DECISION PROCEDURES
FOR SIMPLE EQUATIONAL THEORIES
WITH PERMUTATIVE AXIOMS:

COMPLETE SETS OF PERMUTATIVE REDUCTIONS

D. S. Lankford and A. M. Ballantyne

April 1977 ATP-37

DECISION PROCEDURES FOR SIMPLE EQUATIONAL THEORIES WITH PERMUTATIVE AXIOMS: COMPLETE SETS OF PERMUTATIVE REDUCTIONS

D. S. Lankford
1310 Piedmont
Austin, Texas 78757

A. M. Ballantyne
University of Texas
Mathematics Department
Austin, Texas 78712

ABSTRACT

Complete sets of permutative reductions are defined and two mathematical characterizations of the unique termination property are established. These mathematical characterizations of unique termination are used as the basis of new theorem proving techniques for first order logic with equality.

March 1977, revised April 1977

INTRODUCTION

Most practical mechanical theorem proving systems for first order logics with equality have treated the equational inferences through algebraic simplification methods. The work of Knuth (1), Knuth and Bendix (2), Lankford (3), Nevins (4), and Slagle (5) provides a theoretical basis and experimental justification for using algebraic simplification methods based on the concepts, properties, and techniques related to complete sets of reductions. We assume familiarity with those concepts, properties, and techniques, especially, immediate reduction, finite termination property, unique termination property, complete set of reductions, the diamond lemma, the unique termination theorem, the unique termination algorithm, and the Knuth and Bendix completion attempting technique.

In this article we consider the problem encountered by Knuth and Bendix (2) of treating commutative axioms by reduction mehtods. The difficulty is that commutative axioms cannot be used directly as rewrite rules because they allow infinite sequences of immediate reductions. For example, $f(x,y) \longrightarrow f(y,x)$ results in the infinite sequence of immediate reductions $f(a,b) \longrightarrow f(b,a) \longrightarrow f(a,b) \longrightarrow \ldots$.

Here we develop one approach to the commutative problem by extending the complete set of reductions concepts, properties, and techniques to equivalence classes of terms. The central result of this article is a mathematical characterization of the unique termination property for finite sets of certain equivalence class rewrite rules. With this mathematical characterization of unique termination, we generalize the Knuth and Bendix completion attempting technique to equivalence classes of rewrite rules and show how the extended completion attempting technique may be used for mechanical theorem proving in first order logics with equality.

COMPLETE SETS OF PERMUTATIVE REDUCTIONS

Let $f_1, \ldots, f_N$ be the function symbols and $v_1, v_2, v_3, \ldots$ be the countable number of variable symbols from which terms are constructed. Constants are function symbols of degree zero. A term is a variable symbol, constant, or an expression $f_i(t_1, \ldots, t_{d_i})$ where $t_1, \ldots, t_{d_i}$ are terms and d_i is the degree of f_i. Let $n(x,Y)$ be the number of occurrences of the symbol x in the term Y. An equation is an expression $t = u$, where t and u are terms. A permutation equation is an equation $t = u$ such that $n(x,t) = n(x,u)$ for each symbol x. Let $\mathcal{P}$ be a finite set of permutation equations and let $\approx$ be the equivalence relation defined by $t \approx u$ iff $t = u$ is a consequence of $\mathcal{P}$ or any equation of the form $v = v$ using the inference rule substitution of equals. It follows that for any term t, the equivalence class of t, denoted $\approx(t)$, is a finite set.

