COMPLETION FOR REWRITING MODULO A CONGRUENCE *

Leo Bachmair
Department of Computer Science
SUNY at Stony Brook
Stony Brook, New York 11794, U.S.A.

Nachum Dershowitz
Department of Computer Science
University of Illinois at Urbana-Champaign
Urbana, Illinois 61801, U.S.A.

Abstract. We present completion methods for rewriting modulo a congruence, generalizing previous methods by Peterson and Stickel (1981) and Jouannaud and Kirchner (1986). We formalize our methods as equational inference systems and describe techniques for reasoning about such systems.

1. Introduction

Rewrite methods have been applied to a variety of problems in automated deduction, equational programming, and symbolic computation. Unfortunately, standard rewrite techniques such as the Knuth-Bendix completion method are inadequate for many equational theories. For example, using commutativity as a rewrite rule destroys the termination property and causes standard completion to fail. Equational theories comprising such problematic axioms can often be handled by generalizing the basic concepts of rewriting, matching, and unification, defining them with respect to the congruence generated by a given set of equational axioms A . Various methods have been proposed for rewriting modulo a congruence. Lankford and Ballantyne (1977) present Church-Rosser theorems for sets A of permutativity axioms; Peterson and Stickel (1981) describe a completion procedure for associative-commutative rewriting; Jouannaud (1983) and Jouannaud and Kirchner (1986) formulate completion for congruences with finite equivalence classes.

In this paper, we formalize completion for rewriting modulo a congruence as an equational inference system. The individual inference rules represent elementary computation steps of completion. They can be combined in different ways to yield a wide range of completion procedures. We outline techniques for reasoning about such inference systems, adapting the concept of proof ordering (Bachmair, Dershowitz and Hsiang 1986). Correctness proofs based on these techniques are comparatively simple and cover a large class of completion procedures, not just a specific version.

* This research was supported in part by the National Science Foundation under grant DCR 85-13417.

We first present a completion method that can be applied to theories A for which the subterm ordering modulo A is well-founded. This method includes, as a special case, the procedure described by Jouannaud and Kirchner (1986). It is less restrictive, in general, and allows construction of reduced canonical systems, since we do not require the use of protected or extended rules. We also prove a conjecture by Jouannaud and Kirchner (1986) that the assumption of well-foundedness of the A-subsumption ordering is not needed for establishing the correctness of their completion procedure. Furthermore, our results imply the correctness of criteria for deleting redundant critical pairs.

We then present another completion method that generalizes the associative-commutative completion method of Peterson and Stickel (1981) to arbitrary equational theories A. This method is based on the systematic use of extended rules. It imposes no restrictions on A, other than the existence of a finite complete A-unification algorithm. In particular, it can be applied to theories with infinite congruence classes, a case that can not be handled by any other method.

2. Equations and Rewrite Rules

We will consider *terms* over some set of operator symbols F and some set of variables V. We use $s, t, u, \cdots$ to denote terms; $f, g, h, \cdots$ to denote operator symbols; $x, y, z, \cdots$ to denote variables. By t/p we denote the *subterm* of t at position p. We write $s[t]$ to indicate that s contains t as a subterm and (ambiguously) denote by $s[u]$ the result of replacing a particular occurrence of t by u. If necessary, the position p of the replacement may be indicated by writing $s[p/u]$. We write $s[t_1, \ldots, t_n]$ if s contains subterms $t_1, \ldots, t_n$. A subterm of t is called *proper* if it is distinct from t.

By $t\sigma$ we denote the result of applying the substitution σ to t. The term $t\sigma$ is called an *instance* of t. An instance s of t is *proper* if t is not an instance of s. For example, $x+0$ and $x+x$ are proper instances of $x+y$, whereas $x+z$ is not.

A binary relation $\to$ on terms is *monotonic* (with respect to the term structure) if $s \to t$ implies $u[s] \to u[t]$, for all terms s, t and u. It is *stable* (under substitution) if $s \to t$ implies $s\sigma \to t\sigma$, for any substitution σ. The symbols $\to^+$, $\to^*$ and $\leftrightarrow$ denote the transitive, transitive-reflexive, and symmetric closure of $\to$, respectively. A *reduction ordering* is a well-founded ordering that is stable and monotonic.

An *equation* is a pair of terms $s = t$. For any set of equations E, $\leftrightarrow_E$ denotes the smallest stable, monotonic, and symmetric relation that contains E. The relation $\overset{*}{\leftrightarrow}_E$ is the smallest stable congruence that contains E; a congruence is, by definition, monotonic. Directed equations are called *rewrite rules* and are written $s \to t$. A *rewrite system* is a set of rewrite rules. The *reduction relation* $\to_R$ is the smallest stable and monotonic binary relation that contains R.

Let A be a set of equations and R be a rewrite system. The rewrite system R/A (R *mod* A) consists of all rewrite rules $l \to r$ such that $l \overset{*}{\leftrightarrow}_A u \to_R v \overset{*}{\leftrightarrow}_A r$, for some terms u and v. The system $R \cdot A$ consists of all rules $l \to r$ such that $l \overset{*}{\leftrightarrow}_A u\sigma$ and $r \equiv v\sigma$, for some rule $u \to v$ in R and some substitution σ. For example, if A consists of the associativity and commutativity axioms for addition, and R contains rules $-x+x \to 0$ and $f(x,x) \to g(x)$, then $f(x+y, y+x)$ is irreducible in R, but reduces to $g(x+y)$ in $R \cdot A$. The term $-x+(x+y)$ is irreducible in $R \cdot A$, whereas it reduces to $0+y$ in R/A. A rewrite step in $R \cdot A$ corresponds to the application of a rule in R using *A-matching,* i.e. matching with respect to the congruence $\overset{*}{\leftrightarrow}_A$. Thus, we speak of *rewriting modulo a congruence.*

We will study rewrite systems R that are partitioned into two sets L and N, where L contains only left-linear rules, and consider corresponding rewrite relations $R^A \equiv L \cup N \cdot A$. (A rule is left-linear if no variable occurs more than once on its left-hand side.) Thus, $s \rightarrow_{R^A} t$ if and only if $s \rightarrow_L t$ or $s \rightarrow_{N \cdot A} t$. In other words, A-matching is restricted to rules in N.

