Canonical Sets of Horn Clauses*

Nachum Dershowitz
Department of Computer Science
University of Illinois
1304 West Springfield Avenue
Urbana, IL 61801, U.S.A.
email: nachum@cs.uiuc.edu

1 Background

Rewrite rules are oriented equations used to replace equals-by-equals in the specified direction. Input terms are repeatedly rewritten according to the rules. When and if no rule applies, the resultant *normal form* is considered the value of the initial term. If no infinite sequences of rewrites is possible, a rewrite system is said to have the *termination* property. *Confluence* of a rewrite system is a property that ensures that no term has more than one normal form. A *convergent* rewrite system is one with both the confluence and termination properties.

Let $\mathcal{T}$ be a set of (first-order) terms, with variables taken from a set $\mathcal{X}$, and $\mathcal{G}$ be its subset of *ground* (variable-free) terms. If t is a term in $\mathcal{T}$, by $t|_\pi$ we signify the subterm of t rooted at position π and by $t[s]_\pi$ (or simply $t[s]$) we denote t with its subterm $t|_\pi$ replaced by a term s. We use the following notations for equational deduction: $s \simeq t$ stands for the usual sense of equality in logical systems; $s \leftrightarrow_e t$ (or just $s \leftrightarrow t$) denotes one step of replacement of equals for equals (using equation e); $s \rightarrow_R t$ (or just $s \rightarrow t$) stands for one replacement according to the orientation of a rewrite rule (in R); $s \rightarrow^* t$, for any number (including zero) of rewrites; $s \leftrightarrow t$ also stands for one rewrite step in either direction. Two terms s and t are said to be *joinable* if there is a term v such that $s \rightarrow^* v \leftarrow^* t$, or $s \downarrow t$ for short. For convergent R, an identity $s \simeq t$ holds in the theory defined by R (each rule viewed as an equation) if and only if the normal forms of s and t are identical. Thus, validity of equations is decidable for finite convergent R, since the joinability ($\downarrow$) relation is decidable. A *ground convergent* rewrite system is one that terminates and defines *unique* normal forms for all ground terms. Ground convergent systems can be used to decide validity by skolemizing s and t and reducing to normal form. For a survey of the theory of rewriting, see [Dershowitz and Jouannaud, 1990].

A *conditional equation* is a universally-quantified (definite) Horn clause in which the only predicate symbol is equality. We write such a clause in the form $e_1 \wedge \cdots \wedge e_n \Rightarrow s \simeq t$ ($n \geq 0$), meaning that equality $s \simeq t$ holds whenever all the antecedent equations e_i, hold. The term s will be called the *left-hand side*; t is the *right-hand side*; and the e_i are the *conditions*. If $n = 0$, then the (positive unit) clause will be called an *unconditional equation*. Conditional equations are important for specifying abstract data types and expressing logic programs with equations.

A *conditional (rewrite) rule* is an equational implication in which the equation in the consequent ($s \simeq t$) is oriented. To give operational semantics to such a system, the conditions under which a rewrite may be performed need to made precise. The most popular convention (see [Dershowitz and Okada, 1990]) for conditional rewriting is that the terms in each condition be

*This research supported in part by the National Science Foundation under Grant CCR-9007195.

joinable. Thus, a rule $u_1 \simeq v_1 \wedge \cdots \wedge u_n \simeq v_n \Rightarrow l \rightarrow r$, is applied to a term t containing an instance $l\sigma$ of the left-hand side, if $u_i\sigma \downarrow v_i\sigma$ for each condition $u_i \simeq v_i$, in which case $t[l\sigma] \rightarrow t[r\sigma]$. We call sets of such rules *(standard) conditional rewrite systems*; they provide an applicative programming language with especially clean syntax and semantics, and can be extended to logic programming paradigms. The ground normal forms of ground convergent conditional systems form an initial algebra for the underlying system of conditional equations. In fact, a first-order theory admits initial term models if and only if it is a universal Horn theory (see [Makowsky, 1985]). In this sense, (ground convergent) conditional rewriting implements the initial-algebra semantics for operations constrained by conditional equations.

One of the basic results in (unconditional) rewriting is the Critical Pair Lemma [Knuth and Bendix, 1970], which states that confluence of (finite) terminating systems can be effectively tested by checking joinability of a finite set of equations, called "critical pairs", formed by overlapping left-hand sides. In the conditional case, we propose the following definition: Let $\succ$ be some partial ordering on ground terms with the "replacement" property, $s \succ t$ implies $u[s] \succ u[t]$ for all contexts $u[\cdot]$. We write $s \succ t$ for nonground terms if $s\sigma \succ t\sigma$ for all ground substitutions σ and $s \not\succ t$ if $s\sigma \not\succ t\sigma$ for some σ. If $p \Rightarrow l \simeq r$ and $q \Rightarrow u \simeq v$ are conditional equations, then the conditional equation $p\mu \wedge q\mu \Rightarrow u\mu[r\mu]_\pi \simeq v\mu$ is an *(ordered) conditional critical pair* if l unifies via most general unifier $(mgu)\,\mu$ with a nonvariable subterm $u|_\pi$ of u, $u\mu \not\prec v\mu, u\mu[r\mu]_\pi$, and also $u\mu \not\prec p\mu, q\mu$ (meaning that $u\mu$ is not smaller than *any* side of an instantiated condition in $p\mu$ or $q\mu$). It was shown in [Dershowitz *et al.*, 1987] that there exists a terminating conditional rewrite system all critical pairs of which are joinable, but which is not confluent. On the other hand, when the conditional system is such that recursively evaluating the conditions also terminates, the critical pair condition suffices. More precisely, we say that a conditional system is *decreasing* if there exists a well-founded extension $\succ$ of $\rightarrow$ (in other words, rewriting always reduces terms in the ordering) with two additional requirements: $\succ$ has the "subterm" property (each term is greater under $\succ$ than its proper subterms) and conditions for rule application are smaller than the term that gets rewritten (for each rule $c \Rightarrow l \rightarrow r$ and substitution σ, $u[l\sigma] \succ c\sigma$). For such decreasing systems, all the basic notions are decidable, i.e., the rewrite relation, joinability relation, and normal form attribute are all recursive. Decreasing systems generalize the concept of "hierarchy" in [Rémy and Zhang, 1984], and are slightly more general than the "simplifying" and "reductive" systems considered in [Kaplan, 1987] and [Jouannaud and Waldmann, 1986], respectively. In fact, it can be shown [Dershowitz and Okada, 1990] that decreasing systems exactly capture the finiteness of recursive evaluation of terms. Thus, they are ideal for most computational purposes.

