PROVING A SUBSET OF SECOND-ORDER LOGIC WITH FIRST-ORDER PROOF PROCEDURES

by

John T. Minor, III

August 1979 ATP-54

ABSTRACT

PROVING A SUBSET OF SECOND-ORDER LOGIC

WITH FIRST-ORDER PROOF PROCEDURES

John T. Minor, III

August 1979

A mechanical procedure is described for reducing a subset of second-order logic to an expanded first-order logic, which remains provable by existing first-order proof procedures. This reduction is accomplished by first eliminating predicate quantifiers from second-order expressions, using a procedure based on the theoretical work of W. Ackermann and H. Behmann. Their papers on the classic Elimination Problem of Mathematical Logic were written in the 1920's and 1930's. Function quantifiers are reduced next by finding logically equivalent expressions in first-order logic augmented by a special constant predicate, D(x,y,z) defined as x(y)=z, which is axiomatized in a way that can be used by first-order provers.

ACKNOWLEDGMENTS

I would like to thank Dr. Woodrow W. Bledsoe and Dr. Norman M. Martin for the time and guidance they gave me so that this paper could be completed. Dr. Ewing L. Lusk of the University of Northern Illinois was kind enough to run some of my results through his university's fine resolution prover.

This work was supported in part by NSF grant MCS 77-20701.

CONTENTS

CHAPTER I

INTRODUCTION

Section 1 : Summary

Many times in mathematical logic, it is easier to write a formula, or possible theorem, in second-order logic, although the efficient, complete proof procedures are all first order. It thus becomes important to know when a second-order expression is equivalent to a first-order one, and to which first-order expression it reduces. That is the aim of this paper. For example, consider the two second-order theorems:

(1) $$\forall x\, A(x,x) \wedge \overline{A(b,a)} \wedge \overline{A(c,b)} \rightarrow \exists P(\overline{P(a)} \wedge P(b) \wedge \overline{P(c)})$$

and

(2) $$\exists f\, \forall x(f(b)=a \wedge (x \neq b \rightarrow f(x)=c))$$

The normal second-order (and higher-order) proof procedures attempt to construct a predicate P in the proof of (1) and a function f in the proof of (2) which satisfy their respective expressions. The mechanical procedure discussed in this paper will instead convert (1) to

$$\forall x\ A(x,x) \wedge \overline{A(b,a)} \wedge \overline{A(c,b)} \longrightarrow (a \neq b \wedge c \neq b)$$

and (2) to

$$\forall x\ \exists u((x=b \longrightarrow u=a) \wedge (x \neq b \longrightarrow u=c))$$

which are both easily proved by existing first-order procedures.

Chapter II of this paper discusses problems of type (1), that is, the elimination of predicate quantifiers from second-order expressions. This part is based on the theoretical work of H. Behmann and W. Ackermann from the 1920's and 1930's, when this problem was called the Elimination Problem. The first section concerns the Ackermann case,[1] which is $\exists P\ \mathcal{E}(P)$ where all individual quantifiers in $\mathcal{E}$ are universal. Here also is given an easy way to decide if an second-order expression will reduce to a finite first-order formula by this procedure. In section 2 we allow existential quantifiers also, although it is possible for a problem of type (2) to arise in this section after the elimination of the predicate quantifiers. Behmann's special case[4], the pure monadic second-order logic, is touched on in section 3.

Chapter III discusses problems of type (2), that is, how to handle function quantifiers in second-order expressions. Here we describe a procedure to replace these second-order expressions with equivalent first-order formulas augmented with a higher-order predicate D, whose axioms can still be utilized by first-order proof procedures. Section restricts the problem to one-place functions and universally quantified individuals, while section 2 allows extentions of this case. Finally section 3 will give some examples.

Section 2 : Notation

The second-order language being used is that of standard first-order[7] augmented with variable predicate symbols and variable function symbols, which can be quantified universally, $\forall$, or existentially, $\exists$, like variable individuals. These second-order quantifiers obey syntactic and semantic rules which correspond to those obeyed by first-order quantifiers.[6,9]

Symbol conventions being followed are:

(1) individuals	– constants	a, b, c, ...	(first of alphabet)
	– variables	... x, y, z	(last of alphabet)
(2) predicates	– constants	A, B, C, ...	
	– equality	= (special constant)	
	– variables	P, Q, R, ...	
(3) functions	– constants/variables	f, g, h, ...	
(4) connectives	– and $\wedge$, implies $\rightarrow$, equivalent $\leftrightarrow$.		
	or $\vee$, not $\overline{\quad}$ (over-lined)		

In cases where there is a question about what is constant or variable, we will assume that any symbol that is not bound by a quantifier, that is, it appears <u>free</u>, represents a constant, and any bound by a quantifier must be a variable. Script capital letters like $\mathcal{A}$, $\mathcal{B}$, $\mathcal{E}$, $\mathcal{M}$, etc. are metasymbols representing arbitrary expressions in the language.

Note that it is not necessary to have function symbols in second-order logic, since they can be replaced by predicates. For example, a two-place predicate F can replace the one-place variable function f in

$$\exists f\, \mathcal{E}(f(a)=b)$$

by writing

$$\exists F(\forall x \forall y(F(x,y) \wedge \forall z(F(x,z) \rightarrow z=y)) \wedge \mathcal{E}(F(a,b)).$$

In fact, in the second chapter of the paper, it is convenient to assume that all function quantifiers have been replaced by their predicate equivalent. Then the problem becomes to eliminate <u>only</u> predicate quantifiers, one at a time, until the problem is reduced to first order, or it is known the expression does not reduce. Unfortunately during this process, Skolem-function quantifiers are sometimes introduced (see section 2). These are handled in Chapter III, where we <u>now</u> can assume that only function quantifiers exist, as all predicate quantifiers have been eliminated previously.

<u>Rule R</u>

Frequent use will be made of the rule

$$\mathcal{E}(c) \longleftrightarrow \forall x(\mathcal{E}(x) \vee x \neq c)$$

in order to make all positions in a predicate or function universally-quantified variables, or in making some simplifications. This will be referred to as using Rule R.

Section 3 : The Dual Case

The problem being discussed in this paper is how to treat expressions like $\exists P\ \mathcal{E}(P)$ or $\exists f\ \mathcal{E}(f)$ when they appear in the conclusion of a theorem which is to be proven. When these expressions appear in the hypothesis (or an axiom, a known property, a previously proved lemma, etc.), then we can assume the variable predicate or function exists, replace it with a constant, and ignore the quantifier. When they appear in the conclusion, no such simple process exists to treat the quantifier.

The dual problem to the one above is when expressions like $\forall P\ \mathcal{E}(P)$ or $\forall f\ \mathcal{E}(f)$ appear in a hypothesis. This problem will not be treated separately. Instead this problem can be solved by taking the negation of the given expression, solving the resulting problem by the methods described in the following chapters, and then taking the negation of the resulting solution. It is possible to give procedures and rules for the dual case, but this is unnecessary.

CHAPTER II

ELIMINATION OF PREDICATE QUANTIFIERS

Section 1 : Universally Quantified Individuals

Assume the inmost predicate quantifier of a given formula and its scope is represented by $\exists P\ \mathcal{E}(P)$, where $\mathcal{E}(P)$ is a first order expression except for containing the n-place predicate variable P, where $n \geq 1$. (We will ignore sentential variables, the n=0 case, as they cause no problem.) We can assume $\mathcal{E}(P)$ will not separate into $\mathcal{E}_1(P) \vee \mathcal{E}_2(P)$, because if it will, we can consider it as two problems, $\exists P\ \mathcal{E}_1(P) \vee \exists P'\ \mathcal{E}_2(P')$.

In this section we will further assume that all individual quantifiers in $\mathcal{E}$ are universal. In section 2 we will treat the case when existentially quantified variables are allowed in $\mathcal{E}$.

