Ordering-Based Strategies for Horn Clauses*

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

Abstract

Two new theorem-proving procedures for equational Horn clauses are presented. The largest literal is selected for paramodulation in both strategies, except that one method treats positive literals as larger than negative ones and results in a unit strategy. Both use term orderings to restrict paramodulation to potentially maximal sides of equations and to increase the amount of allowable simplification (demodulation). Completeness is shown using proof orderings.

1 Introduction

The completeness of positive-unit resolution for sets of Horn clauses $p_1 \wedge \cdots \wedge p_n \Rightarrow p_{n+1}$ is well-known. An advantage of a unit strategy is that the number of literals in clauses never grows; it suffers from the disadvantage of being a bottom-up method. Ordered resolution, in which the literals of each clause are arranged in a linear order $>$ and only the largest literal may serve as a resolvent, is also complete for Horn clauses [Boyer, 1971]. The purpose here is to design Horn clause strategies that make more comprehensive use of orderings in controlling inference.

A *conditional equation* is a universally-quantified Horn clause in which the only predicate symbol is equality ($\simeq$). Conditional equations are important for specifying abstract data types and expressing logic programs with equations. We write such a clause in the form $e_1 \wedge \cdots \wedge e_n \Rightarrow s \simeq t$ ($n \geq 0$), meaning that the equality $s \simeq t$ holds whenever all the equations e_i, called *conditions*, hold. If $n = 0$, then the (positive unit) clause, $s \simeq t$, will be called an *unconditional equation*. Horn clauses with both equality and non-equality literals can be expressed as conditional equations with equality literals only by turning each nonequality atom l into a Boolean equation $l \simeq T$, for the truth constant T. A conditional equation $e_1 \wedge \cdots \wedge e_n \Rightarrow s \simeq t$ is valid for E iff $s \simeq t$ is valid for $E \cup \{e_1, \ldots, e_n\}$; hence, proving validity of conditional equations reduces to proving validity of unconditional ones.

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

Positive-unit resolution, or any other complete variation of resolution, could be used to prove theorems in equational Horn theories (the equality axioms, including functional reflexivity, are Horn), but the cost of treating equality axioms like any other clause is prohibitive. For this reason, special inference mechanisms for equality, notably paramodulation [Robinson and Wos, 1969], have been devised. In the Horn case, a unit strategy can be combined with paramodulation [Henschen and Wos, 1974; Furbach, 1987].

In this paper, we describe two complete theorem-proving methods for equational Horn theories. As in [Hsiang and Rusinowitch, 1986; Kounalis and Rusinowitch, 1987; Zhang and Kapur, 1988; Rusinowitch, 1989; Bachmair and Ganzinger, 1990; Nieuwenhuis and Orejas, 1990], our goal is to minimize the amount of paramodulation, while maximizing the amount of simplification—without threatening completeness. Orderings, described in detail in Section 2, are used to choose which literals participate in a paramodulation step, and which side of an equality literal to use. They utilize orderings of terms and atoms to restrict inferences, and are generalizations of *ordered completion* [Bachmair *et al.*, 1986; Hsiang and Rusinowitch, 1987], an "unfailing" extension of the "completion procedure" in [Knuth and Bendix, 1970] for unconditional equational inference. Completion operates on asymmetrical equations, that is, on *rewrite rules*, and has as its goal the production of confluent (Church-Rosser) systems of rules that can be used to decide validity. To achieve this, the larger sides of rules are overlapped on (non-variable) subterms of each other, producing equations that are called "critical pairs". Brown [1975] and Lankford [1975] first suggested combining completion for oriented unconditional equations, with paramodulation for unorientable ones and resolution for non-equality atoms. Paul [1986] studied the application of completion to sets of Horn clauses with equality.

Completion was extended to conditional equations by Kaplan [1987], who turns equations into rules only if they satisfy a certain "decreasingness" condition. The problem is that the critical pair of two decreasing rules can easily be nondecreasing. Like standard completion, both these methods may fail on account of inability to form new rules. Kounalis and Rusinowitch [1987] suggested narrowing conditions to achieve completeness.