It is well known that any conditional equational theory is expressible as a set of universally quantified Horn clauses (in which the equality symbol is uninterpreted), since the axioms of equality are themselves Horn. Thus, positive-unit resolution, or any other variation of resolution that is complete for Horn clauses, could be used to prove theorems in equational Horn theories, but the cost of treating equality axioms like any other clause is prohibitively high. For this reason, special inference mechanisms for equality, notably paramodulation [Robinson and Wos, 1969], have been devised. In recent years, term orderings have been proposed as an appropriate tool with which to restrict paramodulation. On the flip side, any Horn theory can be expressed as an unconditional equational theory. Some of the implications of this correspondence are explored in Section 2.

In [Knuth and Bendix, 1970], it was suggested that a nonconfluent unconditional system be "completed" by adding new rules (according to some user-supplied partial ordering) whenever a critical pair fails the joinability test. When this process succeeds, a finite set of equations is obtained from which all theorems follow by rewriting. Completion, as defined in [Knuth and Bendix, 1970] and studied in [Huet, 1981], fails when a critical pair, after its two sides have

been reduced to normal form, is neither trivial nor orientable by the ordering supplied to the procedure for this purpose. Completion was first extended to conditional equations by Kaplan [1987]. Equations are turned into rules only if they satisfy a decreasingness condition. The problem is that the critical pair of two decreasing rules can easily be nondecreasing. Ganzinger [1987] suggested narrowing the conditions of nondecreasing rules. Like standard completion, both these methods may fail on account of inability to form new rules. In Section 3, we extend these methods—analogous to unfailing ordered completion (as described in [Bachmair *et al.*, 1989])—to provide an ordering-based theorem-proving method.

As in [Hsiang and Rusinowitch, 1986; Kounalis and Rusinowitch, 1987; Zhang and Kapur, 1988; Rusinowitch, 1989; Bachmair and Ganzinger, 1990; Nieuwenhuis and Orejas, 1990; Dershowitz, 1991], our goal in developing theorem proving procedures is to minimize the amount of paramodulation, while maximizing the amount of simplification, without threatening completeness thereby. Orderings are used to choose which literals participate in a paramodulation step, and which side of an equality literal to use. Our method also allows for (almost unrestricted) simplification (demodulation) by directed decreasing equations. It requires less paramodulation and offers more simplification than [Kounalis and Rusinowitch, 1987], for example. For our completeness proofs, we adapt the proof-ordering method of [Bachmair *et al.*, 1986; Bachmair and Dershowitz, to appear] to conditional proofs (using an ordering that is much simpler than the one in [Ganzinger, 1987]).

A *reduced* rewrite system is one such that each right-hand side is in normal form, as are proper generalizations and proper subterms of all left-hand sides. (For convergent systems, this is equivalent to the definition in [Huet, 1981] which requires that left-hand sides not be rewritable by other rules.) Reduced convergent systems are called *canonical* in [Dershowitz and Jouannaud, 1990]. If two canonical systems have the same equational theory and are contained in the same well-founded ordering, then they must be literally similar (i.e. the same except for variable renamings). This important result was first mentioned in [Butler and Lankford, 1980]. It means that all implementations of (standard) completion must yield the same system, given the same inputs E and $\succ$, provided they use the *encompassment* relation [Dershowitz and Jouannaud, 1990] for simplification of rules. In our view, simplification in completion is intimately related to reduction: by striving to find *the* unique reduced convergent systems, necessary simplifications are illumed. To guide the choice of simplification strategies for conditional completion, we develop, in Section 4, a notion of reduced conditional system, and look for an appropriate uniqueness result. Only in circumstances that ensure that a convergent system will be found whenever there is one, do we consider it reasonable to refer to a conditional inference mechanism as "completion", rather than "theorem proving".

2 Horn theories

We begin our discussion with Horn clauses not containing (interpreted) equality symbols. Any Horn clause $p_1 \wedge \cdots \wedge p_n \Rightarrow q$ is logically equivalent to (the equivalence) $p_1 \wedge \cdots \wedge p_n \wedge q \equiv p_1 \wedge \cdots \wedge p_n$. Since the left-hand side is longer than the right, we view this as a terminating unconditional rewrite rule $p_1 \wedge \cdots \wedge p_n \wedge q \rightarrow p_1 \wedge \cdots \wedge p_n$, with the order of conjuncts left intact. Let H be a set of Horn clauses and $\rightarrow$ be the corresponding rewrite relation. The completeness of selected positive-unit (SPU) resolution means, in this framework, that, for an arbitrary conjunction P of atoms, $H \vdash P$ by first-order reasoning if and only if $P \rightarrow^* (T \wedge \cdots \wedge T)$ can be derived from rules generated in the following manner:

From $p \wedge s \wedge q \rightarrow p \wedge s$ and $p' \rightarrow T$, where atoms p and p' are unifiable with most general unifier μ, q is any atom, and s is any conjunction of atoms, infer $s\mu \wedge q\mu \rightarrow s\mu$. When s is empty, this is $q\mu \rightarrow T$.

For example, from the two Horn clauses

$$\begin{aligned} p(a) &\rightarrow T \\ p(x) \wedge p(f(x)) &\rightarrow p(x) \end{aligned}$$

all $p(f^i(a)) \rightarrow T$ are generated, one after the other.