Now if we eliminate $\rightarrow$ and $\longleftrightarrow$ symbols and write $\mathcal{E}$ in conjunctive normal form (CNF), with the ranges of quantifiers and negation signs restricted as much as possible, then we can separate the appearing conjuncts into three classes:

Class $\alpha(P)$: P always appears positively (unnegated) in the conjunct;

Class $\beta(\overline{P})$: P always appears negated in the conjunct;

Class $\gamma(P\overline{P})$: P appears as both negated and positive in the conjunct, and because of quantifier scopes cannot be separated into the two classes $\alpha(P)$ and $\beta(\overline{P})$.

Note that P or $\overline{P}$ must appear in all the conjuncts of $\mathcal{E}$, or else the conjunct is outside the scope of $\exists P$.

We need the following definition:

<u>Definition</u> $\alpha(P)$ (or $\beta(\overline{P})$) is a <u>unary</u> <u>class</u> if and only if every conjunct in the class has only one appearance of P (or $\overline{P}$) in it.

Now we proceed to the elimination of P from the second-order expression $\exists P\, \mathcal{E}(P)$. There are three distinct cases:

<u>Case 1</u> : Class $\alpha(P)$ is empty, or class $\beta(\overline{P})$ is empty. In this case $\exists P\, \mathcal{E}(P)$ is equivalent to universal truth.

<u>Proof</u> If class β is empty, then $\mathcal{E}(P) = \alpha(P) \wedge \gamma(P\overline{P})$, and thus P will appear positively in every conjunct. So by letting P be the universal truth predicate, we can make $\mathcal{E}(P)$ true, and thus $\exists P\, \mathcal{E}(P)$ is equivalent to universal truth.

Similarly when class α is empty, we can let $\overline{P}$ be the universal false predicate

<u>Case 2</u> : Class $\gamma(P\bar{P})$ is empty and either class $\alpha(P)$ is unary or class $\beta(\bar{P})$ is unary. In this case $\exists P\, \mathcal{E}(P)$ is equivalent to a finite first-order expression. The procedure for producing it is described below, followed by a proof of its correctness.

<u>Procedure</u> If we assume $\alpha(P)$ is unary, then all the conjuncts in α can be collected together into the one conjunct:

$$\forall x_1 \forall x_2 \ldots \forall x_n (P(x_1,x_2,\ldots,x_n) \vee \mathcal{Q}(x_1,x_2,\ldots,x_n)) .$$

This is done by first using Rule R to make sure every position in P is a universally quantified variable. Then by renaming the variables in each conjunct in α, we can factor them into one conjunct, letting $\mathcal{Q}$ represent the conjunction of the non-P parts. For example:

$$(P(a) \vee A) \wedge \forall x(P(x) \vee B(x))$$

can be rewritten by using Rule R as:

$$\forall z(P(z) \vee z \neq a \vee A) \wedge \forall x(P(x) \vee B(x)).$$

Now by renaming variable z as x, we can factor the above into:

$$\forall x(P(x) \vee [(x \neq a \vee A) \wedge B(x)])$$

where the part in brackets will be referred to as $\mathcal{Q}(x)$.

Thus $\exists P\, \mathcal{E}(P)$ can be rewritten as

$$\exists P(\forall x_1 \ldots \forall x_n (Px_1,\ldots,x_n) \vee \mathcal{Q}(x_1,\ldots,x_n)) \wedge \beta(\bar{P}))$$

which we now claim is equivalent to the first-order expression

$$\beta(\mathcal{Q}).$$

That is, the reduction is accomplished by simply replacing each appearance of $\bar{P}$ in β with the predicate $\lambda t_1 \ldots t_n.\ \mathcal{Q}(t_1,\ldots,t_n)$.

Similarly if $\beta(\overline{P})$ is unary, then $\exists P\, \mathcal{E}(P)$ can be rewritten as

$$\exists P(\forall x_1 \ldots \forall x_n(\overline{P(x_1,\ldots,x_n)} \vee \mathcal{B}(x_1,\ldots,x_n)) \wedge \alpha(P))$$

which we claim is equivalent to

$$\alpha(\mathcal{B}).$$

<u>Proof</u> We now prove the claim that

$$\exists P(\forall x_1 \ldots \forall x_n(P(x_1,\ldots,x_n) \vee \mathcal{A}(x_1,\ldots,x_n)) \wedge \beta(\overline{P}))$$

$$\longleftrightarrow \beta(\mathcal{A}).$$

($\longleftarrow$) comes from the fact that we can let P be $\overline{\mathcal{A}}$, which gives

$$\forall x_1 \ldots \forall x_n(\overline{\mathcal{A}(x_1,\ldots,x_n)} \vee \mathcal{A}(x_1,\ldots,x_n)) \wedge \beta(\overline{\overline{\mathcal{A}}}).$$

Now since the first conjunct is a tautology, this reduces to

$$\beta(\mathcal{A}).$$

($\longrightarrow$) comes from a property of β, namely that whenever

$$\forall x_1 \ldots \forall x_n(A(x_1,\ldots,x_n) \longrightarrow B(x_1,\ldots,x_n))$$

is true then

$$\beta(A) \longrightarrow \beta(B)$$

must follow. Now let P_0 be the predicate that fulfills the hypothesis, so that

$$\forall x_1 \ldots \forall x_n(P_0(x_1,\ldots,x_n) \vee \mathcal{A}(x_1,\ldots,x_n)) \wedge \beta(\overline{P_0}).$$

This can be rewritten as

$$\forall x_1 \ldots \forall x_n(\overline{P_0(x_1,\ldots,x_n)} \longrightarrow \mathcal{A}(x_1,\ldots,x_n)) \wedge \beta(\overline{P_0})$$

and therefore

$$(\beta(\overline{P_0}) \longrightarrow \beta(\mathcal{A})) \wedge \beta(\overline{P_0})$$

is true, so that by modus ponens we can imply $\beta(\mathcal{A})$.

A similar proof goes through for the claim:

$$\exists P(\forall x_1 \ldots \forall x_n(\overline{P(x_1,\ldots,x_n)} \vee \mathcal{B}(x_1,\ldots,x_n)) \wedge \alpha(P)) \longleftrightarrow \alpha(\mathcal{B})$$

by letting P be $\mathcal{B}$, and by noticing that α satisfies the above same property that β does.

Case 3 : The conditions of case 1 and case 2 are not satisfied. That is, either all three classes are present, or both α and β exist but are non-unary. In this case $\exists P\ \mathcal{E}(P)$ will not reduce to a finite first-order expression by these methods, but rather to an infinite conjunction of the form $\bigwedge_{i=1}^{\infty} (\mathcal{E}_i)$, where each $\mathcal{E}_i$ is first order. Ackermann's general procedure generates this infinite expression, but since the result is useless for the purposes of this paper, we will not give it here. Instead we will treat this case as non-reducible to first order.

