ON SIMPLIFYING THE MATRIX OF A WFF

by

Peter B. Andrews

Report 67-1

revised
January, 1967

On Simplifying the Matrix of a Wff

by Peter Andrews[1]

§1. Introduction. In [3], [4], and [5] Joyce Friedman formulated and investigated certain rules which constitute a semi-decision procedure for wffs of first order predicate calculus in closed prenex normal form with prefixes of the form $\forall x_1 \ldots \forall x_k \exists y_1 \ldots \exists y_m \forall z_1 \ldots \forall z_n$. Given such a wff QM, where Q is the prefix and M is the matrix in conjunctive normal form, Friedman's rules can be used, in effect, to construct a matrix M* which is obtained from M by deleting certain conjuncts of M. Obviously $\vdash QM \supset QM^*$. Using the Herbrand-Gödel Theorem for first order predicate calculus, Friedman showed that $\vdash QM$ if and only if $\vdash QM^*$. Clearly if M* is the empty conjunct (i.e., a tautology), $\vdash QM^*$ so $\vdash QM$. Friedman also showed that for certain classes of wffs, such as those in which $m \leq 2$ or $n = 0$ in the prefix above, $\vdash QM$ if and only if M* is the empty conjunct. Hence for such classes of wffs the rules constitute a decision procedure. Computer implementation [4] of the procedure has shown it to be quite efficient by present standards.

The purpose of this paper is to present two theorems which are generalizations of Friedman's rules, and can be applied to wffs of higher order logics as well as first order logic. The theorems will apply to wffs in prenex normal form with arbitrary prefixes. Moreover (using the notation above),

---

[1] This research was partially supported by NSF Grant GP-4494.

|~ QM ≡ QM*. Therefore the theorems can be used to simplify the matrices of certain wffs whether or not they are valid.

We then go on to consider how these theorems can be applied to wffs from which existential quantifiers have been eliminated through the introduction of Skolem functions. We shall show that after one has simplified the matrix, one can go back to a wff with existential quantifiers but no Skolem functions, which is the original wff with a simplified matrix. Finally we shall show how to use these theorems as the basis for a complete proof procedure for first order logic.

§2. Many-Sorted Logic

We shall prove our theorems in the context of many-sorted first order logic with function symbols. The theorems in § 3 apply whether or not function symbols are present in the language, but in §7 we shall show that the theorems can be used as the basis of a complete proof procedure for first order logic when function symbols are present. The number of sorts may be finite or infinite. When there is just one sort, we have the usual first order predicate calculus. We shall present below a formulation of type theory whose wffs can be regarded as those of a many-sorted first order logic. Thus our theorems can be applied to type theory.

We now present the primitive basis for many-sorted first order logic. We assume given a non-empty, finite or denumerably infinite collection of symbols a_ι called sort symbols.

(a) ~~Improper symbols~~: [ ] T F ~ ∧ ∨ ∀ ∃ (brackets, truth, falsehood, negation, conjunction, disjunction, universal and existential quantifiers).

(b) Proper symbols: Let $\alpha, \alpha_1, \ldots, \alpha_n$ be sort symbols, where $n \geq 1$, and let i range over positive integers. Then the variables which may occur are individual variables x^i_α, function variables $f^i_{\alpha\alpha_1\ldots\alpha_n}$, and predicate variables $P^i_{\alpha_1\ldots\alpha_n}$. (Constants of various types may also occur, but for our present purposes they may usually be replaced by variables.)

Formation Rules

Terms are defined inductively as follows:

(a) x^i_α is a term of sort α.

(b) If $w_1, \ldots, w_n$ are terms of sorts $\alpha_1, \ldots, \alpha_n$, respectively, then $f^i_{\alpha\alpha_1\ldots\alpha_n} w_1 \ldots w_n$ is a term of sort α.

(No parentheses are required, since the number of arguments of each function variable is indicated by its subscripts.)

Wffs are defined inductively as follows:

(a) T and F are wffs.

(b) If $w_1, \ldots, w_n$ are terms of sorts $\alpha_1, \ldots, \alpha_n$ respectively, then $P^i_{\alpha_1\ldots\alpha_n} w_1 \ldots w_n$ is a wff.

(c) If A and B are wffs, then $\sim A$, $[A \wedge B]$, $[A \vee B]$, $\forall x^i_\alpha A$ and $\exists x^i_\alpha A$ are wffs.

Wffs of type (a) and (b) are atomic wffs.

For our present purposes it is not necessary to specify an economical set of axioms and rules of inference for our system. We simply state that the following familiar principles of quantification theory are primitive or derived rules of inference of our system. $\equiv$ and $\supset$ are introduced by appropriate definitions. A, A_1, B, C stand for arbitrary wffs, u, u_1, v stand for variables of any sort, and w, w_i stand for terms of any sort. \r A means that A is a theorem.S (S) denotes substitution for all(free)occurrences of the variables in question, following the notation of Church [2]. A term w is <u>free for</u> a variable u in a wff A if no free occurrence of u in A is in a wf part of A of the form VvC or 3vC, where v is a (free) variable in the term w.

<u>Rules of Inference</u>

I. (Rule P) If B is a substitution instance of a tautology, HB. If $[A_1$ A ... A $A_n]$ ^ B is a substitution instance of a tautology and h A_i for each i ($1 \leq i \leq n$)9 then *Y* B.

II. (Rule of alphabetic change of bound variables.) If u and v are of the same sort and u does not occur free in C and v does not occur in C, then the result of replacing one occurrence of C in a theorem by an occurrence of S^u_v C is a theorem.

