ICASE

INSTANTIATION AND DECISION PROCEDURES FOR CERTAIN CLASSES
OF QUANTIFIED SET-THEORETIC FORMULAE

(NASA-CR-185750) INSTANTIATION AND DECISION PROCEDURES FOR CERTAIN CLASSES OF QUANTIFIED SET-THEORETIC FORMULAE (ICASE) 22 p

N89-71431

Unclas
00/64 0224325

Jacob T. Schwartz

Report Number 78-10

August 11, 1978

INSTITUTE FOR COMPUTER APPLICATIONS IN SCIENCE AND ENGINEERING
NASA Langley Research Center, Hampton, Virginia

Operated by the

UNIVERSITIES SPACE USRA RESEARCH ASSOCIATION

INSTANTIATION AND DECISION PROCEDURES FOR CERTAIN CLASSES OF QUANTIFIED SET-THEORETIC FORMULAE

Jacob T. Schwartz *

Department of Computer Science
Courant Institute, New York University

ABSTRACT

Set-theoretically oriented mechanical theorem provers can exploit the fact that all notions in set theory can be defined in terms of the two primitives equality and set membership. However, since set theory permits very general constructions, such provers find it hard to decide, even in apparently trivial cases, how existentially quantified set variables should be instantiated. Extending results of Behmann (1922) we give algorithms for instantiating set- and map-valued variables in simple set-theoretic formulae, and also for calculating the truth-values of these formulae.

* This report was prepared as a result of work performed under NASA Contract No. NAS1-14101 at ICASE, NASA Langley Research Center, Hampton, VA 23665.

I. Introduction.

The correctness of any program ultimately rests upon various mathematical facts implicit in it; and, depending upon the sophistication of the program, these mathematical facts may be arbitrarily deep. Thus a powerful, general proof checker will be a necessary part of any mature program verification system. Such a proof checker is an interactive programmed system into which one can enter sequences of logical/mathematical formulae, which it will accept as long as it can perform some computation which guarantees that each new formula is a logical consequence of preceding formulae. Such a verifier ensures rigorously against logical error, possibly at the price of requiring its user to key in a burdensome mass of intermediate detail. The weight of detail required will be inversely proportional to the size of the inferences which the system is able to make automatically. For this reason, the developing technology of program verification requires considerably improved automatic theorem provers.

Automatic proof of mathematical theorems has been studied very actively since 1967. But progress has been slow; inevitably so in view of the very fundamental nature of the problems which need to be faced, most of which are unsolvable if stated in perfect generality and hyperexponentially difficult even in restricted cases. Nevertheless there do exist a number of proof techniques which, although general enough to cover important classes of statements, are nevertheless specialized enough to attain greater efficiency than the perfectly general resolution provers that have been most studied. An important technique of this kind is the systematic use of definitions, in reverse, to eliminate defined predicates and operators.

This technique rests upon an important general metamathematical <u>principle of definition</u>, which we can state as follows:

A. Let S be any collection of predicate formulae, and let $e(x_1,\ldots,x_n)$ be any predicate formula whose free variables are $x_1,\ldots,x_n$. Let F be any completely new predicate symbol, i.e. symbol not appearing in any formula of S, and let f be any completely new function symbol. Then without affecting the consistency of S we can extend it by adding either the formula

$$(\forall x_1 \ldots x_n)\ (F(x_1,\ldots,x_n) \longleftrightarrow e(x_1,\ldots,x_n)) \tag{1}$$

or the formula

$$(\forall x_2 \ldots x_n)\ ((\exists x_1) e(x_1,\ldots x_n) \longrightarrow e(f(x_2,\ldots,x_n)\ ,\ x_2,\ldots x_n)) \tag{2}$$

to S. Formula (1) (resp. (2)) is then called the <u>definition</u> of the new predicate symbol F (resp. function symbol f.)

B. Any formula of first order logic which follows from S together with (1) (or (2)) and <u>which does not contain any occurence of the defined symbol</u> F (or f) <u>follows from the formulae of</u> S <u>alone</u>.

This tells us that a formula P which can be proved from S and from a definition (1) (or (2)) can always be proved as follows: First use (1) (or (2)) to eliminate every occurence of F (or f) from P (by making appropriate substitutions, e.g. $e(x_1,\ldots,x_n)$ for $F(x_1,\ldots,x_n)$). Then the proof can be completed using formulae of S only, but no definition (1) or (2) need ever be used again.

This technique applies with particular advantage to proofs in set theory, since set theory involves only a very few primitive axioms, and only the two primitive predicates equality and set membership. All other predicates and operators of set theory are definable, and definable rapidly, in terms of these two primitives. This fact has been

exploited by [Carvalho, 1974], and by [Bledsoe, 1977a] and his group at the University of Texas, who have built set-theoretic theorem provers that incorporate definition-reversing rewrite rules and that have been able to prove theorems in elementary set theory and topology going considerably beyond what could be done by any pure resolution technique. (See also [Bledsoe & Bruell, 1974].)

