THE CASE FOR USING EQUALITY AXIOMS
IN AUTOMATIC DEMONSTRATION

Robert Kowalski

Introduction.

The use of equality axioms in resolution refutation systems has seemed to be particularly inefficient. In order to remedy this difficulty several modifications of the resolution method have been proposed ([4] , [13] , [15] , [17] and [21] and more recently [2] and [10]). Of these the paramodulation strategy of [15] seems to be particularly simple and efficient. The method for dealing with equality investigated in this paper consists of using equality axioms and of applying the version of hyper-resolution proposed in [5] . The hyper-resolution and paramodulation methods are compared and a simple interpretation of the former is found in a subsystem of the latter, providing a straightforward proof for the completeness of this subsystem of paramodulation. Several proposals are put forward for modifying the hyper-resolution method and these modifications are seen to induce corresponding modifications of the paramodulation strategy.

The method of this paper need not be confined to equality and can be applied to the special treatment of more general sets of axioms.

Preliminaries.

If L is a literal then $|L|$ denotes the atom A such that $L = A$ or $L = \overline{A}$. An expression (literal, clause, set of clauses) is a ground expression if it contains no variables. Constants are function symbols with no arguments. A set of expressions E is unifiable with unifier σ if $E\sigma$ is a singleton. If E is unifiable then there is a substitution θ , called a most general unifier (m.g.u.) of E, such that θ unifies E and for any unifier σ of E, $\sigma = \theta\lambda$ for some λ . Similarly a family of sets of expressions $\mathcal{E}$ is simultaneously unifiable with simultaneous unifier σ if $E\sigma$ is a singleton for each $E \in \mathcal{E}$. If $\mathcal{E}$ is simultaneously unifiable then there exists a simultaneous unifier θ of $\mathcal{E}$ such that for any simultaneous unifier σ of $\mathcal{E}$, $\sigma = \theta\lambda$ for some λ ; θ is called a most general simultaneous unifier (m.g.s.u.) of $\mathcal{E}$.

A set of ground clauses $\mathcal{C} = \{A_1,\dots,A_n,B\}$ where, for $1 \le i \le n$, $A_i = \{L_i\} \dot\cup A_{0i}$ and $B = \{\overline{L}_1,\dots,\overline{L}_n\} \dot\cup B_0$ is a clash ($\dot\cup$ denotes disjoint union as in Andrews' [1]). The resolvent of $\mathcal{C}$ is the clause $C = A_{01} \cup \dots \cup A_{0n} \cup B_0$. The clauses in $\mathcal{C}$ are the parents of C; $A_1,\dots, A_n$ are the satellites and B the nucleus of $\mathcal{C}$. The literals $L_1,\dots,L_n$ and their complements $\overline{L}_1,\dots\overline{L}_n$ are said to be literals resolved upon in $\mathcal{C}$. $\mathcal{C}$ is restricted if $L \notin C$ when L is resolved upon in $\mathcal{C}$. If $\mathcal{C}$ contains only two clauses then $\mathcal{C}$ and C are said to be binary. A clause is positive if all its literals are positive (i.e. unnegated atoms). The resolvent of a restricted clash is called a hyper-resolvent if all its satellite parents are positive and if all the negative literals in its nucleus parent are resolved upon in the clash. A P_1-resolvent is a binary resolvent with one positive parent. Every hyper-resolvent can be obtained by a sequence of P_1-resolutions [11].

To define the general notion of clash (called latent clash in [12] and [18]) we first define the notion of factor of a clause. The definition below, introduced in [5], differs both from that of Wos and Robinson [20] and from that more recently introduced by J.A. Robinson in [14]. Given a clause A and a unifiable subset $E \subseteq A$ with m.g.u. θ then the clause $A\theta$ together with its distinguished literal $E\theta$ is called a satellite factor of A. Given a clause B and a unifiable family $\mathcal{E}$ of subsets of B with m.g.s.u. θ then the clause $B\theta$ together with the set of its distinguished literals $\mathcal{E}\theta$ is called a nucleus factor of B. In case $\mathcal{E}$ contains only one set of literals then the corresponding nucleus factor of B is also a satellite factor. Conversely any satellite factor can be regarded as a nucleus factor. We write the distinguished literals of a factor as its first literals. A nucleus factor is complete if the set of its distinguished literals coincides with the set of its negative literals.

For the general case we define clash resolution for sets of factors and we insist that all and only distinguished literals be resolved upon. Given n satellite factors of the form $A_1 = \{L_1\} \dot{\cup} A_{01},\dots,A_n = \{L_n\} \dot{\cup} A_{0n}$ and nucleus factor $B = \{\overline{K}_1,\dots,\overline{K}_n\} \dot{\cup} B_0$ (where none of the factors $A_1,\dots,A_n,B$ share common variables), the set $\mathcal{C} = \{A_1,\dots,A_n,B\}$ is a clash if the family $\mathcal{E} = \{\{L_1,K_1\},\dots,\{L_n,K_n\}\}$ is unifiable. If $\mathcal{C}$ is unifiable with m.g.s.u. θ, then $C = (A_{01} \cup \dots \cup A_{0n} \cup B_0)\theta$ is the resolvent of $\mathcal{C}$. $\mathcal{C}$ is restricted if $L\theta \not\subseteq C$ when L is resolved upon in $\mathcal{C}$ and θ is the m.g.s.u. of $\mathcal{C}$. Satellites, nucleus, hyper-resolvent, etc. are defined as for ground clauses. Notice that the nucleus parent of a hyper-resolvent is always complete. It is easy to show, as in [5], that these notions of factoring and clash resolution improve the usual notions by restricting the generation of redundant inferences and of repeated calculation of m.g.s.u.s.

An arbitrary set of factors $\mathcal{C}$ is a clash if some set $\mathcal{C}'$ of variants of factors in $\mathcal{C}$ is a clash, i.e. $\mathcal{C}'$ is $\mathcal{C}\sigma$ where $A\sigma$ is a variant of A for each $A \in \mathcal{C}$ and where no two factors in $\mathcal{C}'$ contain common variables. The resolvent of $\mathcal{C}$ is the resolvent of $\mathcal{C}'$. Similarly an arbitrary set of clauses $\mathcal{C}$ is a clash if some set of factors $\mathcal{C}'$ is a clash where $\mathcal{C}'$ contains exactly one factor for each clause in $\mathcal{C}$ and where each factor in $\mathcal{C}'$ is a factor of some clause in $\mathcal{C}$. Again the resolvent of $\mathcal{C}$ is the resolvent of $\mathcal{C}'$.

