COMMUTATION, TRANSFORMATION, AND TERMINATION*

Leo Bachmair

Nachum Dershowitz

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

Abstract. In this paper we study the use of *commutation* properties for proving *termination* of rewrite systems. Commutation properties may be used to prove termination of a combined system $R \cup S$ by proving termination of R and S separately. We present termination methods for ordinary and for equational rewrite systems. Commutation is also important for *transformation* techniques. We outline the application of transforms—mappings from terms to terms—to termination in general, and describe various specific transforms, including transforms for associative-commutative rewrite systems.

1. Introduction

Rewrite techniques have been applied to various problems, including the word problem in universal algebra (Knuth and Bendix, 1970), theorem proving in first order logic (Hsiang, 1985), proofs of inductive properties of abstract data types (Musser, 1980; Huet & Hullot, 1982), and computing with rewrite programs (O'Donnell, 1985; Dershowitz, 1985a). Many of these applications require a *terminating* rewrite system (see Dershowitz, 1985b). In this paper we study the use of *commutation* properties for proving termination of rewrite systems. We present termination methods for ordinary and for *equational* rewrite systems. In particular, we consider termination of *associative-commutative* rewrite systems.

Commutation was used by Rosen (1973) for establishing Church–Rosser properties of combinations of rewrite systems, and by Raoult and Vuillemin (1980) for proving operational and semantic equivalence between recursive programs. Dershowitz (1981) and Guttag, et al. (1983) apply properties similar to commutation to termination. We use commutation to reduce the problem of proving termination of a combined system $R \cup S$ to the problem of proving termination of the individual systems R and S separately. These commutation properties can often be easily established for certain systems, such as linear rewrite systems.

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

The use of well-founded sets is fundamental for termination arguments. Given a rewrite system R and a well-founded ordering $>$ on a set W, the problem is to find a mapping from terms to W, such that well-foundedness of $>$ implies termination of R. We study *transforms,* that is, mappings T from terms to terms, and derive conditions on R, T and $>$ that are sufficient for termination of R. It turns out that commutation properties play an important role in such transformation techniques. We present methods for both ordinary and equational rewrite system. The transforms we describe may be used, for instance, to prove termination of associative–commutative rewrite systems.

2. Definitions

Let $\mathcal{T}$ be the set of *terms* over some set of operator symbols F and some set of variables V. Terms containing no variables are called *ground terms.* We write $s[t]$ to indicate that a term s contains t as a subterm and denote by $s[t/u]$ or just $s[u]$ the result of replacing a particular occurrence of t by u.

A binary relation $\to$ on $\mathcal{T}$ is *monotonic* if $s \to t$ implies $u[s] \to u[t]$, for all terms u, s, and t. It is *stable (under substitution)* if $s \to t$ implies $s\sigma \to t\sigma$, for all terms s and t, and every substitution σ. The symbols $\to^+$, $\to^*$ and $\leftrightarrow$ denote the transitive, transitive–reflexive, and symmetric closure of $\to$, respectively. The inverse of $\to$ is denoted by $\leftarrow$. A relation $\to$ is *Noetherian* if there is no infinite sequence $t_1 \to t_2 \to t_3 \to \cdots$. A transitive Noetherian relation is called *well-founded.* A *reduction ordering* is a stable and monotonic well-founded ordering.

An *equation* is a pair (s,t), written $s=t$, where s and t are terms. For any set of equations E, $\leftrightarrow_E$ denotes the smallest symmetric relation that contains E and is monotonic and stable. That is, $s \leftrightarrow_E t$ if and only if $s=c[u\sigma]$ and $t=c[v\sigma]$, where $u=v$ or $v=u$ is in E. A reduction ordering $>$ is *compatible* with E if $s \overset{*}{\leftrightarrow}_E u > v \overset{*}{\leftrightarrow}_E t$ implies $s > t$, for all terms s, t, u, and v. *Directed* equations, in which every variable appearing on the right–hand side also appears on the left–hand side, are called *rewrite rules* and are written $s \to t$. A *rewrite system* is any set R of rewrite rules. The *reduction relation* $\to_R$ is the smallest stable and monotonic relation that contains R, i.e. $s \to_R t$ if and only if $s=c[l\sigma]$ and $t=c[r\sigma]$, for some rewrite rule $l \to r$ in R. We use R^{-1} to denote the inverse of R, and $R^{\leftrightarrow}$ to denote $(R \cup R^{-1})^*$.

Let E be a set of equations and R be a rewrite system. The *equational rewrite system* R/E (R *mod* E) is the set consisting of all rules $l \to r$ such that $l \overset{*}{\leftrightarrow}_E u \to_R v \overset{*}{\leftrightarrow}_E r$, for some terms u and v. Consequently, the reduction relation $\to_{R/E}$ is the relation $\overset{*}{\leftrightarrow}_E \circ \to_R \circ \overset{*}{\leftrightarrow}_E$, where $\circ$ denotes composition of relations. Analogously, if S is a rewrite system, we let R/S be the set of all rewrite rules $l \to r$ such that $l \overset{*}{\to}_S u \to_R v \overset{*}{\to}_S r$, for some terms u and v; the relation $\to_{R/S}$ is $\overset{*}{\to}_S \circ \to_R \circ \overset{*}{\to}_S$.

Let R/E be an equational rewrite system. We write $s \downarrow_{R/E} t$ to indicate that there exists a term u such that $s \overset{*}{\to}_{R/E} u \overset{*}{\leftarrow}_{R/E} t$. The system R/E is *Church–Rosser* if $s \overset{*}{\leftrightarrow}_{R/E} t$ implies $s \downarrow_{R/E} t$, for all terms s and t. It is *terminating* if $\to_{R/E}$ is Noetherian. An equational rewrite system R/E terminates if and only if there exists a reduction ordering $>$ that contains R and is compatible with $\overset{*}{\leftrightarrow}_E$. A terminating Church–Rosser rewrite system is called *canonical.* A term

t is *irreducible* in R/E if there is no term t' such that $t \to_{R/E} t'$. If $t \to^*_{R/E} t'$ and t' is irreducible in R/E, then t' is called an *R/E–normal form* of t. In a canonical system R/E any two normal forms t_1 and t_2 of a term t are equivalent in E. An ordinary rewrite system R may be regarded as an equational rewrite system R/E, where E is the empty set. Hence, all the definitions above apply to ordinary rewrite systems.