III. (Rule of Substitution) If H A, and $u_1,...,u_n$ are distinct and for each i ($1 \leq i \leq n$), w_i is of the same sort as u. and free for u. in A. then h $S^{u_1 \ldots u_n}_{\quad\quad n}$A.

IV, Let w be of the same sort as u, let A(u) be a wff in which w is free for u, and let A(w) be S^u_wA. Then *h* VuA(u) =3 A(w) ; if *h* A(w) ^ B then V-VuA(u) ^ B. Also H A(w) 3 3uA(u) .

V. If I- A ^ B and u does not occur free in A then h- A ^ VuB,.

VI. If K A ^ B and u does not occur free in B then H ^{a}uA 3.B,.

VII. If h A 3 B then h VuA => VuB and H 3uA => 3uB.

If h A = B then H VuA = VuB and h 3uA ≡ 3uB.

VIII. If K ^ .A s B and u does not occur free in C, then hC ⇒ .VuA = VuB and h C ^ .3uA ≡ 3uB.

IX. (Substitutivity of Equivalence) If HA = B, then the result of replacing an occurrence of A by an occurrence of B in a theorem is a theorem.

X. If u is not free in A , then HVufA V B] ≡ .A V VuB and H Vu [B V A] ≡ VuB V A.

XI. M u [A V B] ≡ .3uA V 3uB.

XII. |- Vu ~ A s ~ 3uA.

Of course, in many contexts it is possible to reduce many-sorted logic to first order logic by introducing unary predicate constants $\$_\alpha$ for each sort *a 3* and writing Vx $_\alpha$A(x $_\alpha$) as V x f ^ ⇒ A(x)] and a^A(x^) as 3 X [^ X A A (X)] (see [9]). However, when one is concerned with the practical problems of searching for proofs of theorems of a discipline in which the individuals can naturally be divided into sorts, a many-sorted underlying logic may be a distinct advantage, since one is automatically prevented from considering certain wffs which express nonsense from an intuitive point of view.

We next present a formulation of type theory which constitutes a particularly useful example of a many-sorted logic. We define <u>type symbols</u> inductively as follows;

(a) *c* is a type symbol (the type of individuals).

(b) If T.J, . . . $_n$T are type symbols, then *(T^.*₀T$_n$)* is a type symbol. ((^{T}i***$^T{}_n$) ^s the type of propositional functions with n arguments, of types *T^,...T$_n$,* respectively.)

We take the type symbols as sort symbols for a many-sorted logic in which (for convenience) there are no function variables, and the only predicate constants of the form $u_{(\tau_1,\ldots,\tau_n)}$, where $\tau_1,\ldots,\tau_n$ are type symbols. Then an atomic wff $u_{(\tau_1,\ldots,\tau_n)} v^1_{\tau_1} \ldots v^n_{\tau_n}$ may be unambiguously abbreviated $u v^1 \ldots v^n$, and interpreted as meaning that $v^1_{\tau_1},\ldots,v^n_{\tau_n}$ stand in the relation $u_{(\tau_1\ldots\tau_n)}$. Of course, in addition to the rules of inference listed above one would assume the comprehension axioms

$$\exists u_{(\tau_1\ldots\tau_n)} \forall v_{\tau_1} \ldots \forall v_{\tau_n} [u_{(\tau_1\ldots\tau_n)} v_{\tau_1} \ldots v_{\tau_n} \equiv A],$$

where $u_{(\tau_1,\ldots,\tau_n)}$ does not occur free in the wff A.

§ 3. Theorems

We shall use the following notations and conventions. A <u>sign</u> is + or ~ . If A is a wff and σ is + , σA is A. If σ is ~ , σA is ~A unless A has the form ~B ; σ~B may stand for ~~B or B , the context determining the appropriate choice. An empty disjunction is F , and an empty conjunction is T.

Let QM be a wff in prenex normal form with prefix Q and matrix M. The wff may contain free variables, M is in full disjunctive normal form; i.e., M is a disjunction $D_1 \vee \ldots \vee D_n$ of disjuncts D_k, and each disjunct is a conjunction $P_{k1} \wedge \ldots \wedge P_{ku}$. The conjuncts P_{kj} are atoms or the negations of atoms, and each atom which occurs in M occurs exactly once in each disjunct. The quantifiers in Q are $\forall y_1, \ldots, \forall y_m$ (where $m \geq 0$) and $\exists z_1, \ldots, \exists z_n$ (where $n \geq 0$). (The Reduction Theorem stated below is vacuous for the case $m = 0$. The reader who wishes to compare the theorems below with Friedman's rules may consider that QM is the negation of the wff on which Friedman's rules operate; hence the reversal of the roles of universal and existential quantifiers.)

We shall say that a variable of the wff is absolutely stable if it is free in the wff, or if it is existentially quantified but its quantifier is in the scope of no universal quantifier.

Reduction Theorem

Let $w_1, \ldots, w_m$ be any m-tuple of terms such that w_i is of the same sort as y_i for $1 \leq i \leq m$. We define a variable of the wff to be stable (with respect to this m-tuple) if it is free in the wff, or if it is existentially quantified but its quantifier is in the scope of no universal quantifier $\forall y_i$ such that $w_i \neq y_i$. Let the unstable existentially quantified variables of the wff be $z_p, \ldots, z_n$. Let $t_p, \ldots, t_n$ be distinct variables which do not occur in the w_i or in the wff such that t_j has the same sort as z_j for $p \leq j \leq n$. Let $A_1, \ldots A_L$ be any set of atoms of the matrix in which none of $z_p, \ldots, z_n$ occur. Let $\sigma_1, \ldots, \sigma_L$ be signs.

