THE TYPED λ-CALCULUS IS NOT ELEMENTARY RECURSIVE

Richard Statman
Department of Philosophy
The University of Michigan
Ann Arbor, Mi. 48109

I. Historically, the principal interest in the typed λ-calculus is in connection with Gödel's functional ("Dialectica") interpretation of intuitionistic arithmetic. However, since the early sixties interest has shifted to a wide variety of applications in diverse branches of logic, algebra, and computer science. For example, in proof-theory (see for example, Prawitz), in constructive logic (see for example, Lauchli), in the theory of functionals (see for example, Friedman), in cartesian closed categories (see for example, Mann), in automatic theorem proving (see for example, Huet), and in the semantics of natural languages (see for example, Montague).

In almost all such applications there is a point at which one must ask, for closed terms t_1 and t_2, whether t_1 β-converts to t_2.[1] We shall show that in general this question cannot be answered by a Turing machine in elementary time (for a more precise statement of our principal result see the theorem stated below).[2]

We shall also investigate the computational complexity of related questions concerning the typed λ-calculus (for example, the question of whether a given type contains a closed term).[3]

II. The language of type theory, Ω, is the language of set-theory where each variable has a natural number type and there are two constants $\underline{0}$, $\underline{1}$ of type **0**. We require that prime formulae be "stratified", i.e. each prime formula has one of the forms $\underline{0} \in \mathbf{X}^1$, $\underline{1} \in \mathbf{X}^1$, and $y^n \in \mathbf{Z}^{n+1}$. Arbitrary formulae are built-up from prime ones by ¬, ∧, and ∀. The intended interpretation of Ω has $\underline{0}$ denoting 0, $\underline{1}$ denoting 1 and X^n ranging over $\mathcal{D}_n$ where $\mathcal{D}_0 = \{0,1\}$ and $\mathcal{D}_{n+1}$ = powerset $(\mathcal{D}_n)$. If $A = A(x_1^{n_1},\ldots,x_m^{n_m})$ and $\alpha_i \in \mathcal{D}_{n_i}$ we write $A[\alpha_1,\ldots,\alpha_m]$ for A with $x_i^{n_i}$ denoting α_i.[4]

Proposition (Fischer and Meyer, Statman): The problem of determining if an arbitrary Ω-sentence is true cannot be solved in elementary time.

Corollary: Let L be the language of set-theory supplemented by a constant for each V_n (nεω), then the problem of determining if an arbitrary Δ_0-sentence of L is true cannot be solved in elementary-time.

We shall use the above proposition together with a coding argument to prove the following theorem.

Theorem: For each type $\sigma \neq 0 \to 0$ of the typed λ-calculus Λ containing some closed term there is a closed term t^σ such that the problem of determining for arbitrary closed terms t' of type σ whether t' β-conv. t^σ (t' β-red. t^σ, t^σ is the β-normal form of t') cannot be solved in elementary time ($0 \to 0$ is anomolous because it contains only one β-normal closed term). (Moreover if $\sigma = (0\to0) \to (0\to0)$[5] and Λ^+ is any consistent extension of Λ + β-conversion then the problem of determining for arbitrary closed terms t' of type σ whether $\Lambda^+ \vdash t' = t^\sigma$ cannot be solved in elementary time.)

III.1 We consider the typed λ-calculus Λ with a single ground type 0, no constants, only power types (→) and β-conversion. The reader not familiar with the typed λ-calculus should consult Hindley, Lercher and Seldin.

We shall adopt the usual convention of ignoring α-conversion, deleting type superscripts except where important and omitting parentheses selectively (association to the left). We shall also make use of the substitution prefix [/] both for substituting a term for a variable and for substituting a type for 0.

$O =_{df} (0\to0) \to (0\to0)$ is the type of Λ-numbers. It is easy to verify that the closed β-normal terms of type 0 are just λxx and for each n $\lambda xy\ \underbrace{x(\ldots(x}_{n}y)\ldots)$.

Setting $\underline{n} =_{df} \lambda xy\ \underbrace{x(\ldots(x}_{n}y)\ldots)$, if t is a closed term of type $\underbrace{0\to(\ldots(0}_{m}\to 0)\ldots)$ for each $n_1,\ldots,n_m$ there is a unique n such $t\ \underline{n_1},\ldots,\underline{n_m}$ β-η-conv. $\underline{n}$. In this way t defines an m-ary number-theoretic function.

