MIT/LCS/TM-33

A DECISION PROCEDURE FOR THE FIRST ORDER THEORY OF REAL ADDITION WITH ORDER

Jeanne Ferrante
Charles Rackoff

May 1973

MAC TECHNICAL MEMORANDUM 33

A DECISION PROCEDURE FOR THE FIRST ORDER THEORY OF REAL ADDITION WITH ORDER

Jeanne Ferrante

Charles Rackoff

May 1973

This research was supported in part by the National Science Foundation under research grant GJ34671, and in part by the Advanced Research Projects Agency of the Department of Defense under ARPA Order No. 433 which was monitored by ONR Contract No. N00014-70-A-0362-0001.

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

PROJECT MAC

CAMBRIDGE MASSACHUSETTS 02139

Abstract

Consider the first order theory of the real numbers with the predicates + (plus) and < (less than). Let S be the set of true sentences. We first present an elimination of quantifiers decision procedure for S, and then analyse it to show that it takes at most time $2^{2^{cn}}$, c a constant, to decide sentences of length n.

Looking more closely at this procedure, we arrive at a second procedure by showing that a given sentence doesn't change in truth value when each of the quantifiers is limited to range over an appropriately chosen <u>finite</u> set of rationals. This fact leads to a decision procedure for S which takes <u>space</u> 2^{cn}. We also remark that our methods lead to a decision procedure for Presburger arithmetic which operates in <u>space</u> $2^{2^{cn}}$.

These upper bounds should be compared with the results of Fischer and Rabin (Proceedings of A.M.S. Symp. on Complexity of Real Computation Processes, to appear) that for some constant c, time 2^{cn} for real addition, and time $2^{2^{cn}}$ for Presburger arithmetic, is required to decide some sentences of length n for infinitely many n.

A DECISION PROCEDURE FOR THE FIRST ORDER THEORY OF REAL ADDITION WITH ORDER

by

Jeanne Ferrante and Charles Rackoff[†]

Spring 1973

1. Introduction. In this paper we exhibit an efficient decision procedure for the theory of the real numbers with + (plus) and < (less than). Of course, as stated in a paper by Hodes [1], who also gives such a procedure, the decidability of the theory in question is a consequence of Tarski's theorem that the real numbers under +, • (times) and < is decidable; however, Tarski's procedure is far from efficient for the restricted theory we are interested in. We propose to exhibit a procedure which, as it turns out, is nearly optimal in computational efficiency. Fischer [2] shows that there is a constant $c > 0$ such that any nondeterministic Turing machine which decides real addition (even without order) requires for almost every n time 2^{cn} to decide some sentences of length n. We exhibit a deterministic procedure for addition on the ordered set of real numbers which uses space 2^{dn}, d a constant, and time $2^{2^{gn}}$, g a constant, to decide sentences of length n. Thus, there appears to be a gap of approximately one exponential between the upper and lower time bounds. But since the upper bound is deterministic and the lower bound is nondeterministic, this gap should be viewed in the light of a long-standing, unproved conjecture of automata theory which states that nondeterministic time t is equal in power to deterministic time 2^t.

The procedure we give replaces unbounded quantifiers by quantifiers ranging over a finite set of rationals; truth of the sentence in the real numbers will thus be determined by checking finitely many instances of a matrix. In order to prove the correctness of our procedure, we first exhibit an elimination-of-quantifiers procedure with the important feature that it does <u>not</u> require the sentence to be put in disjunctive normal form at each elimination of quantifiers.

In section 2 we define the language under consideration. In section 3 we give our elimination-of-quantifiers procedure. Our method utilizes an idea used by Cooper [3] in deciding integral addition. In section 4 we show, via an analysis of section 3, that each quantifier in a formula can be replaced by a suitably bounded quantifier, and then show that the desired space bound can be achieved. In section 5 we remark on further applications of our methods.

2. <u>Notation</u>. We consider the following language:

Variables (with subscripts written in binary)	$x_0, x_1, x_{10}, \ldots$	
Integral constants (written in binary)	0, 1, 10, 11, ...	
Propositional constants	T, F	
Unary symbol	$-$	(minus)
Binary symbols	$<$, $=$, $+$, $/$	(less than, equal, plus, divided by)

and the usual logical symbols $\neg$, $\wedge$, $\vee$, $\forall$, $\exists$, (,).