Let S be a set of factors, define $\mathcal{R}(S)$ as the union of S and of the set of satellite factors of binary resolvents whose parents belong to S. Define $\mathcal{H}(S)$ similarly as the union of S and of the set of satellite factors of hyper-resolvents whose parents belong to S. For unfactored clauses S let $\mathcal{R}^0(S)$ be the set of all satellite factors of clauses in S, let $\mathcal{H}^0(S)$ be the set of all satellite factors of positive clauses in S and of all complete nucleus factors of non-positive clauses in S. Given any operation $\mathcal{O}$ (such as $\mathcal{R}$ or $\mathcal{H}$) from sets of factors to sets of factors and operation $\mathcal{O}^0$ (such as $\mathcal{R}^0$ or $\mathcal{H}^0$) from sets of unfactored clauses to sets of factors define $\mathcal{O}^{n+1}(S) = \mathcal{O}(\mathcal{O}^n(S))$ for $n \geq 0$. The completeness theorems for binary resolution and for hyper-resolution state that given an unsatisfiable set of clauses S_0 then $\square \in \mathcal{R}^n(S_0)$ and $\square \in \mathcal{H}^m(S_0)$ for some $n \geq 0$ and $m \geq 0$.

Let $\mathcal{O}$ be a derivation operation such as $\mathcal{R}$ or $\mathcal{H}$ above then given clauses S and $C \in \mathcal{O}^n(S)$ for some n there corresponds to C in a natural way at least one derivation tree T of C from clauses in S. It is convenient not to exhibit in T the operation of factoring or the operation of standardising variables in clauses occurring in clashes. We shall say that C occurs at the <u>root</u> of T and clauses from S at the <u>tips</u> of T. We shall think of T as a partially ordered set of occurrences of clauses with the occurrences at the tips being maximal elements and the occurrence at the root being the least element lying below all others. Given such a tree T and $C \in T$ we call T' the <u>subtree of T rooted in C</u> if T' consists of all of T lying above C and including C at its root. Thus if T is a derivation from clauses in S then any such T' is also a derivation from clauses in S.

<u>Equality Axioms and the Hyper-Resolution Method.</u>

For the equality symbol = we write $s = t$ instead of $=(s,t)$ and $s \neq t$ for $\overline{s = t}$.

Let S_0 be a set of clauses. Let $E = E_1 \cup E_2 \cup E_3$ where

$E_1 = \{ x = x \}$,

$E_2 = \{ x_i \neq y_i, f(x_1,\ldots,x_i,\ldots,x_n) = f(x_1,\ldots,y_i,\ldots,x_n) \mid$ for f in the vocabulary of S_0, for $n \geq 1$ and $1 \leq i \leq n \}$,

$E_3 = \{ x_i \neq y_i, \overline{P}(x_1,\ldots,x_i,\ldots,x_n), P(x_1,\ldots,y_i,\ldots,x_n) \mid$ for P the equality symbol and for P in the vocabulary of S_0, $n \geq 1$ and $1 \leq i \leq n \}$.

For simplicity we adopt the convention that $s = t$ is syntactically indistinguishable from $t = s$.

If S_0 has no normal model (i.e. a model in which the equality symbol of S_0 is interpreted as a substitutive identity relation) then $S = S_0 \cup E$ has no model whatsoever. Therefore there exists a hyper-resolution derivation T of $\square$ from S.

The efficiency of obtaining T can be improved in several directions by imposing restrictions on the hyper-resolution method [5]. Among the more important of these is the α-restriction ([5] and [6]). Given a set of clauses S, $\leq$ is an α-ordering for S if $\leq$ is a partial ordering of the set of atoms constructible from the vocabulary of S such that for all substitutions σ,

$$L_1 \leq L_2 \text{ implies } L_1\sigma \leq L_2\sigma.$$

Given S and $\leq$ an α-ordering for S, a satellite factor $C \in \mathcal{H}^n(S)$ for some $n \geq 0$, $C = \{L_1\} \dot{\cup} C_0$, is an <u>$\alpha$-factor</u> if $|L_1| < |L_2|$ for no $L_2 \in C_0$. For all n let $\mathcal{H}_\alpha^n(S)$ be $\mathcal{H}^n(S)$ without satellite factors which are not also α-factors. Then S unsatisfiable implies that $\Box \in \mathcal{H}_\alpha^n(S)$ for some n. (1)

If, for example, $\leq$ orders equality atoms before all others then the α-restriction for $\leq$ implies that we need never generate satellite factors of a clause containing the equality symbol if the clause also contains other predicate letters distinct from the equality symbol.

The derivation T of $\Box$ from $S_0 \cup E$ may be taken to be by hyper-resolution with or without the α-restriction. We shall compare the efficiency of obtaining T to that of obtaining a refutation of S_0 by the Robinson - Wos system of paramodulation and resolution.

<u>Paramodulation and its Completeness.</u>

Given a clause B and a single occurrence of the term t in B we write B(t) to indicate the given occurrence of t in B. For ground level clauses $A = \{t = s\} \dot{\cup} A_0$ and $B = B(t)$ a paramodulant of A and B is the clause $C = B(s/t) \cup A_0$. B(s/t) indicates the result of replacing the distinguished occurrence of t in B(t) by s. When there is no possibility of confusion we shall also indicate the result of this replacement by B(s).

At the general level paramodulation is defined in the context of refutation systems which include a separate rule for factoring. For factors $A = \{t_1 = s\} \dot{\cup} A_0$ and $B = B(t_2)$ where A and B share no variables and where t_1 and t_2 are unifiable with m.g.u. θ, a <u>paramodulant</u> of A and B is the clause $C = A_0\theta \cup B\theta(s\theta/t_2\theta) = (A_0 \cup B(s/t_2))\theta$. We shall refer to the factors A and B respectively as the <u>first and second parents</u> of C. We call the distinguished occurrence of t_2 in B the <u>term paramodulated upon</u>, although in a more precise terminology it would be more cumbersomely referred to as "the distinguished occurrence of the term paramodulated upon". The literals in which the distinguished occurrences of t_1 and t_2 appear are called the literals <u>paramodulated upon</u>. We shall see that these literals may be taken to be precisely the distinguished literals of satellite factors.