Recently, several restrictions of paramodulation based on term orderings have been proposed for the full first-order case, including [Zhang and Kapur, 1988; Rusinowitch, 1989; Bachmair and Ganzinger, 1990]. For a survey of rewriting, see [Dershowitz and Jouannaud, 1990].

Section 3 presents a set of inference rules that severely restricts resolution with paramodulation by incorporating an ordering on (atoms and) terms. Limiting inference partially controls growth; keeping clauses fully simplified stunts growth even further. Such restrictions are of paramount importance in any practical theorem prover, but their (refutational) completeness has been difficult to establish. For our completeness proofs, sketched in Section 4, we adapt the proof-ordering method of [Bachmair *et al.*, 1986] to conditional proofs. Section 4.1 demonstrates the completeness of a unit strategy (suggested in [Dershowitz, 1990]) and Section 4.2 considers a strategy based on conditional completion of decreasing rules. Proof orderings allow us to limit narrowing to negative literals in the unit strategy, something that appears impossible with the recent transfinite-tree proof method used in [Hsiang and Rusinowitch, 1987]. The crux of our proof normalization argument is the observation that any conditional equational proof not in "normal form" must either have a "peak", that is, two applications of equations such that the middle term is the largest of all those involved and all subproofs are in normal form, or a "drop", that is, an application of an equation (or reflexivity of equals) to an instance of a condition in which all subproofs are in normal form. The strategies are designed to eliminate peaks and drops, thereby reducing the complexity assigned to the proof.

Section 5 concludes with a short discussion.

2 Simplification Orderings

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; by $t[s]_\pi$, we denote the term t with its subterm $t|_\pi$ replaced by some term s.

Term orderings are of central importance in the proposed methods. A total ordering $>$ on ground terms $\mathcal{G}$ is called a *complete simplification ordering* [Hsiang and Rusinowitch, 1987] if it has (a) the "replacement property", $s > t$ implies that any term $u[s]_\pi$, with subterm s located at some position π, is greater under $>$ than the term $u[t]_\pi$ with that occurrence of s replaced by t, 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 (see [Dershowitz, 1987]). A *completable simplification ordering* on all terms $\mathcal{T}$ is a *partial* ordering $\succ$ (c) that 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 (e) that the constant T is minimal in $\succ$.

Imagine a total ordering of atoms and with no equations, per se. The method of Section 4.1, then, is just selected positive-unit resolution, in which the largest negative literal is chosen. The appropriate inference rule would be expressed as:

$$\frac{E \cup \left\{ \begin{array}{rcl} q \wedge s \simeq T & \Rightarrow & u \simeq T, \\ & & l \simeq T \end{array} \right\}}{E \cup \left\{ \begin{array}{rcl} q \wedge s \simeq T & \Rightarrow & u \simeq T, \\ & & l \simeq T, \\ q\sigma & \Rightarrow & u\sigma \simeq T \end{array} \right\}}$$

where σ is the most general unifier (mgu) of l and s. Here, the positive unit clause $l \simeq T$ is resolved with the negative literal $s \simeq T$ in the clause $q \wedge s \simeq T \Rightarrow u \simeq T$, and produces a new Horn clause $q\sigma \Rightarrow u\sigma \simeq T$. The new clause is a logical consequence of the two given clauses, since $s\sigma = l\tau\sigma$, where τ renames variables in l so that it shares none with s. The clause would be generated *only* when $s > q$, by which we mean that s is the largest negative literal in its clause.

A total simplification ordering on non-ground literals is not actually possible (which is why the ordering of the parent clause is inherited in ordered resolution), but can be approximated by a partial ordering. If only a partial ordering $\succ$ is given, we resolve negative literals that are potentially maximal. That is, we apply the above rule if $s\sigma \not\prec q\sigma$, or, in other words, if the instance $s\sigma$ of s created by resolution is not necessarily smaller than the other instantiated negative literals. Since some of the rules we consider delete or simplify antecedent clauses, the above format for inference rules, with the equations that participated in the inference also appearing as part of the consequent, is advantageous.