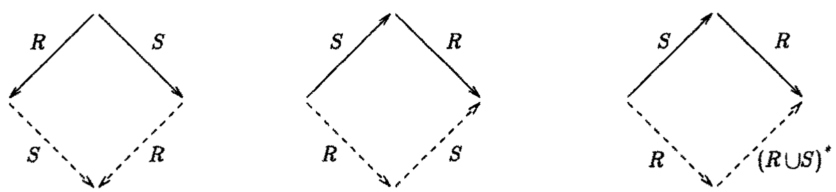
3. Commutation

Commuting rewrite systems have been investigated by Rosen (1973) and Raoult and Vuillemin (1980), among others. In this paper, we present new termination methods based on commutation that apply to ordinary as well as to equational rewrite systems.

Definition 1. Let R and S be rewrite systems. We say that R and S *commute* if $\leftarrow_R \circ \to_S$ is contained in $\to_S \circ \leftarrow_R$ (see Fig. 1).

For termination arguments the following *non–symmetric* commutation properties are also important.

Definition 2. A rewrite system R *commutes over* another system S if $\to_S \circ \to_R$ is contained in $\to_R \circ \to_S$; R *quasi–commutes over* S if $\to_S \circ \to_R$ is contained in $\to_R \circ \to^*_{R \cup S}$ (see Fig. 1). We say that R commutes over a set of equations E if $\leftrightarrow_E \circ \to_R$ is contained in $\to_R \circ \leftrightarrow^*_E$; R quasi–commutes over E if $\leftrightarrow_E \circ \to_R$ is contained in $\to_R \circ \leftrightarrow^*_E \circ \to^*_{R/E}$.



R and S commute   *R commutes over S*   *R quasi–commutes over S*

Fig. 1

Lemma 1. *Let R and S be two rewrite systems. Then the combined system $R \cup S$ is terminating if and only if both R/S and S are.*

Lemma 2. *If a rewrite system R quasi–commutes over another system S, then R/S is terminating if and only if R is.*

Proof. Trivially, if R/S is terminating, so is R. For the other direction, assume that R/S is not terminating. Then there exists an infinite derivation $t_1 \to^*_S t_2 \to_R t_3 \to^*_S t_4 \to_R \cdots$ containing an infinite number of applications of R. By the fact that R quasi–commutes over S, any application of R (beginning with $t_2 \to_R t_3$) can be pushed back through all preceding applications of

S. Thus there must also be an infinite derivation for R alone. □

Combining the above two lemmata, we have

THEOREM 1. *If a rewrite system R quasi-commutes over a rewrite system S, then the combined system $R \cup S$ terminates if and only if R and S both do.*

Syntactic properties of rewrite systems, such as linearity, may be helpful for establishing commutation; see, for example, Raoult and Vuillemin (1980). A term in which no variable appears more than once is called *linear.* A rewrite system R is called *left-linear,* if all left-hand sides of rules in R are linear; *right-linear,* if all right-hand sides are linear; and *linear,* if it is both left- and right-linear. A term s *overlaps* a term t if it can be unified with some non-variable subterm of t. We say that there is no overlap between s and t if neither s overlaps t nor t overlaps s.

Lemma 3. (Raoult and Vuillemin, 1980) *Let R be a left-linear and S be a right-linear rewrite system. If there is no overlap between a left-hand side of R and a right-hand side of S, then R quasi-commutes over S.*

Putting Lemma 3 and Theorem 1 together, we obtain

THEOREM 2. (Dershowitz, 1981) *Let R be a left-linear and S be a right-linear rewrite system. If there is no overlap between left-hand sides of R and right-hand sides of S, then the combined system $R \cup S$ terminates, if and only if R and S both do.*

Example 1. The systems

$$(x+y)\cdot z \quad \rightarrow \quad x\cdot z+y\cdot z$$

and

$$\begin{array}{lcl} x\cdot x & \rightarrow & x \\ x+x & \rightarrow & x \end{array}$$

both terminate. The first is left-linear and the second has only variables on the right; therefore their union also terminates.

Similar results hold for equational rewrite systems. Note that the relations $(R \cup S)/E$ and $R/E \cup S/E$ are the same.

PROPOSITION 1. *Let E be a set of equations and R and S be rewrite systems such that R/E quasi-commutes over S/E. Then $(R \cup S)/E$ terminates if and only if R/E and S/E both do.*

The relation R/E quasi-commutes over S/E if and only if $\rightarrow_S \circ \rightarrow_{R/E}$ is contained in $\rightarrow_{R/E} \circ \overset{*}{\rightarrow}_{(R \cup S)/E}$. This condition is slightly weaker than quasi-commutation of R/E over S.

PROPOSITION 2. (Jouannaud and Munoz, 1984) *Let R/E be an equational rewrite system such that R quasi-commutes over E. Then R terminates if and only if R/E does.*

Again, linearity may be used to advantage.

THEOREM 3. *Suppose E is linear, R is left-linear, and S is right-linear. If there is no overlap between a right-hand side of S and a left-hand side of R or either side of an equation in E, then*

$(R \cup S)/E$ terminates if and only if R/E and S both do.

Example 2. *(Distributive lattices)* Let R be

$$(x \cap y) \cup z \quad \to \quad (x \cup z) \cap (y \cup z)$$

S be

$$\begin{array}{rcl} x \cap (x \cup y) & \to & x \\ x \cup x & \to & x \\ x \cap x & \to & x \end{array}$$

and E be

$$\begin{array}{rcl} x \cup (y \cup z) & = & (x \cup y) \cup z \\ x \cup y & = & y \cup x \\ x \cap (y \cap z) & = & (x \cap y) \cap z \\ x \cap y & = & y \cap x \end{array}$$

E is linear, R is left-linear, and S contains only variables on the right-hand side. By the above theorem, $(R \cup S)/E$ terminates if S and R/E both do. Termination of S is trivial, since every rule in S is length-decreasing. To prove termination of R/E one can, for example, use a polynomial interpretation τ, where $\tau_{\cup}$ is $\lambda xy.x{*}y$ and $\tau_{\cap}$ is $\lambda xy.x+y+1$.

