Article Submitted to Journal of Symbolic Computation

On Using Ground Joinable Equations in Equational Theorem Proving

J. Avenhaus, Th. Hillenbrand and B. Löchner

Fachbereich Informatik, Universität Kaiserslautern
67663 Kaiserslautern, Germany

Abstract

When rewriting and completion techniques are used for equational theorem proving, the axiom set is saturated with the aim to get a rewrite system that is terminating and confluent on ground terms. To reduce the computational effort it should (1) be powerful for rewriting and (2) create not too many critical pairs. These problems become especially important if some operators are associative and commutative (AC). We show in this paper how these two goals can be reached to some extent by using ground joinable equations for simplification purposes and omitting them from the generation of new facts. For the special case of AC-operators we present a simple redundancy criterion which is easy to implement, efficient, and effective in practice, leading to significant speed-ups.

1. Introduction

Equational theorem proving deals with the following problem. Given is a set $E = \{s_i = t_i \mid i = 1, \dots, n\}$ of equations and an equation $u = v$ over a fixed signature sig. All equations are implicitly universally quantified. The question is whether $u = v$ is a logical consequence of E.

In the last years rewriting and completion techniques have proved to be the most powerful tools to solve this problem. The approach is to saturate E into a rewrite system such that $\bar{u} = \bar{v}$ (i. e. the skolemized version of $u = v$) can be proved by joinability. Many state-of-the-art provers based on this technique soon reach their limit whenever some of the operators are associative and commutative: They get stuck in an overwhelmingly large set of newly generated equations. This is due to the fact that the commutativity law is applicable almost everywhere and so creates many critical pairs. This and the associativity axiom alone lead to an infinite set of equations.

In this paper we use ground joinable equations to overcome this problem to some extent. The basic idea is simple. Ground joinable equations may be used for rewriting, but need not to be considered for computing critical pairs. We show that this idea may lead to a large gain in efficiency. A restricted version of this approach contributed significantly to the success of our WALDMEISTER prover (Hillenbrand *et al.*, 1997) at the CADE-16 system competition (Sutcliffe, 2000). There it was by far the most powerful system in the unit equality class.

Completion and rewriting techniques for equational theorem proving go back to the seminal paper (Knuth and Bendix, 1970). To avoid failure of the completion process due to unorientable equations there exist several proposals (Peterson, 1983; Hsiang and Rusinowitch, 1987). In theorem proving it is advantageous if some criteria guarantee that without losing completeness only a subset of the critical pairs needs to be considered (Bonacina and Hsiang, 1995). We use here basically the approach in (Bachmair *et al.*, 1989). It has early been noticed (Lankford, 1975) that standard completion techniques are not powerful enough to handle AC-operators, i. e. operators being associative and commutative. One technique is to complete and rewrite modulo an underlying theory E_0, e. g. AC-theories (Peterson and Stickel, 1981). But this approach needs unification modulo E_0 and matching modulo E_0. For the AC-case both are known to be solvable, but very expensive, and are not easy to implement efficiently. There are other refinements of KB-completion, such as basic completion or the use of constraints (Nieuwenhuis and Rubio, 1995; Peterson, 1990).

Our interest, however, is in techniques that can easily be integrated into existing systems which use the standard (unfailing) approach. We think that this is sensible since these systems have been developed under considerable effort and have been tested extensively. State-of-the-art provers employ sophisticated indexing methods (Graf, 1996) and can cope with millions of facts efficiently due to specialized storing techniques (Buch and Hillenbrand, 1996). So in this paper we study the question how unfailing completion can be refined in a way which is simple to implement in the mentioned systems and improves them for solving more non-trivial problems, especially if AC-operators are involved. For a simple example which shows the considerable improvements achievable, see Chapter 3.

It is known (Lankford, 1975) that saturating the set E of equations in order to approximate only ground confluence is sufficient for equational theorem proving. Many improvements of theorem proving procedures can be formulated within the concept of redundancy (Bachmair and Ganzinger, 1994). For example, equations whose ground instances already have a smaller proof are redundant and can be deleted. We propose to keep such equations for simplification purposes and show in Chapter 4 that despite that, no critical pairs have to be built with them. Therefore, this approach combines the advantage of pruning the search space with the benefits of a stronger simplification relation. The completeness of our proof system can be shown within the framework of (Bachmair and Ganzinger, 1994); but to make the paper self-contained, we give a direct proof here.

To achieve an efficient test for the mentioned redundancy notion, we have to use approximation techniques (cf. Chapter 5). First, instead of searching for arbitrary smaller proofs of the ground instances, we consider smaller rewrite proofs only, i. e., we use a strengthened form of ground joinability. This property still is undecidable in general (Kapur *et al.*, 1990). For rewrite relations embedded in an LPO, a decision procedure is given in (Comon *et al.*, 1998). An efficient realization of this algorithm seems hard to obtain with modest programming effort. Given the power of theorem provers available today, the break even point for such a test may be as low as a few term normalizations. Therefore, our second approximation step is to ensure ground joinability by sufficient criteria. We give a semantic criterion for AC-operators that is cheap in cost. Since it is limited to the specific theory, we augment it with a syntactic test. For our actual implementation of the syntactic criterion we have improved a test proposed in (Martin and Nipkow, 1990) such that it is computationally feasible for our purpose. The test is applicable both for KBO and LPO and relatively easy to implement.

In Chapter 6 we show that using the semantic test alone leads to speed-ups in computation time by a factor of 5 to 20. The syntactic criterion allows an additional (but more modest) speed-up, especially if AC-operators are predominant in the proof task. But we expect more gains by refining the syntactic test in the future.

2. Notations

We use standard notations. A signature $sig = (S, F, \alpha)$ consists of a set S of *sorts*, a set F of *operators* and an *arity function* $\alpha : F \to S^+$. The set of *terms* over sig and a variable system V is denoted by $\mathrm{Term}(F, V)$; and $\mathrm{Term}(F)$ is the set of *ground terms*, i. e. those terms containing no variable. A position p in a term t is defined as usual as a sequence of integers, we notate t/p for the subterm of t at position p, i. e., $t/\lambda \equiv t$ and $f(t_1, \ldots, t_n)/i.p \equiv t_i/p$. $\mathcal{O}(t)$ denotes the set of positions in t. $\mathrm{Var}(t)$ stands for the set of variables of $t \in \mathrm{Term}(F, V)$. A substitution $\sigma : V \to \mathrm{Term}(F, V)$ is a mapping with finite *domain* $\mathrm{dom}(\sigma) = \{x \in V \mid \sigma(x) \not\equiv x\}$ which is sort preserving. For theorem proving we use an infinite set C of new constants. Let $F^e = F \cup C$. We write $\mathrm{GSub}(F^e)$ or GSub for the set of *ground substitutions* σ, i. e., $\sigma(x) \in \mathrm{Term}(F^e)$ for all $x \in \mathrm{dom}(\sigma)$. Furthermore, $\mathrm{GSub}(s, t)$ is the subset of ground substitutions σ with $\mathrm{Var}(s, t) = \mathrm{dom}(\sigma)$.