Suppose E is a set of Horn clauses in conditional equation form. To handle equality literals $l \simeq r$, we need to unify at subterms of conditions, not just at the literal level. Note that whenever we refer to equations in a set, we mean that it, or the symmetric equation (with l and r exchanged), or a variant with variables renamed uniformly, actually appears in the set. With that in mind, if l unifies with a non-variable subterm $s|_\pi$ of a maximal term s in a condition $s \simeq t$ of a conditional equation $q \wedge s \simeq t \Rightarrow u \simeq v$, then a new Horn clause is created by applying the most general unifying substitution σ to the conditional equation, and then replacing $l\sigma$ with $r\sigma$, as per the unit clause $l \simeq r$. The conditions ensure that $s\sigma$ is the (potentially) larger side of the condition that is being paramodulated into and that the replacement yields a (potentially) smaller condition.

3 Inference Rules

We formulate our theorem-proving procedure as an inference system operating on a set of conditional equations, and parameterized by a completable ordering $\succ$. We define a symmetric binary relation $\leftrightarrow$, for a particular set of conditional equations E, as the smallest relation satisfying $t[l\sigma]_\pi \leftrightarrow t[r\sigma]_\pi$ for all $u_1 \simeq v_1 \wedge \cdots \wedge u_n \simeq v_n \Rightarrow l \simeq r$ in E such that $u_i\sigma \leftrightarrow^* v_i\sigma$ for each i, where $\leftrightarrow^*$ is the reflexive-transitive closure of $\leftrightarrow$. This relation corresponds to "substitution of equals" according to the axioms in E. We also define a *decreasing rewrite* relation $\rightarrow_E$ on terms $\mathcal{T}$. An instance $p\sigma \Rightarrow u\sigma \simeq v\sigma$ of a conditional equation is

"decreasing" if $u\sigma \succ v\sigma$ in the completable ordering and the proofs of the conditions only involve terms smaller than $u\sigma$. We write $u \rightarrow_e v$ (with respect to a partial ordering $\succ$), if $u \leftrightarrow_e v$ using a decreasing instance of e. For unit equation e, $\rightarrow_e$ is just the intersection of $\leftrightarrow_e$ and $\succ$. Decreasingness is essentially the same condition as imposed on conditional rewrite rules by the completion-like procedures of [Kaplan, 1987; Ganzinger, 1987]. In these methods, superposition is used when the left-hand side is larger than the conditions; narrowing, when a condition dominates the left-hand side. As theorem provers, however, they are refutationally *in*complete, since they make no provision for "unorientable" equations $s \simeq t$ such that $s \not\succ t$ and $t \not\succ s$.

The inference rules we present may be classified into three "expansion" rules and four "contraction" rules. Contraction rules significantly reduce space requirements, but make proofs of completeness much more subtle.

Superpose:

$$\frac{E \cup \left\{ \begin{array}{l} p \Rightarrow l \simeq r, \\ q \Rightarrow u \simeq v \end{array} \right\}}{E \cup \left\{ \begin{array}{l} p \Rightarrow l \simeq r, \\ q \Rightarrow u \simeq v, \\ p\mu \wedge q\mu \Rightarrow u\mu[r\mu]_\pi \simeq v\mu \end{array} \right\}}$$

$$\text{if } \left\{ \begin{array}{l} u|_\pi \notin \mathcal{X} \\ \mu = mgu(u|_\pi, l) \\ u\mu \not\succ p\mu, q\mu, v\mu, u\mu[r\mu]_\pi \end{array} \right.$$

Superposition (i.e. oriented paramodulation of positive equational literals) is performed only at non-variable positions ($u|_\pi \notin \mathcal{X}$). Only positive equations are used in this rule, and only in a decreasing direction ($u\mu \not\prec p\mu, q\mu$). Either side of an equation may be used for superposition, but only if, in the context of the paramodulation, it is potentially the largest term involved ($u\mu \not\prec v\mu, u\mu[r\mu]_\pi$). Note that the two conditional equations may actually be the same (except for renaming). Here and later, when a rule refers to a clause of the form $q \Rightarrow u \simeq v$, an unconditional equation ($u \simeq v$) is also intended. When both participating equations are unconditional, an unconditional "ordered" critical pair is generated.