Suppose there is no disjunct D_k of the matrix in which

(a) A_i occurs with sign σ_i for all i $(1 \leq i \leq L)$,

and in which

(b) for any two atoms B_1 and B_2 of the matrix, if

$S^{y_1 \ldots y_m z_p \ldots z_n}_{w_1 \ldots w_m t_p \ldots t_n} B_1$ is the same as $S^{y_1 \ldots y_m z_p \ldots z_n}_{w_1 \ldots w_m t_p \ldots t_n} B_2$

then B_1 and B_2 occur with the same sign in D_k.

Then let N be the disjunction of all disjuncts D_k of the matrix in which $S^{y_1 \ldots y_m}_{w_1 \ldots w_m} A_i$ occurs with sign σ_i for all i $(1 \le i \le L)$, and let $\tilde{N}$ be the disjunction of all remaining disjuncts of the matrix. Then $\vdash QM \equiv Q\tilde{N}$.

<u>Splitting Theorem</u>

Let $\mathcal{V}_1, \ldots, \mathcal{V}_q$ be disjoint (perhaps empty) sets of variables which are universally quantified in the wff, where $2 \le q \le m + 2$. If $\mathcal{V}_i$ is non-empty let its members be $y_{i1}, \ldots, y_{iR_i}$. For each variable y_{ij} occurring in one of these sets let w_{ij} be a term of the same sort. Let $A_{i1}, \ldots, A_{iL_i}$ (where $L_i \ge 1$) be atoms of the matrix in which only variables in $\mathcal{V}_i$ and absolutely stable variables occur. For each such atom A_{ij} let a_{ij} be a sign.

Suppose there is no disjunct of the matrix in which A_{ij} occurs with sign a_{ij} for all j $(1 \le j \le L_i)$ and all i $(1 \le i \le q)$. Form q disjunctions $N_1, \ldots, N_q$ of the disjuncts D_k as follows: N_i is the disjunction of all those disjuncts of the matrix in which

$S^{y_{i1} \ldots y_{iR_i}}_{w_{i1} \ldots w_{iR_i}} A_{ij}$ occurs with sign a_{ij} for all $j (1 \le j \le L_i)$.

Let $\tilde{N}_i$ be the disjunction of all the disjuncts of the matrix which are not in N_i. Then

$$\vdash QM \equiv \bigvee_{i=1} QN_i$$

Note: To facilitate the discussion of particular applications of these theorems, we shall refer to w.(w..) as the substitution term for y.(y..). When a substitution term for y. is not specified, the reader is to understand that w_1 is y_1.

§ 4. An example

Before proving the theorems we illustrate how they may be applied by using them to prove the following rather trivial theorem of second order logic:

Va3Rat.3v[Patv => Paav] A .Vu[VbRbau => VwGwtu]

^ 3x.VyRyxt ^ Sz.Pxaz A Gztx.

We shall refer to this wff as C. Evidently P, G, and R are are variables of type (tit)* and the remaining letters in C are variables of type t.

We put ~ C into prenex normal form and obtain aaVRVtVu3bVvVwVxVyVz. [Patv A ~ Paav] V . [~ Rbau V Gwtu] A Ryxt A [~ Pxaz V ~ Gztx]. We must next put the matrix of this wff into fully developed disjunctive normal form. Rather than write this matrix out completely we represent it by Figure 1.

Each row in Figure 1 represents all those disjuncts (i.e., conjunctions of signed atoms) in which each atom occurs with the sign indicated. If no sign occurs for some atom in a row, then the sign of that atom is arbitrary in disjuncts associated with that row. Of course some disjuncts are represented by more than one row; for example Patv A ~ Paav A ~ Rbau A ~ Gwtu A Ryxt A Pxaz A ~ Gztx is represented by rows (1) and (3). What is important is that a conjunction of signed atoms is a disjunct of the matrix if and only if it is represented by some row in

Figure 1. Matrix of — C

	Patv	Paav	Kbau	Gwtu	Ryxt	Pxaz	Gztx
(1)	+	~					
(2)			~		+	~	
(3)			~		+		~
(4)				+	+	~	
(5)				+	+		~

Figure 2. $\tilde{N}_2$ '

	Patv	Paav	Rbau	Gwtu	Ryxt	Pxaz	Gztx
(6)	+	~				+	
(7)			~		+	+	~
(8)				+	+	+	~

Figure 3. Amplified $\tilde{N}_1$

Patv	Paav	Rbau	Gwtu	Ryxt	Pxaz	Gztx	Paaa
+	~						
	~	~		+	~		
	~	~		+		~	
	~		+	+	~		
	~		+	+		~	

Figure 1.

We first apply the Splitting Theorem. Let [ϑ^ l = [vj and ^a ii^A ii = +Paav. Let [ϑ2 = (R,t,x,y] and ^a 2i^A 2l ~-~ Ryxt. The substitution terms for v,R,t,x,y are respectively v,P,z, a,x. Now there is no disjunct of the matrix in which + PaaV and ~ Ryxt both occur, so l— C = .QÑ̃1 V QÑ2, where Q is the prefix of ~ C, N1 is the disjunction of all disjuncts in Figure 1 which do not contain + Paav and N2 is the disjunction of all disjuncts which do not contain ~ Pxaz (see Figure 2) .

