SOME COMPLETENESS RESULTS FOR A CLASS OF INEQUALITY PROVERS

by

W.W. Bledsoe, Robert Neveln and Robert Shostak

March 1981 ATP-60

This work was supported by NSF Grant MCS79-24198 and (SRI) AFOSR F49620-79-C-2099.

Some Completeness Results for a Class of Inequality Provers

by

W. W. Bledsoe, Robert Neveln and Robert Shostak

Abstract. A modified resolution procedure, RCF, which uses a restricted form of inequality chaining and variable elimination is proved to be complete, for first order logic. RCF allows chaining only on terms of the form $f(t_1, \ldots, t_n)$ where f is an uninstantiated function symbol and $n \geq 1$. (E.g., we never chain on variables.) Other results are given. A prover using RCS+, an extension of RCF, has been implemented and used to prove several moderately difficult inequality theorems, not proved earlier by general purpose automatic provers.

1. Introduction

One of the most effective procedures used in our inequality prover [1] is that of variable elimination, whereby a variable which is "eligible" (see below) in a clause, can be eliminated from that clause. For example, the clause

(1) $a \not< x \vee x \not< b \vee c \leq d$

can be replaced by the clause

(1') $a \not< b \vee c \leq d$

by elimination of the variable x (assuming that x does not occur in a,b,c, or d). Also, the variable x (which does not occur in a,b, or c) can be eliminated from the clause

(2) $a \not< x \vee b \leq c$

to produce the clause

(2') $b \leq c$.

In general, the variable x (which does not occur in a_i, b_j, or E) can be eliminated from the clause

$$(\bigvee_{i=1}^{n} a_i \not< x \vee \bigvee_{j=1}^{m} x \not< b_j \vee E)$$

to produce

$$(\bigvee_{i=1}^{n} \bigvee_{j=1}^{m} a_i \not< b_j \vee E) .$$

A variable is eligible in a clause if it does not occur within the arguments of an uninstantiated function symbol. Thus x is eligible in (1) but not in (3).

(3) $$a \not< x \vee x \not< b \vee f(x) \leq c ,$$

because it occurs as an argument of the uninstantiated function symbol f. The term $f(x)$ is called a shielding term because it "shields" the variable x, thereby preventing it from being eligible in (3).

The principal objective of the inequality prover [1] is to remove such shielding terms, by inequality "chaining" and other procedures (see below), so that variables can be eliminated.

The clause

$$R = (a \leq c \vee E_1 \vee E_2)\sigma$$

is said to be a chain-resolvent of clauses

$$C_1 = (a \leq b \vee E_1) ,$$

and

$$C_2 = (b' \leq c \vee E_2) ,$$

if σ is the Mgu of $\{b,b'\}$. We also allow "self-chaining" whereby $E\sigma$ is inferred from $(b < b' \vee E)$.

We will designate by RC ("resolution chaining") a procedure which only uses chaining (as described above) and factoring. RC was shown to be complete by Slagle [2,3]. (See also Lemma 4, Section 3.) Unfortunately RC alone is not very powerful as a prover. In order to strengthen RC, we have added VE (variable elimination, as described above), and have imposed restrictions on the chaining process, which help control proof search tree.

Two such procedures are RCF and RCS, which are described as follows. Both RCF and RCS use VE, and both restrict chaining as follows: Let

$$R = (a \leq c \vee E_1 \vee E_2)\sigma$$

be the chain resolvent of

$$C_1 = (a \leq b \vee E_1) \quad \text{and} \quad C_2 = (b' \leq c \vee E_2) \ ,$$

where $\sigma = \text{Mgu}(b,b')$. We accept R as an RCF chain resolvent if

(1) all of a,b,b',c are ground terms (and hence $b = b'$), or

(2) b and b' are both of the form $f(t_1, \ldots, t_n)$ where f is an uninstantiated function symbol, and $n \geq 1$.

And we accept R as an RCS chain resolvent, if additionally, in case (2), either b or b' is non-ground, i.e., either b or b' is a shielding term.

Other restrictions on RC include RCM and RC+. RCM uses "multiple cuts", where, for example, two clauses

$$C_1 = (a \leq c \vee b \leq c \vee E_1)$$

and

$$C_2 = (c \leq d \vee c \leq e \vee E_2)$$

are chained, in one step, on both c's in C_1 and both c's in C_2 to obtain

$$(a \leq d \vee a \leq e \vee b \leq d \vee b \leq e \vee E_1 \vee E_2) .$$

RC+ permits literals of the form

$$a_1 + \ldots + a_n \leq b_1 + \ldots + b_m ,$$

where the a_i and b_j are traditional terms (with no occurrence of +). Two such literals are chained by cancelling like terms (after unification). For example,

$$f(x) + a \leq h(x)$$

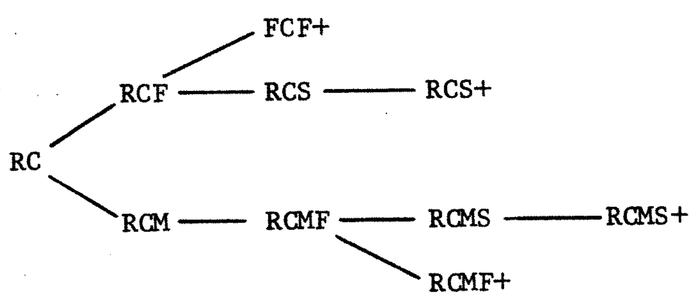
and

$$b \leq f(c)$$

are RC+ chained to obtain

$$b + a \leq h(c) .$$

By combining these restrictions we obtain the following diagram



where more restrictive (stronger) procedures are shown to the right.

It is the purpose of this paper to prove that RCF, RCF+, RCM, RCMF, and RCMF+ are complete.

It is conjectured that RCS is also complete, as well as RCS+, RCMS, and RCMS+.

RCS+ is the procedure described in [1]. But RCF+, which is proved complete here, is equally as strong as RCS on the examples given in [1]. Since we allow quantification and uninterpreted function symbols, we can encode all of first order logic. For example, the atom $P(x,y)$ can be written as

$$f(x,y) \leq 0$$

where f is a new uninterpreted function symbol associated with P. Hence our procedures RC, RCF, etc. are complete for all of first order logic.

In each of RCF, RCS, RCM, etc., it is required that variable elimination (VE) be applied immediately when a variable becomes eligible in a clause C, and that C be discarded and replaced by its VE-resolvent.

The reader might prefer to skip to Section 3, page 19, and refer back to Section 2 as needed.

2. Definitions and Logical Basis

2.1. Axioms for total (linear) order: T

1. $x \nless x$ — Anti-reflexive
2. $x < y \rightarrow y \nless x$ — Anti-symmetry
3. $x < y \wedge y < z \rightarrow x < z$ — Transitivity
4. $y \nless x \wedge z \nless y \rightarrow z \nless x$ — "

It is convenient (but not necessary) to also use the symbol "$\leq$", where $a \leq b$ is equivalent to $b \nless a$. Then axioms 1-4 can be written

1. $x \leq x$
2. $x < y \rightarrow x \leq y$
3. $x < y \wedge y < z \rightarrow x < z$
4. $x \leq y \wedge y \leq z \rightarrow x \leq z$

The axioms of 1 - 4 are also called the inequality axioms.

Definition. Let $S_{\leq}$ be the set of clauses corresponding to the inequality axioms,

$$S_{\leq} = \{x \leq x,\ y \leq x \vee x \leq y,\ y \leq x \vee z \leq y \vee x < z,\ y < x \vee z < y \vee x \leq z\}\ .$$

2.2. Interpollation Axioms: I

1. $\forall x \exists y\ (y < x)$
2. $\forall x \exists y\ (x < y)$
3. $\forall xy\ (x < y \rightarrow \exists w\ (x < w < y))$
4. $\forall xyz\ (x < z \wedge y < z \rightarrow \exists w\ (x < w < z \wedge y < w < z))$

...