A permutative rewrite rule relative to $\mathcal{P}$ is an expression $\approx(L) \longrightarrow \approx(R)$ where L and R are terms and each variable symbol which occurs in R also occurs in L. We say $\approx(u)$ is an immediate permutative reduction of $\approx(t)$ by $\approx(L) \longrightarrow \approx(R)$ relative to $\mathcal{P}$ iff there exist a substitution θ, t' in $\approx(t)$, u' in $\approx(u)$, L' in $\approx(L)$, and R' in $\approx(R)$ such that u' is the result of replacing one occurrence of $L'\theta$ in t' by $R'\theta$. When $\approx(u)$ is an immediate permutative reduction of $\approx(t)$ we write $\approx(t) \longrightarrow \approx(u)$. A set $\mathcal{R}$ of permutative rewrite rules has the finite termination property iff there are no infinite sequences $\approx(t_1) \longrightarrow \approx(t_2) \longrightarrow \approx(t_3) \longrightarrow \ldots$ of immediate permutative reductions. An equivalence class is irreducible iff it has no immediate permutative reductions.

Let $\longrightarrow_c$ be the reflexive, transitive completion of $\longrightarrow$. We say that $\approx(t)$ terminates naturally with $\approx(u)$ iff $\approx(t) \longrightarrow_c \approx(u)$ and $\approx(u)$ is irreducible. A set $\mathcal{R}$ of permutative rewrite rules has the unique termination property iff for each equivalence class $\approx(t)$, if $\approx(t)$ terminates naturally with $\approx(u)$ and $\approx(v)$, then $\approx(u) = \approx(v)$. A set $\mathcal{R}$ of permutative rewrite rules is a complete set of permutative reductions iff $\mathcal{R}$ has the finite and unique termination properties.

The <u>functional reflexive axioms</u> for a set $\mathcal{E}$ of equations are the equations $f(v_1,\ldots,v_{d_f}) = f(v_1,\ldots,v_{d_f})$, where f is any function symbol which occurs in any term of any equation of $\mathcal{E}$. Let $\mathcal{R}_0$ be the set of all equations $L' = R$ where L' is in $\approx(L)$ and $\approx(L) \longrightarrow \approx(R)$ is in $\mathcal{R}$, and define $\mathcal{R}_{i+1} = \mathcal{R}_i \cup P$ where P is the set of all paramodulants $t = u$ of (i) an equation $L = R$ of $\mathcal{R}_i$ and and equation $p = q$ of $\mathcal{P}$, where t corresponds to q and paramodulation is by L into p on a subterm of p that is not a variable, or t corresponds to L and paramodulation is by p on a subterm of L that is not a variable, or (ii) an equation $L = R$ of $\mathcal{R}_i$ and a functional reflexive axiom $p = p$ for $\mathcal{P} \cup \mathcal{R}_0$ where $p = p$ paramodulates onto a variable symbol of L , t corresponds to L , and u corresponds to R . Let $\mathcal{R}_\infty = \bigcup \mathcal{R}_i$

<u>First Unique Termination Theorem</u> If a set $\mathcal{R}$ of permutative rewrite rules relative to $\mathcal{P}$ has the finite termination property, then $\mathcal{R}$ has the unique termination property iff for each paramodulant $v = w$ of $L_1 = R_1$ of $\mathcal{R}_\infty$ and $L_2 = R_2$ of $\mathcal{R}_0$ by left sides into left sides on a subterm that is not a variable, $\approx(v)^* = \approx(w)^*$ where $\approx(v)$ terminates naturally with $\approx(v)^*$ and $\approx(w)$ terminates naturally with $\approx(w)^*$.

Proof ($\Longrightarrow$) Let $v = w$ be a paramodulant of $L_1 = R_1$ and $L_2 = R_2$ of $\mathcal{R}$ by left sides into left sides on a subterm that is not a variable, and let μ be the most general unifier of paramodulation. Without loss of generality, assume L_1 paramodulates into L_2. Since $\approx(R_1)$ is an immediate permutative reduction of $\approx(L_1)$ and $\approx(R_2)$ is an immediate permutative reduction of $\approx(L_2)$, it follows that $\approx(v)$ is an immediate permutative reduction of $\approx(L_2\mu)$ and $\approx(w)$ is an immediate permutative reduction of $\approx(L_2\mu)$. Since $\mathcal{R}$ has the unique termination property, it follows that $\approx(v)^* = \approx(w)^*$.