4. Transformation

The notion of well-foundedness suggests the following straightforward method of proving termination (Manna and Ness, 1970, and Lankford, 1975). Given a rewrite system R, find a well-founded ordering $>$ on terms, such that

$s \to_R t$ implies $s > t$, for all terms s and t.

It is frequently convenient to separate the well-founded ordering $>$ into two parts: a *termination function* τ that maps terms in $\mathcal{T}$ to a set $\mathcal{W}$, and a "standard" well-founded ordering $\succ$ on $\mathcal{W}$. We will consider, in this section, mappings τ, called *transforms*, that map terms into terms and can be represented by a canonical rewrite system T. That is, τ maps a term t to its (unique) T-normal form t^*. We denote by $T!$ the rewrite system consisting of all rules $t \to t^*$. We assume that the ordering $\succ$ is a reduction ordering, and thus may also be characterized by some (possibly infinite) rewrite system S. We will next present termination methods that are based on certain commutation properties of S and T.

Convention. From now on we will use the symbols R, R^* and R^+ to ambiguously denote the relations $\to_R$, $\xrightarrow{*}_R$ and $\xrightarrow{+}_R$, respectively.

Definition 3. A rewrite system R is *reducing relative to S and T* if it is contained in $T^* \circ S \circ (T^*)^{-1}$ (see Fig. 2).

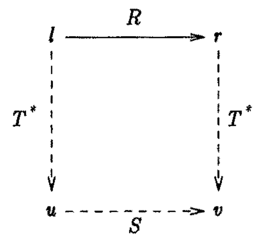


Fig. 2

THEOREM 4. *Let R, S, and T be rewrite systems such that T is canonical, S terminates, and S and T! commute. If R is reducing relative to S and T, then $R/T^{\leftrightarrow}$ terminates.*

Proof. Suppose that $R/T^{\leftrightarrow}$ is not terminating. Then there is an infinite sequence $t_1 \longrightarrow_R t_2 \overset{*}{\leftrightarrow}_T t_3 \longrightarrow_R t_4 \overset{*}{\leftrightarrow}_T \cdots$. Using the facts that R is reducing, T is canonical, and S and $T!$ commute, we can construct an infinite sequence $u_1 \longrightarrow_S u_2 \longrightarrow_S u_3 \longrightarrow_S \cdots$ as shown in Fig. 3.

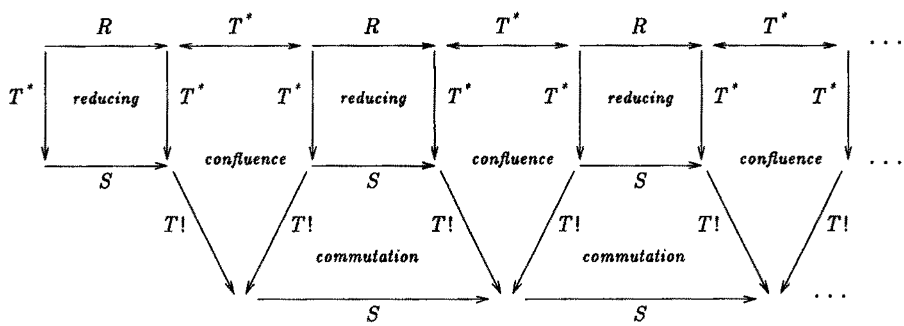


Fig. 3

This contradicts the fact that S is terminating. □

COROLLARY 1. *Let R, S, T, and T' be rewrite systems such that T is canonical, S terminates, and S and $T!$ commute. If T' is contained in $T^{\leftrightarrow}$ and R is reducing relative to S and T, then R/T' terminates.*

For termination proofs *symbolic interpretations* of operators are often useful. These consist of a single rewrite rule $f(x_1, \ldots, x_n) \longrightarrow t[x_1, \ldots, x_n]$, where t is a term containing all variables $x_1, \ldots, x_n$, but not containing f. Such transforms are obviously canonical. They may be used, for instance, to declare two operators equivalent (for the purpose of proving termination). The *T-normalized version* R_T of R consists of all rewrite rules $l^* \longrightarrow r^*$, where l^* and r^* are T-normal forms of l and r, respectively, for some rule $l \longrightarrow r$ is in R.

Lemma 4. *Let R be a rewrite system, T be a symbolic interpretation, and R_T be the T–normalized version of R. Then R is reducing relative to R_T and T, and R_T^+ and $T!$ commute.*

Proof. That R is reducing relative to R_T and T follows immediately from the definition of R_T. To prove commutation of R_T^+ and $T!$ we show that, for all rules $l \rightarrow r$ in R_T, $u[l\sigma] \rightarrow_{R_T} u[r\sigma]$ implies $l' \rightarrow_{R_T} r'$, where l' and r' are T–normal forms of $u[l\sigma]$ and $u[r\sigma]$, respectively. These normal forms may be obtained by first applying T in the substitution part of σ, and then applying further reduction steps in the context u. That is, $u[l\sigma] \rightarrow_T^* u[l\rho] \rightarrow_{T!} v[l\rho, \ldots, l\rho] = l'$ and, similarly, $u[r\sigma] \rightarrow_T^* u[r\rho] \rightarrow_{T!} v[r\rho, \ldots, r\rho] = r'$. Obviously, $l' \rightarrow_{R_T}^+ r'$. □

Combining Corollary 1 and Lemma 4, we obtain

PROPOSITION 3. *Let R and T' be rewrite systems and T be a symbolic interpretation and suppose that T' is contained in $T^{\leftrightarrow}$. Then R/T' is terminating if R_T is.*

Example 3. Let R be

$$\begin{array}{rcl} g(x,y) & \rightarrow & h(x,y) \\ h(f(x),y) & \rightarrow & f(g(x,y)) \end{array}$$

We use the first rule as a transform T and let R' be the second rule. The T–normalized version $R_T{}'$ of R' is

$$h(f(x),y) \quad \rightarrow \quad f(h(x,y))$$

$R_T{}'$ terminates, since it decreases the summed length of all the terms with outermost operator h. By Proposition 3, this implies termination of R'/T. Since T is terminating, so is $R = R' \cup T$.