An extended polynomial is a polynomial built-up from variables, 0, 1, +, ·, sg and $\overline{sg}$.

Proposition (Schwichtenberg, Statman): The λ-definable m-ary number-theoretic functions are just the extended polynomials of m variables.

In particular, there are closed terms $\underline{+}$, $\underline{\cdot}$, $\underline{sg}$ and $\underline{\overline{sg}}$ which λ-define resp. +, ·, sg, and $\overline{sg}$.

There are some very short definitions of very large numbers in Λ. Let $2_1 = 2$ and $2_{n+1} = 2^{(2_n)}$ and set $a_1 = \underline{2}$, and $a_{n+1} = ([^{0\to0}/0]a_n)a_1$; by an old computation of Church a_n β=conv. $\underline{2_n}$.[6]

We define recursively $N + 1 = N \to 0$. The following definitions are central to what follows:

$e_0 =_{df} \lambda xy\ (\underline{+}(\underline{\cdot}(\underline{sg}x)(\underline{\overline{sg}}y))(\underline{\cdot}(\underline{\overline{sg}}x)(\underline{sg}y)))$

$V_0 =_{df} \lambda h\ (\underline{+}(h\underline{0})(h\underline{1}))$

$C =_{df} \lambda g\ (\underline{+}(g(\lambda x\underline{1}))(g(\lambda xx)))$

$p_{n+1}(x,z) =_{df} C\ (\lambda f(V_n(\lambda w(z(\lambda y\ \underline{\cdot}\ (f(e_n^{(xy)}wy)))))))$

$e_{n+1} =_{df} \lambda xy\ (V_n(\lambda z(e_0(xz)(yz))))$

$V_{n+1} =_{df} \lambda y\ ((([^{N+2}/0]a_{n+1})(\lambda zx\ p_{n+1}(x,z))y)\lambda w\underline{1})$.

They will be used to construct (in elementary time) for each Ω-sentence A a closed term A* of type 0 such that $A \iff A^*$ β-conv. $\underline{0}$ and $\neg A \iff A^*$ β-conv. $\underline{1}$. A* will be constructed in such a way that the quantifier elimination for Ω-sentences applied to A can be simulated by β-conversion applied to A*.

III.2 We define the notion of a definition of an object of type n as follows:

(a) $def^0(0) = \{\underline{0}\}$

(b) $def^0(1) = \{\underline{1}\}$

(c) if $\alpha \in \mathcal{D}_{n+1}$ then $def^{n+1}(\alpha) = \{\lambda y \cdot r_1(\ldots(\cdot r_{2_{n+1}} \underline{1})\ldots) : r_i = \underline{1}$ or $r_i = e_n t y$ for $t \in def^n(\beta)$ and $\beta \in \alpha$, for each $\beta \in \alpha$ for some $t \in def^n(\beta)$ there is some i s.t. $r_i = e_n t y\}$.

We set $def_n = \bigcup_{\alpha \in \mathcal{D}_n} def^n(\alpha)$. The notion of a notation for a definition is defined by

(a) $N_0 = \{0,1\}$, $0^\# = \underline{0}$, and $1^\# = \underline{1}$

(b) $N_{n+1} = [1, 2_{n+1}](N_n \times N_0)$, and for $\eta \in N_{n+1}$ $\eta^\# = \lambda y \cdot r_1(\ldots(\cdot r_{2_{n+1}} \underline{1})\ldots)$

where $r_i = \underline{1}$ if $\pi_2\eta(i) = 0$ and $r_i = e_n(\pi_1\eta(i))^\# y$ if $\pi_2\eta(i) = 1$.

N_n is ordered according to the following rules:
(a) sets of numbers have their natural order,
(b) products have the reverse product order, and
(c) powers have the reverse lexicographic order.