A reduction ordering $>$ is *compatible* with A if $s > t$ implies $u > v$, for all terms s, t, u, and v with $u \overset{*}{\leftrightarrow}_A s$ and $t \overset{*}{\leftrightarrow}_A v$. Any ordering compatible with A induces an ordering on congruence classes of $\overset{*}{\leftrightarrow}_A$. A system R/A is terminating if and only if there is a reduction ordering $>$ that contains R and is compatible with A. A system R is called *Church-Rosser modulo A* if, for all terms s and t with $s \overset{*}{\leftrightarrow}_{A \cup R} t$, there are terms u and v, such that $s \overset{*}{\rightarrow}_R u \overset{*}{\leftrightarrow}_A v \overset{*}{\leftarrow}_R t$. We say that R is *canonical modulo A* if R/A is terminating and R is Church-Rosser modulo A.

3. Proof Orderings

The concept of proof orderings (Bachmair, Dershowitz, and Hsiang 1986) is the key to our approach to rewriting modulo a congruence.

Let E be a set of equations and R be a rewrite system. A *proof* in $E \cup R$ of an equation $s = t$ is a sequence $(s_0, \ldots, s_n)$, such that s_0 is s, s_n is t and, for $0 < i \leq n$, one of $s_{i-1} \leftrightarrow_E s_i$, $s_{i-1} \rightarrow_R s_i$, or $s_{i-1} \leftarrow_R s_i$ holds. Every single proof step (s_{i-1}, s_i) has to be justified by an equation $u_i = v_i$, a substitution σ_i, and a position p_i, such that $s_{i-1}/p_i \equiv u_i \sigma_i$, $s_i \equiv s_{i-1}[p_i / v_i \sigma_i]$, and $u_i \doteq v_i$ is in $E \cup R$ ($u \doteq v$ denotes, ambiguously, $u = v$ or $v = u$). The *justification* of a proof is the multiset of all tuples $(s_{i-1}, s_i, u_i, v_i, \sigma_i, p_i)$, $1 \leq i \leq n$. It may be (partially) indicated by writing $s_0 \leftrightarrow_E s_1 \rightarrow_R \cdots \leftarrow_R s_n$, etc. A proof step $s \leftrightarrow_E t$ is called an *equality step*; a step $s \rightarrow_R t$, a *rewrite step*; a proof $s \leftarrow_R u \rightarrow_R t$, a *peak*. We abbreviate a proof $s_0 \rightarrow_R \cdots \rightarrow_R s_n$ by $s_0 \overset{*}{\rightarrow}_R s_n$. A proof $s \overset{*}{\rightarrow}_R u \overset{*}{\leftrightarrow}_E v \overset{*}{\leftarrow}_R t$ is called a *rewrite proof modulo E.*

We use the symbols P and Q to denote proofs. If P is $(s_0, \ldots, s_n)$, then P^{-1} denotes $(s_n, \ldots, s_0)$. The notation $P[Q]$ indicates that P contains Q as a subproof. A binary relation $\Rightarrow$ on (justified) proofs is *monotonic* if $Q \Rightarrow Q'$ implies $P[Q] \Rightarrow P[Q']$, for all proofs P, Q, and Q'. It is *stable* if $P \equiv (s, \ldots, u_i, \ldots, t) \Rightarrow (s, \ldots, v_j, \ldots, t) \equiv Q$ implies $(c[s\sigma], \ldots, c[u_i \sigma], \ldots, c[t\sigma]) \Rightarrow (c[s\sigma], \ldots, c[v_j \sigma], \ldots, c[t\sigma])$, for all proofs P and Q, terms c, and substitutions σ. A *proof (reduction) ordering* is stable, monotonic and well-founded ordering on proofs.

A *proof pattern* is a schema for a class of proofs and describes proofs that share a common structure. For example, the pattern $s \rightarrow_R t$, where s and t are metavariables denoting arbitrary terms and R denotes an arbitrary rewrite system, characterizes all single step rewrite proofs in R; $s \overset{*}{\rightarrow}_R u \overset{*}{\leftarrow}_R t$ describes all rewrite proofs in R; $s \leftarrow_R u \rightarrow_R t$, all peaks. An *instance* of a pattern is any specific proof of the given structure. An *elimination pattern* is a pair of proof patterns. For any set of elimination patterns S, we denote by $\Rightarrow_S$ the smallest stable and monotonic ordering that contains any instance of an elimination pattern of S.

4. Completion for Rewriting Modulo a Congruence

We describe methods for constructing, given sets of equations A and E, a rewrite system $R \equiv L \cup N$ such that $L \cup N \cdot A$ is canonical modulo A and the congruence relations $\overset{*}{\leftrightarrow}_{A \cup E}$

and $\overset{*}{\leftrightarrow}_{A\cup R}$ are the same. The set A is assumed to be symmetric, for simplicity. Thus, the relations $\rightarrow_A$ and $\leftrightarrow_A$ are identical. We formulate completion as an equational inference system for manipulating pairs (E_i, R_i) of sets of equations E_i and rewrite systems R_i.