(negation, conjunction, disjunction, for all, there exists, parentheses)

Terms are of the form

$$\sum_{i=0}^{k} (a_i/b_i)\, y_i \qquad a_i, b_i \text{ signed integral constants,}$$

$b_i \neq 0$, y_i distinct variables. If t_1, t_2 denote terms, then $t_1 < t_2$ and $t_1 = t_2$ are atomic formulas. We will assume that to begin with, and prior to each elimination of quantifiers, all atomic formula are of the form $t > 0$ or $t = 0$. We use the usual definitions of formula and sentence.

Now let S be the set of those sentences in the above language which are true when the quantifiers range over the real numbers, with integral constants interpreted in the obvious way, $<$ interpreted as the usual order on the real numbers, $=$ as equality, $+$, $-$ and $/$ as ordinary real addition, minus, and division. We propose to exhibit a decision procedure for S(that is, an algorithmic procedure for deciding whether an arbitrary sentence in our language is in S or not) such that if B is a sentence of length n, the algorithm determines in space 2^{dn}, d a constant, whether or not $B \in S$.

3. <u>Elimination of Quantifiers</u>. We assume we have a formula $\exists x_1\, B(x_1,\ldots,x_n)$, where $B(x_1,\ldots,x_n)$ is a quantifier-free formula containing only the variables $x_1,\ldots,x_n$ free. We will exhibit a quantifier-free formula $B'(x_2,\ldots,x_n)$ which is equivalent to $\exists x_1\, B(x_1,\ldots,x_n)$ in the theory S.

The procedure is as follows:

1. "Solve for x_1" in each atomic formula. i.e. replace each atomic formula involving x_1 by an equivalent one of the form

$$\begin{array}{ll} x_1 < t & (1) \\ u < x_1 & (2) \\ x_1 = v & (3) \end{array}$$

where t, u, v are terms not containing x_1. Let $C(x_1,\ldots,x_n)$ denote the result of solving for x_1 in each atomic formula of $B(x_1,\ldots,x_n)$ containing x_1. Thus, $B(x_1,..,x_n)$ will be replaced by an equivalent formula $C(x_1,\ldots,x_n)$, $C(x_1,\ldots,x_n)$ a Boolean combination of atomic formulas of forms (1), (2), and (3) involving x_1, and atomic formulas not involving x_1.

2. We now make the following definitions:

Given $C(x_1,\ldots,x_n)$ to get $C_{-\infty}(C_{+\infty})$:

$$\text{replace}\qquad \begin{array}{l} x_1 < t \text{ in } C \text{ by} \\ u < x_1 \\ v = x_1 \end{array} \qquad \begin{array}{c} T \\ F \\ F \end{array} \qquad \left(\begin{array}{c} F \\ T \\ F. \end{array}\right)$$

Clearly, for any real numbers $r_2,\ldots,r_n$, and r_1 a sufficiently small real number, $C(r_1,\ldots,r_n)$ and $C_{-\infty}(r_2,\ldots,r_n)$ are equivalent. A similar statement can be made for $C_{+\infty}$ for r_1 sufficiently large.

3. Let U be the set of terms t, u, v in the atomic formulas of type (1), (2) and (3) occurring in $C(x_1,\dots,x_n)$. We now claim $\exists x_1\, C(x_1,\dots,x_n)$ is equivalent to

$$C_{-\infty} \vee C_{+\infty} \qquad \bigvee_{w,z \in U} C((w+z)/2,\ x_2,\dots,x_n).$$

<u>Proof</u>: Suppose we are given real numbers $r_2,\dots,r_n$.

($\Leftarrow$) Suppose $C_{-\infty} \vee C_{+\infty} \vee \bigvee_{w,z \in U} C((w+z)/2,\ r_2,\dots,r_n)$ is true.

If one of the disjuncts $C((w+z)/2,\ r_2,\dots,r_n)$ is true, so is $\exists x_1\, C(x_1,r_2,\dots,r_n)$. So suppose one of the first two disjuncts is true, say $C_{-\infty}$. (The proof for $C_{+\infty}$ is similar). Then since we can pick r_1 sufficiently small so $C(r_1,\dots,r_n)$ is equivalent to $C_{-\infty}$, $\exists x_1\, C(x_1,\ r_2,\dots,r_n)$ is true.