Using, "$\leq$", these can be expanded to include

$$\forall x \; \exists y \; (y \leq x)$$
$$\forall x \; \exists y \; (x \leq y)$$
$$\forall xy \; (x \leq y \rightarrow \exists w \; (x \leq w \leq y))$$
$$\forall xyz \; (x \leq z \wedge y \leq z \rightarrow \exists w \; (x \leq w \leq z \wedge y \leq w \leq z))$$
$$\forall xyz \; (x \leq z \wedge y < z \rightarrow \exists w \; (x \leq w \leq z \wedge y < w < z))$$
$$\ldots$$

More precisely, let I, the <u>interpolation axiom</u>, be the infinite set

$$I = \{P: \exists n \in \mathbb{N} \; \exists m \in \mathbb{N} \; \exists L$$
$$(L \text{ is a function on } \{0,1,\ldots,n-1\} \times \{0,1,\ldots,n-1\}$$
$$\text{to } \{\leq, <\} \wedge P \text{ is}$$
$$\forall x_1 \cdots x_n \; \forall y_1 \cdots \forall m \; (\bigwedge_{i=1}^{n} \bigwedge_{j=1}^{m} (x_i L_{ij} y_j)$$
$$\rightarrow \exists w \; (\bigwedge_{i=1}^{n} \bigwedge_{j=1}^{n} x_i L_{ij} w \wedge w \; L_{ij} y_j)))\} ,$$

where $\mathbb{N} = \{0,1,2,\ldots\}$.

<u>Definition</u>. Let S_I be the (infinite) set of clauses corresponding to I, i.e.,

$$S_I = \{w_{10}(x) < x, \quad w'_{10}(x) \leq x , \quad x < w_{01}(x) , \quad x \leq w'_{01}(x) ,$$
$$x < w_{11}(x,y) \vee y \leq x , \quad x \leq w'_{11}(x,y) \vee y < x ,$$
$$x < w_{11}(x,y) \vee y \leq x , \quad x \leq w'_{11}(x,y) \vee y < x ,$$
$$w_{11}(x,y) < y \vee y \leq x , \quad w'_{11}(x,y) \leq y \vee y < x ,$$

(continued)

$$x < w_{21}(x,y,z) \vee z \leq x \vee z \leq y \ ,$$

$$y < w_{21}(x,y,z) \vee z \leq x \vee z \leq y \ ,$$

$$w_{21}(x,y,z) < z \vee z \leq x \vee z \leq y \ ,$$

$$x \leq w'_{21}(x,y,z) \vee z < x \vee z < y \ ,$$

$$y \leq w'_{21}(x,y,z) \vee z < x \vee z < y \ ,$$

$$w'_{21}(x,y,z) \leq z \vee z < x \vee z < y \ ,$$

$$x \leq w''_{21}(x,y,z) \vee z < x \vee z \leq y \ ,$$

$$\ldots \qquad \} \ .$$

More precisely, let

$$S_I = \{C: \exists\, n \in \mathbb{N}\ \exists\, m \in \mathbb{N}\ \exists\, k \in \mathbb{N}\ \exists\, \ell \in \mathbb{N}\ \exists\, L$$

$$(L \text{ is a function on } \{0,1,\ldots,n-1\} \times \{0,1,\ldots,m-1\}$$

$$\text{to } \{\leq, <\} \wedge k < n \wedge \ell < m \wedge$$

$$[C = (\bigvee_{i=1}^{n} \bigvee_{j=1}^{m} \sim (x_i L_{ij} y_j) \vee x_k L_{k\ell} y_\ell)$$

$$\vee\ C = (\bigvee_{i=1}^{n} \bigvee_{j=1}^{m} \sim (x_i L_{ij} y_j) \vee y_\ell L_{k\ell} x_k))\} \ .$$

The axioms for total order plus the interpolation axioms define the theory of dense linear order without endpoints [5]. This theory is decidable [6]. However, the class of formulas we are investigating contains quantification and uninterpreted function symbols and hence is undecidable (since any formula in first order logic can be encoded).

2.3. Equality Axioms

Definition. If S is a set of clauses then S_E is the set of clauses corresponding to the equality axioms for S. (See [8].)

2.4. Axioms for +

1.	$(x+y)+z \leq x+(y+z)$	Associativity
2.	$x+(y+z) \leq (x+y)+z$	Associativity
3.	$x+0 \leq x$	Zero
4.	$x \leq x+0$	Zero
5.	$x+y \leq y+x$	Commutativity
6.	$x+y \leq x+z \rightarrow y \leq z$	Cancellation
7.	$x+y \leq x \rightarrow y \leq 0$	Cancellation
8.	$x+y < x \rightarrow y < 0$	Cancellation

Definition. Let S_+ be the clauses corresponding to the axioms for $+$,

$$
\begin{aligned}
S_+ = \{ & (x+y)+z \leq x+(y+z) \, , \\
& x+(y+z) \leq (x+y)+z \, , \\
& x+y \leq y+x \, , \\
& x+z < x+y \vee y \leq z \, , \\
& x+z \leq x+y \vee y < z \, , \\
& x+0 \leq x \, , \\
& x \leq x+0 \, , \\
& x < x+y \vee y \leq 0 \, , \\
& x \leq x+y \vee y < 0 \} \, .
\end{aligned}
$$

2.5. Additional Definitions

Definition. Let S be a set of inequality clauses.

A term t is said to be isolated in a literal L of S if t occurs in L not within the arguments of any uninterpreted function symbol. t is isolated in S if it is isolated in a literal of S.

Thus t is isolated in each of $t \leq a$, $b < t + c$, $t \leq f(t)$.

A variable x is said to be eligible in a clause C (and in S) if it is isolated in C and does not occur within the arguments of an uninstantiated function symbol.

A term t is a shielding term of a clause C (and of S) if t has the form

$$f(t_1, \ldots, t_n)$$

where f is an uninstantiated function symbol, and t is isolated and not ground.

For example, x is eligible and f(y) is a shielding term in the clause

$$x + a \leq b \vee f(y) \leq c \ .$$

t and t' are called half literals of the literals $t \leq t'$ and $t < t'$.

Definition. A set S of inequality clauses is said to be:

RC-unsatisfiable if $(S \cup S_{\leq})$ is unsatisfiable, and we write $S \overset{RC}{\models} \square$.

Definition. If C is an inequality clause of the form

$$\bigvee_{i=1}^{n} (a_i L_i' x) \vee \bigvee_{j=1}^{m} (x L_j'' b_j) \vee E \ ,$$

where x is a variable which does not occur in E or one of the a_i or b_j, and for each i, j, L'_i is either $\leq$ or $<$, and L''_j is either $\leq$ or $<$, then

$$R = \bigvee_{i=1}^{n} \bigvee_{j=1}^{n} (a_i L_{ij} b_j) \vee E ,$$

is called a <u>VE-resolvent of C upon x,</u> where L_{ij} is $<$ if both L'_i and L''_j are $<$, and L_{ij} is $\leq$ otherwise.

Note that x is <u>eligible</u> in C.

<u>Definition</u>. If C is an inequality clause of the form

$$\bigvee_{i=1}^{n} (a_i L'_i x + a'_i) \vee \bigvee_{j=1}^{m} (x + b'_j L''_j b_j) + E ,$$

where x is a variable which does not occur in E or one of the a_i, a'_i, b_j or b'_j, and for each i, j, $L'_i, L'_j \in \{\leq, <\}$, then

$$R = \bigvee_{i=1}^{n} \bigvee_{j=1}^{n} (a_i + b'_j L_{ij} b_j + a'_i) \vee E ,$$

is called a <u>VE+ Resolvent of C upon x,</u> where L_{ij} is $<$ if both L'_i and L''_j are, and $\leq$ otherwise.