Let $>$ be a reduction ordering that is compatible with A. The inference system **A** (*completion for rewriting modulo a congruence*) consists of the following inference rules, where E may be any set of equations and R any rewrite system contained in $>$:

Orienting an equation

$$\frac{(E\cup\{s\doteq t\},R)}{(E,R\cup\{s\rightarrow t\})} \qquad \text{if } s>t \tag{1}$$

Adding an equational consequence

$$\frac{(E,R)}{(E\cup\{s=t\},R)} \qquad \text{if } s \overset{*}{\leftarrow}_{R\cup A} u \overset{*}{\rightarrow}_{R\cup A} t \tag{2}$$

Simplifying an equation

$$\frac{(E\cup\{s\doteq t\},R)}{(E\cup\{u\doteq t\},R)} \qquad \text{if } s\rightarrow_{R/A} u \tag{3}$$

Deleting an equation

$$\frac{(E\cup\{s=t\},R)}{(E,R)} \qquad \text{if } s \overset{*}{\leftrightarrow}_A t \tag{4}$$

Simplifying the right-hand side of a rule

$$\frac{(E,R\cup\{s\rightarrow t\})}{(E,R\cup\{s\rightarrow u\})} \qquad \text{if } t\rightarrow_{R/A} u \tag{5}$$

Simplifying the left-hand side of a rule

$$\frac{(E,R\cup\{s\rightarrow t\})}{(E\cup\{u=t\},R)} \qquad \text{if } s\rightarrow_{R/A} u \text{ at a position not at the top} \tag{6}$$

$$\frac{(E,R\cup\{s\rightarrow t\})}{(E\cup\{u=t\},R)} \qquad \text{if } s\rightarrow_{R} u \text{ by } l\rightarrow r \text{ and } s\rhd l \tag{7}$$

The symbol $\rhd$ denotes the proper subsumption ordering.

We write $(E,R)\vdash_{\mathbf{A}}(E',R')$ if (E',R') can be obtained from (E,R) by (one or more) applications of inference rules of **A**. We implicitly assume that R and R' are partitioned into $L\cup N$ and $L'\cup N'$, respectively, where L and L' are left-linear. If a rule $s\rightarrow t$ is in L, then simplification of its right-hand side by (5) yields a rule $s\rightarrow u$ in L'; if $s\rightarrow t$ is in N, then $s\rightarrow u$ is in N'.

The inference system **A** is *sound*, i.e. whenever $(E,R)\vdash_{\mathbf{A}}(E',R')$, then the congruence relations $\overset{*}{\leftrightarrow}_{A\cup E\cup R}$ and $\overset{*}{\leftrightarrow}_{A\cup E'\cup R'}$ are the same.

A (possibly infinite) sequence (E_0,R_0), (E_1,R_1), $\cdots$ is called a *derivation* in **A** if $(E_{i-1},R_{i-1})\vdash_{\mathbf{A}}(E_i,R_i)$, for all $i>0$. The *limit* of a derivation is the pair (E^∞,R^∞) of the set $\cup_{i\geq 0}\cap_{j\geq i}E_j$ of all *persisting equations* and the set $\cup_{i\geq 0}\cap_{j\geq i}R_j$ of all *persisting rules.*

A *completion procedure* (for a given set of equational axioms A) is a strategy for applying inference rules of **A** to given inputs E_0 and R_0 to generate a derivation (E_0,R_0), (E_1,R_1), $\cdots$. (The reduction ordering $>$, which has to be compatible with A, is usually regarded as an additional parameter. The initial set of rules R_0 must be contained in this ordering.) We will derive conditions under which the derivation generated by a completion procedure converges to a limit (E^∞,R^∞) for which $E^\infty\equiv\emptyset$ and $(R^\infty)^A$ is canonical modulo A.

First observe that the application of inference rules of A is reflected on the proof level by an ordering on proofs. For instance, application of inference rules (1), (3), and (4) can be expressed by *equality (elimination) patterns*

$$\begin{array}{lcl} s \leftrightarrow_E t & \Rightarrow & s \rightarrow_{R'} t \\ s \leftrightarrow_E t & \Rightarrow & s \rightarrow_{R'/A} u \leftrightarrow_{E'} t \\ s \leftrightarrow_E t & \Rightarrow & s \overset{*}{\leftrightarrow}_A t \end{array}$$

Application of (5), (6), and (7) can be expressed by the *simplification patterns*

$$\begin{array}{lcl} s \rightarrow_R t & \Rightarrow & s \rightarrow_{R'} u \leftarrow_{R'/A} t \\ s \rightarrow_R t & \Rightarrow & s \rightarrow_{R'/A} v \leftrightarrow_{E'} t \\ s \rightarrow_R t & \Rightarrow & s \rightarrow_{R'} w \leftrightarrow_{E'} t \end{array}$$

where $s \rightarrow_R t$ is by application of a rule $l \rightarrow r$ at position p; $s \rightarrow_{R'} u$ is by $l \rightarrow r'$ at position p; $s \rightarrow_{R'/A} v$ is by application of a rule strictly below p; and $s \rightarrow_{R'} w$ is by a rule $l' \rightarrow r'$ with $l \rhd l'$ at position p. By $\Rightarrow_{\mathrm{C}}$ we denote the ordering induced by these elimination patterns. We have

Lemma 1. *Let $\Rightarrow_{\mathrm{A}}$ be any ordering containing $\Rightarrow_{\mathrm{C}}$. Whenever $(E, R) \vdash_{\mathrm{A}} (E', R')$, then there is, for every proof P in $E \cup R$, a proof P' in $E' \cup R'$, such that $P \overset{*}{\Rightarrow}_{\mathrm{A}} P'$.*

Proof. Only inference rule (2) is not covered by $\Rightarrow_{\mathrm{C}}$. If $(E, R) \vdash_{\mathrm{A}} (E', R')$ by application of (2), then R and R' are identical and E is contained in E'. Therefore every proof P in $A \cup E \cup R$ is also a proof in $A \cup E' \cup R'$. •

Lemma 1 shows that completion can be viewed as a process of transforming proofs. The problem of constructing a Church-Rosser system, on the other hand, consists of transforming any non-rewrite proof into a rewrite proof. A proof in $A \cup E \cup R$ is a rewrite proof modulo A if and only if it contains no equality step $s \leftrightarrow_E t$ and no peak $s \leftarrow_{A \cup R^A} u \rightarrow_{R^A} t$. For construction of a Church-Rosser system it suffices to reduce (i.e. simplify) such "critical proofs" with respect to some (well-founded) ordering on proofs. Proof orderings formalize the intuitive notion of proof simplification.

We extend the ordering $\Rightarrow_{\mathrm{C}}$, which can be used for reducing equality steps, to a proof ordering $\Rightarrow_{\mathrm{A}}$ that can also be used for eliminating peaks.