Next we apply the Reduction Theorem three times to the wff QÑp. First, the substitution terms for x,z are respectively a,v. There is no disjunct of N2 in which ~ Pxaz occurs, so we eliminate from N2 all disjuncts in which ~ Paav occurs. This eliminates all disjuncts in line (6) of Figure 2 (plus certain disjuncts-from lines (7) and (8)). Secondly, the substitution terms for t,x,y are respectively u,a,b. There remains no disjunct in which ~ Ryxt occurs, so we eliminate all disjuncts in which ~ Rbau occurs. Then only certain disjuncts in line (8) remain. Finally, as substitution terms for u,w we take x,z. There is now no disjunct in which M3wtu occurs, so we eliminate all disjuncts in which ~ Gztx occurs. This eliminates all remaining disjuncts, so fr- QS2L = QF. But \- F = QF, so by Rule Pf--C E QÑ1.

Next we turn our attention to QÑ^. First we replace Ñ1 by an equivalent matrix in fully developed disjunctive normal form which contains the atom Paaa in addition to the atoms of N^. (See Figure 3.) The reader may suppose, if he wishes, that we originally included in the matrix of ~ C all atoms which can be constructed from the variables occurring in the wff. Actually if one wishes to construct a general semi-decision procedure based on these theorems, the question of how to amplify a matrix *(i.e., add atoms to it) when necessary as economically as possible assumes considerable practical importance. Friedman has studied this question extensively for certain classes of wffs in [5].

Now we apply the Reduction Theorem twice to the matrix represented by Figure 3. First we take a as the substitution term for v. There is no disjunct in which + Paav occurs, so we eliminate all disjuncts in which + Paaa occurs. Then we take P,a,a,a,a as substitution terms for R,t,v,x,y. Now there is no disjunct in which (a) ~ Ryxt occurs and in which (b) Patv and Paav occur with the same sign. Therefore we eliminate all disjuncts in which ~ Paaa occurs. But this eliminates all remaining disjuncts, so $\vdash QN_1 \equiv F$. Therefore $\vdash \sim C \equiv F$ so $\vdash C$.

Note that when one attempts to use our theorems to prove a wff C as above, one simply attempts to reduce the matrix of ~ C to the empty disjunction, and there are only a finite number of ways in which one can apply the theorems to a given wff, so the process eventually terminates. If the matrix has not been reduced to the empty disjunction and the Splitting Theorem has been used, one is then left with an equivalence of the form $\vdash QM \equiv \bigvee_{i=1}^{p} QM_i$, where QM is equivalent to ~ C and each of the M_i is a disjunction of certain disjuncts of M. If we let N be the disjunction of all disjuncts which occur in some M_i, then $\vdash M_i \supset N$ and $\vdash N \supset M$ so $\vdash QM_i \supset QN$ and $\vdash QN \supset QM$ so $\vdash QM \equiv QN$. Now if N is not the same as M the wff QN is in a certain sense simpler than the wff QM, since it has fewer disjuncts in its matrix. Of course the theorems in §3 can be used to reduce the number of conjuncts in a matrix in full conjunctive normal form by applying them to the negation of the wff.

§5. Proofs

Proof of the Reduction Theorem:

In addition to the notation in §3, we shall use the following notation. Choose r so that $w_i = y_i$ for $i < r$, and $w_r \neq y_r$. Let $z_p, \ldots, z_n$ be the unstable existentially quantified variables of the prefix. Let Q' be the portion of the prefix containing $\forall y_r, \ldots, \forall y_m$ and $\exists z_p, \ldots, \exists z_n$, and let Q'' be the initial portion of the prefix. Then we may write the original wff as $Q''Q'[D_1 \vee \ldots \vee D_c]$. We shall write A_i as $A_i(y_r, \ldots, y_m)$, and use the obvious substitution notation: $A_i(w_r, \ldots, w_m)$ is $S^{y_r \ldots y_m}_{w_r \ldots w_m} A_i$. Similarly we write D_k as

After each line of the proof we indicate by a roman numeral the rules of inference from $\mathcal{J}2$ used to infer that line, and the numbers of the preceding lines from which it is inferred. It may be necessary to apply the rules of inference more than once.

1. $\vdash N \supset \bigwedge_{i=1}^{L} a_i A_i(w_r, \ldots, w_m)$ by Rule P, since each of the disjuncts of N contains $A_i(w_r, \ldots, w_m)$ with sign σ_i for $i = 1, \ldots, L$.

Let D_k be any disjunct of the matrix M, where $1 \leq k \leq c$. Then either case (a) or case (b) must apply:

case (a): D_k contains $\sim a_i A_i$ for some i, say i = j. Then

2a. $\vdash D_k \supset \sim\sigma_j A_j$. Rule P

3a. $\vdash D_k(w_r, \ldots, w_m;\ t_p, \ldots, t_n) \supset \sim\sigma_j A_j(w_r, \ldots, w_m)$ III:2a

case (b): There are atoms ^ and ^ ^ ^ ^ ^ g 1 occur, with positive sign and ^ wm negative sign in D_k but $S^{y_1 \ldots y_m\ z_p \ldots z_n}_{w_1 \ldots w_m\ t_p \ldots t_n} B_1 = S^{y_1 \ldots y_m\ z_p \ldots z_n}_{w_1 \ldots w_m\ t_p \ldots t_n} B_2$.

Denote the latter wff by B.

