Decidability of unification modulo two theories of division

Zhenjiang Dai
*University at Albany, State University of New York*, 934197457@qq.com

The University at Albany community has made this article openly available. Please share how this access benefits you.

Follow this and additional works at: https://scholarsarchive.library.albany.edu/legacy-etd

Part of the Computer Sciences Commons

Recommended Citation

This Master's Thesis is brought to you for free and open access by the The Graduate School at Scholars Archive. It has been accepted for inclusion in Legacy Theses & Dissertations (2009 - 2024) by an authorized administrator of Scholars Archive. Please see Terms of Use. For more information, please contact scholarsarchive@albany.edu.
DECIDABILITY OF UNIFICATION MODULO TWO THEORIES OF
DIVISION

by

Zhenjiang Dai

A Thesis
Submitted to the University at Albany, State University of New York
in Partial Fulfillment of
the Requirements for the Degree of
Master of Science.

College of Engineering and Applied Sciences
Department of Computer Science
2018
ACKNOWLEDGMENT

I wish to thank Professor Paliath Narendran for his help with my thesis. I am really glad to have had Professor Narendran as my thesis advisor. I have taken his courses throughout my graduate career. I would like to thank him for his patience, he is very good at teaching. I have gotten so much help from him while I was writing this thesis. He gave me the reference papers, solved my questions, and helped me revise this thesis. He sacrificed a lot of time for my thesis. I really appreciate that and I felt very comfortable working with him.

I thank Professor Jeong-Hyon Hwang for being part of my committee at very short notice.

I would also like to thank Ph.D. student Yu Zhang for her time and help. At first, I found this topic a little difficult. She was very patient, helpful and she found some definitions which helped me a lot. I thank her for her time and discussing my thesis with me.

Thank you all from my heart, because without your help, I could not have finished this thesis.
ABSTRACT

We study decidability of a term rewriting system $R$ modulo equational theories associative ($A$) or associative-commutative ($AC$). The study of this problem is motivated by possible applications to handle multiplication ($*$) and division ($/$) algebras. We use several steps to prove the term rewriting system $R$ modulo equational theories is decidable.
1 Introduction

It is very difficult to deal with commutative operators in a term rewriting system. This is a major problem since associativity and commutativity are properties that are satisfied by many mathematical operators. The main approach to deal with this issue is to build these properties into the unification and matching algorithms, i.e., we include these two identities into a set $E$, and treat them as two properties of the operator when we apply the other rules in $R$. The standard rewrite step $\to_R$ is changed to $\to_{R,E}$ [1]:

$$s \to_{R,E} t \iff \exists (l \to r) \in R, p \in \text{Pos}(s), \sigma : [s|_p \approx_E \sigma(l) \land t = s[\sigma(r)]_p]$$

This is often called extended rewriting.

In our project, we consider the rewrite relation $\to_{R,E}$ for two equational theories $A$ and $AC$. The rewrite rules of the term rewriting system $R$ are
Equational theories $A$ and $AC$ are:

$$A : x * (y * z) \approx (x * y) * z$$

$$AC : x * (y * z) \approx (x * y) * z, \ x * y \approx y * x$$

In order to prove that unification modulo $R \cup E$ is decidable for each theory $E$, we divide the proof into two parts. First we prove that $\rightarrow_{R, E}$ is convergent modulo $E$. Secondly, we prove that $\rightarrow_{R, E}$ is forward-closed. Thus unification modulo the equational theory $\approx_{R \cup E}$ is decidable.

2 Preliminaries

A term $s$ can be treated as a tree, $\text{Pos}(s)$ means all the positions in the tree. $s|_p = \text{subterm/subtree at position } p$. $\varepsilon$ represents the root position of a tree.

If a term rewriting system is both terminating and (local) confluent, then it is convergent. Hence in our case, in the first step, we want to prove $\rightarrow_{R, E}$ is convergent modulo $E$, we should prove $\rightarrow_{R, E}$ is terminating firstly then prove confluent.

We use lexicographic path ordering ($lpo$) to prove terminating. If $l >_{lpo} r$ for all rules $(l \rightarrow r) \in R$ then $\rightarrow_R$ is terminating.