($\Rightarrow$) Suppose $\exists x_1\, C(x_1,r_2,\dots,r_n)$ is true. Let $t_1,\dots,t_m$ be the distinct real numbers, in increasing order, corresponding to the terms in U which are obtained by substituting $r_2,\dots,r_n$ for $x_2,\dots,x_n$. Since $\exists x_1\, C(x_1,r_2,\dots,r_n)$ is true, there is a real number r_1 such that $C(r_1,\dots,r_n)$ is true. Now, r_1 must satisfy a specific order relation with respect to the numbers $t_1,\dots,t_m$. That is, exactly one of the following must hold:

(a) $r_1 < t_1$

(b) $t_m < r_1$

(c) $r_1 = t_i$ for some $1 \le i \le m$.

(d) $t_i < r_1 < t_{i+1}$, for some $1 \le i \le m-1$.

It is then clear that if r also satisfies the same specific order relations w.r.t. $t_1,\ldots,t_m$ as r_1, $C(r, r_2,\ldots,r_n)$is true. But if (a) holds, $C_{-\infty}$ must be true, if (b) holds $C_{+\infty}$ must be true, if (c) holds $C((t_i+t_i)/2, r_2,\ldots,r_n)$must hold, and in case (d) $C((t_i+t_{i+1})/2, r_2,\ldots,r_n)$ must be true.

It should be noted that this procedure will work just as well for rational addition with <. In fact, the procedure works for any divisible, torsion-free, ordered abelian group. We need the divisibility to solve for x_1; the torsion-free requirement makes this solution for x_1 unique. Thus, in particular, any two divisible, torsion-free, ordered abelian groups are elementarily equivalent. We henceforth assume we are dealing with the rationals.

4. Bounds on the Procedure. The purpose of this section is to show the desired space bound can be attained. In order to do this, we want to compute a space bound on the elimination of quantifiers procedure given in section 3.

It should be noted that we are using as our model of computation the deterministic, one tape Turing machine; space bounds, or the number of tape squares used by the Turing machine, are given as a function of n, the length of the sentence the machine is deciding. As is widely known, this model is not restrictive for bounds as large as exponential since it can simulate a multitape or nondeterministic machine in space at most the square of the space required by the more powerful model [4]. Of course we describe our procedure informally, leaving it to the reader to convince himself that straightforward implementation of our procedure on a Turing machine would achieve the claimed bounds on time and space.

We now compute the amount of space it would take to eliminate quantifiers in a formula E of length m, with s_0 the size of the largest integral constant in E, ℓ the number of quantifiers in E. Our analysis is similar to that given by Oppen [5] for Cooper's decision procedure for Integral Addition. We first put E in prenex normal form using the standard algorithm but always choosing variables with the shortest subscripts possible, obtaining E'. Note that E' is of length $\leq m \log m$. This is so because there are at most m occurrences of variables, and thus any subscript of a variable in E will be increased in length by a factor of at most log m. Note that the prenex normal form procedure does not change the number of quantifiers or the size of constants, and so E' has ℓ quantifiers and largest integral constant of size s_0.

Now, let D be a formula. Let D' be the formula gotten by applying the elimination-of-quantifiers procedure to $\exists x$ D. Let n(n') denote the length of D(D'). Let s(s') be the size of the largest integer constant in D(D'). To compute n' from n, note that "solving for x" involves dividing through in each atom by the coefficient of x; instead of appearing once, each such coefficient can appear n times. Thus, the length of the formula $\exists x$ F gotten from $\exists x$ D by solving for x, is at most n^2. The substitution procedure involves increasing the length to at most $n^2(3(2n + 2)n^2)$, because for each of the at most n^2 pairs of terms (w,z) we must write $F((w+z)/2)$, and then collect terms. To collect terms we have to add up 3 coefficients whose integers are each of length $\leq 2n + 1$ to get a total whose integers are of length $\leq 3(2n + 1) + 2$, so that the size can go up by a factor of at most $3(2n + 2)$. We must also write the formulas $F_{+\infty}$, $F_{-\infty}$ of length at most 2n. Thus, $n' \leq 2n + n^2(3(2n + 2)n^2) \leq 10n^5 \leq n^9$.