Suppose T is a set of occurrences of terms of type σ ordered by the relation ρ, $|T|$ is a power of 2, $T = T_1 \cup T_2$ is the partition of T with $|T_1| = |T_2|$ and $t_1 \in T_1$ & $t_2 \in T_2 \to t_1 \rho t_2$, and z is a variable of type $\sigma \to 0$; we define the term $\sum_{t \in T} zt$ recursively by

$$\sum_{t \in T} zt = \underline{+}(\sum_{t \in T_1} zt)(\sum_{t \in T_2} zt).$$

We shall prove the following.

Proposition: $\forall_n$ β-conv. $\lambda y \sum_{\eta \in N_n} y(\eta^\#)$

We define PN_n^m for $1 \le m \le 2_n$ as follows:

(a) $PN_0^1 = N_0$

(b) $PN_{n+1}^m \overset{[1,m]}{=} (N_n \times N_0)$ and for $\eta \in PN_n^m$ $\eta^\# = \lambda y \cdot r_1(\ldots(\cdot r_m(xy))\ldots)$

where $r_i = \underline{1}$ if $\pi_2\eta(i) = 0$ and $r_i = e_n(\pi_1\eta(i))^\# y$ if $\pi_2\eta(i) = 1$.

PN_n^m is ordered as above.

Fact: $\sum_{\eta \in PN_{n+1}^1} (\sum_{\xi \in PN_{n+1}^k} z[\eta^\#/x]\xi^\#)$ β-conv. $\sum_{\eta \in PN_{n+1}^{k+1}} z\eta^\#$

Lemma: for $1 \le m \le 2_{n+1}$ $([N+2/0]\underline{m})\lambda zx\, p_{n+1}(x,z)$ β-conv. $\lambda zx \sum_{\eta \in PN_{n+1}^m} z\eta^\#$

Proof: By induction on (m,n) ordered as above.

Basis: n = 0. Case: m = 1.

$([2/0]\underline{1})\ \lambda zx\, p_{n+1}(x,z)$ β-conv. $\lambda zx\, p_1(x,z)$ β-conv.

$\lambda zx\ C\ \lambda f(\underline{+}(z(\lambda y \cdot \underline{+} f(e_0 0 y)(xy)))(z(\lambda y \cdot f(e_0 1 y)(xy))))$

β-conv. $\lambda zx \cdot \underline{+}\ (\underline{+}(z(\lambda y \cdot \underline{1}(xy)))(z(\lambda y \cdot \underline{1}(xy))))$

$(\underline{+}(z(\lambda y \cdot (p_0 \underline{0} y)(xy)))(z(\lambda y \cdot (e_0 \underline{1} y)(xy)))) =$

$\lambda zx \sum_{\eta \in PN_1^1} z$. Case: m = 2. $([2/0]\underline{2})\lambda zx p_1(x,z)$

β-conv. $\lambda w\ \lambda zx p_1(x,z)(\lambda zx p_1(x,z)w)$ β-conv.

$\lambda wx \sum_{\eta \in PN_1^1} (\lambda y p_1(y,w))\eta^\#$ β-conv. $\lambda zx \sum_{\eta \in PN_1^1} \sum_{\xi \in PN_1^1} z[\eta^\#/x]\xi^\#$

β-conv. $\lambda zx \sum_{\eta \in PN_1^2} z\eta^\#$

Induction step: n > 0. Case: m = 1.

$([N+2/0]\underline{1})\lambda zx p_{n+1}(x,z)$ β-conv. $\lambda zx p_{n+1}(x,z)$ β-conv.

$\lambda zx\ C\ \lambda f \sum_{\eta \in N_n} (\lambda wz(\lambda y \cdot (f(e_n wy))(xy)))\eta^\#$ β-conv.

$\lambda zx \cdot \underline{+}\ (\sum_{\eta \in N_n} z(\lambda y \cdot \underline{1}(xy)))(\sum_{\eta \in N_n} z(\lambda y \cdot (e_n \eta^\# y)(xy))) =$

$\lambda zx \sum_{\eta \in PN_{n+1}^1} z\eta^\#$. Case m = k+1. $([N+2/0]m)\lambda zx p_{n+1}(x,z)$

β-conv. $\lambda w_1\ \lambda zx p_{n+1}(x,z)(([N+2/0]\underline{k})\ \lambda zx p_{n+1}(x,z)w_1)$