The above inference rule is sufficient for completeness, but our goal is to allow as much simplification as possible. In particular, given a rule $p \wedge q \rightarrow q$, or even $p \wedge r \rightarrow r$, we are tempted to simplify a clause like $p \wedge q \wedge r \equiv p \wedge r$ to $q \wedge r \equiv p \wedge r$. The problem is that the latter has sides of equal length, and cannot, in general, be oriented into a rule (e.g. if p is $x < y$ and q is $y < x$). Hence, adding simplification would lead to incompleteness of this inference mechanism.

To recover completeness, we need inferences that apply to more general equivalences between conjunctions. The idea is to apply the ordered completion method for unconditional equations in [Hsiang and Rusinowitch, 1987; Bachmair *et al.*, 1989; Dershowitz and Jouannaud, 1990] to these equivalences. There is no need to use Boolean identities (hence no need for associative-commutative unification), since reasoning equationally with these equivalences suffices; the only Boolean rule needed is $T \wedge x \rightarrow x$. This results in a better method than the one in [Bachmair *et al.*, 1989] for Horn clauses, since more simplification is possible. Additional optional simplification strategies may be incorporated in this theorem proving strategy, just as long as they are sound and do not make more complex proofs necessary (cf. Section 3).

A total ordering $>$ on ground terms $\mathcal{G}$ is called a *complete simplification ordering* if it has (a) the replacement property, $s > t$ implies $u[s] > u[t]$ for all contexts $u[\cdot]$, and (b) the subterm property, $t \geq t|_\pi$ for all subterms $t|_\pi$ of t. Such a ground-term ordering must be a well-ordering [Dershowitz, 1982]. A *completable simplification ordering* on all terms $\mathcal{T}$ (cf. [Hsiang and Rusinowitch, 1987]) is a well-founded *partial* ordering $\succ$ that (c) can be extended to a complete simplification ordering $>$ on ground terms, such that (d) $s \succ t$ implies that $s\sigma > t\sigma$ for all ground substitutions σ. Furthermore, we will assume that (e) the (truth) constants T and F are minimal in $\succ$. Of course, the empty ordering is completable, as are the polynomial and path orderings commonly used in rewrite-based theorem provers (see [Dershowitz, 1987]). By results in [Bachmair *et al.*, 1989], providing ordered completion with a completable simplification ordering is guaranteed to succeed in finding a canonical system for the given theory, if one exists that is compatible with the given ordering.

Ordered completion—with simplification—is likewise guaranteed to derive a contradiction from Horn clauses H and the Skolemized negation of an atomic formula p such that $H \vdash p$. The point is that the only Boolean equation used (implicitly) in the above SPU-mimicking inference rule is $T \wedge x \simeq x$, from which it follows that the equational representation of H (plus this Boolean equation) provides an equational proof of $p \simeq T$. The completeness of ordered completion for equational reasoning [Bachmair *et al.*, 1989] means that the contradiction $F \simeq T$ will be generated from these equations plus $\hat{p} \simeq F$, where $\hat{p}$ is p with its variables replaced by Skolem constants.

Rather than give the general case (which is no different from ordinary ordered completion—except that associative-commutative matching can, but need not, be used when simplifying one rule via another), we show here how simplification provides, in the propositional case, a quadratic algorithm to convert a set of ground Horn clauses to a unique representation in the form of a (unconditional) canonical rewrite system. Given any well-ordering of atoms, define a

well-ordering $\rhd$ on conjunctions under which longer conjunctions are bigger, and equal-length ones are compared lexicographically. The algorithm operates on Horn clauses expressed as equivalences:

> *Repeat the following, until no longer possible: Choose the equivalence $p \equiv q$ (or $q \equiv p$) that has not yet been considered such that q is minimal among all sides vis-a-vis the total ordering $\rhd$. If all the atoms in p occur together on one side r of any other equivalence $r \equiv s$ (or $s \equiv r$), remove them from r and merge what is left in r with the atoms in q. Delete duplicate atoms and occurrences of the constant T (unless T is the only atom) from all equivalences. Discard equivalences with identical sides and duplicate equivalences.*

For example, the first clause of

$$p \wedge q \equiv p,\ p \wedge q \equiv q,\ p \wedge q \wedge r \equiv p \wedge q$$

rewrites the others (assuming $p < q < r$) to $q \equiv p$ and $p \wedge r \equiv p$. Then, the first becomes $p \wedge p \equiv p$ and is deleted, leaving the Horn clauses $p \Rightarrow q$, $q \Rightarrow p$, and $p \Rightarrow r$.

This algorithm is based on the completion-based congruence closure method in [Lankford, 1975], shown to be doable with low polynomial time complexity in [Gallier *et al.*, 1988]. By the theorem in [Lankford and Ballantyne, 1983] for uniqueness of canonical associative-commutative rewriting systems, it results in a unique set of equivalences, determined by the ordering $\rhd$. The resultant system can be used to decide satisfiability in the given propositional Horn theory, though not as fast as in [Dowling and Gallier, 1984]. The equivalences can optionally be converted back to Horn form.

3 Completion

In this section, we turn to Horn clauses with equality, that is, to conditional equational theories. For efficiency, it is unreasonable to just add axioms of equality and use Horn-clause theorem-proving methods. Instead, we develop an unfailing completion procedure for conditional equations, based on the incomplete method in [Ganzinger, 1987]. (Complete, ordering-based theorem-proving methods for such theories include [Kounalis and Rusinowitch, 1987; Dershowitz, 1991].) The allowable inferences are a stringent restriction of paramodulation. A user-supplied ordering $\succ$ is used to guide the inference mechanism, so that only maximal terms are used in any inference step. When $\succ$ is the empty ordering, the method reduces to "special" paramodulation, in which the functional-reflexive axioms are not needed and paramodulation into variables is not performed (see [Lankford, 1975]). Most important, a nonempty ordering allows conditional equations that are simplifiable to be replaced without compromising (refutational) completeness. Hence, the power of the method, both in minimizing possible inferences and maximizing potential simplifications, is brought to bear by employing orderings that are more complete than the empty one. The method is like the one in [Bertling, 1990], but we give a specific strategy for simplification.