An important case of paramodulation occurs when the term t paramodulated upon in a second parent B(t) is primary in B(t). An occurrence of a term t in B is

---

(1) The same theorem holds if $\mathcal{H}$ is replaced by $\mathcal{R}$, [5]. A weaker theorem holds for set of support.

primary if that occurrence is as an argument of some literal in B [17]. Thus, for example, if $B = \{f(c) \neq c\}$ then $f(c)$ and the second occurrence of c are primary in B but the first occurrence of c is not. We shall say that an application of paramodulation is primary if the term paramodulated upon in the second parent is primary.

We extend the definition of paramodulation to arbitrary factors and to unfactored clauses just as in the case of clashes.

Given clauses S_0 let, E_4 be the set consisting of the clauses $f(x_1,\ldots,x_n) = f(x_1,\ldots,x_n)$ for every function symbol f occurring in the Herbrand universe $H(S_0)$, $n \geq 0$. Let $\mathfrak{U}^0(S_0 \cup E_4)$ be the set of satellite factors of clauses in $S_0 \cup E_4$. Let $\mathfrak{U}(S)$, for any set of factors S be the union of S and of the set of satellite factors of binary resolvents and of paramodulants whose parents belong to S. The following is a version of the completeness theorem reported in [15].

Theorem 1. Suppose that the set of clauses S_0 has no normal model. Then for some $n \geq 0$, $\square \in \mathfrak{U}^n(S_0 \cup E_4)$.

Comparison of the Paramodulation and Hyper-Resolution Methods.

Let S_0 have no normal model and let T be a hyper-resolution derivation of $\square$ from $S = S_0 \cup E$. The clauses in $E_2 \cup E_3$ occur in T only as nuclei of clashes. Moreover we may insist that no clause in E_3 occurring in T be factored with its two negative literals unified; such a factor would be of the form $\{s \neq t, t = s\}$ and would therefore be eliminable as a tautology. Thus to each clause C in E there corresponds exactly one factor. In case C is in E_2 or E_3 then the distinguished literals in the corresponding factor of C are just the negative literals in C. If $C = \{x = x\}$ then $x = x$ is the distinguished literal of the corresponding factor of C. We may identify without confusion the set of clauses E with the set of corresponding factors. The basis for comparison of the hyper-resolution and paramodulation methods rests upon the following two observations (similar observations have been made independently by Chang in [3]):

(1) Every hyper-resolvent in T with nucleus parent in E_3 is a primary paramodulant of its two satellite parents.

(2) Every hyper-resolvent in T with nucleus parent B in E_2 is a paramodulant of its one satellite parent and of an appropriate factor B^* in E_4 (if $B = \{x_i \neq y_i, f(x_1,\ldots,x_i,\ldots,x_n) = f(x_1,\ldots,y_i,\ldots,x_n)\}$ then $B^* = \{f(x_1,\ldots,x_n) = f(x_1,\ldots,x_n)\}$).

To verify (1) suppose that $A = \{s = t\} \dot{\cup} A_0$ and $B = \{P(s_1,\ldots,s_i,\ldots,s_n)\} \dot{\cup} B_0$ are satellite factors of a clash in T having nucleus in E_3. The hyper-resolvent of this clash is the clause $C = (\{P(s_1,\ldots,t,\ldots,s_n)\} \cup B_0)\theta$ where θ is the m.g.u. of the set of terms $\{s,t\}$. But C is also a primary paramodulant of A and B.

To verify (2) let $A = \{s = t\} \dot{\cup} A_0$ be the satellite factor of a clash in T having nucleus B in E_2. The hyper-resolvent of the clash is the clause

$C = \{f(x_1,\ldots,s\ ,\ldots,x_n) = f(x_1,\ldots,t,\ldots,x_n)\} \cup A_0$ for the function letter f and index i of the nucleus B. But C is also a paramodulant whose first parent is A and second parent is the clause $B^* = \{f(x_1,\ldots,x_n) = f(x_1,\ldots,x_n)\} \in E_4$.

For application below we note that (1) and (2) above hold for resolvents of arbitrary clashes $\mathfrak{C}$ provided only that the literals resolved upon in the nucleus of $\mathfrak{C}$ coincide with the subset of its negative literals. In other words, (1) and (2) continue to hold even if $\mathfrak{C}$ is unrestricted and the satellites of $\mathfrak{C}$ are not positive.

Suppose S_0 has no normal model, then $S = S_0 \cup E$ is unsatisfiable but so is $S' = S_0 \cup E_2 \cup E_3 \cup E_4$. Let T' be a hyper-resolution derivation of $\Box$ from S'. Observations (1) and (2) hold equally well for T' as for T. We shall transform T' into a paramodulation and binary resolution derivation T" of $\Box$ from $S_0 \cup E_4$. Delete all tips of T' at which clauses from E_3 occur; replace each clause B from E_2 occurring at a tip of T' by the appropriate clause B* from E_4. The resulting tree is a paramodulation and hyper-resolution derivation of $\Box$ from $S_0 \cup E_4$. If we now decompose each remaining hyper-resolvent into a sequence of P_1-resolvents (see [5] or [11]) we obtain the desired derivation T". The fact that such a derivation T' can always be transformed into a corresponding derivation T" constitutes a proof of Theorem 1. By investigating the structure of T" more closely we see that we have in fact proved the much stronger theorem 2 below.

Let S_0 be a set of clauses and $\leq$ an α-ordering for S_0. Associate with every complete nucleus factor B of a non-positive clause in S_0 a single total ordering of the negative (i.e. distinguished) literals in B. The definitions below of $\mathfrak{U}^0_\alpha$ and $\mathfrak{U}_\alpha$ are formulated to guarantee that each P_1-resolvent in T" is obtained by decomposing a hyper-resolvent in T' in a unique way. This unique decomposition is accomplished by resolving on the distinguished literals of non-positive factors in the order imposed by the original total ordering given to the distinguished literals in complete factors of clauses in S_0. Totally ordering complete nucleus factors eliminates all but one of the n! ways of decomposing hyper-resolvents whose nucleus parent contains n distinguished literals.

Let $\mathfrak{U}^0_\alpha(S_0)$ be the set consisting of

(1^0) all α-factors of positive clauses in S, and

(2^0) all complete factors of all non-positive clauses in S.