The problem of simplifying peaks $s \leftarrow_{A \cup R^A} u \rightarrow_{R^A} t$ can be reduced to the problem of simplifying peaks $s \leftarrow_{A \cup R} u \rightarrow_{R^A} t$. (Recall that $l \rightarrow_{R^A} r$ abbreviates $l \rightarrow_L r$ or $l \rightarrow_{N \cdot A} r$, and that $l \rightarrow_{N \cdot A} r$ abbreviates $l \overset{*}{\leftrightarrow}_A l' \rightarrow_N r$.) Let P be a peak between $A \cup R$ and R^A.

If both proof steps in P apply at disjoint positions, then there is *no overlap.* We have a corresponding elimination pattern

$$u[p/r] \leftarrow_{A \cup R} u \rightarrow_{R^A} u[q/r'] \quad \Rightarrow \quad u[p/r] \rightarrow_{R^A} u[p/r, q/r'] \leftarrow_{A \cup R} u[q/r']$$

where p and q are disjoint positions, u/p is l, u/q is l', $l \rightarrow_{A \cup R} r$, and $l' \rightarrow_{R^A} r'$.

If one step in P applies below the other, then there exist positions p and q and rules $v \rightarrow w$ and $l \rightarrow r$, such that u/p is $v\sigma$ and $v\sigma/q$ is $l\sigma$. (We assume that v and l have no variables in common.) If q is not a position in v or if v/q is a variable, then one rule applies in the variable or substitution part of the other, and P is called a *variable overlap.* We speak of an *overlap* if v/q denotes a non-variable subterm of v.

Variable overlaps have the general structure

$$w\,\sigma[l\,\sigma, \ldots, l\,\sigma] \leftarrow_R v\,\sigma[l\,\sigma, \ldots, l\,\sigma] \rightarrow_{R'} v\,\sigma[r\,\sigma, l\,\sigma, \ldots, l\,\sigma]$$

and can be replaced by proofs

$$w\,\sigma[l\,\sigma, \ldots, l\,\sigma] \overset{*}{\rightarrow}_{R'} w\,\sigma[r\,\sigma, \ldots, r\,\sigma] \leftarrow_R v\,\sigma[r\,\sigma, \ldots, r\,\sigma] \overset{*}{\leftarrow}_{R'} v\,\sigma[r\,\sigma, l\,\sigma, \ldots, l\,\sigma].$$

From this schema we derive elimination patterns

$$\begin{array}{rcl}
s \leftarrow_R u \rightarrow_{R'} t & \Rightarrow & s \overset{*}{\rightarrow}_{R'} v \leftarrow_R w \overset{*}{\leftarrow}_{R'} t \\
s \leftarrow_A u \rightarrow_L t & \Rightarrow & s \overset{*}{\rightarrow}_L v \leftarrow_A w \overset{*}{\leftarrow}_L t \\
s \leftarrow_L u \rightarrow_A t & \Rightarrow & s \overset{*}{\rightarrow}_A v \leftarrow_L t \\
s \leftarrow_A u \rightarrow_{N\cdot A} t & \Rightarrow & s \overset{*}{\rightarrow}_{N\cdot A} v \leftarrow_A w \overset{*}{\leftarrow}_{N\cdot A} t
\end{array}$$

where all left-hand sides denote variable overlaps with the second step below the first (strictly below in the last pattern).

Remark. A variable overlap P of the form $s \leftarrow_N u \rightarrow_A t$, wherein the second step applies below the first, simply translates into a rewrite step $s \leftarrow_{N\cdot A} t$. It could be replaced by a proof Q of the form $(s \overset{*}{\rightarrow}_A v \leftarrow_N w \overset{*}{\leftarrow}_A t)$, but if $u \rightarrow_N s$ is by application of a non-left-linear rule, then Q contains a subproof $v \leftarrow_N w \overset{+}{\leftarrow}_A t$ that is essentially equivalent to the original variable overlap P. (The set A is symmetric.) Thus, replacements of this form do not define a well-founded ordering. The concepts of A-matching and rewriting modulo a congruence provide an effective way of handling such problematic variable overlaps involving non-left-linear rules.

Overlaps can be effectively eliminated if a finite, complete unification algorithm for the theory A is known.

Two terms s and t are *A-unifiable* if there exists a substitution (an *A-unifier*) σ, such that $s\,\sigma \overset{*}{\leftrightarrow}_A t\,\sigma$. A set Σ of A-unifiers of s and t is *complete* if for any A-unifier τ of s and t there exists a substitution ρ, such that $x\,\tau \overset{*}{\leftrightarrow}_A (x\,\sigma)\rho$, for all variables x. We will consider, from now on, sets of axioms A for which a finite complete sets of unifiers for A exist and can be computed. Finite, complete unification algorithms are known for many theories of practical importance (Siekmann 1984). If A is the empty set, then the set consisting of the (unique) most general unifier of s and t is complete.

Let $u \rightarrow v$ and $l \rightarrow r$ be rules in R and R', respectively, with no variables in common (the variables of one rule are renamed if necessary). Let p be a non-variable position in u, such that u/p and l are A-unifiable with a complete set of unifiers Σ. For any σ in Σ, the proof $v\,\sigma \leftarrow_R u\,\sigma \rightarrow_{R' \cdot A} u\,\sigma[p/r\,\sigma]$ is called an *A-critical overlap* of R' on R. The equation $v\,\sigma = u\,\sigma[p/r\,\sigma]$ is called an *A-critical pair* of $l \rightarrow r$ on $u \rightarrow v$ at position p (or an A-critical pair of R' on R). An A-critical pair between R and R' is either an A-critical pair of R on R' or of R' on R. If A is empty, then we speak of *critical pairs.*

The following lemmata characterize the connection between critical pairs and overlaps.