Given a set E of conditional equations, a *proof* in E of an equation $u \simeq v$ is a sequence of terms $u = t_1 \leftrightarrow t_2 \leftrightarrow \cdots \leftrightarrow t_n = v$ $(n \geq 1)$, each step $t_k \leftrightarrow t_{k+1}$ of which is *justified* by an appropriate conditional equation in E, position in t_k, substitution for variables in the equation, and subproofs for each of its conditions. Steps employing an unconditional equation do not have subproofs as part of their justification. Any equation $s \simeq t$ that is valid for E is amenable to such an equational proof. Note that a conditional equation $e_1 \wedge \cdots \wedge e_n \Rightarrow s \simeq t$ is valid for E if

and only if $s \simeq t$ is valid for $E \cup \{e_1, \cdots, e_n\}$. Hence, proving validity of conditional equations reduces to proving validity of unconditional ones.

We write $u \rightarrow_e v$ (with respect to a partial ordering $\succ$), if $u \leftrightarrow_e v$ using an instance $p \Rightarrow s \simeq t$ of e, and $u \succ v, p$ (by which we mean that u is bigger than v and bigger than both sides of each condition in p). A conditional equation may have some ground instances that are decreasing in the complete ordering (if $s > t, p$), and others that are not decreasing. The Critical Pair Lemma of [Kaplan, 1987] for decreasing systems can be adapted to ground confluence of decreasing systems:

> *Let E be a set of conditional equations and $\succ$ a completable simplification ordering. If all ground instances of ordered conditional critical pairs rewrite, under $\rightarrow_E$, to the identical term, then the system is ground confluent.*

However, a counterexample in [Dershowitz *et al.*, 1987] shows that this critical pair condition is insufficient when rewriting by nondecreasing instances of equations is included.

We formulate our theorem-proving procedure as an inference system operating on a set of conditional equations, and parameterized by a completable ordering $\succ$. The rules may be classified into three "expansion" rules and four "contraction" rules. The contraction rules of standard completion significantly reduce its space requirements, but they make proofs of completeness much more subtle.

The first expansion rule generates critical pairs from clauses that may have decreasing instances:

$$\frac{E \cup \left\{ \begin{array}{l} p \Rightarrow l \simeq r, \\ q \Rightarrow u \simeq v \end{array} \right\}}{E \cup \left\{ \begin{array}{c} p \Rightarrow l \simeq r, \\ q \Rightarrow u \simeq v, \\ p\mu \wedge q\mu \Rightarrow u\mu[r\mu]_\pi \simeq v\mu \end{array} \right\}} \quad \text{if} \quad \left\{ \begin{array}{l} u|_\pi \notin \mathcal{X} \\ \mu = mgu(u|_\pi, l) \\ u\mu \not\succ p\mu, q\mu, v\mu, u\mu[r\mu]_\pi \end{array} \right. \tag{A}$$

Superposition (i.e. oriented paramodulation of positive equational literals) is performed only at nonvariable positions ($u|_\pi \notin \mathcal{X}$). Only positive equations are used in this rule, and only in a decreasing direction ($u\mu \not\succ p\mu, q\mu$). Of course, if the relation $\not\succ$ is not known precisely, one must be conservative and apply the inference whenever it cannot be guaranteed that all ground instances of $u\mu$ are larger than the corresponding instances of $p\mu$, $q\mu$, $v\mu$, and $u\mu[r\mu]$. Either side of an equation may be used for superposition, but only if, in the context of the paramodulation, it is (believed to be) potentially the largest term involved ($u\mu \not\succ v\mu, u\mu[r\mu]_\pi$). (This can probably be strengthened a bit to require $l\mu \not\succ p\mu$ instead of $u\mu \not\succ p\mu$.) Now and henceforth, when a rule refers to a clause of the form $q \Rightarrow u \simeq v$, an unconditional equation ($u \simeq v$) is also intended.

We need, additionally, a rule that applies decreasing equations to negative literals:

$$\frac{E \cup \left\{ \begin{array}{rcl} p & \Rightarrow & l \simeq r, \\ q \wedge s \simeq t & \Rightarrow & u \simeq v \end{array} \right\}}{E \cup \left\{ \begin{array}{rcl} p & \Rightarrow & l \simeq r, \\ q \wedge s \simeq t & \Rightarrow & u \simeq v, \\ p\mu \wedge q\mu \wedge s\mu[r\mu]_\pi \simeq t\mu & \Rightarrow & u\mu \simeq v\mu \end{array} \right\}} \quad \text{if} \quad \left\{ \begin{array}{l} s|_\pi \notin \mathcal{X} \\ \mu = mgu(s|_\pi, l) \\ s\mu \not\succ p\mu, q\mu, t\mu, s\mu[r\mu]_\pi \end{array} \right. \tag{B}$$

Whenever this or subsequent rules refer to a conditional equation like $q \wedge s \simeq t \Rightarrow u \simeq v$, the intent is that $s \simeq t$ is any one of the conditions and s is either side of it.

