PROVABILITY IN
ELEMENTARY TYPE THEORY

by

Peter B. Andrews

Report 72-19

September 1972

This research was partially supported by NSF Grant GJ-28457X.

PROVABILITY IN ELEMENTARY TYPE THEORY

by

Peter B. Andrews

Abstract

Results are obtained about special cases of the decision problem for provability in type theory with λ-conversion, minus axioms of extensionality, descriptions, choice, and infinity.

$\vdash \exists x^1 \ldots \exists x^n [A=B]$ iff there is a substitution θ such that $\theta * A = \theta * B$. Hence $\vdash A = B$ iff A conv B. This shows the independence of the axioms of extensionality. If C is quantifier-free, $\vdash \forall x^1 \ldots \forall x^n C$ iff ηC is tautologous. There is no decision procedure for the class of wffs of the form $\exists z [A=B]$, or the class of wffs of the form $\exists z C$ where C is quantifier-free. Hence the only solvable classes of wffs in prenex normal form defined solely by the structure of the prefix are those in which no existential quantifiers occur.

PROVABILITY IN ELEMENTARY TYPE THEORY

by

Peter B. Andrews*

§1 Introduction

In this paper we assume familiarity with, and use the notation of, [1]. The system $\mathfrak{T}$ of [1] is the system of type theory with λ-conversion introduced by Church [5], minus axioms of extensionality, descriptions, choice, and infinity. We shall refer to $\mathfrak{T}$ as <u>elementary type theory</u>, since $\mathfrak{T}$ simply embodies the logic of propositional connectives, quantifiers, and λ-conversion in the context of type theory. In spite of the fact that $\mathfrak{T}$ is analogous to first order logic in certain respects, it is a considerably more complex language, and special cases of the decision problem for provability in $\mathfrak{T}$ seem rather intractable for the most part. We shall use the methods of [1] to obtain information about some very special cases of this decision problem.

We show that a wff of the form $\exists \mathbf{x}^1 \ldots \exists \mathbf{x}^n [\mathbf{A}=\mathbf{B}]$ is a theorem of $\mathfrak{T}$ iff there is a substitution θ such that $\theta\mathbf{A}$ conv $\theta\mathbf{B}$. In particular, $\vdash \mathbf{A} = \mathbf{B}$ iff $\mathbf{A}$ conv $\mathbf{B}$, so we have a solution to the decision problem for wffs of the form $[\mathbf{A}=\mathbf{B}]$. Naturally, the circumstance that only trivial equality

*This research was partially supported by NSF Grant GJ-28457X.

formulas are provable in 3 changes drastically when axioms of extensionality are added to 3, and this fact provides a proof of the independence of the axioms of extensionality. We see that k $3x_D$[A=B] iff there is a wff E_Q such that I- [Ax_Q.A = B]E_O, but the decision problem for the class of
-p — - -p
wffs of the form $3\bar{x}$ [$\bar{A}$=$\bar{B}$] is unsolvable.

1 We solve the decision problem for wffs of the form $Y\bar{x}$ ...$V\bar{x}^n$q, where $\bar{C}$ is quantifier-free, by showing that such a wff is provable in 3 iff rjQ is tautologous. On the other hand, we show the unsolvability of the decision problem for wffs of the form $3\bar{z}$Q, where £ is quantifier-free. Since irrelevant or vacuous quantifiers can always be introduced, this shows that the only solvable classes of wffs of 3 in prenex normal form defined solely by the structure of the prefix are those in which no existential quantifiers occur.

§2 Preliminary Results

We shall often omit type symbols from variables, constants, and wffs once it is clear from the context what the types must be.

To facilitate our discussion of 3, we next present a refutation system B such that any finite set of wffs_o can be refuted in Ji if and only if it can be refuted in 3. (The system ft of [1] is actually stronger than 3, since the negation of the Axiom of Choice can be refuted in ft, but not in 3 (as can be seen from [2]). Of course, any finite set of sentences refutable in R, is refutable in the system 3C obtained by adding the Axiom Schema of Choice to 3>.)

Definition, Let § be any finite set of wffs$_o$ of U. A fi-derivation of E from § is a finite sequence $D^1, \ldots, p^n$ of wffs$_o$ such that p^n is E^ and each p^i is a member of % or is obtained from preceding members of the sequence by one of the following rules of inference;

((Bl) Conversion-I-11. Apply 2.6.1 (Alphabetic change of bound variables) or 2.6.2 (A-contraction) of [1].

(B2) Disjunction rules. Apply 4.2.2.2 of [1].

(B3) Simplification. From M V A V A to infer M V A.

(B4) Negation elimination. From M V ~~ A to infer M V A.

((65) Conjunction elimination. From M V ~[AVBj to infer M V ~ A and M V ~ B.

(R6) Existential instantiation. From M V ^ II$_{o('oa)}$~N A$_{oc}$ to to infer M V ~ A d , where d is any parameter which does not occur in any member of S or any preceding wff of the derivation.

(B7) Universal instantiation. From M V II$_{o(oot)}$~A$_{oa}$ to infer M V A B , where B is any wff .

(S8) Cut. From M V A and N V ^ A_ to infer M V N.

It is understood that M and N^ may be null above, in accordance with 4.1.2 of [1]. The crucial differences between

$\mathfrak{B}$ and the system $\mathfrak{R}$ if [1] are that existential instantiation is more restrictive for $\mathfrak{B}$, and substitution is combined with universal instantiation in $\mathfrak{B}$. In a given derivation, we refer to a parameter $\mathbf{d}_\alpha$ introduced by ($\mathfrak{B}$6) as an <u>existential parameter</u>.