A rewrite relation on $\mathrm{Term}(F, V)$ is a binary relation such that $u \to v$ implies $\sigma(u) \to \sigma(v)$ and $t[u]_p \to t[v]_p$. The relations $\leftrightarrow, \xrightarrow{+}$, and $\xrightarrow{*}$ are defined as usual. Terms s, t are *joinable*, denoted by $s \downarrow t$, if $s \xrightarrow{*} u \xleftarrow{*} t$ for some term u. They are called *ground joinable*, denoted by $s \Downarrow t$, if $\sigma(s) \downarrow \sigma(t)$ for each $\sigma \in \mathrm{GSub}(s, t)$. An ordering $\succ$ on $\mathrm{Term}(F, V)$ is a *reduction ordering* if it is a rewrite relation and well-founded. It is a *ground reduction ordering* if it is in addition total on $\mathrm{Term}(F^e)$. This holds e. g. for any *lexicographic path ordering* (LPO) or *Knuth-Bendix ordering* (KBO) based on a total precedence. The relation $\to$ is *terminating* if $\to \subseteq \succ$ for some reduction ordering $\succ$. It is *confluent* (resp. *ground confluent*) if $s \xleftarrow{*} \cdot \xrightarrow{*} t$ implies $s \downarrow t$ for all $s, t \in \mathrm{Term}(F, V)$ (resp.

$s, t \in \mathrm{Term}(F^e)$). Note that we use here an extended form of ground confluence: We require $\rightarrow$ to be confluent on $\mathrm{Term}(F^e)$, not only on $\mathrm{Term}(F)$.

An *equation* (a *rule*) is of the form $u = v$ (resp. $u \rightarrow v$) with u, v terms of the same sort. We write $u \doteq v$ to mean either $u = v$ or $v = u$. We denote by E (resp. R) a set of equations (rules). They specify the rewrite relation $\rightarrow_R$, the single-step replacement relation $\vdash\dashv_E$, and the E-equality $=_E$ as usual. Given R, E and a reduction ordering $\succ$, we write $R \subseteq \succ$ if $l \succ r$ for each $l \rightarrow r$ in R. Furthermore $E^\succ = \{\sigma(u) \rightarrow \sigma(v) \mid u \doteq v \text{ in } E,\ \sigma(u) \succ \sigma(v)\}$ is the set of orientable instances of equations in E. Let $R(E) = R \cup E^\succ$. We call the pair (R, E) terminating, confluent etc. if the rewrite relation $\rightarrow_{R(E)}$ is.

We notate $\succ_{st}$ for the subterm ordering and $\triangleright$ for the encompassment ordering: $s \triangleright l$ if for some substitution σ either $s \succ_{st} \sigma(l)$ or $s \equiv \sigma(l)$ but s and l are not equal up to a variable renaming.

A *critical pair* of two (variable disjoint) rules or equations $l = r$ and $u = v$ is defined as follows: Let $p \in \mathcal{O}(l)$ be a non-variable position in l, i. e. $l/p \notin V$, and $\sigma = \mathrm{mgu}(u, l/p)$ the most general unifier of u and l/p. Then $\langle \sigma(r), \sigma(l)\,[\sigma(v)]_p \rangle$ is a critical pair if $\sigma(r) \not\succeq \sigma(l)$ and $\sigma(v) \not\succeq \sigma(u)$. Let $\mathrm{CP}(R, E)$ denote the set of all critical pairs computable from rules in R and equations in E.

3. A motivating example

We start with the following well-known fact.

Proposition 3.1: *Let E be a finite set of equations over $sig = (S, F, \alpha)$ and $\succ$ a decidable ground reduction ordering. If $E^\succ$ is confluent on* $\mathrm{Term}(F^e)$ *then the word problem for E is decidable.*

Therefore, our goal is to saturate a given set E of equations for ground confluence which often is easier than getting confluence. The next example may show that the special treatment of ground joinable equations can reduce the computational effort of the unfailing completion procedure UKB.

We assume that $+$ is an AC-operator and write $x_1 + \ldots + x_{n-1} + x_n \equiv x_1 + (\ldots + (x_{n-1} + x_n))$ and $nx \equiv x + \ldots + x$ for all $n \in \mathbb{N}$. To ease understanding, the example is rather simple, but note that in practice these equations often appear as subsystems in more complex specifications.

Example: Consider the equations

(1)	$(x + y) + z = x + (y + z)$	(3)	$x + 0 = x$
(2)	$x + y = y + x$	(4)	$x + x = x$
		(5)	$x + -x = 0$

and the LPO with precedence $- > + > 0$.

a) ACU: We consider the equations (1)–(3). Here standard UKB diverges and produces for each $n \geq 2$

$$x_1 + x_2 + \ldots + x_n = x_{\pi(1)} + x_{\pi(2)} + \ldots + x_{\pi(n)}$$

for almost each permutation π. The number of these equations grows exponentially with n. We will show that all of them with $n > 3$ are ground joinable (Theorem 5.1) and can therefore be deleted. The WM-AC version of our theorem prover WALDMEISTER (see Chapter 6 for a detailed explanation of the different variants) does exactly this and stops with (R_1, E_1):

$$\begin{array}{rcl@{\qquad}rcl} x+0 & \to & x & 0+x & \to & x \\ (x+y)+z & \to & x+(y+z) & & & \\ x+y & = & y+x & x+(y+z) & = & z+(y+x) \\ x+(y+z) & = & y+(x+z) & x+(y+z) & = & y+(z+x) \end{array}$$

b) *ACUI*: We consider the equations (1)–(4). Here, WM-AC diverges (because it uses only the ground joinability test based on Theorem 5.1): It produces (R_1, E_1), the rule $x + x \to x$, and for each $n \geq 2$

$$\begin{array}{l} x_1 + \ldots + x_{n-1} + x_n + x_1 \to x_1 + \ldots + x_{n-1} + x_n \\ x_1 + \ldots + x_{n-1} + x_1 + x_n \to x_1 + \ldots + x_{n-1} + x_n \end{array}$$

Using a stronger test allows one to show that these rules are ground joinable for $n \geq 3$. So WM-DEL – a refined version of WM-AC – terminates with the finite ground confluent system (R_2, E_2) consisting of (R_1, E_1), $x + x \to x$, and $x + x + y \to x + y$.

c) Abelian Groups: We consider the equations (1), (2), (3), and (5), and we want to prove that $x + my + -x = my$ is a logical consequence. For that we use the Skolem constants a and b and extend the precedence of the LPO to $- > + > 0 > a > b$. Then, no finite ground confluent system (R, E) exists: Because of $-a > -b > a > b$, the occurrences of $-a$ and a within sums cannot be sorted to appear immediately together, but may appear at arbitrary distance. So we have to saturate the given equations to (R, E) such that either

$$(i)\;\; a + mb + -a \downarrow mb \qquad \text{or} \qquad (ii)\;\; b + ma + -b \downarrow ma$$

holds. (Note that in general it is totally unclear how to order the Skolem constants!) WM-GJ, a variant of WM-DEL which keeps ground joinable equations for simplification, produces (R_1, E_1) and

$$\begin{array}{rcl@{\qquad}rcl} -0 & \to & 0 & x + -x & \to & 0 \\ --x & \to & x & -(x+y) & \to & -y + -x \end{array}$$

and for each $n \geq 2$

$$\begin{array}{rcl} x_1 + \ldots + x_{n-1} + x_n + -x_1 & \to & x_2 + \ldots + x_n \\ x_1 + \ldots + x_{n-1} + -x_1 + x_n & \to & x_2 + \ldots + x_n \end{array}$$

There is a big difference in the effort to prove (i) or (ii). For (i) one needs only the rule $x_1 + \ldots + x_n + -x_1 \to x_2 + \ldots + x_n$ for $n = 3$, but for (ii) we need it for $n = m + 1$. Assume $m = 7$. Our version of standard UKB needs less than one second for (i), but more than two hours for (ii). This is due to the fact that it computes a huge set of (redundant) equations before it finds the crucial rule. On the other hand, WM-GJ avoids that and proves (i) in less than one second and (ii) in less than two seconds.

d) Abelian Groups, revisited. Changing the precedence of the LPO to $+ > - > 0$, the variant WM-GJ even finds a finite ground confluent system consisting of (R_1, E_1) and

$$\begin{array}{rcl} -0 & \to & 0 \\ --x & \to & x \\ x + -x & \to & 0 \\ -x + y & \to & -(x + -y) \\ x + -(x + y) & \to & -y \\ -(x + -y) & = & y + -x \\ x + -(y + z) & = & -(y + -(x + -z)) \end{array}$$

This implies another decision procedure for Abelian Groups.