The last expansion rule in effect resolves a maximal negative literal with reflexivity of equals ($x \simeq x$):

$$\frac{E \cup \left\{ \begin{array}{rcl} q \wedge s \simeq t & \Rightarrow & u \simeq v \end{array} \right\}}{E \cup \left\{ \begin{array}{rcl} q \wedge s \simeq t & \Rightarrow & u \simeq v, \\ q\mu & \Rightarrow & u\mu \simeq v\mu \end{array} \right\}} \quad \text{if} \quad \left\{ \begin{array}{l} \mu = mgu(s,t) \\ s\mu \not\prec q\mu \end{array} \right. \tag{C}$$

The four contraction rules all simplify the set of conditional equations. The first two eliminate trivial equations:

$$\frac{E \cup \left\{ \begin{array}{rcl} q & \Rightarrow & u \simeq u \end{array} \right\}}{E} \tag{D}$$

$$\frac{E \cup \left\{ \begin{array}{rcl} q \wedge s \simeq s & \Rightarrow & u \simeq v \end{array} \right\}}{E \cup \left\{ \begin{array}{rcl} q & \Rightarrow & u \simeq v \end{array} \right\}} \tag{E}$$

The last two use decreasing clauses to simplify other clauses. One simplifies conditions; the other applies to the equation part. In both cases, the original clause is *replaced* by a version that is equivalent but strictly smaller under $\succ$.

$$\frac{E \cup \left\{ \begin{array}{rcl} p & \Rightarrow & u \simeq v \end{array} \right\}}{E \cup \left\{ \begin{array}{rcl} q & \Rightarrow & u \simeq v \end{array} \right\}} \quad \text{if} \quad p \rightarrow_E q \tag{F}$$

In simplifying equations, we utilize an extension of the encompassment ordering $\rhd$ from terms to clauses (in which terms are larger than proper subterms and smaller than proper instances): Terms are compared with $\succ$; equations are compared by comparing the multiset of their two terms in the multiset extension $\succ_{mul}$ of the term ordering (see [Dershowitz and Manna, 1979]); to compare terms with equations we make s bigger than $u \simeq v$ if $s \succ u, v$; finally, $q \Rightarrow u \simeq v \rhd p \Rightarrow l \simeq r$ if $q \succ_{mul} p$, or $q =_{mul} p$ (i.e. $q = p$ as multisets) and $u \rhd l$ in the encompassment ordering, or $q =_{mul} p$, $u = l$, and $v \succ r$.

$$\frac{E \cup \left\{ \begin{array}{rcl} q & \Rightarrow & u \simeq v \end{array} \right\}}{E \cup \left\{ \begin{array}{rcl} q & \Rightarrow & w \simeq v \end{array} \right\}} \quad \text{if} \quad \left\{ \begin{array}{l} u \rightarrow_e w,\ e \in E \\ q \succ u \vee v \succ u \vee (q \Rightarrow u \simeq v) \rhd e \end{array} \right. \tag{G}$$

Here $q \succ u$ means that there is always one side of one condition in q that is bigger than u; hence, the clause is nondecreasing.

As a simple example, consider the following three clauses:

$$0 < c(0) \simeq T \tag{1}$$

$$c(y) < c(z) \simeq y < z \tag{2}$$

$$c(c(0)) < x \simeq T \Rightarrow c(0) < x \simeq T \tag{3}$$

The first two are decreasing; the third is not. We employ a straightforward ordering (e.g. left-to-right lexicographic path ordering [Kamin and Lévy, 1980; Dershowitz, 1987]). Expansion inference (A) does not apply between (1) and (2), since 0 and $c(y)$ do not unify. By the same token, (B) does not apply between (1) and the condition in (3). Applying (B) between (2) and (3) yields

$$c(0) < x \simeq T \Rightarrow c(0) < c(x) \simeq T$$

which contracts, using (G) and (2), to another nondecreasing clause

$$c(0) < x \simeq T \Rightarrow 0 < x \simeq T \tag{4}$$

Applying (B) to it yields a decreasing clause

$$0 < x \simeq T \quad \Rightarrow \quad 0 < c(x) \quad \simeq \quad T \tag{5}$$

The critical pair obtained by superposing (1) on $0 < c(x)$ gives a trivial equation (contractable by (D)). Since (5) does not unify with the conditions of (3) and (4), we are done. Note that the decreasing rules (1,2,5) reduce any term $c^i(0) < c^j(0)$, such that $i < j$, to T.

A valley proof $s \simeq t$ is one in which the steps take the form $s \downarrow t$. We define a normal-form proof of $s \simeq t$ to be a valley proof in which each subproof is also in normal form and each term in a subproof is smaller than the larger of s and t. Any non-normal-form proof has a peak made from decreasing instances with normal-form subproofs, or has a nondecreasing step with normal-form subproofs, or has a trivial step. We say that a sequence of inferences is *fair* if expansions of all persistent conditional equations have been considered. Formally, that may be expressed as $\mathbf{exp}(E_\infty) \subseteq \cup E_i$, where E_0, E_1, ... is the sequence of conditional equations generated, $E_\infty = \limsup E_j$ is the set of conditional equations that each persist from some E_j on, and $\mathbf{exp}(E_\infty)$ is the set of conditional equations that may be inferred in one expansion step from persisting equations. For a method based on these rules to be complete, we need to show that with enough inferences, any ground theorem eventually has a normal-form proof. Precisely stated:

> *If an inference sequence is fair, then for any proof of $s \simeq t$ in the initial set E_0 of conditional equations, there is a normal-form proof of $s \simeq t$ in the limit E_∞.*

This is a consequence of the following observations: If E' can be inferred from E, then for any proof in E there exists a proof in E' of equal or lesser complexity, and, furthermore, that there are always inferences that can decrease the complexity of non-normal proofs. Complexity may be measured by assigning to each step $s \leftrightarrow t$ in a ground proof or its subproofs the weight $\langle \{q_1\sigma, \ldots, q_n\sigma, s\}, e \rangle$, where e is the conditional equation $q_1 \wedge \cdots \wedge q_n \Rightarrow l \simeq r$ justifying the step, σ is the substitution, and s is the larger of s and t (in the complete simplification ordering $>$ extending $\succ$). Steps are compared in the lexicographic ordering of these pairs. The first components of pairs are compared in the multiset extension of the ordering on equations and terms described above. Second components are compared using $\rhd$. Proofs are compared in the well-founded multiset extension of the lexicographic ordering on steps. We use $\gg$ to denote this proof ordering. It can be shown by standard arguments [Dershowitz and Manna, 1979] that $\gg$ is well-founded.