Let $\mathfrak{U}_\alpha(S)$, for any set of factors S be the union of S and of the set of consisting of

(1) all α-factors of paramodulants whose parents are α-factors in S, and

(2) for every P_1-resolvent C both of whose parents are in S and one of which is an α-factor A and the other of which, B, is non-positive and is resolved upon its first distinguished literal

(a) if C is positive then all α-factors of C, and

(b) if C is non-positive then exactly one factor consisting of the clause C; the distinguished literals of C descend from the distinguished literals of B and are totally ordered by the ordering inherited from that of the distinguished literals of B.

In obtaining $C \in \mathcal{U}_{\alpha}(S)$ we insist that only distinguished literals be paramodulated or resolved upon.

Theorem 2. Suppose that the set of clauses S_0 has no normal model and that $\leq$ is an α-ordering for S_0. Then for some $n \geq 0$, $\square \in \mathcal{U}_{\alpha}^{n}(S_0 \cup E_4)$.

Theorem 2 follows from the fact that we can insist that satellite factors of clashes in T' be α-factors. Further examining the construction of T" from T' we see that Theorem 2 continues to hold withthe following restrictions:

(r1) All applications of paramodulation are primary except when the second parent is a clause $B \in E_4$ in which case the term paramodulated upon is one of the arguments of the function symbol occurring in B.

(r2) If $B \in E_4$ then B is not a first parent of a paramodulant and as parent of a resolvent it may be replaced by the clause $\{x = x\}$.

(r2) follows by constructing the tree T" directly from T instead of from T'.

It should now be fairly clear that the paramodulation method of Theorem 2 incorporating restrictions (r1) and (r2) is, in a sense, isomorphic to the method of hyper-resolution with equality axioms. From this fact it follows that any strategy compatible with the hyper-resolution method translates into a strategy compatible with paramodulation. Clearly deletion of tautologies and deletion of subsuming clauses are two such strategies. Moreover completeness for hyper-resolution of renaming [8] implies the same for paramodulation provided the equality symbol itself is not renamed.

Semantic Trees.

The notion of semantic tree was formulated by Robinson in [13] and investigated in the version described below in [5]. We include a summary of definitions and propositions for the special case of semantic tree used in the proofs of Theorems 3, 4 and 5.

Semantic trees are finitely branching but possibly infinite trees with the root as greatest element lying above all other nodes including any tips which are minimal elements. Thus regard semantic trees as growing downwards rather than upwards as in the case of derivation trees. Given a totally ordered (finite or infinite) set of ground atoms $K = \{A_1,\dots,A_n,\dots\}$ where $i<j$ implies that A_i precedes A_j, a binary semantic tree for K is a binary tree T with sets of literals attached to its nodes, such that

(1) ϕ is attached to the root, and

(2) if $\{A_n\}$ or $\{\overline{A}_n\}$ is attached to the node N then $\{A_{n+1}\}$ and $\{\overline{A}_{n+1}\}$ are attached to the two nodes lying immediately below N.

Given $N \in T$, $\mathfrak{A}_N$ called the assignment at N, is the set consisting of the literals attached to N and to all nodes lying above N in T. A clause C fails at N if for some ground substitution σ the complements of all the literals in $C\sigma$ occur in $\mathfrak{A}_N$. If S is a set of clauses then N is a failure point for S if some $C \in S$ fails at N but no $D \in S$ fails at any node above N. If no $C \in S$ fails at N then N is free for S. T is closed for S if every path beginning at the root and terminating, if at all, only at a tip of T contains a failure point for S. N is an inference node for S if the nodes immediately below N are failure points for S. If S is unsatisfiable and K includes all atoms in some ground unsatisfiable set of instances S' of instances of clauses in S then we say that T is a semantic tree for S (relative to K).

If S is unsatisfiable and T is a semantic tree for S then T is closed for S. If T is closed for a set of clauses S then S is unsatisfiable and moreover T contains at least one inference node N for S. Some clause $C \in \mathcal{R}(\mathcal{R}^0(S))$ fails at N and its parents in S fail at the nodes immediately below N. More generally given any node $N \in T$ free for S then for some n and $C \in \mathcal{R}^n(S)$, C fails at N. Only $\square$ fails at the root of T.

Trivialisation of Inequalities.

Resolving a factor $C = \{s \neq t\} \dot{\cup} C_0$ with $\{x = x\}$ produces the clause $C_0\theta$ where θ is an m.g.u. of the set $\{s, t\}$. We shall call such a resolution the operation of trivialising an inequality [17]. Application of this operation is necessary for both the hyper-resolution and paramodulation methods. Corollary 1 of the more general Theorem 3 below states in effect that Theorem 2 with restrictions (r1) and (r2) continues to hold with the restriction.

(r3) No inequality in a clause C is trivialised unless either C belongs to the original set S_0 or else C is itself the result of trivialising an inequality.

Strictly speaking Theorem 2 with restrictions (r1) - (r3) needs to be modified to allow the trivialisation of distinguished literals other than just the first distinguished literal of non-positive factors.

Theorem 3. Suppose $S = S_0 \dot{\cup} S_1$ is unsatisfiable where S_1 is a satisfiable set of unit clauses. Then the set $S_0 \cup R$ is unsatisfiable where R is the set of resolvents of clashes with nuclei in S_0 and satellites in S_1.

Proof. Assume first that S is a set of ground clauses. Let $S_1 = \{\{L_1\}, \ldots, \{L_n\}\}$. We prove the theorem for this case by showing by induction that for all $k \leq n$:

$U_k = S_0 \cup R_k \cup (S_1 - \{\{L_1\}, \ldots, \{L_k\}\})$ is unsatisfiable where R_k is the set of resolvents of clashes with nuclei in S_0 and satellites in $\{\{L_1\}, \ldots, \{L_k\}\}$.

$U_0 = S$ is unsatisfiable. Suppose that U_k is unsatisfiable for $0 \leq k \leq n$. Let T be a binary semantic tree for U_k relative to the set of atoms occurring in U_k ordered in such a way that the atom $|L_{k+1}|$ occurs last. T is closed for U_k; we claim that T is also closed for U_{k+1} and that U_{k+1} is therefore unsatisfiable. If $\{L_{k+1}\}$ fails on T at a failure point for U_k then it fails below an inference node N for U_k. The clause failing at the second failure point below N belongs to $S_0 \cup R_k$. The resolvent of these two clauses belongs to R_{k+1} and fails at N. Since $R_k \subseteq R_{k+1}$, it follows that T is closed for U_{k+1} and that U_{k+1} is unsatisfiable. But then $U_n = S_0 \cup R$ is unsatisfiable.