4. Theoretical foundations

In this chapter we show that our approach is sound and complete: We present an inference system and show by the technique of proof transformations that the answer "yes" can be produced iff $u = v$ is a logical consequence of E. Our inference system refines that of (Bachmair *et al.*, 1989).

The inference system works on triples (R, E, G) and uses a ground reduction ordering $\succ$. The intention is that $R \subseteq \succ$ stores the rules, E contains the unoriented equations, and G contains equations whose ground instances have a smaller proof in (R, E). Equations in G will be used for the simplification of R and E, but not for computing critical pairs. We do not simplify equations in G.

We first define an ordering on ground proofs in the sense of (Bachmair *et al.*, 1989). Remember that $\succ$ is total on ground terms by assumption. Let s, t be ground terms. A *ground proof* for $s = t$ in (R, E, G) is of the form

$$P = (t_0, \varrho_1, t_1, \ldots, \varrho_n, t_n)$$

where $t_i \in \mathrm{Term}(F^e)$, $t_0 \equiv s$, $t_n \equiv t$, and $t_{i-1}\varrho_i t_i$ with ϱ_i as justification of the ith step, i. e. $\varrho_i \in \{\to_R, \leftarrow_R, \to_{E^\succ}, \leftarrow_{E^\succ}, \vdash\!\dashv_E, \to_{G^\succ}, \leftarrow_{G^\succ}, \vdash\!\dashv_G\}$.

Let $P = (t_0, \varrho_1, t_1, \ldots, \varrho_n, t_n)$ be a ground proof. We define the complexity $c(s\varrho t)$ of a proof step by

$$c(s\varrho t) = \begin{cases} (\{s\}, l, \{t\}) & \text{if } s \to_R t & \text{with } l \to r \\ (\{t\}, l, \{s\}) & \text{if } s \leftarrow_R t & \text{with } l \to r \\ (\{s\}, l, \{t, \top\}) & \text{if } s \to_{(E \cup G)^\succ} t & \text{with } l \to r \\ (\{t\}, l, \{s, \top\}) & \text{if } s \leftarrow_{(E \cup G)^\succ} t & \text{with } l \to r \\ (\{s, t\}, -, -) & \text{if } s \vdash\!\dashv_{(E \cup G)} t & \end{cases}$$

where $\top$ is a new symbol with $\top \succ u$ for all terms u.

We define the ordering $\succ_t$ on these triples as the lexicographic combination $(\succ\!\!\succ, \rhd, \succ\!\!\succ)$. Here $\succ\!\!\succ$ is the multiset extension of the fixed ground reduction ordering $\succ$. Let $\succ\!\!\succ_t$ be the multiset extension of $\succ_t$. We define the complexity $c(P)$ of a ground proof to be the multiset

$$c(P) = \{c(t_{i-1}\varrho_i t_i) \mid i = 1, \ldots, n\}$$

and an ordering $\succ_{\mathcal{P}}$ on ground proofs by

$$P_1 \succ_{\mathcal{P}} P_2 \quad \text{iff} \quad c(P_1) \succ\!\!\succ_t c(P_2)$$

The following definition is useful for the notion of redundancy that an equation is redundant if every ground instance has a smaller proof.

Definition: We write $s = t \succ_{\mathcal{P}} R(E)$ if for any $\sigma \in \mathrm{GSub}(s,t)$ either $\sigma(s) \equiv \sigma(t)$ or there is a ground proof P for $\sigma(s) = \sigma(t)$ in $(R, E, \varnothing)$ with $\sigma(s) \rightarrow_{\{s=t\}^{\succ}} \sigma(t) \succ_{\mathcal{P}} P$ when $\sigma(s) \succ \sigma(t)$, or $\sigma(t) \rightarrow_{\{s=t\}^{\succ}} \sigma(s) \succ_{\mathcal{P}} P$ when $\sigma(t) \succ \sigma(s)$.

In case of such redundancy, the equation at hand is not needed for these smaller proofs:

LEMMA 4.1: *If $s = t \succ_{\mathcal{P}} R(E \cup \{s = t\})$, then $s = t \succ_{\mathcal{P}} R(E)$.*

Proof: By assumption for any $\sigma \in \mathrm{GSub}(s,t)$ there is a proof P in $(R, E \cup \{s = t\}, \varnothing)$ such that $\sigma(s)\varrho\sigma(t) \succ_{\mathcal{P}} P$. We show that there is also such a proof in $(R, E, \varnothing)$, by induction on $\succ_t$; i. e., we order $\mathrm{GSub}(s,t)$ via $\sigma \sqsupset \sigma'$ iff $c(\sigma(s)\varrho\sigma(t)) \succ_t c(\sigma'(s)\varrho'\sigma'(t))$.

Assume there are steps $\sigma'(s)\varrho'\sigma'(t)$ in P. Because of $\sigma(s)\varrho\sigma(t) \succ_{\mathcal{P}} P \succeq_{\mathcal{P}} \sigma'(s)\varrho'\sigma'(t)$, the induction hypothesis applies so that the steps $\sigma'(s)\varrho'\sigma'(t)$ can be replaced by smaller proofs in $(R, E, \varnothing)$. So there is a proof P_0 in $(R, E, \varnothing)$ such that $\sigma(s)\varrho\sigma(t) \succ_{\mathcal{P}} P \succ_{\mathcal{P}} P_0$. $\square$

We now present the inference system $\mathcal{G}$.

Definition: The inference system $\mathcal{G}$ consists of the following inferences.

1. Orienting an equation
   $(R, E \cup \{s \doteq t\}, G) \vdash (R \cup \{s \rightarrow t\}, E, G)$
   if $s \succ t$
2. Adding an equational consequence
   $(R, E, G) \vdash (R, E \cup \{s = t\}, G)$
   if $s \leftrightarrow_{R \cup E} u \leftrightarrow_{R \cup E} t$ and $s \not\prec u$ and $t \not\prec u$
3. Simplifying an equation
   $(R, E \cup \{s \doteq t\}, G) \vdash (R, E \cup \{u = t\}, G)$
   if $s \rightarrow_R u$, or if $s \rightarrow_{(E \cup G)^{\succ}} u$ with $l = r$ and $s \rhd l$

4. Deleting a trivial equation
   $(R, E \cup \{s = s\}, G) \vdash (R, E, G)$
5. Subsuming an equation
   $(R, E \cup \{s = t\}, G) \vdash (R, E, G)$
   if $s \mapsto\!\dashv_{E \cup G}\, t$
6. Shifting a redundant equation from E to G
   $(R, E \cup \{s = t\}, G) \vdash (R, E, G \cup \{s = t\})$
   if $s = t \succ_{\mathcal{P}} R(E \cup G)$
7. Simplifying the right-hand side of a rule
   $(R \cup \{s \to t\}, E, G) \vdash (R \cup \{s \to u\}, E, G)$
   if $t \to_{R(E \cup G)} u$
8. Simplifying the left-hand side of a rule
   $(R \cup \{s \to t\}, E, G) \vdash (R, E \cup \{u = t\}, G)$
   if $s \to_{R(E \cup G)} u$ with $l = r$ and $s \rhd l$

We write $(R, E, G) \vdash (R', E', G')$ if (R', E', G') can be deduced by $\mathcal{G}$ from (R, E, G) in one step. A *$\mathcal{G}$-derivation* is a sequence $(R_i, E_i, G_i)_{i \in \mathbb{N}}$ such that $(R_i, E_i, G_i) \vdash (R_{i+1}, E_{i+1}, G_{i+1})$ for all $i \geq 0$. It is a *$\mathcal{G}$-derivation for E* if $(R_0, E_0, G_0) = (\emptyset, E, \emptyset)$.