We need, additionally, a rule that paramodulates into maximal negative literals:

Narrow:

$$\frac{E \cup \left\{ \begin{array}{rcl} p & \Rightarrow & l \simeq r, \\ q \wedge s \simeq t & \Rightarrow & u \simeq v \end{array} \right\}}{E \cup \left\{ \begin{array}{rcl} p & \Rightarrow & l \simeq r, \\ q \wedge s \simeq t & \Rightarrow & u \simeq v, \\ p\mu \wedge q\mu \wedge s\mu[r\mu]_\pi \simeq t\mu & \Rightarrow & u\mu \simeq v\mu \end{array} \right\}}$$

$$\text{if } \left\{ \begin{array}{l} s|_\pi \notin \mathcal{X} \\ \mu = mgu(s|_\pi, l) \\ s\mu \not\succ p\mu, q\mu, t\mu, s\mu[r\mu]_\pi \end{array} \right.$$

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 u is either side of the implied equation.

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

Reflect:

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

$$\text{if } \left\{ \begin{array}{l} \sigma = mgu(s,t) \\ s\sigma \not\prec q\sigma \end{array} \right.$$

The contraction rules all simplify the set of conditional equations. The first deletes trivial conditional equations:

Delete:

$$\frac{E \cup \{ \; q \;\; \Rightarrow \;\; u \simeq u \; \}}{E}$$

The next rule allows for deletion of conditions that are trivially true:

Condense:

$$\frac{E \cup \{ \; q \wedge s \simeq s \;\; \Rightarrow \;\; u \simeq v \; \}}{E \cup \{ \; q \;\; \Rightarrow \;\; u \simeq v \; \}}$$

The last two contraction rules use decreasing instances to simplify other clauses. One rule simplifies conditions; the other applies to the equation part. In both cases, the original clause is *replaced* by a version that is logically equivalent, assuming the rest of E.

Simplify:

$$\frac{E \cup \{ \; p \;\; \Rightarrow \;\; u \simeq v \; \}}{E \cup \{ \; q \;\; \Rightarrow \;\; u \simeq v \; \}}$$

$$\text{if } \; p \rightarrow_E q$$

Compose:

$$\frac{E \cup \{ \; q \;\; \Rightarrow \;\; u \simeq v \; \}}{E \cup \{ \; q \;\; \Rightarrow \;\; w \simeq v \; \}}$$

$$\text{if } \left\{ \begin{array}{l} u \rightarrow_{p \Rightarrow l \simeq r} w, \; p \Rightarrow l \simeq r \in E \\ v \succ u \vee (u \simeq v) \; \triangleright \; (l \simeq r) \end{array} \right.$$

By $u \simeq v \; \triangleright \; l \simeq r$ we mean that the larger of u and v, say u, is strictly greater than the larger side of $l \simeq r$, say l, in the *encompassment* ordering (wherein a term is larger than its proper subterms and smaller than its proper instances), or that $u = l$ but v is strictly greater than r under $\succ$. This allows the larger side of an equation to be simplified by a more general equation, and the smaller side to be rewritten in any case.

We use the notation $E \vdash E'$ to denote *one* inference step, applying any of the seven rules to a set E of conditional equations to obtain a new set E'. The inference rules are evidently sound, in that the class of provable theorems is unchanged by an inference step.

4 Strategies

Let $>$ be any complete simplification ordering extending the given partial ordering $\succ$. A *proof* of an equation $s \simeq t$ between *ground* terms (any variables in s and t may be treated as Skolem constants) is a "derivation"

$$\begin{array}{ccccccccc} s = t_1 & \overset{\pi_1}{\longleftrightarrow}_{e_1\sigma_1} & t_2 & \overset{\pi_2}{\longleftrightarrow}_{e_2\sigma_2} & \cdots & \overset{\pi_m}{\longleftrightarrow}_{e_m\sigma_m} & t_{m+1} = t \\ & | & & | & & | & \\ & P_1 & & P_2 & & P_m & \end{array}$$

of $m+1$ terms ($m \geq 0$), each step $t_k \leftrightarrow t_{k+1}$ of which is either *trivial* ($t_{k+1} = t_k$), or else is justified

by a conditional equation e_k in E, a position π_k in t_k, a substitution σ_k for variables in the equation, and subproofs P_k (of the same form) for each conditions $u_{k\,j}\sigma_k \simeq v_{k\,j}\sigma_k$ of the applied instance $e_k\sigma_k$. Steps employing an unconditional equation do not have subproofs as part of their justification. (By the completeness of positive-unit resolution for Horn clauses, any equation $s \simeq t$ that is valid for a set E of conditional equations is amenable to such an equational proof.)