If S is not a set of ground clauses let $S' = S_0' \dot{\cup} S_1'$ be an unsatisfiable set of ground instances of clauses in S where S_0' and S_1' are instances of clauses in S_0 and S_1 respectively. Then $S_0' \cup R'$ is unsatisfiable where R' is the set of resolvents of clashes with nuclei in S_0' and satellites in S_1'. But by the lifting lemma for clashes, $S_0' \cup R'$ is a set of ground instances of $S_0 \cup R$, which is therefore unsatisfiable.

<u>Corollary 1</u>. Suppose $S = S_0 \cup E$ is unsatisfiable. Then $S_0 \cup R \cup E_2 \cup E_3$ is unsatisfiable where R is the set of resolvents of clashes with nuclei in S_0 and with satellites in E_1.

<u>Proof</u>. Take $S_0 \cup E_2 \cup E_3$ above to be the S_0 of Theorem 1. Then $U = S_0 \cup R_0 \cup E_2 \cup E_3$ is unsatisfiable where R_0 is the set of resolvents of clashes with nuclei in $S_0 \cup E_2 \cup E_3$ and satellites E_1. We shall show that resolvents of clashes with nuclei in E_2 or E_3 can be removed from R_0 without affecting the unsatisfiability of U.

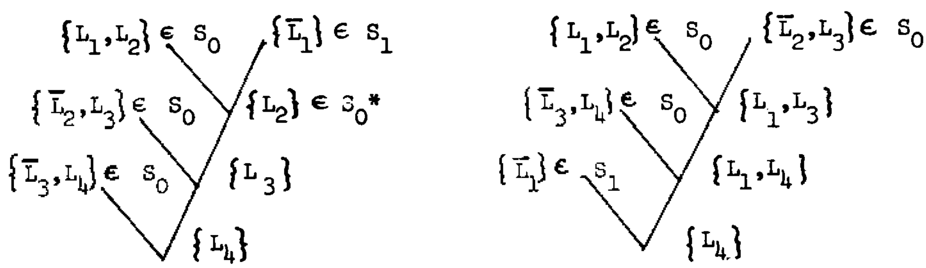
Let S' be an unsatisfiable set of ground instances of clauses in S. We may choose S' so that it contains no tautologies and no instances D' of a clause in E_2 where D' is of the form $\{t_i \neq t_i, f(t_1,\ldots,t_n) = f(t_1,\ldots,t_n)\}$, because such an instance of D is subsumed by the instance $\{f(t_1,\ldots,t_n) = f(t_1,\ldots,t_n)\}$ of $\{x = x\}$. We may assume that each resolvent C in R_0 is obtained by lifting a clash whose nucleus B' and satellites belong to S'. But then it is easy to verify that if C is the resolvent of a clash with nucleus B in E_3 then the corresponding instance B' of B in S' is a tautology and C may be eliminated from U. Similarly if $C \in R_0$ is the resolvent of a clash with nucleus B in E_2 then the corresponding instance B' of B in S' is of the form $\{t_i \neq t_i, f(t_1,\ldots,t_n) = f(t_1,\ldots,t_n)\}$ and B may be eliminated from U.

Thus every clause in $R_0 - R$ may be removed from U without affecting its unsatisfiability. It follows therefore that the set of clauses $S_0 \cup R \cup E_2 \cup E_3$ is unsatisfiable.

Both Theorems 3 and 5 below are versions of the throw-away strategies discussed in [9].

Theorem 3 implies that satisfiable sets S_1 of unit clauses may be effectively preprocessed out of a set of clauses $S = S_0 \dot{\cup} S_1$ before attempting to find a refutation of the resulting set S_0^*. Our intuition is that such preprocessing is likely to increase the efficiency of obtaining proofs of more difficult theorems. The figure below gives a simple example of two derivations of the same clause. Only the first derivation will be generated if the original set S_0 is preprocessed. If the entire set S_0^* must be generated before attempting to find a refutation then this method of preprocessing may be inefficient for proving theorems which have a simple proof which can be detected for instance with less effort than that involved in generating all of S_0^* itself. On the other hand since resolving a clause $A \in S_0$ with a unit clause in S_1 produces a clause containing fewer literals than are contained in A we may expect that this preprocessing procedure will tend to retain the simplest of those derivations which differ by permuting occurrences of clauses from S_1 along their branches. Finally even for the case of simpler theorems preprocessing can be made more efficient by simultaneously generating S_0^* and generating resolvents from S_0^*.

Example.



Notice that the redundancy exemplified here can not be removed by implementing singly connectedness [21] and is not removed by hyper-resolution, since both derivations are by hyper-resolution.

The Subsumption Theorem.

The following theorem, applied in the proof of Theorem 5 below, is of independent interest because it provides partial information about the extent of the deduction completeness of resolution.

Theorem 4. Let S be a non-empty set of clauses and C a non-tautologous clause logically implied by S. Then for some $n \geq 0$ there is a clause $C' \in \mathcal{R}^n(S)$ which subsumes C. Moreover if C is positive then $C' \in \mathcal{H}^m(S)$, for some $m \geq 0$.

Proof. If S implies C then $S \cup \{\overline{C}\}$ is unsatisfiable, where the sentence $\overline{C}$, in prenex normal form, is existential and its matrix is a conjunction of literals. S contains no existential quantifiers. Eliminating existential quantifiers from $S \cup \{\overline{C}\}$ we obtain an unsatisfiable set of clauses $S_0 = S \cup \{\{\overline{L}_1\}, \ldots, \{\overline{L}_n\}\}$ where each $\overline{L}_i$ is a ground literal. Notice that C can be reobtained from $\{L_1, \ldots, L_n\}$ by applying the substitution σ^* which substitutes for each Skolem constant a the variable x in $\overline{C}$ which was replaced by a when eliminating existentially quantified variables.