A main shortcoming of these otherwise surprisingly powerful provers is their inability to deal adequately with the <u>problem of set theoretic instantiation</u>. That this should be so follows directly from the generality of the existential axioms of set theory, which imply the existence of every set definable by a well-structured set former

$$\{e(x) \mid C(x)\} . \tag{3}$$

Although ideal from the human mathematician's point of view, the complete generality of the allowed forms (3) deprives a set-theoretic theorem proving program attempting to instantiate a particular variable of all guidance. It is consequently hard for a proof program to cope with theorems requiring even trivial instantiations. For example, even the easy assertion

$$(\exists C)\ (\forall x)\ (x \subseteq A \vee x \subseteq B \Longrightarrow x \in C) . \tag{4}$$

which follows easily if we supply the apparently obvious instantiation

$$C = \text{powerset}\ (A) \cup \text{powerset}\ (B) \tag{5}$$

manually, is not easy for a fully automatic prover to handle. Improved set-theoretic instantiation techniques thus appear as an important issue in mechanical theorem proving. This problem, the main subject of the

present paper, has also been investigated by [Behmann, 1922], and recently by [Bledsoe, 1977b] and his students (see [Minor, 1978]).

II. Preliminary Reductions; A Few Easy Cases.

The problem of instantiation can be described as that of deciding the conditions under which a formula

$$(\exists x)\, P(x) \tag{6}$$

is valid, and of producing a 'solution' $x = x_0$ for (6) if these conditions hold. If such a solution can be written in terms of the other basic parameters appearing in (6), then (6) can be rewritten in a form not involving the quantifier $(\exists x)$, which may make it possible to handle more complex cases, e.g.,

$$(\exists x)\,(\exists y)\, Q(x,y)\,. \tag{7}$$

Formulae $(\forall x)P(x)$ can be handled by rewriting them as $\sim(\exists x)\sim P(x)$. If desirable, the predicate P appearing in (6) can be normalized as a disjunction of conjunctions, and since $(\exists x)(P_1(x) \vee P_2(x))$ is equivalent to $(\exists x)P_1(x) \vee (\exists x)P_2(x)$, we can always assume that the $P(x)$ in (6) is a conjunction of elementary terms.

Having said this we now turn our attention to the class of formulae studied by Behmann, namely those formulae (6) in which the predicate P is a conjunction of Boolean set-theoretic expressions formed from set-valued variables by use of the set operators $a \cap b$, $a \cup b$, $a - b$, and the set inclusion operator $a \supseteq b$. If we allow ourselves to write set union as a sum, set intersection as an ordinary product, and the complement of the set x as $\bar{x}$, then any such formula (6) can be written as

$$(\exists x)\left(\mathop{\&}_{k=1}^{n}(a_k x + b_k \bar{x} = \phi) \mathop{\&}_{k=1}^{m}(c_k x + d_k \bar{x} \neq \phi)\right) . \tag{8}$$

Since $(a = \phi \,\&\, b = \phi) \longleftrightarrow (a + b = \phi)$, we can always assume $n = 1$ in (8). The detailed treatment of (8) rapidly grows more complicated as m increases; its general treatment, due to Behmann, will be reviewed below. However, since this treatment is hyperexponentially inefficient, we first examine the two simplest cases $m = 0$ and $m = 1$, in which easy and efficient techniques are available.

In the case $m = 0$ we must consider

$$(\exists x)(ax + b\bar{x} = \phi) \tag{9}$$

which is to say $(\exists x)(b \subseteq x \subseteq \bar{a})$. Here a (minimal) solution is $x = b$, and (9) is equivalent to $ab = \phi$. It follows that the multivariable cases corresponding to (9) can be solved easily, e.g. to solve

$$(\exists x,y)(axy + bx\bar{y} + c\bar{x}y + d\bar{x}\bar{y} = \phi) \tag{10}$$

we rewrite it as

$$(\exists x)((ax + c\bar{x})(bx + d\bar{x}) = \phi) . \tag{11}$$

This is equivalent to $abcd = \phi$ and has the solution $x = cd$, from which we obtain the solution $y = bcd + d\bar{c}\bar{d} = d - (c - b)$ for y.