We write $\mathfrak{S} \vdash_{\mathfrak{B}} E$ to indicate that there is a $\mathfrak{B}$-derivation of E from $\mathfrak{S}$, and say that $\mathfrak{S}$ is <u>refutable</u> in $\mathfrak{B}$ iff $\mathfrak{S} \vdash_{\mathfrak{B}} \Box$.

<u>Theorem</u> <u>1</u>. Let $\mathfrak{S}$ be any finite set of wffs$_o$. Then $\mathfrak{S} \vdash_{\mathfrak{B}} \Box$ iff $\mathfrak{S} \vdash_{\mathfrak{T}} \Box$.

Proof: For any finite set $\mathfrak{S}$ of wffs$_o$, we let $\Gamma(\mathfrak{S})$ mean not $\mathfrak{S} \vdash_{\mathfrak{B}} \Box$. It is readily verified that Γ is an abstract consistency property (see 3.1 of [1]). The details are generally similar to those in 5.3.2 of [1], so we remark only that in adapting 5.3.2.4 to the present situation, one may assume that the existential parameters in $\mathbf{C}^1, \ldots, \mathbf{C}^n$ do not occur in $\mathbf{A}$, and the existential parameters in $\mathbf{E}^1, \ldots, \mathbf{E}^m$ do not occur in $\mathbf{B}$ or in $\mathbf{C}^1, \ldots, \mathbf{C}^n$; also, $\eta\mathbf{D}^i$, $\eta\mathbf{A}$, and $\eta\mathbf{E}^i$ may be replaced by $\mathbf{D}^i, \mathbf{A}$, and $\mathbf{E}^i$, respectively. To adapt 5.3.2.7, note that if there is a $\mathfrak{B}$-refutation of $\mathfrak{S} \cup \{\sim \mathbf{A}_{o\alpha}\mathbf{x}_\alpha\}$, where $\mathbf{x}_\alpha$ is a variable which is not free in $\mathbf{A}_{o\alpha}$ or any wff of $\mathfrak{S}$, one can replace all free occurrences of $\mathbf{x}_\alpha$ in the given refutation by occurrences of a new parameter $\mathbf{d}_\alpha$, and thus by ($\mathfrak{B}$6) obtain a $\mathfrak{B}$-refutation of $\mathfrak{S} \cup \{\sim \Pi_{o(o\alpha)}\mathbf{A}_{o\alpha}\}$.

Thus if $\mathfrak{S} \vdash_{\mathfrak{T}} \Box$, then $\mathfrak{S}$ is inconsistent, so by Theorem 3.5 of [1], not $\Gamma(\mathfrak{S})$, i.e., $\mathfrak{S} \vdash_{\mathfrak{B}} \Box$.

Suppose $\mathcal{S} \vdash_{\mathcal{B}} \Box$, and let a particular $\mathcal{B}$-refutation $\underset{\sim}{D}^1,\ldots,\underset{\sim}{D}^n$ of $\mathcal{S}$ be given. Let $\underset{\sim}{M}^i \vee \sim \underset{\sim}{A}^i_{o\alpha_i} \underset{\sim}{d}^i_{\alpha_i}$ (for $1 \leq i \leq k$) be the wffs inferred by ($\mathcal{B}$6) in this refutation, in the order in which they occur. Note that $\underset{\sim}{d}^j$ cannot occur in any wff of $\mathcal{S}$, or in $\underset{\sim}{A}^i$ if $i < j$. Let $\underset{\sim}{E}^i$ be the wff $[\underset{\sim}{A}^i \underset{\sim}{d}^i \supset \Pi_{o(o\alpha_i)} \underset{\sim}{A}^i]$ for $1 \leq i \leq k$. Let $\mathcal{E}^o = \emptyset$ and $\mathcal{E}^i = \{\underset{\sim}{E}^1,\ldots,\underset{\sim}{E}^i\}$ for $1 \leq i \leq k$. Since the rules of inference of $\mathcal{B}$ other than ($\mathcal{B}$6) are all derived rules of inference of $\mathcal{T}$, it is easy to see by induction on j that $\mathcal{S} \cup \mathcal{E}^k \vdash_{\mathcal{T}} \underset{\sim}{D}^j$ for $1 \leq j \leq n$, so $\mathcal{S} \cup \mathcal{E}^k \vdash_{\mathcal{T}} \Box$.

We prove that $\mathcal{S} \cup \mathcal{E}^{k-j} \vdash_{\mathcal{T}} \Box$ for $0 \leq j \leq k$ by induction on j. For the induction step we prove $\mathcal{S} \cup \mathcal{E}^{i-1} \vdash_{\mathcal{T}} \Box$ from

(a) $\mathcal{S} \cup \mathcal{E}^{i-1} \cup \{\underset{\sim}{E}^i\} \vdash_{\mathcal{T}} \Box$ (the inductive hypothesis).

By the deduction theorem ([5],p.62) and propositional calculus we obtain

(b) $\mathcal{S} \cup \mathcal{E}^{i-1} \vdash_{\mathcal{T}} \sim \Pi_{o(o\alpha)} \underset{\sim}{A}^i$ (where α is α_i) and

(c) $\mathcal{S} \cup \mathcal{E}^{i-1} \vdash_{\mathcal{T}} \underset{\sim}{A}^i \underset{\sim}{d}^i$.

Since $\underset{\sim}{d}^i$ does not occur in $\underset{\sim}{A}^i$ or any wff of $\mathcal{S} \cup \mathcal{E}^{i-1}$, we may replace $\underset{\sim}{d}^i$ by a new variable $\underset{\sim}{y}_\alpha$ throughout the proof of (c) to obtain

(d) $\mathcal{S} \cup \mathcal{E}^{i-1} \vdash_{\mathcal{T}} \underset{\sim}{A}^i \underset{\sim}{y}_\alpha$.