Lemma 2. (Critical Pair Lemma, Knuth and Bendix 1970) *If $s \leftarrow_R u \rightarrow_{R'} t$ is an overlap, then $s \equiv v\,[c\,\sigma]$ and $t \equiv v\,[d\,\sigma]$, for some term v and critical pair $c = d$ between R and R'.*

Lemma 3. (Extended Critical Pair Lemma, Jouannaud 1983). *Let A be a set of equations for which there exists a finite complete unification algorithm. Let $u \rightarrow v$ and $l \rightarrow r$ be rules and p a position in u, such that u/p is not a variable and is A-unifiable with l, Σ being a complete set of A-unifiers. Then there exist, for any overlap $v\,\tau \leftarrow_R u\,\tau \rightarrow_{R'} u\,\tau[p/r\,\tau]$, substitutions σ and ρ, σ in Σ, such that $x\,\tau \overset{*}{\leftrightarrow}_A (x\,\sigma)\rho$, for all variables x in $u \rightarrow v$ or $l \rightarrow r$. Consequently, there exists an A-critical pair $c = d$, such that $v\,\tau \overset{*}{\leftrightarrow}_A c\,\rho$ and $u\,\tau[p/r\,\tau] \overset{*}{\leftrightarrow}_A d\,\rho$. If v is not a* *variable, then no equation in* $v\,\tau \overset{*}{\leftrightarrow}_A c\,\rho$ *applies at the top.*

The lemmata are the basis for the *overlap patterns*

$$\begin{array}{ccc}
s \leftarrow_R u \rightarrow_L t & \Rightarrow & s \leftrightarrow_{E'} t \\
s \leftarrow_A u \rightarrow_L t & \Rightarrow & s \rightarrow_{R'} t \\
s \leftarrow_L u \rightarrow_A t & \Rightarrow & s \leftarrow_{R'} t \\
s \leftarrow_R u \rightarrow_{N \cdot A} t & \Rightarrow & s \overset{*}{\leftrightarrow}_A v \leftrightarrow_{E'} w \overset{*}{\leftrightarrow}_A t \\
s \leftarrow_A u \rightarrow_{N \cdot A} t & \Rightarrow & s \overset{*}{\leftrightarrow}_A v \rightarrow_{R'} w \overset{*}{\leftrightarrow}_A t
\end{array}$$

where all left-hand sides denote overlaps with the second step applying below the first step. In addition, in the last pattern, the positions of $u \rightarrow_{N \cdot A} t$ and of all steps in $s \overset{*}{\leftrightarrow}_A v$ are strictly below the position of $u \rightarrow_A s$. The equality steps in $s \overset{*}{\leftrightarrow}_A v$ and $w \overset{*}{\leftrightarrow}_A t$ reflect the fact that an overlap between $N \cdot A$ and $A \cup R$ need not contain an instance of an A-critical pair, but only an equation equivalent to such an instance.

By $\Rightarrow_{\mathrm{A}}$ we denote the ordering induced by the above elimination patterns (including the equality and simplification patterns). This ordering depends on the set of equations A. For certain sets A it is well-founded; hence a proof ordering.

Let P be a proof $(t_0, \ldots, t_n)$ in $A \cup E \cup R$ and let p_i be the position of the i-th proof step (t_{i-1}, t_i). The complexity $M(P)$ of P is the multiset $\{c(t_0, t_1, P), \ldots, c(t_{n-1}, t_n, P)\}$, where $c(t_{i-1}, t_i, P)$ is

$$\begin{array}{ll}
(\{t_{i-1}, t_i\}, -, -, -, -) & \text{if } t_{i-1} \leftrightarrow_E t_i \\
(\{t_{i-1}\}, t_{i-1}/p_i, max, l, t_i) & \text{if } t_{i-1} \leftrightarrow_A t_i \text{ by an equation } l = r \\
(\{t_{i-1}\}, t_{i-1}/p_i, e(t_{i-1}, t_i, P), l, t_i) & \text{if } t_{i-1} \rightarrow_R t_i \text{ by a rule } l \rightarrow r \\
c(t_i, t_{i-1}, P^{-1}) & \text{if } t_{i-1} \leftarrow_R t_i
\end{array}$$

and $e(t_{i-1}, t_i, P)$ is the multiset $\{t_{i-k+1}/p_{i-k+1}, \ldots, t_{i-1}/p_{i-1}\}$, with k being the largest index for which $(t_{i-k}, \ldots, t_{i-1})$ is a proof of the form $t_{i-k} \overset{*}{\leftrightarrow}_A t_{i-1}$ or $t_{i-k} \leftarrow_R t_{i-k+1} \overset{*}{\leftrightarrow}_A t_{i-1}$. The multiset $e(t_{i-1}, t_i, P)$ encodes information about the "environment" of a rewrite step. The symbol *max* denotes a new constant.

The ordering $>^c$ is the lexicographic combination of the extension to multisets of the reduction ordering $>$, the proper subterm ordering modulo A, the extension to multisets of the proper subterm ordering modulo A, the subsumption ordering, and the reduction ordering $>$. (Elements equivalent with respect to A are regarded as being identical when compared in the reduction ordering $>$ or the subterm ordering modulo A. The constant *max* is assumed to be maximal.) This ordering is well-founded if and only if the proper subterm ordering modulo A is well-founded. We define $>_{\mathrm{A}}$ by: $P >_{\mathrm{A}} P'$ if and only if $M(P) \gg^c M(P')$.

Lemma 4. *If the proper subterm ordering modulo* A *is well-founded, then* $\Rightarrow_{\mathrm{A}}$ *is a proof ordering.*

Sketch of proof. We prove that any instance of a right-hand side of an elimination pattern for completion is simpler with respect to $>_{\mathrm{A}}$ than the the corresponding instance of the left-hand side. In may cases, e.g. for equality patterns, the first component in the complexity measure $c(s, t, P)$ suffices to prove this assertion. For overlap patterns, only the first three component are relevant. The second, fourth, and fifth component of $c(s, t, P)$ are used for the simplification patterns, mainly. For details see Bachmair (1987). •

Simplification of overlaps by $\Rightarrow_{\mathrm{A}}$ corresponds to the application of inference rule (2). The following definition is motivated by this connection between inference system and proof ordering.