Next let $m = 1$ and consider

$$(\exists x)(ax + b\bar{x} = \phi \,\&\, cx + d\bar{x} \neq \phi) . \tag{12}$$

$$\longleftrightarrow (\exists x)(b \subseteq x \subseteq \bar{a} \;\&\; cx + d\bar{x} \neq \phi) .$$

By adding a point $z \in c - a$ to a solution x of (12) we never spoil the solution, and hence (12) has the solution $b + (c - a)$ if it has

any solution. A solution will exist if and only if $ab=\phi \& (c-a)+(d-b)\neq\phi$. These conditions, like (12), involve one set equality and one inequality, so that inductive treatment of the n variable case corresponding to (12) is possible. For example,

$$(\exists x,y)(axy + bx\bar{y} + c\bar{x}y + d\bar{x}\bar{y} = \phi \;\&\; exy + fx\bar{y} + g\bar{x}y + h\bar{x}\bar{y} \neq \phi) \tag{13}$$

is equivalent to

$$(\exists x)((ax + c\bar{x})(bx + d\bar{x}) = \phi \;\& \tag{14}$$

$$((e-a)+(f-b))\,x + ((g-c)+(h-d))\,\bar{x} \neq \phi)$$

and hence has the solution

$$x = cd + ((e-a)+(f-b)-ab) \tag{15}$$

if (13) is solvable at all, from which a value for y can be calculated.

As another interesting elementary case we consider quantified formulae built around a single set-theoretic equation $e(x_1,\ldots,x_n)=\phi$ but involving no set inequalities. However, we explicitly allow arbitrary sequences of existential and universal quantifiers, and do not always insist that $e(x_1,\ldots,x_n)$ only involve Boolean operators. Perhaps the simplest case is

$$(\exists x)(\forall y)(e(x,y)=\phi)\,. \tag{16}$$

We will always suppose that existentially quantified variables only appear as arguments of Boolean operators. This assumption allows us to write (16) as

$$(\exists x)(\forall y)(a_y x + b_y \bar{x} = \phi) \longleftrightarrow (\exists x)\ ((\underset{y}{U}\, a_y)x + (\underset{y}{U}\, b_y)\bar{x} = \phi)\ . \qquad (17)$$

Hence (16) is equivalent to $(\forall y,z)(a_y b_z = \phi)$, and has the solution $\underset{y}{U}\, b_y$ if the truth-value of (16) is 'true'. Similar cases involving more complex sequences of existential and universal quantifiers can be treated in much the same way.

III. The General Presburger-Behmann Case.

[Presburger, 1929] gives an algorithm for calculating the truth value of any formula quantified over the integers and involving only addition, subtraction, and inequalities (cf. also [Cooper, 1972], [Shostak, 1977], [Bledsoe, 1975]). [Behmann, 1922] sketches an algorithm for calculating the truth value of any formula quantified over sets and involving only Boolean operators, set inclusion and inequality, the set cardinality operator #s, integer constants, and inequalities. We will now review and combine their techniques, thereby obtaining a decision procedure for formulae quantified over both sets and integers and involving all of the operators just mentioned. Such formulae will be called PB-formulae. As we shall see, the decision procedure to be described can also be regarded as an instantiation procedure for existentially quantified set and integer variables in PB-formulae. However, since by the results of [Rabin,] any general Presburger decision algorithm must be exponentially inefficient, limited but efficient procedures applicable in special cases like those described in the preceding section retain interest even in the presence of the general results which we now present.

As noted previously, in considering any existentially quantified PB-formula $(\exists n)P(n)$ or $(\exists x)P(x)$ (where, here and below, n designates

an integer and x a set) we can assume that P is a disjunction of literal terms. If existentially quantified over an integer, such a formula can therefore be written as

$$(\exists n)\left(\mathop{\&}_{k=1}^{I}(a_k n \geq A_k)\ \&\ \mathop{\&}_{k=1}^{J}(b_k n \leq B_k)\right)\&\ Q \tag{18}$$

where the a_k and b_k are positive integer constants, the A_k and B_k are valid integer-valued PB-terms, and Q is a valid PB-formula. If existentially quantified over a set, a PB-formula can be written as

$$(\exists x)\left(\mathop{\&}_{k=1}^{N}\sum_{j=1}^{M_k} c_{kj}\#(C_j x + D_j \bar{x}) \geq A_k\right)\&\ Q\ , \tag{19}$$

where A_k and Q are as before, each c_{kj} is an integer constant, and C_k and D_k are valid set-valued PB-terms.

We begin by analyzing (18). In order to make the inductive course of the analysis clear we ignore the conjunct Q but introduce additional conjuncts expressing divisibility relationships under the quantifier. Specifically, we consider

$$(\exists n)\left(\mathop{\&}_{k=1}^{I}\left(a_k n \geq A_k\right)\ \&\ \mathop{\&}_{k=1}^{J}(b_k n \leq B_k)\ \mathop{\&}_{k=1}^{L}(c_k | d_k n + E_k)\right) \tag{20}$$

where $m|n$ reads 'm divides n', c_k and d_k are positive integer constants, and E_k is an integer-valued PB-term. Suppose for the sake of definiteness that $I > 0$ in (20), and that (20) admits a solution n. Then among these solutions, all of which exceed the largest among the quantities A_k/a_k, there must exist a smallest n. This n will have the form $(A_k + j)/a_k$ where j is a non-negative integer. Let $\tilde{c}_k$ denote the quotient $c_k/\mathrm{GCD}(c_k, d_k)$ for $k = 1 \ldots L$. Since n is smallest it must be impossible to subtract any common multiple of $a_k, \tilde{c}_1, \ldots, \tilde{c}_L$ from j and still have a non-negative integer. Hence

$$0 \le j \le \Gamma_k = \mathrm{GCD}(a_k, \tilde{c}_1, \ldots, \tilde{c}_L) . \tag{21}$$