2b. $\vdash D_k \supset B_1 \wedge \sim B_2$ Rule P

3b. $\vdash D_k(w_r, \ldots w_m;\ t_p, \ldots, t_n) \supset B \wedge \sim B$ III:2b

Since for each k case (a) or case (b) must hold, we obtain

4. $\vdash N \supset \sim D_k(w_r, \ldots, w_m;\ t_p, \ldots, t_n)$ for $k = 1, \ldots, c$. Rule P:3b or 1 and 3a

5. $\vdash N \supset \sim[\bigvee_{k=1}^{c} D_k(w_r, \ldots, w_m;\ t_p, \ldots, t_n)]$ Rule P:4

6. $\vdash N \supset \sim\exists t_p \ldots \exists t_n [\bigvee_{k=1}^{c} D_k(w_r, \ldots, w_m;\ t_p, \ldots, t_n)]$ V,«,«1!5

7. $\vdash Q' [\bigvee_{k=1}^{c} D_k] \supset \exists t_p \ldots \exists t_n [\bigvee_{k=1}^{c} D_k(w_r, \ldots, w_m;\ t_p, \ldots, t_n)]$ I,II,IV,VII

8. $\vdash Q'M \supset \sim N$ Rule P:6,7

9. $\vdash Q'M \supset .M \equiv \tilde{N}$ Rule P:8

10. $\vdash Q'M \supset Q'M \equiv Q'\tilde{N}$ VIII:9

11. $\vdash Q'M \supset Q'\tilde{N}$ Rule P:10

12. $\vdash \tilde{N} \wedge M$ Rule P

13. $\vdash$ Qiff $o_{Q,M}$ VII:12

14. $\vdash Q'M \supset Q,$^ Rule P:11,13

15. hQ f! Q f M s Q 1! .Q f Ñ VII: 14

This completes the proof of the Reduction Theorem.

Proof of the Splitting Theorem

In addition to the notation in §3^ we shall use the following notation. Let $z_1, \ldots, z_{p-1}$ be the absolutely stable variables of the prefix. Then we may write the prefix Q as $\exists z_1, \ldots \exists z_{p-1}$ Q' where Q' is the remainder of the prefix. For each i ($1 \le i \le q$) we shall introduce new variables $y^i_1, \ldots, y^i_m$, $z^i_p, \ldots, z^i_n$ which are all distinct from one another and from all variables in the w_{ij} or in the given wff; moreover y^i_k is of the same sort as y_k, and z^i_k is of the same sort as z_k. Also let $t_p, \ldots, t_n$ be variables which are distinct from one another and from all variables mentioned above; t_k is of the same sort as z_k.

Define w^i_j for $1 \le i \le q$ and $1 \le j \le R_i$ to be $S^{y_1 \ldots y_m\, z_p \ldots z_n}_{y^i_1 \ldots y^i_m\, z^i_p \ldots z^i_n} w_{ij}$. Define v_{ik} for $1 \le k \le m$ to be y_k if y_k is in none of the sets $\mathcal{Y}_{i1}, \ldots, \mathcal{Y}_{iq}$ and to be w^i_j if y_k is the variable y_{ij} in some set $\mathcal{Y}_{ij}$. (The fact that the sets $\mathcal{Y}_{ij}$ are disjoint assures that this definition is unambiguous.)

We shall write A_{ij} as $A_{ij}(y_1, \ldots, y_m)$, M as $M(y_1, \ldots, y_m;\ z_p, \ldots, z_n)$, and N_i as $N_i(y_1, \ldots, y_m;\ z_p, \ldots, z_n)$, and use the associated substitution notation as above.

In certain lines of the proof below the parameter i occurs as a free variable of our meta-language. In such cases the reader is to understand that the theorem is asserted for each value of i ($1 \le i \le q$).

1. $\vdash N_i(y_1,\ldots,y_m ; z_p,\ldots,z_n) \supset \Lambda^{L}\ \sigma_{ij}A_{ij}(w_{i1},\ldots,w_{iR_i})$

by Rule P, since each of the atoms A. $_{ij}$(^i^ • • • J^{w}iR $_i$)

occurs with sign σ_{ij}. in each disjunct of N_i.

2. HVy^...,^ ; zj,...,zj) ⊃ A$^{L}_{j=i}$ a$_{ij}$A$_{ij}$(w$^1_{i1}$,...,w$^1_{iR_i}$) 111:1

(Consider the definition of w^i_{ij} to see that this is a legitimate substitution.)

3. KQ . M 3 at$_p$..-.':at$_n$M(v$_1$, ...,v$_m$5 t$_p$, ...,t$_n$) I,II,IV ,VII

4. M(y$_p$...,y$_m$; V " 2 ^ 3 ~ * , ^-^{a}ij^{A}ij(y$_{i1}$'," * ' $_{iR}$ ..)

by Rule P, since there is no disjunct of M in which A_{ij} occurs with sign σ_{ij}. for all i and j.

5. hM(v$_p$...,v$_m$; t$_p$,...,t$_n$) ^~ . A$^{q}_{1=1}$ $^{L_i}_{3=1}$;Vij^{A}i$_j$Kl-?-^R$_l$.) III:4

(Here we have replaced y_v by v_v on.the left^ and y. . by w^i_{13}. on the right; if y_K, is y_{13}, then v_v is w^i_{l}.,

so the substitution is legitimate. Also note that only "' variables in $\mathcal{V}_1$ and absolutely stable variables occur in A_{ij}.)

A, hat$_p$...at$_n$M(v$_1$,...,v$_m$; t$_p$,...,t$_n$) 3

~ -1$_{1-1}$ ^$^{L_i}_{J-1}$ ^ij^il^i'-'-^R$_1$.)- VI:5

7. f-Q'M = $\bigvee^q_{i=1}$ ~ N$_i$(yJ;,...,y^ z^,...,z^) RuleP:3,6,2

$\sim \bigvee^q_{i=1}$ Y l "' Ym − p---vzn w i iy l J •••^ym J z p''. "' V

V,IX,X:7

9. hQ'M=> $\bigvee_{i=1}^{q}$ Vy1# ..VymVzp...Vzn ~ N± 11:8

10. HVyi...VymVzp...V2n ~ N ± = - 1 ^ IV

11. h vyi-••vym Vz p---Vz n ~ N i 3 -M -=®i Rule p_10

12. H vy1---vym Vz p---Vz n ~ N i 3 -Q'M £ Q'Nj. vinai

13. i- Q»M => $\bigvee_{i=1}^{q}$ Q»N x. Rule P:9/12

14. h NA => M Rule P

15. H Q'^ =3 Q'M VII: 14

16. V-Q'M= [$\bigvee_{i=1}$ QIN x.] Rule P: 13,15

17. HazjL-'. . az- 1Q'M s azx...azp _x[^ Q'N±] VII:16

18. h QM = . $\bigvee^{q}$ QN: IX,XI:17

This completes the proof of the Splitting Theorem.