β-conv. $\lambda w_1 \lambda zx p_{n+1}(x,z)(\lambda x \sum_{\eta \in PN_{n+1}^k} w_1\eta^\#)$ β-conv. $\lambda zx_2 \cdot \underline{+}$

$(\sum_{\eta \in N_n} (\lambda x \sum_{\xi \in PN_{n+1}^k} z\xi^\#)(\lambda y \cdot \underline{1}(w_2 y)))(\sum_{\eta \in N_n} (\lambda x \sum_{\xi \in PN_{n+1}^k} z\xi^\#)$

$(\lambda y \cdot (e_n \eta^\# y)(w_2 y)))$ β-conv. $\lambda zx \sum_{\eta \in PN_{n+1}^m} z\eta^\#$.

The proposition follows easily from the lemma.

Proposition: Suppose $\alpha, \beta \in \mathcal{D}_n$, $\gamma \in \mathcal{D}_{n+1}$, $t_1 \in def^n(\beta)$, $t_2 \in def^n(\alpha)$ and $t_3 \in def^{n+1}(\gamma)$. Then

(a) $\beta = \alpha \iff e_n t_1 t_2$ β-conv. $\underline{0}$, and

(b) $\beta \in \gamma \iff t_3 t_1$ β-conv. $\underline{0}$.

Proof: by induction on n

Basis: n = 0. By inspection

Induction step: n = m + 1. We have $e_n t_1 t_2$ β-conv. $\sum_{\eta \in N_m} e_0(t_1\eta^\#)(t_2\eta^\#)$. If $\beta = \alpha$ and $\eta^\# \in def^n(\beta)$ by hyp. ind.on (b) $e_0(t_1\eta^\#)(t_2\eta^\#)$ β-conv. $\underline{0}$, and if $\eta^\# \notin def^n(\beta)$ by hyp. ind. on (b) $t_1\eta^\#$, $t_2\eta^\#$ β-conv. $\underline{0}$ so $e_0(t_1\eta^\#)(t_2\eta^\#)$ β-conv. $\underline{0}$. If $\beta \neq \alpha$ w.l.o.g. assume $\delta \in \beta$ and $\delta \notin \alpha$ and $\eta^\# \in def^m(\delta)$. By hyp. ind.on (b) $t_1\eta^\#$ β-conv. $\underline{0}$ and $t_2\eta^\#$ β-conv. $\underline{0}$ so $e_0(t_1\eta^\#)(t_2\eta^\#)$ β-conv. $\underline{1}$. Thus $\alpha = \beta \Rightarrow e_n t_1 t_2$ β-conv. $\underline{0}$ and $\alpha \neq \beta \Rightarrow \underline{sg}(e_n t_1 t_2)$ β-conv. $\underline{1}$. Let $t_3 = \lambda y \cdot r_1(\ldots(\cdot r_{2_{n+1}} \underline{1})\ldots)$. If $\beta \in \gamma$ then for some $t_4 \in def^n(\beta)$ and some i we have $r_i = e_n t_4 y$. By (a) $e_n t_4 t_1$ β-conv. $\underline{0}$ so $t_3 t_1$ β-conv. $\underline{0}$. If $\beta \notin \gamma$ then, for each $r_i = e_n t_4 y$, $t_4 \notin def^n(\beta)$ so by (a) $e_n t_4 t_1$ β-conv. $\underline{0}$ and $\underline{sg}(t_3 t_1)$ β-conv. $\underline{1}$.

III.3 We now define the translation *:

$\underline{0}^* = \underline{0}$

$\underline{1}^* = \underline{1}$

$(x^n)^* = x^N$

$(t_1 \varepsilon t_2)^* = \underline{sg}(t_2^* t_1^*)$

$(A \wedge B)^* = \underline{sg}(+(A^*)(B^*))$

$(\neg A)^* = \underline{\overline{sg}}\ A^*$

$(\forall x^n A)^* = \underline{sg}(\forall_n \lambda x^N A^*)$

Proposition: Suppose $A = A(x_1^{n_1},\ldots,x_m^{n_m})$, $\alpha_i \in \mathcal{D}_n$ and $t_i \in def^{n_i}(\alpha_i)$ then $A[\alpha_1,\ldots,\alpha_m] \Longleftrightarrow (\lambda x^{N_1}\ldots x_m^{N_m} A^*)t_1\ldots t_m$ β-conv. $\underline{0}$.