A proof of the fact that this case is indeed always infinite is included in Appendix I, as it involves understanding of Ackermann's general procedure.[1]

The above classification of conjuncts and the separation of second-order problems into cases is the work of the author. The procedure used in case 2, and the proof of its correctness, is taken from the 1934 paper of Wilhelm Ackermann.[1]

<u>Examples</u> It might be helpful to see how one uses the preceding ideas in some examples.

$$(1)\quad \exists P\, \forall x\, \forall y\, [(A(x,y) \vee P(x,y)) \wedge (B(x,y) \vee \overline{P(x,x)}) \wedge (C(x,y) \vee \overline{P(x,x)} \vee \overline{P(y,y)})]$$

In this second-order expression, the first conjunct is in class α, the remaining are in class β. Since class α is unary, we are in case 2 and need only let $\overline{P}$ be $\lambda x,y.\ A(x,y)$ in the β conjuncts:

$$\forall x\, \forall y\, [(B(x,y) \vee A(x,x)) \wedge (C(x,y) \vee A(x,x) \vee A(y,y))]$$

$$(2)\quad \exists P\, \forall x\, \forall y\, [(P(x) \vee A(x,y)) \wedge (\overline{P(x)} \vee B(x,y)) \wedge (P(x) \vee \overline{P(y)} \vee C(x) \vee C(y))]$$

One might think this last conjunct is in class γ, but it separates

$$(P(x) \vee C(x)) \quad \vee \quad (\overline{P(y)} \vee C(y)).$$

Therefore we can convert (2) into two problems:

$$(2')\quad \exists P\, \forall x\, [(P(x) \vee \forall y\, A(x,y)) \wedge (\overline{P(x)} \vee \forall y\, B(x,y)) \wedge (P(x) \vee C(x))]$$

$$(2'')\quad \exists P\, \forall x\, [(P(x) \vee \forall y\, A(x,y)) \wedge (\overline{P(x)} \vee \forall y\, B(x,y)) \wedge (\overline{P(x)} \vee C(x))]$$

Now only α and β clauses appear in both problems, and both classes are unary. So we now let P be $\lambda x.\ \forall y\, B(x,y)$ in (2') and $\overline{P}$ be $\lambda x.\ \forall y\, A(x,y)$ in (2"):

$$\forall x\, [(\forall y\, B(x,y) \vee \forall y\, A(x,y)) \wedge (\forall y\, B(x,y) \vee C(x))]$$
$$\vee\quad \forall x\, [(\forall y\, A(x,y) \vee \forall y\, B(x,y)) \wedge (\forall y\, A(x,y) \vee C(x))].$$

or after factoring:

$$\forall x \left[(\forall y\, A(x,y) \vee \forall y\, B(x,y)) \wedge ((\forall y\, B(x,y) \vee C(x)) \vee (\forall y\, A(x,y) \vee C(x))) \right]$$

(3) $\exists P(\overline{P(a)} \wedge P(b) \wedge \overline{P(c)})$

(This problem is from the introduction.) Using Rule R, we rewrite

$$\exists P(\forall x(P(x) \vee x \neq b) \wedge \overline{P(a)} \wedge \overline{P(c)})$$

Now we let $\overline{P}$ be $\lambda x.\ x \neq b$, which gives

$$(a \neq b \wedge c \neq b).$$

(4) $\exists P \left[P(0) \wedge \forall x\ \forall y(P(x) \wedge S(x,y) \rightarrow P(y) \wedge \overline{P(a)} \right]$

(This is the contradiction of the induction axiom, where $S(x,y)$ means y is the successor of x.) After eliminating the $\rightarrow$ sign:

$$\exists P \left[P(0) \wedge \overline{P(a)} \wedge \forall x\ \forall y(\overline{P(x)} \vee P(y) \vee \overline{S(x,y)}) \right]$$

Now all three classes appear, and the γ clause cannot be separated so this is case 3, and it will not reduce to a finite first-order expression by this method. (It does reduce to $\bigwedge_{i=0}^{\infty} (a \neq i)$.) Therefore the induction axiom also does not reduce.

Section 2 : The Appearance of Existentially Quantified Individuals

We now come to the case where existential quantifiers of individuals appear in $\mathcal{E}(P)$, the scope of $\exists P$. In many instances this will cause no problem, for as we push the universal quantifiers in (restrict their range) as much as possible, we can often bring the existential quantifiers out front of the universal ones. When they can be moved in front of all the universal quantifiers, then they can be brought in front of the $\exists P$ and the elimination can proceed as in section 1. But assume now that there is a quantifier that cannot be moved completely out front, for example

$$\mathcal{E}(P) = \forall x_1 \ldots \forall x_k \exists y \; \mathcal{E}'(P, x_1, \ldots, x_k, y) .$$

Then we replace y with a function of $x_1, \ldots, x_k$:

$$\mathcal{E}(P) = \exists f \; \forall x_1 \ldots \forall x_k \; \mathcal{E}'(P, x_1, \ldots, x_k, f(x_1, \ldots, x_k))$$

This is the so-called Skolem's procedure, although it is actually an application of the axiom of choice.

After executing the above procedure for all such existential quantifiers, the $\exists f_i$'s can be brought in front of $\exists P$ and the elimination of P can proceed as in section 1. After the elimination of the predicates we are left with a problem like:

$$\exists f_1 \ldots \exists f_m \; \mathcal{E}(f_1, \ldots, f_m)$$

In some circumstances this is still an easy problem, since we can use the reversal of Skolem's procedure to eliminate the function quantifiers, such as:

$$\exists f \; \forall x_1 \ldots \forall x_k \; \mathcal{E}'(f(x_1, \ldots, x_k), x_1, \ldots, x_k)$$
$$\longleftrightarrow \forall x_1 \ldots \forall x_k \; \exists y \; \mathcal{E}'(y, x_1, \ldots, x_k) .$$

In general this will not be the case, as the form of $\mathcal{E}(P)$ is substantially changed during the elimination of P. We will attempt this problem in Chapter III.

Note that replacing a n-place variable function by its predicate equivalent will not help, since the predicate used will appear as

$$\exists P(\forall x_1 \ldots \forall x_n \exists y\, P(x_1,\ldots,x_n,y) \wedge \ldots).$$

In order to eliminate P we must introduce a Skolem-function for y, and thus we return to the same type of problem.

<u>Examples</u> We give here two examples where we must introduce function quantifiers in order to proceed with a predicate elimination. In the first one, we are able to reverse Skolem's procedure after the elimination; in the second, this is not possible.

(1) $\exists P \left[\forall x\, \exists y(A(x,y) \wedge P(x,y)) \wedge \forall x\, \exists y(B(x,y) \wedge \overline{P(x,y)})\right]$

We introduce two functions to take the place of the y's:

$$\exists f\, \exists g\, \exists P\, \forall x \left[A(x,f(x)) \wedge P(x,f(x)) \wedge B(x,g(x)) \wedge \overline{P(x,g(x))}\right]$$

We can now reduce the scope of $\exists P$ even more:

$$\exists f\, \exists g \left[\forall x(A(x,f(x)) \wedge B(x,g(x))) \wedge \exists P\, \forall x(P(x,f(x)) \wedge \overline{P(x,g(x))})\right]$$

Using Rule R we can rewrite this last part as:

$$\exists P \left[\forall x\, \forall y(P(x,y) \vee y \neq f(x)) \wedge \forall x\, \overline{P(x,g(x))}\right]$$

which reduces by the procedure in section 1 to

$$\forall x\, (g(x) \neq f(x)).$$

Therefore (1) is equivalent to

$$\exists f\ \exists g\ \forall x\ [A(x,f(x)) \wedge B(x,g(x)) \wedge g(x) \neq f(x)]$$

or after reverse Skolemization:

$$\forall x\ \exists u\ \exists v\ [A(x,u) \wedge B(x,v) \wedge u \neq v]$$

which is a simple first-order expression.

(2) $\exists P\ \forall x\ \exists t\ [(\overline{P(t)} \vee A(x,t)) \wedge \forall y(P(y) \vee B(y,t))]$

First we replace t by a function:

$$\exists f\ \exists P\ \forall x\ [(\overline{P(f(x))} \vee A(x,f(x))) \wedge \forall y(P(y) \vee B(y,f(x)))]$$

or after restricting the range of x and renaming:

$$\exists f\ \exists P\ [\ \forall x(\overline{P(f(x))} \vee A(x,f(x))) \wedge \forall y(P(y) \vee \forall z\ B(y,f(z)))]$$

Now we let $\overline{P}$ be $\lambda y.\ \forall z\ B(y,f(z))$

$$\exists f\ \forall x\ [\ \forall z\ B(f(x),f(z)) \vee A(x,f(x))]$$

We cannot reduce this by reverse Skolemization, since f appears as a function of two different variables. We will show how to treat this type of problem in Chapter III.

