_{n-1} &=^?_E x_n + x_n \\ x_n &=^?_E a \end{aligned}$$

If $\theta \models \Pi_n$, then θx contains 2^n a's. Therefore we need 2^n reduction steps to take $\theta(x + b)$ to its normal form b, since each application of the rule $a + b \to b$ removes a single a.

We conclude this section explaining why we use inner reductions instead of innermost ones. Let's consider the same set of problems $\{\Pi_n\}$ above, but now let $E := AC \cup \{x + b \approx b\}$ and $T := \{x + b \to b\}$. As before, if $\theta \models \Pi_n$ then θx contains 2^n a's. If we used innermost reductions then we would need 2^n reduction steps to take $\theta(x+b)$ to its normal form b. On the other hand, $\theta(x+b) \longmapsto b$ by just *one* inner reduction step. To sum it up: using innermost reductions there is no polynomial narrowing bound for T, while using inner reductions (one can prove) there is.

4.2 Application in Process Algebra

As mentioned before, applications of our method can be found in *Process Algebra* [4]. We can in particular prove NP-completeness of unifiability modulo bisimulation in minimal process algebra with proper iteration (MPA_δ^+) [7]. This is the so-called *compatibility checking* problem for MPA_δ^+, a significant extension of that for $BCCSP$, studied in [8]. See [8, 10] for motivation and a survey of the compatibility checking.

In the following, let A be a fixed set of actions. The signature of MPA_δ^+ consists of a constant δ, which represents *deadlock*, the binary *alternative composition* $x + y$, the unary prefix *sequential composition* $a(x)$ and the proper *iteration* $a^+(x)$, for $a \in A$. Often, $a(t)$ and $a^+(t)$ will be abbreviated by at and a^+t, which bind stronger than the alternative composition $+$.

The following is a complete equational axiomatization of bisimulation equivalence for MPA_δ^+ [7]:

$$
\begin{aligned}
(x + y) + z &\approx x + (y + z) \\
x + y &\approx y + x \\
x + x &\approx x \\
x + \delta &\approx x \\
a(a^+x + x) &\approx a^+x \qquad \forall a \in A \\
a^+(a^+x + x) &\approx a^+x \qquad \forall a \in A
\end{aligned}
$$

We call this theory Bis^+. So we would like to decide Bis^+-unifiability. One could notice that Bis^+ can be seen as the union of $ACI1$ and two axioms for iteration. $ACI1$-unifiability is decidable [16] (we will give a new proof in the next section), so one may hope to use standard combination techniques for the union of equational theories. But the combination techniques currently available, see for instance [1], can not deal with this case, because these would require the whole equational theory to be equal to a union of equational theories over *disjoint* signatures, which is impossible because of the axiom $a(a^+x + x) \approx a^+x$.

We can of course try to apply our results on AC-narrowing, so we need a convergent AC-TRS equivalent to Bis^+. Such an AC-TRS is reported in Table 2 [7], and we call it T. This shifts the problem towards finding a narrowing bound for T. But *size* is such!

Theorem 6. *Size is a polynomial narrowing bound for T.*

$x + x \to x$		
$x + \delta \to x$		
$a(a^+x + x) \to a^+x$	$\forall a \in A$
$a^+(a^+x + x) \to a^+x$	$\forall a \in A$
$a(a^+\delta) \to a^+\delta$	$\forall a \in A$
$a^+(a^+\delta) \to a^+\delta$	$\forall a \in A$

Table 2. Rewrite rules of the AC-TRS T

Proof. We prove that if $s = t + u$, where both t and u are in normal form, then $s\overset{1}{\downarrow}_{T/AC}$. The rest of the proof proceeds exactly as that of Corollary 1.

If s is in normal form then we are done.

If $t = \delta$ ($u = \delta$) then $s \longmapsto_{T/AC} u$ (t) and we are done.

Otherwise, we reduce by the rule $x + x \to x$. Intuitively, we simply have to choose the greatest substitution that fits. More formally, we associate to every term v the multiset $M(v)$, which is defined as follows:

$$\begin{array}{ll} M(v) := M(w) \cup M(w') & \text{if } v = w + w' \\ M(v) := \{[v]_{AC}\} & \text{otherwise} \end{array}$$

where $\cup$ is the union between multisets [2] and $[v]_{AC}$ is the equivalence class of v modulo AC. Now consider the case where $t \neq \delta$, $u \neq \delta$ and $t + u$ is not in normal form. Let w be a term such that $M(w) = M(t) \cap M(u)$, and reduce applying the rule $x + x \to x$ with substitution $\theta := \{x \leftarrow w\}$. It is easily seen that we get a normal form.

In any case, we perform at most one inner reduction step, so we can conclude $s\overset{1}{\downarrow}_{T/AC}$. □

Applying Theorem 5, we get that Bis^+-unifiability is in NP. In [8] it is proven that Bis-unifiability (Bis is Bis^+ without the two axioms for iteration) is NP-hard. The proof also works for Bis^+-unifiability. So the upper bound on the complexity of Bis^+-unifiability we have just shown is tight:

Theorem 7. *Bis^+-unifiability is NP-complete.*

To conclude, we point out that Bis^+-unifiability is (polynomially) equivalent to unifiability modulo bisimulation in minimal process algebra with prefix iteration (MPA^*_δ) [10].

4.3 Other Applications

We briefly discuss other applications of our decision procedure.