We now compute s' in terms of s. Again, since "solving for x" involves dividing through in each atom by the coefficient of x, which is limited in numerator and denominator by s, the largest constant becomes at most s^2. The substitution procedure involves dividing by 2 and collecting like coefficients. Since in each atom gotten via the substitution process there can be at most three occurrences of the variable $y (y \neq x)$ and the three coefficients in question are limited in numerator and denominator by size $2s^2$, their sum is limited in like manner by $3(2s^2)^3$. Thus $s' \leq 24s^6 \leq s^{11}$ (if $s \geq 2$).

Let $n_{E'}$ be the length of the largest formula D gotten from the formula E' by elimination of quantifiers; let $s_{E'}$ be the size of the largest integral constant similarly obtained. Since deciding E' requires ℓ eliminations of quantifiers,

$$n_{E'} \leq (m \log m)^{9^{\ell}} \qquad \text{and}$$

$$s_{E'} \leq (s_0)^{11^{\ell}} \quad , \qquad \text{if } s_0 \geq 2,$$

and since it is not hard to see that the storage required for bookkeeping is no longer than the size of the largest expansion, to decide E' takes at most space $(m \log m)^{9^{\ell}}$. Therefore, we need at most $2^{2^{s \cdot m}}$ space, s a constant independent of m, to decide formulas of length m. It should also be noted that the time bound is of the same order; that is, $2^{2^{q \cdot m}}$, q a constant, time is at most needed to perform the elimination-of-quantifiers procedure. We need especially the fact that the size of the largest constant grows no larger than $s_0^{2^{p \cdot \ell}}$, p a constant independent of m, ℓ and s_0, in deciding formulas of length m with ℓ quantifiers and largest integral constant of size $\leq s_0$, if $s_0 \geq 2$.

Definition. A rational number r is limited by the positive integer k iff $r = a/b$ in lowest terms, and $|a| \leq k$, $|b| \leq k$. A quantifier $\exists x$ or $\forall x$ is limited by the positive integer k, written $\exists x \leq k$ or $\forall x \leq k$, if instead of ranging over all rationals, the quantifier ranges over all rationals limited by the positive integer k. Note that if r_1 and r_2 are rational numbers limited by the positive integers w_1, w_2, respectively, then $r_1 + r_2$ is limited by $2(w_1 \cdot w_2)$.

Lemma. $\exists$ a constant $c > 0$ such that for all ℓ, i and $w_0, w_1, \ldots, w_i$ if for $j = 1, \ldots i$, w_j is a positive integer, $w_0 = 1$, and $Qx\, F(x, y_1, \ldots, y_i)$ is a formula with ℓ quantifiers (where Q is $\forall$ or $\exists$), with largest integral constant s_0, $s_0 \geq 2$ and $r_1, \ldots, r_i$ are any rational numbers limited by $w_1, \ldots, w_i$, respectively, then $Qx\, F(x, r_1, \ldots, r_i)$ is true iff

$$Qx \leq s_0^{2^{c(\ell+i)}} (w_o \cdots w_i)^2 \; F(x_1, r_1, \ldots, r_i) \text{ is true.}$$

Proof. Consider $F(x,y_1,\ldots,y_i)$ with $\leq \ell$ quantifiers. By the results of section 3, we can replace $F(x,y_1,\ldots,y_i)$ by an equivalent quantifier-free formula $B(x,y,\ldots,y_i)$, such that all rational constants appearing in B are limited by $s_0^{2^{p\cdot\ell}}$, p a constant independent of ℓ and F. Thus it will be sufficient to show $Qx\ B(x,r_1,\ldots,r_i)$ true iff

$$Qx \leq s_0^{2^{c\cdot\ell}} (w_0\cdots w_i)^2\ B(x,\ r_1,\ldots,r_i).$$

We can assume, without loss of generality, that Q is $\exists$. Consider $\exists x\ B(x,r_1,\ldots,r_i)$. By the results of section 3, if such an x exists, then it is either less than all such terms appearing in the above formula after solving for x; or greater than all such terms; or equal to one; or can be assumed to be the average of two of them. We therefore calculate a limit for the terms appearing in $\exists x\ B(x,r_1,\ldots,r_i)$ after solving for x.