Section 3 : Special Case - Pure Monadic Second-Order Logic

One of the first special cases of the Elimination Problem to be completely solved was the pure monadic second-order case. In fact Behmann[4] and others[9] have shown it to be equivalent to first order by always being able to eliminate the predicate quantifiers from expressions in this subset of second-order logic.

The pure monadic case puts two restrictions on second-order logic, namely there cannot be any constant or variable functions, and all constant and variable predicates must be one-place, or monadic. Under these restrictions we can make the following observations:

(1) Both classes α and β will always be unary, when they exist;

(2) Class γ will never exist; and

(3) Existential quantifiers oan always be moved out front of all universal quantifiers.

Therefore in section 1, we will always have case 1 or 2, by the above observations (1) and (2), and in section 2 we will never have to introduce function quantifiers, by observation (3). Hence the result of the elimination will always be a finite first-order expression, and therefore we can say the pure monadic second-order case is equivalent to first-order logic.

Note also that if equality of individuals, the dyadic predicate =, is added to this special case, all expressions still remain equivalent to first-order expressions. This is easy to understand when one realizes that the definition of equality is a monadic second-order expression, namely

$$x=y \longleftrightarrow \forall P(P(x) \longleftrightarrow P(y)).$$

CHAPTER III

REDUCTION OF FUNCTION QUANTIFIERS

Section 1 : One-place Functions and Universal Variables

In this section we will assume that we are faced with the problem:

(1) $\exists f_1 \exists f_2 \ldots \exists f_m \mathcal{E}(f_1, f_2, \ldots, f_m)$ $(m \geq 1)$

where the f_i's are all one-place functions, and $\mathcal{E}$ is a first-order expression except for containing the f_i's. Further assume that all variables in $\mathcal{E}$ are universally quantified and, for convenience, is in conjunctive normal form. We will consider extensions to this problem in the next section.

First we show that (1) can be written in the fundamental form:

(2) $\exists f_1 \ldots \exists f_k \forall x_1 \ldots \forall x_n \mathcal{M}(x_1, \ldots, x_n, f_1(x_{n_1}), \ldots, f_k(x_{n_k}))$

where $\mathcal{M}$ is a first-order expression in which the f_i's appear only as shown, and the x_{n_i}'s are a sequence of variables taken from $x_1, \ldots, x_n$. $(k \geq n$ and $k \geq m)$

The process of getting this form involves two steps. We first use Rule R to make sure all the f_i's are functions of universally quantified variables only. We next make each function name f_i a function of a unique variable name x_{n_i}. In many instances this can be accomplished simply by renaming variables between conjuncts. In those cases where it is impossible to do this, for example $f(x)$ and $f(y)$ appear inside the same conjunct $\mathcal{C}$ as:

$$\exists f(\ \ldots \wedge \forall x \ \forall y \ \mathcal{C}(x,y,f(x),f(y)) \wedge \ldots \ )$$

then we introduce a new function name f', and rewrite the above as:

$$\exists f \ \exists f'(\ \ldots \wedge \forall x \ \forall y \ \mathcal{C}(x,y,f(x),f(y)) \\ \wedge \forall x \ \forall y(x \neq y \vee f(x)=f(y)) \wedge \ldots \ )$$

where the added conjunct just says $f=f'$. We continue this process of introducing new function names until all functions appear as functions of unique variable names.

Now we claim this fundamental form (2) is equivalent to

$$(3) \quad \exists f_1 \ldots \exists f_k \forall x_1 \ldots \forall x_n \exists y_1 \ldots \exists y_k \\ [\mathcal{M}(x_1,\ldots,x_n,y_1,\ldots,y_k) \\ \wedge D(f_1,x_{n_1},y_1) \wedge \ldots \wedge D(f_k,x_{n_k},y_k)]$$

where the y_i's are new variable names, and $D(f,x,y)$ is a new predicate which is true if and only if $f(x)=y$. The proof of this claim follows easily by substituting the definition of D into (3), and then using the dual case of Rule R, that is

$$\exists y_i(\mathcal{M}(y_i) \wedge f_i(x_{n_i})=y_i) \longleftrightarrow \mathcal{M}'(f_i(x_{n_i}))$$

for $i=1,\ldots,k$ to obtain form (2).

We can make this expression (3) a little simpler by using the reverse of the procedure of introducing Skolem-functions. For example, assume that in (3) f_1, f_2, and f_3 are all dependent on the one variable x_1, that is $x_{n_1} = x_{n_2} = x_{n_3} = x_1$. Then (3) is equivalent to

$$(4) \quad \exists f_4 \ldots \exists f_k \forall x_1 \exists y_1 \exists y_2 \exists y_3 \forall x_2 \ldots \forall x_n \exists y_4 \ldots \exists y_k \Big[\mathcal{M}(x_1, \ldots, x_n, y_1, \ldots, y_k) \wedge D(f_4, x_{n_4}, y_4) \wedge \ldots \wedge D(f_k, x_{n_k}, y_k)\Big]$$

In other words, we can eliminate the function quantifiers and corresponding D-predicates for all functions dependent on <u>one</u> of the x_i's. When $n > 1$, the choice of which functions to eliminate and which to keep in D-form becomes a heuristic decision, which will be discussed further in section 3 with the examples.

Note that $\mathcal{M}$ in both (3) and (4) is completely first order in the sense that it contains no second-order variables. Instead these variables, the f_i's, appear only in the first position of the D-predicate, and in a first-order prover they will be treated as variable individuals. D is a higher-order predicate, but like equality, it can be described by a set of first-order axioms.

<u>The D-Axioms</u>

(1) Naturally if f is a one-place function <u>symbol</u> in our domain, $\forall x\ D(\underline{f}, x, f(x))$ should be added as an axiom for the D-predicate, where $\underline{f}$ stands for the function $\lambda x.\ f(x)$ and will be treated as a constant by the first-order prover.

Unfortunately not all one-place functions will appear as "$f(x)$" in the given problem. For example:

(2) The <u>identity</u> <u>function</u> $i(x)=x$ exists in all domains, so we need

$$\forall x\ D(i,x,x).$$

(3) If f and g are one-place functions in our domain, then the <u>compositions</u> $f\cdot g$, $f\cdot f$, $g\cdot f\cdot g$, etc. are all one-place functions even though they may not appear explicitly. To handle compositions, we add the axiom:

$$\forall f\ \forall g\ \exists h\ \forall x\ \forall y\ \forall z(D(f,x,y) \wedge D(g,y,z) \longrightarrow D(h,x,z)).$$

(4) If c is a constant symbol appearing in our domain, then the <u>constant</u> <u>function</u> $\underline{c}(x)=c$ can be considered a one-place function. Therefore for each constant appearing, we add the axiom

$$\forall x\ D(\underline{c},x,c).$$

(5) Each n-place function symbol g, $n \geq 2$, appearing in our domain and depending on only one variable, can be considered a one-place function. We thus add the axiom:

$$\forall f_1 \ldots \forall f_n\ \exists h\ \forall x\ \forall x_1 \ldots \forall x_n (D(f_1,x,x_1) \wedge \ldots \wedge D(f_n,x,x_n) \longrightarrow D(h(g),x,g(x_1,\ldots,x_n)))$$

The validity of the above axioms is obvious, but to handle if-then-else combinations of two one-place functions, we need a somewhat more complicated axiom. First notice that when proving our form (3) each x_{n_i} becomes a constant functional of all the f_i's and appears in the D-predicate as $D(f_i,x_{n_i}(f_1,\ldots,f_i,\ldots,f_k),y_i)$.