§6. Functional Form

The reader may have noticed that existential quantifiers are in a certain sense in the way when one wishes to apply the meta~theorems in §3. However it is well known that for each wff B one can find a wff #(B)3 called the functional form of B, such that 3(B) is satisfiable if and only if B is satisfiable, and such that 5(B) contains no existential quantifiers. J5(B) is obtained from B by replacing existential quantifiers by function variables in an appropriate way. Thus it is natural to apply our meta-theorems to 3(B) rather than to B. If the matrix of 3(B) can be reduced to the empty disjunction,, then B is not satisfiable; if not, then there is a wff C such that 3(B) has been reduced to 3(c)'/ so H 3(B) = %(C), and it is natural to ask whether HB = C. We shall show that this is so. To simplify our notation, we henceforth restrict our attention to one-sorted first order logic.

<u>Definitions</u> Let B be a wff of first order logic in which no variable occurs both free and bound, or occurs in two quantifiers, and in which no quantifier is in the scope of a negation symbol.

(1) If B contains existential quantifiers, let 3zD(z) be the first (leftmost) wf part of B consisting of an existential quantifier and its scope. Let $Vy^1 \ldots Vy^k$ be the quantifiers of B (in left to right order) which contain 3zD(z) in their scope, and whose variables occur (free) in D(z), and let f be the first k-ary function variable which does not occur in B. (We omit the subscripts and superscript of f for convenience.) Let $J5^1$ (B) be the result of replacing 3zD (z) by D(fy^{Ik}. . .y) in B. (If k = 0, f is an individual variable, and we use f in place of fy^{Ik} . . .y .)

(2) Let 3°(B) be B, and let 3^{j+1}(B) be ^ (3^j (B)) .

(3) '<*(B) is 3^n (B) , where n is the number of existential quantifiers in B.

Note that hD(fy ^{1}. . .y^k) ^ 3zD(z), so it is easily proved that h#^{1}(B) => B. (Here we use the fact that the only propositional connectives in B which contain 2zD(z) in their scope are A and V.) Hence h 3(B) ^ B. Note that every wff can easily be transformed into an equivalent wff satisfying the conditions of the definition.

Next we wish to embed our first order logic into a higher order logic so that we can quantify over function variables.

To avoid the necessity for describing explicitly the system of higher order logic we have in mind, we shall use the formulation /of type theory presented by Church in [1] and proved weakly complete by Henkin in [6]. We take as axioms only axioms 1 - 6 of [1] and call this system 3* . Let * be the wff

Vpot* azcpo(,Zt ^potfc6(Oc)poc^ which is a formulation of the axiom of choice with the constant c (/0M, denoting a choice function. Let 3* be the result of adding * to 3" as an additional axiom. We shall write \r2* A (kA^HnA) to mean that A is a theorem of 2T* (%, first order logic, respectively) . Every wff of first order logic can be regarded in a natural way as a wff of 3_y and we shall tacitly use this embedding of first order logic into 2. In the argument below we shall sometimes quantify on the constant cL(QL\ , • This will be a shorthand way of indicating the result of replacing it by an appropriately chosen variable, and then quantifying. Also we shall refer to derived rules of inference of 3* by the same numbers as were used for the corresponding rules of inference of first order logic in § 2.

Definition Given a wff B of first order logic such that 3(B) is defined, we define a wff 3* (B) of 3' by modifying the definition of 3 so that 3*°(B) = B and %* ^+1 (B) is obtained from <* J(B) upon replacing 3zD(z) by D(Gy . . .y Ik), where G is the wff [Ay ...Ay Ik . c ... .AzD(z)], and 3z is the jth existential quantifier originally present in B. (Thus we ignore quantifiers in the G's previously introduced.) Again 5*(B) is #*n(B), where n is the number of existential quantifiers in B.

Lemma |— ^B = 3 (B)

Proof:

,lh2,ªz[[AzD(z)]z] => [AzD(z)] [c t(oc) .AzD(z)]

by instantiation of [AzD (z)] for P_{Qt} in *.

.2 ⊢2* ∃zD(z) 3 [^zD(z)] [Gy¹...yᵏ]

by rules of A-conversion applied to .1.

.3 ⊢2* ∃zD(z) ⊃ D(Gy¹...yᵏ)

by rules of A-conversion applied to .2.

.4 -.K^DtGy¹...yᵏ) => 3zD(z) IV

.5 H2*ªzD(z) ≡ D(Gy¹...yᵏ) Rule P:.3,.4

.6 ^ 3*3 (B) s 3* J+1(B) IX:. 5,1

Hence h o.B ≡ 3* (B)

Theorem Let B be a wff of first order logic such that 3 (B) is defined. Let f¹ ^...^fⁿ be the (function or individual) variables which occur in & (B) but not in B. Then

⊢2* B ≡ ∃f¹...∃fⁿ℥(B)

Proof:

.1 h 2^-^ (B) - "^ B since h-3 (B) ^ B as remarked above.