Thus (20) is equivalent to the following finite disjunction:

$$\bigvee_{i=1}^{I} \bigvee_{j=1}^{\Gamma_i} \Bigg(\mathop{\&}_{k=1}^{I} (a_k(A_i + j) \ge a_i A_k) \;\&\; \mathop{\&}_{k=1}^{J} (b_k(A_i + j) \le a_i B_k) \tag{22}$$

$$\& \mathop{\&}_{k=1}^{L} (a_i c_k \mid d_k(A_i + j) + a_i E_k) \& (a_i \mid A_i + j) \Bigg).$$

Note that (22) has essentially the same form as (20), but has one less existential quantifier. Moreover, in passing from (20) to (22) we have essentially 'solved' for n: n is $(A_i + j)/a_i$, where (22) serves to locate i and j within the finite set $\{[i,j] : 1 \le i \le I,\ 1 \le j \le \Gamma_i\}$.

Next we consider (19), once more ignoring the conjunct Q. We handle this by forming all possible intersections H_i of the sets C_k, D_k, and their complements. This gives us a collection $H_1, \ldots, H_R$ of sets. Each of the sets C_k, D_k can then be written as a disjoint union of the H_i:

$$C_k = \bigcup_{j \in \gamma_k} H_j , \quad D_k = \bigcup_{j \in \delta_k} H_j , \quad k = 1 \ldots n , \tag{23}$$

where γ_k and δ_k are subsets of $\{1, \ldots, R\}$. The set x appearing in (19) can then be written as a union of its disjoint subparts $x \cap H_j$, and (19) only constrains the cardinality of these sets, which we now assume to be finite. Hence (19) can be rewritten as

$$(\exists n_1, \ldots n_R) \Big(\mathop{\&}_{k=1}^{R} n_k \le \# H_k \;\&\; \mathop{\&}_{k=1}^{N} \Bigg(\sum_{i=1}^{M_k} c_{ki} \Big(\sum_{j \in \gamma_i \cap \delta_i} \# H_j + \sum_{j \in \gamma_i \ominus \delta_i} n_j \Big) \ge A_k \Bigg) \Big). \tag{24}$$

Once having put (19) into the form (24) we can apply the Presburger technique described above, repeatedly, to eliminate the integer quantifiers $\exists n_1,\ldots,n_R$. This will ultimately yield a valid PB-formula equivalent to (19) but containing one less quantifier. Once the integers $n_1 \ldots n_R$ are instantiated we can clearly use them to instantiate $x = \bigcup_{j=1}^{R} (x \cap H_j)$; note that for simplicity's sake it is always best to instantiate each n_j either as $n_j = 0$ or $n_j = \#H_j$ if this is possible.

IV. Sets of Infinite Cardinality.

In the preceding section we have only considered arithmetic formulae quantified over finite integers, and hence were only able to consider set-theoretic formulae quantified over finite sets. However, as was shown by [Tarski, 1956], the additive theory of infinite cardinals is also decidable, and this fact makes it easy to extend our discussion to the infinite case. That is, we can consider formulae involving all the operators listed in the preceding section (but omiting arithmetic subtraction, which is not well defined in the infinite case), and quantified over either general sets or general cardinals. Let us call this class of formulae TPB-formulae. Suppose that (in this section) we write n for finite integers, N for cardinals finite or infinite, ν for cardinals known to be infinite. Then for any predicate P we have

$$(\exists N)P(N) \longleftrightarrow ((\exists n)P(n) \vee (\exists \nu)P(\nu)) . \tag{25}$$

Formulae quantified over integers can be handled in the manner described in the preceding section. A TPB-formula of the form $(\exists \nu)P(\nu)$ can be written as a disjunction of clauses

$$(\exists\nu)\left(\mathop{\&}_{k=1}^{J}(a_k\nu + A_k > b_k\nu + B_k)\,\&\,\mathop{\&}_{k=1}^{L}(c_k\nu + C_k = d_k\nu + D_k)\right), \tag{26}$$

where each a_k, b_k, c_k, d_k is either 0 or 1, and each A_k, B_k, C_k, D_k is a well-formed, cardinal-valued, TPB-term.