(6) For each x_{n_i} appearing in a D-predicate as above, we add:

$$\forall f\ \forall g\ \exists c\ \exists d\ \forall y\ \forall z\ \forall w_1 \ldots \forall w_{i-1}\ \forall w_{i+1} \ldots \forall w_k$$
$$\Big[D(f,x_{n_i}(w_1,\ldots,c,\ldots,w_k),y) \rightarrow D(c,x_{n_i}(w_1,\ldots,c,\ldots,w_k),y)$$
$$\wedge D(g,x_{n_i}(w_1,\ldots,d,\ldots,w_k),z) \rightarrow D(d,x_{n_i}(w_1,\ldots,d,\ldots,w_k),z)$$
$$\wedge x_{n_i}(w_1,\ldots,c,\ldots,w_k) = x_{n_i}(w_1,\ldots,d,\ldots,w_k)\Big]$$

Proof Axiom (6) is derived by eliminating the predicate P from

$$\forall P\ \forall f\ \forall g\ \exists c\,\forall x((P(x) \rightarrow D(c,x,f(x))) \wedge (\overline{P(x)} \rightarrow D(c,x,g(x)))$$

which is true since we can let c be $\lambda x. \begin{cases} f(x) \text{ if } P(x) \\ g(x) \text{ if } \overline{P(x)}. \end{cases}$

First we bring the $\forall x$ out front of $\forall P$ by making it a function of c. After rewriting in disjunctive normal form:

$$\forall f\ \forall g\ \forall x\ \forall P\ \Big[\exists c(P(x(c)) \wedge D(c,x(c),f(x(c))))$$
$$\vee \exists c(\overline{P(x(c))} \wedge D(c,x(c),g(x(c))))$$
$$\vee \exists c(D(c,x(c),f(x(c))) \wedge D(c,x(c),g(x(c))))\Big]$$

Now the last disjunct just says that f=g, which we can assume is false. We rename c in the second disjunct d, and by using the dual of Rule R, rewrite as

$$\forall f\ \forall g\ \forall x\ \forall P\ \Big[\exists z(P(z) \wedge \exists c(z=x(c) \wedge D(c,x(c),f(x(c)))))$$
$$\vee \exists d(\overline{P(x(d))} \wedge D(d,x(d),g(x(d))))\Big]$$

We eliminate P by letting $\overline{P}$ be $\lambda z. \exists c(z=x(c) \wedge D(c,x(c),f(x(c))))$

$$\forall f\ \forall g\ \forall x\ \exists c\ \exists d(\ x(d)=x(c) \wedge D(c,x(c),f(x(c)))$$
$$\wedge D(d,x(d),g(x(d))))$$

To handle the variable functions f and g, we add two more D-terms to finally get:

For any functional x,

$$\forall f \, \forall g \, \exists c \, \exists d \, \forall y \, \forall z \, \big[x(d)=x(c) \wedge D(f,x(c),y) \rightarrow D(c,x(c),y) \wedge D(g,x(d),z) \rightarrow D(d,x(d),z) \big]$$

Now noticing that the only functionals to appear in a D-predicate are the x_{n_i} in fundamental form (3), we have axiom (6).

One may have noticed that if we let n=0 in axiom (5), that is, let g be a constant, then we get axiom (4). Also if we let n=1 then we get a combination of axioms (1) and (3). Therefore an alternate and shorter formulation of the D-axioms would be (2), (6), and

(5') For each n-place function symbol g, $n \geq 0$, then

$$\forall f_1 \ldots \forall f_n \, \exists h \, \forall x \, \forall x_1 \ldots \forall x_n (D(f_1,x,x_1) \wedge \ldots \wedge D(f_n,x,x_n) \longrightarrow D(h(g),x,g(x_1,\ldots,x_n))).$$

Section 2 : Extensions to Section 1

Existentially-quantified Variables Assume that not all variables in $\mathcal{E}$ are universally quantified, for example

$$\exists f_1 \ldots \exists f_m \forall x_1 \ldots \forall x_n \exists y\ \mathcal{E}'(f_1, \ldots, f_m, x_1, \ldots, x_n, y)$$

where it is not possible to move y any farther to the left. This case will cause no problem in obtaining expression (3) of the preceding section, and also no problem when eliminating function quantifiers that depend on a variable from $x_1, \ldots, x_n$, to get form (4). However if one wishes to eliminate functions that depend on a variable to the right of $\exists y$, then it will be necessary to replace y by a n-place function g, as:

$$\exists f_1 \ldots \exists f_m \exists g \forall x_1 \ldots \forall x_n\ \mathcal{E}'(f_1, \ldots, f_m, x_1, \ldots, x_n, g(x_1, \ldots, x_n))$$

The solution of this problem, that is, how to handle a n-place function, is discussed below.

Notice also that if y in the above expression were a k-place function instead of a variable, we can still move it out in front of the universally-quantified variables by replacing y by a (n+k)-place function.

N-place Functions Assume we now have the problem:

$$\exists f_1 \ldots \exists f_m\ \mathcal{E}(f_1, \ldots, f_m)$$

where the f_i's are all n, or less, -placed functions. We can consider all the functions as n-placed, for example, f(x) is thought of as $f(x,\ldots,x)$, and then by the Löwenheim process we can reduce all functions to one-placed. (This process involves transforming the problem from the original domain of individuals J to the Cartesian-product domain JxJx...xJ, see 1 and 10 for details.) Now we can reduce the functions by the previously-discussed procedures over this new domain. Finally the reverse Loweheim process is used on the resulting first-order expression and the D-axioms to get back to our original domain.

The above discussion is correct theoretically, but in practice, it is not necessary to go through this difficult procedure explicitly. For example, let us consider the n=2 case, where the functions are all one or two-placed. For this case, the above just means firstly that the steps used to get the fundamental form are extended naturally, eg. if $f(u,v)$ is to be renamed as $f'(u,v)$, then one adds the conjunct

$$\forall x \forall y \forall u \forall v (x \neq u \vee y \neq v \vee f(x,y)=f(u,v))$$

Now when converting to form (3) or (4), D becomes a four-place predicate and the definition becomes:

$$D(f,x,y,z) \longleftrightarrow f(x,y)=z.$$

Thus if we are letting v take the place of a two-place function $g(x,y)$ in $\mathcal{M}$, then we add the conjunct $D(g,x,y,v)$. Similarly if u is to take the place of a one-place function $f(x)$, then one adds the term $D(f,x,x,u)$.

The axioms for the n=2 case become:

The D_2-Axioms

(1) $\forall g \exists h \forall x \forall y \forall z(D(g,x,y,z) \rightarrow D(h,y,x,z))$

(the symmetric function)

(2) $\forall x \forall y\ D(i,x,y,x)$ (the projection function)

(3) For each n-place function symbol g, $n \geq 0$,

$$\forall f_1 \ldots \forall f_n \exists h \forall x \forall y \forall x_1 \ldots \forall x_n$$
$$(D(f_1,x,y,x_1) \wedge \ldots \wedge D(f_n,x,y,x_n)$$
$$\longrightarrow D(h(\underline{g}),x,y,g(x_1,\ldots,x_n)))$$

(4) For each functional-pair (x_{n_i}, y_{n_i}) which appears in a D-predicate as

$$D(f_i, x_{n_i}(f_1,\ldots,f_i,\ldots,f_k), y_{n_i}(f_1,\ldots,f_i,\ldots,f_k), u_i)$$

we write as an axiom:

$$\forall f \forall g \exists c \exists d \forall u \forall v \forall w_1 \ldots \forall w_{i-1} \forall w_{i+1} \ldots \forall w_k$$
$$\cdot\big[D(f, x_{n_i}(w_1,\ldots,c,\ldots,w_k), y_{n_i}(w_1,\ldots,c,\ldots,w_k), u)$$
$$\longrightarrow D(c, x_{n_i}(w_1,\ldots,c,\ldots,w_k), y_{n_i}(w_1,\ldots,c,\ldots,w_k), u)$$
$$\wedge D(g, x_{n_i}(w_1,\ldots,d,\ldots,w_k), y_{n_i}(w_1,\ldots,d,\ldots,w_k), v)$$
$$\longrightarrow D(d, x_{n_i}(w_1,\ldots,d,\ldots,w_k), y_{n_i}(w_1,\ldots,d,\ldots,w_k), v)$$
$$\wedge\ x_{n_i}(w_1,\ldots,c,\ldots,w_k) = x_{n_i}(w_1,\ldots,d,\ldots,w_k)$$
$$\wedge\ y_{n_i}(w_1,\ldots,c,\ldots,w_k) = y_{n_i}(w_1,\ldots,d,\ldots,w_k)\big]$$

The extension to higher-placed functions and thus higher-placed D-predicates proceeds naturally.

