Rewrite Systems
Spring 1997
Course Notes

N. Dershowitz

May 19, 2010

1 Introduction

Definition 1 (Rewrite System) *A rewrite system is a set of ordered equations.*

Example 1 (Insertion Sort)

$$\begin{array}{rcl}
max(0,x) & \rightarrow & x \\
max(x,0) & \rightarrow & x \\
max(s(x),s(y)) & \rightarrow & s(max(x,y)) \\
min(0,x) & \rightarrow & 0 \\
min(x,0) & \rightarrow & 0 \\
min(s(x),s(y)) & \rightarrow & s(min(x,y)) \\
sort(nil) & \rightarrow & nil \\
sort(cons(x,y)) & \rightarrow & insert(x,sort(y)) \\
insert(x,nil) & \rightarrow & cons(x,nil) \\
insert(x,cons(y,z)) & \rightarrow & cons(max(x,y),insert(min(x,y),z))
\end{array}$$

A *substitution* σ is a mapping $\{x_1 \mapsto t_1, \ldots, x_n \mapsto t_n\}$ of variables x_i to terms t_i. If t is a term and σ a substitution, then $t\sigma$ is t with all occurrences of the variables x_i replaced by t_i.

We say that s *rewrites to* t is s has a subterm $l\sigma$ that is an instance of a left-hand side l of a rule $l \rightarrow r$, and t is s with that instance $l\sigma$ replaced by $r\sigma$. We write $s \rightarrow t$ for one step of rewriting and $s \rightarrow^* t$ for finitely many.

We say that t is a *normal form* of s if $s \rightarrow^* t$ but t cannot be rewritten.

2 Confluence

Definition 2 (Termination) *A relation* $\rightarrow$ *is* terminating *if there are no endless derivations* $t_1 \rightarrow t_2 \rightarrow \cdots$.

This implies that every term has a normal form.

Definition 3 (Confluence) *A relation* $\rightarrow$ *is* confluent *if* $s \rightarrow^* v$ *and* $t \rightarrow^* v$, *for some* v, *whenever if* $u \rightarrow^* s$ *and* $u \rightarrow^* t$, *for some* u.

This implies that every term has at most one normal form.

Definition 4 (Church-Rosser Property) *A relation* $\rightarrow$ *is* Church-Rosser *if* $s \rightarrow^* v$ *and* $t \rightarrow^* v$, *for some* v, *whenever if* $s \leftrightarrow^* t$.

Theorem 1 *A relation is Church-Rosser iff it is confluent.*

Definition 5 (Local Confluence) *A relation* $\rightarrow$ *is* locally confluent *if* $s \rightarrow^* v$ *and* $t \rightarrow^* v$, *for some* v, *whenever if* $u \rightarrow s$ *and* $u \rightarrow t$, *for some* u.

Theorem 2 (Diamond Lemma) *A terminating relation is Church-Rosser iff it is locally confluent.*

Theorem 3 *A rewrite system is locally confluent if no left-hand side unifies with a non-variable subterm of any left-hand side (with its variables renamed).*

3 Termination

A partial ordering is *well-founded* if it allows no infinite descending sequences.

Definition 6 (Reduction Ordering) *A* reduction ordering $>$ *is a well-founded ordering such that* $s > t$ *implies* $f(\ldots, s, \ldots) > f(\ldots, t, \ldots)$, *for all* f.

Theorem 4 *A rewrite system terminates if* $l\sigma \succ r\sigma$, *for all rules* $l \rightarrow r$, *and ground substitutions* σ, *for some reduction ordering* $\succ$.

Definition 7 (Lexicographic Ordering) *We say that* $\langle a_1, \ldots, a_m \rangle$ *is* lexicographically *greater than* $\langle b_1, \ldots, b_n \rangle$ *if, for some* i, a_i *is greater than* b_i, *and* a_j *is equal (or equivalent) to* b_j *for all* $j < i$. *If* $i > m$ *(*$j > n$*), we take* $a_i = 0$ *(*$b_j = 0$*).*

Definition 8 (Multiset Ordering) *We say that a (finite) multiset* $\{a_1, \ldots, a_m\}$ *is greater than a multiset* $\{b_1, \ldots, b_n\}$ *if* $m > 0$ *and* $n = 0$ *or if* a_1 *is greater than each of* $b_1, \ldots, b_i$, *for some* i, *and* $\{a_2, \ldots, a_n\}$ *is greater than* $\{b_{i+1}, \ldots, b_n\}$. *Multisets are unordered, but multiplicity of elements matters.*

Theorem 5 *Lexicographic and multiset orderings are well-founded if the orderings on elements are.*