By induction with respect to $\gg$, the eventual existence of a normal-form proof follows: If P is a non-normal-form proof in E, there exists a proof P', using equations in E and $\mathbf{exp}(E)$, such that the complexity of P is strictly greater (in the proof ordering $\gg$) that that of P'. In particular, trivial steps can be eliminated, reducing complexity by removing elements from the multiset of proof steps. Peaks between decreasing steps will have smaller proofs on account of inference rule (A) and the Critical Pair Lemma. A nondecreasing step $s \rightarrow_e t$ with a decreasing step out of its largest condition $p\sigma$ breaks down into two cases: If the decreasing step $p\sigma \rightarrow q$ is in the nonsubstitution part of $p\sigma$, then an application of rule (B) supplies a new equation that can be used in a step of smaller complexity (since $p\sigma$, which was the largest element of the first component of the complexity of the step $s \rightarrow_e t$, is replaced by q). If the decreasing step takes place in the substitution part, then there is an alternative proof $s \rightarrow^* s' \rightarrow_e t' \leftarrow^* t$, where s and t are rewritten by the same decreasing equation. The new e step is smaller that the old one since its conditions are. Any new steps introduced are smaller than the eliminated cost of $p\sigma \rightarrow q$, since they apply to terms smaller than $p\sigma$. Lastly, a nondecreasing step with trivial subproofs can be replaced after generating a new equation using (C).

The contraction rules were also designed to decrease proof complexity. Thus, any fair sequence of inferences must allow for a simpler proof, and eventually a normal-form proof must persist.

An alternative completion procedure may be based on the fact [Dershowitz *et al.*, 1987] that a system is confluent if all its critical pairs are joinable and are formed from overlaps between left-hand sides at their *topmost* position. In such a procedure, any non-root critical pair would be eliminated by pulling out subterms. For example, the rules $a \rightarrow b$ and $h(f(a)) \rightarrow c$ overlap, but not at the top. To get around that, the second rule can be replaced by the more powerful $x \simeq a \Rightarrow h(f(x)) \rightarrow c$, eliminating the offending pair. Note that interpreting Horn clauses as conditional rules (rewriting predicates to T) gives a system satisfying the above constraint, because predicate symbols are never nested in the head of a clause. Furthermore, all critical pairs are joinable, since all right-hand sides are the same. This also applies to pattern-directed functional languages in which defined functions are not nested on left-hand sides.

4 Uniqueness of Systems

In our view, there is a qualitative difference between theorem proving and completion. As pointed out in [Huet and Oppen, 1980], completion is a compilation-like process; the goal is to find a convergent system that can later be used to prove (a certain class of) theorems effectively. A *theorem prover* is, accordingly, deemed "complete" if it can prove any provable theorem (in the class of theorems under consideration); a *completion procedure*, on the other hand, is "complete" (in the sense of [Dershowitz, 1989]) if it will find a convergent system whenever there is one (for the given ordering). The unit method of [Dershowitz, 1991], for example, should not qualify as a completion procedure for conditional rules, since it may go off producing (perhaps infinitely) many unconditional rules, even when one conditional rule suffices. For example, given the *confluent* system $\{h(f(x)) \rightarrow h(x),\ h(x) = h(a) \Rightarrow g(x) \rightarrow c\}$, it will proceed to add superfluous consequences $g(f^i(a)) \rightarrow c$ (among others).

Suppose R is a convergent (conditional) rewrite system for some theory E and the rewrite relation $\rightarrow_R$ is contained in a partial ordering $\succ$. Then, the normal form of any term t is the element in the E-congruence class of t that is minimal vis-a-vis $\succ$ [Avenhaus, 1986]. Hence, if R and S are two such systems for the same theory E and ordering $\succ$, then R and S have the same normal forms and the same reducibility relation. We say that a term t is *reduced*, with respect to theory E and ordering $\succ$, if, of all elements in its E-congruence class, it is minimal with respect to $\succ$. An unconditional rewrite system is said to be reduced if, for each of its rules, $l \rightarrow r$, the right-hand side r is reduced and all terms s less than l in the encompassment ordering are also reduced. The contraction inference rules for unconditional systems (see [Bachmair *et al.*, 1986]) are themselves "confluent", implying that the same reduced system is obtained regardless of the order in which they are appplied to a given confluent system.

Reduced unconditional systems are unique with respect to $\succ$ in the stronger sense that if R and S are canonical, have the same theory, and their rewrite relations are both contained in $\succ$, then R and S are (essentially) identical (cf. [Butler and Lankford, 1980; Métivier, 1983]). We saw in Section 2 how this gives a unique representation for nonequational Horn clauses. But for conditional systems, reduction is clearly insufficient. For example, the two equivalent rules, $a \simeq b \Rightarrow f(a) \rightarrow c$ and $a \simeq b \Rightarrow f(b) \rightarrow c$, are each convergent and reduced in the above sense. Applying the contraction rules of Section 3 to a set of conditional equations (a process that will of necessity terminate) is not enough for this purpose. One needs, first of all, some sort of "contextual rewriting" (à la [Zhang and Rémy, 1985]) to reduce the left-hand side of the rule so that it contains the smaller of the hypothesized-equal terms a and b. This suggests an additional

inference rule like:

$$\frac{E \cup \left\{ \begin{array}{lcl} q & \Rightarrow & r \end{array} \right\}}{E \cup \left\{ \begin{array}{lcl} q & \Rightarrow & s \end{array} \right\}} \quad \text{if} \quad r \rightarrow_e s,\ e \in \mathcal{T}h(E \cup q) \tag{H}$$

where $\mathcal{T}h(E \cup q)$ is the set of equational consequences of E and q. But even this ineffective rule is insufficient, as can be seen from the following alternatives: $a \simeq b \wedge a \simeq c \Rightarrow f(b) \rightarrow c$ vs. $a \simeq b \wedge a \simeq c \Rightarrow f(c) \rightarrow c$. If $a \succ b, c$, we still need to choose between the minimal terms b and c.