Section 3 : Examples

(1) $$\exists f\ \forall x\ \forall z(B(f(x),f(z)) \vee A(x,f(x)))$$

This example is a continuation of (2) from section 2 of Chapter II. We must first introduce a new function name, since f depends on both x and z in the same conjunct:

$$\exists f\ \exists g\ \forall x\ \forall z\ \left[(B(f(x),g(z)) \vee A(x,f(x))) \wedge (x \neq z \vee f(x)=g(z))\right]$$

Now this can be written in D-form as:

$$\exists f\ \forall z\ \exists v\ \forall x\ \exists u\ \left[(B(u,v) \vee A(x,u)) \wedge (x \neq z \vee u=v) \wedge D(f,x,u)\right]$$

or as:

$$\exists g\ \forall x\ \exists u\ \forall z\ \exists v\ \left[(B(u,v) \vee A(x,u)) \wedge (x \neq z \vee u=v) \wedge D(g,z,v)\right]$$

It will make no difference which form of the result is used, since the two functions f and g must be equal.

The following examples are actual theorems which can be proved with existing first-order proof systems:

(2) $((B \subseteq A \wedge B \neq \emptyset) \longrightarrow \exists f(f:A \rightarrow B \wedge f \text{ is onto}))$

Putting in the definitions of the symbols gives us the second-order expression: ($A(x)$ means $x \in A$)

$$(\forall x(B(x) \rightarrow A(x)) \wedge \exists b\ B(b) \longrightarrow \exists f(\forall x(A(x) \rightarrow B(f(x))) \wedge \forall y(B(y) \longrightarrow \exists t(A(t) \wedge f(t)=y)))$$

Now we put the conclusion in CNF:

$$\exists f \left[\forall x(\overline{A(x)} \vee B(f(x))) \wedge \forall y\ \exists t((\overline{B(y)} \vee A(t)) \wedge (\overline{B(y)} \vee f(t)=y)))\right]$$

We put a function in for t:

$$\exists f\ \exists g \left[\forall x(\overline{A(x)} \vee B(f(x))) \wedge \forall y(\overline{B(y)} \vee A(g(y))) \wedge \forall y(\overline{B(y)} \vee f(g(y))=y)\right]$$

Using Rule R we make f depend on a variable in the last conjunct:

$$\exists f\ \exists g \left[\forall x(\overline{A(x)} \vee B(f(x))) \wedge \forall y(\overline{B(y)} \vee A(g(y))) \wedge \forall y\ \forall z(\overline{B(y)} \vee f(z)=y \vee g(y) \neq z)\right]$$

Now by renaming we can make f and g depend on unique variables:

$$\exists f\ \exists g\ \forall x\ \forall y \left[(\overline{A(x)} \vee B(f(x))) \wedge (\overline{B(y)} \vee A(g(y))) \wedge (\overline{B(y)} \vee f(x)=y \vee x=g(y))\right]$$

This can be written as either

(2A) $$\exists g\ \forall x\ \exists u\ \forall y\ \exists v \left[(\overline{A(x)} \vee B(u)) \wedge (\overline{B(y)} \vee A(v)) \wedge (\overline{B(y)} \vee u=y \vee x \neq v) \wedge D(g,y,v)\right]$$

or

(2B) $$\exists f\ \forall y\ \exists v\ \forall x\ \exists u \left[(\overline{A(x)} \vee B(u)) \wedge (\overline{B(y)} \vee A(y)) \wedge (\overline{B(y)} \vee u=y \vee x \neq v) \wedge D(f,x,u)\right]$$

Here the choice between (2A) and (2B) does make a difference in the difficulty of the problem. (2A) can be proved with only the addition of the identity function axiom. (2B) requires also the axiom for the constant b, and the axiom for if-then-else combinations involving the variable x.

Both of these theorems were proved on the University of Northern Illinois's resolution-type, first-order prover. The proof of (2A) took 3.46 seconds, while (2B) took 9.25 seconds.

(3) $\exists f \, \forall x$(f is continuous at x)

$$\exists f \, \forall x \, \forall e(e>0 \rightarrow \exists d(d>0 \wedge \forall y(|x-y| \leq d \rightarrow |f(x)-f(y)| \leq e)))$$

Rewriting in CNF: (G(x,y) means x > y and a(x,y) means |x-y|)

$$\exists f \, \forall x \, \forall e \, \exists d \, \forall y \left[(\overline{G(e,0)} \vee G(d,0)) \wedge (\overline{G(e,0)} \vee G(a(x,y),d) \vee \overline{G(a(f(x),f(y)),e)}) \right]$$

Since f appears as a function of both x and y, we introduce g:

$$\exists f \, \exists g \, \forall x \, \forall e \, \exists d \, \forall y \left[(\overline{G(e,0)} \vee G(d,0)) \wedge (\overline{G(e,0)} \vee G(a(x,y),d) \vee \overline{G(a(f(x),g(y)),e)}) \wedge (x \neq y \vee f(x)=g(y)) \right]$$

This now reduces to :

$$\exists g \, \forall x \, \exists u \, \forall e \, \exists d \, \forall y \, \exists v \left[(\overline{G(e,0)} \vee G(d,0)) \wedge (\overline{G(e,0)} \vee G(a(x,y),d) \vee \overline{G(a(u,v),e)}) \wedge (x \neq y \vee u=v) \wedge D(g,y,v) \right]$$

This theorem can be proved by simply adding the axiom for the identity function. It can also be proved by adding the axiom for the constant 0, which appears in the formula, the anti-symmetry property for G, and the fact that a(x,x)=0.

(4) $\exists f\ \forall x(f \text{ is continuous at } x \wedge f(0)=0 \wedge f(1)=2)$

Using the definition of continuity from example (3), we rewrite the above using Rule R as

$$\exists f\ \forall x(\underline{\text{cont}}(f,x) \wedge (x\neq 0 \vee f(x)=0) \wedge (x\neq 1 \vee f(x)=2))$$

This reduces to:

$$\exists g\ \forall x\ \exists u\ \forall e\ \exists d\ \forall y\ \exists v\Big[(\overline{G(e,0)} \vee G(d,0)) \wedge (\overline{G(e,0)} \vee G(a(x,y),d) \vee \overline{G(a(u,v),e)}) \wedge (x\neq y \vee u=v) \wedge D(g,y,v) \wedge (x\neq 0 \vee u=0) \wedge (x\neq 1 \vee u=2)\Big]$$

This theorem can be proved by adding the D-axioms for the identity function and the constant 2. Also needed are the properties of multiplication (existence of identity, commutativity, associativity, existence of inverse, and the D-axiom), properties allowing us to multiply both sides of an equality or an inequality, and a property of a, namely, $a(z\cdot x, z\cdot y)=z\cdot a(x,y)$ if $z>0$.