(e) $\mathcal{S} \cup \mathcal{E}^{i-1} \vdash_{\mathcal{T}} \Pi_{o(o\alpha)} \underset{\sim}{A}^i$ by Generalization.

(f) $\mathcal{S} \cup \mathcal{E}^{i-1} \vdash_{\mathcal{T}} \Box$ from (b) and (c).

Thus when $j = k$ (or if $k = 0$) we have $\mathcal{S} \vdash_{\mathcal{T}} \Box$, so the proof is complete.

Recall that a wff is in λ-<u>normal form</u> iff it has no wf parts of the form $[[\lambda \underset{\sim}{x}_\alpha \underset{\sim}{B}_\beta] \underset{\sim}{A}_\alpha]$.

<u>Lemma 1</u>. Every wff $\underset{\sim}{C}_\gamma$ in λ-normal form is of the form $[\lambda \underset{\sim}{x}_\beta \underset{\sim}{B}_\alpha]$ (provided that $\gamma = (\alpha\beta)$) or $\underset{\sim}{p}_{\gamma\delta_1\ldots\delta_k} \underset{\sim}{D}^k_{\delta_k} \ldots \underset{\sim}{D}^1_{\delta_1}$, where $\underset{\sim}{p}_{\gamma\delta_1\ldots\delta_k}$ is a variable or constant and $k \geq 0$. (If $k = 0$, $\underset{\sim}{C}_\gamma$ is $\underset{\sim}{p}_\gamma$.)

Proof: If $\underset{\sim}{C}_\gamma$ is not of the form $[\lambda \underset{\sim}{x}_\beta \underset{\sim}{B}_\alpha]$, it must be a variable or constant or of the form $[\underset{\sim}{A}_{\gamma\delta} \underset{\sim}{D}_\gamma]$. $\underset{\sim}{A}_{\gamma\delta}$ cannot have the form $[\lambda \underset{\sim}{x}_\delta \underset{\sim}{B}_\gamma]$, so it is a variable or constant or of the form $[\underset{\sim}{A}^2_{\gamma\delta\delta_2} \underset{\sim}{D}^2_{\delta_2}]$. The same considerations apply to $\underset{\sim}{A}^2_{\gamma\delta\delta_2}$, and by continuing in this way one sees that $\underset{\sim}{C}_\gamma$ must have the indicated form.

A <u>substitution</u> is a particular type of mapping from wffs to wffs which is determined on all wffs by its behavior on variables. (We shall consider only substitutions which map each variable to a wff of the same type.) Given a set $\mathfrak{V}$ of variables, we say that θ is a substitution <u>for</u> the variables in $\mathfrak{V}$ iff θ is a substitution such that $\theta \underset{\sim}{y} = \underset{\sim}{y}$ for each variable $\underset{\sim}{y}$ which is not in $\mathfrak{V}$. If $\underset{\sim}{x}^1, \ldots, \underset{\sim}{x}^n$ are distinct variables and $\underset{\sim}{A}^i$ is a wff of the same type as $\underset{\sim}{x}^i$ for $1 \leq i \leq n$, we denote by $\underset{\sim}{S}^{\underset{\sim}{x}^1 \ldots \underset{\sim}{x}^n}_{\underset{\sim}{A}^1 \ldots \underset{\sim}{A}^n}$ the substitution of $\underset{\sim}{A}^i$ for all free occurrences of $\underset{\sim}{x}^i$ for $1 \leq i \leq n$. As in [4], for each substitution θ and wff $\underset{\sim}{B}$, we let $\theta * \underset{\sim}{B}$ denote $\eta[[\lambda \underset{\sim}{x}^1 \ldots \lambda \underset{\sim}{x}^n \underset{\sim}{B}](\theta \underset{\sim}{x}^1) \ldots (\theta \underset{\sim}{x}^n)]$, where $\underset{\sim}{x}^1, \ldots, \underset{\sim}{x}^n$ are the free variables of $\underset{\sim}{B}$. ($\eta \underset{\sim}{A}$ is a particular λ-normal form of $\underset{\sim}{A}$; see 2.7.5 of [1].) Thus $\theta * \underset{\sim}{B}$ is obtained by making the substitution θ for the free variables of $\underset{\sim}{B}$ (after making any necessary alphabetic changes of bound variables in $\underset{\sim}{B}$), and putting the resulting wff into λ-normal form. When θ is the identity substitution or $\underset{\sim}{B}$ is closed, $\theta^*\underset{\sim}{B} = \eta\underset{\sim}{B}$.

§3 Equality and Universal Formulas

Theorem 2. Let $\underset{\sim}{A}_\alpha$ and $\underset{\sim}{B}_\alpha$ be wffs of $\mathcal{J}$ and $n \geq 0$. Then $\vdash_{\mathcal{J}} \exists \underset{\sim}{x}^1_{\beta_1} \ldots \exists \underset{\sim}{x}^n_{\beta_n} [\underset{\sim}{A}_\alpha = \underset{\sim}{B}_\alpha]$ iff there is a substitution θ for the variables $\underset{\sim}{x}^1_{\beta_1}, \ldots, \underset{\sim}{x}^n_{\beta_n}$ such that $\theta^*\underset{\sim}{A}_\alpha = \theta^*\underset{\sim}{B}_\alpha$.

Proof: We may assume $\underset{\sim}{x}^1, \ldots, \underset{\sim}{x}^n$ are distinct, for otherwise vacuous quantifiers may be deleted.