Let T be a binary semantic tree for S_0 relative to some set of ground atoms K containing all atoms in some ground unsatisfiable set S_0' of instances of clauses in S_0. Let K be ordered in such a way that the atoms $|L_1|$,..., $|L_n|$ precede all other atoms in K. Let T' be the subtree of T rooted in the node N to which is assigned the set of literals $\{\overline{L}_1,\ldots,\overline{L}_n\}$ (N exists because C is not a tautology). T and T' are both closed for S_0. Moreover, since no clause $\{\overline{L}_i\}$ fails in T', T' is closed for S and some $C' \in \mathcal{R}^n(S)$ fails at N. But then, by the definition of failure, there is a substitution σ such that $C'\sigma \subseteq \{L_1,\ldots,L_n\}$. Let $\sigma' = \sigma\sigma^*$ then $C'\sigma' \subseteq \{L_1,\ldots,L_n\}\sigma^* = C$ and therefore C' subsumes C.

If C is positive we take T to be an M-clash tree for S_0 where M is the set of all negative ground literals which are complements of the atoms occurring in some unsatisfiable set S_0' of ground instances of clauses in S_0(see [5]). Let T' be any subtree of T rooted in a node to which is assigned the set of literals $\{\overline{L}_1,\ldots,\overline{L}_n\}$. Some $C' \in \mathcal{H}^n(S)$, for some $n \geq 0$, fails at the root of T'. It follows that C' subsumes C.

A weaker version of Theorem 4 was first reported in [7] . More recently a more general theorem has appeared in [19] . Theorem 4 unfortunately does not settle the problem for resolution of deriving consequences from assumptions. That this is so is due to the fact that if A and B are sentences of the first-order logic, if A implies B, and if A* and B* are the sets of clauses corresponding to A and B, then it is not generally true that A* implies B*. $A = \exists y \forall x P(x,y)$ and $B = \forall x \exists y P(x,y)$ provide a simple counterexample.

Permutation of Inferences.

Theorem 3 and its corollary are permutation theorems in the sense that they can be interpreted as stating that inferences in certain derivation trees can be permuted in some regular way. Theorem 5 and its corollary are permutation theorems in the same sense. The corollary to Theorem 5, stated in terms of paramodulation, asserts that Theorem 1 continues to hold with restrictions (r1) - (r5) where (r4) and (r5) are the following:

(r4) No resolvent is the parent of a paramodulant.

(r5) Given any complete resolution method for the predicate calculus (i.e. set-of-support, P_1-deduction, AM-clashes, etc.) we may insist that every resolvent be generated in accordance with that method.

The completeness of the method corresponding to Theorem 1 and restrictions (r1), (r2), (r4) and (r5) can be obtained by analyzing the abstract of the original Robinson-Wos completeness proof [16] . It was in fact this observation which originally motivated Theorem 5. Theorem 1 and restrictions (r3) and (r4) assert that any paramodulation and resolution refutation can be obtained in the canonical form where all trivialisations of inequalities precede all paramodulations which precede resolutions.

Suppose that $S = S_0 \dot{\cup} S_1$ and that each clause in S_1 is non-positive. Define the set of <u>S_1-resolvents from S_0</u> to be the smallest set containing

(1) each clause $C \in S_0$ and

(2) each resolvent of a clash with nucleus a complete factor of some clause in S_1 and with satellites factors of S_1-resolvents from S_0.

Notice that each resolvent obtained by (2) is obtained by resolving on all and only on the distinguished literals of the complete nucleus factor of the clash. In case $S_1 = E_2 \cup E_3$ each S_1-resolvent from S_0 is either a clause in S_0 or a clause obtainable from $S_0 \cup E_4$ by primary paramodulation without resolution.

<u>Theorem 5.</u> If $S = S_0 \dot{\cup} S_1$ is unsatisfiable then some finite set S^* of S_1-resolvents from S_0 is also unsatisfiable.

<u>Corollary 2.</u> If the set of clauses S has no normal model and if S_0 is the closure of S under the operation of trivialising inequalities, then there is a finite unsatisfiable set of clauses S^* such that $C \in S^*$ implies that $C \in S_0$ or C can be derived from $S_0 \cup E_4$ by paramodulation without resolution.

<u>Proof of Corollary 2.</u> If S has no normal model then $S \cup E$ is unsatisfiable and, by Corollary 1, $S_0 \cup E_2 \cup E_3$ is unsatisfiable. Taking $E_2 \cup E_3 = S_1$, applying Theorem 5 and the definition of S_1-resolvent from S_0, the conclusion of the corollary follows.

The proof of Theorem 5 requires two lemmas.

<u>Lemma 1.</u> Let T be a hyper-resolution derivation of a positive non-tautologous ground clause C from ground clauses $S \dot{\cup} \{D\}$ where D is non-positive and occurs in T only at the nucleus node of T immediately above the root. Then there is a hyper-resolution derivation T^* of a clause $C' \subseteq C$ from clauses S^* where S^* is a set of $\{D\}$-resolvents from S.

<u>Proof of Lemma 1.</u> Let $D = \{\overline{L}_1,\ldots,\overline{L}_n\} \dot{\cup} D_0$ where D_0 is the maximal positive subclause of D; let $C = \{K_1,\ldots,K_m\}$. Then $S_0 = S \cup D \cup \{\{\overline{K}_1\},\ldots,\{\overline{K}_m\}\}$ is unsatisfiable since $S \cup D$ implies C. Let $S_0' = S \cup R \cup \{\{\overline{K}_1\},\ldots,\{\overline{K}_m\}\}$ where R is the set of resolvents of clashes $\mathcal{C}$ having clauses in S as satellites, D as nucleus and where the literals $\overline{L}_1,\ldots,\overline{L}_n$ are the literals in D resolved upon in $\mathcal{C}$. $S^* = S \cup R$ is a set of $\{D\}$-resolvents from S. We shall show that S_0' is unsatisfiable. By the unsatisfiability of S_0' it will follow that S^* implies C and by Theorem 4, since C is not a tautology, there is a hyper-resolution derivation T^* of a clause $C' \subseteq C$ from S^*.

To prove the lemma it remains to show that S_0' is unsatisfiable. Let T' be a binary semantic tree for S_0 relative to the set of atoms occurring in S_0

ordered in any way. Then T' is closed for S_0 since S_0 is unsatisfiable. It suffices to show that if $\mathcal{B}$ is a complete path from the root of T' to a tip of T' such that D fails at some node $N \in \mathcal{B}$ then some clause $D' \in R$ fails at some node $N' \in \mathcal{B}$. From this it follows that T' is closed for S_0' and that S_0' is unsatisfiable.