Let us comment on two inferences. In Inference 2 the equation $s = t$ is in practice only added if $\langle s, t \rangle \in \mathrm{CP}(R, E)$. If Inference 6 is never applied we get unfailing completion as in (Bachmair *et al.*, 1989).

Our next lemma states that $\mathcal{G}$ is sound.

Lemma 4.2: *Let $(R_i, E_i, G_i)_{i \in \mathbb{N}}$ be a $\mathcal{G}$-derivation for E. Then we have*
a) $R_i \subseteq \succ$
b) $=_E \,=\, =_{R_i \cup E_i \cup G_i}$ *on* $\mathrm{Term}(F, V)$

Both properties are shown via induction on i and case analysis with respect to the inferences. The same holds for the following lemma which is an adaption from (Bachmair *et al.*, 1989): The inference system does not only preserve equality, but also preserves or decreases ground proofs.

Lemma 4.3: *Let $(R_i, E_i, G_i)_{i \in \mathbb{N}}$ be a $\mathcal{G}$-derivation. For any ground proof P for $u = v$ in (R_i, E_i, G_i) there is a ground proof P' for $u = v$ in $(R_{i+1}, E_{i+1}, G_{i+1})$ with $P \succeq_{\mathcal{P}} P'$.*

The next lemma is crucial for our approach. It states that any G_i-step in a ground proof can be replaced by a smaller proof in (R_i, E_i). Lemma 4.1 is needed in order to deal with cycles of the form: $s = t$ in G simplifies a rule $l \to r$ which was used to shift $s = t$ from E to G.

Lemma 4.4: *Let $(R_i, E_i, G_i)_{i \in \mathbb{N}}$ be a $\mathcal{G}$-derivation for E. For all $i \in \mathbb{N}$ we have: If $s = t$ in G_i, then $s = t \succ_{\mathcal{P}} R_i(E_i)$.*

Proof: Induction on i: For $i = 0$ the claim is trivial. For the induction step $(R_i, E_i, G_i) \vdash (R_{i+1}, E_{i+1}, G_{i+1})$ we consider all inferences of $\mathcal{G}$ in turn. The cases of Inferences 1, 2 and 4 are easy. Inferences 7 and 8 are similar to Inference 3. So we consider here Inferences 3, 5 and 6 in detail.

Inference 3: Let $R = R_i$, $E \cup \{s = t\} = E_i$, $E \cup \{u = t\} = E_{i+1}$, and $G = G_i$; where $s \rightarrow_R u$, or $s \rightarrow_{(E \cup G)^{\succ}} u$ with $l = r$ and $s \rhd l$. The inference at hand then is $(R, E \cup \{s = t\}, G) \vdash (R, E \cup \{u = t\}, G)$. We have to show that $s' = t' \succ_{\mathcal{P}} R(E \cup \{u = t\})$ for all $s' = t' \in G$.

a) We first show that $s = t \succ_{\mathcal{P}} R(E \cup \{u = t\})$: Since the inference is proof decreasing (Lemma 4.3), we get that $s = t \succ_{\mathcal{P}} R(E \cup \{u = t\} \cup G)$. Then by induction hypothesis $s = t \succ_{\mathcal{P}} R(E \cup \{u = t\} \cup \{s = t\})$, and by Lemma 4.1 $s = t \succ_{\mathcal{P}} R(E \cup \{u = t\})$.

b) Now consider $s' = t'$ in G: By induction hypothesis we have $s' = t' \succ_{\mathcal{P}} R(E \cup \{s = t\})$, and hence $s' = t' \succ_{\mathcal{P}} R(E \cup \{u = t\})$ by a).

Inference 5: Let $(R, E \cup \{s = t\}, G) \vdash (R, E, G)$ and $s \vdash\!\dashv_{E \cup G} t$, say by $u = v$ in $E \cup G$. We have to prove $s' = t' \succ R(E)$ for all $s' = t'$ in G.

The induction hypothesis entails $s' = t' \succ_{\mathcal{P}} R(E \cup \{s = t\})$; the inference being proof decreasing gives $s' = t' \succ_{\mathcal{P}} R(E \cup \{u = v\})$. If $u = v \in E$ then this is already $s' = t' \succ_{\mathcal{P}} R(E)$. Otherwise $u = v \in G$, and just as for $s' = t'$ we get that $u = v \succ_{\mathcal{P}} R(E \cup \{u = v\})$, which by Lemma 4.1 implies $u = v \succ_{\mathcal{P}} R(E)$ so that finally $s' = t' \succ_{\mathcal{P}} R(E)$.

Inference 6: Let $(R, E \cup \{s = t\}, G) \vdash (R, E, G \cup \{s = t\})$ and $s = t \succ_{\mathcal{P}} R(E \cup G)$. We show that $s' = t' \succ_{\mathcal{P}} R(E)$ holds for all $s' = t'$ in $G \cup \{s = t\}$.

a) $s' = t'$ is $s = t$: The condition $s = t \succ_{\mathcal{P}} R(E \cup G)$ and the induction hypothesis imply $s = t \succ_{\mathcal{P}} R(E \cup \{s = t\})$; then by Lemma 4.1 we get $s = t \succ_{\mathcal{P}} R(E)$.

b) $s' = t'$ is in G: By induction hypothesis $s' = t' \succ_{\mathcal{P}} R(E \cup \{s = t\})$, and by a) hence $s' = t' \succ_{\mathcal{P}} R(E)$. $\square$

A straightforward corollary is that in any derivation G_i is not needed to preserve equality on ground terms, and that G_i-steps are not needed in ground proofs.

Corollary 4.1: *Let $(R_i, E_i, G_i)_{i \in \mathbb{N}}$ be a $\mathcal{G}$-derivation for E. If $u, v \in \mathrm{Term}(F^e)$ and $u =_E v$ then there exist ground proofs P_i of $u = v$ in $(R_i, E_i, \varnothing)$ with $P_i \succeq_{\mathcal{P}} P_{i+1}$ for all $i \in \mathbb{N}$. So we have $=_E \; = \; =_{R_i \cup E_i}$ on $\mathrm{Term}(F^e)$ for all $i \in \mathbb{N}$.* $\square$

This motivates the definition of a fair $\mathcal{G}$-derivation: Equations in G_i need not be considered for computing critical pairs because for each ground proof with G_i-steps, there is a smaller one without.