Definition 1. A derivation (E_0,R_0), (E_1,R_1), $\cdots$ in $\mathbf{A}$ is fair if (a) $E^\infty \equiv \emptyset$, (b) all critical pairs of L^∞ on R^∞ and all A-critical pairs of N^∞ on R^∞ are contained in $\bigcup_k E_k$, and (c) all critical pairs between L^∞ and A and all A-critical pairs of N^∞ on A are contained in $\bigcup_k R_k$.

A fair derivation may not be possible from an arbitrary pair (E_i, R_i), since equations could be generated that can not be oriented, simplified, or deleted. Thus, a completion procedure may *fail* for certain inputs E, R and $>$. We say that a completion procedure is *fair* if it generates only fair derivations unless it fails.

THEOREM 1. *Let A be a set of equations with a finite complete unification algorithm for which the proper subterm ordering modulo A is well-founded. Let E be a set of equations, $R \equiv L \cup N$ be a rewrite system, and $>$ be a reduction ordering that is compatible with A and contains R. If C is a fair completion procedure and does not fail for inputs E, R and $>$, then $E^\infty \equiv \emptyset$ and $(R^\infty)^A$ is canonical modulo A.*

Sketch of proof. Let (E_0,R_0), (E_1,R_1), $\cdots$ be a fair derivation in $\mathbf{A}$. We prove that whenever a proof P of $s = t$ in $A \cup E_i \cup R_i$ is not a rewrite proof modulo A in $(R^\infty)^A$, then there is a proof Q of of $s = t$ in $A \cup E_j \cup R_j$, for some $j \geq i$, such that $P \Rightarrow_{\mathrm{A}} Q$. We can then infer, by induction on $\Rightarrow_{\mathrm{A}}$, that $(R^\infty)^A$ is Church-Rosser modulo A. Termination follows from the fact that the reduction ordering $>$ is compatible with A and contains R^∞.

Let P be a proof in $A \cup E_i \cup R_i$. If P contains an equality step $u \leftrightarrow_{E_i} v$, then, by part (a) of the fairness requirement, eventually one of the inference rules (1), (3), or (4) has to be applied, resulting in a proof Q in $A \cup E_j \cup R_j$, for some $j \geq i$, such that $P \Rightarrow_{\mathrm{A}} Q$. Similarly, if P uses a non-persisting rewrite step, application of (5), (6), or (7) will yield a simpler proof Q. Finally, suppose that P uses only persisting rules or equations in A, i.e. is a proof in $A \cup R^\infty$, but is not a rewrite proof. Then P must contain a peak $v \leftarrow_{A \cup R_i} u \rightarrow_{R_i^A} w$. If this peak is a variable overlap, or not an overlap at all, then it can be eliminated by rearranging its proof steps, as described in the above elimination patterns. On the other hand, parts (b) and (c) of the fairness hypothesis guarantee that all critical pairs necessary for elimination of overlaps are computed. In either case, there is a proof Q in $A \cup E_j \cup R_j$, for some $j \geq i$, such that $P \Rightarrow_{\mathrm{A}} Q$. •

A system R^A is called *reduced* if, for every rule $l \rightarrow r$ in R, l is irreducible in $(R - \{l \rightarrow r\})^A$ and r is irreducible in R^A. Completion procedures based on the inference system $\mathbf{A}$ do not allow construction of reduced systems, in general, since inference rule (7) does not permit reductions by $N \cdot A$. Thus a final (canonical) system R^∞ may contain two rules $l \rightarrow r$ and $u \rightarrow v$, for which $l \leftrightarrow_A^* u\sigma$, for some substitution σ. But a reduced canonical system can be easily obtained (see also Jouannaud and Kirchner 1986):

PROPOSITION 1. *Let R be a (finite) rewrite system and A be a set of equations, such that R^A is canonical modulo A. Let R' be the system obtained from R by deleting one by one any rule $l \rightarrow r$ for which there is a rule $u \rightarrow v$ in N, distinct from $l \rightarrow r$, such that $l \leftrightarrow_A^* u\sigma$, for some substitution σ. Then $(R')^A$ is canonical modulo A.*

The restriction of inference rule (7) to simplification by R is a major limitation of rewriting modulo a congruence. This limitation can be relaxed (at the cost of imposing other restrictions).

Let $v\,\sigma \leftarrow_A u\,\sigma \rightarrow_{N\cdot A} u\,\sigma[p\,/r\,\sigma]$ be an A-critical overlap of $l \rightarrow r$ on $u \rightarrow v$ at position p. Jouannaud and Kirchner (1986) use inference rule (2) not for adding the A-critical pair $v\,\sigma = u\,\sigma[r\,\sigma]$, but for generating either an equation $w = u\,\sigma[r\,\sigma]$, if there exists a term w such that $v\,\sigma \rightarrow_{R^A} w$, or an *extended rule* $u\,[p\,/l\,] \rightarrow u\,[p\,/r\,]$, if $v\,\sigma$ is irreducible in R^A.

This use of inference rule (2) can be viewed as combining several inference step, namely generation of a rule $v\,\sigma \rightarrow u\,\sigma[r\,\sigma]$ with simplification of its left-hand side. If possible, a term w is chosen that can be obtained by reducing a proper subterm of $v\,\sigma$ in $R\,/A$, or by reducing $v\,\sigma$ at the top in R. If $v\,\sigma$ can only be reduced in $N\cdot A$ at the top, using a rule $l' \rightarrow r'$ in N, say, then $l' \rightarrow r'$ has to be *protected* from simplification at the left-hand side. In other words, left-hand sides of protected rules can not be further simplified. The introduction of an extended rule renders the term $v\,\sigma$ reducible. More precisely, we have $v\,\sigma \rightarrow_{N\cdot A} u\,\sigma[r\,\sigma$ by applying the extended rule $u\,[l\,] \rightarrow u\,[r\,]$ at the top. (Extended rules are added to the set N.) Consequently, extended rules have to be protected. (Without protection, the rule $u\,[l\,] \rightarrow u\,[r\,]$ could be reduced to a trivial equation $u\,[r\,] = u\,[r\,]$ by $l \rightarrow r$.)