A convergent rewrite system $R$ is forward-closed if and only if every innermost redex (reducible expression) can be reduced to its $R$-normal form in one step. A term $t$ is an innermost redex of a rewrite system $R$ if and only if all proper subterms of $t$ are irreducible and $t$ is an instance of the left-hand side of a rule in $R$ [4].
3 Proving $\rightarrow_{R_1 \cup R_2}$ is convergent modulo $\approx_{R_2}$ for some $R_1$ and $R_2$

Lemma 1. If $\rightarrow_{R_1 \cup R_2}$ is convergent, $\rightarrow_{R_1 \cup R_2}$ is terminating and the following commuting property

$$\forall t, t_1, t_2 : \left[ t_1 \rightarrow_{R_2} t \land t \rightarrow_{R_1 \cup R_2} t_2 \iff \exists t_3 : t_1 \rightarrow_{R_1 \cup R_2} t_3 \land t_2 \downarrow_{R_1 \cup R_2} t_3 \right]$$

holds (see Figure 1), then $\rightarrow_{R_1 \cup R_2}$ is convergent modulo $\approx_{R_2}$.

Proof. If the commuting property holds, then the following more general commuting property can be proved by induction:

$$\forall t, t_1, t_2 : t_1 \rightarrow_{R_2} t \land t \rightarrow_{R_1 \cup R_2} t_2 \Rightarrow \exists t_3 : t_1 \rightarrow_{R_1 \cup R_2} t_3 \land t_2 \downarrow_{R_1 \cup R_2} t_3$$

Suppose $\rightarrow_{R_1 \cup R_2}$ is not confluent modulo $\approx_{R_2}$. Let $s_1$ and $s_2$ be terms such that $s_1 \approx_{R_1 \cup R_2} s_2$, $s_1 \neq_{R_2} s_2$ and both $s_1$ and $s_2$ are in normal form with respect to $\rightarrow_{R_1 \cup R_2}$. Since $s_1 \neq_{R_2} s_2$ and $s_1 \approx_{R_1 \cup R_2} s_2$, we can assume, without loss of generality, that there exist terms $s'_1$ and $s''_1$ such that $s_1 \rightarrow_{R_2} s'_1 \rightarrow_{R_1} s''_1$. But then it follows from the general commuting property that $s_1$ itself is reducible by $\rightarrow_{R_1 \cup R_2}$ which is a contradiction. \hfill \Box

4 Proving convergence modulo $A$

In this section, we first prove that $\rightarrow_{R \cup A}$ is terminating, then we prove $\rightarrow_{R \cup A}$ is confluent. By combining theses two proofs we can conclude that $\rightarrow_{R \cup A}$ is convergent modulo $A$.

4.1 Proving termination

Lemma 2. The rewriting system $\rightarrow_{R \cup A}$ is terminating.
Proof. $R$ is size-decreasing and right-linear and $A$ is size-preserving and linear. □

4.2 Proving confluence

In this section we prove $\rightarrow_{R,A}$ is confluent modulo $A$.

Lemma 3. The rewriting system $\rightarrow_{R,A}$ is convergent.

Proof. Termination can be shown using the lexicographic path ordering ($lpo$). Confluence can be shown by demonstrating that every critical pair is joinable. For instance, when we consider rule 1 and rule $A$ ($u*(v*w) \approx (u*v)*w$), we have the critical pairs

$$\langle f(u,y), f((u*v)*w, y*(v*w)) \rangle, \text{ and } \langle f(x,u), f(x*(v*w), (u*v)*w) \rangle.$$

In both cases, the term on the right can be reduced to the left term by applying rule $A$ then applying rule 1 twice in these two critical pairs. □
Lemma 4. (a) Let $t = f(t_1, t_2)$ be an A-redex, i.e., $t \approx_A \sigma(l)$ for some left-hand side $l$. Then, for all $t'$ such that $t \approx_A t'$, we have $t' \rightarrow_{R,A} \sigma(r)$.

(b) Let $t = t_1 * t_2 \approx_A \sigma(l)$ for some left-hand side $l$. Then for all $t'$ such that $t \approx_A t'$, there exists $t''$ such that $t' \rightarrow_{R} t''$ and $t'' \downarrow_{R,A} \sigma(r)$.

Proof. Since $t' \approx_A t$ and $t \approx_A \sigma(l)$, we have $t' \approx_A \sigma(l)$, then we can get $t' \rightarrow_{R} t''$ and $t'' \downarrow_{R,A} \sigma(r)$. \hfill \square

Lemma 5. Let $t_1 \rightarrow_{R_2}^{q} t \rightarrow_{R_1,R_2}^{p} t_2$ and $p \preceq q$. Then $t_1 \rightarrow_{R_1,R_2}^{p} t_2$.