Let $\mathcal{B}$ be such a path and $N \in \mathcal{B}$ such a node. For $1 \le i \le n$ let $\mathcal{B}_i$ be the complete path of T' which differs from $\mathcal{B}$ only in L_i, i.e. $\mathcal{B}_i = (\mathcal{B} - \{L_i\}) \cup \{\overline{L}_i\}$. Then each such $\mathcal{B}_i$ contains a failure point N_i for some clause $A_i = \{L_i\} \mathbin{\dot\cup} A_{0i} \in S_0$. But $A_i \neq D$ since $\mathcal{B}_i$ does not contain L_i and $A_i \neq \overline{K}_j$ for any j, $1 \le j \le m$, since L_i is positive and $\overline{K}_j$ is negative. Therefore $A_i \in S$. Let $D' = A_{01} \cup \ldots \cup A_{0n} \cup D_0$. Then D' is the resolvent of the clash $\mathcal{C} = \{A_1, \ldots, A_n, D\}$ and D' fails at some node $N' \in \mathcal{B}$.

<u>Lemma 2</u>. Suppose T is a hyper-resolution derivation of $\square$ from ground clauses S and suppose $C \in S$ is a positive clause which occurs at a tip $N \in T$. Let $C' \subseteq C$. Then there is a hyper-resolution derivation T' of $\square$ and a one-one correspondence Φ from the tips of T' onto a subset of the tips of T such that

(1) C' occurs at the tip $N_0' = \Phi^{-1}(N_0)$ in T', and

(2) for all tips $N' \in T'$, N' N_0', the clause occurring at N' in T' is identical to the clause occurring at $\Phi(N')$ in T.

<u>Proof of Lemma 2</u>. (by induction on the number n of nodes in T). If n = 1 then C = C' = $\square$, T' = T and the correspondence Φ is the identity. Suppose now that T has k nodes and that the lemma holds for any derivation tree having fewer than k nodes. Let $\mathcal{C}$ be the hyper-resolution clash of which C is a satellite at N_0. There are two cases to consider: (1) the L in C resolved upon in $\mathcal{C}$ occurs in C' and (2) L does not occur in C'.

<u>Case (1)</u>. Let $\mathcal{C}' = (\mathcal{C} - \{C\}) \cup \{C'\}$. Then $\mathcal{C}'$ is a hyper-resolution clash and its hyper-resolvent D' subsumes the hyper-resolvent D of $\mathcal{C}$. Let T_1 be the derivation obtained by ignoring all of the nodes in T lying above the node N_1 which lies immediately below N_0. Then T_1 is a hyper-resolution derivation of $\square$ and the clause D at N_1 is subsumed by D'. T_1 contains fewer than k nodes and by induction hypothesis therefore there is a hyper-resolution derivation T_1' and one-one correspondence Φ_1 from the tips of T_1' onto tips of T_1 such that D' occurs at $\Phi_1^{-1}(N_1)$ and for $N' \in T_1'$, $N' \neq \Phi_1^{-1}(N_1)$, the clauses occurring at N' and $\Phi_1(N')$ are identical. Let T_0' be obtained from the subtree T_0 of T rooted in N_1 by replacing the clauses C and D at N_0 and N_1 by C' and D' respectively. Let $\Phi_0(N) = N$ for every tip N of T_0'. T_0' is a hyper-resolution derivation of D'. Let T' be obtained by identifying the tip $\Phi_1^{-1}(N_1)$ of T_1' with the root of T_0'. Then T' is the desired hyper-resolution derivation of $\square$ and the desired mapping Φ is defined as Φ_1 for tips of T' which belong to T_1' and as Φ_0 for tips of T' which belong to T_0'.

Case (2). If $L \notin C'$ then C' subsumes the resolvent D of $\mathcal{C}$. Let N_1 and T_1 be as in case (1). Since T_1 contains fewer than k nodes and since C' subsumes D, the induction hypothesis applies to T_1 and to the node $N_1 \in T_1$. The derivation T_1' and mapping Φ_1 such that C' occurs at $\Phi_1^{-1}(N_1)$ are the desired hyper-resolution derivation T' of $\Box$ and mapping Φ.

Proof of Theorem 5. Suppose first that S is a set of ground clauses. Let S^* be the finite set of all S_1-resolvents from S_0. Let T be a hyper-resolution derivation of $\Box$ from S containing no tautologies and let T' be obtained from T by consecutively deleting all nodes above each S_1-resolvent from S_0, i.e. T' is the hyper-resolution subtree of T which derives $\Box$ from clauses in $S^* \cup S_1$ and which contains S_1-resolvents only at its tips. We shall transform T' into a tree T_0 which derives $\Box$ from clauses in S^*. It will follow that the finite set S^* is unsatisfiable.

The construction of T_0 is by induction on the number n of occurrences of clauses in S_1 at the tips of T'. If $n = 0$ then T' is already a derivation of $\Box$ from some subset of clauses in S^*. Suppose then that T' contains $k > 0$ occurrences of clauses from S_1 at its tips and suppose that any hyper-resolution derivation T'' of $\Box$ from $S^* \cup S_1$ which contains fewer than k such occurrences and no tautologies can be transformed into a derivation T_0 of $\Box$ from S^*. We shall transform T' into such a tree T''. Then T_0, the transform of T'', is also the desired transformation tree for T'.

Let N be an interior node in T' such that the hyper-resolvent C occurring at N is the resolvent of a clash with nucleus $D \in S_1$ and such that the tips of T' lying above N contain only this one occurrence of a clause from S_1. The subtree of T' rooted in N derives C from $S^* \dot{\cup} \{D\}$. By Lemma 1, since C is not a tautology, there is a hyper-resolution derivation T_1 of some $C' \subseteq C$ from S^*. Let T_2 be obtained from T' by ignoring all of T' above the node N. Then, by Lemma 2, there is a hyper-resolution derivation T_3 of $\Box$ from $S^* \cup S_1 \cup \{C'\}$ and a one-one correspondence Φ from the tips of T_3 onto a subset of the tips of T_2. T_3 contains fewer than k occurrences of clauses from S_1 at its tips and the clause C' occurs at the tip $\Phi^{-1}(N)$ of T_3 corresponding to N in T_2. Let T'' be obtained from T_1 and T_3 by identifying the root of T_1 with the tip $\Phi^{-1}(N)$ of T_3. T'' is the desired hyper-resolution derivation of $\Box$ from $S^* \cup S_1$. That T'' contains no tautologies can be verified by checking that the derivations T_1 and T_3 contain no tautologies.

