Rewrite Closures for Ground and Cancellative AC Theories

Ashish Tiwari

SRI International,
333 Ravenswood Ave,
Menlo Park, CA, U.S.A
tiwari@csl.sri.com

Abstract. Given a binary relation $E \cup R$ on the set of ground terms over some signature, we define an abstract rewrite closure for $E \cup R$. An abstract rewrite closure is a specialized bottom-up tree automata and it can be used to efficiently decide the reachability relation $\rightarrow_{E \cup E^- \cup R}$. It is constructed using a completion like procedure. Correctness is established using proof ordering techniques. The procedure is extended, in a modular way, to deal with signatures containing cancellative associative commutative function symbols.

1 Introduction

Completion techniques for term rewriting systems have been traditionally used for reasoning about a congruence relation on the set of terms, i.e., equivalence relations that are also closed under substitutions and contexts. They have successfully yielded uniform methods to deal with several specialized theories and algebras. This is useful from various perspectives—for one, it replaces the axioms of the special theory of interest (which increase the search space) by inference rules. Second, it is useful when considering combinations of these procedures and their incorporation with a general purpose theorem proving system. Third, a description in terms of a well studied method like completion helps to incorporate optimizations by avoiding redundant inferences, incorporating more simplification, and adding ordering restrictions. However, several relations of interest, for instance reachability or the ordering relations, are not congruence relations and standard rewriting techniques are not applicable directly.

In recent years, there has been work on extending rewriting techniques to deal with non-symmetric relations. Sound and refutationally complete inference systems have been obtained for dealing with partial congruence and partial equivalence relations in this way [6]. Usually one obtains suitably restricted (via ordering restrictions) chaining calculi. The gain in efficiency with an ordered system over the unordered variants of chaining are comparable to the improvements achieved by superposition over unrestricted paramodulation.

This paper presents a completion based approach to decide the rewrite relation induced by a set of directed (i.e. asymmetric) and undirected (i.e. symmetric) equations. The basic technique involves combining standard completion (for undirected equations) with asymmetric completion (for directed equations). Standard completion is reflected in a *superposition* inference rule that deduces critical pairs between undirected equations. Asymmetric completion yields a *chaining* inference rule to deduce critical pairs between directed equations. Finally, the interaction between the two kinds of equations is captured using a *paramodulation* inference rule. We first consider the problem of constructing a "convergent system", called a *rewrite closure*, for a set of ground (directed and undirected) equations. Subsequently, we extend the method to allow for cancellative associative commutative function symbols in the signature as well.

Correctness of the inference system is established using the concept of proof orderings. The basic idea here is that each proof is assigned a measure and all inference rules are seen as attempts to transform a proof with a more complex measure into a proof with a smaller measure. The desired form of proof, for example a rewrite proof or a valley proof, is assigned a minimal measure. Correctness arguments based on proof orderings are important because they also show compatibility of the inference systems with certain kinds of simplifications. More specifically, any equation which has a "simpler" proof can be deleted. This paper also demonstrates that proof orderings can be used to reason about asymmetric completion and a combination of asymmetric and regular completion.

If all input equations are undirected, then the problem reduces to the construction of congruence closure. We recently presented a completion based inference system to compute an abstract congruence closure. The length of any derivation using these inference rules is quadratic in the worst case. These rules form the starting point of our investigation. We enhance them with additional rules to handle directed equations.

Our work is also part of the thread of research that considers tree automata techniques to decide certain properties of (ground) rewrite systems. Decidability of confluence of ground term rewriting systems was first shown in [16] using tree automata techniques. Subsequently, the result was improved and the (first-order) theory of ground rewrite system was shown to be decidable [17]. The approach in this paper further refines the notion of a "ground tree transducer" by additional conditions that make the rewrite relation "convergent". It is then easily observed that reachability problem for ground term rewriting systems has a polynomial time solution, and so does the problem of deciding the composition of the reachability relation induced by ground rewrite systems. Reachability for ground rewrite systems was shown to be decidable in polynomial time in [24, 23].

Apart from our interest in extending rewriting techniques to non-symmetric relations, this work is also motivated by developing abstract transformation rules for constraint solving. Efficient constraint solving is crucial for several practical theorem proving systems based on inference rules with ordering restrictions. Typical constraints consist of equational constraints (which are solved by a unification procedure) and ordering constraints (where the ordering usually is a recursive path ordering or something similar). Moreover, sometimes the signature consists of associative commutative function symbols. In this case, AC unification procedures are required to be combined with procedures that decide some

AC compatible ordering. If we ignore the particular aspects of specific orderings and consider only the fact that they define a (irreflexive) rewrite relation, then we are reduced to the problem that we consider here. Note that in this particular application, additional unification rules are required to handle equality constraints, but that can be easily done. In fact, the cancellative axiom is satisfied by any AC compatible total simplification ordering.

In this paper we consider the combination of transitivity, monotonicity and inverse monotonicity, where by inverse monotonicity we mean the property that $C[s] \approx C[t]$ implies $s \approx t$. This is motivated by the theory of ordered fields, where we have $xy > xz$ implies $y > z$ (assuming $x > 0$). Given a finite set of polynomial equations, the theory of Gröbner basis decides several interesting problems related to the *congruence* generated by the set of equations and the polynomial ring axioms [14]. A special case of a set of polynomial equations is a finitely presented commutative semigroup, which defines a binomial ideal [22]. In part, our motivation is to develop a similar theory for certain partial congruence relations over the theory of polynomial rings. In this paper, we consider the *generalized rewrite closure* relation for the case of binomials. Using a completion like procedure, we construct a basis which implies the decidability of this relation.

Petri nets are one of the most popular formal models studied in the literature. Petri nets are mathematically equivalent to vector addition systems. The reachability problem for petri nets was shown to be decidable in [25, 21]. The petri net reachability problem is equivalent to the problem of deciding the transitive and monotone closure (under additional AC axioms) of a relation specified over a freely generated commutative semigroup. Note that the symmetric, monotonic and transitive closure is decided by the Gröbner basis algorithm. For decidability results for petri nets, see [18].

Preliminaries

Let Σ be a set, called a *signature*, with an associated *arity function* $\alpha : \Sigma \to 2^{\mathbb{N}}$ and let $\mathcal{V}$ be a disjoint (denumerable) set. We define $\mathcal{T}(\Sigma, \mathcal{V})$ as the smallest set containing $\mathcal{V}$ and such that $f(t_1, \ldots, t_n) \in \mathcal{T}(\Sigma, \mathcal{V})$ whenever $f \in \Sigma, n \in \alpha(f)$ and $t_1, \ldots, t_n \in \mathcal{T}(\Sigma, \mathcal{V})$. The elements of the sets Σ, $\mathcal{V}$ and $\mathcal{T}(\Sigma, \mathcal{V})$ are respectively called *function symbols*, *variables* and *terms* (over Σ and $\mathcal{V}$). Elements c in Σ for which $\alpha(c) = \{0\}$ are called *constants*. By $\mathcal{T}(\Sigma)$ we denote the set $\mathcal{T}(\Sigma, \emptyset)$ of all variable-free, or *ground* terms. The symbols $s, t, u, \ldots$ are used to denote terms; $f, g, \ldots$, function symbols; and $x, y, z, \ldots$, variables. We write $t[s]$ to indicate that a term t contains s as a subterm and (ambiguously) denote by $t[u]$ the result of replacing a particular occurrence of s by u.

An *(undirected) equation* is an unordered pair of terms, written $s \approx t$. A *directed equation* or *rule* is an ordered pair of terms, written $s \to t$. If E is a set of rules, then we define $E^- = \{s \to t : t \to s \in E\}$ and $E^{\pm} = E \cup E^-$. A set E of rules is called a *rewrite system* and the *rewrite relation* $\to_E$ induced by E is defined by: $u \to_E v$ if, and only if, $u = u[l\sigma]$, $v = u[r\sigma]$, $l \approx r$ is in E, and σ is some substitution.

If $\rightarrow$ is a binary relation, then $\leftarrow$ denotes its inverse, $\leftrightarrow$ its symmetric closure, $\rightarrow^+$ its transitive closure and $\rightarrow^*$ its reflexive-transitive closure. A set of rules E is *terminating* if there exists no infinite reduction sequence $s_0 \rightarrow_E s_1 \rightarrow_E s_2 \cdots$ of terms.

We will mostly be interested in ground rewrite systems $E \cup R$ and the rewrite relation $\rightarrow^*_{E^\pm \cup R}$. A *proof* of $s \rightarrow t$ (in E) is a finite sequence $s = s_0 \rightarrow_E s_1,\ s_1 \rightarrow_E s_2,\ \cdots, s_{k-1} \rightarrow_E s_k = t (k \geq 0)$, which is usually written in abbreviated form as $s = s_0 \rightarrow_E s_1 \rightarrow_E \cdots \rightarrow_E s_k = t (k \geq 0)$.

2 Abstract Rewrite Closure

We closely follow the idea of an abstract congruence closure [9] in defining the notion of an abstract rewrite closure. More specifically, we *flatten* out terms via introduction of new constants and corresponding definitions.

Definition 1. *Let Σ be a signature and K be a set of constants disjoint from Σ. A* D-rule *(with respect to Σ and K) is a rewrite rule of the form $f(c_1, \ldots, c_k) \rightarrow c$ where $f \in \Sigma$ is a k-ary function symbol and $c_1, \ldots, c_k, c$ are constants in set K. A rewrite rule of the form $c \rightarrow f(c_1, \ldots, c_k)$ will be called a* reverse D-rule.

A C-rule *(with respect to K) is a rule $c \rightarrow d$, where c and d are constants in K.*

A set of D-rules and C-rules (with respect to Σ and K) is a specification of a bottom-up tree automaton transitions [15]. The set K represent "states" in the tree automaton. Thus, C-rules represent ϵ-transitions.

A set of ground equations and rules, say $I_0 = \{f(g(a, b), g(a, b)) \approx a,\ a \rightarrow b\}$ can be flattened and represented as $I_1 = \{f(c_3, c_3) \approx c_1,\ c_1 \rightarrow c_2\}$ by introducing the set $E_0 = \{a \rightarrow c_1, b \rightarrow c_2, g(c_1, c_2) \rightarrow c_3\}$ of D-rules. This transformation preserves the underlying rewrite theory (in the sense of Definition 2).

A constant c in K is said to *represent* a term t in $\mathcal{T}(\Sigma)$ via the rewrite system E if $t \leftrightarrow^*_E c$. For example, the constant c_3 represents the term $g(a, b)$ via E_0.

Definition 2 (Abstract rewrite closure). *Let Σ be a signature and K be a set of constants disjoint from Σ. A ground rewrite system $E \cup F \cup B$ is said to be an* (abstract) rewrite closure *(with respect to Σ and K) if*

(i) E and F are both sets of D-rules and C-rules, B is a set of reverse D-rules and C-rules such that each constant $c \in K$ represents some term $t \in \mathcal{T}(\Sigma)$ via E, and

(ii) the rewrite systems $F \cup E$ and $B^- \cup E$ are terminating; and for all terms $s, t \in \mathcal{T}(\Sigma)$, if $s \rightarrow^*_{F \cup B \cup E^\pm} t$ then $s \rightarrow^*_{F \cup E} \circ \rightarrow^*_{B \cup E^-} t$.

Moreover, if $I = \mathbb{E} \cup \mathbb{R}$ is a set of ground equations and rules (over $\mathcal{T}(\Sigma)$) such that

(iii) for all terms s and t in $\mathcal{T}(\Sigma)$, $s \rightarrow^*_{\mathbb{R} \cup \mathbb{E}^\pm} t$ if and only if $s \rightarrow^*_{F \cup B \cup E^\pm} t$, then $E \cup F \cup B$ will be called an (abstract) rewrite closure for I.

The set $E \cup F \cup B$ defines a pair of (bottom-up) tree automata [15]: the set $F \cup E$ defines the transitions of the first automaton and the set $B^{-} \cup E$ defines the transitions of the second automaton (over the same set K of "states"). Such a pair defines a binary relation $\rightarrow^*_{F \cup E} \circ \rightarrow^*_{B \cup E^-}$ on the set of ground terms and is called a "ground tree transducer" in the tree automata literature [15]. Thus, the notion of a rewrite closure is more strict than that of a ground tree transducer due to additional conditions in (i) and (ii) above.