<u>Definition</u>. If C_1 and C_2 are inequality clauses of the form

$$C_1 = (a L' b \vee E_1) ,$$
$$C_2 = (b' L'' c \vee E_2) ,$$

where L' and L'' are in $\{\leq, <\}$, and b and b' are unifiable, then

$$R = (A L c \vee E_1 \vee E_2)\sigma$$

is said to be a chain resolvent of C_1 and C_2 upon b and b', where $\sigma = \mathrm{Mgu}\{b,b'\}$ and L is $<$ if either of L' or L'' is $<$, and $\leq$ otherwise.

Definition. If C is an inequality clause of the form

$$C = (b < b' \vee E)$$

and $\sigma = \mathrm{Mgu}\{b,b'\}$, then $E\sigma$ is said to be self-chain resolvent of C upon b and b', $E\sigma$ is also called a chain-resolvent of C.

Definition. If R is a chain resolvent of C_1 and C_2 upon b and b' or a self-chain resolvent of C upon b and b', and

(1) b and b' are both ground, or

(2) b and b' both have the form

$$f(t_1, \ldots, t_n)$$

where f is an uninstantiated function symbol with $n \geq 1$,

then R is called an RCF-chain resolvent of C_1 and C_2 upon b and b', (or of C upon b and b').

Definition. If R is an RCF-chain resolvent of C_1 and C_2 upon b and b', and either b or b' is a shielding term then R is called an RCS-chain resolvent of C_1 and C_2 upon b and b', (or of C upon b and b').

Definition. Let C_1 and C_2 be inequality clauses of the form

$$C_1 = (a\, L' \sum_{i=1}^{n} b_i) \vee E_1 ,$$

$$C_2 = (\sum_{j=1}^{m} b_i'\, L''\, c) \vee E_2 ,$$

where $L', L'' \in \{\leq, <\}$, $k \in \{1,\ldots,n\}$, $\ell \in \{1,\ldots,m\}$, $\sigma = \mathrm{Mgu}\{b_k, b'_\ell\}$, and let

$$R = ((a + \sum_{\substack{j=1 \\ j\neq \ell}}^{m} L\ c + \sum_{\substack{i=1 \\ i\neq k}}^{n}) \vee E_1 \vee E_2)\sigma ,$$

where L is $<$ if both L' and L'' are, and $\leq$ otherwise, and let R' be obtained from R by algebraic simplification whereby like terms on opposite sides of L are cancelled, (if all terms on one side of L are cancelled that side is replaced by 0). Then R' is called an <u>RC+ chain resolvent of</u> C_1 <u>and</u> C_2 <u>upon the literals</u> b_k <u>and</u> b'_ℓ. Also (the self-chaining case) if

$$C = (\sum_{i=1}^{n} a_i L \sum_{j=1}^{m} b_j) \vee E ,$$

where $L \in \{\leq, <\}$, $\sigma = \mathrm{Mgu}\{a_k, b_\ell\}$, then

$$R = ((\sum_{\substack{i=1 \\ i\neq k}}^{n} a_i L \sum_{\substack{j=1 \\ j\neq \ell}}^{m} b_j) + E)\sigma ,$$

(algebraically simplified), is called an <u>RC+ chain resolvent of</u> C <u>upon</u> a_k <u>and</u> b_ℓ.

<u>RCF+ and RCS+ chain resolvents</u> are defined similarly, where the appropriate restrictions are maintained on b_k, b_ℓ and a_k.

We note that, in all of these cases, we do <u>not</u> chain-resolve two clauses unless at least one term is cancelled. Thus we would not chain-resolve $a + b \leq c$ and $d + e \leq f$ to get $a + b + d + e \leq c + f$, unless $c = d$, $c = e$, $f = a$, or $f = b$. Also when an intermediate resolvent R is obtained which is simplified to R' by cancelling like terms, we keep only R' and discard R.

Definition. If C is a clause let

$$LE(C) = \begin{cases} '<' & \text{if every literal of } C \text{ has the predicate } '<' , \\ '\leq' & \text{otherwise .} \end{cases}$$

Definition. If C_1 and C_2 are inequality clauses of the form

$$C_1 = (\bigvee_{i=1}^{n} a_i L'_i b_i) \vee E_1 ,$$

$$C_2 = (\bigvee_{j=1}^{m} b'_j L''_j c_j) \vee E_2 ,$$

where $L'_i , L''_j \in \{\leq , <\}$, $\{b_1 , \ldots, b_n , b'_1 , \ldots, b_m\}$ is unifiable with Mgu σ, then

$$R = ((\bigvee_{i=1}^{n} \bigvee_{j=1}^{n} a_i L_{ij} b_j) \vee E_1 \vee E_2)\sigma$$

is called a multiple cut chain resolvent of C_1 and C_2 upon $b_1 , \ldots, b_n$, $b'_1 , \ldots, b'_m$, where $L_{ij} = LE(L_i , L_j)$. It is also called an RCM-chain resolvent of C_1 and C_2. Also Self-Chain Resolvents are called multiple cut chain resolvents, or RCM-chain resolvents.

RCMF, RCMS, RCMF+, and RCMS+ chain resolvents are defined in a similar way.

Definition. Let C be an inequality clause,

$$C = C' \vee D, \; C' = (a_1 \underset{1}{<} b_1 \vee \ldots \vee a_n \underset{n}{<} b_n), \; n \geq 2 ,$$

where $\underset{i}{<}$ is either $\leq$ or $<$, and let σ be a Mgu of $\{a_1 \leq b_1 , \ldots, a_n \leq b_n\}$, with the restriction that

(1) if one of the a_i's is a variable then no b_i can be a variable and σ is a Mgu of $\{b_1, \ldots, b_n\}$, and

(2) if one of the b_i's is a variable then no a_i can be a variable and σ is a Mgu of $\{a_1, \ldots, a_n\}$.

Then $((a_1 \underset{\cdot\cdot}{<} b_1) \vee D)\sigma$ is called an RCS-factor of C, where $\underset{\cdot\cdot}{<} = LE(C')$.

Thus $(a \leq f(a) \vee g(a) \leq c)$ is an RCS-factor of $(a < f(x) \vee x \leq f(a) \vee g(x) \leq c)$ but not of $(a \leq f(a) \vee x \leq f(a) \vee g(x) \leq c)$. That is, for RCS-factors, we do not allow a variable to unify with a (different) term unless that unification is forced by the unification of other non-variable terms.

Definition. An RC-factor is the same as an RCS-factor, except conditions (1) and (2) are removed.

Definition.

$$FACT(S) = S \cup \{C' : \exists\, C \in S (C' \text{ is an RC-factor of } C)\}.$$

$$FACT\text{-}S(S) = S \cup \{C' : \exists\, C \in S (C' \text{ is an RCS-factor of } C)\}.$$

Definition. If S is a set of inequality clauses, then

$$RC(S) = \{R : \exists\, C_1 \in FACT(S)\ \exists\, C_2 \in FACT(S)\ (R \text{ is a chain resolvent of } C_1 \text{ and } C_2)\}\ .$$

$$RC^0(S) = S\ ,$$

$$RC^{n+1}(S) = \cup\, RC(RC^n(S))\ , \qquad n \in \mathbb{N}\ ,$$

$$RC^\infty(S) = \bigcup_{n \in \mathbb{N}} RC^n(S)\ .$$

<u>Definition</u>. If $\Box \in RC^{\infty}(S)$ then we write

$$S \vdash^{RC} \Box$$

and say that there is an RC-deducting of $\Box$ from S (or there is an RC-refutation of S).