Definition 9 (Recursive Path Ordering) *Let* $\succ$ *be a well-founded partial ordering of function symbols and constants and let some function symbols have "lexicographic status" and the rest "multiset status". The* recursive path ordering $\succ_{rpo}$ *defined as follows:*

$$s = f(\ldots, s_i, \ldots) \succ_{rpo} g(\ldots, t_j, \ldots) = t$$

if either

1. *some* $s_i \succ_{rpo} t$, *or* $s_i = t$ *(up to reordering of arguments of multiset symbols), or*
2. *if* $s \succ_{rpo} t_1, \ldots, t_n$ *and one of the following holds:*
   (a) $f > g$;
   (b) $f = g$ *is lexicographic and* $\langle \ldots, s_i, \ldots \rangle$ *is lexicographically greater than* $\langle \ldots, t_j, \ldots \rangle$;
   (c) $f = g$ *is multiset and* $\{\ldots, s_i, \ldots\}$ *is multiset greater than* $\{\ldots, t_j, \ldots\}$.

Theorem 6 *The recursive path ordering is a reduction ordering.*

4 Critical Pairs

Definition 10 (Critical Pair) *If* $l \to r$ *and* $s \to t$ *are two rewrite rules (with variables made distinct),* p *is the position of a non-variable subterm of* s, *and* μ *is a most general unifier of* $s|_p$ *and* l, *then the equation* $t\mu = s\mu[r\mu]_p$ *is a critical pair formed from those rules.*

Definition 11 (Rewrite Proof) *A* rewrite proof *of $s = t$ is a derivation $s \rightarrow^* \leftarrow^* t$.*

Theorem 7 (Critical Pair Lemma) *A rewrite system is locally confluent iff all its critical pairs have rewrite proofs.*

A system is *left-linear* if no variable appears more than once on a left-hand side.

Definition 12 (Orthogonality) *A rewrite system is* orthogonal *if it is left-linear and has no critical pairs.*

Theorem 8 *Orthogonal systems are confluent.*

Theorem 9 *If s has a normal form t with respect to an orthogonal system, then outermost-fair rewriting of s will result in t.*

5 Completion

Definition 13 (Encompassment) *The encompassment ordering $\rhd$ is such that $s \rhd t$ if a subterm of s is an instance of t, but not vice-versa.*

Definition 14 (Reduced System) *A system R is reduced if, for each rule $l \rightarrow r$ in R, the right-hand side r is irreducible (i.e. is in R-normal-form) and if $l' \lhd l$, for the left-hand side l, then l' is irreducible (i.e. the proper subterms of l are in normal form, as is any term that is more general than l).*

Definition 15 (Canonical System) *A rewrite system that is confluent, terminating, and reduced is called* canonical.

Theorem 10 (Uniqueness) *Suppose R and S are two canonical (but not necessarily finite) rewrite systems having the same normal forms. Suppose further that the combined system $R \cup S$ is terminating. Then R and S must be same (up to renaming of variables).*

"Ordered rewriting" means using either side of an equation to rewrite, but only in the direction that reduces the term it is applied to in a given ordering.

Definition 16 (Complete Simplification Ordering) *A reduction ordering $>$ is called a complete simplification ordering if (1) it has the subterm property $f(\ldots, s, \ldots) > s$ and (2) it is total on ground (variable-free) terms, that is, if for any two distinct ground terms u and v, either $u > v$ or $v > u$.*

Definition 17 (Ordered Critical Pair) *Given a reduction ordering $\succ$, if $l = r$ and $s = t$ are two (not necessarily distinct) equations (with variables distinct), p is the position of a non-variable subterm of s, μ is a most general unifier of $s|_p$ and l, and $s\mu$ is sometimes (that is, for some complete simplification ordering that extends $\succ$ and for some ground substitution) larger than both $t\mu$ and $s\mu[r\mu]_p$, then the equation $t\mu = s\mu[r\mu]_p$ is an ordered critical pair formed from those rules.*

Let $\succ$ be a reduction ordering that can be extended to a complete simplification ordering, and let $\rhd$ be the encompassment ordering. An equation $l = r$ can be used to simplify another equation $s[l\sigma] = t$ (to $s[r\sigma] = t$) provided $s[l\sigma] \succ s[r\sigma]$ or $s \rhd l$. Ordered completion may be described as follows:

> Let E be a set of equations. Repeat the following steps forever (in any order):
>
> - Add new ordered critical pairs to E.
> - Use E to simplify equations in E.
> - Remove any equation in E whose reduced sides are identical.