The set E_0 (and $E_0 \cup I_1$) is not a rewrite closure for I_0 as condition (iii) above is violated. But we can transform the set $E_0 \cup I_1$, using a combination of standard completion and asymmetric completion, to obtain a rewrite closure

$$\begin{array}{ll} E_1 = \{a \rightarrow c_1,\ b \rightarrow c_2,\ g(c_1, c_2) \rightarrow c_2,\ f(c_3, c_3) \rightarrow c_1\} & \\ F_1 = \{c_1 \rightarrow c_2\} \qquad\qquad B_1 = \{c_3 \rightarrow g(c_2, c_2)\}. & \end{array}$$

Note that the rewrite rules in E_1 semantically encode a symmetric relation whereas the rules in R_1 are interpreted asymmetrically. A rewrite closures for $\mathbb{E} \cup \mathbb{R}$ gives a decision procedure for (deciding) the rewrite relation $\rightarrow^*_{\mathbb{R} \cup \mathbb{E}^{\pm}}$.

3 Construction of Rewrite Closure

We next present an inference system to construct a rewrite closure for a finite set I of ground equations and rules over the signature Σ. Our description is fairly abstract, in terms of transition rules that operate on tuples (I, E, R), where $I = \mathbb{E} \cup \mathbb{R}$ is a set of ground equations and rules (over Σ), and E and R are sets of D-rules and C-rules. Tuples represent possible *states* in the process of constructing a rewrite closure. The initial state is $(I_0, \emptyset, \emptyset)$, where I_0 is the input set of ground equations and rules (over $\mathcal{T}(\Sigma)$).

The transition rules can be derived from those for standard completion and asymmetric completion as described in [3] and [19], with some differences so that a system is constructed over an *extended* signature. The transition rules do *not* require a total reduction ordering[1] on terms in $\mathcal{T}(\Sigma)$, but simply an ordering on $\mathcal{T}(\Sigma \cup U)$ (that is, terms in $\mathcal{T}(\Sigma)$ need not be comparable in this ordering) where U is an infinite set disjoint from Σ from which new constants are chosen. In particular, we assume $\succ_U$ is any ordering on the set U and define $\succ$ by: $t \succ c$ if either $t \succ c$ is a D-rule or it is a C-rule such that $t \succ_U d$. For simplicity, we take U to be the set $\{c_0, c_1, c_2, \ldots\}$ and assume that $c_i \succ_U c_j$ if, and only if, $i < j$.

Since an abstract congruence closure [9] is a special case of a rewrite closure (i.e. when $\mathbb{R}_0 = \emptyset$), we use the abstract congruence closure inference rules to handle equations.

Equations and rules are flattened using extension and simplification.

Extension: $$\frac{(I[s], E, R)}{(I[c], E \cup \{s \rightarrow c\}, R)}$$

[1] By an *ordering* we mean any irreflexive and transitive relation on terms. A *reduction ordering* is an ordering that is also a well-founded replacement relation. An ordering $\succ$ is *total* if for any two distinct elements s and t, either $s \succ t$ or $t \succ s$.

if $s \to c$ is a D-rule and $c \in U$ is a new constant.

Simplification1: $$\frac{(I[s], E, R)}{(I[c], E, R)}$$

if[2] $s \to c \in E$.

Once an equations or rule in I is in the form of a D-rule, reverse D-rule, or a C-rule, it can be oriented.

Orientation1: $$\frac{(I \cup \{s \approx c\}, E, R)}{(I, E \cup \{s \to c\}, R)}$$

if $s \to c$ is a D-rule or a C-rule with $s \succ c$.

Orientation2: $$\frac{(I \cup \{s \to t\}, E, R)}{(I, E, R \cup \{s \to t\})}$$

if $s \to t$ is either a C-rule, D-rule, or a reverse D-rule.

Trivial equations and rules are deleted.

Deletion1: $$\frac{(I \cup \{s \approx s\}, E, R)}{(I, E, R)}$$

Deletion2: $$\frac{(I \cup \{s \to s\}, E, R)}{(I, E, R)}$$

Deletion3: $$\frac{(I, E, R \cup \{s \to s\})}{(I, E, R)}$$

Deduction in standard completion, as well as in asymmetric completion, is based on computation of critical pairs. There are three kinds of critical pair computations—(i) between two rules in E, which are handled by superposition; (ii) between a rule in E and a rule in R, which are handled by paramodulation; and (iii) between two rules in R, which are handled by chaining.

Superposition: $$\frac{(I, E \cup \{t \to c, s[t] \to d\}, R)}{(I, E \cup \{t \to c, l \to r\}, R)}$$

if either (i) $s[t] \neq t$, $l = s[c]$, and $r = d$; or, (ii) $s[t] = t$, $d \succ c$, $l = d$, and $r = c$.

Whereas all rules in E are decreasing with respect to the ordering $\succ$, the rules in R are not so. The set R can be parititioned into the set $F = \{s \to t : s \to t \in R \textit{ and } s \succ t\}$ of *forward* rules and the set $B = \{s \to t : s \to t \in R \textit{ and } t \succ s\}$ of *backward* rules.

[2] The notation $I[s]$ denotes that s occurs as a subterm in some equation or rule in I and $I[c]$ then denotes the new set obtained by replacing that occurrence of s in I by c.

Definition 3. *Let E and R be sets of D-rules and C-rules. The set $CP(E,R)$ of critical pairs between rules in E and R is defined as:*

$$\begin{aligned} CP(E,R) = &\{f(\ldots,d,\ldots) \to c : f(\ldots,d',\ldots) \to c \in E \text{ and } d \to d' \in B\} \\ &\cup \{c \to f(\ldots,d,\ldots) : f(\ldots,d',\ldots) \to c \in E \text{ and } d' \to d \in F\}. \end{aligned}$$

The set $CP(R)$ of critical pairs between rules in R is defined as:

$$\begin{aligned} CP(R) = &\{t[d] \to c : d \to s \in B \text{ and } t[s] \to c \in F\} \\ &\cup \{c \to t[d] : c \to t[s] \in B \text{ and } s \to d \in F\}. \end{aligned}$$

Note that if the sets E and R contain only D-rules, reverse D-rules, and C-rules, then so do the sets $CP(E,R)$ and $CP(R)$.

Paramodulation: $$\frac{(I,E,R)}{(I,E,R \cup \{s \to t\})}$$

if $s \to t \in CP(E,R)$.

Chaining: $$\frac{(I,E,R)}{(I,E,R \cup \{s \to t\})}$$

if $s \to t \in CP(R)$.

A crucial component of deductive inference systems is simplification. In the ground case, several deduction steps reduce to simplification. In particular, the rules in E can be used to simplify terms in R.

Simplification2: $$\frac{(I,E \cup \{s \to c\}, R[s])}{(I,E \cup \{s \to c\}, R[c])}$$

Composition: $$\frac{(I,E \cup \{t \to c, u \to s[t]\}, R)}{(I,E \cup \{t \to c, u \to s[c]\}, R)}$$

Example 1. Consider the set $I_0 = \{f(g(a,b),g(a,b)) \approx a, a \to b\}$ of equations and inequations. An abstract rewrite closure for I_0 can be derived from $(I_0,E_0,R_0) = (I_0,\emptyset,\emptyset)$ as follows:

i	Input I_i	Equations E_i	Rules R_i	Transition Rule
0	I_0	$\emptyset$	$\emptyset$	
1	$\{fgabgab \approx a\}$	$\{a \to c_1, b \to c_2\}$	$\{c_1 \to c_2\}$	$\mathbf{Ext}^2 \circ \mathbf{Ori}$
2	$\{fc_3c_3 \approx a\}$	$E_1 \cup \{gc_1c_2 \to c_3\}$	R_1	$\mathbf{Sim}^4 \circ \mathbf{Ext} \circ \mathbf{Sim}$
3	$\emptyset$	$E_2 \cup \{fc_3c_3 \to c_1\}$	R_1	$\mathbf{Sim} \circ \mathbf{Ori}$
4	$\emptyset$	E_3	$R_1 \cup \{c_3 \to gc_2c_2\}$	**Par**

Since no further rules are added, the rewrite system $E_4 \cup F_4 \cup B_4$, where $F_4 = \{c_1 \to c_2\}$ and $B_4 = \{c_3 \to gc_2c_2\}$, is an abstract rewrite closure for I_0.

4 Correctness

Definition 4. *We use the symbol $\vdash$ to denote the one-step transition relation on states induced by the above transition rules. A derivation is a sequence of states $\xi_0 \vdash \xi_1 \vdash \cdots$. A derivation is said to be fair if any transition rule which is continuously enabled is eventually applied. The set E_∞ of persisting rules is defined as $\cup_i \cap_{j>i} E_j$; and similarly, $R_\infty = \cup_i \cap_{j>i} R_j$.*

We shall prove that any fair derivation will only generate finitely many persisting rewrite rules in the second and third components.

Theorem 1. *Let I_0 be a finite set of ground equations and inequations. The set $E_\infty \cup R_\infty$ of persisting rules in any fair derivation starting from the state $(I_0, \emptyset, \emptyset)$ is finite.*

Proof. Each inference step either reduces, or leaves unchanged, the number of Σ-symbols in the I-component. The inference rule which introduces new constants, extension, always reduces this number. Therefore, it follows that the number of new constants introduced in any derivation is finite. Let this number be n.

If the maximum arity of any function symbol in Σ is c, then the number of distinct D-rules is bounded by $|\Sigma|n^{c+1}$ and the number of distinct C-rules is n^2. Consequently, the sets E_∞ and R_∞ are finite. ■

Theorem 2 (Soundness). *If $(\mathbb{E}_0 \cup \mathbb{R}_0, E_0, R_0) \vdash (\mathbb{E}_1 \cup \mathbb{R}_1, E_1, R_1)$, then, the rewrite relation defined by $\mathbb{E}_1^{\pm} \cup \mathbb{R}_1 \cup E_1^{\pm} \cup R_1$ is identical to the rewrite relation defined by $\mathbb{E}_0^{\pm} \cup \mathbb{R}_0 \cup E_0^{\pm} \cup R_0$ over the set $\mathcal{T}(\Sigma \cup K_0)$ of terms, where $K_0 \subset U$ is the set of new constants introduced until state (I_0, E_0, R_0).*

Proof. For the congruence closure inference rules, viz extension, simplification1, orientation, superposition, and composition, this follows from the soundness of those rules, see [7]. The argument for extension and simplification1, when used on rules in the I-component, is identical to the case when they are used on equations. Furthermore, the claim easily follows for the deletion and orientation rules when these are used on rules.

Finally, we need to prove the claim for chaining, paramodulation, and simplification2. Suppose $(I_0, E_0, R_0) \vdash (I_1 = I_0, E_1 = E_0, R_1 = R_0 \cup \{s \to t\})$, using chaining or paramodulation. Clearly, the rewrite relation induced by $\mathbb{E}_0^{\pm} \cup \mathbb{R}_0 \cup E_0^{\pm} \cup R_0$ is contained in the rewrite relation induced by $\mathbb{E}_1^{\pm} \cup \mathbb{R}_1 \cup E_1^{\pm} \cup R_1$. For the other direction, note that every critical pair in $CP(E_0, R_0)$ and $CP(R_0)$ is contained in the rewrite relation defined by $\mathbb{R}_0 \cup \mathbb{E}_0^{\pm} \cup E_0^{\pm} \cup R_0$. In case of simplification2, if $s \to t[u] \in R_0$ is simplified to $s \to t[v] \in R_1$ via $u \to v \in E_0$, then we have $s \to_{R_1} t[v] \leftarrow_{E_1} t[u]$ and $s \to_{R_0} t[u] \to_{E_0} t[v]$. The case when simplification2 is used to simplify a left-hand side term in R_0 is similar. ■

Proof Ordering

The correctness of the procedure will be established using proof simplification techniques, as described by Bachmair [1] and Bachmair and Dershowitz [2], but specialized to our case of regular and non-symmetric ground completion. Let $\succ$ be any reduction ordering containing $\succ_U$ and that orients D-rules from left to right. For instance, a recursive path ordering with an appropriate precedence on function symbols is such an ordering.