<u>Definition</u>. If S is a set of inequality clauses, then

$$VE(S) = \{R: \exists C \in S \text{ (R is a VE-Resolvent of C)}\} \cup S \sim \{C \in S: \text{C has a VE-Resolvent}\},$$

VE+(S) is defined similarly,

$RCF(S) = VE(S')$, where

$$S' = \{R: \exists C_1 \in \text{FACT-S}(S) \; \exists C_2 \in \text{FACT-S}(S) \text{ (R is a RCF-chain resolvent of } C_1 \text{ and } C_2)\}$$

$RCS(S) = VE(S')$, where

$$S' = \{R: \exists C_1 \in \text{FACT-S}(S) \; \exists C_2 \in \text{FACT-S}(S) \text{ (R is a RCS-chain resolvent of } C_1 \text{ and } C_2)\}$$

etc. for RCF+(S), RCM(S), RCMF(S), RCMS(S), RCMF+(S), and (RMS+(S), except that FACT(S) is used in the definition of RCM(S) (only).

Note that variable elimination is applied immediately to a new resolvent R, when it has an eligible variable, and R is discarded and replaced by its VE-resolvent.

<u>Definition</u>.

$$RCF^{o}(S) = S \ ,$$

$$RCF^{n+1}(S) = RCF^{n}(S) \cup RCF(RCF^{n}(S)) \ ,$$

$$RCF^{\infty}(S) = \bigcup_{n \in \mathbb{N}} RCF^{n}(S) \ .$$

Similarly for $RCS^{\infty}(S),\ldots,RCMS+^{\infty}(S)$.

<u>Definition</u>. If $\square \in RCF^{\infty}(S)$ we write

$$S \ \vdash_{RCF} \square$$

and say that there is an RCF-deduction of $\square$ from S. Similarly for

$$S \ \vdash_{RCF} \square$$

.

.

.

$$S \ \vdash_{RCMS+} \square \ .$$

3. Completeness Results

3.1. RCF Completeness

Lemma 1. If S is a set of inequality clauses, σS is ground, S is not ground, and S has no eligible variables, then S contains a shielding term t for which $t\sigma \neq x\sigma$ for all isolated variables x in S.

Proof. If S has no isolated variable we are finished. So let

x_1 be an isolated variable in clause C_1,
$f_1(x_1)$ be a shielding term in C_1 (since x_1 is not eligible, by hypothesis).

Now if $f_1(x_1)\sigma \neq V\sigma$ for each isolated variable V in S, we are finished. So suppose that

$f_1(x_1)\sigma = x_2\sigma$ for some isolated variable in clause C_2,
$f_2(x_2)$ is a shielding term in C_2,
...
x_n is an isolated variable in clause C_n
$f_{n-1}(x_{n-1})\sigma = x_n\sigma$,
$f_n(x_n)$ is a shielding term in C_n
....

If this were the case then we would have

$$f_1(x_1)/x_2, \quad f_2(x_2)/x_3, \ldots, f_n(x_n)/x_{n+1}, \ldots$$

or

$$f_n f_{n-1} f_{n-2} \ldots f_2 f_1(x_1)/x_{n+1} .$$

But σ has finite depth, so this process has to terminate. It can only terminate if one of the x_i is eligible, or if one of the $f_i(x_i)$ is such that

$$f_i(x_i)\sigma \neq x\sigma$$

for any isolated variable x in S.

Q.E.D.

Lemma 2. If S is an RC-unsatisfiable set of ground clauses, and c is a half literal of S (i.e., $c \leq d$, $d \leq c$, $c < d$, or $d < c$ is in S, for some d), then there is an RC-refutation $\mathcal{D}$ of S for which any chaining on terms other than c is done on clauses not containing c (as a half literal).

(That is, all chainings on c are done first, and then only clauses not containing c are retained for the remainder of the refutation.)

Proof. The proof is by induction on the excess literal parameter $k(S)$.*

Case 1. $k(S) = -1$. Then $\square \in S$ and we are finished.

Case 2. $k(S) = 0$, $\square \notin S$.

In this case the clauses of S are all units and by Lemma 2, Appendix I, S contains a sequence of unit clauses

$$a_1 \lesssim a_2 : a_2 \lesssim a_3 : \ldots : a_{n-1} \lesssim a_n : a_n \lesssim a_1 ,$$

*The excess literal parameter $k(S)$ is defined as

$$k(S) = (\sum_{C \in S} |C|) - |S| .$$

That is $k(S)$ is the total number of occurrances of literals minus the number of clauses in S.

where each $\lessdot$ is either $\leq$ or $<$ and at least one of the $\lessdot$ is $<$.

If any of the a_i are c's, then they can be chained upon first.

Case 3. (Induction Step)

Suppose $k(S) = n$, $n \geq 1$, and that for each set S' of ground clauses which is RC-unsatisfiable and for which $k(S\ ) - n$, there is an RC-refutation $\mathcal{D}'$ of S' for which any chaining on a term other than c is done on clauses not containing c (as a half literal).

Then S has at least one non-unit clause C (since $k(S) > 0$). Let

$$C = C' \vee L$$

where C' is a clause and L is a unit clause. Let

$$S_0 = S \sim \{C\} ,$$

$$S_1 = S_0 \cup \{C'\} , \quad S_2 = S_0 \cup \{L\} .$$

Then S_1 and S_2 sub some S and hence are RC-unsatisfiable. Also $k(S_1) < n$, $k(S_2) < n$, and hence by the induction hypothesis, there are RC-refutations $\mathcal{D}_1$ and $\mathcal{D}_2$ of S_1 and S_2, respectively, for which any chaining on terms other than c is done on clauses not contain c.

Let $\mathcal{D}_{11}$ be the first part of $\mathcal{D}_1$ in which chaining is done only on c, and $\mathcal{D}_{12}$ be the rest of $\mathcal{D}_1$ (the last part of $\mathcal{D}_1$). And let S_1' be a set of resolutents produced by $\mathcal{D}_{11}$ which do not contain c (as a half literal), but such that $\mathcal{D}_{12}$ produces $\square$ from S_1'.

$$\begin{array}{ccc} S_0 \cup \{C'\} & \qquad & S_0 \cup \{L\} \\ \Downarrow \mathcal{D}_{11} & & \Downarrow \mathcal{D}_2 \\ S_1' & & \square \\ \Downarrow & & \\ \square & & \end{array}$$

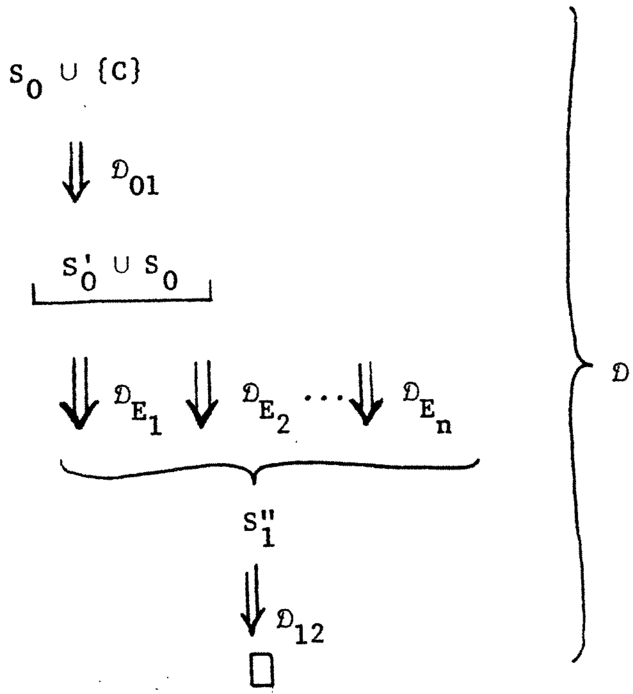
Now build $\mathcal{D}$ out of $\mathcal{D}_{11}$, $\mathcal{D}_2$, and $\mathcal{D}_{12}$ as follows:

Let $\mathcal{D}_{01}$ be the same as $\mathcal{D}_{11}$ except that C' is replaced by C (and some descendents of C' have the additional literal L), and let S_0' be produced by $\mathcal{D}_{01}$ from S (similarly as S_1' is produced by $\mathcal{D}_{11}$ from S_1).