"Local" commutation of S and T in general does not imply commutation of S and $T!$, but only commutation of S and T^*. If S/T terminates, then a commutation property may be used that can be established by a local test.

Lemma 5. *Suppose that T is canonical and S/T terminates. Then $(S/T)^+$ and T^* commute, if $\leftarrow_T \circ \rightarrow_S$ is contained in $\rightarrow_{S/T}^+ \circ \leftarrow_T^*$.*

Proof. By Noetherian induction on $S \cup T$. Note that $S \cup T$ is Noetherian, since both T and S/T are. □

Again linearity is useful for establishing commutation. A rewrite rule $l \rightarrow r$ is *non–annihilating* if every variable appearing in l also appears in r.

Lemma 6. *Let S and T be rewrite systems. If T is left–linear and non–annihilating and there is no overlap between left–hand sides of S and T, then $\leftarrow_T \circ \rightarrow_S$ is contained in $\rightarrow_{S/T}^+ \circ \leftarrow_T^*$.*

Proof. Suppose that $c \leftarrow_T t \rightarrow_S d$. We distinguish three cases.

a) If the two reduction steps apply at disjoint positions, i.e. $u[r,l'] \leftarrow_T u[l,r] \rightarrow_S u[l,r']$, then $u[r,l'] \rightarrow_S u[r,r'] \leftarrow_T u[l,r']$.

b) If the S–reduction step applies in the variable part of the T–reduction step, i.e. $v[l, \ldots, l] \leftarrow_T u[l] \rightarrow_S u[r]$, then $v[l, \ldots, l] \rightarrow_S^+ v[r, \ldots, r] \leftarrow_T u[r]$ (there has to be at least one S–reduction step, since T is non–annihilating).

c) If the T–reduction step applies in the variable part of the S–reduction step, i.e.

$u[r] \leftarrow_T u[l] \rightarrow_S v[l, \ldots, l]$, then we have $u[r] \rightarrow_S v[r, \ldots, r] \overset{*}{\leftarrow}_T v[l, \ldots, l]$. □

THEOREM 5. *Let R, S, and T be rewrite systems such that T is canonical, S/T terminates, and $(S/T)^+$ and T^* commute. If R is reducing relative to S/T and T, then $R/T^{\leftrightarrow}$ terminates.*

Proof. The same as the proof of Theorem 4, except that instead of S we have S/T, and instead of $T!$ we have T^*. □

Example 4. Let R be the following rewrite system for computing the factorial function (Kamin and Levy, 1980):

$$\begin{array}{rcl} f(s(x)) & \rightarrow & f(p(s(x))) \\ f(0) & \rightarrow & s(0) \\ p(s(x)) & \rightarrow & x \end{array}$$

We use the last rule as a transform T and let R' be $R-T$. T is length-decreasing, hence terminating. The T-normalized version $R_T{}'$ of R' is

$$\begin{array}{rcl} f(s(x)) & \rightarrow & f(x) \\ f(0) & \rightarrow & s(0) \end{array}$$

$R_T{}' \cup T$ is terminating, since each rule either decreases the length of a term, or maintains the length and decreases the number of occurrences of f. Also, since T is linear, non-annihilating, and does not overlap with left-hand sides of $R_T{}'$, the relations $(R_T{}'/T)^+$ and T^* commute. By Theorem 5, R'/T is terminating, which, together with termination of T, implies termination of R.

The termination methods outlined above may also be applied to equational rewrite systems R/E by using transforms T such that E is contained in $T^{\leftrightarrow}$.

Suppose I consists of the axioms for identity, $f(x,e)=x$ and $f(e,x)=x$. Let T_I be the transform $\{f(x,e) \rightarrow x, f(e,x) \rightarrow x\}$. This transform is canonical. Given a rewrite system R, let $R_I{}'$ consist of all rules $u \rightarrow v$, where u and v are T_I-normal forms of $l\sigma$ and $r\sigma$, respectively, $l \rightarrow r$ is in R, and σ is a substitution such that $x\sigma$ is either x or e, for all variables x. If $l \rightarrow r$ is in $R_I{}'$, and $x\sigma$ is either x or e, then $l' \rightarrow r'$ is also in $R_I{}'$, where l' and r' are T_I-normal forms of $l\sigma$ and $r\sigma$, respectively. Let R_I contain $R_I{}'$ and, in addition, for every rule $e \rightarrow r$ in $R_I{}'$, where $r \neq e$, rules $x \rightarrow f(x,r)$ and $x \rightarrow f(r,x)$; for every rule $l \rightarrow e$ in $R_I{}'$, where $l \neq e$, rules $f(x,l) \rightarrow x$ and $f(l,x) \rightarrow x$; and the rule $x \rightarrow x$, if $e \rightarrow e$ is in $R_I{}'$ (the additional rules are necessary for commutation of R_I and T_I). If R is finite, so is R_I.

Lemma 7. *Let R be a rewrite system and T_I and R_I be as defined above. Then R is reducing relative to T_I and R_I, and R_I and $T_I!$ commute.*

Proof. That R is reducing relative to T_I and R_I follows from the definition of R_I. For commutation, it suffices to show that, for all rules $l \rightarrow r$ in R_I and all terms c and substitutions σ, $u \rightarrow_{R_I} v$, where u and v are T_I-normal forms of $c[l\sigma]$ and $u[r\sigma]$, respectively. Without loss of generality, we may assume that c and σ are irreducible in T_I. Let σ' be a substitution such that $x\sigma'$ is e, if $x\sigma$ is e, and $x\sigma'$ is x, otherwise. The assertion can be easily shown if $l \rightarrow r$ is not in $R_I{}'$. If $l \rightarrow r$ is in $R_I{}'$, then, by the remark above, $l' \rightarrow r'$ is in $R_I{}'$, where l' and r' are T-normal forms of $l\sigma'$ and $r\sigma'$, respectively. Since $\sigma=\sigma'\circ\rho$, for some substitution ρ, we obtain $l\sigma\rightarrow_{T_I!}l'\rho$ and $r\sigma\rightarrow_{T_I!}r'\rho$. Since c, $l'\rho$, and $r'\rho$ are irreducible in T_I, are irreducible in T_I, the assertion can be easily established. □

PROPOSITION 4. *An equational system R/I terminates if and only if R_I terminates.*

Proof. The if–direction follows from Lemma 7. The only–if–direction holds because R_I is contained in R/I. □

The requirement—in the theorems above—that the transform T be canonical may be somewhat relaxed. We say that a rewrite system R is *confluent modulo E* if, for all terms s, t, u, and v with $u\overset{*}{\leftarrow}_R s\overset{*}{\leftrightarrow}_E t\overset{*}{\rightarrow}_R v$ there exist terms u' and v' such that $u\overset{*}{\rightarrow}_R u' \overset{*}{\leftrightarrow}_E v'\overset{*}{\leftarrow}_R v$.