Suppose there is such a substitution θ. Since some $\underset{\sim}{x}^i$ may occur in some $\theta\underset{\sim}{x}^j$, let $\underset{\sim}{y}^1_{\beta_1}, \ldots, \underset{\sim}{y}^n_{\beta_n}$ be variables distinct from one another, $\underset{\sim}{x}^1, \ldots, \underset{\sim}{x}^n$, and the variables in $\underset{\sim}{A}_\alpha, \underset{\sim}{B}_\alpha$, and $\theta\underset{\sim}{x}^1, \ldots, \theta\underset{\sim}{x}^n$.

(1) $\vdash_{\mathcal{J}} \theta^*\underset{\sim}{A} = \theta^*\underset{\sim}{B}$ equality theorem

(2) $\vdash_{\mathcal{J}} [[\lambda\underset{\sim}{x}^1 \ldots \lambda\underset{\sim}{x}^n\underset{\sim}{A}](\theta\underset{\sim}{x}^1) \ldots (\theta\underset{\sim}{x}^n)] = [[\lambda\underset{\sim}{x}^1 \ldots \lambda\underset{\sim}{x}^n\underset{\sim}{B}](\theta\underset{\sim}{x}^1) \ldots (\theta\underset{\sim}{x}^n)]$ λ-conversion

(3) $\vdash_{\mathcal{J}} \exists\underset{\sim}{y}^1 \ldots \exists\underset{\sim}{y}^n . [[\lambda\underset{\sim}{x}^1 \ldots \lambda\underset{\sim}{x}^n\underset{\sim}{A}]\underset{\sim}{y}^1 \ldots \underset{\sim}{y}^n] = [[\lambda\underset{\sim}{x}^1 \ldots \lambda\underset{\sim}{x}^n\underset{\sim}{B}]\underset{\sim}{y}^1 \ldots \underset{\sim}{y}^n]$ existential generalization

(4) $\vdash_{\mathcal{J}} \exists\underset{\sim}{x}^1 \ldots \exists\underset{\sim}{x}^n . [[\lambda\underset{\sim}{x}^1 \ldots \lambda\underset{\sim}{x}^n\underset{\sim}{A}]\underset{\sim}{x}^1 \ldots \underset{\sim}{x}^n] = [[\lambda\underset{\sim}{x}^1 \ldots \lambda\underset{\sim}{x}^n\underset{\sim}{B}]\underset{\sim}{x}^1 \ldots \underset{\sim}{x}^n]$ alphabetic change of bound variable

(5) $\vdash_{\mathcal{J}} \exists\underset{\sim}{x}^1 \ldots \exists\underset{\sim}{x}^n . \underset{\sim}{A} = \underset{\sim}{B}$ λ-conversion

In the proof of the converse implication, we shall assume that $n = 2$ for the sake of notational simplicity; it will be obvious how to adapt the proof to other values of n.

Suppose that $\vdash_{\mathfrak{J}} \exists x_\beta \exists y_\gamma [A_\alpha = B_\alpha]$. Hence

$$\forall x_\beta \forall y_\gamma \sim [[\lambda x_\beta \lambda y_\gamma A_\alpha] x_\beta y_\gamma = [\lambda x_\beta \lambda y_\gamma B_\alpha] x_\beta y_\gamma] \vdash_{\mathfrak{J}} \Box$$

so by Theorem 1 and the definitions of $\forall$ and $=$ there is a $\mathfrak{B}$-refutation of

(6) $\Pi_{o(o\beta)} \cdot \lambda x_\beta \cdot \Pi_{o(o\gamma)} \cdot \lambda y_\gamma \cdot \sim \Pi_{o(o(o\alpha))} \cdot \lambda f_{o\alpha} \cdot \sim f_{o\alpha} [[\lambda x_\beta \lambda y_\gamma A_\alpha] x_\beta y_\gamma]$

$\vee f_{o\alpha} [[\lambda x_\beta \lambda y_\gamma B_\alpha] x_\beta y_\gamma]$,

where $f_{o\alpha}$ is distinct from x_β, y_γ, and the free variables of A_α and B_α.

By appropriate alphabetic changes of bound variables, we may assume that y_γ and $f_{o\alpha}$ are not free in the wffs C_β and D_γ introduced below. We assert that in any $\mathfrak{B}$-refutation of (6), each line must be obtainable by ($\mathfrak{B}$1) from some line of the following refutation (for appropriate choices of C_β, D_γ, and $d_{o\alpha}$):

(7)	$[\lambda x . \Pi . \lambda y . \sim \Pi . \lambda f . \sim f[[\lambda x \lambda y A] xy] \vee f[[\lambda x \lambda y B] xy]] C_\beta$ for some wff C_β	$\mathfrak{B}$7: 6
(8)	$\Pi . \lambda y . \sim \Pi . \lambda f . \sim f[[\lambda x \lambda y A] Cy] \vee f[[\lambda x \lambda y B] Cy]$	$\mathfrak{B}$1: 7
(9)	$[\lambda y . \sim \Pi . \lambda f . \sim f[[\lambda x \lambda y A] Cy] \vee f[[\lambda x \lambda y B] Cy]] D_\gamma$	$\mathfrak{B}$7: 8
(10)	$\sim \Pi . \lambda f . \sim f[[\lambda x \lambda y A] CD] \vee f[[\lambda x \lambda y B] CD]$	$\mathfrak{B}$1: 9
(11)	$\sim [\lambda f . \sim f[[\lambda x \lambda y A] CD] \vee f[[\lambda x \lambda y B] CD]] d_{o\alpha}$ for some parameter $d_{o\alpha}$ which does not occur in A, B, C, or D.	$\mathfrak{B}$6: 10
(12)	$\sim . \sim d[[\lambda x \lambda y A] CD] \vee d[[\lambda x \lambda y B] CD]$	$\mathfrak{B}$1: 11