Let $p \Rightarrow l \rightarrow r$ be a conditional rule e in a system R. It is deemed *reduced* if r and all terms smaller than l in the encompassment ordering are reduced with respect to $E \wedge p$, l itself is reduced with respect to $R \cup p - \{e\}$, and there is no logically weaker condition such that l is reducible. Let R and S be two reduced convergent conditional systems for E and $\succ$. If $p \Rightarrow l \rightarrow r$ is in R, then $l \simeq r$ has a proof in $S \cup p$. Even if we could show that l must be a left-hand side of a rule e' in S which must have right-hand side r (a question we leave open), the conditions in e and e' may differ, and additional completion and simplification are required to preclude that. Imagine a rule $p \Rightarrow l \rightarrow r$. To get true uniqueness, one must complete the equations p (modulo any other equations) to find a unique representation (that is, the finite canonical system) for p (if one exists at all). Also, one would want to eliminate conditions of the form $x \simeq t$; otherwise, the conditional rule $x \simeq a \Rightarrow f(x) \rightarrow b$ could be preferred over $f(a) \rightarrow b$.

Acknowledgment

I thank Subrata Mitra and the referees for their comments.

References

[Avenhaus, 1986] Jürgen Avenhaus. On the descriptive power of term rewriting systems. *J. Symbolic Computation*, 2:109–122, 1986.

[Bachmair and Dershowitz, to appear] Leo Bachmair and Nachum Dershowitz. Equational inference, canonical proofs, and proof orderings. *J. of the Association for Computing Machinery*, to appear.

[Bachmair and Ganzinger, 1990] Leo Bachmair and Harald Ganzinger. Completion of first-order clauses with equality. In M. Okada, editor, *Proceedings of the Second International Workshop on Conditional and Typed Rewriting Systems*, Montreal, Canada, June 1990. *Lecture Notes in Computer Science*, Springer, Berlin.

[Bachmair *et al.*, 1986] Leo Bachmair, Nachum Dershowitz, and Jieh Hsiang. Orderings for equational proofs. In *Proceedings of the IEEE Symposium on Logic in Computer Science*, pages 346–357, Cambridge, MA, June 1986.

[Bachmair *et al.*, 1989] Leo Bachmair, Nachum Dershowitz, and David A. Plaisted. Completion without failure. In H. Aït-Kaci and M. Nivat, editors, *Resolution of Equations in Algebraic Structures 2: Rewriting Techniques*, chapter 1, pages 1–30. Academic Press, New York, 1989.

[Bertling, 1990] Hubert Bertling. Knuth-Bendix completion of Horn clause programs for restricted linear resolution and paramodulation. In S. Kaplan and M. Okada, editors, *Extended Abstracts of the Second International Workshop on Conditional and Typed Rewriting Systems*, pages 89–95, Montreal, Canada, June 1990. Revised version to appear in *Lecture Notes in Computer Science*, Springer, Berlin.

[Butler and Lankford, 1980] George Butler and Dallas S. Lankford. Experiments with computer implementations of procedures which often derive decision algorithms for the word problem

in abstract algebras. Memo MTP-7, Department of Mathematics, Louisiana Tech. University, Ruston, LA, August 1980.

[Dershowitz and Jouannaud, 1990] Nachum Dershowitz and Jean-Pierre Jouannaud. Rewrite systems. In J. van Leeuwen, editor, *Handbook of Theoretical Computer Science B: Formal Methods and Semantics*, chapter 6, pages 243–320. North-Holland, Amsterdam, 1990.

[Dershowitz and Manna, 1979] Nachum Dershowitz and Zohar Manna. Proving termination with multiset orderings. *Communications of the ACM*, 22(8):465–476, August 1979.

[Dershowitz and Okada, 1990] Nachum Dershowitz and Mitsuhiro Okada. A rationale for conditional equational programming. *Theoretical Computer Science*, 75:111–138, 1990.

[Dershowitz *et al.*, 1987] Nachum Dershowitz, Mitsuhiro Okada, and G. Sivakumar. Confluence of conditional rewrite systems. In S. Kaplan and J.-P. Jouannaud, editors, *Proceedings of the First International Workshop on Conditional Term Rewriting Systems*, pages 31–44, Orsay, France, July 1987. Vol. 308 of *Lecture Notes in Computer Science*, Springer, Berlin (1988).

[Dershowitz, 1982] Nachum Dershowitz. Orderings for term-rewriting systems. *Theoretical Computer Science*, 17(3):279–301, March 1982.

[Dershowitz, 1987] Nachum Dershowitz. Termination of rewriting. *J. of Symbolic Computation*, 3(1&2):69–115, February/April 1987. Corrigendum: *4*, 3 (December 1987), 409–410.

[Dershowitz, 1989] Nachum Dershowitz. Completion and its applications. In H. Aït-Kaci and M. Nivat, editors, *Resolution of Equations in Algebraic Structures 2: Rewriting Techniques*, chapter 2, pages 31–86. Academic Press, New York, 1989.

[Dershowitz, 1991] Nachum Dershowitz. Ordering-based strategies for Horn clauses. In *Proceedings of the 12th International Joint Conference on Artificial Intelligence*, Sydney, Australia, August 1991. To appear.

[Dowling and Gallier, 1984] William F. Dowling and Jean H. Gallier. Linear-time algorithms for testing the satisfiability of propositional Horn formulae. *J. of Logic Programming*, 1(3):267–284, 1984.

[Gallier *et al.*, 1988] Jean Gallier, Paliath Narendran, David Plaisted, Stan Raatz, and Wayne Snyder. Finding canonical rewriting systems equivalent to a finite set of ground equations in polynomial time. In E. Lusk and R. Overbeek, editors, *Proceedings of the Ninth International Conference on Automated Deduction*, pages 182–196, Argonne, Illinois, May 1988. Vol. 310 of *Lecture Notes in Computer Science*, Springer, Berlin.