Lemma 8. (Huet, 1980) *Let R be a terminating rewrite system. Then R is confluent modulo E if and only if, for all terms s and t, $s\overset{*}{\leftrightarrow}_{E\cup R}t$ implies $s\rightarrow_{R!}\circ\overset{*}{\leftrightarrow}_E\circ\leftarrow_{R!}t$.*

In other words, if R is terminating and confluent modulo E, then two terms are equivalent in $E\cup R$ if and only if their respective R–normal forms are equivalent in E.

THEOREM 6. *Let R, S, and T be rewrite systems and E be an equational theory. Suppose that T is terminating and confluent modulo E, S/E is terminating, and S and T! commute. If R is reducing relative to S and T, then $R/(E\cup T^{\leftrightarrow})$ terminates.*

Proof. Let $t_1\rightarrow_R t_2\overset{*}{\leftrightarrow}_{E\cup T} t_3\rightarrow_R t_4\overset{*}{\leftrightarrow}_{E\cup T}\cdots$ be an infinite sequence. Under the given assumptions, an infinite sequence of S/E reduction steps can be constructed as follows:

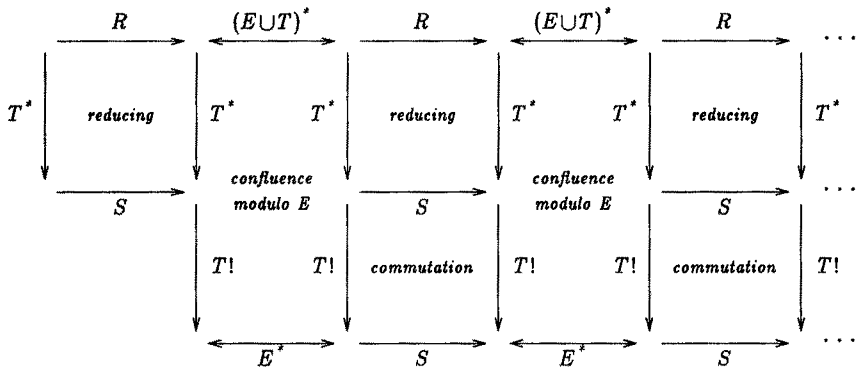


Fig. 4

□

COROLLARY 2. *Let R, S, and T be rewrite systems and E be an equational theory. Suppose that T is terminating and confluent modulo E, $(S/T)/E$ is terminating, and $(S/T)^+$ and T^* commute. If R is reducing relative to S/T and T, then $R/(E\cup T^{\leftrightarrow})$ terminates.*

Recall that Lemma 5 provides a local test for commutation of $(S/T)^+$ and T^*. In the next section we consider particular transforms in depth.

5. Transforms Based on Distributivity and Associativity

Equational rewrite systems R/E, where E is a set of associativity and commutativity axioms, are of particular importance in practice. We will apply the transformation techniques outlined above to the termination problem for such systems (*AC termination*).

Let f be some operator symbol in F. An *associativity axiom* for f is an equation of the form $f(x,f(y,z))=f(f(x,y),z)$ or $f(f(x,y),z)=f(x,f(y,z))$, a *commutativity axiom* is an equation of the form $f(x,y)=f(y,x)$. An equational rewrite system R/E is called *associative-commutative* if E contains only associativity and commutativity axioms. From now on let AC denote a set of associativity and commutativity axioms for which any associative operator is also commutative and vice versa. We say that f *is in* AC to indicate that f is an associative-commutative operator.

Let $>$ be an ordering, called a *precedence ordering*, on the set of operator symbols F. We define the rewrite relation RPO recursively as follows:

a) $f(\cdots s \cdots) \rightarrow_{RPO} s$,
b) $f(\cdots s \cdots) \rightarrow_{RPO} f(\cdots s_1 \cdots s_n \cdots)$, if $s \rightarrow_{RPO} s_i$, for $1 \le i \le n$,
c) $s=f(s_1, \ldots, s_n) \rightarrow_{RPO} g(t_1, \ldots, t_k)$, if $f > g$ and $s \rightarrow_{RPO} t_i$, for $1 \le i \le k$.

The *recursive path ordering* $>_{rpo}$ associated with $>$ is the transitive closure $\rightarrow^+_{RPO}$ of $\rightarrow_{RPO}$.

Lemma 9. (Dershowitz, 1982) *Let $>$ be a precedence ordering on the set of operator symbols F. Then $>_{rpo}$ is well-founded if and only if $>$ is well-founded.*

Recall that a reduction ordering $>$ is *compatible* with AC if $s \overset{*}{\leftrightarrow}_{AC} u > v \overset{*}{\leftrightarrow}_{AC} t$ implies $s>t$, for all terms s, t, u, and v. A rewrite system R/AC terminates if and only if there is a reduction ordering $>$ that is compatible with AC, such that $l \rightarrow_R r$ implies $l>r$. Unfortunately, many reduction orderings are not compatible with AC. For instance, the recursive path ordering $>_{rpo}$ is not: if f is in AC and $a >_{rpo} b$, then

$$f(a,f(b,b)) \leftrightarrow_{AC} f(f(a,b),b) >_{rpo} f(a,f(b,b)),$$

but $f(a,f(b,b)) >_{rpo} f(a,f(b,b))$ is false.