For each clause E in S_1', we have by Lemma 1, Appendix I, that either E or $(E \vee L)$ is in S_0'. For each such $(E \vee L)$ in S_0', let $\mathcal{D}_E$ be the same as $\mathcal{D}_2$ except that L is replaced by $(E \vee L)$ and some descendents of $(E \vee L)$ have additional literals from E. Thus $\mathcal{D}_E$ when applied to $S_0 \cup \{E \vee L\}$ will produce a clause E' which subsumes E. (By Lemma 1, Appendix I).

By applying such a deducting $\mathcal{D}_E$ to each such $(E \vee L)$ in S_0', we obtain from $(S_0' \cup S_0)$ a set S_1'' of clauses which subsumes S_1'. And then we apply $\mathcal{D}_{12}$ to S_1'' to obtain $\square$.

$\mathcal{D}$ is made up of $\mathcal{D}_{01}$, several of the $\mathcal{D}_E$'s, and $\mathcal{D}_{12}$.



Since $\mathcal{D}_{01}$ consists of chainings only on c, since the first part of $\mathcal{D}_{E_i}$ consists of chainings only on c for each i, since the $\mathcal{D}_{E_i}$ are done in parallel, and since $\mathcal{D}_{12}$ chains only on clauses not containing c, it follows that $\mathcal{D}$ has the desired properties.

Q.E.D.

A different proof of Lemma 2, due to Ken Kunen, is given in Appendix II.

Lemma 3. If S is an RC-unsatisfiable set of clauses (S may contain more than one variant of a particular clause), $S\sigma$ is ground and RC-unsatisfiable, t is a half literal of S,

$$\mathscr{C} = \{t' : t' \text{ is a half literal of } S \text{ and } t'\sigma = t\sigma\} ,$$

then there is an RC-deduction $\mathcal{D}'$ of a set S' from S for which

(1) each step in $\mathcal{D}'$ is a chaining on a member of $\mathscr{C}$,

(2) S' contains no member of $\mathscr{C}$ as a half literal,

(3) $S'\sigma$ (and therefore S') is RC-unsatisfiable.

Proof. Apply Lemma 2 to $S\sigma$, with $t\sigma$ for c, to obtain an RC-refutation $\mathcal{D}''$ of $S\sigma$ for which any chaining on terms other than $t\sigma$ is done on clauses not containing $t\sigma$ (as a half literal).

Let S'' be the clauses obtained by $\mathcal{D}''$ on $S\sigma$ where only chainings on $t\sigma$ are done, and let S'_0 be those clauses of $S'' \cup S\sigma$ not containing $t\sigma$ (as a half literal). Since any chaining on terms other than $t\sigma$ is done on clauses not containing $t\sigma$, it follows that $\mathcal{D}''$ is an RC-refutation of S'_0.

$\mathcal{D}'$ is obtained from $\mathcal{D}''$ and S' from S'_0 by lifting. Conclusions (1), (2) and (3) follow immediately.

Lemma 4. (RC-completeness Theorem)

If S is an RC-unsatisfiable set of clauses then there is an RC-deduction of $\square$ from S.

Proof. Let S' be an RC-unsatisfiable set of ground instances of S. Then by Lemma 2 there is an RC-refutation $\mathcal{D}$ of S'. Lifting $\mathcal{D}$ gives the desired conclusion.

Remark. The deductions provided by Lemmas 2 and 4 may employ tautologies, as the following example shows.

Example

1.	$b \leq a$	$c \leq a$	$d \leq a$	S
2.	$a < b$	$a < c$	$a < d$	
3.	$c \leq b$			
4.	$b \leq c$			
5.	$d \leq b$			
6.	$b \leq d$			

Notice that each chaining on S results in a tautology. To show that S is RC-unsatisfiable, the following deduction (using tautologies) is given.

7.	$c \leq a \quad d \leq a \quad a < c \quad a < d$	1,2
8.	$c \leq a \quad d \leq a \quad b < c \quad a < d$	1,7
9.	$c \leq a \quad d \leq a \quad b < c \quad b < d$	1,8
10.	$c < b \quad d \leq a \quad b < c \quad b < d \quad a < c \quad a < d$	9,2
11.	$c < b \quad d \leq a \quad b < c \quad b < d \quad a < d$	9,10
12.	$c < d \quad d \leq a \quad b < c \quad b < d \quad c < d$	9,11
13.	$c < b \quad d < b \quad b < c \quad b < d \quad c < d \quad a < c \quad a < d$	12,2
14.	$c < b \quad d < b \quad b < c \quad b < d \quad c < d \quad d < c \quad a < d$	12,13
15.	$c < b \quad d < b \quad b < c \quad b < d \quad c < d \quad d < c$	12,14
16.	$c \leq d$	3,6
17.	$d \leq c$	5,4
18.	$\square$	15,4,6,3,5,17,16

The use of tautologies in RC proofs can be avoided if we use "multiple cuts" whereby for example clauses 1 and 2 above produce in one step the clause 15, and intermediate clauses 7-14 are not produced or retained. See [9].

Lemma 5. If S is an RC-unsatisfiable set of clauses, $S\sigma$ is ground and RC-unsatisfiable, $C \in S$, x is a variable,

$$C = \left(\bigvee_{i=1}^{n} x < a_i \vee \bigvee_{j=1}^{m} b_j < x \vee E\right)$$

where x does not occur in a_i, b_j or E, then

$$S' = S \sim \{C\} \cup \{ \bigvee_{i=1}^{n} \bigvee_{j=1}^{n} b_j < a_i \vee E\}$$

is RC-unsatisfiable, and $S'\sigma$ is RC-unsatisfiable. Also the shielding terms of S' are those of S. (A similar theorem holds when some or all of the '$<$' in C are replaced by '$\leq$', and appropriate changes are made in S'.)

<u>Proof</u>. Let

$$C' = (\bigvee_{i=1}^{n} \bigvee_{j=1}^{m} b_j < a_i \vee E) ,$$

$$S_0 = S \sim \{C\} .$$

We must show that $(S_0 \cup \{C'\})\sigma$ is unsatisfiable. We will show that any model for $(S_0 \cup \{C'\})\sigma$ is a model for $S\sigma = (S_0 \cup \{C\})\sigma$.

Suppose M is a model for $(S_0 \cup \{C'\})\sigma$. If M is a model for $E\sigma$ then M is a model for $C\sigma$ and we are through. Otherwise M is a model for $(b_j\sigma < a_i\sigma)$, for some i, j.

If M is already defined on $(x\sigma < a_i\sigma)$ and $(b_j\sigma < x\sigma)$, then, since $(b_j\sigma < a_i\sigma)$ is TRUE under M, it follows that either $(x\sigma < a_i\sigma)$ or $(b_j\sigma < x\sigma)$ is TRUE under M. If M is not defined on these two literals, we arbitrarily define it to be TRUE on the first and FALSE on the second (or vice versa). In either case M is a model for $C\sigma$ and is therefore a model for $S\sigma$.

Clearly the shielding terms of S' are those of S.

Q.E.D.

<u>Lemma 6</u>. If S is an RC-unsatisfiable set of clauses then there exists a set S_1 of variants of S and a substitution σ such that $S_1\sigma$ is ground and RC-unsatisfiable.

Theorem 1. If S is an RC-unsatisfiable set of clauses then there is an RCF-refutation of S.

Proof. By Lemma 6 there is a set S_1 of variants of S and a substitution σ for which $S_1\sigma$ is ground and RC-unsatisfiable. WLOG assume that S has no eligible variable.

Recursively define $S_2, S_3, \ldots$ as follows:

If S_i is ground, halt.

If S_i is ground, halt.