We use $\leftarrow$ for the inverse of $\rightarrow$, and $\rightarrow^*$ and $\leftarrow^*$ for the reflexive-transitive closures of $\rightarrow$ and $\leftarrow$, respectively. By a *peak*, we mean a proof segment of the form $s \leftarrow u \rightarrow t$; by a *valley*, we mean a proof segment of the form $u \rightarrow^* w \leftarrow^* t$; by a *drop*, we mean a step $s \rightarrow t$ with valley subproofs; a *plateau* is a trivial subproof of form $s \leftrightarrow s$. The *depth* of a proof is the maximum nesting of subproofs; it is one more than the maximum depth of its subproofs.

4.1 Unit Stratgey

The inference rules of the previous section are designed to allow any equational proof to be transformed into normal form. A strategy based on these rules is complete if we can show that, with enough inferences, any theorem has a normal-form proof. For the unit strategy, a *normal-form* proof is a valley proof of depth 0. That is the same as saying that a normal-form proof has no peaks, no drops, and no plateaus. Normal-form proofs may be thought of as "direct" proofs; in a refutational framework the existence of such a proof for $s \simeq t$ means that demodulation of s and t using positive unit equations suffices to derive a contradiction between the Skolemized negation $s' \not\simeq t'$ of the given theorem and $x \simeq x$.

We must demonstrate that for any proof $s \leftrightarrow^* t$ of $s \simeq t$ in E_0, there eventually exists an unconditional valley proof $s \rightarrow^* w \leftarrow^* t$. In the unit strategy, only expansions involving an unconditional equation are necessary. Specifically, both equations used by **superpose** are unconditional and the positive literal used in **narrow** is a unit. Were it not for contraction rules, it would be relatively easy to show that **narrow** and **reflect** eventually provide an unconditional proof of $s \simeq t$, and that **superpose** eventually turns that into a valley.

We call an inference "fair" if all persistent superpositions of *unit* clauses, narrowings via unit clauses, and reflections have been considered:

Unit Strategy: An inference sequence $E_0 \vdash E_1 \vdash \cdots$ is *fair* with respect to the unit strategy if

$$\mathbf{exp}^1(E_\infty) \quad \subseteq \quad \bigcup_{i\geq 0} E_i,$$

where E_∞ is the set $\liminf_j E_j = \cup_{i\geq 0} \cap_{j\geq i} E_j$ of *persisting* conditional equations and $\mathbf{exp}^1(E_\infty)$ is the set of conditional equations that may be inferred from persisting equations by one application of **superpose** with p and q empty, **narrow** with p empty, or **reflect**.

Theorem 1. *If an inference sequence $E_0 \vdash E_1 \vdash \cdots$ is fair for the unit strategy, then for any proof of $s \simeq t$ in E_0, there is a normal-form proof of $s \simeq t$ in E_∞.*

This is shown by transfinite induction on proofs. The term ordering $>$ is extended to the transitive closure of it and the proper subterm ordering. This in turn is extended to equations by considering the equation as a multiset of two terms, and using the multiset extension of this ordering. (In the multiset ordering [Dershowitz and Manna, 1979], a multiset is decreased by replacing an element with any finite number of smaller elements.) An equation is greater than a term if and only if one of its sides is. Conjunctions of equations are compared as multisets of these multisets, and a conjunction is larger than a term if one of its conjuncts is. Proofs are measured in the following way: Consider a step

$$s = w[l\sigma]_\pi \quad \underset{e\sigma}{\overset{\pi}{\longleftrightarrow}} \quad w[r\sigma]_\pi = t$$

in a ground proof or its subproofs, where e is the conditional equation $q \Rightarrow l \simeq r$ justifying the step, σ is the substitution, and s is the larger of s and t (in the complete simplification ordering $>$ extending $\succ$). To each such step, we assign the weight

$$\langle \{q\sigma, s, l\sigma\}, e \rangle$$

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 conjunctions and terms described above. (Note that s is always greater or equal to $l\sigma$, and that for decreasing instances it is also greater than $q\sigma$.) Second components are compared using the extension $\rhd$ of the encompassment ordering described earlier. 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 (see, e.g., [Dershowitz and Jouannaud, 1990]) that $\gg$ is well-founded.