(13) $\sim \underset{\sim}{d}[[\lambda \underset{\sim}{x} \lambda \underset{\sim}{y} \underset{\sim}{B}] \underset{\sim}{C} \underset{\sim}{D}]$ $\qquad$ $\mathfrak{B}5$: 12

(14) $\sim \sim \underset{\sim}{d}[[\lambda \underset{\sim}{x} \lambda \underset{\sim}{y} \underset{\sim}{A}] \underset{\sim}{C} \underset{\sim}{D}]$ $\qquad$ $\mathfrak{B}5$: 12

(15) $\underset{\sim}{d}[[\lambda \underset{\sim}{x} \lambda \underset{\sim}{y} \underset{\sim}{A}] \underset{\sim}{C} \underset{\sim}{D}]$ $\qquad$ $\mathfrak{B}4$: 14

(16) $\square$ $\qquad$ $\mathfrak{B}1, \mathfrak{B}8$: 13,15 (or 14)

To verify the assertion above, note that if $\underset{\sim}{G}$ is any of lines (6)-(16), and $\underset{\sim}{J}$ is obtained from $\underset{\sim}{G}$ by ($\mathfrak{B}1$), and $\underset{\sim}{K}$ is obtained from $\underset{\sim}{J}$ by any rule of $\mathfrak{B}$, then $\underset{\sim}{K}$ is obtainable by ($\mathfrak{B}1$) from some wff $\underset{\sim}{H}$ which is one of lines (6)-(16) and is obtained from $\underset{\sim}{G}$ by a rule of $\mathfrak{B}$.

It is clear that in order to derive $\square$, there must be wffs $\underset{\sim}{C}_\beta$ and $\underset{\sim}{D}_\gamma$ such that $\square$ is derivable by ($\mathfrak{B}1$) and ($\mathfrak{B}8$) from (13) and (15), so one must have $\eta[[\lambda \underset{\sim}{x} \lambda \underset{\sim}{y} \underset{\sim}{A}] \underset{\sim}{C} \underset{\sim}{D}] = \eta[[\lambda \underset{\sim}{x} \lambda \underset{\sim}{y} \underset{\sim}{B}] \underset{\sim}{C} \underset{\sim}{D}]$. Thus, when $\theta = \mathrm{S}^{\underset{\sim}{x}\ \underset{\sim}{y}}_{\cdot \underset{\sim}{C}\ \underset{\sim}{D}}$, we have $\theta^* \underset{\sim}{A} = \theta^* \underset{\sim}{B}$.

<u>Corollary 1</u>. $\vdash_{\mathfrak{T}} \underset{\sim}{A}_\alpha = \underset{\sim}{B}_\alpha$ iff $\underset{\sim}{A}_\alpha$ conv $\underset{\sim}{B}_\alpha$.

Proof: When the proof of Theorem 2 is specialized to the case $n = 0$, one obtains $\vdash \underset{\sim}{A} = \underset{\sim}{B}$ iff $\eta \underset{\sim}{A} = \eta \underset{\sim}{B}$, which means $\underset{\sim}{A}$ conv $\underset{\sim}{B}$.

Since it can be effectively decided whether or not $\underset{\sim}{A}_\alpha$ conv $\underset{\sim}{B}_\alpha$ simply by comparing $\eta \underset{\sim}{A}_\alpha$ with $\eta \underset{\sim}{B}_\alpha$, we have a decision procedure for the provability of equality formulas in $\mathfrak{T}$.

Note that the wff $f_{\alpha\beta} = [\lambda x_\beta . f_{\alpha\beta} x_\beta]$ is not a theorem of $\mathfrak{T}$, though it is readily derived from the Axiom of Extensionality (6.1.1 of [1]). Hence we have a proof of the independence of the Axiom of Extensionality quite different from that in [3].

It is not generally true that if $\vdash \exists x_{\alpha} C_{o}$, then there is a wff E_{o} such that hr[AxDC]j;Q, even if C is quantifier-free. For with the aid of Theorems 1 and 3 (below) it is easy to see that \-^ 3x [dQ x => . da A dQ b] (where a, b, and d are parameters), but there is no wff E such that k.[Ax .d x z>.d a A d b]E . (Note that this is essentially an example from first order logic.) Nevertheless, such a situation does occur whenever C is an equality formula, as we next note.

Corollary 2. $\vdash \exists x_{\beta}[A_{\alpha} = B_{\alpha}]$ iff there is a wff E_{β} such that $\vdash [\lambda x_{\beta} . A_{\alpha} = B_{\alpha}] = E_{\beta}$.

Proof: If $\vdash [\lambda x . A = B] E$, then $\vdash \exists x . [\lambda x . A = B] x$ by existential generalization, so f- 3x[^=Sl 1°Y A-conversion. If |- 3x[A=g], then by Theorem 2 there is a substitution 9 for x such that 8*& = 9^B. Let Eg = 6x so rj [[AxA] E] = T) [[AxB] E], so f-vj[AxA]E = [AxB]E. Hence |-^ [Ax. [A^A]x = [AJJ5]X]E and [-«[Ax.A = J3]E by \-conversion.

A wff of the form A = B is (by virtue of the definition of =) of the form Yj£ Q, where Q has no accessible quantifiers (though quantifiers might be buried in & or B) . We next note that this solvable case of the decision problem can be generalized in a rather obvious way.