If S_i is not ground, use Lemma 1 to select a shielding term t from S_i for which $\sigma t \neq \sigma x$ for any isolated variable x in S_i, and let

$$\mathscr{C} = \{t' : t'\sigma = t\sigma \wedge t' \text{ is a half literal of } S_i\} ,$$

and use Lemma 3 to obtain an RC-deduction $\mathfrak{D}_i$ of a set S'_{i+1} from S_i for which each step in $\mathfrak{D}_i$ is a chaining on a member of $\mathscr{C}$, S'_{i+1} contains no member of $\mathscr{C}$, (as a half literal), and S'_{i+1} and $S'_{i+1}\sigma$ are RC-unsatisfiable. Let $S_{i+1} = VE(S'_{i+1})$.

We observe that variable elimination (i.e., the use of Lemma 4) on a set S' does not increase the number of half literals in $S'\sigma$. Furthermore, in applying Lemma 3, the half literals of S_{i+1} are a subset of those of S_i, and $t\sigma$ is a half literal of $S_i\sigma$ but not $S_{i+1}\sigma$. So the use of Lemma 3 steadily decreases the number of half literals in $S_i\sigma$. Therefore the sequence, $S_1, S_2, \ldots,$ must terminate in an RC-unsatisfiable ground set S_n. Let $\mathfrak{D}_G$ be the RCF-refutation of S_n.

Since the shielding term chosen by Lemma 1 is such that

$$t\sigma \neq x\sigma$$

for any variable x, it follows that if $t\sigma = t'\sigma$, then t and t' have the form

$$f(t_1, \ldots, t_n)$$

where f is an uninstantiated function symbol, and therefore each member of $\mathscr{C}$ has this form. And since $\mathcal{D}_i$ chains only on members of $\mathscr{C}$ it follows that each of the steps of $\mathcal{D}_i$ produces an RCF-resolvent.

Since variable elimination steps are also RCF-steps it would appear that $\mathcal{D}_i$ and $\mathcal{D}'_i$ together form a RCF-deduction of S_{i+1} from S_i. But in the definition of $RCF^n(S)$ we required that variable elimination be applied on a resolvent immediately when it is produced (if it has an eligible variable), so we cannot follow $\mathcal{D}_i$ by $\mathcal{D}'_i$, but must intermingle the two, by reording the VE and RCF steps. In particular, by [11], there is an RCF-deduction $\mathcal{D}''_i$ of S_{i+1} from S_i, for each i, $i = 1, n-1$.

And by putting together the deductions

$$\mathcal{D}''_1, \mathcal{D}''_2, \ldots, \mathcal{D}''_{n-1}, \mathcal{D}_G,$$

we obtain an RCF-refutation of S.

Q.E.D.

Theorem 2. (RCF Completeness Theorem)

Let

S be a set of inequality clauses,

$S_{\leq}$ be the set of clauses for the inequality axioms,

S_I be the set of clauses for the interpolation axioms, and suppose $(S \cup S_{\leq} \cup S_I)$ is unsatisfiable. Then there is an RCF-deduction of

from S.

<u>Proof</u>. By definition $(S \cup S_I)$ is RC-unsatisfiable. Thus by Theorem 1 there is an RCF-deduction $\mathcal{D}$ of from $(S \cup S_I)$. But no clause of S_I can be a part of a (productive) step in $\mathcal{D}$, so $\mathcal{D}$ is an RCF-deduction of $\square$ from S.

To see why a clause of S_I cannot be part of a (productive) step in $\mathcal{D}$, recall that S_I is the set of clauses

$$x_k \leq w_{nm}(x_1, \ldots, x_n, y_1, \ldots, y_m) \vee \bigvee_{i=1}^{n} \bigvee_{j=1}^{n} (y_j < x_i)$$

$$w_{nm}(x_1, \ldots, x_n, y_1, \ldots, y_m) \leq y_\ell \vee \bigvee_{i=1}^{n} \bigvee_{j=1}^{n} (y_j < x_i)$$

$$k = 1, n ; \quad \ell = 1, m; \quad n \geq 0 ; \quad m \geq 0 ,$$

together with similar clauses when $\leq$ and $<$ are interchanged.

Consider the case when $n = 1$, $m = 1$.

$$CI_1 = (x \leq w(x,y) \vee y < x)$$

$$CI_2 = (w(x,y) \leq y \vee y < x)$$

(we have dropped the subscript on w). Since the symbol 'w' occurs only in CI_1 and CI_2 and nowhere else in S, it follows that no chaining on $w(x,y)$ with another clause in S is allowed in $\mathcal{D}$, because it would have to match a variable. And chaining CI_1 with CI_2 would produce the tautology

$$x \leq y \vee y < x$$

which again cannot be used in any step of $\mathcal{D}$ since matching on variables is forbidden. Hence CI_1 and CI_2 are not used in a productive way in $\mathcal{D}$ and can be removed from $S \cup S_I$. Similarly other members of S_I can be removed.

Q.E.D.

Lemma 7. If

S is a set of inequality and equality clauses,

$S_{\leq}$ is the set of clauses for the inequality axioms,

S'' is obtained from S by replacing each literal of the form $(a=b)$ by $(a \leq b \wedge b \leq a)$ and reclausing if necessary,

and S is unsatisfiable, then $(S'' \cup S_{\leq})$ is RC-unsatisfiable.

Proof. The following is a partial sketch of the proof for the ground case. Lifting gives the general case.

Suppose two clauses

$$C_1 = (a = b \vee E_1)$$
$$C_2 = (a \neq b \vee E_2)$$

in S are resolved to obtain

$$R = (E_1 \vee E_2) .$$

If C_1 and C_2 have no other "=" symbol then C_1 is converted to the two clauses in S'',

$$C_{1.1} = (a \leq b \vee E_1)$$
$$C_{1.2} = (b \leq a \vee E_1)$$

and C_2 is converted to

$$C_2' = (a < b \vee b < a \vee E_2) .$$

RC-chaining $C_{1.1}$ and $C_{1.2}$ with C_2' gives R.

Theorem 3. Let

S be a set of inequality and equality clauses,

$S_{\leq}$ be the set of clauses for the inequality axioms,

S_E be the set of clauses for the equality axioms for the sets S,

S_I be the set of clauses for the interpolation axioms,

S' be obtained from $S \cup S_E$ by replacing each literal $a = b$ by $(a \leq b \wedge b \leq a)$ and reclausing if necessary,

and suppose $(S \cup S_{\leq} \cup S_I)$ is E-unsatisfiable, and $S \cap S_I = \emptyset$. Then there is an RCF-deduction of $\square$ from S'.

Proof. In this proof we use the following notation: For any set U of inequality and equality clauses,

U_E is the set of clauses for the equality axioms for U,

U'' is obtained from U by replacing each literal of the form $a = b$ by $(a \leq b \wedge b \leq a)$ and reclausing if necessary.

Thus, in the above, $S' = S'' \cup S_E''$, and we must show that there is an RCF-deduction of $\square$ from $S'' \cup S_E''$.

We first give an outline of the proof:

$S \cup S_{\leq} \cup S_I$ is E-unsatisfiable (Hypothesis of Theorem 3)

↓ Reference [8]

$S \cup S_{\leq} \cup S_I \cup S_E \cup S_{IE}$ is unsatisfiable

↓ Lemma 7

$S'' \cup S_{\leq} \cup S_I \cup S''_E \cup S''_{IE}$ is RC-unsatisfiable

(Note $S''_{\leq} = S_{\leq}$, $S''_I = S_I$)

↓ Theorem 2 (with $S'' \cup S''_E \cup S''_{IE}$ for S)

There is an RCF-deduction of □ from $(S'' \cup S''_E \cup S''_{IE})$

↓ See below.

There is an RCF-deduction of □ from $(S'' \cup S''_E)$.

The last step follows because if $\mathcal{D}$ is an RCF-deduction of □ from $S'' \cup S''_E \cup S''_{IE}$ then we can omit from $\mathcal{D}$ those steps involving S''_{IE} . Because S''_{IE} has only clauses of the form

$$C_{I1} = x_1 < x'_1 \vee x'_1 < x_1 \vee \ldots \vee y_m < y'_m \vee y_m < y_m$$
$$\vee\ w_{nm}(x_1, \ldots, x_n, y_1, \ldots, y_m) \leq w_{nm}(x'_1, \ldots, x'_n, y'_1, \ldots, y'_m) ,$$

(and similar clauses, see Section 2), and since the symbol "w_{nm}" does not occur in $S'' \cup S''_E$, no RCF step can use C_I unless C_I is chained with itself.