Note that if $s \rightarrow_e t$, then the cost of this step is always greater than the cost of the steps in its subproofs. Also, if $s \rightarrow t \rightarrow u$, then the cost of the first step is larger than that of the second.

We need to show that inferences never increase the complexity of proofs and, furthermore, that there are always inferences that can decrease the complexity of non-normal proofs. Then, by induction with respect to $\gg$, the eventual existence of a normal-form proof follows.

Lemma 1. *If $E \vdash E'$, then for any proof P in E of an equation $s \simeq t$, there exists a proof P' in E' of $s \simeq t$, such that $P \gg P'$ or $P = P'$.*

This is established by consideration of the effects of each contracting inference rule that deletes or replaces equations, since for expansion rules, $E \subseteq E'$, and we can take $P' = P$. The conditions imposed on **compose** are essential for showing a decrease in $\gg$. (A more general contraction rule would simply allow deletion of any equation that admits a smaller proof vis-a-vis $\gg$.)

Lemma 2. *If P is a non-normal-form proof in E, then there exists a proof P' in $E \cup \mathbf{exp}^1(E)$ such that $P \gg P'$.*

The argument depends on a distinction between "non-critical" subproofs, for which there is a proof P' in E

itself, and "critical" subproofs, for which equations in $\mathbf{exp}^1(E)$ are needed. A peak

$$t' \leftarrow^{\pi}_{p\sigma \Rightarrow l\sigma \simeq r\sigma} t \rightarrow^{\rho}_{q\tau \Rightarrow u\tau \simeq v\tau} t''$$

where $t = w[l\sigma]_\pi[u\tau]_\rho$, is *critical* if the position π is at or below the position ρ in w at which $u \simeq v$ is applied, but not at or below a position corresponding to any variable in u, or (symmetrically) if ρ falls within the non-variable part of the occurrence of l in w. Similarly, a drop $t \rightarrow^{\pi}_{q\sigma \Rightarrow e\sigma} t''$ is *critical* if the first or last step of one of the subproofs for $q\sigma$ takes place within the non-variable part of the condition q.

Since any proof must have at least one subproof of depth 0, any non-normal proof must have a plateau, an *unconditional* peak, or a drop of depth 1 with (unconditional) valley subproofs. Thus, we need not worry about peaks involving a conditional rule, nor drops in which the proof of some condition is not unconditional. All plateaus can be spliced out. Critical unconditional peaks, critical drops with non-empty unconditional valley subproofs, and drops with empty proofs of conditions can each be replaced by a smaller proof, using the conditional equation generated by a required application of **superpose**, **narrow**, or **reflect** inference, respectively. Narrowing can be restricted to the maximal side of the maximal condition, since a drop with non-empty subproofs must have a step emanating from the larger side of its largest condition.

Non-critical unconditional peaks $t' \leftarrow t \rightarrow t''$ have alternative, smaller proofs $t' \rightarrow^* t \leftarrow^* t''$ in E by the version of the Critical Pair Lemma in [Lankford, 1975]. Consider a non-critical drop $w[u\sigma] \leftrightarrow_{q\sigma \Rightarrow u\sigma \simeq v\sigma} w[v\sigma]$, with unconditional subproof $p\sigma \rightarrow p' \rightarrow^* p'' \leftarrow^* p'''$, where $p\sigma$ is no smaller than any other term in the subproof $q\sigma$. Suppose p has a variable x at position π and the first step applies within the variable part $p|_\pi$. That is, $p\sigma = p\sigma[x\sigma]_\pi \rightarrow p\sigma[r]_\pi = p'$. Let τ be the same substitution as σ except that $\tau : x \mapsto r$. There is a smaller proof (smaller, vis-a-vis $\gg$) in E: $w[u\sigma] \leftarrow^* w[u\tau] \leftrightarrow_{q\sigma \Rightarrow u\sigma \simeq v\sigma} w[v\tau] \rightarrow^* w[v\sigma]$. Any rewrites $x\sigma \rightarrow r$ that need to be added to turn a proof of $q\sigma$ into a proof of $q\tau$ are also smaller.