Consider any such term t. $t = \sum_{j=1}^{i} (a_j/b_j)(1/a)r_j$, where a is the coefficient of x we divide by to solve for x. Thus t is limited by $2^i(s_0^{2^{p\ell+1}})^i\ (w_0\cdots w_i) \leq s_0^{2^{p\ell+2i}} (w_0\cdots w_i)$. Thus $(t+u)/2$, t, u any two such terms as above, is limited by $2(s_0^{2^{p\ell+2i}}\ w_0\cdots w_i)^2 \leq s_0^{2^{p\ell+2i+2}} (w_0\cdots w_i)^2$. Thus we can limit x by $s_0^{2^{p\ell+2i+2}} (w_0\cdots w_i)^2 + 1 \leq s_0^{2^{c(\ell+i)}} (w_0\cdots w_i)^2$, c a constant, where the 1 must be added to handle the cases where x is either less than or greater than all such terms.

Thus $\exists x\ B(x,r_1,\ldots,r_i)$ is equivalent to $\exists x \leq s_0^{2^{c(\ell+i)}} (w_0\cdots w_i)^2\ B(x,r_1,\ldots,r_i)$.

We can now state:

Theorem. Let c be the constant of the previous lemma, $Q_1y_1 \cdots Q_\ell y_\ell\ F(y_1,\ldots,y_\ell)$be a sentence in prenex normal form with largest integral constants $\leq s_0$, $s_0 \geq 2$. Let $w_1 = s_0^{2^{c\ell}}$, $w_{k+1} = s_0^{2^{c\ell}}(w_1 \cdots w_k)^2$. Then, $Q_1\ y_1 \cdots\ Q_\ell y_\ell\ F(y_1,\ldots,y_\ell)$is true iff $Q_1\ y_1 \leq w \ \ldots\ Q_\ell y_\ell \leq w_\ell\ F(y_1,\ldots,y_\ell)$ is true.

Proof. Immediate, from the previous lemma.

We now have:

Theorem. $\exists$ a constant $d > 0$, and a decision procedure for rational addition with $<$, such that to decide a sentence B of length n takes at most 2^{dn} space.

Proof. Let B be a sentence of length n with largest integral constant $\leq s_0$. Let B' be its equivalent prenex normal form of length at most n log n. Then, using the above theorem, $B' = Q_1y_1 \ \ldots\ Q_\ell y_\ell\ F(y_1 \cdots y_\ell)$ is true iff $Q_1y_1 \leq w_1 \ \ldots\ Q_\ell y_\ell \leq w_\ell\ F(y_1,\ldots,y_\ell)$ is true, w_i defined as above. We now wish to show $w_\ell = w_1^{3^{\ell-1}}$. But it is easy to see $w_{k+1} = w_k^3$ since $w_{k+1} = w_1(w_1 \cdots w_{k-1}\ w_k)^2 = [w_1(w_1 \cdots w_{k-1})^2\ ]\ w_k^2 = w_k\ w_k^2 = w_k^3$, and thus $w_{k+1} = w_1^{3^k}$. Thus $w_\ell = (s_0^{2^{c\ell}})^{3^{\ell-1}}$. This is the largest bound we encounter in limiting the quantifiers of B'.

We thus must evaluate the matrix of B', of length at most n log n, at rationals limited by $(s_0^{2^{c\ell}})^{3^{\ell-1}} = 2^{2^{c'n}}$, c' a constant, since s_0 is limited by 2^n and $\ell \le n$. But then the obvious checking procedure in which integral constants are written in binary notation takes space at most 2^{dn}, d a constant.

The upper bound on the decision procedure thus obtained should be compared to the lower bound obtained by Fischer [2].

5. Applications. The idea of deciding truth in a particular theory, as outlined above, can be applied to many other theories, thereby obtaining procedures of considerable computational efficiency. That is, given a particular theory, one gives an elimination-of-quantifiers procedure, analyzes it to see how "large" constants can grow, and uses this analysis and the elimination-of-quantifiers procedure in a manner similar to that given above to limit quantifiers to range over finite sets instead of an infinite domain. In particular, we can use the quite efficient elimination-of-quantifiers procedure given by Cooper [3] for deciding truth in the first order theory of the following language L:

Integral constants	0, 1, 10, 11, ...
Unary symbol	- (minus)
Binary symbols	<, =, +, $\vert$. (less than, equals, plus, divides)

and the usual variables and logical symbols, where terms are of the form $\sum_{i=1}^{k} a_i y_i + a_{k+1}$, a_i signed integral constants, y_i distinct variables; atomic formulas are of the form $t_1 < t_2$, $t_1 = t_2$ and $n \mid t_1$, n an integral constant, t_1, t_2 terms.