The above procedure can be conveniently described by an inference rule for

Simplifying the left-hand side of a rewrite rule

$$\frac{(E\,, R \cup \{s \rightarrow t\,\})}{(E \cup \{u = t\,\}, R\,)} \qquad \text{if } s \rightarrow_{N\cdot A} u \text{ by a protected rule } l \rightarrow r \qquad (8)$$

Let $\mathbf{P}$ be the inference system consisting of inference rules (1)-(8), but with application of (6), (7), and (8) confined to unprotected rules. The modifications in the simplification rules are reflected by changes in the corresponding elimination patterns. The resulting ordering $\Rightarrow_{\mathbf{P}}$ is well-founded; hence a proof ordering. This can be proved by using a similar complexity measure as for $\Rightarrow_{\mathbf{A}}$ in which a distinction is made between rewrite steps by a protected or an unprotected, respectively. In particular, any proof step $s \rightarrow_{N\cdot A} t$ that uses a protected rules has to be considered as a single proof step (not as an abbreviation for a proof $s \leftrightarrow_A^* u \rightarrow_N t$). Thus, the equality steps in $s \leftrightarrow_A^* u$ do not directly contribute to the complexity of a proof. Theorem 1 is also valid for completion procedures based on $\mathbf{P}$ (Bachmair 1987). The procedure described by Jouannaud and Kirchner (1986) can be formulated within $\mathbf{P}$. Jouannaud and Kirchner (1986) prove the correctness of their procedure under the assumptions that congruence classes generated by A are finite and that the proper subsumption ordering modulo A is well-founded. The first assumption implies that the subterm ordering modulo A is well-founded. Thus, our results show that the second assumption is not needed at all.

Formulating completion as an inference system has the additional advantage of providing more flexibility for implementing specific versions of completion. The inference system $\mathbf{A}$ is a special case of $\mathbf{P}$, in which protected rules are never generated. This indicates protected rules are not necessary for construction of a canonical system. They may be useful, though (see the discussion in Jouannaud and Kirchner 1986).

5. Completion for the Infinite Congruence Class Case

Extended rules were introduced by Peterson and Stickel (1981) in the context of associative-commutative rewriting. Jouannaud and Kirchner (1986) generalized the concept to rewriting modulo a congruence, in general. In this section, we describe a completion method that systematically uses extended rules and can be applied to any set of equations A with a finite complete unification algorithm. In particular, the method can be used for equational theories that generate infinite congruence classes, e.g. theories with identity, $f(x,e)=x$, or equipotency, $f(f(x))=x$.

Let $R \equiv L \cup N$ be a rewrite system, where L contains only left-linear rules. A rule $l \rightarrow r$ in N and equation $u=v$ in A determine an extended rule $u[l] \rightarrow u[r]$, if l is A-unifiable with some proper (non-variable) subterm u/p of u.

Extended rules have to be protected from simplification on the left-hand side. This may preclude construction of fully reduced systems. But extended rules do have advantages. Consider an A-critical overlap $v\sigma \leftrightarrow_A u\sigma \overset{*}{\leftrightarrow}_A u\sigma[l\sigma]$ of $l \rightarrow r$ on $u=v$ at position p. The term $v\sigma$ reduces to $u\sigma[r\sigma]$ by application of $u[l] \rightarrow u[r]$. In other words, in the presence of an extended rule, the A-critical pair $v\sigma \rightarrow u\sigma[r\sigma]$ simplifies to a trivial equation $u\sigma[r\sigma]=u\sigma[r\sigma]$; hence need not be computed in the first place. This argument applies to any A-critical pair of $l \rightarrow r$ on $u=v$ at position p. Therefore, it suffices to compute a single extended rule, instead of a possibly large set of A-critical pairs. Usually, extended rule can be computed more efficiently than A-critical pairs, since they require only a test for A-unifiability.

Let A be a symmetric set of equations and $>$ be a reduction ordering compatible with A. The inference system $\mathbf{E}$ consists of inference rules (1)-(6), plus the following rule for

Simplifying the left-hand side of a rewrite rule

$$\frac{(E, R \cup \{s \rightarrow t\})}{(E \cup \{u=t\}, R)} \qquad \text{if } s \rightarrow_{R/A} u \text{ by a rule } l \rightarrow r \text{ with } s \rhd l \qquad (9)$$

Here $\rhd$ may be any well-founded ordering on terms, e.g. terms may be compared by their size.

The proof ordering techniques outlined in the preceding sections can readily be applied to the inference system $\mathbf{E}$. Again, application of inference rules of $\mathbf{E}$ is reflected on the proof level by a proof ordering $\Rightarrow_{\mathbf{E}}$ (Bachmair 1987). The ordering $\rhd$ takes on the role of the subterm ordering modulo A in proving that $\Rightarrow_{\mathbf{E}}$ is well-founded. We have the following fairness condition:

Definition 2. A derivation $(E_0,R_0), (E_1,R_1), \cdots$ in $\mathbf{E}$ is *fair* if (a) $E^{\infty} \equiv \emptyset$, (b) all critical pairs of L^{∞} on R^{∞} and all A-critical pairs of N^{∞} on R^{∞} are contained in $\cup_k E_k$, and (c) whenever $l \rightarrow r$ is an extended rule of N^{∞} and A or a critical pair between L^{∞} and A, then R^{∞} contains a rule $l \rightarrow u$, where $r \overset{*}{\rightarrow}_{\cup R_i} u$.

Part (c) expresses the fact that extended rules and critical pairs between L^{∞} and A are protected from simplification on the left-hand side.

