Available online at www.sciencedirect.com
ScienceDirect
Information and Computation 205 (2007) 624–650
Information and Computation
www.elsevier.com/locate/ic

Permutative rewriting and unification☆

Thierry Boy de la Tour *, Mnacho Echenim

LEIBNIZ laboratory, IMAG - CNRS INPG, 46 avenue Félix Viallet, F-38031 Grenoble Cedex, France

Received 9 September 2005; revised 29 September 2006
Available online 25 January 2007

Abstract

Permutative rewriting provides a way of analyzing deduction modulo a theory defined by leaf-permutative equations. Our analysis naturally leads to the definition of the class of *unify-stable* axiom sets, in order to enforce a simple reduction strategy. We then give a uniform unification algorithm modulo theories E axiomatized this way. We prove that it computes complete sets of unifiers of simply exponential cardinality, and that the E-unification decision problem belongs to **NP**.

Keywords: Equational theories; Term rewriting; E-unification; Permutation groups

1. Introduction

Unification, or the task of solving equations, is among the fundamental tools of Automated Reasoning. In *equational unification*, equations must be solved modulo a theory given by a set E of equational axioms. This is especially useful when E does not lead to a terminating rewrite relation, as in the well-studied theories C (commutativity, see [4]) and AC (C + associativity, see [21,9,10]). By contrast with the general case, C and AC-unification are decidable and *finitary*, i.e. any equation admits a finite set of minimal solutions w.r.t. subsumption.

☆ This work has been supported by CNRS and MENRT.
* Corresponding author. Fax: +33 4 76 57 50 81.
E-mail addresses: Thierry.Boy-de-la-Tour@imag.fr (T. Boy de la Tour), M.Echenim@imag.fr (M. Echenim).

0890-5401/$ - see front matter
doi:10.1016/j.ic.2006.11.001

This raises the problem of extending such results to *classes* of theories containing C or AC. In [20] Schmidt-Schauß considered the class of *permutative* theories (defined by axioms $s \approx t$ where t can be obtained from s by permuting occurrences of symbols), and proved the undecidability of unification in one such theory. This result was later extended in [17] to the smaller class of *variable-permuting* theories (where only occurrences of variables may be permuted). The even smaller class of *leaf-permutative* theories is obtained by restricting the terms in the axioms to be linear. The decidability status of leaf-permutative unification is not known, while the existence of infinitary problems, questioned in [14], has been established in [19], by considering a theory defined by two axioms involving two function symbols. In [15], a similar result was proved with a leaf-permutative theory defined by a single axiom with a single function symbol, namely

$$f(f(x_1,x_2), f(x_3,x_4)) \approx f(f(x_1,x_3), f(x_2,x_4)).$$

Actually, we can exhibit an infinitary unification problem with an even simpler axiom: $f(f(x, y),z) \approx f(f(y,x),z)$. If we call $C1$ this theory (the arguments of an occurrence of f commute when it appears as the first argument of another occurrence of f) and consider the unification problem $f(x,z) =^?_{C1} f(y,z)$, it is easy to see that

$$\theta_n = \begin{cases} x \leftarrow f(x_1, f(\ldots, f(x_n, f(u,v))\ldots)) \\ y \leftarrow f(x_1, f(\ldots, f(x_n, f(v,u))\ldots)) \end{cases}$$

is a $C1$-unifier of our problem; the fact that $x\theta_n$ occurs as first argument of f in $f(x,z)\theta_n$ triggers a cascade of commutations, down to $f(f(u,v),x_n) \approx f(f(v,u),x_n)$, and similarly for $y\theta_n$. Yet these unifiers are independent of each other, i.e. for any $m < n$, θ_m does not $C1$-subsume θ_n.

The problem is of course the overlap between the axioms (or the self-overlap of an axiom). However, at the other end of the spectrum, it was proved in [1] that unification modulo theories with *flat* leaf-permutative axioms (of depth 1, and without constant symbols), is finitary. Hence some amount of overlapping is admissible, as in the theory $S4$ defined by the two axioms

$$f(x, y,z,u) \approx f(y,x,z,u) \text{ and } f(x, y,z,u) \approx f(y,z,u,x);$$

which contains all identities $f(x, y,z,u) \approx f(x, y,z,u)\sigma$ for permutations σ of $\{x, y,z,u\}$. This is due to the fact that the two permutations $(x\ y)$ and $(x\ y\ z\ u)$ generate the whole symmetric group on $\{x, y,z,u\}$.

Our goal is to exploit this group-theoretic structure, by introducing *permutative rewriting* in Section 3 (here, *permutative* refers to the use of permutation groups). The rewriting system is represented concisely by a set $\mathcal{C}$ of linear terms and a function that to each of these terms associates a group of permutations of its variables.

However, all the terms congruent to the left-hand side of a leaf-permutative axiom may not be obtained by permutations of the variables, for instance the theory AC can be defined by two leaf-permutative axioms $f(x, y) \approx f(y,x)$ and $f(f(x, y),z) \approx f(f(y,z),x)$, which entail the axiom of associativity $f(f(x, y),z) \approx f(x, f(y,z))$, and this axiom is not leaf-permutative. We therefore define a condition of *unify-stability* on $\mathcal{C}$ that rules out this possibility, by ensuring that the underlying rewriting system is closed under critical pairs.