Let $s = C[u] \to C[v] = t$ be a proof step using the equation or rule $u \approx v \in \mathbb{E}^{\pm} \cup \mathbb{R} \cup E^{\pm} \cup R$. The complexity of this proof step is defined by

$$\begin{array}{rlrl} (\{s,t\},\bot,\bot,\bot) & \texttt{if}\ \ u \approx v \in \mathbb{E}^{\pm} & (\{s,t\},\bot,\bot,\bot) & \texttt{if}\ \ u \to v \in \mathbb{R} \\ (\{s\},u,\bot,t) & \texttt{if}\ \ u \to v \in E & (\{s\},u,\top,t) & \texttt{if}\ \ u \to v \in R, u \succ v \\ (\{t\},v,\bot,s) & \texttt{if}\ \ u \to v \in E^{-1} & (\{t\},v,\top,s) & \texttt{if}\ \ u \to v \in R, v \succ u \end{array}$$

where $\bot$ and $\top$ are new symbols assumed to be minimum and maximum respectively. Tuples are compared lexicographically using the multiset extension of the ordering $\succ$ on terms in the first component, and the ordering $\succ$ in the second and fourth component. The complexity of a proof is the multiset of complexities of its proof steps. The multiset extension of the ordering on tuples yields a proof ordering, denoted by $\succ_P$. The ordering $\succ_P$ is well-founded as it is a lexicographic combination of well-founded orderings.

Lemma 1. *Suppose* $(I_0, E_0, R_0) \vdash (I_1, E_1, R_1)$. *If* π *is a ground proof,* $s_0 \to s_1 \to \cdots \to s_k$*, in* $\mathbb{E}_0^{\pm} \cup \mathbb{R}_0 \cup E_0^{\pm} \cup R_0$*, then there is a proof* π', $s_0 = s'_0 \to s'_1 \to \cdots \to s'_l = s_k$*, in* $\mathbb{E}_1^{\pm} \cup \mathbb{R}_1 \cup E_1^{\pm} \cup R_1$*, such that* $\pi \succeq_{\mathcal{P}} \pi'$.

Proof. We need to check that each equation or rule in $(\mathbb{E}_0 - \mathbb{E}_1)^{\pm} \cup (\mathbb{R}_0 - \mathbb{R}_1)^{\pm} \cup (E_0 - E_1) \cup (R_0 - R_1)$ has a simpler proof in $\mathbb{E}_1^{\pm} \cup \mathbb{R}_1 \cup E_1^{\pm} \cup R_1$ for each transition rule application. In detail, we have the following cases:

(i) *Congruence Closure Rules.* For the congruence closure inference rules, viz extension, simplification, orientation, deletion, superposition, and composition, the claim follows from the corresponding claim proved for the construction of congruence closure in [7].

In case extension or simplification1 is applied to a rule in $\mathbb{R}_0$, the proof $t[s] \to_{\mathbb{R}_0} u$ is replaced by the proof $t[s] \to_{E_1} t[c] \to_{\mathbb{R}_1} u$. The new proof is smaller as $\{t[s], u\} \succ^m \{t[s]\}$, and $\{t[s], u\} \succ^m \{t[c], u\}$. We can argue similarly for the case when extension or simplification1 is applied on the right-hand side term of an inequation.

In case of orientation, we have that $c \to_{\mathbb{R}_0} d$ is more complex than $c \to_{R_1} d$ because $\{c, d\} \succ^m \{c\}$ and $\{c, d\} \succ^m \{d\}$.

In case of deletion, the proof step that uses the deleted rule can be eliminated and the resulting proof will be smaller.

(ii) *Chaining and Paramodulation.* In this case, the set $(I_0 - I_1) \cup (E_0 - E_1) \cup (R_0 - R_1)$ is empty.

(iii) *Simplification2.* There are different cases to consider here. First, suppose $s[u] \to t \in R_0$ is simplified to $s[v] \to t \in R_1$ by the rule $u \to v \in E_0$. The old proof $s[u] \to_{R_0} t$ is replaced by the new proof $s[u] \to_{E_1} s[v] \to_{R_1} t$. If $s[u] \succ t$, then the new proof is smaller because the rewrite step $s[u] \to_{R_0} t$ is more complex than (a) the proof step $s[u] \to s[v]$ in either the second component, if $s[u] \neq u$, or the third component; and (b) the proof step $s[v] \to t$ in the first component as $s[u] \succ s[v]$ and $s[u] \succ t$. Next suppose that $t \succ s[u]$. In this case, the old rewrite step $s[u] \to_{R_0} t$ is more complex than (a) the proof step $s[u] \to s[v]$ in the first component as $t \succ s[u]$; and (b) the proof step $s[v] \to t$ in the fourth component as $s[u] \succ s[v]$. In case simplification2 reduces the right-hand side of a rule in R_0, the argument is similar.

This completes the proof of the lemma. ∎

The set R_∞ of persisting rules can be partitioned into the set $B_\infty = \{s \to t \in R_\infty : t \succ s\}$ of *backward* rules, and the set $F_\infty = \{s \to t \in R_\infty : s \succ t\}$ of *forward* rules.

Theorem 3 (Completeness). *Let I_0 be a finite set of equations and inequations. If $(I_\infty, E_\infty, F_\infty \cup B_\infty)$ is the persisting state of a fair derivation starting from $(I_0, \emptyset, \emptyset)$, then, the rewrite system $E_\infty \cup F_\infty \cup B_\infty$ is an abstract rewrite closure for I_0.*

Proof. Fairness implies that all superposition, paramodulation, and chaining inferences between rules in E_∞ and R_∞ are contained in the set $(\cup_i E_i) \cup (\cup_i R_i)$. Since all deduced rules are either D-rules, reverse D-rules, or C-rules, the sets E_∞ and R_∞ contain only such rules. Fairness also implies that I_∞ is empty, since every equation or inequation in I_0 can be converted into a D-rule, reverse D-rule, or C-rule via extension and simplification, and every such rule can be either deleted or oriented.

Since the proof ordering is well-founded, it follows from Lemma 1 that for every proof in $\mathbb{E}_i^{\pm} \cup \mathbb{R}_i \cup E_i^{\pm} \cup R_i$, there exists a minimal proof π in $E_\infty^{\pm} \cup R_i$. We argue by contradiction that certain proof patterns can not occur in the minimal proof π: specifically, there can not be any peaks $s \to_{E_\infty}^{-1} u \to_{E_\infty} t$, $s \to_{E_\infty}^{-1} u \to_{F_\infty} t$, $s \to_{B_\infty} u \to_{E_\infty} t$, or $s \to_{B_\infty} u \to_{F_\infty} t$.

A non-overlap peak, $C[t,u] \to C[s,u] \to C[t,v]$, between rules $t \to s$ $(s \succ t)$ and $u \to v$ $(u \succ v)$ can be eliminated by commuting the two proof steps, $C[t,u] \to C[t,v] \to C[s,v]$. The new proof is smaller because the largest term, $C[s,u]$, is eliminated.

Next suppose that there is a proper overlap $t \to s[u] \to s[v]$ with $s = s[u] \succ t$ and $u \succ v$. We can consider different cases now:
(a) if $s[u] \to t \in E_\infty$ and $u \to v \in E_\infty$, then there is a possible superposition inference and fairness guarantees that $t \to s[v] \in \cup_i E_i^{\pm}$, for some i.
(b) if $s[u] \to t \in E_\infty$ and $u \to v \in R_\infty$, then there is a possible paramodulation inference if $s[u] \neq u$, and a possible simplification2 inference if $s[u] = u$, and fairness guarantees that $t \to s[v] \in \cup_i R_i$, for some i.
(c) if $t \to s[u] \in R_\infty$ and $u \to v \in E_\infty$, then there is a possible simplification2 inference and fairness guarantees that $t \to s[v] \in \cup_i R_i$, for some i.
(d) if $t \to s[u] \in R_\infty$ and $u \to v \in R_\infty$, then there is a possible chaining inference and fairness guarantees that $t \to s[v] \in \cup_i R_i$, for some i.

Thus, the original peak has a smaller proof, $t \to s[v]$, in $E_i^{\pm} \cup R_i$. This new proof is smaller because the largest term, $s[u]$, has been eliminated from the proof. Using Lemma 1, we may infer that there is a smaller proof in $E_\infty^{\pm} \cup R_\infty$, a contradiction. This proves that the minimal proof can not have any peaks. This implies that for all terms $s, t \in \mathcal{T}(\Sigma)$, if $s \to^*_{F_\infty \cup B_\infty \cup E_\infty^{\pm}} t$ then $s \to^*_{F_\infty \cup E_\infty} \circ \to^*_{B_\infty \cup E_\infty^-} t$.

Since $E_\infty \cup F_\infty \cup B_\infty^-$ are all contained in the ordering $\succ$, hence the rewrite systems $E_\infty \cup F_\infty$ and $E_\infty \cup B_\infty^-$ are terminating. In order to prove that $F_\infty \cup B_\infty \cup E_\infty$ is a rewrite closure, note that property (i) of Definition 2 follows from observation and the correctness of congruence closure inference rules. Finally, to prove property (iii), if $s \to^*_{\mathbb{E}_0^{\pm} \cup \mathbb{R}_0} t$, then Lemma 1 implies that there is a proof $s \to^*_{E_\infty^{\pm} \cup R_\infty} t$. This establishes that $E_\infty \cup F_\infty \cup B_\infty$ is a rewrite closure *for* $\mathbb{E}_0 \cup \mathbb{R}_0$. ■

Since $R_\infty \cup E_\infty$ is finite, there exists a k such that $R_\infty \cup E_\infty \subset R_k \cup E_k$, and we can identify the finite set of persisting rules if we eagerly apply simplification rules. Note that the relation $\to^*_{F \cup E} \circ \to^*_{B \cup E^{-1}}$ is decidable as the rewrite systems $F \cup E$ and $B^- \cup E$ are terminating, see [19] for details. The search for a rewrite proof involves a *search*: the F and B^- proof steps are "don't know" non-deterministic (i.e. we need to make the right guess to get a rewrite proof), whereas E proof steps are "don't care" non-deterministic (and we can apply any such step and we will still get a proof if one exists).

Other Remarks

In case there are no input inequations, i.e. $\mathbb{R}_0 = \emptyset$, the above set of inference rules construct an abstract congruence closure for $\mathbb{E}_0$. A crucial component of this presentation is the introduction of new constants to enrich the signature. In the case of congruence closure, this ensures that the derivation length is at worst quadratic in the input size [10]. In contrast, naive ground completion could be worst case exponential. In case of construction of abstract rewrite closure, using the above result for construction of congruence closure, we can show that we can reach a state consisting of all persisting rules using derivations of length $O(n^2 + n^{c+1})$, where n is the size of the input and c is the maximum arity of any symbol in Σ.

It is known that the first-order theory of ground rewrite systems is decidable [17]. The proof is based on associating a ground tree transducer with the rewrite relation induced by a ground rewrite system and associating inductively an automaton of a more general class (RR) with any formula. Existence of a finite rewrite closure for an arbitrary set of ground equations and rules follows from the above more general result—as any undirected equation, $s \approx t$, can be treated as two rules, $s \to t$ and $t \to s$. In fact, the construction in our approach is equivalent to construction of a ground tree transducer. However, there are the following difference in our approach: (a) Undirected equations are treated using congruence closure, and not as two distinct rules; (b) The steps for construction of a ground tree transducer are explicit and the construction is not a consequence of the closure properties of RR automata under certain boolean or set operations; (c) Our procedure is based on standadrd completion techniques; (d) The correctness argument is in terms of proof orderings; and, (e) Our procedure can be extended to AC symbols, whereas tree automata techniques have not been extended to such richer signatures. We explain the last two points further below.

Correctness arguments based on proof orderings allow for clear identification of redundant inferences. Consequently, additional simplification rules can be easily added without compromising correctness. To illustrate this point, consider the following inference rule:

Optimization: $$\frac{(I, E, R \cup \{s \to t, t \to s\})}{(I, E \cup \{s \to t\}, R)}$$

if $s \succ t$.

This inference rule is clearly sound. The completeness of the inference system that includes this rule easily follows by observing that the deleted rules $s \to t$ and $t \to s$ have simpler proofs using the new rule in the E-component. The new proofs are simpler in the third component.

Finally, we can extend our presentation to handle cancellative associative commutative function symbols, whereas tree automata techniques have not been extended to such richer signatures. In fact, suitably interpreted, our procedure indicates the kind of generalization in tree automata required to incorporate associative commutative symbols into them.