We will design a *transform* T such that, for some set of equations E, (a) T is terminating and confluent modulo E, (b) AC is contained in $E \cup T^{\leftrightarrow}$, (c) $(S/T)/E$ is terminating, and (d) $(S/T)^+$ and T^* commute. For S we will use the recursive path ordering, restricted to terms irreducible in T. For E we use the *permutation congruence* $\sim$, which is the smallest stable congruence, such that $f(X,u,Y,v,Z) \sim f(X,v,Y,u,Z)$. If property (a) is satisfied then T-irreducible terms are unique up to equivalence in E and may serve as representatives for AC-equivalence classes. A natural choice for such a canonical representation are "flattened" terms. Let L be the rewrite system consisting of all reduction rules (on varyadic terms) of the form $f(X,f(Y),Z) \rightarrow f(X,Y,Z)$, where f is in AC, Y denotes a sequence of variables $y_1, \ldots, y_n$ of length $n \ge 2$, and X and Z are sequence of variables of length k and l, respectively, where $k+l \ge 1$. For example, $f(x,f(y,z)) \rightarrow f(x,y,z)$ is a "flattening rule", but $f(f(x)) \rightarrow f(x)$ is not.

Terms irreducible in L are called *flattened*.

Lemma 10. *The rewrite system L is canonical, $L/\sim$ is terminating, and AC is contained in $\sim \cup L^{\leftrightarrow}$.*

Any recursive path ordering $>_{rpo}$ contains L and is compatible with the permutation congruence $\sim$. Therefore $(RPO/L)/\sim$ is terminating. Unfortunately, the commutation property (d) is not satisfied, as the following example illustrates: if f is in AC and $f>g$, then $f(a,b) \to_{RPO} g(a,b)$ and

$$f(a,b,c) \leftarrow_L f(f(a,b),c) \to_{RPO} f(g(a,b),c).$$

Both $f(a,b,c)$ and $f(g(a,b),c)$ are flattened, but $f(g(a,b),c) \to_{RPO} f(a,b,c)$. However, if the transform T contains, in addition to L, the rewrite rule $f(g(x,y),z) \to g(f(x,z),f(y,z))$, then

$$f(a,b,c) \to_{RPO} g(f(a,c),f(b,c)) \leftarrow_T g(f(a,b),c).$$

Let $>$ be a well-founded precedence ordering. A *distributivity rule* for f and g is a rewrite rule of the form

$$f(X,g(Y),Z) \to g(f(X,y_1,Z), \cdots, f(X,y_n,Z)),$$

where Y is a sequence $y_1, \ldots, y_n$ of length $n \geq 1$, $f>g$, and neither f nor g are constants. For example, $x^*(y+z) \to x^*y+x^*z$ and $-(x+y) \to (-x)+(-y)$ are distributivity rules. Such sets of distributivity rules are terminating (they are contained in $>_{rpo}$) but not canonical, in general. For example, if f distributes over both g and h, then the term $f(g(x),h(y))$ can be transformed to two different terms, $g(h(f(x,y)))$ or $h(g(f(x,y)))$. To guarantee that properties (a)-(d) above are satisfied, we have to impose certain restrictions on sets of distributivity rules.

Let F_D be a set of non-constant operator symbols f containing all AC operators. Let D be the set of all distributivity rules for f and g, where f and g are in F_D and $f>g$. The rewrite system $T = L \cup D$, where L consists of all flattening rules for operators in F_D, is called the *A-transform* corresponding to $>$ and F_D. Let F' be $F-\{c\}$, if c is minimal among all constants, or F, if there is no such constant.

Definition 4. A precedence ordering $>$ satisfies the *associative path condition* for F_D, if F_D can be partitioned into two sets $\{f_1, \ldots, f_n\}$ and $\{g_1, \ldots, g_m\}$, such that $n \leq m$ and

a) g_i is minimal in F', for $1 \leq i \leq m$,

b) $f_i > g_i$, for $1 \leq i \leq n$,

c) f_i is minimal in $F' - \{g_i\}$, for $1 \leq i \leq n$.

For example, if f, g, h and i are in F_D, then the precedence orderings shown in Figs. 5(a) and 5(b) do not satisfy the associative path condition, but the ordering in Fig. 5(c) does.

Lemma 11. *Let $>$ be a precedence ordering that satisfies the associative path condition, T be the corresponding A-transform, and S be the corresponding rewrite system consisting of all pairs $l \to r$ such that $l >_{rpo} r$ and l and r are irreducible in T. Then*

a) T is terminating and confluent modulo $\sim$,

b) AC is contained in $E \cup T^{\leftrightarrow}$,

c) $(S/T)/\sim$ is terminating, and

d) $(S/T)^+$ and T^* commute.

Sketch of proof. Part (b) follows from Lemma 10. The recursive path ordering $>_{rpo}$ contains both S and T and is compatible with the permutation congruence $\sim$. Therefore $(S/T)/\sim$ is terminating. For confluence T modulo $\sim$ it suffices to prove $c \xrightarrow{*}_T s \sim t \xleftarrow{*}_T d$, for all "critical overlaps" $c \leftarrow_T u \rightarrow_T d$ or $c \leftarrow_T u \sim d$. The restrictions on the precedence ordering $>$ are essential for the proof of this confluence property.

By Lemma 5, $(S/T)^+$ and T^* commute if, for all terms s, t, and u with $s \leftarrow_T u \rightarrow_S t$, there exist terms v and w, such that $s \xrightarrow{*}_T v \rightarrow_S w \xleftarrow{*}_T$. This is implied by the following two properties:

(i) *Monotonicity.* If $l \rightarrow r$ is in S, then, for any term c, $l' \xrightarrow{+}_S r'$, where l' and r' are T–normal forms of $c[l]$ and $c[r]$, respectively.

(ii) *Stability.* If $l \rightarrow r$ is in S, then, for any substitution σ, $l' \xrightarrow{+}_S r'$, where l' and r' are T–normal forms of $l\sigma$ and $r\sigma$, respectively.