The sum of two cardinals, A and B, at least one of which is infinite, is always the maximum of A and B. Thus the elementary clauses which appear in (26) can be simplified by use of the following equivalences:

$\nu + A = \nu + B$ is equivalent to $A = B \vee (\nu \geq A \,\&\, \nu \geq B)$ (27a)

$\nu + A = B$ is equivalent to $(\nu \geq A \,\&\, \nu = B) \vee (\nu < A \,\&\, A = B)$ (27b)

$\nu + A > B$ is equivalent to $\nu > A \vee A > B$ (27c)

$A > \nu + B$ is equivalent to $A > \nu \,\&\, A > B$ (27d)

$\nu + A > \nu + B$ is equivalent to $A > \nu \,\&\, A > B$. (27e)

To treat (26) inductively it is convenient to introduce one more operator and a family of predicates. By σ we denote the operator which maps each cardinal ν to the next larger cardinal $\sigma\nu$. The predicates $\Pi_n(\nu)$ are defined by $\Pi_n(\nu) = (\exists\nu_1)(\sigma^n\nu_1 = \nu)$. For infinite cardinals we have $\sigma(\nu_1 + \nu_2) = \sigma\nu_1 + \sigma\nu_2$ and $\nu + \sigma\nu = \sigma\nu$. Moreover $\Pi_n(\sigma\nu) \longleftrightarrow \Pi_{n-1}(\nu)$, where $\Pi_{-1}(\nu)$ is identically true; and

$$\Pi_n(\nu_1 + \nu_2) = (\nu_1 > \nu_2 \,\&\, \Pi_n(\nu_1)) \vee (\nu_2 \geq \nu_1 \,\&\, \Pi_n(\nu_2)). \tag{28}$$

Call a TPB-formula containing occurrences of the operator σ and the predicates Π_n a <u>generalized TPB-formula</u>. Then any generalized TPB-formula existentially quantified over an infinite cardinal ν can be written as a disjunction of clauses

$$(\exists\nu)\left(\mathop{\&}_{k=1}^{J}((a_k\sigma^{n_k}\nu+A_k)>(b_k\sigma^{m_k}\nu+B_k))\ \&\right. \tag{29}$$

$$\left.\mathop{\&}_{k=1}^{L}((c_k\sigma^{p_k}\nu+C_k)=(d_k\sigma^{q_k}\nu+D_k))\ \&\ \Pi_r(\nu)\right)\&\ Q\ ,$$

where Q is independent of ν; and then simplified by the use of the identities (27), (28) etc. to a disjunction of clauses

$$(\exists\nu)\left(\mathop{\&}_{k=1}^{I}(\sigma^{n_k}\nu>A_k)\ \&\ \mathop{\&}_{k=1}^{J}(B_k>\sigma^{m_k}\nu)\ \&\ \mathop{\&}_{k=1}^{L}(\sigma^{p_k}\nu=C_k)\ \&\ \Pi_r(\nu)\right)\&\ Q\ , \tag{30}$$

where as before A_k, B_k, and C_k are well-formed cardinal-valued TPB-terms, and r, n_k, m_k, and p_k are integer-valued constants. Moreover, since $A>B$ if and only if $\sigma A>\sigma B$, (30) can be further simplified to

$$(\exists\nu)\left(\mathop{\&}_{k=1}^{I}(\sigma^n\nu>A_k)\ \&\ \mathop{\&}_{k=1}^{J}(B_k>\sigma^n\nu)\ \&\ \mathop{\&}_{k=1}^{L}(\sigma^n\nu=C_k)\ \&\ \Pi_r(\nu)\right). \tag{31}$$

If $L\geq 1$, then (31) is clearly equivalent to

$$\mathop{\&}_{k=2}^{L}(C_1=C_k)\ \&\ \mathop{\&}_{k=1}^{I}(C_1>A_k)\ \&\ \mathop{\&}_{k=1}^{J}(B_k>C_1)\ \&\ \Pi_{r+n}(C_1)\ . \tag{32}$$

If $L=0$ but $I\geq 1$, then (31) can be written as

$$\mathop{\&}_{k=1}^{I}\ \mathop{\&}_{j=1}^{J}(B_k>\sigma A_j)\&\left(\bigvee_{k=1}^{I}\ \mathop{\&}_{j=1}^{I}(A_k\geq A_j\ \&\ \Pi_{n+r-1}(A_k))\right)\ . \tag{33}$$

The case $L=I=0$, $J\geq 1$ can be handled similarly. Thus (26) can always be reduced to a disjunction of generalized TPB-clauses with one fewer quantifier, so that recursive evaluation of the truth value of any TPB-clause is always possible.