Definition: Let $(R_i, E_i, G_i)_{i\in\mathbb{N}}$ be a $\mathcal{G}$-derivation and let

$$R^\infty = \bigcup_{i\geq 0}\bigcap_{j\geq i} R_j \qquad E^\infty = \bigcup_{i\geq 0}\bigcap_{j\geq i} E_j$$

be the set of persistent rules and equations, respectively. The $\mathcal{G}$-derivation is *fair* if $\mathrm{CP}(R^\infty, E^\infty) \subseteq \bigcup_{i\geq 0} E_i$.

Now we can formulate the main theorem of this chapter.

THEOREM 4.1: *Let $(R_i, E_i, G_i)_{i\in\mathbb{N}}$ be a fair $\mathcal{G}$-derivation for E.*
a) $R^\infty(E^\infty)$ is ground confluent and terminating.
b) For any $u, v \in \mathrm{Term}(F^e)$, if $u =_E v$ then $u{\downarrow}v$ in $R_i(E_i)$ for some i.

Proof: Let $u, v \in \mathrm{Term}(F^e)$ and $u =_E v$. By Corollary 4.1 there is a sequence $P_0, P_1, P_2, \ldots$ of proofs for $u = v$ in $R_i(E_i)$ with $P_i \succeq_{\mathcal{P}} P_{i+1}$. Since $\succ_{\mathcal{P}}$ is well-founded this sequence has a minimum, say from P_k on. Because of the fairness condition P_k can have no peak, so it is of the form $u \xrightarrow{*} \cdot \xleftarrow{*} v$. Since $P_k = P_{k+i}$ for all $i \geq 0$ this is also a proof in $R^\infty(E^\infty)$. Therefore $R^\infty(E^\infty)$ is ground confluent and we have $=_E \;=\; =_{R^\infty\cup E^\infty}$ on ground terms. $R^\infty(E^\infty)$ is terminating since $R^\infty(E^\infty) \subseteq \succ$. □

We now discuss how to transform the inference system $\mathcal{G}$ into an algorithm. The main problem is how to check that $s = t \succ_{\mathcal{P}} R(E\cup G)$ holds. We will do this by a strengthened ground joinability test. Since for the test itself the distinction between E and G is not needed, we omit G in the following when convenient.

In the next definition we write $u \overset{s\triangleright}{\rightarrow}_{R(E)} v$ if $u \rightarrow_{R(E)} v$ with $l = r$ in $R \cup E$ and $s \triangleright l$.

Definition: We define $s \Downarrow_{\triangleright} t$ in $R(E)$ iff for any $\sigma \in \mathrm{GSub}(s,t)$ either
a) $\sigma(s) \equiv \sigma(t)$, or
b) $\sigma(s) \succ \sigma(t)$ and $\sigma(s) \overset{s\triangleright}{\rightarrow}_{R(E)} s_1 \downarrow \sigma(t)$, or
c) $\sigma(t) \succ \sigma(s)$ and $\sigma(t) \overset{t\triangleright}{\rightarrow}_{R(E)} t_1 \downarrow \sigma(s)$.

LEMMA 4.5: *If $s \Downarrow_{\triangleright} t$ in $R(E)$ then $s = t \succ_{\mathcal{P}} R(E)$.*

Proof: Assume $\sigma(s) \succ \sigma(t)$ and let P be the proof $\sigma(s) \overset{s\triangleright}{\rightarrow}_{R(E)} s_1 \xrightarrow{*} \cdot \xleftarrow{*} \sigma(t)$. All proof steps $u\varrho v$ in P are $\succ_t$-smaller than $\sigma(s) \rightarrow_{\{s=t\}^\succ} \sigma(t)$: This holds true for the first proof step by the second component of its complexity and for all other proof steps by the first component. The case $\sigma(t) \succ \sigma(s)$ is similar. So we have $s = t \succ R(E)$. □

We will discuss in the next chapter how one can apply this lemma.

It is quite natural to ask whether the preceding Lemma still holds if we replace the strengthened ground joinability test $s \Downarrow_{\triangleright} t$ by the normal one, i. e. by $s \Downarrow t$.

The answer is "no"; e. g. E might simply just be $\{s = t\}$, and R empty. The situation is even worse: If we replaced in Inference 6 the condition $s = t \succ_{\mathcal{P}} R(E \cup G)$ by $s \Downarrow t$ in $R(E \cup G)$ then any equation could be used to make itself redundant.

This observation shows that for a theorem prover employing interreduction one has to be careful in substantiating the basic idea "ground joinable equations may be used for simplification, but need not be considered for computing critical pairs". In contrast, when testing a given rewrite system for ground confluence, the test $\Downarrow$ is sufficient (Martin and Nipkow, 1990).

5. Proving ground joinability

We distinguish here between semantic and syntactic criteria. We call a criterion semantic if it guarantees ground joinability of an equation at hand by an easy semantics-based test for a given theory. This is possible, for example, for AC-theories. The semantics of the AC-theory tells us that the ground joinability test reduces to sorting and testing for identity.

THEOREM 5.1: *Let $\succ$ be any LPO or KBO which is total on* $\mathrm{Term}(F^e)$. *Let*

$$\begin{array}{lrclrcl} R_0: & f(f(x,y),z) & \to & f(x,f(y,z)) & & & \\ E_0: & f(x,y) & = & f(y,x) & f(x,f(y,z)) & = & f(z,f(y,x)) \\ & f(x,f(y,z)) & = & f(y,f(x,z)) & f(x,f(y,z)) & = & f(y,f(z,x)) \end{array}$$

*If $s = t$ cannot be simplified or subsumed by R_0 or E_0 then $s =_{R_0 \cup E_0} t$ implies $s \Downarrow_{\rhd} t$ in $R_0(E_0)$.**

Proof: $R_0(E_0)$ is terminating by construction. For every critical pair, all of its ground instances are joinable; case splits on the ordering relations between variable instances are necessary for doing so. Hence $R_0(E_0)$ is confluent on $\mathrm{Term}(F^e)$. Consequently, if $s =_{R_0 \cup E_0} t$, then $\sigma(s) \downarrow \sigma(t)$ for any ground instance. The condition that $s = t$ cannot be simplified or subsumed ensures that the first or the last step of the rewrite chain for the joinability proof is an $\stackrel{s\rhd}{\to}$ or $\stackrel{t\rhd}{\to}$ step, respectively. □

This theorem constitutes a semantic test to show $s = t \succ_{\mathcal{P}} R(E)$ whenever $R_0 \subseteq R$ and $E_0 \subseteq E$. The criterion is basically a test on $R_0 \cup E_0$ equality, i. e. AC-equality. Hence it can easily be implemented by sorting AC-subterms, and is moreover cheap in practice. It is very effective, too: The KB-procedure started with E containing the rules/equations as in Theorem 5.1 computes an infinite set of equations. By the results of the previous chapter, all these additional equations can be used for simplification, but need not be used to compute critical pairs.

*The notion of strengthened ground joinability can be refined such that Theorem 5.1 holds for any $s = t$ not in $R_0 \cup E_0$, and even without the two equations in the right column.

We therefore have the freedom not to build them at all. – Theorem 5.1 can be extended to the case of several AC-operators as well as to other theories such as ACI.

To go beyond given fixed theories, we extend the approach by a syntactic criterion, which currently is implemented as a simple splitting by cases. Suppose $s = t$ is the equation at hand and $\mathrm{Var}(s,t) = \{x_1, \ldots, x_n\}$. In (Martin and Nipkow, 1990) it is proposed to consider any ordering relation $\sigma(x_{i_1}) \sim_1 \ldots \sim_{n-1} \sigma(x_{i_n})$, $\sim_i \in \{\succ, \equiv\}$, between ground instances $\sigma(x_1), \ldots, \sigma(x_n)$ and to prove $s{\downarrow}t$ under each of these constraints. This implies $s \Downarrow t$; the refinement needed for $s \Downarrow_{\triangleright} t$ is straightforward: For every instance to be analyzed, one just has to be careful with the first rewrite step on $\sigma(s)$ and $\sigma(t)$.