.2 h2^3f¹...3fⁿ℥(B) ⊃ B VI:.1

Now we may assume that fⁱ is the variable which was introduced in forming 3¹(B) from 3¹""¹(B). Let G¹ be the corresponding wff introduced in forming 5¹(B) from 3 *¹"" ¹(B). fl fU Note that 3 (B) is S x n 3 (B), and that G¹ is free for f in 3 (B). Hence

.3 K*3*(B) z> 3f^X . . . 3f^n 3 (B) IV(n times), I.

.4 h^.B ≡ 3 (B) by the Lemma.
2*

.5 h ^ B = 3f^X . . . 3f^n J? (B) Rule P:.2,.3,.4

Lemma Let N be the standard model for ff (in the sense of [6]) in which the domain of individuals is the set of natural numbers. Then [3c /~$_f$x*] is true in N.

Proof: Since in a standard model the collection of functions of type (c *(Ou)*) includes all possible functions from subsets of the domain of individuals to individuals, it includes the function which maps the empty set onto 1 and every non-empty set onto its least member. But this function fulfills the requirements on the choice function c . $_{/rw}$ % .

Note: By assuming the Axiom of Choice in our meta-language, we could prove that [^c$_{i/r}$. **] is true in every standard model for ff. However the weaker result of the lemma is sufficient for our purposes.

Theorem Let B and C be wffs of first order logic such that 3(B) and #(C) are defined. Assume that no variable occurs free in 5(B) and C but not in B, and no variable occurs free in 5 (C) and B but not in C. If H ^ (B) ≡ 3(C), then *h*$_±$*B* ≡ C.

Proof: Let f^1 ,...,f^n be the set of variables which occur in 3(B) but not in B, or in 3 (C) but not in C. Then none of these occur free in B or in C.

.1 h$_2$*3(B) ≡ 3(c) since ^ (B) ≡ 3(C) .

.2 H$_2$^af$^1$...af^{n}ff(B) s afi.^af^cc) viir.i.

.3 h^B ≡ 3f^{1} . . .3f^{n} 3(B) by the theorem above, plus the introduction of vacuous quantifiers, if necessary.

.4 h_2^. C ≡ &f^{1}. . . 3f^{n}3 (C) as for .3.

.5 b_2* B ≡ C Rule P:.2,.3,.4.

.6 H_2* =3 .B ≡ C by the Deduction Theorem for 3*.

.7 h_2 t^{a}c$_{\iota(o\iota)}$*] ⊃ .B ≡ C VI: .6.

Now in order to show that (-$_{1}$ B ≡ C, it suffices to show that B ≡ C is valid in the domain of natural numbers, by Gödel's Completeness Theorem. But every theorem of 0* is valid, and by the Lemma [3c$_{\iota(o\iota)}$ ^] is true in N, so B ≡ C is true for every assignment of values to its free variables (of any type) in N. But this means B ≡ C is valid in the domain of natural numbers, so h-$_{1}$B ≡ C.

For the sake of completeness, we go on to prove the following:

<u>Theorem</u> Let B be a wff of first order logic such that 3(B) is defined. Then B is satisfiable if and only if ?(B) is satisfiable.

Proof: If 3(B) is satisfiable, then B is, since K$_{1}$3 (B) ^ B and every theorem is valid.

If B is satisfiable, then it is satisfiable in the domain of natural numbers by Löwenheim's Theorem. Now

$\vdash_{2*}$B ≡ ∃f^{1}...∃f^{n}𝔉(B) so $\vdash_2$[∃c$_{\iota(o\iota)}$*] ⊃ .B ≡ ∃f^{1}...∃f^{n}𝔉(B).

Arguing as above we see that B ≡ 3f^{1} ...3f^{n}3(B) is valid in N. There is an assignment of values in N to the free variables of B which makes it true, so the same assignment makes Bf^{1}...3f^{n}3(B) true. Hence 3(B) is satisfiable.

7. The Reduction-Amplification Method

In this section we shall show that the Reduction Theorem can be used as the basis for a complete proof procedure for first order logic. To simplify the notation we again restrict our attention to one-sorted logic.

Definitions

1) A wff is in functional normal form if its is in prenex normal form and contains no existential quantifiers.
2) The lexicon (Herbrand universe) of a wff is the class of all terms constructible from the free individual variables of the wff (if there are none, the first individual variable which does not occur in the wff) and the function variables in the wff.
3) A lexical instance of a wff in functional normal form is a quantifier-free wff obtained from the given wff by instantiating all of its quantifiers with terms from its lexicon.
4) If QM is a wff in prenex normal form, an amplification of its matrix M is any quantifier-free wff N in full disjunctive normal form such that $M \equiv N$ is a substitution instance of a tautology, and every atom in N is constructed from variables in M and the lexicon of $-QM$.

These definitions are adapted from [7] and [4]. Quine shows in [7] that a wff in functional normal form is not satisfiable if and only if some finite conjunction of its lexical instances is a contradiction.

Theorem Let QM_1 be an unsatisfiable wff in functional normal form with matrix M_1 in full disjunctive normal form. Then there is an amplification M_2 of M_1 such that QM_2 is reducible to QF by any sequence of applications of the Reduction Theorem, such that no further applications are possible.

Proof: Since QM_1 is not satisfiable, there is some finite conjunction $L_1 \wedge \ldots \wedge L_p$ of its lexical instances which is a contradiction. M_1 is a disjunction $D_1 \vee \ldots \vee D_c$, so each lexical instance L_i has the form $D_1^i \vee \ldots \vee D_c^i$, where D_k^i is obtained from D_k by substitution. Let M_2 be the amplification of M_1 obtained by adding all atoms which occur in $L_1 \wedge \ldots \wedge L_p$ to M_1. Let QM_3 be any wff obtained from QM_2 by a sequence of applications of the Reduction Theorem, such that no further applications are possible. We must show that M_3 is F. So suppose it is not. Then M_3 is a disjunction $E_1 \vee \ldots \vee E_e$ with $e \geq 1$.