V. Instantiation of Single-Valued and 1-1 Mappings.

Next we consider quantified set-theoretic formulae of the form

$$(\exists f)e(f[E_1],\ldots,f[E_M],\ \underline{\text{domain}}\ f) \tag{34}$$

where f ranges over all single-valued maps, $f[s]$ designates the range of f on the set s, $e = e(x_1,\ldots,x_M)$ is any valid PB-expression, and $E_1,\ldots,E_R$ are sets or set-valued expressions. We can also consider formulae having this same internal structure but quantified over 1-1 maps F. (Generally speaking, on the next few pages we will use letters f, g, etc. to designate single-valued maps, and letters F, G, etc. to designate 1-1 maps.) Going still further, we will consider formulae

$$(\exists f)e(f^{n_1}[E_1],\ldots,f^{n_M}[E_M],\ \underline{\text{domain}}\ f) \tag{35}$$

where the n_j are positive integers, and where f^n designates the n-th power of f. The 1-1 map case corresponding to (35) can also be considered.

We take up (34) first. This case is handled by forming all possible intersections H_i of the sets E_k, and <u>domain</u> f, and their complements. This gives us a collection $H_1,\ldots,H_R$ of sets, and then <u>domain</u> f, as well as each of the sets E_k can be written as a disjoint union:

$$E_k = \bigcup_{j\in\eta_k} H_j\ ,\ \underline{\text{domain}}\ f = \bigcup_{j\in\delta} H_j \tag{36}$$

where δ and η_k are subsets of $\{1,\ldots,R\}$. Then $f[E_k] = \bigcup_{j\in\eta_k} f[H_j]$; moreover the image sets $x_j = f[H_j]$ can be chosen independently and arbitrarily subject only to the restriction $\#x_j \le \#H_j$ and $\#x_j \ge 1$ if $j \in \delta$. Hence (25) can be rewritten as

$$(\exists x_1,\ldots,x_R)\Big(e(\bigcup_{j\in\eta_1} x_j,\ldots,\bigcup_{j\in\eta_M} x_j,\bigcup_{j\in\delta} x_j)\ \&\ \mathop{\&}_{j=1}^{R}(\#x_j\le\#H_j)\ \&\ \mathop{\&}_{j\in\delta}(\#x_j\ge 1\vee\#H_j=0)\Big)\ . \tag{37}$$

The techniques described in the preceding section can then be used to eliminate the quantified set variables $x_1,\ldots,x_R$, after which (34) will have been converted into a set-theoretic formula having the same structure as (34) but containing one fewer quantifier. Clearly, sets $x_1,\ldots,x_R$ instantiating (37) define a map f instantiating (34).

Even if the existentially quantified map variable in (25) is required to be 1-1, much the same technique can be used. In this case, we have only to insist that each x_j have the same cardinality as H_j, and that distinct x_j be disjoint. This means that in the 1-1 case (25) should be rewritten as

$$(\exists x_1,\ldots,x_R)\Big(e(\bigcup_{j\in\eta_1} x_j,\ldots,\bigcup_{j\in\eta_M} x_j,\bigcup_{j\in\delta} x_j)\ \&\ \mathop{\&}_{j=1}^{R}(\#x_j=\#H_j)\ \&\ \mathop{\&}_{j=1}^{R}\mathop{\&}_{i=j}^{j-1}(\#x_ix_j=0)\Big)\ . \tag{38}$$

To handle the somewhat more general cases (35), first suppose that $n_1\ge 1$. Then (35) can be written as

$$(\exists f,x_1,\ldots,x_{n_1})\Big(e(x_{n_1},f^{n_2}[E_2],\ldots,f^{n_M}[E_M])\ \&\ x_1=f[E_1]\ \&\ \mathop{\&}_{j=2}^{n_1}(x_j=f[x_{j-1}])\Big)\ . \tag{39}$$

Exactly the same transformation applies even if f is required to be 1-1. Thus in any case (35) can be reduced to a formula like (34).

The case of (35) in which all n_j are negative can also be regarded as a case of (35) in which all n_j are positive but in which the quantified map variable ranges over one-to-many instead of single-valued many-to-one maps. The transformation which leads from (34) to (37) can still be applied; thus in the case considered we can confine our attention to formulae of the form (34), but in which f ranges over one-to-many maps rather than single-valued maps. In this case, the image sets $x_j = f[H_j]$ which appear in (37) can still be chosen independently, but must be disjoint and are subject to the condition $\#x_j \geq \#H_j$. Hence for f quantified over the <u>inverses</u> of single-valued maps, (34) is equivalent to

$$(\exists x_1,\ldots,x_R)\Big(e(\bigcup_{j\in\eta_1} x_j,\ldots,\bigcup_{j\in\eta_M} x_j,\bigcup_{j\in\delta} x_j)\ \&\ \mathop{\&}_{j=1}^{R}(\#x_j \geq \#H_j)\ \&\ \mathop{\&}_{j=1}^{R}\ \mathop{\&}_{l=1}^{j-1}(\#x_2 x_j = 0)\Big)\ . \tag{40}$$

Note also that since inverses of 1-1 maps are simply 1-1 maps, (38) and (39) apply without change in the 1-1 case even if all the n_j in (35) are negative.