Since the number of cases grows exponentially with n we refine this idea. Instead of doing case splits wrt. all the variables, we only split wrt. a subset and try to show ground joinability with this restricted split already. To make the approach precise we model the ordering constraints on variable instances by a quasi ordering $\succsim_V$ on $V_0 \subseteq \mathrm{Var}(s,t)$ and extend the reduction ordering $\succ$ to a quasi ordering $\succsim_0$ on $\mathrm{Term}(F,V)$ containing $\succsim_V$. We first formulate requirements on $\succsim_0$ that will allow us to approximate rewriting on $\mathrm{Term}(F^e)$ by rewriting on $\mathrm{Term}(F,V)$.

Definition: a) We say that a quasi ordering $\succsim_0$ *covers* a ground substitution $\sigma \in \mathrm{GSub}(s,t)$ wrt. a reduction ordering $\succ$ if for $x, y \in V$ the relation $x \succ_0 y$ implies $\sigma(x) \succ \sigma(y)$ and the relation $x \approx_0 y$ implies $\sigma(x) \equiv \sigma(y)$.

b) The ordering $\succsim_0$ on $\mathrm{Term}(F,V)$ is *compatible* with $\succ$ if for all $s,t \in \mathrm{Term}(F,V)$ and all $\sigma \in \mathrm{GSub}(s,t)$ covered by $\succsim_0$ we have: If $s \succ_0 t$, then $\sigma(s) \succ \sigma(t)$.

For example, the quasi ordering $x \succsim_0 y$ covers the substitution $\sigma = \{x \leftarrow f(a), y \leftarrow a\}$ say wrt. to a compatible LPO $\succ$. We then have e. g. $s \equiv x + y \succsim_0 y + x \equiv t$, which corresponds to $\sigma(s) \equiv f(a) + a \succ a + f(a) \equiv \sigma(t)$. Later we will show for any LPO $\succ$: If we extend its precedence $\succ_F$ by a quasi ordering $\succsim_V$ on the variables, then this extended LPO $\succsim_0$ is compatible with $\succ$.

In case of compatibility, rewrite steps under $\succ_0$ (denoted as $s \rightarrow^{\succ_0}_{R(E)} t$) imply rewrite steps under $\succ$ on the covered ground instances:

Lemma 5.1: *Let $\succsim_0$ be compatible with $\succ$. If $s \rightarrow^{\succ_0}_{R(E)} t$, then $\sigma(s) \rightarrow_{R(E)} \sigma(t)$ for all $\sigma \in \mathrm{GSub}(s,t)$ that are covered by $\succsim_0$.*

Proof: Let $s \rightarrow^{\succ_0}_{R(E)} t$ with $l = r \in R \cup E$, substitution τ and position $p \in \mathcal{O}(s)$, i. e. $s \equiv s[\tau(l)]_p \rightarrow s[\tau(r)]_p \equiv t$ and $\tau(l) \succ_0 \tau(r)$. Since $\succsim_0$ is compatible with $\succ$, for any covered $\sigma \in \mathrm{GSub}(s,t)$ follows that $\sigma\tau(l) \succ \sigma\tau(r)$ and therefore $\sigma(s) \equiv \sigma(s)[\sigma\tau(l)]_p \rightarrow \sigma(s)[\sigma\tau(r)]_p \equiv \sigma(t)$. □

Continuing the example above, the commutativity axiom allows under the quasi ordering $x \succsim_0 y$ to rewrite the term $x+y$ to $y+x$ which covers the rewrite step $f(a)+a \to a+f(a)$ of the ground instance σ.

Iterating the argumentation, we get the same result for joinability under $\succ_0$ (written as $\downarrow^{\succ_0}$):

COROLLARY 5.1: *Let $\succsim_0$ be compatible with $\succ$. If $s \downarrow^{\succ_0} t$, then $\sigma(s) \downarrow \sigma(t)$ for all $\sigma \in \mathrm{GSub}(s,t)$ that are covered by $\succsim_0$.* □

This enables us to formulate a syntactic test for ground joinability.

THEOREM 5.2: *Let the reduction ordering $\succ$ and two terms $s, t \in \mathrm{Term}(F,V)$ be given. Let $O = \{\succsim_1, \ldots, \succsim_k\}$ be a set of term orderings such that for each $\succsim_i \in O$ the ordering $\succsim_i$ is compatible with $\succ$ and that for each $\sigma \in \mathrm{GSub}(s,t)$ there exists an ordering $\succsim_i \in O$ such that $\succsim_i$ covers σ.*

If for all $i \in \{1, \ldots, k\}$ we have $s \downarrow^{\succ_i} t$, then $s \Downarrow t$.

Proof: We have to show that for each $\sigma \in \mathrm{GSub}(s,t)$ $\sigma(s) \downarrow \sigma(t)$ holds. By assumption, there exists an ordering $\succsim_i \in O$ which covers σ. Since $\succsim_i$ is compatible with $\succ$ and $s \downarrow^{\succ_i} t$ we have $\sigma(s) \downarrow \sigma(t)$ as a consequence of the corollary above. Therefore, $s \Downarrow t$. □

There are two questions left: (1) Given a reduction ordering $\succ$ and a constraint $\succsim_V$ on V_0, how to find an ordering $\succsim_0$ such that $\succsim_V \subseteq \succsim_0$ and $\succsim_0$ is compatible with $\succ$? (2) How to find a small set O of orderings that cover each $\sigma \in \mathrm{GSub}(s,t)$?

We answer question (1) for the LPO and the KBO. This seems to be folklore, but we know of no reference for it. So we add it here for the reason of completeness. In both cases, the proof is by induction on the term structure.

LEMMA 5.2: *Let $\succ_F$ be a precedence on F and $\succsim_V$ a quasi ordering on V. Let $\succ$ be the LPO with precedence $\succ_F$ and $\succsim_0$ the LPO with precedence $\succ_F \cup \succsim_V$. Then $\succsim_0$ is compatible with $\succ$.*

Proof: Let $s \succ_0 t$ and $\succsim_0$ cover $\sigma \in \mathrm{GSub}(s,t)$. We show by induction on $|s|+|t|$ that then $\sigma(s) \succ \sigma(t)$, inspecting the possible justifications for $s \succ_0 t$.

(α) $s \equiv f(s_1, \ldots, s_m),\ \exists i.\, s_i \succsim_0 t$:
If $s_i \approx_0 t$, then $\sigma(s_i) \approx_0 \sigma(t)$ and hence $\sigma(s_i) \equiv \sigma(t)$. Otherwise we have $s_i \succ_0 t$ and by induction hypotheses $\sigma(s_i) \succ \sigma(t)$. In both cases $\sigma(s_i) \succeq \sigma(t)$ holds and therefore $\sigma(s) \succ \sigma(t)$.

(βV) $s \equiv x,\ t \equiv y,\ s \succ_V t$:
This entails $x \succ_0 y$. Since $\succsim_0$ covers σ wrt. $\succ$, we get that $\sigma(s) \succ \sigma(t)$.

(βF) $s \equiv f(s_1, \ldots, s_m),\ t \equiv g(t_1, \ldots, t_n),\ f \succ_F g,\ \forall j.\, s \succ_0 t_j$:
The induction hypothesis implies $\sigma(s) \succ \sigma(t_j)$ for all j and thus $\sigma(s) \succ \sigma(t)$.