If S is not a set of ground clauses then let $S' = S_0' \dot{\cup} S_1'$ be an unsatisfiable set of ground instances of clauses in S, where S_0' and S_1' are instances of clauses in S_0 and S_1 respectively. By the part of the theorem already proved, there is a finite unsatisfiable set $S^{*\prime}$ of S_1-resolvents from S_0'. By the lifting lemma for clashes, for every clause $A' \in S^{*\prime}$ there is an S_1-resolvent A from S_0

which has A' as an instance. Let S* be the set of all such A for all A' $\in$ S*'. Then S* is unsatisfiable since its set of instances S*' is unsatisfiable.

The reader familiar with Andrews' paper [1] will note the similarity between the proof of Theorem 5 using Lemmas 1 and 2 and the proof in [1] of Theorem 1 using Lemmas 1-5.

Concluding Remarks.

(1) The argument for using hyper-resolution with equality axioms is based on a comparison with paramodulation and resolution applied to sets of clauses containing the axioms E_4. In this connection it should be noted that Robinson and Wos [15] conjecture the completeness of a more restricted paramodulation system: in this system one adds to a set of clauses S_0 which has no normal model just the clause $\{x = x\}$ and applies paramodulation and resolution to derive $\Box$. Interpretation of this system in terms of hyper-resolution is not entirely straight-forward and comparison of these two systems is therefore correspondingly more difficult.

(2) The set E_2 need not include axioms for Skolem-function letters f which result in S_0 from the elimination of existential quantifiers. That this is so is easily verified by noting that before eliminating existential quantifiers we need only include axioms of functional substitutivity E_2 for the function letters actually occurring in the original fully quantified set of sentences. This improvement of the hyper-resolution method induces a corresponding improvement of (r1) and (r2) in the paramodulation method. In the case where the original quantified set of sentences contains no function letters, the set E_2 is empty, and for paramodulation, (r1) and (r2) state that E_4 may be replaced by the single clause $\{x = x\}$. We do not consider that the well-known procedure for eliminating function letters by introducing new predicate letters reduces the problem of proving the Robinson-Wos conjecture to the special case just verified. This conjecture remains an important problem which has counterparts in the f-matching method [4], in the lifting lemma for generalised resolution [13] and in E-resolution [10].

References.

[1] Andrews, P.B., "Resolution with Merging", Journal of the Association for Computing Machinery, 15, 367-381, July 1968.

[2] Brown, T.C. Jr., "Resolution with Covering strategies and Equality Theory", internal memorandum, California Institute of Technology, 1968.

[3] Chang, C.L., "Renamable Paramodulation for Automatic Theorem-Proving with Equality", internal memorandum, National Institutes of Health, Bethesda, Maryland, 1969.

[4] Darlington, J.L., "Automatic Theorem-Proving with Equality Substitutions and Mathematical Induction", Machine Intelligence 3, edited D. Michie, Edinburgh University Press , 113-127, 1968.

[5] Hayes, P.J., and Kowalski, R., "Semantic Trees in Automatic Theorem-Proving", Machine Intelligence 4, edited B. Meltzer and D. Michie, Edinburgh University Press, 1969.

[6] Kowalski, R., "Studies in the Completeness and Efficiency of Theorem-Proving by Resolution", Ph.D. thesis, University of Edinburgh, 1969.

[7] Lee, Char-tung, "A Completeness Theorem and a Computer Program for Finding Theorems Derivable from Given Axioms", Ph.D. thesis, University of California, Berkeley, 1967.

[8] Meltzer, B., "Theorem-Proving for Computers: some results on resolution and renaming", Computer J. 8, 341-343, 1966.

[9] Meltzer, B., "Some Notes on Resolution Strategies", Machine Intelligence 3, edited D. Michie, Edinburgh University Press, 71-76, 1968.

[10] Morris, J.B., "E-Resolution: Extension of Resolution to Include the Equality Relation", Proceedings of the International Joint Conference on Artificial Intelligence, Washington, D.C., 1969.

[11] Robinson, J.A., "Automatic Deduction with Hyper-resolution", Int.J. Computer Math. 1, 227-234, 1965.

[12] Robinson, J.A., "A Review of Automatic Theorem-Proving", Proceedings of Symposia in Applied Mathematics, 19, Mathematical Aspects of Computer Science, American Mathematical Society, 1967.

[13] Robinson, J.A., "The Generalised Resolution Principle", Machine Intelligence 3, edited D. Michie, Edinburgh University Press, 77-93, 1968.

[14] Robinson, J.A., "The Present State of Mechanical Theorem-Proving", Fourth Annual Systems Symposium, to appear in Proceedings.

[15] Robinson, G., and Wos, L., "Paramodulation and Theorem-Proving in First-Order Theories with Equality", Machine Intelligence 4, edited B. Meltzer and D. Michie, Edinburgh University Press, 1969.

[16] Robinson, G., and Wos, L., "Completeness of Paramodulation", Journal of Symbolic Logic, 34, 160, March, 1969.

[17] Silbert, E.E., "A Machine-Oriented Logic Incorporating the Equality Relation", Machine Intelligence 4, edited B. Meltzer and D. Michie , Edinburgh University Press, 1969.

[18] Slagle, J.R., "Automatic Theorem Proving With Renamable and Semantic Resolution", Journal of the Association for Computing Machinery, 14, 687-697, October 1967.

[19] Slagle, J., Chang, C. and Lee, C., "Completeness Theorems for Semantic Resolution in Consequence Finding", Proceedings of the International Joint Conference on Artificial Intelligence, Washington, D.C., 1969.

[20] Wos, L., Carson, D., and Robinson, G., "The Unit Preference Strategy in Theorem Proving", A.F.I.P.S. Conference Proceedings 26, Washington, D.C., 615-621: Spartan Books, 1964.

[21] Wos, L., Robinson, G., Carson, D.F., and Shalla, L., "The Concept of Demodulation in Theorem-Proving", Journal of the Association for Computing Machinery, 14, 698-709, October 1967.