This procedure, given

$$\begin{array}{rclcrcl} x \cdot 1 & = & x & & x \cdot y & = & y \cdot x \\ x \cdot (y \cdot z) & = & (x \cdot y) \cdot z & & x \cdot x^- & = & 1 \end{array}$$

and a lexicographic path ordering, will generate

$$\begin{array}{rcl@{\qquad}rcl} 1^- & \to & 1 & x \cdot y & \leftrightarrow & y \cdot x \\ x \cdot 1 & \to & x & x \cdot (y \cdot z) & \leftrightarrow & y \cdot (x \cdot z) \\ 1 \cdot x & \to & x & (x \cdot y) \cdot z & \to & x \cdot (y \cdot z) \\ (x^-)^- & \to & 1 & x \cdot (x^- \cdot z) & \to & z \\ x \cdot x^- & \to & 1 & (y \cdot x)^- & \to & x^- \cdot y^- \end{array}$$

(Those equations that can only be used to rewrite in one direction are given as rules.) Using an "Ordered Critical Pair Lemma," it can be shown that ordered rewriting with this system has the confluence property.

In general, with fairness (no persisting ordered critical ignored forever), a rewrite proof between two ground terms s and t will eventually be generated from a starting set of equations E iff $s \leftrightarrow_E^* t$. Thus, the word problem in arbitrary equational theories can always be semidecided by ordered completion.

Furthermore, ordered completion must succeed in generating a canonical set of rules whenever one exists for the given reduction ordering $\succ$, provided $\succ$ can be extended to a complete reduction ordering. For example, if $f \succ c \succ a$, ordered completion produces the following sequence of equations.

$$b = c,\ f(b) \rightarrow a,\ d \rightarrow b,\ f(c) \rightarrow c$$
$$b = c,\ f(c) = a,\ f(b) \rightarrow a,\ d \rightarrow b,\ f(c) \rightarrow c$$
$$b = c,\ c = a,\ f(b) \rightarrow a,\ d \rightarrow b,\ f(c) \rightarrow c,\ f(c) \rightarrow a$$
$$f(a) \rightarrow a,\ b \rightarrow a,\ c \rightarrow a,\ d \rightarrow a$$

6 Term-Rewriting Induction

For ground-convergent systems R, any equation between distinct R-normal forms is considered to be *inconsistent* with R. The observation that an equation $s = t$ is true for all *ground* instances iff no inconsistency follows from $R \cup \{s = t\}$ is the basis of the *proof by consistency* method of inductive theorem proving. If there exists a ground-convergent system R', with the same ground normal forms as R, and which has the same equational theory as $R \cup \{s = t\}$, then inconsistency is precluded. If R and R' are both ground convergent and every left-hand side of one system is ground reducible by the other then they have the same inductive theorems.

Definition 18 (Ground Reducibility) *For any rewrite system R, a term s is ground reducible, if all its ground instances $s\gamma$ are rewritable.*

Theorem 11 *If R is finite, ground reducibility is decidable.*

For example, let R be the following canonical system for interleaving stacks:

$$\begin{aligned} alternate(\Lambda, z) &\rightarrow z \\ alternate(push(x, y), z) &\rightarrow push(x, alternate(z, y)) \end{aligned}$$

and suppose we wish to prove that $alternate(y, \Lambda) = y$ is an inductive theorem. This equation can be oriented from left to right. Since the critical pairs $\Lambda = \Lambda$ and $push(x, y) = push(x, alternate(\Lambda, y))$ are provable by rewriting, completion ends with the system $R' = R \cup \{alternate(y, \Lambda) \rightarrow y\}$. Since the left-hand side $alternate(y, \Lambda)$ of the new rule is ground R-reducible, for all ground terms y made up of Λ, *push*, and *alternate*, the theorem holds. In more complicated cases, additional lemmata may be generated along the way.

Definition 19 (Cover Set) *A* cover set *S for an ordering $\succ$ and set of equations E is such that every ground term t is equal (by the axioms in E) to an instance of a term in S which is no larger in the ordering $\succ$ than t.*

For any given rewrite system R, we use the ordering $\succ_R$ on equations that is (possibly an extension of) the transitive closure of the union of the rewriting relation of R and taking subterms of the sides of the equation.

Definition 20 (Term-Rewriting Induction) *Let R be a rewrite system and C be a cover set for $\succ_R$.* Term rewriting induction *is the rule of inference which allows one to conclude that an equation $s = t$ is true for all* ground *substitutions of its variables, by showing that $s\sigma_i = t\sigma_i$, for each substitution σ_i in C, follows (equationally) from R and instances $s\tau = t\tau$ of the hypothesis that are smaller (under $\succ_R$) than the case in question.*

The requirement that the cover set instances be smaller than the ground term is necessary: Suppose we have the rules

$$\begin{array}{rcl} f(f(x)) & \rightarrow & f(x) \\ f(g(x)) & \rightarrow & g(x) \\ g(f(x)) & \rightarrow & f(x) \\ g(g(x)) & \rightarrow & g(x) \\ a & \rightarrow & b \end{array}$$

and want to prove $f(x) = g(x)$ and were allowed to use a cover set $\{a, f(a), g(a)\}$. Then we could prove $f(a) = g(a)$ from the smaller instance $f(b) = g(b)$. (An appropriate cover set would have b instead of a.)