5 Ground Cancellative *AC* Theories

We next enrich the signature with additional AC symbols Σ_{AC}. We consider AC symbols to be varyadic, with arity $\alpha(f) = \{2, 3, 4, \ldots\}$ for $f \in \Sigma_{AC}$. Apart from the associative and commutative axioms, the symbols $f \in \Sigma_{AC}$ also satisfy the cancellative axioms (or inverse monotonicity axioms),

$$\begin{array}{l} f(x_1, x_2, \ldots, x_m) \approx f(x_1, y_2, \ldots, y_m) \text{ iff } f(x_2, \ldots, x_m) \approx f(y_2, \ldots, y_m) \\ f(x_1, x_2, \ldots, x_m) \to f(x_1, y_2, \ldots, y_m) \text{ iff } f(x_2, \ldots, x_m) \to f(y_2, \ldots, y_m), \end{array}$$

and the identity axiom $f(x, e_f) \approx x$, where e_f is the identity element for f.

If $f \in \Sigma_{AC}$, then the *extension* of a rule $f(s_1, s_2) \to t$, call it ρ, is defined as $f(f(s_1, s_2), x) \to f(t, x)$ and is denoted by ρ^e. Given a rewrite system R, by R^e we denote the set R plus extensions of rules in R. By $AC\backslash R$ we denote the rewrite system consisting of all rules $u \to v$ such that $u \leftrightarrow^*_{AC} u'\sigma$ and $v = v'\sigma$, for some rule $u' \to v'$ in R and some substitution σ. To simplify notation, we shall denote $\to_{AC\backslash R^e}$ by just $\to_R$.

In the presence of AC-symbols, apart from the D-rules and C-rules, we additionally require A-rules of the form

$$f(c_1, c_2, \ldots, c_m) \to f(d_1, d_2, \ldots, d_k) \qquad m, k \in \alpha(f).$$

Unlike D-rules and C-rules, A-rules do not correspond to any standard notion of a transition in a bottom-up tree automata.

We first consider a simple case of cancellative abelian monoid. The final set of inference rules for the general case will be obtained as a combination of the rules for dealing with standard symbols and rules for dealing with an individual AC symbol.

6 Cancellative Abelian Monoid

Let the signature $\Sigma = \{\cdot\}$ consists of an associative commutative function symbol $\cdot$ which also satisfies the cancellative axioms. Let $K = \{e, c_1, c_2, \cdots, c_m\}$ be a finite number of constants where e is an identity element for $\cdot$. We denote an application of $\cdot$ by juxtaposition and use exponentiation notation and write, for example, c_1^2 for the term $c_1 \cdot c_1$. Moreover, we denote by $[s, t]$ the term that is the greatest common divisor of s and t. Thus, $[c_1^2 c_2 c_3, c_1 c_2^2 c_4] = c_1 c_2$.

Let $R_0 = \{s_1 \to t_1, s_2 \to t_2, \ldots, s_n \to t_n\}$ be a set of directed rules over the signature $\Sigma \cup K$. We first show how to "complete" this set. Each rule $s_1 \to t_1$ is (when fully flattened and reduced using the identity axiom) either a D-rule, a reverse D-rule, a C-rule, or a A-rule.

We shall associate a measure with every rule. The measure will be a vector from the set N^n, where $N = \{0, 1, 2, \ldots\}$ is the set of natural numbers. For the initial set of equations, we assign measures as follows: the rule $s_i \to t_i$ is assigned the measure $\boldsymbol{\varepsilon_i} = \langle 0, 0, \ldots, 0, 1, 0, \ldots, 0\rangle$, where 1 is in exactly the i-th component. The purpose of the measure is to assign a complexity to each rule so that we can use *collapse* to delete rules with large measures.

We maintain the invariant that the greatest common divisor $[l_i, r_i]$ is e for all rules $l_i \to r_i \in R$ and hence, we assume that $[s_i, t_i] = e$ for every $i = 1, 2, \ldots, n$. We shall use an AC compatible total simplification ordering[3] $\succ$ on the set of terms over Σ to restrict the deduction steps. For instance, the lexicographic ordering, or the total degree lexicographic ordering are such orderings [11].

Recall that we rewrite modulo AC and hence there is a proper overlap between terms t and u only if $[t, u] \neq e$.

ACC-Chaining: $$\frac{(I, E, R \cup \{s \to t, u \to v\})}{(I, E, R \cup \{s \to t, u \to v, \frac{su}{[s,v][t,u]} \to \frac{tv}{[s,v][t,u]}\})}$$

if $[t, u] \neq e$ and either (a) $t \succ s$ and $u \succ v$; or (b) $s \succ t$, $u \succ v$, and $s \to t$ is not a C-rule; or (c) $t \succ s$, $v \succ u$, and $u \to v$ is not a C-rule. The new rule is assigned the measure $\boldsymbol{\alpha} + \boldsymbol{\beta}$, where $\boldsymbol{\alpha}$ is the measure associated with the rule $s \to t$ and $\boldsymbol{\beta}$ is the measure associated with the rule $u \to v$. Note that the

[3] In this context, an AC-compatible total simplification ordering (on ground terms) is a well-founded ordering with the following three properties: (i) $su \succ sv$ whenever $u \succ v$, (ii) $su \succ u$ whenever $s \neq I$, (iii) $s' \succ t'$ whenever $s' \leftrightarrow^*_{AC} s$, $t' \leftrightarrow^*_{AC} t$ and $s \succ t$, and (iv) either $s \succ t$ or $t \succ s$ or $s \leftrightarrow^*_{AC} t$, for all terms s, t, u, v, s', and t'.

ordering restrictions in this inference rule are weaker than the restriction in a superposition rule (where we require $t \succ s$ *and* $u \succ v$).

In order to ensure termination, we need to identify and delete redundant rules.

$$\textbf{ACC-Collapse1:} \qquad \frac{(I, E, R \cup \{s \to t, u' \to v'\})}{(I, E, R \cup \{s \to t, u \to v\})}$$

if $u' \leftrightarrow^*_{AC} su, v' \leftrightarrow^*_{AC} tv$, and $\boldsymbol{\alpha} < \boldsymbol{\beta}$, where $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$ are the measures associated with the rules $s \to t$ and $u' \to v'$ respectively. The rule $u \to v$ is assigned the measure $\boldsymbol{\beta} - \boldsymbol{\alpha}$.

Along with the deletion3 rule, this forms a set of transformations that can be used to complete a given finite set of directed rules over a signature containing exactly one cancellative AC function symbol and finitely many constants.

Example 2. Consider the set $R_0 = \{c_1^2 \to c_2, c_2^2 \to c_1\}$ of directed rules. We can complete this set as follows (we show only the third component of the state here as the other components remain unchanged):

i	Rules R_i	Measure	Transition Rule
0	R_0		
1	$R_0 \cup \{c_1c_2 \to e\}$	$[1,1]$	$\mathbf{ACC-Ch}$
2	$R_1 \cup \{c_1^3 \to e\}$	$[2,1]$	$\mathbf{ACC-Ch}$
3	$R_2 \cup \{c_2^3 \to e\}$	$[1,2]$	$\mathbf{ACC-Ch}$
4	$R_3 \cup \{c_1^2c_2^2 \to e\}$	$[2,2]$	$\mathbf{ACC-Ch}$
5	R_3		$\mathbf{ACC-Col1}$

Any further rule deduced by chaining can be simplified by collapse and no additional rules are added to the set R_3. Thus, the system R_3 is the desired completion.

Correctness

If R is a rewrite system and there is a proof $s \to^*_{R\cup AC} t$ using the cancellative axioms, then there exists a term u such that there is a proof $s \cdot u \to^*_{R\cup AC} t \cdot u$. We say $s \to^{[]}_R t$ if, and only if, there exists a term u such that $s \cdot u \to_R t \cdot u$. The reflexive-transitive closure of the relation $\to^{[]}_R$ and is denoted by $\to^{[*]}_R$. We need the following technical lemma to establish correctness of the inference rules outlined above.

Lemma 2. *Let $R_0 = \{s_1 \approx t_1, \ldots, s_n \approx t_n\}$ be a set of terms over $\Sigma \cup K$. Suppose s and t are terms such that $\frac{s}{t} = (\frac{s_1}{t_1})^{\alpha_1}(\frac{s_2}{t_2})^{\alpha_2} \cdots (\frac{s_n}{t_n})^{\alpha_n}$ for some $\alpha_1, \ldots, \alpha_n \in N$. Then, $s \to^{[*]}_{AC\backslash R_0^e} \circ \leftrightarrow^*_{AC} t$.*

Proof. We shall show that $ss_1^{\alpha_1}s_2^{\alpha_2}\ldots s_n^{\alpha_n}$ can be reduced to $ts_1^{\alpha_1}s_2^{\alpha_2}\ldots s_n^{\alpha_n}$ via $R_0 \cup AC$. This follows from

$$ss_1^{\alpha_1}s_2^{\alpha_2}\ldots s_n^{\alpha_n} \to^*_{AC\backslash R_0^e} st_1^{\alpha_1}s_2^{\alpha_2}\ldots s_n^{\alpha_n} \to^*_{AC\backslash R_0^e} \cdots \to^*_{AC\backslash R_0^e} st_1^{\alpha_1}t_2^{\alpha_2}\ldots t_n^{\alpha_n}$$

and the fact that $st_1^{\alpha_1}t_2^{\alpha_2}\ldots t_n^{\alpha_n} \leftrightarrow^*_{AC} ts_1^{\alpha_1}s_2^{\alpha^2}\ldots s_n^{\alpha_n}$. ∎

Note that if $s \to t \in \cup_i R_i$, then $[s,t]=e$. Furthermore, if $\boldsymbol{\alpha} = \langle \alpha_1, \ldots, \alpha_n \rangle$ is the measure associated with $s \approx t$, then $s/t = (s_1/t_1)^{\alpha_1}\cdots(s_n/t_n)^{\alpha_n}$, where $s_i \approx t_i \in R_0$ are the initial set of rules. It thus follows from the above lemma that any two rules with the same measure are identical.

We shall prove that any fair derivation will only generate finitely many persisting rewrite rules using Dickson's lemma [11]. Since the number of constansts $|K|$ is finite, the divisibility relation on terms defines a Dickson partial order.

Theorem 4. *Let R_0 be a finite set of ground rules over $\Sigma \cup K$. The set R_∞ of persisting rules in any fair derivation starting from the state $(\emptyset, \emptyset, R_0)$ is finite.*

Proof. Suppose the set R_∞ is not finite. By Dickson's lemma, there exists an infinite chain of rules in the set R_∞

$$u_0 \approx v_0,\ u_1 \approx v_1,\ u_2 \approx v_2,\ u_3 \approx v_3, \ldots$$

with measures $\boldsymbol{\alpha_0}, \boldsymbol{\alpha_1}, \boldsymbol{\alpha_2}, \ldots$ such that for all $i = 0, 1, 2, \ldots$, we have $u_i | u_{i+1}$, $v_i | v_{i+1}$, and $\boldsymbol{\alpha_i} \leq \boldsymbol{\alpha_{i+1}}$. Since the rules in the above sequence are assumed to be distinct, the measure α_i's are distinct (by the observation following Lemma 2). But, now consider the rules $u_0 \approx v_0$ and $u_1 \approx v_1$. We can use ACC-Collapse1 to delete the second rule. This implies that $u_1 \approx v_1 \notin R_\infty$, a contradiction. ∎

Proof Ordering

As before, the correctness of the procedure will be established using proof simplification techniques. Recall that $\succ$ is some AC-compatible total simplification ordering over terms in $\mathcal{T}(\Sigma \cup K)$. Let $s = s_0 s' \to_{AC\backslash R^e \cup AC} t_0 s' = t$ be a proof step using the (extension of) rule $s_0 \to t_0 \in R \cup AC$. The complexity of this proof step is defined by

$$\begin{array}{rl} (\{s_0 s'\}, s_0, \top, t_0 s') & \texttt{if}\ \ s_0 \approx t_0 \in R, s_0 \succ t_0 \\ (\{t_0 s'\}, t_0, \top, s_0 s') & \texttt{if}\ \ s_0 \approx t_0 \in R, t_0 \succ s_0 \\ (\{s_0 s'\}, \bot, \bot, \bot) & \texttt{if}\ \ s_0 \approx t_0 \in AC \end{array}$$

where $\bot$ is a new constant symbol assumed to be minimum, and $\boldsymbol{\alpha}$ is a measure, given as a vector in N^n, associated with the corresponding rule. Tuples are compared lexicographically using the multiset extension of the ordering $\succ$ on terms in the first component and the ordering $\succ$ on terms in the second and fourth components. The complexity of a proof is the tuple consisting of (i) the product of left-hand sides of all R rules used in the proof and (ii) the multiset of complexities of the proof steps in the proof. Proof complexities are compared using a lexicographic combination of the ordering $\succ$ in the first component and the ordering on proof steps in the second component. This ordering on proofs can be verified to be a proof ordering [4] which we denote by $\succ_P$. The ordering $\succ_P$ is well-founded as it is a lexicographic combination of well-founded orderings.