[Ganzinger, 1987] Harald Ganzinger. A completion procedure for conditional equations. In S. Kaplan and J.-P. Jouannaud, editors, *Proceedings of the First International Workshop on Conditional Term Rewriting Systems*, pages 62–83, Orsay, France, July 1987. Vol. 308 of *Lecture Notes in Computer Science*, Springer, Berlin (1988).

[Hsiang and Rusinowitch, 1986] Jieh Hsiang and Michaël Rusinowitch. A new method for establishing refutational completeness in theorem proving. In J. H. Siekmann, editor, *Proceedings of the Eighth International Conference on Automated Deduction*, pages 141–152, Oxford, England, July 1986. Vol. 230 of *Lecture Notes in Computer Science*, Springer, Berlin.

[Hsiang and Rusinowitch, 1987] Jieh Hsiang and Michaël Rusinowitch. On word problems in equational theories. In T. Ottmann, editor, *Proceedings of the Fourteenth EATCS International Conference on Automata, Languages and Programming*, pages 54–71, Karlsruhe, West Germany, July 1987. Vol. 267 of *Lecture Notes in Computer Science*, Springer, Berlin.

[Huet and Oppen, 1980] Gérard Huet and Derek C. Oppen. Equations and rewrite rules: A survey. In R. Book, editor, *Formal Language Theory: Perspectives and Open Problems*, pages 349–405. Academic Press, New York, 1980.

[Huet, 1981] Gérard Huet. A complete proof of correctness of the Knuth-Bendix completion algorithm. *J. Computer and System Sciences*, 23(1):11–21, 1981.

[Jouannaud and Waldmann, 1986] Jean-Pierre Jouannaud and Bernard Waldmann. Reductive conditional term rewriting systems. In *Proceedings of the Third IFIP Working Conference on Formal Description of Programming Concepts*, Ebberup, Denmark, 1986.

[Kamin and Lévy, 1980] Sam Kamin and Jean-Jacques Lévy. Two generalizations of the recursive path ordering. Unpublished note, Department of Computer Science, University of Illinois, Urbana, IL, February 1980.

[Kaplan, 1987] Stéphane Kaplan. Simplifying conditional term rewriting systems: Unification, termination and confluence. *J. Symbolic Computation*, 4(3):295–334, December 1987.

[Knuth and Bendix, 1970] Donald E. Knuth and P. B. Bendix. Simple word problems in universal algebras. In J. Leech, editor, *Computational Problems in Abstract Algebra*, pages 263–297. Pergamon Press, Oxford, U. K., 1970. Reprinted in *Automation of Reasoning 2*, Springer, Berlin, pp. 342–376 (1983).

[Kounalis and Rusinowitch, 1987] Emmanuel Kounalis and Michaël Rusinowitch. On word problems in Horn theories. In S. Kaplan and J.-P. Jouannaud, editors, *Proceedings of the First International Workshop on Conditional Term Rewriting Systems*, pages 144–160, Orsay, France, July 1987. Vol. 308 of *Lecture Notes in Computer Science*, Springer, Berlin (1988).

[Lankford and Ballantyne, 1983] Dallas S. Lankford and A. Michael Ballantyne. On the uniqueness of term rewriting systems. Unpublished note, Department of Mathematics, Louisiana Tech. University, Ruston, LA, December 1983.

[Lankford, 1975] Dallas S. Lankford. Canonical inference. Memo ATP-32, Automatic Theorem Proving Project, University of Texas, Austin, TX, December 1975.

[Makowsky, 1985] J. A. Makowsky. Why Horn formulas matter in computer science: Initial structures and generic examples. In *Mathematical Foundations of Software Development*, pages 374–385, 1985. Vol. 185 of *Lecture Notes in Computer Science*, Springer, Berlin.

[Métivier, 1983] Yves Métivier. About the rewriting systems produced by the Knuth-Bendix completion algorithm. *Information Processing Letters*, 16(1):31–34, January 1983.

[Nieuwenhuis and Orejas, 1990] Robert Nieuwenhuis and Fernando Orejas. Clausal rewriting. In S. Kaplan and M. Okada, editors, *Extended Abstracts of the Second International Workshop on Conditional and Typed Rewriting Systems*, pages 81–88, Montreal, Canada, June 1990. Concordia University. Revised version to appear in *Lecture Notes in Computer Science*, Springer, Berlin.

[Rémy and Zhang, 1984] Jean-Luc Rémy and Hantao Zhang. REVEUR4: A system for validating conditional algebraic specifications of abstract data types. In *Proceedings of the Sixth European Conference on Artificial Intelligence*, pages 563–572, Pisa, Italy, 1984.

[Robinson and Wos, 1969] G. Robinson and L. Wos. Paramodulation and theorem-proving in first order theories with equality. In B. Meltzer and D. Michie, editors, *Machine Intelligence 4*, pages 135–150. Edinburgh University Press, Edinburgh, Scotland, 1969.

[Rusinowitch, 1989] Michaël Rusinowitch. *Démonstration Automatique: Techniques de réécriture*. InterEditions, Paris, France, 1989.

[Zhang and Kapur, 1988] Hantao Zhang and Deepak Kapur. First-order theorem proving using conditional equations. In E. Lusk and R. Overbeek, editors, *Proceedings of the Ninth International Conference on Automated Deduction*, pages 1–20, Argonne, Illinois, May 1988. Vol. 310 of *Lecture Notes in Computer Science*, Springer, Berlin.

[Zhang and Rémy, 1985] Hantao Zhang and Jean-Luc Rémy. Contextual rewriting. In *Proceedings of the First International Conference on Rewriting Techniques and Applications*, pages 46–62, Dijon, France, May 1985. Vol. 202 of *Lecture Notes in Computer Science*, Springer, Berlin (September 1985).