We say that a wff$_{o}$ Q of IT is <u>tautologous</u> iff there is a tautology P of the propositional calculus in which the sole connectives are negation and disjunction, such that Q is (the wff abbreviated by) $S^{\mathbf{x}^1 \ldots \mathbf{x}^n}_{\mathbf{B}^1 \ldots \mathbf{B}^n} \mathbf{C}$, where $\mathbf{x}^1, \ldots, \mathbf{x}^n$ are the propositional variables of $\mathbf{C}$ and $\mathbf{B}^1, \ldots, \mathbf{B}^n$ are wffs$_o$ of 3. (The result of the indicated substitution is only an abbreviation for a wff of 3, since in 3 $[\mathbf{A} \vee \mathbf{B}]$ is an abbreviation for $[[\vee \mathbf{A}]\mathbf{B}]$.)

A wff $\mathbf{C}$ of 3 is quantifier-free iff none of the constants $\Pi_{o(oa)}$ occur in $\mathbf{C}$.

Theorem 3. Let $\mathbf{C}$ be a quantifier-free wff$_o$ of 3, and $n \geq 0$. Then $\vdash_3 \forall \mathbf{x}^1 \ldots \forall \mathbf{x}^n \mathbf{C}$ iff $\mathbf{C}$ is tautologous.

Proof: If $\mathbf{C}$ is tautologous, then $\vdash_3 \mathbf{C}$ (see [5]) so $\vdash_3 \mathbf{C}$ by λ-conversion, and $\vdash_3 \forall \mathbf{x}^1 \ldots \forall \mathbf{x}^n \mathbf{C}$ by generalization.

Next suppose $\vdash_3 \forall \mathbf{x}^1 \ldots \forall \mathbf{x}^n \mathbf{C}$. Then $\vdash_3 \mathbf{C}$ so $\vdash \mathbf{C}$ so $\sim \mathbf{C} \vdash \square$ by Theorem 1. Let $\mathbf{D}^1, \ldots, \mathbf{D}^k$ be a $\mathcal{B}$-refutation of $\sim \mathbf{C}$. Since $\sim \mathbf{C}$ is quantifier-free, rules (B6) and (B7) cannot be used in this refutation, so it is clear that $\eta \mathbf{D}^1, \ldots, \eta \mathbf{D}^k$ is a R-refutation of $\sim \eta \mathbf{C}$ in which only rules (R2)-(R5) and (B8) are used. (Of course, $\eta \mathbf{D}^j = \eta \mathbf{D}^i$ if $\mathbf{D}^j$ was obtained from $\mathbf{D}^i$ by (B1).) These are essentially rules of propositional calculus, so if we regard $\eta \square$ as a propositional constant denoting falsehood, it is easy to establish by induction on j that $[\sim \eta \mathbf{C} \supset \eta \mathbf{D}^j]$ is tautologous for $1 \leq j \leq k$. Since $\mathbf{D}^k$ is $\square$, $\eta \mathbf{C}$ is tautologous.

§4 Undecidability of the 3gQ Case

Huet [6] and Lucchesi [7] have independently shown that there is no decision procedure for determining, of two arbitrary wffs A_α and B_α, whether there is a substitution 6 such that 9*A_α = 0*B_α. Thus the decision problem for the entire class of wffs dealt with in Theorem 2 is unsolvable, though we have a decision procedure for the subclass obtained by setting n = 0. By appropriately modifying Huet's ideas in [6], we obtain the following results:

Theorem £. There are no decision procedures for provability in U for the classes of wffs of the following forms:

(I) SZ_K[A_a = B_a].

(II) ^3i<;£> where C is quantifier-free.

Proof: We let £ = (a , b }, the alphabet whose letters are the parameters a and b of 3'. A word over £ is a finite sequence of letters from £. An instance of the Post Correspondence Problem over £ is determined by an integer $n \geq 1$ and two sequences $X_1, \ldots, X_n$ and $Y_1, \ldots, Y_n$ of length n of words over L. A finite sequence $i_1, \ldots, i_m$ of integers such that $m \geq 1$ and $1 \leq i_j \leq n$ for $1 \leq j \leq m$ is a solution to this instance of the Post Correspondence Problem iff $X_{i_1} \ldots X_{i_m} = Y_{i_1} \ldots Y_{i_m}$. It is known (see [8]) that the problem of determining whether an arbitrary instance of the Post Correspondence Problem has a solution is unsolvable.

Let $\wp$ be an arbitrary instance of the Post Correspondence Problem, determined by sequences $X^1,\ldots,X^n$ and $Y^1,\ldots,Y^n$ of words over Σ. Let κ be the type symbol $((\iota\iota)(\iota\iota)\ldots(\iota\iota))$, in which $(\iota\iota)$ occurs $n+1$ times. We shall subsequently use the variables t_ι, $u^1_{\iota\iota},\ldots,u^n_{\iota\iota}$, and z_κ, and the parameters $a_{\iota\iota}, b_{\iota\iota}, c_\iota, d_{o\iota(\iota\iota)(\iota\iota)\kappa}$, and $e_{\alpha\iota(\iota\iota)(\iota\iota)}$ of $\mathfrak{T}$, which we henceforth write without type symbols. For any word W over Σ, say $W = w^1\ldots w^k$ (where $w^j \in \Sigma$ for $1 \leq j \leq k$), let $\tilde{W}_{\iota\iota}$ be $[\lambda t[w^1[\ldots[w^k t]\ldots]]]$, which is a wff$_{\iota\iota}$ of $\mathfrak{T}$.