[4] A relation $\succ$ on proofs is a proof ordering if whenever $P \succ Q$, then $s[P] \succ s[Q]$ and $R[P] \succ R[Q]$ for any term context $s[\_]$ and proof context $R[\_]$.

Lemma 3. *Suppose $(\emptyset, \emptyset, R) \vdash (\emptyset, \emptyset, R')$. Then, for any two terms s and t, it is the case that $s \rightarrow^{[*]}_{R \cup AC} t$ if, and only if, $s \rightarrow^{[*]}_{R' \cup AC} t$. Furthermore, if π is a ground proof, $s_0 \rightarrow s_1 \rightarrow \cdots \rightarrow s_k$, in $AC \cup R$, then there is a proof π', $s_0 = s'_0 \rightarrow s'_1 \rightarrow \cdots \rightarrow s'_l = s_k$, in $AC \cup R'$ such that $\pi \succeq_{\mathcal{P}} \pi'$.*

Proof. The first part of the lemma, which states that the relation $\rightarrow^{[*]}$ is invariant across the derivation, is easily verified for the transition rule ACC-chaining and deletion3. Consider the ACC-collapse1 rule now. Clearly, the deleted rule $u' \approx v'$ has a proof $u' \leftrightarrow^*_{AC} su \rightarrow_{R'} tu \rightarrow^*_{R'} tv \leftrightarrow^*_{AC} v'$ in the new set R'. For the other direction, we need to show that there is a proof for $u \approx v$ in R. Note that

$$\tfrac{s}{t} = (\tfrac{s_1}{t_1})^{\alpha_1} \cdots (\tfrac{s_n}{t_n})^{\alpha_n} \qquad \tfrac{u'}{v'} = (\tfrac{s_1}{t_1})^{\beta_1} \cdots (\tfrac{s_n}{t_n})^{\beta_n}$$

together imply $\frac{u}{v} = (\frac{s_1}{t_1})^{\beta_1 - \alpha_1} \cdots (\frac{s_n}{t_n})^{\beta_n - \alpha_n}$, and hence the claim follows from Lemma 2 and noting that the equations in the original set E_0 are never deleted by any of the transition rules (because the measure associated with each of those rules is minimal and ACC-collapse1 can delete rules with non-minimal measures only).

For the second part, one needs to check that each equation in $(R - R')$ has a simpler proof in R' for each transition rule application. The only non-trivial case is that of ACC-collapse1. In this case, the deleted equation $su \rightarrow tv$ has a new proof in R' given by $su \rightarrow_{R'} tu \rightarrow_{R'} tv$. The new proof and the old proof have the same term, su, as the first component of their proof complexity. In comparing the second components, without loss of generality, we consider the case when $su \succ tv$. In this case, either $s \succ t$ or $u \succ v$.
(i) In the case when $s \succ t$ *and* $u \succ v$, the old proof step $su \rightarrow tv$ in more complex than (a) the proof steps $su \rightarrow tu$ in the second component, as $su \succ s$ because u can not be e; and (b) the proof step $tu \rightarrow tv$ in the first component, as $su \succ tu$.
(ii) In the case when $s \succ t$ *and* $v \succ u$, the old proof step $su \rightarrow tv$ in more complex than (a) the proof steps $su \rightarrow tu$ in either the second component if $u \neq e$, or the fourth component (as $tv \succ tu$); and (b) the proof step $tu \rightarrow tv$ in the first component, as $su \succ tv$.
(iii) In the case when $t \succ s$ *and* $u \succ v$, the old proof step $su \rightarrow tv$ in more complex than the new proof $su \rightarrow sv \rightarrow tv$ for the same reason as in case (ii).

This completes the proof of the lemma. ∎

Theorem 5 (Soundness). *Suppose $s \approx t \in R_i$, where $(\emptyset, \emptyset, R_i)$ is a state in any derivation starting from state $(\emptyset, \emptyset, R_0)$. Then, $s \rightarrow^{[*]}_{R_0 \cup AC} t$.*

Proof. By induction on the length i of the derivation. The base case is trivial. For the induction step, we use Lemma 3. ∎

Theorem 6 (Completeness). *Let R_0 be a finite set of rules over the signature $\Sigma \cup K$ and let $(\emptyset, \emptyset, R_\infty = F \cup B)$ be the persisting state of a fair derivation starting from $(\emptyset, \emptyset, R_0)$. If $s \rightarrow^{[*]}_{R_0 \cup AC} t$, then there is a proof of the form $s \rightarrow^*_{AC \backslash F^e} \circ \leftrightarrow^*_{AC} \circ \leftarrow^*_{AC \backslash B^{-e}} t$.*

Proof. Fairness implies that all ACC-chaining inferences between rules in R_∞ are contained in the set $\cup_i R_i$. Since the proof ordering is well-founded, for every proof in R_i, there exists a minimal proof π in R_∞. We argue by contradiction that certain proof patterns, like peaks and cliffs, can not occur in the minimal proof π.

(i) *Cliffs.* Since the signature contains exactly one function symbol, we have $\leftrightarrow_{AC} \circ \rightarrow_{AC\backslash R^e_\infty} \subseteq \rightarrow_{AC\backslash R^e_\infty}$. Hence, all cliffs are taken care of by rewriting using extensions.

(ii) *Peaks.* Non-overlap peaks and variable overlap peaks are not possible since all $\rightarrow_{AC\backslash R^e_\infty}$ proof steps are applied at the top. Next suppose that there is a proper overlap[5] $s \rightarrow_{AC\backslash B^e} \circ \rightarrow_{AC\backslash F^e} t$ between rules $s_1 \approx t_1 \in B$ and $s_2 \approx t_2 \in F$.

First consider the case when $[t_1, s_2] = e$. In this case a simpler proof is obtained by commuting the two steps. In the other case, there is a possible *ACC-chaining* inference between the two rules, and hence fairness guarantees that the critical pair is contained in some R_i. Thus, there is a smaller proof in R_i for the above peak. Note that the proof is smaller because the first component of the proof complexity is reduced (as $[t_1, s_2] \neq e$). Using Lemma 3, we may infer that there is a proof π' in R_∞ such that π' is strictly smaller than π, a contradiction.

Now, if $s \rightarrow^{[*]}_{R_0 \cup AC} t$, then there exists a u such that $s \cdot u \rightarrow^*_{R_0 \cup AC} t \cdot u$. The minimal proof in R_∞ can not contain any peaks or cliffs, and hence it can only be of the form, $s \cdot u \rightarrow^*_{AC\backslash F^e} \circ \leftrightarrow^*_{AC} \circ \rightarrow^*_{AC\backslash B^e} t \cdot u$. We need to show there is a proof where $u = e$.

We say that the rules $s \rightarrow t$ and $u \rightarrow v$ *commute* if $[s, v] = [t, u] = e$. Let F_C denote the set of C-rules in F and B_C denote the set of C-rules in B. Let $F_{AC} = F - F_C$ and $B_{AC} = B - B_C$. Let $R_{AC} = F_{AC} \cup B_{AC}$. We next make the following observations about the minimal proof:

(i) If a proof step that uses a F_{AC}-rule (B_{AC}-rule), ρ, is followed by a proof step that uses a F_{AC}-rule (B_{AC}-rule), ρ', then ρ and ρ' commute: If not, then we can reduce the complexity of the proof using the rule deduced by ACC-chaining applied to ρ and ρ'.

(ii) A proof step that uses a F_{AC}-rule, say $s \rightarrow t$, cannot be followed by a proof step that uses a F_C-rule, say $c \rightarrow d$: There are two cases: If $[t, c] = c$, then the rule deduced by ACC-chaining gives a simpler proof. If $[t, c] = e$, then the two proof steps can be commuted to give a smaller proof.

(iii) A proof step that uses a B_{AC}-rule, cannot be preceded by a proof step that uses a B_C-rule: For the same reason as above.

It follows that the proof is of the form

$$s \cdot u \rightarrow^*_{F_C} \circ \rightarrow^*_{AC\backslash F^e_{AC}} \circ \leftrightarrow^*_{AC} \circ \rightarrow^*_{AC\backslash B^e_{AC}} \circ \rightarrow^*_{B_C} t \cdot u.$$

Using an argument similar to (i), we can also claim that all the F_{AC}-rules used in the first half (and the B_{AC}-rules used in the second half) of the above proof

[5] When rules are oriented backwards, as is the case with B-rules, we use the notation $s \rightarrow_{AC\backslash B^e} t$ to denote $t \leftarrow_{AC\backslash B^{-e}} s$.

commute (with each other), for otherwise we could again reduce the first component of the proof complexity by using a suitably deduced rule. Therefore, the proof now is of the following form,

$$\begin{array}{llll} s \cdot u & \rightarrow^*_{F_C} & s_0 s_1 s_2 \cdots s_k \rightarrow^*_{AC \backslash F^e_{AC}} & s_0 t_1 t_2 \cdots t_k \leftrightarrow^*_{AC} u_0 u_1 u_2 \cdots u_l \\ u_0 u_1 u_2 \cdots u_l & \rightarrow^*_{AC \backslash B^e_{AC}} & u_0 v_1 v_2 \cdots v_l \rightarrow^*_{B_C} & t \cdot u, \end{array}$$

where $s_i \rightarrow t_i \in F_{AC}$ for $i = 1, \ldots, k$, $u_i \rightarrow v_i \in B_{AC}$ for $i = 1, \ldots, l$, $[s_i, t_j] = e$ for $1 \leq i, j \leq k$ and $[u_i, v_j] = e$ for $1 \leq i, j \leq l$. We next claim that $[s_i, v_j] = e$ for $1 \leq i \leq k, 1 \leq j \leq l$. If not, then we can get a smaller proof using the rule deduced by considering the peak $s_i u_j \rightarrow_{B_{AC}} s_i v_j \rightarrow_{F_{AC}} t_i v_j$.

Amongst all possible proofs, let the above proof be the one that minimizes u and the proof complexity. We show by contradiction that either $u = e$ or we can reduce the proof complexity of the above proof. Assume without loss of generality that u is a constant. Now, if $u \neq e$, then there are subproofs $u \rightarrow^*_{E_C \cup F_C} c$ and $d \rightarrow^*_{E_C \cup F_C} u$ for some c and d in the above proof. If $u = c = d$, then we can "cancel" u throughout the proof as u would be left unchanged by the R_{AC}-rules, and we are left with a proof of $s \rightarrow^*_F \circ \leftrightarrow^*_{AC} \circ \rightarrow^*_B t$. If $u \neq c$ and $u = d$, then let $u \rightarrow u_1$ be a C-rule used in the above proof. Now, u is either produced by a B_{AC}-rule, or by a F_{AC}-rule. In either case, we can get a proof for $u_1 \cdot s \rightarrow^*_{R_\infty} u_1 \cdot t$, and clearly $u \succ u_1$, a contradiction. The other case, $u = c$ and $u \neq d$, is symmetric. Finally, in the case when $u \neq c$ and $u \neq d$, let $u \rightarrow u_1$ and $u_2 \rightarrow u$ be the C-rules used in the above proof. By using the critical pair $u_2 \rightarrow u_1$, we can obtain a proof of $u_1 \cdot s \rightarrow^*_{R_\infty \cup AC} u_1 \cdot t$, a contradiction.

The minimal proof π in $R_\infty \cup AC$ can, therefore, only be of the form $s \rightarrow^*_{AC \backslash F^e}$ $s' \leftrightarrow^*_{AC} \circ \rightarrow^*_{AC \backslash B^e} t$; which is the desired form. ■

6.1 Combining with Equations

Next assume that the E-component contains D-rules, C-rules, and A-rules (over the signature $\Sigma \cup K$ as before). In this case, we need (i) a ACC-superposition inference rule to take care of the additional critical pairs between rules in the E-component; and (ii) a ACC-paramodulation rule to deal with critical pairs between rules in E and rules in R.

ACC-Superposition: $$\frac{(I, E \cup \{s \rightarrow t, u \rightarrow v\}, R)}{(I, E \cup \{s \rightarrow t, u \rightarrow v, s' \rightarrow t'\}, R)}$$

if either (i) $[s, u] \neq e$, $s' = tu/([s, u][t, v])$, $t' = sv/([s, u][t, v])$, and $s' \succ t'$; or (ii) $[t, u] \neq e$, $s' = su/([t, u][s, v])$, and $t' = tv/([t, u][s, v])$.