(γF) $s \equiv f(s_1, \ldots, s_m),\ t \equiv f(t_1, \ldots, t_m),\ \forall i < k.\, s_i \approx_0 t_i,\ s_k \succ_0 t_k,\ \forall j.s \succ_0 t_j$:
Again $s_i \approx_0 t_i$ implies $\sigma(s_i) \equiv \sigma(t_i)$. Furthermore by induction hypothesis $\sigma(s_k) \succ \sigma(t_k)$ and $\sigma(s) \succ \sigma(t_j)$ for all j.

(δ) $s \equiv s[z]_{i.p},\ t \equiv z$:
Here we have $\sigma(s)|_{i.p} \equiv \sigma(z) \equiv z$ and thereby $\sigma(s) \succ \sigma(t)$. □

Note that the proof indeed requires that the precedence relation $\succ_F$ is a strict ordering; but an LPO to a quasi precedence is not a ground reduction ordering anyway. – For the KBO a result similar to Lemma 5.2 holds. Let $|t|_x$ denote the x-length of t, i. e. the number of occurrences of x in t.

LEMMA 5.3: *Let $\succ_F$ be a precedence on F and $\succsim_V$ a quasi ordering on V_0. Let $\varphi : F \cup V \to \mathbb{N}$ be a weight function with $\varphi(x) = 1$ for all $x \in V$. Let $\succsim_0$ be given by*

- $s \equiv f(s_1, \ldots, s_m) \succsim_0 g(t_1, \ldots, t_l) \equiv t$ *iff*

$$\begin{array}{lll} (1) & \sum\limits_{y \succsim_V x} |s|_y \geq \sum\limits_{y \succsim_V x} |t|_y & \textit{for all } x \in V \textit{ and} \\ (2a) & \varphi(s) > \varphi(t) & \textit{or} \\ (2b) & \varphi(s) = \varphi(t),\ f \succ_F g & \textit{or} \\ (2c) & \varphi(s) = \varphi(t),\ f = g, & (s_1, \ldots, s_m) \succsim_{0,lex} (t_1, \ldots, t_l) \end{array}$$

- $s \succsim_0 x$ *iff there exists* $y \in \mathrm{Var}(s)$: $y \succsim_V x$.

Let $\succ$ be the corresponding KBO, i. e., (1) is replaced by $|s|_x \geq |t|_x$ for all $x \in V$ and $s \succ x$ iff $s \succ_{st} x$. Then $\succsim_0$ is compatible with $\succ$. □

In both cases $\succsim_0$ and $\succsim_V$ coincide on V and cover therefore the same ground substitutions. Thus, we can concentrate on $\succsim_V$ to answer question (2). The idea is to fix a set $V_0 \subseteq \mathrm{Var}(s,t)$ and to consider all total quasi orderings $\succsim_{V_i}$ on V_0.

LEMMA 5.4: *Let $V_0 \subseteq \mathrm{Var}(s,t)$, and let O denote the set of all total quasi orderings on V_0. Then for each $\sigma \in \mathrm{GSub}(s,t)$ there exists an ordering $\succsim_V \in O$ such that $\succsim_V$ covers σ wrt. the reduction ordering $\succ$.*

Proof: The substitution σ determines with $\succ$ a quasi ordering $\succsim_V$ on V via $x \approx_V y$ iff $\sigma(s) \equiv \sigma(y)$ and $x \succ_V y$ iff $\sigma(x) \succ \sigma(y)$. Obviously, $\succsim_V$ covers σ. Since $V_0 \subseteq \mathrm{dom}(\sigma)$, the quasi ordering $\succsim_V$ is total on V_0. But then $\succsim_V \in O$. □

This leads to a straightforward construction of the set O of Theorem 5.2. For example, if $V_0 = \{x, y\}$ and $\succsim_1$, $\succsim_2$, and $\succsim_3$ are the extended LPOs of $\succ$ with $x \succ_1 y$, $y \succ_2 x$ and $x \approx_3 y$ (see Lemma 5.2 above), then $O = \{\succsim_1, \succsim_2, \succsim_3\}$ has the desired properties. To show ground joinability, each of the three cases has to be checked separately.

A simple way to implement variable constraints $\succsim_V$ is to introduce new constants $c_1 \succ \cdots \succ c_n$, map the ordering relation $\succsim_V$ onto a corresponding substitution $\rho : V_0 \to \{c_1, \dots, c_n\}$, and try to join the instance $\rho(s) = \rho(t)$ with the reduction ordering modified as indicated in Lemma 5.2 resp. 5.3. To fix the set V_0, we select two variables from $\mathrm{Var}(s,t)$ through some heuristic and extend V_0 if the test does not succeed. If the size of $\mathrm{Var}(s,t)$ is larger than a given limit, we prefer to select for V_0 different small sets, say of two or three elements, instead of continously extending V_0. The advantage is that then the number of cases depends polynomially on the number of variables of s and t. This is important to make the test feasible in practice. Of course, it then might not detect all ground joinable equations. But the test is not complete anyway since a variable x is not necessarily comparable to a term t when $x \notin \mathrm{Var}(t)$. For example, the equation $x_1 + x_2 + x_3 + f(x_4) = f(x_4) + x_1 + x_2 + x_3$ cannot be shown to be ground joinable in $R_0(E_0)$ with the syntactic criterion: if $x_4 \succsim_V x_3$, then $f(x_4) \succ_0 x_3$, but if $x_3 \succ_V x_4$, then $f(x_4)$ is in $\succ_0$ not comparable with x_3 for both LPO or KBO. On the other hand, the semantic criterion can easily detect the equation to be redundant. So the syntactic criterion, although more effective in practice, is not a strict extension of the semantic one.

6. Experimental evaluation

To evaluate our approach and to gain some insights into the practical applicability we considered four variants of our WALDMEISTER theorem prover. They are all running in autonomous mode (Hillenbrand *et al.*, 1999) and differ only in the following way:

- WM uses none of the mentioned techniques and serves as baseline in the experiments
- WM-AC employs only the semantic criterion of Theorem 5.1 to detect ground joinable equations and deletes these equations immediately
- WM-DEL uses additionally the syntactic criterion and deletes the ground joinable equations immediately
- WM-GJ also uses both criteria, but keeps the ground joinable equations for simplification and for the test on ground joinability

These variants are a subset of the nine variations that one obtains employing each of syntactic and semantic criterion either not at all, with immediate deletion of redundant equations, or keeping these equations. Using the syntactic criterion without prior semantic test is not interesting in practice because the former is not a strict extension of the former which is also faster in case it succeeds. As to the semantic criterion with immediate deletion vs. without, we did not notice any benefit in practice from keeping this special form of redundant equations. Hence the above-mentioned variants remain as the relevant ones.

As a basis for our experiments we chose from the 424 unit equality problems of the TPTP (Sutcliffe and Suttner, 1998, Vers. 2.3.0) those 397 for which WALDMEISTER can find a proof in 5 minutes. Of these, 186 specifications contain at least one AC-operator such that the semantic criterion is applicable. All tests were performed on SPARCStations Ultra-10/333 MHz.

For nearly 300 proof tasks we found no or only negligible differences between the four versions. This had to be expected since most of them are proved in a fraction of a second and the criteria work in more complicated situations only.