But such a chaining only produces a RCF-resolvent

$$x_1 < x_1' \vee \ldots \vee y_m < y_m' \\ \vee w_{nm}(x_1, \ldots, y_m) \leq w_{nm}(x_1, \ldots, y_m)$$

which can again only be used against members of $RCF^{\infty}(S''_{IE})$. So no interaction with $S'' \cup S''_E$ is possible.

3.2. RCF+ Completeness

Lemma 9 (Ground unit RC+ Completeness). If S is an RC+ unsatisfiable set of ground unit clauses, then there is an RC+ deduction of $\square$ from S.

This follows essentially from a consistency criterion used in linear programming. See [10]. Also see Lemma 3, Appendix I.

Lemma 10. If S is an RC+ unsatisfiable set of ground unit clauses, and c is an isolated term* of S, then there is an RC+ refutation $\mathcal{D}$ of S for which any chaining on terms other than c is done on clauses not containing c (as an isolated term).

Proof. Use Lemma 9.

Lemma 11. (Like Lemma 2) If S is an RC+ unsatisfiable set of ground clauses, and c is an isolated term of S, then there is an RC+ refutation $\mathcal{D}$ of S for which any chaining on terms other than c is done on clauses not containing c (as an isolated term).

Proof. The proof is by induction on the excess literal parameter k(S).

Case 1. $k(S) = -1$. Then $\square \in S$.

Case 2. $k(S) = 0$, $\square \notin S$.

In this case the clauses of S are ground unit clauses, and the desired result follows from Lemma 10.

Case 3. (Induction Step) The proof of this case follows exactly as the proof of Case 3 in Lemma 2, except the expression "half literal" is replaced by "isolated term".

---

*Recall that a term is isolated if it occurs not within the arguments of any uninstantiated function symbol. E.g., $t \leq a$, $t + a \leq b$, $a + t + b < c$, etc.

Lemma 12. (Like Lemma 3) If S is an RC+ unsatisfiable set of clauses, $S\sigma$ is ground and RC+ unsatisfiable, t is an isolated term of S,

$$\mathscr{C} = \{t': t \text{ is an isolated term of } S \text{ and } t'\sigma = t\sigma\} ,$$

then there is an RC+ deduction $\mathscr{D}'$ of a set S' from S for which

(1) each step in $\mathscr{D}'$ is a chaining on a member of $\mathscr{C}$,

(2) S' contains no member of $\mathscr{C}$ (as an isolated term),

(3) $S'\sigma$ (and therefore S) is RC+ unsatisfiable.

Proof. Similar to that of Lemma 3.

Lemma 13. (Like Lemma 5) If S is an RC+ unsatisfiable set of clauses, $C \in S$, x is an eligible variable in C, and R is a VE+ Resolvent of C upon x, then $S \sim \{C\} \cup \{R\}$ is RC+ unsatisfiable.

Proof. The proof is similar to that of Lemma 5.

Theorem 4. If S is an RC+ unsatisfiable set of clauses then there is an RCF+ refutation of S.

Proof. Very much like that of Theorem 1.

Appendix I

Lemma 1. If S is a set of ground inequality clauses, C and E are ground inequality clauses, and $\mathcal{D}$ is an RC-deduction of □ from $S \cup \{C\}$, then there is a clause E' which subsumes E, and an RC-deduction $\mathcal{D}'$ of E' from $S \cup \{C \vee E\}$.

Remark. If E is the unit clause L, then E' is either □ of L.

Lemma 2. If S is a finite RC-unsatisfiable set of unit ground inequality clauses, then S contains a sequence,

(1) $$a_1 \underset{1}{<} a_2 \; , \; a_2 \underset{2}{<} a_3 \; , \ldots , \; a_n \underset{n}{<} a_1 \; ,$$

where each of the $\underset{i}{<}$ is $\leq$ or $<$, and at least one of the $\underset{i}{<}$ is $<$. In case $n = 1$, we have $a_1 < a_1$ in S.

Proof. Since S is RC-unsatisfiable it follows that $S \cup S_{\leq}$ is unsatisfiable where $S_{\leq}$ consists of the four clauses

1. $x \leq x$
2. $x \leq y \vee y \leq x$
3. $y \leq x \vee z \leq y \vee x < z$
4. $y < x \vee z < y \vee x \leq z.$

S must have at least one '<' clause, for otherwise $S \cup S_{\leq}$ has the trivial model whereby all members of the alphabet of S are mapped into one point (e.g., 0).

The proof is by induction on $|S|$, the size of S.

If $|S| = 1$ then S consists of one clause $a < b$. But then b must be identical to a, because otherwise $\{a < b, a \leq b\}$ would be a model for $S \cup S_{\leq}$.

So assume the theorem holds for all sets $\overline{S}$ for which $|\overline{S}| < K$, and assume that $|S| = K > 1$.

Let $(a < b) \in S$, and let

$$S_0 = S \sim \{a < b\}$$

$$S_{i+1} = S_i \cup \{x \leq z: x < y \in S_i \vee \exists y (x \leq y \in S_i \wedge y \leq z \in S_i)\}$$
$$\cup \{x < z: \exists y ((x < y \in S_i \wedge y \leq z \in S_i)$$
$$\vee (x \leq y \in S_i \wedge y < z \in S_i))\}, \quad \text{for} \quad i = 0, 1, 2, \ldots .$$

Since S has a finite alphabet there is an n for which $S_{n+1} = S_n$.

If S_0 is unsatisfiable then we are finished by the induction hypothesis. So let M be a model of $S_0 \cup S_{\leq}$. Hence

$$S_0 \subseteq M .$$

Since each S_{i+1} is obtained by applying axioms 2 - 4 to S_i, it follows that $S_n \subseteq M$, and M is a model for S_n. Thus

(2) $\quad (b \leq a) \in S_n$ or $(b < a) \in S_n$

for othewise $M \cup \{a < b,\ a \leq b\}$ would be a model of $S_n \cup \{a < b\} \cup S_{\leq}$, and therefore of $(S \cup S_{\leq})$.

Also for each i,

$$x \leq z \in S_{i+1} \text{ iff } x \leq z \in S_i \text{ or } x < z \in S_i ,$$
$$\text{or for some } y,\ x \leq y \in S_i \text{ and } y \leq z \in S_i ,$$

and

$$x < z \in S_{i+1} \text{ iff } x < y \in S_i$$
$$\text{or for some } y,\ x < y \in S_i \text{ and } y \leq z \in S_i ,$$
$$\text{or } x \leq y \in S_i \text{ and } y < z \in S_i .$$

So by induction, if $b \leq a \in S_n$ or $b < a \in S$, then there is a sequence of clauses

(3) $$b \underset{1}{<} a_2 ,\ a_2 \underset{2}{<} a_3 , \ldots , a_{n-1} \underset{n-1}{<} a$$

in S, where each $\underset{i}{<}$ is $\leq$ or $<$, (and if $b < a \in S$ then at least one of the $\underset{i}{<}$ must be $<$).

So by (2) we have (3), and since $(a < b) \in S$, we have the desired sequence (1) (where $a_1 = b$, and $a_n = a$).

Q.E.D.

Lemma 3. Suppose we have a set of linear inequalities

$$\sum_{j \in n} a_{ij}x_j \geq 0 \quad \text{for} \quad i \in r$$

$$\sum_{j \in n} a_{ij}x_j > 0 \quad \text{for} \quad i \in p \sim r$$

where $a_{ij} \in \mathbb{Z}$ for $i \in p$, $j \in n$ and $0 \leq r \leq p$.