Definition 5. *Let E and R be sets of A-rules, D-rules and C-rules (over the signature $\Sigma \cup K$). If ρ is the rule $s \to t \in E$ and ρ' is the rule $u \to v \in R$, then*

$$
CP^1_{AC}(\rho, \rho') = \begin{cases} \frac{su}{[t,u][s,v]} \to \frac{tv}{[t,u][s,v]} & \texttt{if } (v \succ u \textit{ and } [v,s] \neq e) \textit{ or} \\ & (u \succ v, [t,u] \neq e, \textit{ and } s,t \notin K) \textit{ or} \\ & (u \succ v, [v,s] \neq e, \textit{ and } u,v \notin K) \end{cases}
$$

$$
CP^2_{AC}(\rho, \rho') = \begin{cases} \frac{tu}{[s,u][t,v]} \to \frac{sv}{[s,u][t,v]} & \texttt{if } (u \succ v \textit{ and } [u,s] \neq e) \textit{ or} \\ & (v \succ u, [t,v] \neq e, \textit{ and } s,t \notin K) \textit{ or} \\ & (v \succ u, [u,s] \neq e, \textit{ and } u,v \notin K) \end{cases}
$$

The set $CP_{AC}(E,R)$ is defined as the union of $CP^1_{AC}(\rho,\rho')$ and $CP^2_{AC}(\rho,\rho')$ for every $\rho \in E$ and $\rho' \in R$. Each rule in $CP_{AC}(E,R)$ is assigned a measure equal to the measure of the participating R-rule $u \to v$.

ACC-Paramodulation: $$\frac{(I,E,R)}{(I,E,R \cup \{s \to t\})}$$

if $s \to t \in CP_{AC}(E,R)$.

We need additional collapse rules to handle equations. First we modify the ACC-collapse1 rule.

ACC-Collapse1: $$\frac{(I,E,R \cup \{su \to tv\})}{(I,E,R \cup \{u \to v\})}$$

if either (i) $s \to t \in E$ or $t \to s \in E$, in which case the new rule is assigned a measure equal to that of $su \to tv$; or, (ii) $s \to t \in R$, the measure $\boldsymbol{\beta}$ associated with $su \to tv$ is larger (component-wise) than the measure $\boldsymbol{\alpha}$ associated with $s \to t$, and $\boldsymbol{\beta} - \boldsymbol{\alpha} \neq \mathbf{0}$. The new rule $u \to v$ is assigned the measure $\boldsymbol{\beta} - \boldsymbol{\alpha}$. If $\boldsymbol{\beta} = \boldsymbol{\alpha}$ then we delete the rule $u \to v$ as well.

ACC-Collapse2: $$\frac{(I,E \cup \{s \to t, su \to tv\},R)}{(I,E \cup \{s \to t, u' \to v'\},R)}$$

if either (i) $u \succ v$, $u' = u$, and $v' = v$; or (ii) $v \succ u$, $u' = v$, and $v' = u$.

The set of inference rules consisting of ACC-chaining, deletion3, ACC-superposition, ACC-paramodulation, ACC-collapse1, and ACC-collapse2 can now be used to "complete" a set of A-rules, C-rules, and D-rules over the signature $\Sigma \cup K$. Denote by $\vdash_{ACC}$ the one-step transition relation induced by this set of rules on states.

Correctness

We shall assume that E_0 and R_0 are finite sets of ground rules over the signature $\Sigma \cup K$ such that for every rule $s \to t \in E_0$, it is the case that $s \succ t$.

We can suitably generalize the results of the previous section.

Theorem 7. *Let $E_0 \cup R_0$ be as above. The set $E_\infty \cup R_\infty$ of persisting rules in any fair ACC-derivation starting from the state $(\emptyset, E_0, R_0)$ is finite.*

Proof. Finiteness of the set R_∞ follows from Theorem 4. The argument for showing that E_∞ is finite is identical. ■

We use the same proof ordering as before, but extend it to deal with rules in the set E as follows: If $s = s_0 s' \rightarrow_{AC\backslash E^{\pm e}} t_0 s' = t$ is a proof step using the rule $s_0 \rightarrow t_0 \in E^{\pm}$, then the complexity of this proof step is defined by

$$\begin{array}{ll} (\{s_0 s'\}, s_0, \perp, t_0 s') & \texttt{if} \;\; s_0 \rightarrow t_0 \in E, \\ (\{t_0 s'\}, t_0, \perp, s_0 s') & \texttt{if} \;\; s_0 \rightarrow t_0 \in E^-. \end{array}$$

The complexity of a proof and the ordering $\succ_P$ is defined in the same way.

First we need a generalization of the technical lemma from before.

Lemma 4. *Let $(\emptyset, E_0, R_0) \vdash_{ACC} (\emptyset, E_1, R_1) \vdash_{ACC} \cdots$ be a derivation. Then, if the measure of a rule $s \rightarrow t \in R_j$ is $\boldsymbol{\alpha}$, and $s_i \rightarrow t_i, i = 1, \ldots, k$ are rules in R_j with measures $\boldsymbol{\varepsilon_i}, i = 1, \ldots, k$, then*

$$s t_1^{\alpha_1} t_2^{\alpha_2} \cdots t_k^{\alpha_k} \leftrightarrow^{[*]}_{E_j \cup AC} t s_1^{\alpha_1} s_2^{\alpha_2} \cdots s_k^{\alpha_k}.$$

(If there is no rule with measure $\boldsymbol{\varepsilon_i}$ for some i, then we set $s_i = t_i = e$ in the above.)

Proof. By induction on the length j of the derivation. It is trivially true when $j = 0$. Next assume that $(\emptyset, E_j, R_j) \vdash_{ACC} (\emptyset, E_{j+1}, R_{j+1})$. We prove the claim for each possible inference rule. For inference rules deletion3, ACC-collapse1, and ACC-superposition the claim is easily verified. In case of ACC-chaining, suppose $s \rightarrow t$ (measure $\boldsymbol{\alpha}$) and $u \rightarrow v$ (measure $\boldsymbol{\beta}$) are used to generate the derived rule with measure $\boldsymbol{\alpha} + \boldsymbol{\beta}$. Let s_i, t_i be as in the statement of the lemma. By induction hypothesis, we have

$$\begin{array}{l} s t_1^{\alpha_1} t_2^{\alpha_2} \cdots t_k^{\alpha_k} \leftrightarrow^{[*]}_{E_j \cup AC} t s_1^{\alpha_1} s_2^{\alpha_2} \cdots s_k^{\alpha_k} \\ u t_1^{\beta_1} t_2^{\beta_2} \cdots t_k^{\beta_k} \leftrightarrow^{[*]}_{E_j \cup AC} v s_1^{\beta_1} s_2^{\beta_2} \cdots s_k^{\beta_k} \end{array}$$

and it therefore follows that,

$$\begin{array}{rl} s u t_1^{\alpha_1+\beta_1} t_2^{\alpha_2+\beta_2} \cdots t_k^{\alpha_k+\beta_k} & \leftrightarrow^{[*]}_{E_j \cup AC} t v s_1^{\alpha_1+\beta_1} s_2^{\alpha_2+\beta_2} \cdots s_k^{\alpha_k+\beta_k} \\ \frac{su}{[s,v][t,u]} t_1^{\alpha_1+\beta_1} t_2^{\alpha_2+\beta_2} \cdots t_k^{\alpha_k+\beta_k} & \leftrightarrow^{[*]}_{E_j \cup AC} \frac{tv}{[s,v][t,u]} s_1^{\alpha_1+\beta_1} s_2^{\alpha_2+\beta_2} \cdots s_k^{\alpha_k+\beta_k}. \end{array}$$

The proof is completed by noting that $E_j \subseteq E_{j+1}$.

In case of ACC-paramodulation, suppose $s \rightarrow t \in E_j$ and $u \rightarrow v \in R_j$ (measure $\boldsymbol{\alpha}$) are used to generate the derived rule with measure $\boldsymbol{\alpha}$. Let s_i, t_i be as in the statement of the lemma. By induction hypothesis, we have

$$u t_1^{\alpha_1} t_2^{\alpha_2} \cdots t_k^{\alpha_k} \leftrightarrow^{[*]}_{E_j \cup AC} v s_1^{\alpha_1} s_2^{\alpha_2} \cdots s_k^{\alpha_k}$$

and it therefore follows that,

$$\begin{array}{llll} sut_1^{\alpha_1}t_2^{\alpha_2}\cdots t_k^{\alpha_k} & \leftrightarrow^{[*]}_{E_j\cup AC} tut_1^{\alpha_1}t_2^{\alpha_2}\cdots t_k^{\alpha_k} & \leftrightarrow^{[*]}_{E_j\cup AC} tvs_1^{\alpha_1}s_2^{\alpha_2}\cdots s_k^{\alpha_k} \\ \frac{su}{[s,v][t,u]}t_1^{\alpha_1}t_2^{\alpha_2}\cdots t_k^{\alpha_k} & \leftrightarrow^{[*]}_{E_j\cup AC} \frac{tv}{[s,v][t,u]}s_1^{\alpha_1}s_2^{\alpha_2}\cdots s_k^{\alpha_k}. & \end{array}$$

Finally, the case of inference rule ACC-collapse2 is similar to ACC-chaining and ACC-paramodulation. ■

Lemma 5. *Suppose* $(\emptyset, E_0, R_0) \vdash_{ACC} (\emptyset, E_1, R_1)$. *Then, for any two terms* s *and* t, *it is the case that* $s \to^{[*]}_{E_0^{\pm}\cup R_0\cup AC} t$ *if, and only if,* $s \to^{[*]}_{E_1^{\pm}\cup R_1\cup AC} t$. *Furthermore, if* π *is a ground proof,* $s_0 \to s_1 \to \cdots \to s_k$, *in* $AC \cup E_0^{\pm} \cup R_0$, *then there is a proof* π', $s_0 = s'_0 \to s'_1 \to \cdots \to s'_l = s_k$, *in* $AC \cup E_1^{\pm} \cup R_1$ *such that* $\pi \succeq_{\mathcal{P}} \pi'$.

Proof. The first part of the lemma, which states that the relation $\to^{[*]}$ is invariant across the derivation, is easily verified for the transition rule ACC-chaining, deletion3, ACC-superposition and ACC-paramodulation. In the case of ACC-collapse2, it is clear that the new rule $u \to_{E_1^{\pm}} v$ has a proof $su \to_{E_0} tv \to_{E_0^-} sv$, which shows that $u \to^{[*]}_{E_0} v$. It is clear that the deleted rule $su \to tv$ has a proof in $E_1^{\pm}$. The first part of the claim for ACC-collapse1 inference rule follows from Lemma 4.

For the second part, we prove, using arguments identical to the one for ACC-collapse1 in Lemma 3, that the rule deleted by ACC-collapse2 has a smaller proof. In the new version of ACC-collapse1, we have a new case where a rule $su \to tv$ in R is collapsed using a rule (wlog) $s \to t$ in E. The new proof $su \to_E tu \to_R tv$ is simpler. This is because the first component of the proof complexity is identical, and in the second component the complexity of the proof step $su \to tv$ is larger than (a) the complexity of $su \to_E tu$ either in the first component (if $tv \succ su$), or in the second component (if $su \succ tv$ and $u \neq e$) or in the third component (if $su \succ tv$ and $u = e$); (b) the complexity of the $tu \to tv$ in either the first component (if $su \succ tv$), or in the second component (if $tv \succ su$ and $t \neq e$) or in the fourth component (if $tv \succ su$ and $t = e$). ■

Theorem 8 (Soundness). *Suppose* $s \approx t \in E_i^{\pm} \cup R_i$, *where* $(\emptyset, E_i, R_i)$ *is a state in any derivation starting from state* $(\emptyset, E_0, R_0)$. *Then,* $s \to^{[*]}_{E_0^{\pm}\cup R_0\cup AC} t$.