(5) The following example is from the paper 5, in which this counterexample is wanted for a suspected false first-order formula.

$$\exists g\ \exists f\ \exists a\ \exists b\ \exists c\ [a \leq b \wedge f(a) \leq 0 \wedge 0 \leq f(b)$$
$$\wedge \forall x(a \leq x \leq b \wedge 0 < f(x) \rightarrow g(x) < x \wedge \forall s(g(x) < s \leq x \rightarrow 0 < f(s)))$$
$$\wedge (0 < f(g(b)) \vee g(b) \leq c)]$$

First we write it in CNF: $(G(x,y)$ means $x > y)$

$$\exists g\ \exists f\ \exists a\ \exists b\ \exists c\ [\overline{G(a,b)} \wedge \overline{G(f(a),0)} \wedge \overline{G(0,f(b))}$$
$$\wedge \forall x(G(a,x) \vee G(x,b) \vee \overline{G(f(x),0)} \vee G(x,g(x)))$$
$$\wedge \forall x\ \forall s(G(a,x) \vee G(x,b) \vee \overline{G(f(x),0)} \vee \overline{G(s,g(x))}$$
$$\vee G(s,x) \vee G(f(s),0))$$
$$\wedge (G(f(g(b)),0) \vee \overline{G(g(b),c)})]$$

Using Rule R we make the functions dependent on variables:

$$\exists g\ \exists f\ \exists a\ \exists b\ \exists c\ \forall x\ \forall s\ [\overline{G(a,b)} \wedge (x \neq a \vee \overline{G(f(x),0)})$$
$$\wedge (x \neq b \vee \overline{G(0,f(x))})$$
$$\wedge (G(a,x) \vee G(x,b) \vee \overline{G(f(x),0)} \vee G(x,g(x)))$$
$$\wedge (G(a,x) \vee G(x,b) \vee \overline{G(f(x),0)} \vee \overline{G(s,g(x))}$$
$$\vee G(s,x) \vee G(f(s),0))$$
$$\wedge (x \neq b \vee s \neq g(x) \vee G(f(s),0) \vee \overline{G(g(x),c)})]$$

Now since f appears as a function of both x and s in the same conjunct, we must introduce a new function symbol h:

$$\exists g\ \exists f\ \exists h\ \exists a\ \exists b\ \exists c\ \forall x\ \forall s\ \Big[\overline{G(a,b)} \wedge (x\neq a \vee \overline{G(f(x),0)})$$
$$\wedge (x\neq b \vee \overline{G(0,f(x))})$$
$$\wedge (G(a,x) \vee G(x,b) \vee \overline{G(f(x),0)} \vee G(x,g(x)))$$
$$\wedge (G(a,x) \vee G(x,b) \vee \overline{G(f(x),0)} \vee \overline{G(s,g(x))}$$
$$\vee G(s,x) \vee G(h(s),0))$$
$$\wedge (x\neq b \vee s\neq g(x) \vee G(h(s),0) \vee \overline{G(g(x),c)})$$
$$\wedge (x\neq s \vee f(x)=h(s))\Big]$$

Finally we can rewrite it in first-order as:

$$\exists h\ \exists a\ \exists b\ \exists c\ \forall x\ \exists u\ \exists v\ \forall s\ \exists w\ \Big[\overline{G(a,b)} \wedge (x\neq a \vee \overline{G(u,0)})$$
$$\wedge (x\neq b \vee \overline{G(0,u)})$$
$$\wedge (G(a,x) \vee G(x,b) \vee \overline{G(u,0)} \vee G(x,v))$$
$$\wedge (G(a,x) \vee G(x,b) \vee \overline{G(u,0)} \vee \overline{G(s,v)} \vee G(s,x)$$
$$\vee G(w,0))$$
$$\wedge (x\neq b \vee s\neq v \vee G(w,0) \vee \overline{G(v,c)})$$
$$\wedge (x\neq s \vee u=w) \wedge D(h,s,w)\Big]$$

A proof of this theorem, and thus a counterexample to the original problem, can be found simply by adding the D-axiom for the identity function, and the antisymmetry and antireflexive properties for G.

(6) An important example that illustrates the entire procedure discussed in both Chapter II and Chapter III is Cantor's Theorem from set theory:

Cantor's Theorem[8] For any set S and function $F:S \rightarrow 2^S$

$$\exists A(A \subseteq S \wedge \forall x(x \in S \rightarrow A \neq F(x)))$$

We first put in the definitions of $\subseteq$ and $\neq$ for sets:

($S(x)$ means $x \in S$)

$$\exists A \left[\forall z(A(z) \rightarrow S(z)) \wedge \forall x(S(x) \rightarrow \exists t((A(t) \rightarrow \overline{F(x,t)}) \wedge (\overline{A(t)} \rightarrow F(x,t))))\right]$$

Now we put this second-order expression in CNF:

$$\exists A \left[\forall z(\overline{A(z)} \vee S(z)) \wedge \forall x \, \exists t((\overline{S(x)} \vee \overline{A(t)} \vee \overline{F(x,t)}) \wedge (\overline{S(x)} \vee A(t) \vee F(x,t)))\right]$$

We must introduce a function for t:

$$\exists g \, \exists A \left[\forall z(\overline{A(z)} \vee S(z)) \wedge \forall x(\overline{S(x)} \vee \overline{A(g(x))} \vee \overline{F(x,g(x))}) \wedge \forall y(\overline{S(y)} \vee A(g(y)) \vee F(y,g(y)))\right]$$

Now we notice that the first two conjuncts are type β and the last is type α, and both classes are unary. Therefore we can eliminate A. First we make A dependent on a variable in the α conjunct by using Rule R:

$$\exists g \, \exists A \left[\forall z(\overline{A(z)} \vee S(z)) \wedge \forall x(\overline{S(x)} \vee \overline{A(g(x))} \vee \overline{F(x,g(x))}) \wedge \forall z(A(z) \vee \forall y(z \neq g(y) \vee \overline{S(y)} \vee F(y,g(y))))\right]$$

Then we let $\overline{A}$ be $\lambda z. \forall y(z \neq g(y) \vee \overline{S(y)} \vee F(y,g(y)))$

$$\exists g \left[\forall z \, \forall y(z \neq g(y) \vee \overline{S(y)} \vee F(y,g(y)) \vee S(z)) \wedge \forall x \, \forall y(\overline{S(x)} \vee \overline{F(x,g(x))} \vee g(x) \neq g(y) \vee \overline{S(y)} \vee F(y,g(y)))\right]$$

We can simplify by using Rule R to eliminate z:

$$\exists g \, \forall x \, \forall y \, \Big[(\overline{S(y)} \vee F(y,g(y)) \vee S(g(y))) \wedge (\overline{S(x)} \vee \overline{F(x,g(x))} \vee g(x) \neq g(y) \vee \overline{S(y)} \vee F(y,g(y))) \Big]$$

Now since g appears as a function of x and y in the second conjunct we must introduce a new function symbol h:

$$\exists g \, \exists h \, \forall x \, \forall y \, \Big[(\overline{S(y)} \vee F(y,g(y)) \vee S(g(y))) \wedge (\overline{S(x)} \vee \overline{F(x,h(x))} \vee h(x) \neq g(y) \vee \overline{S(y)} \vee F(y,g(y))) \wedge (x \neq y \vee h(x) = g(y)) \Big]$$

We can reduce to first order:

$$\exists g \, \forall x \, \exists u \, \forall y \, \exists v \, \Big[(S(v) \vee F(y,v) \vee \overline{S(y)}) \wedge (\overline{S(x)} \vee \overline{F(x,u)} \vee u \neq v \vee F(y,v) \vee \overline{S(y)}) \wedge (x \neq y \vee u = v) \wedge D(g,y,v) \Big]$$

We could have selected to eliminate the function g and write a D-predicate involving h instead, but it makes no difference in this problem, as g=h.

Since no constants nor constant function symbols appear in this theorem, and no other properties are used in the proof, we need to add only one D-axiom, namely $\forall x \, D(i,x,x)$. This theorem was proved by the University of Northern Illinois's resolution-type first-order prover in 2.75 seconds.