<u>Lemma</u> For each disjunct E_j of M_3 and for each lexical instance L_i $(1 \leq i \leq p)$ there is some disjunct D_k^i of L_i such that $\vdash E_j \Rightarrow D_k^i$.

Proof: Let $A_1, \ldots, A_r$ be the atoms of M_1 and let $A_1^i, \ldots, A_r^i$ be the corresponding atoms of L_i. Each of these atoms occurs in E_j with some sign, so E_j may be written as $\sigma_1 A_1^i \wedge \ldots \wedge \sigma_r A_r^i \wedge H$, where H is the conjunction of the other signed atoms in E_j. (Of course $A_1^i, \ldots, A_r^i$ may not all be distinct, but this causes no difficulty if we let $\sigma_s = \sigma_t$ whenever $A_s^i = A_t^i$.) Suppose no disjunct D_k^i of L_i has the form $\sigma_1 A_1^i \wedge \ldots \wedge \sigma_r A_r^i$. Then no disjunct D_k of M_1 has the form $\sigma_1 A_1 \wedge \ldots \wedge \sigma_r A_r$, so no disjunct of M_2 contains $\sigma_1 A_1 \wedge \ldots \wedge \sigma_r A_r$ (since M_2 is simply an amplification of M_1).

so no disjunct of M_3 contains or $A_1' \wedge \ldots \wedge$ or A_L' (since every disjunct of M_3 is a disjunct of M_2). Then E_j can be eliminated from M_3 by the Reduction Theorem. But this contradicts the condition on M_3, so L_i has a disjunct D_k' of the form $a_1 A_1' \wedge \ldots \wedge a_L A_L'$, so $\vdash E_j \supset D_k'$. This proves the lemma.

Now $\vdash D_k' \supset L_i$ so $\vdash E_j \supset L_i$ for each disjunct E_j of M_3 and each lexical instance L_i. Hence $\vdash [E_1 \vee \ldots \vee E_e] \supset [L_1 \wedge \ldots \wedge L_p]$, so $\vdash M_3 \supset F$. Hence M_3 must be the empty disjunction. This proves the theorem.

Let us summarize briefly the way the Reduction Theorem can be used as the basis of a complete proof procedure for first order logic. Given a wff C, one can find a wff B equivalent to ~ C such that 3(B) is defined, and the prenex normal form QM of #(B) is in functional normal form. Hence C is valid if and only if some amplification of M can be reduced to F. Of course in practice one would amplify only a little at a time, when no further Reductions are possible, as mentioned by Friedman in [4]. We shall call this proof procedure the Reduction-Amplification procedure.

We have shown that the Splitting Theorem is in principle dispensable in this context, but of course it may be an important aid to efficiency, since it permits one to split a matrix into several simpler matrices. Similarly clause (b) in the statement of the Reduction Theorem can be omitted without loss of completeness, since we have not used it. (It is easy to see that several applications of the Reduction Theorem without clause (b) can give the same results as an application of the full Theorem when sufficiently many atoms are present in the matrix, and there are no existential quantifiers.) The resulting statement of the Reduction Theorem for use in this context is pleasingly simple.

Friedman recognized in [4] and [5] that the crucial problem in using the Reduction-Amplification procedure efficiently is the _amplification problem_, i.e. the problem of choosing the appropriate atoms by which to amplify the matrix. It is now obvious that this is basically the same as the _instantiation problem_, i.e. the problem of choosing lexical instances appropriately in Quine's proof procedure [7], or of choosing resolvents appropriately in the Resolution method [8].

From the abstract point of view the outstanding difference between the Resolution method and the Reduction-Amplification method seems to be that in the Resolution method one looks at small parts of the matrix quite carefully, whereas in the Reduction-Amplification method one scans the whole matrix at once. It is not surprising that each method should have its advantages. What is now needed is a unified proof procedure which incorporates the advantages of both.

BIBLIOGRAPHY

[1] Alonzo Churchy A Formulation of the Simple Theory of Types, Journal of Symbolic Logic, vol. 5 (1940), pp. 56-68.

[2] Alonzo Church, Introduction to Mathematical Logic, vol. I, Princeton University Press, 1956.

[3] Joyce Friedman, A Semi-Decision Procedure for the Functional Calculus, Journal of the Association for Computing^ Machinery, vol. 10 (1963), pp. 1-24.

[4] Joyce Friedman, A Computer Program for a Solvable Case of the Decision Problem, Journal of the Association for Computing Machinery, vol. 10 (1963), pp. 348-356.

[5] Joyce Friedman, A New Decision Procedure in Logic with a. Computer Realization, Ph.D. thesis, Harvard University, 1964.

[6] Leon Henkin, Completeness in The Theory of Types, Journal. of Symbolic Logic, vol. 15 (1950), pp. 81-91.

[7] W. V. Quine, A Proof Procedure for Quantification Theory, Journal of Symbolic Logic, vol. 20 (1955), pp. 141-149.

[8] J. A. Robinson, A Machine-Oriented Logic Based on the Resolution Principle, Journal of the Association for Computing Machinery, vol. 12 (1965), pp. 23-41.

[9] Hao Wang, Logic of Many-Sorted Theories, Journal of Symbolic Logic, vol. 17 (1952), pp. 105-116.

Carnegie Institute of Technology