Proof. By induction on the length i of the derivation. The base case is trivial. For the induction step, we use Lemma 5. ■

Theorem 9 (Completeness). *Let* $E_0 \cup R_0$ *be a finite set of rules over the signature* $\Sigma \cup K$ *and let* $(\emptyset, E_\infty, R_\infty = F \cup B)$ *be the persisting state of a fair derivation starting from* $(\emptyset, E_0, R_0)$. *If* $s \to^{[*]}_{E_0^{\pm}\cup R_0\cup AC} t$, *then there is a proof of the form* $s \to^*_{AC\setminus E^e_\infty \cup F^e} \circ \leftrightarrow^*_{AC} \circ \leftarrow^*_{AC\setminus E_\infty{}^e\cup B^{-e}} t$.

The proof for this is identical to the earlier proof. We only need reason about more cases now, but using similar arguments as before.

7 The General Case

We combine the inference rules for the individual cancellative AC symbols and the inference rules for uninterpreted ground terms to get a procedure for constructing a rewrite closure for a set of equations and rules over a signature containing cancellative associative commutative function symbols. There are a few technical difficulties here however. First, in the case of a monoid, the length of the measure vector assigned to a rule was determined by the number of rules in the initial R-component, R_0. In the general case, these rules are created by orientation and moved from the I-component to the R-component. Secondly, in the case of a monoid, all the C-rules in the R-component had exactly one measure vector associated with them. In case of a signature with $|\Sigma_{AC}|$ associative commutative function symbols, each C-rule will have a measure vector associated with it for each $f \in \Sigma_{AC}$. Finally, we need an AC-compatible ordering that orients the D-rules in the right way. For this purpose, we use the ordering $\succ$ defined in [27]. When comparing two terms from a monoid, it orients them in the same way as a total degree lexicographic ordering would.

For purposes of explanation, we partition the set E and R into disjoint subsets.

$$
\begin{array}{ll}
E_C = \{c \to d \in E : c, d \in K\} & E_f = \{s \to t \in E : top(s) = f\} \\
E_{AC} = \cup_{f \in \Sigma_{AC}} E_f & E_D = E - E_C - E_{AC}
\end{array}
$$

Inference Rules

We give the combined set of inference rules for the general case.

Extension: $$\frac{(I[s], E, R)}{(I[c], E \cup \{s \to c\}, R)}$$

if $s \to c$ is a D-rule and c is a new constant.

Simplification1: $$\frac{(I[s], E, R)}{(I[t], E, R)}$$

if $s \to_{AC \backslash E^e} t$.

Orientation1: $$\frac{(I \cup \{s \approx t\}, E, R)}{(I, E \cup \{s \to t\}, R)}$$

if $s \to t$ is either a D-rule, or a C-rule, or a A-rule, and $s \succ t$.

Orientation2: $$\frac{(I \cup \{s > t\}, E, R)}{(I, E, R \cup \{s \to t\})}$$

if $s \to t$ is either a (reverse) D-rule, or a C-rule, or a A-rule. If either $top(s)$ or $top(t)$ is an associative commutative function symbol f, then the length of the f-measure vector is incremented by one: the rule $s \to t$ is assigned a f-measure $\langle 0, 0, \ldots, 0, 1\rangle$, and the f-measure of all other rules (wherever defined) is appended by a zero. If $s \to t$ is a C-rule, then the length of f-measure vector, for all $f \in \Sigma_{AC}$ is incremented: the C-rule $s \to t$ is assigned a f-measure $\langle 0, 0, \ldots, 0, 1\rangle$ and the f-measure of all other rules (wherever defined) is appended by a zero.

Deletion1: $$\frac{(I \cup \{s \approx t\}, E, R)}{(I, E, R)}$$

if $s \leftrightarrow^*_{AC} t$.

Deletion2: $$\frac{(I \cup \{s > t\}, E, R)}{(I, E, R)}$$

if $s \leftrightarrow^*_{AC} t$.

Deletion3: $$\frac{(I, E, R \cup \{s \to t\})}{(I, E, R)}$$

if $s \leftrightarrow^*_{AC} t$.

Superposition: $$\frac{(I, E \cup \{t \to c, s[t] \to u\}, R)}{(I, E \cup \{t \to c, l \to r\}, R)}$$

if $top(t) \notin \Sigma_{AC}$ and either (i) $s[t] \neq t$, $l = max(s[c], u)$, and $r = min(s[c], u)$; or, (ii) $s[t] = t$, $u \succ c$, $l = u$, and $r = c$.

Composition: $$\frac{(I, E \cup \{t \to c, u \to s[t]\}, R)}{(I, E \cup \{t \to c, u \to s[c]\}, R)}$$

if $top(t) \notin \Sigma_{AC}$.

SimplificationL: $$\frac{(I, E \cup \{t \to c\}, R \cup \{s[t] \to u\})}{(I, E \cup \{t \to c\}, R \cup \{s[c] \to u\})}$$

if $top(t) \notin \Sigma_{AC}$. The rule $s[c] \to u$ inherits its measure from $s[t] \to u$.

SimplificationR: $$\frac{(I, E \cup \{t \to c\}, R \cup \{u \to s[t]\})}{(I, E \cup \{t \to c\}, R \cup \{u \to s[c]\})}$$

if $top(t) \notin \Sigma_{AC}$. The rule $u \to s[c]$ inherits its measure from $u \to s[t]$.

Chaining: $$\frac{(I, E, R)}{(I, E, R \cup \{s \to t\})}$$

if $s \to t \in CP(R_D \cup R_C)$.

Paramodulation: $$\frac{(I, E, R)}{(I, E, R \cup \{s \to t\})}$$

if $s \to t \in CP(E_D, R_D)$.

ACC-Chaining: $$\frac{(I, E, R \cup \{s \to t, u \to v\})}{(I, E, R \cup \{s \to t, u \to v, \frac{su}{[s,v][t,u]} \to \frac{tv}{[s,v][t,u]}\})}$$

if $s \to t \in R_{AC} \cup R_C$, $u \to v \in R_{AC} \cup R_C$, $[t, u] \neq e$ and either (i) $t \succ s$ and $u \succ v$; or (ii) $s \succ t$, $u \succ v$, and $s \to t \notin R_C$; or (iii) $t \succ s$, $v \succ u$, and $u \to v \notin R_C$. The new rule is assigned the measure $\boldsymbol{\alpha} + \boldsymbol{\beta}$, where $\boldsymbol{\alpha}$ is the measure associated with the rule $s \to t$ and $\boldsymbol{\beta}$ is the measure associated with the rule $u \to v$.

ACC-Superposition: $$\frac{(I, E \cup \{s \to t, u \to v\}, R)}{(I, E \cup \{s \to t, u \to v, s' \to t'\}, R)}$$

if $s \to t \in E_{AC} \cup E_C$, $u \to v \in E_{AC} \cup E_C$, either (i) $[s,u] \neq e$, $s' = tu/([s,u][t,v])$, $t' = sv/([s,u][t,v])$, and $s' \succ t'$; or (ii) $[t,u] \neq e$, $s \to t \notin R_C$. $s' = su/([t,u][s,v])$, and $t' = tv/([t,u][s,v])$.

ACC-Paramodulation: $$\frac{(I, E, R)}{(I, E, R \cup \{s \to t\})}$$

if $s \to t \in CP_{AC}(E_C \cup E_{AC}, R_C \cup R_{AC})$.

ACC-Collapse1: $$\frac{(I, E, R \cup \{su \to tv\})}{(I, E, R \cup \{u \to v\})}$$

if $su \to tv \in R_{AC}$ and either (i) $s \to t \in E$ or $t \to s \in E$, in which case the new rule is assigned a measure equal to that of $su \to tv$; or, (ii) $s \to t \in R$, the measure $\boldsymbol{\beta}$ associated with $su \to tv$ is larger (component-wise) than the measure $\boldsymbol{\alpha}$ associated with $s \to t$, and $\boldsymbol{\beta} - \boldsymbol{\alpha} \neq \mathbf{0}$, in which case the new rule $u \to v$ is assigned the measure $\boldsymbol{\beta} - \boldsymbol{\alpha}$. If $\boldsymbol{\beta} = \boldsymbol{\alpha}$ then we delete the rule $u \to v$ as well.

ACC-Collapse2: $$\frac{(I, E \cup \{s \to t, su \to tv\}, R)}{(I, E \cup \{s \to t, u \to v\}, R)}$$

if $su \to tv \in E_{AC}$.

We can prove finiteness of the set of persisting equations and rules in the same way.

Theorem 10. *Let I_0 be a finite set of ground equations and inequations over a signature possibly containing cancellative associative commutative function symbols. The set $E_\infty \cup R_\infty$ of persisting rules in any fair derivation starting from the state $(I_0, \emptyset, \emptyset)$ is finite.*

Since each individual application of the inference rule is sound, we get soundness of the set of all inference rules.

Theorem 11 (Soundness). *Suppose $s \approx t \in R_i$, where (I_i, E_i, R_i) is a state in any derivation starting from state $(I_0, \emptyset, \emptyset)$. Then, $s \rightarrow^{[*]}_{\mathbb{E}_0^{\pm} \cup \mathbb{R}_0} t$.*

We can define the proof complexity by putting together the proof complexities for individual monoids and for the case of uninterpreted symbols. Let $s = s[u\sigma] \rightarrow s[v\sigma] = t$ be a proof step using the equation (rule) $u \approx u \in AC \cup I \cup E^e \cup R^e$. The complexity of this proof step is defined by

$$
\begin{array}{rll@{\qquad}rll}
(\{s,t\}, \bot, \bot, \bot) & \texttt{if} & u \approx v \in I & (\{s,t\}, \bot, \bot, \bot) & \texttt{if} & u > v \in I \\
(\{s\}, u, \bot, t) & \texttt{if} & u \rightarrow v \in E & (\{t\}, v, \bot, s) & \texttt{if} & u \rightarrow v \in E^{-1} \\
(\{s\}, u, \top, t) & \texttt{if} & u \rightarrow v \in R, u \succ v & (\{t\}, v, \top, s) & \texttt{if} & u \rightarrow v \in R, v \succ u \\
(\{s\}, \bot, \bot, \bot) & \texttt{if} & u \approx v \in AC & & &
\end{array}
$$

where $\bot$ and $\top$ are new constant symbols assumed to be minimum and maximum respectively. Tuples are compared are before.

The complexity of a proof is a tuple consisting of (i) the multiset of complexities of the $\approx$ and $>$ proof steps in the first component, (ii) for each function symbol $f \in \Sigma_{AC}$, the product of left-hand sides of all $E_f \cup R_f$ rules used in the proof, and (iii) the multiset of complexities of all the proof steps in the last component. Thus, the complexity of a proof is a $|\Sigma_{AC}| + 2$-tuple. Proof complexities are compared using a lexicographic combination of the multiset extension of the ordering on proof steps in the first and last component and the ordering $\succ$ on terms in the intermediate components. This ordering on proofs can be verified to be a proof ordering, which we denote by $\succ_P$. The ordering $\succ_P$ is well-founded as it is a lexicographic combination of well-founded orderings.

By putting together the proof simplification arguments of the constituent parts, we can establish the following.

Lemma 6. *Let $I = \mathbb{E} \cup \mathbb{R}$ be a finite set of equations and inequations and let $(\emptyset, E, R = F \cup B)$ be the persisting state of a fair derivation starting from $(I, \emptyset, \emptyset)$. If $s \rightarrow^*_{\mathbb{E}^{\pm} \cup \mathbb{R} \cup AC} t$, then then there is a proof of the form $s \rightarrow^*_{AC \backslash F^e \cup E^e} \circ \leftrightarrow^*_{AC} \circ \leftarrow^*_{AC \backslash B^{-e} \cup E^e} t$.*

Theorem 12 (Completeness). *Let I_0 be a finite set of equations and inequations over a signature containing cancellative associative commutative symbols. Let $(\emptyset, E, R = F \cup B)$ be the persisting state of a fair derivation starting from $(I_0, \emptyset, \emptyset)$. If we can prove $v \rightarrow w$ using I_0 and the axioms for cancellative monoids, then there is a proof of the form $v \rightarrow^*_{AC \backslash F^e \cup E^e} \circ \leftrightarrow^*_{AC} \circ \leftarrow^*_{AC \backslash B^{-e} \cup E^e} w$.*

Proof. Using Lemma 1, Lemma 3, and Lemma 5, we know that there is a proof of $v \rightarrow w$ using $E \cup R$ and the cancellative monoid axioms. We shall show that there is a proof $v \rightarrow^*_{E^{\pm} \cup R \cup AC} w$ and the claim would then follow from Lemma 6.