APPENDIX I

PROOF OF CASE 3

We now want to show that case 3 (see page 10) always leads to an infinite first-order expression under the general elimination procedure of W. Ackermann.[1] That is, we need to prove that whenever

(1) classes $\alpha(P)$ and $\beta(\bar{P})$ exist and are both non-unary,

or

(2) all three classes exist,

then the elimination result is infinite.

Proof We will assume that the predicate to be eliminated, P, has been reduced to a one-place predicate by the Löwenheim process.[9] (This is required by the Ackermann procedure.)

We first show that hypothesis (1) implies hypothesis (2) under this procedure. By hypothesis (1) we must have, at least, the two conjuncts:

$$\forall x_1 \ldots \forall x_m (P(x_1) \vee \ldots \vee P(x_m) \vee \mathcal{A}(x_1, \ldots, x_m)) \quad \text{with } m \geq 2$$

$$\forall y_1 \ldots \forall y_n (\overline{P(y_1)} \vee \ldots \vee \overline{P(y_n)} \vee \mathcal{B}(y_1, \ldots, y_n)) \quad \text{with } n \geq 2$$

Therefore we have Ackermann's fundamental-terms:

$$\mathcal{A}_{x_1, \ldots, x_m} \text{ and } \mathcal{B}^{y_1, \ldots, y_n}$$

which can be combined to form a new fundamental-term:

$$\forall z(\mathcal{A}_{z,x_2,\ldots,x_m} \vee \mathcal{B}^{z,y_2,\ldots,y_n})$$

But this term has the general form

$$\mathcal{C}^{y_2,\ldots,y_n}_{x_2,\ldots,x_m}$$

and since $n \geq 2$ and $m \geq 2$, this is the form of a fundamental-term derived from a conjunct of class $\gamma(P\overline{P})$, namely

$$\forall x_2 \ldots \forall x_m \forall y_2 \ldots \forall y_n (P(x_2) \vee \ldots \vee P(x_n) \vee \overline{P(y_2)} \vee \ldots \vee \overline{P(y_n)} \vee \mathcal{C}(x_2,\ldots,x_m,y_2,\ldots,y_n))$$

Therefore the results of hypothesis (1) are no different than if one assumes (2).

Now to prove (2) leads to an infinite result, we first solve the simplest case, that is, assume

$\forall x(P(x) \vee \mathcal{A}(x))$ appears in class α,

$\forall y(\overline{P(y)} \vee \mathcal{B}(y))$ appears in class β, and

$\forall x \, \forall y(P(x) \vee \overline{P(y)} \vee \mathcal{C}(x,y))$ appears in class γ.

Then we will have fundamental-terms:

$$\mathcal{A}_x, \mathcal{B}^y, \text{ and } \mathcal{C}^y_x$$

which can be combined to give the infinite sequence of terms:

$$\forall x_1 \ldots \forall x_n (\mathcal{A}_{x_1} \vee \mathcal{C}^{x_1}_{x_2} \vee \mathcal{C}^{x_2}_{x_3} \vee \ldots \vee \mathcal{C}^{x_{n-1}}_{x_n} \vee \mathcal{B}^{x_n})$$

for all $n \geq 1$.

Now since these terms make up the resultant of Ackermann's elimination, the resultant must be infinite.

If the problem given does not have these simple conjuncts appearing in all the classes, terms of the same form can always be built from more complicated terms by use of the combining rule. For example, from the terms

$$\mathcal{A}_x, \mathcal{B}^y, \text{ and } \mathcal{C}^{y_1,\ldots,y_n}_{x_1,\ldots,x_m} \quad \text{where } m > 1 \text{ or } n > 1$$

we can generate the term

$$\forall x_2 \ldots \forall x_m \forall y_2 \ldots \forall y_n (\mathcal{B}^{x_2} \vee \ldots \vee \mathcal{B}^{x_m} \vee \mathcal{C}^{y_1,\ldots,y_n}_{x_1,\ldots,x_m} \vee \mathcal{A}_{y_2} \vee \cdots \vee \mathcal{A}_{y_n})$$

which is of the form $\mathcal{C}'^{y_1}_{x_1}$.

By induction one can get proofs of similar reductions to the simplest case for the other classes α and β.

APPENDIX II

TWO FALSE SIMPLIFICATIONS

Since the name of the function that is substituted for f in an instantiation of D-predicate D(f,x,y) is not important, only the fact that there _is_ such a function, one might believe that it is possible to simplify our definition of D by eliminating the f from it. That is, one defines D(x,y) to mean "the value of y is dependent on the value of x", or in other words, D(x,y) is true if and only if there exists a function such that when applied to x, the the value equals y. This makes the axiomization of D _much_ simpler, but it also leads to counterexamples. For instance, we should be able to say that the false expression

$$\exists f \; \forall x \; \forall y (f(x) \neq y)$$

is equivalent to

$$\forall x \; \forall y \; \exists u (u \neq y \wedge D(x,u)).$$

Unfortunately in a domain with at least 2 individuals, eg. 0 and 1, then we can prove this last expression is true by using the two D-axioms $\forall x \; D(x,0)$ and $\forall x \; D(x,1)$.

The author also tried another simplification that would have allowed us to eliminate the if-then-else axioms, which are the most difficult and complicated to use. This was done by making each x that appeared in a D-predicate as D(f,x,y) independent of its own function f when Skolemizing, although it would still depend on all other functions appearing, as is normally the case. This means for the two-function case, that we should be able to say the following for arbitrary expression $\mathcal{E}$,

$$\exists f\ \exists g\ \forall x\ \forall y\ \mathcal{E}(x,y,f(x),g(y))$$
$$\longleftrightarrow \forall X\ \forall Y\ \exists u\ \exists g\ \exists v \left[\mathcal{E}\ (X(g),Y(u),u,v) \wedge D(g,Y(u),v)\right]$$

where X is a functional and Y is a function. The ($\longrightarrow$) direction is always true, but a counterexample can be found for the other direction. Namely, in a domain with <u>only</u> two individuals, 0 and 1, we let $\mathcal{E}$ be the expression that is true for the following quadruples:

(0,0,1,1), (0,1,1,1), (0,1,0,1)

(1,0,0,0), (1,0,1,1), (1,1,0,1)

and false for all other quadruples. In this instance, the last expression can be shown to be true by using the axioms $\forall x\ D(\underline{0},x,0)$ and $\forall x\ D(1,x,1)$, and the property $\forall x(x=0 \vee x=1)$. On the other hand, the first part of the equivalence can be shown to be false for this $\mathcal{E}$ in this domain of individuals.

BIBLIOGRAPHY

1) Ackermann, Wilhelm, "Untersuchungen über das Eliminationsproblem der mathematischen Logik", _Math Annalen_, Vol. 110 (1934), pp. 390-413.

2) ________, "Zum Eliminationsproblem der mathematischen Logik", _Math Annalen_, Vol. 111 (1935), pp. 61-63.

3) ________, _Solvable Cases of the Decision Problem_. North Holland, 1954.

4) Behmann, Heinrich, "Beiträge zur Algebra der Logik, insbesondere zum Entscheidungsproblem", _Math Annalen_, Vol. 86 (1922), pp. 163-229.

5) Bledsoe, W. W. and A. Michael Ballantyne, _Unskolemizing_. The University of Texas at Austin, Math Dept. Memo ATP-41, (July 1978).

6) Boolos, George S. and Richard C. Jeffrey, _Computability and Logic_. Cambridge University Press, 1974.

7) Chang, Chin-Liang and Richard Lee, _Symbolic Logic and Mechanical Theorem Proving_. Academic Press, 1973.

8) Halmos, Paul R., _Naive Set Theory_. D. Van Nostrand Company, 1960.

9) Hilbert, D. and W. Ackermann, _Mathematical Logic_, (Second edition, translated). Chelsea Publishing Company, 1950.

10) Löwenheim, Leopold, "Über Möglichkeiten im Relativkalkül", <u>Math Annalen</u>, Vol. 76 (1915), pp. 137-148.