VI. <u>Another Special Case</u>.

The all too obvious inefficiency of the general techniques described in the two preceding sections makes it clear that more efficient special instantiation methods will remain useful. We shall now extend the introductory result derived in Section II above by considering the existentially quantified formula

$$(\exists x)(ax + b\bar{x} = \phi\ \&\ c_1 x + d_1 \bar{x} \neq \phi\ \&\ c_2 x + d_2 \bar{x} \neq \phi)\ . \tag{41}$$

(This corresponds to $m = 2$ in the notation of Section II.) In this case a solution for x can be expressed as follows:

$$x = \text{if } (c_1 + c_2 - a) \neq \phi \,\&\, ((c_1 \subseteq a \,\&\, d_2 \subseteq b \,\&\, c_2 - a = d_1 - b) \vee \tag{42}$$

$$(c_2 \subseteq a \,\&\, d_1 \subseteq b \,\&\, c_1 - a = d_2 - b)) \text{ then}$$

$$b + \{\epsilon (c_1 + c_2 - a)\}$$

$$\text{else if } (c_1 \subseteq a \,\&\, d_1 - b \subseteq c_2 - a) \vee (c_2 \subseteq a \,\&\, d_2 - b \subseteq c_1 - a) \text{ then}$$

$$b + ((c_1 - d_2) + (c_2 - d_1) - a)$$

$$\text{else } b + (c_1 + c_2 - a) .$$

Here $\{\epsilon s\}$ denotes an arbitrary singleton subset of the set s. To show that (42) solves (41) if (41) has any solution, we first note that a solution can only exist if $ab = \phi$, and that any solution x of (41) must satisfy $b \subseteq x \subseteq \bar{a}$. Hence we can assume that $ab = \phi$, and then we argue by cases. Clearly $x_0 = b + (c_1 + c_2 - a)$ is a solution of (41) unless $c_1 \subseteq a$ or $c_2 \subseteq a$. Moreover, if $c_1 \subseteq a$ & $c_2 \subseteq a$, then $x_0 = b$, and since any solution of (41) must include b it follows in this case that x_0 solves (41) if any solution exists. Hence special consideration is only required for cases in which one but not both of the inclusions $c_1 \subseteq a$, $c_2 \subseteq a$ holds. Suppose for the sake of definiteness that $c_1 \subseteq a, \neg c_2 \subseteq a$. In this case, x_0 solves (41) unless $d_1 \subseteq x_0 = b + (c_2 - a)$. If we now suppose that $c_2 - a \neq d_1 - b$, then $x_1 = b + (c_2 - d_1 - a)$ is a solution of (41). Since $c_1 - a = \phi$, this solution can be written symmetrically as $b + ((c_2 - d_1) + (c_1 - d_2) - a)$. Moreover, even if $c_2 - a = d_1 - b$, $x_1 = b$ still solves (41) unless $d_2 \subseteq b$. The remaining subcase is that in which

$c_1 + c_2 - a \neq \phi$, $c_1 \subseteq a$, $d_2 \subseteq b$, $c_2 - a = d_1 - b$, in which case a solution exists if and only if $c_2 - a$ has more than one element. In this subcase, the union of b and any proper part of $c_2 - a$ is a solution of (41).

The argument that we have just given justifies the solution (42) and shows that the Boolean expression (41) is equivalent to

$$
\begin{aligned}
ab = \phi \;\&\; (&c_1 - a \neq \phi \;\&\; c_2 - a \neq \phi \\
&v(c_1 + c_2 - a = \phi \;\&\; d_1 - b \neq \phi \;\&\; d_2 - b \neq \phi) \\
&v(c_1 - a = \phi \;\&\; c_2 - a \neq \phi \;\&\; d_1 - (b + c_2 - a) \neq \phi) \\
&v(c_1 - a = \phi \;\&\; c_2 - a \neq \phi \;\&\; d_1 - b \neq c_2 - a) \\
&v(c_1 - a = \phi \;\&\; c_2 - a \neq \phi \;\&\; d_2 - b \neq \phi) \\
&v(c_2 - a = \phi \;\&\; c_1 - a \neq \phi \;\&\; d_2 - (b + c_1 - a) \neq \phi) \\
&v(c_2 - a = \phi \;\&\; c_1 - a \neq \phi \;\&\; d_2 - b \neq c_1 - a) \\
&v(c_2 - a = \phi \;\&\; c_1 - a \neq \phi \;\&\; d_1 - b \neq \phi) \\
&v(c_1 - a = \phi \;\&\; d_2 - b = \phi \;\&\; c_2 - a = d_1 - b \;\&\; \#(c_2 - a) > 1) \\
&v(c_2 - a = \phi \;\&\; d_1 - b = \phi \;\&\; c_1 - a = d_2 - b \;\&\; \#(c_1 - a) > 1) .
\end{aligned}
\tag{43}
$$

All but the two final disjuncts in (43) involve two set-theoretic inequalities, i.e., have the same form as (41). The two final disjuncts have the form $A = \phi \;\&\; \#B > 1$, for which reason it is worth examining existentially quantified statements of this form, i.e.,

$$(\exists x)(ax + b\bar{x} = \phi \;\&\; \#(cx + d\bar{x}) > k) , \tag{44}$$

a little more closely.