THEOREM 2. *Let A and E be sets of equations, $R \equiv L \cup N$ be a rewrite system, and $>$ be a reduction ordering that contains R and is compatible with A. If C is a fair $\mathbf{E}$-completion procedure and does not fail for inputs E, R and $>$, then $E^{\infty} \equiv \emptyset$ and $(R^{\infty})^A$ is canonical modulo A.*

The associative-commutative completion procedure by Peterson and Stickel (1981) can be formulated within the inference system $\mathbf{E}$. This procedure applies to sets AC of associativity and commutativity axioms and employs the rewrite relation $R \cdot AC$. For simplification of left-hand sides an ordering $\rhd$ is used in which terms are first compared by size, then with respect to the proper subsumption ordering modulo AC. The only extended rules, originating from rules $f\ (s\ ,t\ )\rightarrow u$ with an AC-operator f as outermost symbol on the left-hand side, are $f\ (x\ ,f\ (s\ ,t\ ))\rightarrow f\ (x\ ,u\ )$ and $f\ (f\ (s\ ,t\ ),x\ )\rightarrow f\ (u\ ,x\ )$, where x is a new variable not appearing in s , t , or u . (Since both rules are equivalent, only one is actually needed. Extensions of extended rules are superfluous.) A large number of canonical systems have been derived with this completion method (e.g. Hullot 1980).

6. Critical Pair Criteria

Computation of critical pairs, as required by fairness, guarantees simplification of overlaps. Often overlaps can be reduced without computing the corresponding critical pair. A *critical pair criterion* characterizes critical pairs that are redundant in this sense. Various criteria have been designed for standard completion; see Bachmair and Dershowitz (1986) for a uniform treatment and further references. Similar criteria can be applied to rewriting modulo a congruence (e.g. Küchlin 1986). We generalize the concept of *compositeness* (Kapur, Musser, and Narendran 1986).

Definition 3. (a) A critical pair $c = d$ of $l \rightarrow r$ on $u \rightarrow v$ at position p , with corresponding unifier σ, is called *composite*, if $u\,\sigma$ is reducible by $R\ /A$ at a position strictly below p .
(b) An A -critical pair $c = d$ of $l \rightarrow r$ on $u \rightarrow v$ at position p , with corresponding A -unifier σ, is called *composite*, if one of the terms $u\,\sigma$ or $u\,\sigma[p\ /l\,\sigma]$ is reducible by $R\ /A$ at a position strictly below p .

Composite critical pairs are redundant for (certain) completion procedures based on the inference system **A**. Consider, for example, an A -critical overlap

$$P \equiv (v\,\sigma \leftarrow_R u\,\sigma \rightarrow_{N\cdot A} u\,\sigma[p\ /r\,\sigma]).$$

If $u\,\sigma$ reduces to s , at a position strictly below critical pair position p , then the overlap P can be decomposed into two peaks

$$Q \equiv (v\,\sigma \leftarrow_R u\,\sigma \rightarrow_{R\,/A} s \leftarrow_{R\,/A} u\,\sigma \rightarrow_{N\cdot A} u\,\sigma[p\ /r\,\sigma]).$$

Now, the first proof step has smaller complexity in Q than in P , because its neighboring rewrite step applies at a lower position. A similar argument applies to the last proof step. The additional proof steps in Q apply at lower positions; hence are less complex. Therefore, we have $P >_{\mathbf{A}} Q$. In other words, any overlap corresponding to a composite A -critical pair of N on R can be simplified. Similar arguments apply to other critical overlaps, but *not* to overlaps involving extended rules. (A slightly different complexity measure is used for extended rules!)

An special case of compositeness is blocking. An A -critical pair $c = d$ is called *blocked* if $x\,\sigma$ is irreducible in $R\ /A$, for all variables x , σ being the A -unifier corresponding to $c = d$. Unblocked critical pairs are composite; hence redundant. Kapur, Musser and Narendran (1986) report that the application of blocking to the associative-commutative completion method of Peterson and Stickel (1981) typically results in considerable savings of computation time. Associative-commutative completion is based on extended rules, however, and the correctness of blocked (or composite) criteria for this case is an open problem.

References

[1] Bachmair, L. (1987). Proof methods for equational theories. Ph.D. thesis, Dept. of Computer Science, Univ. of Illinois at Urbana-Champaign.

[2] Bachmair, L., and Dershowitz, N. (1986). Critical pair criteria for the Knuth-Bendix completion method. *Proc. Symp. on Symbolic and Algebraic Computation,* B. W. Char, ed., Waterloo, Canada, 215-217. (Revised version to appear in *J. Symbolic Computation.*)

[3] Bachmair, L., Dershowitz, N., and Hsiang, J. (1986). Orderings for equational proofs. *Proc. IEEE Symp. Logic in Computer Science,* Cambridge, Massachussetts, 346-357.

[4] Hullot, J.-M. (1980). A catalogue of canonical term rewriting systems. Tech. Rep. CSL-113, SRI International, Menlo Park, California.

[5] Jouannaud, J.-P. (1983). Confluent and coherent equational term rewriting systems: Application to proofs in abstract data types. *Proc. 8th Coll. on Trees in Algebra and Programming,* G. Ausiello and M. Protasi, eds., Lect. Notes in Comp. Sci., vol. 59, Springer-Verlag, Berlin, 269-283.

[6] Jouannaud, J.-P., and Kirchner, H. (1986). Completion of a set of rules modulo a set of equations. *SIAM J. Computing* 15, 1155-1194.

[7] Kapur, D., Musser, D.R., and Narendran, P. (1986). Only prime superpositions need be considered in the Knuth-Bendix procedure. Unpublished manuscript, Computer Science Branch, Corporate Research and Development, General Electric, Schenectady, New York.

[8] Knuth, D., and Bendix, P. (1970). Simple word problems in universal algebras. *Computational Problems in Abstract Algebra,* J. Leech, ed., Pergamon Press, 263-297.

[9] Küchlin, W. (1986). Equational Completion by Proof Simplification. Report No. 86-02, Mathematik, ETH Zürich, Switzerland.

[10] Lankford, D., and Ballantyne, A. (1977). Decision procedures for simple equational theories with permutative axioms: Canonical sets of permutative reductions. Memo ATP-37, Dept. of Mathematics and Computer Science, University of Texas, Austin, Texas.

[11] Peterson, G., and Stickel, M. (1981). Complete sets of reductions for some equational theories. *J. ACM* 28, 233-264.

[12] Siekman, J. (1984). Universal unification. *Proc. 7th Conf. Automated Deduction,* R. E. Shostak, ed., Lect. Notes in Comp. Sci., vol. 170, Springer-Verlag, Berlin, 1-42.