NP-decidability of both ACI-unifiability and $ACI1$-unifiability are well-known results, which can be proven via *ad hoc* decision procedures [16] or via combination techniques [1].

Our method can be used to reobtain them under a different and unified point of view: the *AC-TRS* $\{x+x \to x\}$ and $\{x+x \to x, x+1 \to x\}$ are convergent and equivalent to ACI and $ACI1$, respectively. Furthermore, $size$ is a polynomial narrowing bound for them (the proof is a sub-case of the proof of Theorem 6). So our results hold and we get NP-decidability. It follows that our method can be used to prove NP-decidability of Bis-unifiability, since this is the same as $ACI1$-unifiability [8].

5 Conclusion

We have presented a narrowing-based method to decide E-unifiability when E is equivalent to a convergent (AC-)TRS. The method guarantees NP-decidability when a polynomial narrowing bound exists, and we have studied general conditions under which this existence is guaranteed.

These results have been used to provide an optimal and new result in Process Algebra, namely Bis^+-unifiability. They have also given (new) proofs under a unified point of view of NP-decidability of $I, ACI, ACI1$-unifiability and of unifiability in quasi-groups and central groupoids.

Our approach shows that sometimes E-unifiability can be shifted towards finding a narrowing bound for a convergent (AC-)TRS equivalent to E. We are currently working on weaker conditions which guarantee the existence of a polynomial narrowing bound for a convergent (AC-)TRS.

Acknowledgment: I thank professor Marisa Venturini Zilli for having introduced me to the unification problems and for her helpful reading of this paper.

References

1. F. Baader and K. U. Schulz. Unification in the union of disjoint equational theories: combining decision procedures. *Journal of Symbolic Computation*, 21(2):211-244, 1996.
2. F. Baader and T. Nipkow. *Term rewriting and all that.* Cambridge University Press, 1998.
3. F. Baader, W. Snyder. Unification theory. In A. Robinson and A. Voronkov, editors, *Handbook of automated reasoning*, Elsevier Science Publishers B.V., 1999.
4. J. C. M. Baeten and W. P. Weijland. *Process Algebra.* Cambridge University Press, 1990.
5. H.-J. Bürckert. A resolution principle for a logic with restricted quantifiers. LNAI vol. 568, Springer Verlag, 1991.
6. A. Colmerauer. An introduction to PROLOG III. *C. ACM* 33, 69-90, 1990.
7. W. Fokkink. A complete equational axiomatization for prefix iteration. *Information processing letters*, 52(6):333-337, 1994.
8. Q. Guo, P. Narendran, and S. K. Shukla. Unification and Matching in process Algebras. In T. Nipkow, editor, *Proceedings of 9th RTA*, LNCS vol. 1379, 1998.
9. J.-M. Hullot. Canonical forms and unification. In W. Bibel and R. Kowalski, editors, *Proceedings of the 5th International Conference on Automated Deduction*, LNCS vol. 87, 318-334, 1980.
10. B. Intrigila, M. Venturini Zilli and E. Viola. Unification problems over process languages. Technical Report SI-00/01. Dipartimento di Scienze dell'Informazione, University of Rome "La Sapienza", Rome, 2000.

11. J.-P. Jouannaud, C. Kirchner. Solving equations in abstract algebras: A rule-based survey of unification. In J.-L. Lassez and G. Plotkin, editors, *Computational Logic: Essays in Honor of A. Robinson*, MIT Press, Cambridge, MA, 1991.
12. D. Kapur and P. Narendran. Complexity of unification problems with associative-commutative operators. *J. Automated Reasoning* 9:261-288, 1992.
13. D. Kapur and P. Narendran. Matching, unification and complexity. *SIGSAM Bulletin,* 1987.
14. D. Kapur and P. Narendran. Double exponential complexity of computing complete sets of AC-unifiers. In *Proceedings of the 7th Annual IEEE Symposium on Logic in Computer Science*, Santa Cruz, California, 11-21, 1992.
15. C. Kirchner, H. Kirchner and M. Rusinowitch. Deduction with symbolic constraints. *Revue d'Intelligence Artificielle* (Special issue on Automatic Deduction), 4(3):9-52, 1990.
16. P. Narendran. Unification modulo ACI+1+0. *Fundamenta Informaticae*, 25(1):49-57, 1996.
17. R. Nieuwenhuis. On Narrowing, Refutation proofs and Constraints. In J. Hsiang, editor, *Proceedings of 6th RTA*, LNCS vol. 914, 1995.
18. R. Nieuwenhuis. Decidability and Complexity Analysis by Basic Paramodulation. *Information and Computation* 147:1-21, 1998.
19. M. Paterson, M. Wegman. Linear unification. *Journal of Computer and System Sciences*, 16(2):158-167, 1978.
20. G. Peterson, M. Stickel. Complete sets of reductions for equational theories with complete unification algorithms. *Journal of the ACM* 28(2):233-264, 1981.
21. G. Plotkin. Building-in Equational Theories. *Machine Intelligence*, 7:73-90 1972.
22. L. Vigneron. Automated Deduction Techniques for Studying Rough Algebras. *Fundamenta Informaticae* 33, 85-103, 1998.
23. E. Viola. *E-unificabilità: decidibilità, complessità e algebre di processi*. B.S. Thesis, Dipartimento di Scienze dell'Informazione, University of Rome "La Sapienza", Rome, 2000.