If not, then there is a proof of $v \rightarrow w$ that uses as subproofs equations and rules derived using the cancellation axioms. Let $s \rightarrow t$ be a derived rule such that its proof uses exactly one application of the cancellation axiom. Therefore, we have $u \cdot s \rightarrow^*_{E^{\pm} \cup R \cup AC} u \cdot t$, where u, s and t are arbitrary terms. But now, there is a proof $u \cdot s \rightarrow^*_{E \cup F} \circ \leftrightarrow^*_{AC} \circ \rightarrow^*_{E^- \cup B} u \cdot t$. Now, let

$$
\begin{aligned}
s &= c_1 c_2 \ldots c_? p_1 p_2 \ldots p_? \\
t &= d_1 d_2 \ldots d_? q_1 q_2 \ldots q_? \\
u &= u_1 u_2 \ldots u_? r_1 r_2 \ldots r_?
\end{aligned}
$$

where p_i, q_i and r_i are the subterms of s, t and u respectively that are not headed with $\cdot$ and c_i, d_i and u_i are constants from K. Note that the rewriting step that are applicable to $u \cdot t$ at the top (i.e. using some $E_{AC} \cup R_{AC}$-rule headed with AC symbol $\cdot$) overlap with other rules that are applicable on q_i's only at the (extended) variable position. If some p_i, q_i or r_i is not completely collapsed to a constant in K, then we can remove the corresponding p_i, q_i pair or the r_i and retain the rest of the proof. If they are completely collapsed, then we replace them with the constants from K they are collapsed into. Thus, finally we have a proof of the form of Theorem 6 or Theorem 9, and hence there is a proof that does not use the cancellation axioms. ∎

Other Remarks

The equational theory induced by a set of ground equations over a signature containing AC (no cancellative axiom) symbols can be conservatively represented by D-rules, C-rules, and A-rules [7]. But, if we are interested in the rewrite relation, then the problem becomes much harder, as classical petrinet reachability is equivalent to the decidability of the rewrite relation induced by a set of ground rules over a signature consisting of exactly one AC function symbol and a finite number of constants. As is expected, a derivation using the the inference rules presented here does not converge in the case of abelian semigroups. For instance, consider the a petrinet with two states, c_1 and c_2 and two transitions $c_1^4 c_2 \rightarrow c_1 c_2^2$ and $c_1^4 c_2 \rightarrow c_1^3 c_2^2$. ACC-Chaining inferences (assume a total degree lexicographic ordering with $c_1 \succ c_2$) yield new rules $c_1^5 c_2 \rightarrow c_1 c_2^3$, $c_1^6 c_2 \rightarrow c_1 c_2^4, \cdots, c_1^n c_2 \rightarrow c_1 c_2^{n-2}$.

The problem of deciding reachability in the case of a cancellative monoid is related to solving a system of linear diophantine equations by "duality". Consider the system $\{4x_1 - x_2 - 2x_3 = 0, 3x_1 - 4x_2 + 5x_3 = 0\}$. Since there are two equations, we introduce two constants, say c_1 and c_2. Now, the above system can be transformed into the three rewrite rules $c_1^4 c_2^3 \rightarrow e$, $e \rightarrow c_1 c_2^4$, and $c_2^5 \rightarrow c_1^2$. Now, note that the original system has a non-trivial solution if and only if $e \rightarrow^+ e$. The converse translation can be similarly done. This connection is not surprising since one motivation for considering the cancellative axiom for AC-symbols comes from AC unification and linear diophantine equations arise naturally in that context.

8 Conclusion

We have presented a set of inference rules, derived from standard completion and asymmetric completion, to construct a rewrite closure for a set of ground equations and rules over a signature that can possibly contain cancellative AC symbols. The procedure works over an extended signature, incorporates essential simplifications, and is terminating.

There are several directions in which we envisage future work. The inference rules can be extended by including new rules for special kinds of rewrite relations, like lexicographic path orderings, or recursive path orderings, and for unification. This would give abstract transformation rules for constraint solving. Another possible extension is to (obtain decision procedures for) ordered fields. In this context, the asymmetric relation will be interpreted as the ordering relation $>$ on the field elements. This work can also be extended along the lines of tree automata techniques and be used to obtain *efficient* decision procedures for several kinds of rewrite systems.

Different subsets of the set of equality axioms have been considered and various specialized inference rules have been proposed in the literature to eliminate the need to use the original axioms, thus reducing the search space significantly, in a theorem proving system. The paramodulation rule [26] and its restricted forms like superposition handle the congruence relation. Bachmair and Ganzinger [5, 6] have outlined a complete inference system based on ordered chaining to handle transitivity. They also point out how to handle a symmetric and transitive relation. Manna and Waldinger [20] give a set of inference rules that can handle any specified combination of monotonicity, anti-monotonicity, transitivity and symmetry. However, they showed that their system is not complete. Bachmair and Ganzinger [5] also point out some difficulties with dealing with transitive and monotone relations using a chaining calculus. Ordered chaining based calculi for dealing with total orderings is discussed in Bachmair and Ganzinger [4]. Levy and Agusti [19] introduced the notion of extended critical pairs to deal with transitive and monotone relations. Unfortunately, the number of extended critical pairs is usually infinite, and hence this is not very useful in general (though they show some success for a specific inclusion theory of non-distributive lattices). Bledsoe and Hines [12] give a set of inference rules to deal with the theory of dense total orderings with no endpoints over a signature enhanced with uninterpreted function symbols. A later paper [13] established that this system is sound and refutationally complete. Bachmair et. al. [8] considered the rewrite closure of a relation specified over the free term algebra. However, the interest in [8] was in finding a normal form for a given *initial term* and the proposed completion based method works for relations that satisfy certain additional conditions.

Though the work presented in this paper is similar in spirit to the aforementioned results, our work is orthogonal to the above results. We considered here a specific theory, that of commutative semigroups, and a monotone and transitive relation which also satisfies an additional inverse monotonicity axiom. This is a first step towards incorporating *non-linear* terms to inequality reasoning in the framework of specialized inference rules alluded to above. One important difference with other work is that our interest is in *decision procedures* and not just sound and refutationally complete inference systems. Having a good base of cooperating decision procedures as the back end of a prover helps tremendously in improving its utility [28]. One drawback of the inference system we presented is the lack of ordering restrictions on the chaining rule. Such restrictions are crucial for efficiency, but we need unrestricted chaining in order to prove Theorem 6.

References

[1] L. Bachmair. *Canonical Equational Proofs.* Birkhäuser, Boston, 1991.

[2] L. Bachmair and N. Dershowitz. Completion for rewriting modulo a congruence. *Theoretical Computer Science*, 67(2 & 3):173–201, October 1989.

[3] L. Bachmair and N. Dershowitz. Equational inference, canonical proofs, and proof orderings. *Journal of the ACM*, 41:236–276, 1994.

[4] L. Bachmair and H. Ganzinger. Ordered chaining for total orderings. In Alan Bundy, editor, *Proceedings of the 12th International Conference on Computer Aided Deduction*, pages 435–450, 1994. Vol. 814 of *Lecture Notes in Artificial Intelligence*, Springer, Berlin.

[5] L. Bachmair and H. Ganzinger. Rewrite techniques for transitive relations. In *9th Annual IEEE Symposium on Logic in Computer Science*, pages 384–393, 1994.

[6] L. Bachmair and H. Ganzinger. *Ordered chaining calculi for first-order theories of binary relations.* Technical Report MPI-I-95-2-009, 1995.

[7] L. Bachmair, I.V.Ramakrishnan, A. Tiwari, and L. Vigneron. Congruence closure modulo associativity and commutativity. In H. Kirchner and C. Ringeissen, editors, *Frontiers of Combining Systems, 3rd Intl Workshop FroCoS 2000*, volume 1794 of *Lecture Notes in Artificial Intelligence*, pages 245–259, Nancy, France, March 2000. Springer-Verlag.

[8] L. Bachmair, C.R. Ramakrishnan, I.V.Ramakrishnan, and A. Tiwari. Normalization via rewrite closures. In P. Narendran and M. Rusinowitch, editors, *Rewriting Techniques and Applications, RTA 1999*, volume 1631 of *Lecture Notes in Computer Science*, pages 190–204, Trento, Italy, July 1999. Springer-Verlag.

[9] Leo Bachmair and Ashish Tiwari. Abstract congruence closure and specializations. In David McAllester, editor, *Conference on Automated Deduction, CADE '2000*, volume 1831 of *Lecture Notes in Artificial Intelligence*, pages 64–78, Pittsburgh, PA, June 2000. Springer-Verlag.

[10] Leo Bachmair, Ashish Tiwari, and Laurent Vigneron. Abstract congruence closure. In *J. of Automated Reasoning*, 2001. Submitted for publication.

[11] T. Becker and V. Weispfenning. *Gröbner bases: a computational approach to commutative algebra.* Springer-Verlag, Berlin, 1993.

[12] W. W. Bledsoe and L. M. Hines. Variable elimination and chaining in a resolution-based prover for inequalities. In W. Bibel and R. Kowalski, editors, *Proc. 5th Conf. on Automated Deduction CADE-5*, pages 70–87, Les Arcs, France, 1980. Springer-Verlag, Berlin. LNCS 87.

[13] W. W. Bledsoe, K. Kunen, and R. Shostak. Completeness proofs for inequality provers. *J. of Artificial Intelligence*, 27(3):255–288, 1985.

[14] B. Buchberger. Gröbner bases: An algorithmic method in polynomial ideal theory. In N. K. Bose, editor, *Recent Trends in Multidimensional Systems Theory*, pages 184–232. Reidel, 1985.

[15] H. Comon, M. Dauchet, R. Gilleron, F. Jacquemard, D. Lugiez, S. Tison, and M. Tommasi. Tree automata techniques and applications. Available on: `http://www.grappa.univ-lille3.fr/tata`, 1997.

[16] M. Dauchet, T. Heuillard, P. Lescanne, and S. Tison. Decidability of the confluence of ground term rewriting systems. In *Proc of the IEEE Symposium on Logic in Computer Science*, pages 353–359, Ithaca, NY, June 1987. IEEE Computer Society Press.

[17] M. Dauchet and S. Tison. The theory of ground rewrite systems is decidable. In *Proc of the 5th IEEE Symposium on Logic in Computer Science*, pages 242–248, Philadelphia, PA, June 1990. IEEE Computer Society Press.

[18] J. Esparza and M. Nielsen. Decidability issues for petri nets. *J. Inform. Process. Cybernet EIK*, 30(3):143–160, 1994.

[19] A. Levy and J. Agusti. Bi-rewriting, a term rewriting technique for monotone order relations. In C. Kirchner, editor, *Rewriting Techniques and Applications RTA-93*, pages 17–31, 1993. LNCS 690.

[20] Z. Manna and R. Waldinger. The special-relation rules are incomplete. In D. Kapur, editor, *Automated Deduction CADE-11*, pages 492–506, 1992. LNAI 607.

[21] E. W. Mayr. Persistence of vector replacement systems is decidable. *Acta Informatica 15*, pages 309–318, 1981. NewsletterInfo: 8.

[22] E. W. Mayr and A. R. Meyer. The complexity of the word problems for commutative semigroups and polynomial ideals. *Advances in Mathematics*, 46:305–329, 1982.

[23] M. Oyamaguchi. The church-rosser property for ground term rewriting systems is decidable. *TCS*, 49:43–79, 1987.

[24] D. A. Plaisted. Polynomial time termination and constraint satisfaction tests. In *Rewriting Techniques and Applications, RTA-93*, volume 690 of *Lecture Notes in Computer Science*, pages 405–420, Montreal, Canada, 1993. Springer-Verlag.

[25] S. Rao Kosaraju. Decidability of reachability in vector addition systems. In *Proc. of the fourteenth annual ACM symposium on theory of computing*, pages 267–281, San Francisco, California, May 1982.

[26] G. A. Robinson and L. T. Wos. Paramodulation and theorem proving in first order theories with equality. In B. Meltzer and D. Michie, editors, *Machine Intelligence 4*, pages 133–150, New York, 1969. American Elsevier.

[27] A. Rubio and R. Nieuwenhuis. A precedence-based total AC-compatible ordering. In C. Kirchner, editor, *Proceedings of the 5 Intl. Conference on Rewriting Techniques and Applications*, pages 374–388, 1993. Vol. 690 of *Lecture Notes in Computer Science*, Springer.

[28] N. Shankar, S. Owre, and J. M. Rushby. *The PVS Proof Checker: A Reference Manual.* Computer Science Lab, SRI International, 1993.