Let $A_{\iota\iota\kappa}$ be $[\lambda z.z[\lambda tt]\ldots[\lambda tt]]$, let $B_{\iota\iota\kappa}$ be $[\lambda z.z[\lambda tc]\ldots[\lambda tc]]$, let $X_{\iota\kappa}$ be $[\lambda z.z\tilde{X}^1\ldots\tilde{X}^n c]$, and let $Y_{\iota\kappa}$ be $[\lambda z.z\tilde{Y}^1\ldots\tilde{Y}^n c]$. We shall show that the following conditions are equivalent:

(i) $\vdash_{\mathfrak{T}} \exists z.e[Az][Bz][Xz] = e[\lambda tt][\lambda tc][Yz]$

(ii) $\vdash_{\mathfrak{T}} \exists z.\sim dz[Az][Bz][Xz] \vee dz[\lambda tt][\lambda tc][Yz]$

(iii) There is a wff $\mathbf{Z}_\kappa$ such that (a) $A\mathbf{Z}$ conv $[\lambda tt]$, (b) $B\mathbf{Z}$ conv $[\lambda tc]$, and (c) $X\mathbf{Z}$ conv $Y\mathbf{Z}$.

(iv) $\wp$ has a solution.

This will prove our theorem, since a decision procedure for all wffs of the form $\exists \mathbf{z}_\kappa[\mathbf{A}_\alpha = \mathbf{B}_\alpha]$, or for all wffs of the form $\exists \mathbf{z}_\kappa \mathbf{C}$, where $\mathbf{C}$ is quantifier-free, would provide a decision procedure for the Post Correspondence Problem.

If (iii) holds, then

$\vdash_{\mathfrak{T}} e[A\mathbf{Z}][B\mathbf{Z}][X\mathbf{Z}] = e[\lambda tt][\lambda tc][Y\mathbf{Z}]$ and

$\vdash_{\mathfrak{T}} \sim d\mathbf{Z}[A\mathbf{Z}][B\mathbf{Z}][X\mathbf{Z}] \vee d\mathbf{Z}[\lambda tt][\lambda tc][Y\mathbf{Z}]$, so (i) and (ii) follow by existential generalization.

If (i) holds, then by Theorem 2 there is a substitution 6 for z such that 9*e [Az] [Bz] [Xz] = 8*e [Att] [Ate] [Yz] . Let Z_K be 9z, and (iii) quickly follows.

Next we show that (ii) implies (iii). If (ii) holds, then there is a refutation in 3_3 and hence in ft, of

(1) n , „* [Az.~.~ dz[Az] [Bz] [Xz] V dz [Att] [Ate] [Yz]] .
o (oft)

As in the proof of Theorem 2, it is clear that in any ft-refutation of (1) each line must be obtainable by (ftl) from some line of the following refutation (for some choice of g^) :

(2)	[Az.-.- dz[Az] [Bz] [Xz] V dz [Att] [Ate] [Yz]]Z_K		
	for some wff Z_K	ft7:	1
(3)	~. ~ dZ[AZ] [BZ] [XZ] V dZ[Att] [Ate] [Y£]	ftl:	2
(4)	- dZ[Att] [Ate] [YZ]	«5:	3
(5)	— dZ[AZ] [BZ] [XZ]	ft5:	3
(6)	dZjAZ] [BZ] [XZ]	B4:	5
(7)	•	B1,B8:	4,6 (or 5)

Thus it is clear that (7) must be obtainable from (4) and (6) by (<B1) and (R8) , so the same wff Z (up to equivalence by A-conversion) must occur in (4) and in (6), and rj(4) must be — 17(6) . Hence (iii) must hold.

Thus (i),(ii), and (iii) are equivalent. We complete the proof by showing that (iii) and (iv) are equivalent. Suppose $i_1,\ldots,i_m$ is a solution to P (so m ^ 1). Let Z_K be $[Au^1...Au^nAt.u^{i}_{1}[\ldots[u^{i}_{m}t]\ldots]]$. Clearly AZconv [Att] and BZ conv $[\lambda tc]$. Also, since $X^{i_1}\dots X^{i_m} = Y^{i_1}\dots Y^{i_m}$, XZ conv $[\tilde{X}^{i_1}[\dots[\tilde{X}^{i_m}c]\dots]]$ conv $[\tilde{Y}^{i_1}[\dots[\tilde{Y}^{i_m}c]\dots]]$ conv YZ, so (iii) holds.

Next suppose (iii) holds; we shall prove (iv). We may assume that $\mathbf{Z}_\kappa$ has the form $[\lambda\mathbf{u}^1_{\iota\iota}\dots\lambda\mathbf{u}^n_{\iota\iota}\mathbf{G}_{\iota\iota}]$, where $\mathbf{G}_{\iota\iota}$ is in λ-normal form and the $\mathbf{u}^i_{\iota\iota}$ are distinct. For if not, let $\mathbf{Z}'_\kappa$ be $[\lambda\mathbf{u}^1_{\iota\iota}\dots\lambda\mathbf{u}^n_{\iota\iota}\cdot\eta[\mathbf{Z}\mathbf{u}^1_{\iota\iota}\dots\mathbf{u}^n_{\iota\iota}]]$, where $\mathbf{u}^1_{\iota\iota},\dots,\mathbf{u}^n_{\iota\iota}$ are distinct variables which do not occur free in $\mathbf{Z}$. Then $\mathbf{Z}'_\kappa$ also satisfies (a), (b), and (c).

Now $\mathbf{G}_{\iota\iota}$ must satisfy Lemma 1.