Theorem 1 follows: If $s \simeq t$ is provable in E_0, then (by Lemma 1) it has a proof P in the limit E_∞. If P is non-normal, then (by Lemma 2) it admits a smaller proof P' using (in addition to E_∞) a finite number of equations in $\mathbf{exp}^1(E_\infty)$. By fairness, each of those equations appeared at least once along the way. Subsequent inferences (by Lemma 1) can only decrease the complexity of the proof of such an equation once it appears in a set E_i (and has a one-step proof). Thus, each equation needed in P' has a proof of no greater complexity in E_∞ itself, and hence (by the multiset nature of the proof measure), there is a proof of $s \simeq t$ in E_∞ that is strictly smaller than P. Since the ordering on proofs is well-founded, by induction there must be a normal proof in E_∞.

4.2 Decreasing Strategy

In the above method, only unconditional equations are used for superposition and narrowing. An alternative is to design an inference system that distinguishes between decreasing and nondecreasing non-unit clauses. We give here a method based on the incomplete completion method in [Ganzinger, 1987]. The required inferences (using **superpose** and **narrow**) are again a stringent restriction of paramodulation.

For the decreasing method, we redefine 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; see [Dershowitz and Okada, 1988]. 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. The Critical Pair Lemma of [Kaplan, 1987] for decreasing systems can be adapted to ground confluence of decreasing systems. Superposition is needed between decreasing conditional rules. As before, we must perform enough expansions with persistent conditional equations for there to always be a normal-form proof in the limit.

Decreasing Strategy: An inference sequence $E_0 \vdash E_1 \vdash \cdots$ is *fair* with respect to the decreasing strategy if

$$\mathbf{exp}(E_\infty) \quad \subseteq \quad \bigcup_{i \geq 0} E_i,$$

where $\mathbf{exp}(E_\infty)$ is the set of conditional equations that may be inferred from persisting equations by one application of an expansion rule **superpose**, **narrow**, or **reflect**.

Theorem 2. *If an inference sequence is fair for the decreasing strategy, 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_∞.*

5 Discussion

We presented two complete theorem-proving strategies based on the use of term-orderings. Both strategies provide for simplification (demodulation) by what we called "decreasing" equations.

Our unit strategy is the first to combine a restriction to paramodulation with unit equations with a strategy based on maximal terms. It limited inferences in the following ways: (1) The functional reflexive axioms are not needed and, at the same time, paramodulation into variables is avoided (as for some versions of paramodulation); (2) for all (resolution and paramodulation) inferences, at least one of the equations must be unconditional (as in positive unit resolution and positive unit paramodulation); (3) unless an equation is unconditional only its conditional part is used for paramodulation (analogous to positive-unit resolution); (4) only maximal terms (with respect to a given ordering) are used (analogous to ordered resolution). Unlike [Kounalis and Rusinowitch, 1987], we use only unit clauses when paramodulating into conditions; unlike [Bachmair *et al.*, 1989], all inferences use only the maximal side of an equation.

The second strategy prefers paramodulation between positive literals. It requires less paramodulation and offers more simplification than [Kounalis and Rusinowitch, 1987], for example. In essence, it treats decreasing

equations like unit clauses of the first strategy. When the ordering supplied to the prover is empty (the empty ordering is completable), 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]). The limitations on paramodulation are like those in [Bertling, 1990], but we give a specific, practical strategy for simplification.

The strength of these methods, both in minimizing possible inferences and maximizing potential simplifications, is brought to bear by employing more complete orderings than the empty one. A nonempty ordering eliminates many potential paramodulations and allows conditional equations that are simplifiable to be replaced without compromising (refutation) completeness. In practice, any efficiently computable ordering should be better than uncontrolled paramodulation. The polynomial and path orderings commonly used in rewrite-based theorem provers [Dershowitz, 1987] are completable. In particular, the recursive path orderings have decidability properties [Jouannaud and Okada, 1991] that make it ideal for this purpose. Choosing an ordering that takes the goal (theorem) into account can impart a top-down flavor to an otherwise bottom-up procedure.