Proof. Since $t_1 \rightarrow_{R_2}^{q} t \rightarrow_{R_1,R_2}^{p} t_2$, there must be rules $(l \rightarrow r) \in R_1$ and $(l' \rightarrow r') \in R_2$ such that

$$t|_p \approx_{R_2} \sigma(l) \text{ and } t_1|_q \approx_{R_2} \sigma'(l')$$

for some substitutions $\sigma, \sigma'$. Since variables in the rules can be renamed we can assume that $\sigma = \sigma'$. Thus $t = t_1[\sigma'(r')]_q$. Since $p \preceq q$ we get $t_1|_p \approx_{R_2} t|_p \approx_{R_2} \sigma(l)$, and thus $t_1|_p \rightarrow_{R_1,R_2}^{p} \sigma(r) = t_2|_p$. It follows that $t_1 \rightarrow_{R_1,R_2}^{p} t_2$. \hfill \square

Lemma 6. For any term $t$, if $t \rightarrow_{R,A} t_2$ and $t \rightarrow_{A^{-1}} t_1$, then there exists a term $t_3$, having $t_1 \rightarrow_{R,A} t_3$ and $t_2 \downarrow_{R,A} t_3$. (Figure 4)

Proof. First of all, we can assume that all the terms we consider are ground terms. For any term $t$, if $t \rightarrow_{R,A} t_2$ then

$$\exists (l_1 \rightarrow r_1) \in R, p \in Pos(t), \sigma_1 : t|_p \approx_{A} \sigma_1 l_1 \land t_2 = t[\sigma_1 r_1]|_p.$$ 

If $t \rightarrow_{A^{-1}} t_1$ then

$$\exists q \in Pos(t), \sigma_2 : t|_q \approx_{A} \sigma_2 r_1 \land t_1 = t[\sigma_2 l_1]|_q$$
Figure 5: If $p$ and $q$ are disjoint positions where $A^{-1} = (r_A = (x * y)^* z \approx x * (y * z) = l_A)$. We now have to analyse all the possible relations between $p$ and $q$.

If $p$ and $q$ are disjoint positions, then it is trivial to prove this lemma as shown in Figure 5.

If $p$ and $q$ are comparable, then we need to consider 3 different cases with respect to 3 different relations between $p$ and $q$.

Case 1: If $p = q$ then this case can be proved by Lemma 4.

Case 2: Suppose $q \prec p$. We can assume that $q = \epsilon$. Then $t = (s_1 * s_2) * s_3$ and $t_1 = s_1 * (s_2 * s_3)$ for some terms $s_1$, $s_2$ and $s_3$. We only need to consider the case $p = 1$, since if $11 \preceq p$, $12 \preceq p$ or $2 \preceq p$, then $t_1$ is also reducible by $\rightarrow_{R,A}$ and the result follows.

If $p = 1$, then $s_1 * s_2 \approx_A \sigma(X) * 1$ for some substitution $\sigma$, or $s_1 * s_2 \approx_A 1 * \sigma(X)$ for some substitution $\sigma$. In the first case, it is not hard to see that the substitution $\sigma$ can be extended to $\sigma' = \{X \mapsto \sigma(X) * s_3\}$ such that $(s_1 * s_2) * s_3 \approx_A \sigma'(X) * 1$. The other case follows from symmetry.

Case 3: The case $p = \epsilon \preceq q$ follows from Lemma 5. □

**Lemma 7.** The term rewriting system $\rightarrow_{R,A}$ is confluent modulo $A$.

**Proof.** This follows from Lemma 1. □

**Lemma 8.** The term rewriting system $\rightarrow_{R,A}$ is convergent modulo $A$.

**Proof.** From Section 4.1 we get the term rewriting system $\rightarrow_{R,A}$ is terminating. According to Section 4.2 we prove $\rightarrow_{R,A}$ is confluent modulo $A$. Hence the term rewriting system $\rightarrow_{R,A}$ is convergent modulo $A$. □
5 Proving $\rightarrow_{R,A}$ is forward-closed

**Lemma 9.** The term rewriting system $\rightarrow_{R,A}$ is forward-closed.

**Proof.** According to the lemma proved in [4], we need to figure out whether every innermost redex can be reduced to its normal form with respect to $\rightarrow_{R,A}$ in one step. We analyse all possible innermost redexes for every rule in $R$:

Rule 1: An innermost redex of rule 1 can be viewed as $f(t_1 \ast t_2, t_3)$ where $t_1$, $t_2$ and $t_3$ are any terms that are irreducible and not equal to 1 whereas $t_1 \neq t_3$. Then the whole term can be reduced to $f(t_1, t_3)$ by just applying rule 1 in one step. If the new term $f(t_1, t_3)$ is irreducible then it is in normal form with respect to $\rightarrow_{R,A}$. Otherwise, the new term $f(t_1, t_3)$ can only be reduced by rule 5 or 6, which means $t_3 = t_4 \ast t_1$ or $t_1 = t_4 \ast t_3$. Then in this case, the original term $f(t_1 \ast t_2, t_3) \ast t_2$ can be reduced to normal form $f(1, t_4)$ or $f(t_4, 1)$ by $\rightarrow_{R,A}$ in one step.

It is trivial to prove innermost redex of rules 2, 3, and 4 can be reduced to their normal forms in one step.

Rule 5: An innermost redex of rule 5 can be viewed as $f(t_1, t_2 \ast t_1)$ where $t_1$ and $t_2$ are any terms that are irreducible and not equal to 1. Then it can be reduced to a new term $f(1, t_2)$ which is in normal form in one step.

Rule 6: This case is almost the same as that of rule 5.

Hence every innermost redex can be reduced to normal form with respect to $\rightarrow_{R,A}$ in one step. Therefore $\rightarrow_{R,A}$ is forward-closed.

6 Proving unification modulo $\approx_{R \cup A}$ is decidable

**Lemma 10.** Unification modulo $\approx_{R \cup A}$ is decidable.

**Proof.** Since $\rightarrow_{R,A}$ is convergent and forward-closed, unification modulo $\approx_{R \cup A}$ is decidable.

7 Proving convergence modulo AC

**Lemma 11.** The term rewriting system $\rightarrow_{R,AC}$ is convergent modulo AC.
Proof. The rewriting system can be checked convergence modulo $AC$ automatically by using RRL. Here we give an example of critical pair. When we superpose rule 1 and $C(u*v \approx v*u)$, we have the critical pair $(f(u,y), f(v*u,y*v))$, however the right term can reduce to the left term by applying $\rightarrow_{R,AC}$ in one step. Hence the critical pair is joinable. 

8 Proving $\rightarrow_{R,AC}$ is forward-closed

Lemma 12. The term rewriting system $\rightarrow_{R,AC}$ is forward-closed.

Proof. Just as for Lemma 9, we need to analyse all possible innermost redexes for all rules in $R$:

If the root symbol of an innermost redex is $f$, then the term is of the form $f(s_1, s_2)$.

If it is the innermost redex of rule 1, then we have $s_1 \approx_{AC} \sigma(x) * \sigma(z)$ and $s_2 \approx_{AC} \sigma(y) * \sigma(z)$ whereas $\sigma(z)$ is the biggest common part between $s_1$ and $s_2$. Then the whole redex can be reduced to $f(\sigma(x), \sigma(y))$ in one step. Since there is no common part between $\sigma(x)$ and $\sigma(y)$, $f(\sigma(x), \sigma(y))$ will be in normal form with respect to $\rightarrow_{R,AC}$.

If it is the innermost redex of rule 2, then $s_1 = s_2$ and it can be reduced to 1 in one step.

If it is the innermost redex of rule 5, then we have $s_1 \approx_{AC} \sigma(z)$ and $s_2 \approx_{AC} \sigma(y) * \sigma(z)$ whereas $\sigma(y)$ is not equal to 1. Then the redex can be reduced to $f(1, \sigma(y))$ which is in normal form.

If it is the innermost redex of rule 6, then we have $s_1 \approx_{AC} \sigma(x) * \sigma(z)$ and $s_2 \approx_{AC} \sigma(z)$ whereas $\sigma(x)$ is not equal to 1. Then the redex can be reduced in one step to $f(\sigma(x), 1)$ which is in normal form.

If the root symbol of an innermost redex is $\ast$, then the term can be viewed as $t_1 * t_2$, and at least one of $t_1$ and $t_2$ should be 1. Suppose $t_1 = 1$, then this innermost redex can be reduced in one step to $t_2$ which is in normal form. 

9 Proving unification modulo $\approx_{R \cup AC}$ is decidable

Lemma 13. Unification modulo $\approx_{R \cup AC}$ is decidable.

Proof. Since $\rightarrow_{R,AC}$ is convergent and forward-closed, unification modulo $\approx_{R \cup AC}$ is decidable. 

References