Both properties can be proved by induction on the length of l and r. □

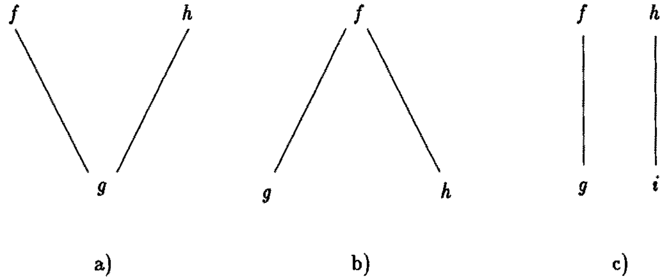


Fig. 5

Definition 5. Let T be the A–transform corresponding to some precedence ordering $>$. The *associative path ordering* $>_{apo}$ is defined by:

$s >_{apo} t$ *if and only if,* $s^* >_{rpo} t^*$,

where s^* and t^* are T–normal forms of s and t, respectively.

Summarizing the results above we have the following theorems for AC termination.

THEOREM 7. *If $>$ is a well-founded precedence ordering that satisfies the associative path condition, then the corresponding associative path ordering $>_{apo}$ is a reduction ordering and is compatible with AC.*

THEOREM 8. *Let $>$ be a precedence ordering that satisfies the associative path condition and T be the corresponding A-transform. Suppose that T' is contained in $T^{\leftrightarrow}$. If $l >_{apo} r$, for every rule $l \rightarrow r$ in R, then $R/(T' \cup AC)$ terminates.*

Transformation techniques for AC termination were first suggested by Dershowitz, et al. (1983). The associative path ordering described above is simpler than the ordering given by Bachmair and Plaisted (1985). In particular, Theorem 7 implies that

if $s >_{apo} t$, *then* $s\sigma >_{apo} t\sigma$, *for any substitution* σ.

This "lifting lemma" allows efficient implementations of the associative path ordering based on the recursive path ordering. The A-transform may also be used in combination with a lexicographic path ordering. More precisely, operators that are not in AC may be given lexicographic status, i.e. some positions in a term may be given more significance than others (see Kamin & Levy, 1980). A-transforms may be extended to include symbolic interpretations of non-AC operators. That is, the results above also hold for transforms $T=T_1 \cup T_2$, where T_1 is an A-transform corresponding to a precedence ordering $>$ and a set of operator symbols F_D, and T_2 consists of a single rule $f(x_1, \ldots, x_n) \rightarrow t[x_1, \ldots, x_n]$, where f is not in F_D.

Example 5. *(Boolean algebra).* The following canonical rewrite system for boolean algebra is due to Hsiang (1985). We outline a termination proof using an associative path ordering. R consists of the following rules:

$$\begin{array}{rcl}
x \oplus false & \rightarrow & x \\
x \wedge false & \rightarrow & false \\
x \wedge true & \rightarrow & x \\
x \wedge x & \rightarrow & x \\
(x \oplus y) \wedge z & \rightarrow & (x \wedge z) \oplus (y \wedge z) \\
x \oplus x & \rightarrow & false \\
x \vee y & \rightarrow & (x \wedge y) \oplus (x \oplus y) \\
x \supset y & \rightarrow & (x \wedge y) \oplus (x \oplus true) \\
x \equiv y & \rightarrow & (x \oplus y) \oplus true \\
\neg x & \rightarrow & x \oplus true
\end{array}$$

The operators $\oplus$ and $\wedge$ are in AC. Let $>$ be the precedence ordering shown in the Hasse diagram in Fig. 6, and T be the A-transform corresponding to $>$ and $F_D=\{\wedge,\oplus\}$, extended by a symbolic interpretation $\{false \rightarrow true\}$. The fifth rule of R is a distributivity rule and is placed in T'. Let R' be $R-T'$. Since $l >_{apo} r$, for all rules $l \rightarrow r$ in R', we may conclude, by Theorem 8, that $R'/(T' \cup AC)$ terminates. The system T'/AC also terminates (see Example 2), which implies termination of $R/AC=(R' \cup T')/AC$.

Example 6. *(Modules).* Let A be an associative-commutative ring with identity. An A-module M over A is an algebraic structure consisting of operations $\oplus: M \times M \rightarrow M$ and $\cdot: A \times M \rightarrow M$, such that $(M,\oplus)$ is an abelian group (the identity of the group is denoted by Ω, the inverse to $\oplus$ by I) and the following identities hold: $\alpha \cdot (\beta \cdot x)=(\alpha * \beta) \cdot x$, $1 \cdot x = x$, $(\alpha+\beta) \cdot x=(\alpha \cdot x)(\beta \cdot x)$ and $\alpha \cdot (xy)=(\alpha \cdot x)(\alpha \cdot y)$. For the sake of readability we use Greek letters for variables ranging over elements of A, and Roman letters for variables ranging over elements of M. The following rewrite system R was obtained with the rewrite rule laboratory RRL (see Kapur & Sivakumar, 1984):

$$
\begin{array}{rcl}
\alpha+0 & \longrightarrow & \alpha \\
\alpha+(-\alpha) & \longrightarrow & 0 \\
-0 & \longrightarrow & 0 \\
-(-\alpha) & \longrightarrow & \alpha \\
-(\alpha+\beta) & \longrightarrow & (-\alpha)+(-\beta) \\
\alpha*(\beta+\gamma) & \longrightarrow & (\alpha*\beta)+(\alpha*\gamma) \\
\alpha*0 & \longrightarrow & 0 \\
\alpha*(-\beta) & \longrightarrow & -(\alpha*\beta) \\
\alpha*1 & \longrightarrow & \alpha \\
x\oplus\Omega & \longrightarrow & x \\
\alpha\cdot(\beta\cdot x) & \longrightarrow & (\alpha*\beta)\cdot x \\
1\cdot x & \longrightarrow & x \\
(\alpha+\beta)\cdot x & \longrightarrow & (\alpha\cdot x)\oplus(\beta\cdot x) \\
\alpha\cdot(x\oplus y) & \longrightarrow & (\alpha\cdot x)\oplus(\alpha\cdot y) \\
(-\alpha\cdot x)\oplus(\alpha\cdot x) & \longrightarrow & \Omega \\
(-1\cdot x)\oplus x & \longrightarrow & \Omega \\
0\cdot x & \longrightarrow & \Omega \\
\alpha\cdot\Omega & \longrightarrow & \Omega \\
I(x) & \longrightarrow & (-1)\cdot x
\end{array}
$$

The operators $+$, $*$, and $\oplus$ are in AC. To prove termination of R/AC we use the associative path ordering corresponding to the precedence ordering $>$ shown in the Hasse diagram in Fig. 7. The operator $\cdot$ has lexicographic status (right to left). Let T' consist of the sixth and eighth rule, and R' be $R-T'$. Then T' is contained in the A-transform T corresponding to $>$. Since $l >_{apo} r$, for all rules $l \longrightarrow r$ in R', $R'/(T' \cup AC)$ is terminating. Termination of T'/AC can be proved separately, which implies termination of R/AC.