Case 1. $\mathbf{G}_{\iota\iota}$ has the form $\mathbf{p}_{\iota\iota\delta_1\dots\delta_k}\mathbf{D}^k_{\delta_k}\dots\mathbf{D}^1_{\delta_1}$, where $k \geq 0$ and $\mathbf{p}$ is a constant or variable.
If $\mathbf{p}$ is distinct from each of the $\mathbf{u}^i_{\iota\iota}$, then (a) is contradicted. Hence there exists i $(1 \leq i \leq n)$ such that $\mathbf{p}$ is $\mathbf{u}^i_{\iota\iota}$, so $k = 0$ and $\mathbf{Z}_\kappa$ is $[\lambda\mathbf{u}^1_{\iota\iota}\dots\lambda\mathbf{u}^n_{\iota\iota}\mathbf{u}^i_{\iota\iota}]$. Thus by (c), $\tilde{X}^i c$ conv $\mathbf{Z}\tilde{X}^1\dots\tilde{X}^n c$ conv $X\mathbf{Z}$ conv $Y\mathbf{Z}$ conv $\mathbf{Z}\tilde{Y}^1\dots\tilde{Y}^n c$ conv $\tilde{Y}^i c$, so $\eta\tilde{X}^i c = \eta\tilde{Y}^i c$, so $X^i = Y^i$ and i is a (rather trivial) solution to $\mathcal{P}$.

Case 2. $\mathbf{G}_{\iota\iota}$ has the form $[\lambda\mathbf{t}_\iota\mathbf{H}_\iota]$.
Since $\mathbf{G}_{\iota\iota}$ is in λ-normal form, $\mathbf{H}_\iota$ must be also, and so by Lemma 1 has the form $\mathbf{p}_{\iota\delta_1\dots\delta_k}\mathbf{D}^k_{\delta_k}\dots\mathbf{D}^1_{\delta_1}$, where $k \geq 0$ and $\mathbf{p}$ is a variable or constant. Thus $\mathbf{Z}$ has the form $[\lambda\mathbf{u}^1_{\iota\iota}\dots\lambda\mathbf{u}^n_{\iota\iota}\lambda\mathbf{t}_\iota\cdot\mathbf{p}_{\iota\delta_1\dots\delta_k}\mathbf{D}^k_{\delta_k}\dots\mathbf{D}^1_{\delta_1}]$.

If $\underset{\sim}{p}$ is $\underset{\sim}{t}_\iota$ (so $k = 0$), (b) is contradicted. If $\underset{\sim}{p}$ is distinct from $\underset{\sim}{t}_\iota$ and each of the $\underset{\sim}{u}^i_{\iota\iota}$, (a) is contradicted. Hence $\underset{\sim}{p}$ must be some $\underset{\sim}{u}^i_{\iota\iota}$ (so $k = 1$). Thus for some $m \geq 1$, $\underset{\sim}{Z}$ has the form $[\lambda\underset{\sim}{u}^1_{\iota\iota}\ldots\lambda\underset{\sim}{u}^n_{\iota\iota}\lambda\underset{\sim}{t}_\iota.\underset{\sim}{u}^{i_1}_{\iota\iota}[\ldots[\underset{\sim}{u}^{i_m}_{\iota\iota}\underset{\sim}{K}_\iota]\ldots]]$, where $\underset{\sim}{K}_\iota$ is in λ-normal form, and by choosing m large enough it may be assured that $\underset{\sim}{K}_\iota$ does not have the form $\underset{\sim}{u}^j_{\iota\iota}M_\iota$.

Thus by Lemma 1, $\underset{\sim}{K}_\iota$ must have the form $\underset{\sim}{q}_{\iota\delta_k\ldots\delta_1}\underset{\sim}{D}^1_{\delta_1}\ldots\underset{\sim}{D}^k_{\delta_k}$, where $k \geq 0$ and $\underset{\sim}{q}$ is a constant or variable distinct from each of the $\underset{\sim}{u}^j_{\iota\iota}$. If $\underset{\sim}{q}$ is not $\underset{\sim}{t}_\iota$, (a) is contradicted, so $\underset{\sim}{q}$ is $\underset{\sim}{t}_\iota$ and $k = 0$ and $\underset{\sim}{Z}$ is $[\lambda\underset{\sim}{u}^1_{\iota\iota}\ldots\lambda\underset{\sim}{u}^n_{\iota\iota}\lambda\underset{\sim}{t}.\underset{\sim}{u}^{i_1}_{\iota\iota}[\ldots[\underset{\sim}{u}^{i_m}_{\iota\iota}\underset{\sim}{t}_\iota]\ldots]]$. Thus by (c), $\eta[\tilde{X}^{i_1}\ldots[\tilde{X}^{i_m}c]\ldots] = \eta[X\underset{\sim}{Z}] = \eta[Y\underset{\sim}{Z}] = \eta[Y^{i_1}\ldots[Y^{i_m}c]\ldots]$, so $X^{i_1}\ldots X^{i_m} = Y^{i_1}\ldots Y^{i_m}$ and $i_1,\ldots,i_m$ is a solution to $\wp$.

This completes the proof.

Bibliography

[1] Peter B. Andrews, "Resolution in Type Theory", Journal of Symbolic Logic, vol. 36(1971), 414-432.

[2] ________________, "General Models, Descriptions, and Choice in Type Theory", Journal of Symbolic Logic (to appear).

[3] ________________, "General Models and Extensionality", Journal of Symbolic Logic (to appear).

[4] ________________, "Resolution and the Consistency of Analysis", Notre Dame Journal of Formal Logic (to appear).

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

[6] Gerard P. Huet, "The Undecidability of the Existence of a Unifying Substitution Between Two Terms in the Simple Theory of Types", Information and Control (to appear).

[7] Claudio L. Lucchesi, "The Undecidability of the Unification Problem for 3rd Order Languages", University of Waterloo report CSRR-2059, February, 1972.

[8] Emil L. Post, "A Variant of a Recursively Unsolvable Problem", Bulletin of the American Mathematical Society, vol. 52(1946), 264-268.

Department of Mathematics
Carnegie-Mellon University
Pittsburgh, Pennsylvania 15213

/ps -- 9/7/72