Nearly all of the problems which show noticeable effects belong to one of five problem domains: (i) Robbins algebra, (ii) non-associative rings, (iii) lattices, (iv) rings where $x^n = x$ implies commutativity, and (v) lattice-ordered groups. All of them contain AC-operators. As we expected, the effects are very similar for the proof tasks in the different domains, with some variations between the domains. We therefore present some data from representative examples for each of the five domains in the tables. GRP177-2 is a problem in the (v) domain; LAT023-1 a modularity property for quasilattices (iii); RNG027-5 the right Moufang identity for (ii); RNG035-7 the instance of (iv) where $n = 4$; and ROB006-1 the theorem that the Winker condition $\exists x, y : x+y = y$ makes a Robbins algebra (i) Boolean.

Table 1: Running times in seconds for representative examples.

Problem	WM	WM-AC	WM-DEL	WM-GJ
GRP177-2	14.3	8.6	8.9	8.9
LAT023-1	12.2	5.6	10.9	4.8
RNG027-5	258.6	16.3	24.6	24.2
RNG035-7	29.5	21.1	346.6	19.8
ROB006-1	1028.5	161.4	131.5	107.1

Table 2: Number of oriented/unoriented activated facts for representative examples.

Problem	WM	WM-AC	WM-DEL	WM-GJ
GRP177-2	1601 + 8	1201 + 6	1201 + 6	1201 + 6
LAT023-1	246 + 87	211 + 37	276 + 48	214 + 29
RNG027-5	974 + 106	264 + 32	368 + 19	373 + 41
RNG035-7	498 + 56	482 + 13	840 + 14	460 + 13
ROB006-1	1638 + 818	1604 + 7	1615 + 7	1575 + 7

We now compare the behavior of WM with that of its modified variants.

WM-AC: As we can see the use of the semantic criterion alone can lead to significant speed-ups (we measured a factor of up to 20). It often reduces (sometimes drastically) the number of unoriented facts as can be seen in Table 2. This is especially useful, since such equations typically lead to huge numbers of critical pairs. This criterion contributed significantly to the superior performance of WALDMEISTER 7/99 on the Moufang identities in the CADE-16 ATP system competition (Sutcliffe, 2000).

WM-DEL: This variant shows an unstable behavior. While there are examples for positive effects, there is a modest number of proof tasks where WM-DEL performs even worse than WM, for example RNG035-7.

WM-GJ: The combination of the semantic criterion with the syntactic one here further reduces the number of generated critical pairs up to 50 % (compared to WM-AC). This can even be seen in the running times, since we get speed-ups although the syntactic criterion is computationally much more expensive than the semantic one. This effect is especially significant when AC-axioms play a dominant role such as in the Robbins domain.

An interesting question is why the variants WM-DEL and WM-GJ behave so differently. Analyzing the number of ground joinable facts in Table 3 we come to the following conclusion: Since WM-DEL deletes ground joinable facts, the simplification relation gets weakened, in some cases even significantly. Therefore, facts which could easily be shown to be redundant by a normal joinability test now have to be eliminated via the far more expensive ground joinability test. Since WM-GJ avoids this weakening of the simplification relation it shows a much better behavior. This justifies the complications in the theoretical part to allow the use of ground joinable equations for interreduction.

Table 3: Number of ground joinable facts (by semantic/syntactic criterion).

Problem	WM-AC	WM-DEL	WM-GJ
GRP177-2	84 + 0	111 + 15	84 + 9
LAT023-1	863 + 0	1958 + 790	491 + 37
RNG027-5	305 + 0	348 + 45	407 + 59
RNG035-7	1656 + 0	35053 + 17299	1139 + 8
ROB006-1	4892 + 0	6613 + 1045	3621 + 153

7. Conclusion and further work

To our knowledge, this is the first successful integration of ground joinability criteria into a high-performance prover. The experiments clearly demonstrate that the new techniques significantly improve the power of our system, especially when AC-operators are present. As the WM-AC variant shows, already the semantic criterion leads to tremendous speed-ups, which is really surprising, considering the tiny implementation effort. The different behavior of WM-DEL and WM-GJ shows the advantage to have the possibility to retain ground joinable equations for simplification purposes.

These results encourage us to investigate further improvements of our theoretical approach. The developed theoretical framework gives rise to a variety of criteria to show ground joinability. Therefore, we search for new criteria which are more powerful, but still computationally feasible.

References

L. Bachmair, N. Dershowitz, and D. A. Plaisted (1989). Completion without failure. In H. Aït-Kaci (Ed.): *Resolution of Equations in Algebraic Structures*, volume 2, pages 1–30. Academic Press.

L. Bachmair and H. Ganzinger (1994). Rewrite-based equational theorem proving with selection and simplification. Journal of Logic and Computation, **4**, pages 217–247.

M. P. Bonacina and J. Hsiang (1995). Towards a foundation of completion procedures as semidecision procedures. Theoretical Computer Science, **146**, pages 199–242.

A. Buch and Th. Hillenbrand (1996). WALDMEISTER: Development of a High Performance Completion-Based Theorem Prover. SEKI-Report 96-01, Universität Kaiserslautern.

H. Comon, P. Narendran, R. Nieuwenhuis, and M. Rusinowitch (1998). Decision problems in ordered rewriting. In *Proceedings of the 13th Annual IEEE Symposium on Logic in Computer Science*, IEEE Computer Society, pages 276–286.

P. Graf (1996). *Term Indexing*, LNCS 1053.

Th. Hillenbrand, A. Buch, R. Vogt, and B. Löchner (1997). WALDMEISTER: High performance equational deduction. J. of Automated Reasoning, **18**, pages 265–270.

Th. Hillenbrand, A. Jaeger, and B. Löchner (1999). System description: WALDMEISTER – improvements in performance and ease of use. In *Proceedings of the 16th International Conference on Automated Deduction*, LNAI 1632, pages 232–236.

J. Hsiang and M. Rusinowitch (1987). On word problems in equational theories. In *Proceedings of the 14th International Colloquium on Automata, Languages and Programming*, LNCS 267, pages 54–71.

D. E. Knuth and P. B. Bendix (1970). Simple word problems in universal algebras. In J. Leech (Ed.): *Combinatorial Problems in Abstract Algebra*, pages 263–297. Pergamon Press.

D. Kapur, P. Narendran, and F. Otto (1990). On ground-confluence of term rewriting systems. Information and Computation, **86**, pages 14–31.

D. Lankford (1975). Canonical Inference. Technical Report ATP-32, Department of Mathematics and Computer Science, University of Texas, Austin.

U. Martin and T. Nipkow (1990). Ordered rewriting and confluence. In *Proceedings of the 10th International Conference on Automated Deduction*, LNCS 449, pages 366–380.

R. Nieuwenhuis and A. Rubio (1995). Theorem proving with ordering and equality constrained clauses. Journal of Symbolic Computation, **19**, pages 321–352.

G. E. Peterson (1990). Complete sets of reductions with constraints. In *Proceedings of the 10th International Conference on Automated Deduction*, LNCS 449, pages 381–395.

G. Peterson and M. Stickel (1981). Complete sets of reduction for some equational theories. Journal of the ACM, **28**, pages 233–264.

G. Peterson (1983). A technique to establish completeness results in theorem proving with equality. SIAM Journal of Computing, **12**, pages 82–100.

G. Sutcliffe and G. Suttner (1998). The TPTP problem library. CNF release v.1.2.1. Journal of Automated Reasoning, **21**, pages 177–203.

G. Sutcliffe (2000). The CADE-16 system competition. Journal of Automated Reasoning, **24**, pages 371–396.