We used the same ordering for simplification as for choosing the maximal literal. In fact, a different selection strategy can be used for choosing the literal to narrow, as in [Bertling and Ganzinger, 1989], but then the term ordering must be used to choose the larger side of the equality.

References

[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)*, Berlin, June 1990.

[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*, volume 2: Rewriting Techniques, chapter 1, pages 1–30. Academic Press, New York, 1989.

[Bertling and Ganzinger, 1989] Hubert Bertling and Harald Ganzinger. Completion-time optimization of rewrite-time goal solving. In N. Dershowitz, editor, *Proceedings of the Third International Conference on Rewriting Techniques and Applications (Chapel Hill, NC)*, volume 355, pages 45–58, Berlin, April 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-Verlag, Berlin.

[Boyer, 1971] Robert S. Boyer. *Locking: A restriction of resolution.* PhD thesis, University of Texas at Austin, Austin, TX, 1971.

[Brown, 1975] Thomas Carl Brown, Jr. *A Structured Design-Method for Specialized Proof Procedures.* PhD thesis, California Institute of Technology, Pasadena, CA, 1975.

[Dershowitz and Jouannaud, 1990] Nachum Dershowitz and Jean-Pierre Jouannaud. Rewrite systems. In J. van Leeuwen, editor, *Handbook of Theoretical Computer Science*, volume 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, 1988] Nachum Dershowitz and Mitsuhiro Okada. Proof-theoretic techniques and the theory of rewriting. In *Proceedings of the Third IEEE Symposium on Logic in Computer Science*, pages 104–111, Edinburgh, Scotland, July 1988.

[Dershowitz, 1987] Nachum Dershowitz. Termination of rewriting. 3(1&2):69–115, February/April 1987. Corrigendum: *4*, 3 (December 1987), 409–410; reprinted in *Rewriting Techniques and Applications*, J.-P. Jouannaud, ed., pp. 69—115, Academic Press, 1987.

[Dershowitz, 1990] Nachum Dershowitz. A maximal-literal unit strategy for Horn clauses. In S. Kaplan and M. Okada, editors, *Extended Abstracts of the Second International Workshop on Conditional and Typed Rewriting Systems*, pages 21–27, Montreal, Canada, June 1990. Concordia University. Revised version in *Lecture Notes in Computer Science 516*, Springer-Verlag, Berlin.

[Furbach, 1987] Ulrich Furbach. Oldy but goody: Paramodulation revisited. In Morik, editor, *Proceedings of the GI Workshop on Artificial Intelligence*, pages 195–200, 1987. Vol. 152 of *Informatik Fachberichte*.

[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*, volume 308, pages 62–83, Orsay, France, July 1987.

[Henschen and Wos, 1974] L. Henschen and L. Wos. Unit refutations and Horn sets. *J. of the Association for Computing Machinery*, 21:590–605, 1974.

[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 (Oxford, England)*, volume 230, pages 141–152, Berlin, July 1986.

[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 (Karlsruhe, West Germany)*, volume 267, pages 54–71, Berlin, July 1987.

[Jouannaud and Okada, 1991] Jean-Pierre Jouannaud and Mitsuhiro Okada. Satisfiability of systems of ordinal notations with the subterm property is decidable. In J. Leach Albert, B. Monien, and M. Rodríguez Artalejo, editors, *Proceedings of the Eighteenth EATCS Colloquium on Automata, Languages and Programming (Madrid, Spain)*, volume 510, pages 455–468, Berlin, July 1991.

[Kaplan, 1987] Stéphane Kaplan. Simplifying conditional term rewriting systems: Unification, termination and confluence. 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-Verlag, 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 (Orsay, France)*, volume 308, pages 144–160, Berlin, July 1987.

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

[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-Verlag, Berlin.

[Paul, 1986] Etienne Paul. On solving the equality problem in theories defined by Horn clauses. *Theoretical Computer Science*, 44(2):127–153, 1986.

[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 (Argonne, Illinois)*, volume 310, pages 1–20, Berlin, May 1988.