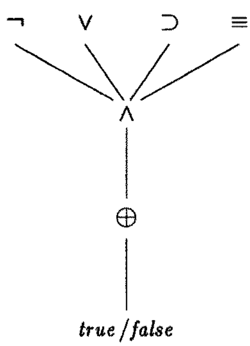


Fig. 6

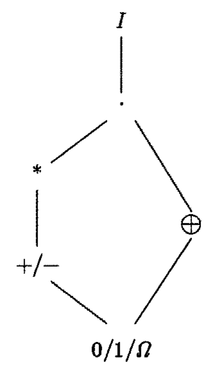


Fig. 7

A-transforms may also be used for proving termination of ordinary rewrite systems.

Example 7. *(Associativity and endomorphism).* Let R be the following rewrite system (Ben Cherifa and Lescanne, 1985):

$$\begin{array}{rcl} (x\cdot y)\cdot z & \longrightarrow & x\cdot(y\cdot z) \\ f(x)\cdot f(y) & \longrightarrow & f(x\cdot y) \\ f(x)\cdot(f(y)\cdot z) & \longrightarrow & f(x\cdot y)\cdot z \end{array}$$

Let T' be the first rule of R and R' be $R-R'$. Since T' is terminating, R terminates if R'/T' terminates. Let T be the A-transform corresponding to a precedence ordering $>$, where f is smaller than $\cdot$ and f and $\cdot$ are in F_D. Then we have $l >_{apo} r$, for both rewrite rules $l \longrightarrow r$ in R'. Since T' is contained in $T^{\leftrightarrow}$, R'/T' is terminating.

6. Summary

We have presented termination methods based on commutation properties, and have developed an abstract framework for describing transformation techniques. These general results have led us to the development of various particular transforms, including methods for proving termination of equational rewrite systems R/E, where E contains associativity, commutativity, and identity axioms. It should be possible to automate, to a certain degree, the process of developing transforms for certain classes of rewrite systems by using a "completion-like" procedure as suggested by Jouannaud and Munoz (1984).

References

[1] Bachmair, L., and Plaisted, D.A. (1985). Termination orderings for associative-commutative rewriting systems, *J. of Symbolic Computation 1,* 329–349.

[2] Ben Cherifa, A., and Lescanne, P. (1985). A method for proving termination of rewriting systems based on elementary computations on polynomials, unpublished manuscript.

[3] Dershowitz, N. (1981). Termination of linear rewriting systems, *Proc. 8th EATCS Int. Colloquium on Automata, Languages and Programming,* S. Even and O. Kariv, eds., Lect. Notes in Comp. Science 115, New York, Springer, 448–458.

[4] Dershowitz, N. (1982). Orderings for term-rewriting systems, *Theoretical Computer Science 17,* 279–301.

[5] Dershowitz, N. (1985a). Computing with rewrite systems, *Information and Control 64,* 122–157.

[6] Dershowitz, N. (1985b). Termination. *Proc. 1st Int. Conf. on Rewriting Techniques and Applications,* Dijon, France, Lect. Notes in Comp. Science, Springer, 180–224.

[7] Dershowitz, N., Hsiang, J., Josephson, N.A., and Plaisted, D.A. (1984). Associative-commutative rewriting. *Proc. 8th IJCAI,* Karlsruhe, 940–944.

[8] Guttag, J.V., Kapur, D., and Musser, D.R. (1983). On proving uniform termination and restricted termination of rewriting systems. *SIAM Computing 12,* 189–214.

[9] Hsiang, J. (1985). Refutational theorem proving using term–rewriting systems. *Artificial Intelligence 25,* 255–300.

[10] Huet, G. (1980). Confluent reductions: abstract properties and applications to term rewriting systems. *J. ACM 27,* 797–821.

[11] Huet, G. and Hullot, J.M. (1982). Proofs by induction in equational theories with constructors. *J. of Comp. and System Sciences 25,* 239–266.

[12] Jouannaud, J.–P., and Munoz, M. (1984). Termination of a set of rules modulo a set of equations, *Proc. 7th Int. Conf. on Automated Deduction,* R. Shostak, ed., Lect. Notes in Comp. Science 170, Berlin, Springer, 175–193.

[13] Kamin, S., and Levy, J.J. (1980). Two generalizations of the recursive path ordering. Unpublished manuscript, Univ. of Illinois at Urbana–Champaign.

[14] Kapur, D., and Sivakumar, G. (1984). Architecture of and experiments with RRL, a rewrite rule laboratory. *Proc. NSF Workshop on the Rewrite Rule Laboratory,* Rensellaerville, New York, 33–56.

[15] Lankford, D.S. (1979). On proving term rewriting systems are noetherian. Memo MTP–3, Mathematics Department, Louisiana Tech. Univ., Ruston, Louisiana.

[16] Manna, Z., and Ness, S. (1970). On the termination of Markov algorithms. *Proc. Third Hawaii Int. Conf. on System Science,* 789–792.

[17] Musser, D.R. (1980). On proving inductive properties of abstract data types. *Proc. 7th ACM Symp. on Principles of Programming Languages,* Las Vegas, 154–162.

[18] O'Donnell, M.J. (1985). *Equational logic as a programming language.* MIT Press, Cambridge, Massachusetts.

[19] Plaisted, D.A. (1984). Associative path orderings, *Proc. NSF Workshop on the Rewrite Rule Laboratory,* Rensellaerville, New York, 123–126.

[20] Raoult, J.C., and Vuillemin, J. (1980). Operational and semantic equivalence between recursive programs, *J. ACM 27,* 772–796.

[21] Rosen, B. (1973). Tree–manipulating systems and Church–Rosser theorems, *J. ACM 20,* 160–187.