If there is no real solution $\{x_j\}_{j \in n}$ then for some $\{\lambda_i\}_{i \in p}$, $\lambda_i \in \mathbb{Z}$ and $\lambda_i \geq 0$ for $i \in p$,

$\sum_{i \in p} \lambda_i a_{ij} = 0$ for each $j \in n$ and $\lambda_i > 0$ for some $i \in p \sim r$.

Proof.

Note that if $r = p$ then $x_j = 0$ for $j \in n$ is a solution. Hence we may assume that $r < p$.

Let $F(x) = \underset{i \in p}{\mathrm{Tp}} \sum_{j \in n} a_{ij}x_i$ so that

$$F: \mathbb{R}^n \to \mathbb{R}^p$$

is a linear function. (We use the notation $\underset{i \in p}{\mathrm{Tp}}\ \underline{ui}$ to denote the p-tuple whose i-th coordinate is $\underline{ui}$ for each $i \in p$.)

Let $S = \mathrm{rng}\ F$. S is a linear subspace of $\mathbb{R}^p$.

If $S = \mathbb{R}^p$ then the given inequalities have a solution. We may therefore assume that $S \neq \mathbb{R}^p$.

We have then that $S^\perp$ is at least one dimensional. We wish to produce a basis A of $S^\perp$ such that $A \subset \mathbb{Z}^p$. We have that $u \in S^\perp$ iff $u \cdot z = 0$ for all $z \in S$. Since the n vectors $\underset{i \in p}{\mathrm{Tp}}\, a_{ij}$ span S, we have that $u \in S^\perp$ iff $\sum_{i \in p} u_i a_{ij} = 0$ for all $j \in n$. But this is a set of linear homogeneous equations which may be solved by Gaussian elimination. Since the a_{ij}'s are integers, we may choose a fundamental system of solutions b_{ji} such that $u \in S^\perp$ iff u is an arbitrary linear combination of the q vectors $\underset{i \in p}{\mathrm{Tp}}\, b_{ji}$ where the b_{ji}'s are all integers.

Let $P = [0,\infty)^r \times (0,\infty)^{p \sim r}$. So $x \in P \Leftrightarrow x \in \mathbb{R}^p$ and $\underset{i \in p}{\forall} (x_i \geq 0$ and $(i \in p \sim r \to x_i > 0))$. So, given $w \in \mathbb{R}^q$, $w \in Q \Leftrightarrow \underset{y \in P}{\exists}\ \underset{j \in q}{\forall} (y \cdot b_j = w_j)$.

Clearly, the existence of solutions to the given inequalities is equivalent to $P \cap S \neq \emptyset$.

Since we assume there are none, we have

$$
\begin{aligned}
P \cap S = \emptyset &\to \forall\, y \in P \quad (y \notin S) \\
&\to \forall\, y \in P\ \forall\, v \in S^\perp \quad (y \cdot v = 0) \\
&\to \forall\, y \in P \sim \forall\, j \in q \quad (y \cdot b_j = 0) \\
&\to \sim \exists\, y \in P\ \forall\, j \in q \quad (y \cdot b_j = 0) \\
&\to \sim \overline{0} \in Q\,.
\end{aligned}
$$

Now Q is a convex cone generated by the p vectors $\underset{j \in q}{\mathrm{Tp}}\, b_{ji}$ (as may be seen by letting y be the i-th unit vector), where the scalars are strictly positive for the last $p - r$ terms.

If these p vectors lie in the same direction, then let μ be any one of them which is not zero, so $\mu \cdot x > 0$ for $x \in Q$. If the p generators do not lie in the same direction, then the cone Q has faces, at least of one which must be open. Pick $i \in p \sim r$, then any face not holding the vector $\underset{j \in q}{Tp}\, b_{ji}$ must be open. Choose an open face and pick out its generators from among the $\underset{j \in q}{Tp}\, b_{ji}$'s. To get a normal to this face we must choose a vector perpendicular to each generator. Since this can be done by Gaussian elimination and the b_{ji}'s are integers we can get a normal vector which is integral. Changing its sign if necessary we get then a $\mu \in \mathbb{Z}^q$ such that

$$\mu \cdot x > 0 \quad \text{for} \quad x \in Q \,.$$

Hence

$$\sum_{j \in q} \mu_j x_j > 0 \qquad \text{for} \quad x \in Q$$

i.e.

$$\sum_{j \in q} \mu_j \, (y \cdot b_j) > 0 \qquad \text{for} \quad y \in P$$

$$\sum_{j \in q} \mu_j \sum_{i \in p} (y_i b_{ji}) > 0 \qquad \text{for} \quad y \in P$$

$$\sum_{i \in p} \left(\sum_{j \in q} \mu_j b_{ji} \right) y_i > 0$$

or

$$\sum_{i \in p} \lambda_i y_i > 0 \qquad \text{for} \quad y \in P$$

where

$$\lambda_i = \sum_{j \in q} \mu_j b_{ji} \,.$$

Since the μ_j's and b_{ji}'s are integral so are the λ_i's.

Now choosing $y \in P$ with y_i small except for $i = j$ which we choose large, we conclude from $\sum_{i\epsilon p} \lambda_i y_i > 0$ that $\lambda_j \geq 0$ for $j \in p$.

If it were the case that $\lambda_j = 0$ for all $j \in p \equiv r$ then by choosing $y_j = 0$ for $j \in r$, $y_j > 0$ for $j \in p \sim r$ we would have $y \in P$, but $\sum_{j\epsilon p} \lambda_j y_j = 0$, a contradiction.

Hence $\lambda_j > 0$ for some $j \in p \equiv r$.

Now $\sum_{i\epsilon p} \lambda_i a_{ij} = 0$ for all $j \in n \Leftrightarrow \sum_{i\epsilon p} \lambda_i x_i = 0$ for $x \in S$ since the $\underset{i\epsilon p}{Tp}$, a_{ij}'s span S. So given $x \in S$ we look at

$$\sum_{i\epsilon p} \lambda_i x_i = \sum_{i\epsilon p} \sum_{j\epsilon q} \mu_j b_{ji} x_i = \sum_{j\epsilon q} \mu_j \left(\sum_{i\epsilon p} b_{ji} x_i \right) .$$

But

$$\sum_{i\epsilon p} b_{ji} x_i = 0$$

since b_j is a basis vector for $S^{\perp}$. Hence $\sum_{i\epsilon p} \lambda_i a_{ij} = 0$ for all $j \in n$.

References

1. W.W. Bledsoe and L.M. Hines. Variable elimination and chaining in a resolution-based prover for inequalities. Proc. 5-th Conference on Automated Deduction, Les Arcs, France, July 1980, Springer-Verlag.

2. J.R. Slagle. Automatic theorem-proving with built-in theories of equality, partial order and sets. J. ACM 19(1972), 120-135.

3. J.R. Slagle and L. Norton. Experiments with an automatic theorem prover having partial ordering rules. Comm. ACM 16(1973), 682-688.

4. Robert Kowalski. Studies in the completeness and efficiency of theorem-proving by resolution. University of Edinburgh, Meta-mathematics Unit Memo 29, Ph.D. Thesis, April 1970.

5.

6.

7. L. Wos and G.A. Robinson. Paramodulation and set of support. Proc. Symp. Automatic Demonstration, Versailles, France, 1968, Springer-Verlag, New York, 276-310.

8. D.W. Loveland. <u>Automated theorem proving: a logical basis</u>. North Holland, Amsterdam, 1978, Chapter 5.

9. Kenneth Kunen. A completeness theorem for multiple chaining. Univ. of Texas Math. Dept. Memo ATP-61, August 1980.

10. K. Fan. Systems of Linear Inequalities. In <u>Linear Equalities and Related Systems</u>, by H. Kuhn, et al. Princeton U. Press, 1956.

11. Michael Richter. ATP62, March 1981.

Department of Mathematics
The University of Texas
Austin, TX 78712
U.S.A.