If we use the analysis of Cooper's procedure by Oppen [5] as stated below, we can derive a further result on an upper bound on space for deciding this theory. We first state:

Definition. An integer n is limited by the positive integer k if $|n| \leq k$.

A quantifier Qx, where Q is $\forall$ or $\exists$, in L is limited by the positive k, written $Qx \leq k$, if instead of ranging over all integers, it ranges over all integers limited by k.

Theorem. (Oppen): $\exists$ a constant $e > 0$ such that if Cooper's elimination-of-quantifiers procedure is applied to a sentence with integral constants limited by the positive integer s_0, $s_0 \geq 2$, and ℓ quantifiers, the size of any integral constant appearing at any point of the procedure is limited by $s_0^{2^{2^{e \cdot \ell}}}$.

We can now state:

Lemma. $\exists$ a constant $f > 0$ such that given $\exists x\, F(x, y_1, \ldots, y_i)$ with integral constants limited by the positive integer s_0, $s_0 \geq 2$ and ℓ quantifiers, and integers $n_1, \ldots, n_i$ limited by the positive integer w, ($w = 1$ if $i = 0$)

then $\exists x\ F(x,n_1,\dots,n_i)$ is true iff $\exists x \le s_0^{2^{2^{f(i+\ell)}}} (w\cdot i)\ F(x, n_1,\dots,n_i)$

Proof. Using the previous theorem, Cooper's procedure, and an analysis similar to that given for real addition.

Theorem. $\exists$ a constant $g > 0$ such that if $Q_1 x_1 \dots Q_\ell x_\ell\ B(x_1,\dots,x_\ell)$ is in prenex normal form with integral constants limited by the positive integer $s_0 \ge 2$, B quantifier-free, then $Q_1x_1 \dots Q_\ell x_\ell\ B(x_1,\dots,x_\ell)$ is true iff $Q_1x_1 \le s_0^{2^{2^{g\ell+1}}} \dots Q_ix_i \le s_0^{2^{2^{g\ell+i}}} \dots Q_\ell x_\ell \le s_0^{2^{2^{g\ell+\ell}}}\ B(x_1,\dots,x_\ell)$.

Proof. Apply the previous lemma.

It is then clear that:

Theorem. $\exists$ a constant $h > 0$, and a decision procedure for integral addition with $<$, such that to decide a sentence of length n takes at most $2^{2^{h\cdot n}}$ space.

This theorem should be compared to that obtained by Fischer and Rabin [2]:

Theorem. (Fischer and Rabin): $\exists$ a constant $j > 0$ such that any non-deterministic Turing machine which decides integral addition (even without order) requires for almost every n time $2^{2^{jn}}$ to decide some sentences of length n.

Acknowledgement

We would like to acknowledge some helpful suggestions by Henry Baker in the early stages of our work and the assistance of Professor Albert Meyer in the conception and preparation of this paper. We would also like to thank Sharyn Cohn for her generous assistance in typing this manuscript.

Bibliography

1. Louis Hodes, "Solving Problems by Formula Manipulation In Logic and Linear Inequalities", Second International Conf. on Art. Int., British Computer Society, (1971), 553-559.

2. M. Fischer and M.O. Rabin, to appear in the Proceedings of the Symp. on the Complexity of Real Computation Processes, New York, N.Y., April, 1973.

3. C. D. Cooper, "Theorem-proving in Arithmetic Without Multiplication", U.C. of Swansea Computer and Logic Research Group Memorandum No. 16, April, 1972.

4. J. Hopcroft and J. Ullman, Formal Languages and Their Relation to Automata, Addison Wesley, 1969.

5. D. C. Oppen, "Elementary Bounds for Presburger Arithmetic", to appear in the Proceedings of the Austin SIGACT Conf., May, 1973.