($\Longleftarrow$) This case requires a diamond lemma: if a set of permutative rewrite rules $\mathcal{R}$ relative to $\mathcal{P}$ has the finite termination property, then $\mathcal{R}$ has the unique termination property iff for each $\approx(t)$ and each pair $\approx(t) \longrightarrow \approx(u)$ and $\approx(t) \longrightarrow \approx(v)$ of immediate permutative reductions of $\approx(t)$, there exists $\approx(w)$ such that $\approx(u) \longrightarrow c \approx(w)$ and $\approx(v) \longrightarrow c \approx(w)$. Let t' and t'' be in $\approx(t)$, $\approx(L_1) \longrightarrow \approx(R_1)$ and $\approx(L_2) \longrightarrow \approx(R_2)$ be in $\mathcal{R}$, L_1' be in $\approx(L_1)$, L_2' be in $\approx(L_2)$, θ_1 and θ_2 be substitutions, u be the result of replacing one occurrence of $L_1'\theta_1$ in t' by $R_1\theta_1$, and v be the result of replacing one occurrence of $L_2'\theta_2$ in t'' by $R_2\theta_2$. If t' and t'' are identical, then methods like those of Knuth and Bendix (2) and Lankford (3) may be used to complete the proof. When t' and t'' are not identical, let $t' = t_1, \ldots, t_n = t''$ be a deduction of t''

from t' by equations of $\mathcal{P}$.

Let t_2 be obtained from t_1 by replacing one occurrence of $p\lambda$ in t_1 by $q\lambda$ where $p = q$ is in $\mathcal{P}$. If $p\lambda$ and $L_1\theta_1$ do not interact, then it follows that there exists u' in $\approx(u)$ such that u' is the result of replacing one occurrence of $L_1\theta_1$ in t_2 by $R_1\theta_1$, and thus we have reduced the problem to considering showter deductions. If $p\lambda$ occurs in $L_1\theta_1$ in a position that corresponds to a variable in L_1, then paramodulate into $L_1 = R_1$ with the functional reflexive axioms until a member $L_1' = R_1'$ of $\mathcal{R}_\infty$ is produced which is such that $L_1\theta_1$ is an instance of L_1' and the occurrence of $p\lambda$ in $L_1\theta_1$ does not correspond to a variable in L_1'. Thus there is a paramodulant $L_3 = R_3$ of $L_1' = R_1'$ and $p = q$ by p into L_1' such that u is the result of replacing $L_3\sigma$ in t_2 by $R_3\sigma$, and we have reduced the problem to considering shorter deductions. The cases when $L_1\theta_1$ occurs in $p\lambda$ are treated similarly. By iterating the reduction of the problem to shorter deductions, we eventually consider the case of $L_1\theta_1$ and $L_2\theta_2$ interacting, where $L_1 = R_1$ is in $\mathcal{R}_\infty$ and $L_2 = R_2$ is in $\mathcal{R}_0$. This case is treated by techniques like those of Knuth and Bendix (2) and Lankford (3).

The practical disadvantage of the first unique termination theroem is twofold, the functional reflexive axioms match with almost everything in sight, and a completion attempting algorithm based on it may not terminate after a complete set of permutative reductions is found. The second unique termination theorem below shows that we may dispense with the functional reflexive axioms while restricting paramodulation into subterms which are not variables. The techniques of proof are essentially the same as the first case even though they appear superficially different. The halting problem will not be considered here.

Let us define the <u>$\mathcal{P}$-inferences</u> of $\mathcal{R}$ as follows. The $\mathcal{P}$-inferences of degree 0 are $L_i' = R_i'$ where $L_i' \in \approx(L_i)$, $R_i' \in \approx(R_i)$ and $\approx(L_i) \longrightarrow \approx(R_i) \in \mathcal{R}$. The $\mathcal{P}$-inferences $L_k = R_k$ of degree $j + 1$ are obtained from the $\mathcal{P}$-inferences $L_p = R_p$ of degree j as follows: $L_k = R_k$ is a paramodulant of $L_p = R_p$ by a member of $\mathcal{P}$ into or by L_p on a subterm that is not a variable.