A solution x of (44) must satisfy $b \subseteq x \subseteq \bar{a}$; and the only elements $y \in \bar{a} - b$ that it pays to include in the solution are those which belong to c. Hence if a solution exists then $b + (c - a)$ is a solution. It follows that (44) is equivalent to $ab = \phi \;\&\; \#((c - a) + (d - b)) > k$; thus multiply quantified statements of the form (44) can be handled using the techniques described in this Section and in Section II above.

VII. Is This an Application?

We consider the Schröder-Bernstein theorem, a set-theoretic formula also considered in [Minor, 1978]. This can be written as follows:

$$(\forall x,y,F,G)((\underline{\text{domain}}\ F = x \;\&\; \underline{\text{domain}}\ G = y \;\&\; F[x] \subseteq y \;\&\; G[y] \subseteq x) \longrightarrow (\exists H)\, H[x] = y)\ , \tag{45}$$

where as previously F, G, H designate 1-1 maps. The evaluation algorithm for formulae quantified over maps described in the preceding pages will verify this assertion without difficulty, essentially reducing it via the following sequence of equivalent forms:

$$(\forall x,y,F,G)((\underline{\text{domain}}\ F = x \;\&\; \underline{\text{domain}}\ G = y \;\&\; F[x] \subseteq y \;\&\; G[y] \subseteq x) \longrightarrow (\#x = \#y))\ . \tag{46a}$$

$$(\forall x,y,F,u)((\underline{\text{domain}}\ F = x \;\&\; F[x] \subseteq y \;\&\; u \subseteq x \;\&\; (\#u = \#y) \longrightarrow (\#x = \#y))\ . \tag{46b}$$

$$(\forall x,y,v,u)(u \subseteq x \;\&\; v \subseteq y \;\&\; (\#u \leq \#y) \;\&\; (\#v \leq \#x) \longrightarrow (\#x = \#y))\ . \tag{46c}$$

This last formula is verified almost immediately by the basic TPB-verification algorithm.

From the point of view of the verification system designer, this is an interesting and perfectly legitimate application of the techniques we have developed. Note however that from the foundational point of view this "application" is circular and hence a bit spurious, since the TPB-formula verifier implicitly embodies facts concerning cardinals which are distinctly deeper than the Schröder-Bernstein theorem being verified.

REFERENCES

Behmann, H. [1922]: Beiträge Zur Algebra der Logik, insbesondere zum Entscheidungsproblem, Math. Annalen, Vol. 86, pp. 163-220.

Bledsoe, W. W. and Bruell, P. [1974]: A Man-Machine Theorem Proving System, Artificial Intelligence, Vol. 5, pp. 51-72.

Bledsoe, W. W. [1975]: A New Method for Proving Certain Presburger Formulas, Proc. Fourth Int. Joint Conf. Artif. Intelligence, Tiblisi, U.S.S.R.

Bledsoe, W. W. [1977a]: Non-resolution Theorem Proving, Artificial Intelligence, Vol. 9, pp. 1-35.

Bledsoe, W. W. [1977b]: A Maximal Method for Set Variables in Automatic Theorem Proving, Tech. Rept. ATP 33A, Automatic Theorem Proving Project, University of Texas, Austin, Texas.

de Carvalho, R. L. [1974]: Some Results in Automatic Theorem-Proving With Applications in Elementary Set Theory and Topology, Tech. Rept. 71, Dept. of Computer Science, University of Toronto.

Cooper, D. C. [1972]: Theorem-Proving in Arithmetic Without Multiplication, Machine Intelligence, John Wiley Publishers, Vol. 7, pp. 91-99.

Minor, J. T. [1978]: Eliminating Function Quantifiers from Second Order Logic Expressions, Thesis Draft, University of Texas, Austin, Texas.

Presburger, M. [1929]: Uber die Vollstandigkeit eines gewissen Systems der Arithmetik ganzer Zahlen, in welchem die Addition als einzige Operation vortritt. Comptes Rendus der Ier Congrès des Mathématiciens des Pays Slaves., Warsawa, pp. 92-101.

Rabin, M. O. and Fisher, M. J. [1973]: Super-Exponential Complexity of Theorem-Proving Procedures. Proc. AMS/SIAM Symp. Appl. Math., pp. 27-42. Amer. Math Soc., Providence, Rhode Island.

Shostak, R. E. [1977]: On the SUP-INF Method for Proving Presburger Formulas, J.A.C.M., Vol. 24, pp.

Tarski, A. [1956]: Ordinal Algebras, North-Holland Publishing Co., Amsterdam.