A <u>critical pair</u> is a pair $\approx(t)$, $\approx(u)$ where $t = u$ is a paramodulant of a $\mathcal{P}$-inference $L = R$ and $L_i' = R_i'$ on left sides, by left sides, on a subterm which is not a variable, where $L_i' \in \approx(L_i)$, $R_i' \in \approx(R_i)$, and $\approx(L_i) \longrightarrow \approx(R_i) \in \mathcal{R}$.

Second Unique Termination Theorem If $\mathcal{R}, \mathcal{P}$ has the finite termination property, then $\mathcal{R}, \mathcal{P}$ has the unique termination property iff for all critical pairs $\approx(t)$, $\approx(u)$, $\approx(t)^* = \approx(u)^*$.

Proof ($\Longrightarrow$) Obvious. ($\Longleftarrow$) We show that the permutative diamond lemma is satisfied. Let

$$\begin{array}{ccccc} t_1 & \approx & \cdots & \approx & t_n \\ \downarrow & L_1 \longrightarrow R_1 & & & \downarrow \; L_2 \longrightarrow R_2 \\ u & & & & v \end{array}$$

depict the hypothesis of the permutative diamond lemma. Let $\approx(t) = \approx(t_1)$ $(= \{ t_1 , \dots , t_n , \dots \})$, and let $\approx(t)$ be well-ordered by $<$ such that t_n is the $<$-least member of $\approx(t)$. It can be shown that there is a derivation of t_n from t_1 such that $t_1 > t_2 > \dots > t_{n-1} > t_n$ and paramodulants $p_1 = q_1 , \dots , p_{n-1} = q_{n-1}$ such that t_{i+1} is obtained from t_i by replacing an instance of p_i in t_i by the same instance of q_i and the $p_j = q_j$ are obtained by iterated paramodulation of members of $\mathcal{P}$. If $p_1 = q_1$ paramodulates into a variable position in L_1 , then replace all occurrences corresponding to that variable position, and we are reduced to considering shorter deductions. If $p_1 = q_1$ paramodulates into a position that does not correspond to a variable, then we obtain a $\mathcal{P}$-inference $L = R$ of $L_1 = R_1$ by paramodulating $p_1 = q_1$ into $L_1 = R_1$, and this $\mathcal{P}$-inference $L = R$

"reduces" t_2 . Thus we are reduced to considering shorter derivations. Eventually we must consider a $\mathcal{P}$-inference $L = R$ "reducing" t_n , which gives rise to the consideration of critical pairs.

CONCLUSIONS

The unique termination theorems provide a semi-decision procedure for non-unique termination for those sets of permutative rewrite rules that are known to have the finite termination property. We are presently studying the feasibility of implementing a permutative non-unique termination procedure as the basis of a permutative canonical inference theorem prover. We also plan to study refutation completeness questions for blocked resolution, permutative narrowing, and complete sets of permutative reductions.

ACKNOWLEDGEMENT

We thank Professor W. W. Bledsoe for his support through the Automatic Theorem Proving Project.

REFERENCES

1. Knuth, D. E. Notes on central groupoids. J. of Comb. Th. 8 (1970), 376-390.

2. Knuth, D. E. and Bendix, P. B. Simple word problems in universal algebras. Computational Problems in Abstract Algebra, J. Leech, Ed., Pergamon Press, 1970, 263-297.

3. Lankford, D. S. Canonical inference. Automatic Theorem Proving Project, Depts. Math. and Comput. Sci., Univ. of Texas, report ATP-32, Dec. 1975.

4. Nevins, A. J. A human oriented logic for automatic theorem-proving. JACM 21, 4 (Oct. 1974), 606-621.

5. Slagle, J. R. Automated theorem proving for theories with simplifiers, commutativity, and associativity. JACM 21, 4 (Oct. 1974), 622-642.