Proof: By induction on A

Basis: A is prime. By the lemma for e_n(b)

Induction step. Cases $A = B \wedge C$, $A = \neg B$. Immediate by hyp. ind. Case: $A = \forall x^n B$. We have $A[\alpha_1\ldots\alpha_m] \Longleftrightarrow$ $\forall \beta \in \mathcal{D}_n\ B[\alpha_1\ldots\alpha_m\beta] \Longleftrightarrow \forall t \in def_n(\lambda x_1^{N_1}\ldots x_m^{N_m} x^N B^*)t_1\ldots t_m t$ β-conv. $\underline{0} \Longleftrightarrow \underline{sg}(\sum_{\eta \in N_n} (\lambda x_1^{N_1}\ldots x_m^{N_n} x^N B^*)t_1\ldots t_m \eta\#)$ β-conv. $\underline{0} \Longleftrightarrow (\lambda x_1^{N_1}\ldots x_m^{N_m} \underline{sg}(\sum_{\eta \in N_m} (\lambda x^N B^*)\eta\#))t_1\ldots t_m$ β-conv. $\underline{0} \Longleftrightarrow (\lambda x_1^{N_1}\ldots x_m^{N_m} \underline{sg}(\forall_n \lambda x^N B^*))t_1\ldots t_m$ β-conv. $\underline{0} \Longleftrightarrow$ $(\lambda x_1^{N_1}\ldots x_m^{N_m} A^*)t_1\ldots t_m$ β-conv. $\underline{0}$.

We can now prove the theorem:

Proof of theorem: The above proposition establishes the theorem for $\sigma = 0$ with $t^\sigma = \underline{0}$. Note that for Ω-sentences A $A \Longleftrightarrow A^*$ β-conv. $\underline{0}$ and $\neg A \Longleftrightarrow A^*$ β-conv. $\underline{1}$. Case: $\sigma = \underbrace{0 \to (\ldots(0 \to 0)\ldots)}_{m}$ for $m > 1$. We have for closed t of type 0, t β-conv. $\underline{0} \Longleftrightarrow t(\lambda V_0^0 V_1^0)V_2^0$ β-conv. $V_2^0 \Longleftrightarrow \lambda V_1^0\ldots V_m^0(t(\lambda V_0^0 V_1^0)V_2^0)$ β-conv. $\lambda V_1^0\ldots V_m^0 V_2^0$ so we can set $t^\sigma = \lambda V_1^0\ldots V_m^0 V_2^0$. Case: otherwise. We say that σ contains a splinter if there is a closed term t of type σ and a closed term s of type $\sigma \to \sigma$ such that the β-normal forms of t, st, ..., s(...(st)...),... are all distinct. It is easy to prove that σ contains a splinter $\Longleftrightarrow$ σ contains a closed term and σ does not have the form $0 \to (\ldots(0 \to 0)\ldots)$. Suppose α contains a splinter generated by t and s; we have, for closed t_1 of type 0, t_1 β-conv. $\underline{0} \Longleftrightarrow [\sigma/0]t_1$ β-conv. $[\sigma/0]\underline{0} \Longleftrightarrow$ $(([\sigma/0]t_1)s)t$ β-conv. t so we can set $t^\sigma = t$.

By a consistent extension Λ^+ of Λ we mean an extension of Λ with a model whose ground domain has ≥ 2 elements. (Note that Λ^+ need not be closed under the inductive definition of β-convertibility. Similarly we admit non-extensional models whose theories are not closed under this inductive definition unlike the models considered by Friedman for β-η-conversion. However, our consistent extensions are all fragments of Friedman's. In particular, there is an extensional model of Λ with a ground domain of 2 elements that satisfies all consistent closed equations. This model can be constructed by using the following version of Bohm's theorem for Λ:

Proposition (Statman): Let $\sigma = \sigma_1 \to (\ldots(\alpha_n \to 0)\ldots)$ and let t_1, t_2 be closed terms of type σ, then $t_1 = t_2$ is consistent with $\Lambda \Longleftrightarrow$ for all t_3 of type $\sigma \to 0$ containing only free variables of type 0 $t_3 t_1$ β-conv. $t_3 t_2$ $\Longleftrightarrow$ for all s_i of type σ_i containing only free variables of type 0 $t_1 s_1\ldots s_n$ β-conv. $t_2 s_1\ldots s_n$.) If Λ^+ is an extension of Λ and $\Lambda^+ \vdash \underline{0} = \underline{1}$ then $\Lambda^+ \vdash V_1^0 = V_2^0$ so Λ^+ is not consistent. Thus if Λ^+ is a consistent extension of Λ, for Ω-sentences A, $A \Longleftrightarrow \Lambda^+ \vdash A^* = \underline{0}$.

Corollaries:

(1) The rank of a type is defined as follows: rnk(0) = 0, and $rnk(\sigma \to \tau) = \max\{rnk(\sigma)+1, rnk(\tau)\}$. Let $T_n = \{t \in \Lambda$: each subterm of t has type with rnk $\leq n\}$. It is easy to see that for each n the problem for arbitrary closed terms t_1, $t_2 \in T_n$ of whether t_1 β-conv. t_2 can be solved in elementary time (analysis of the normal form theorem). By modifying the above construction (using Meyer's result for the monadic predicate calculus instead of Ω) it is easy to find an n such that the problem, for arbitrary closed $t \in T_n$ of whether t β-conv. $\underline{0}$ cannot be solved in polynomial time.

(2) If F is a finite set of types let $T_F = \{t \in \Lambda$: each subterm of t has type $\in F\}$. By modifying the above construction (using the Meyer-Stockmeyer result for B_ω instead of Ω) it is easy to find an F such that the problem for arbitrary closed $t \in T_F$ of whether t β-conv. $\underline{0}$ is polynomial-space hard.

IV. We now consider the typed λ-calculus with infinitely many ground types $0_1,\ldots,0_n,\ldots$, still called 'Λ', and the problem of whether an arbitrary type contains a closed term. We shall show that this problem is p-space complete (it is easy to see that with only finitely many ground types the problem can be solved in polynomial time).

By a well known result of Howard's (see Prawitz) σ contains a closed term $\Longleftrightarrow$ σ considered as a propositional formula is ~~institutionally~~ intuitionistically valid. We shall show that the validity problem for intuitionistic implicational logic is p-space complete.

Let B_ω be classical second-order propositional logic (quantified Boolean formulae). Se shall define polynomial time translations *: $B_\omega \longrightarrow$ intuitionistic propositional logic and #: intuitionistic propositional logic $\longrightarrow$ intuitionistic implicational logic satisfying; $A \Longleftrightarrow A^*$ is intuitionistically provable and A is intuitionistically provable $\Longleftrightarrow A\#$ is intuitionistically provable. The result follows from the existence of * and # by the result of Meyer and Stockmeyer that B_ω is p-space complete and Kreisel's completeness proof for intuitionistic implicational logic. (Note that validity here means validity under the intended interpretation as well as validity in all Kripke models.)

It is convenient for purposes of the proof to consider two different formulations of intuitionistic propositional logic; the cut-free sequent calculus (with sequents $\Gamma \longrightarrow A$ for Γ a finite set of formulae) and natural deduction (see Prawitz). The full language is built-up from propositional variables, $\perp$(absurdity), $\wedge$, $\vee$, $\to$ with $\neg A =_{df} A \to \perp$. Let $A = Q_n x_n\ldots Q_1 x_1 B_0$ be a prenex B_ω sentence with B_0 quantifier-free, $Q_i = \forall$ or $\exists$, and set $B_{k+1} = Q_{k+1} x_{k+1} B_k$. Define A^+ as follows: $B_0^+ = \neg\neg B_0$, $B_{k+1}^+ = (x_{k+1} \vee \neg x_{k+1}) \to B_k^+$ if $Q_{k+1} = \forall$, and $B_{k+1}^+ = (x_{k+1} \to B_k^+) \vee (\neg x_{k+1} \to B_k^+)$ if $Q = \exists$. Select new variables $y_0\ldots y_n$ and define $B_k^\checkmark$ by $B_0^\checkmark = \neg\neg B_0 \leftrightarrow y_0$, $B_{k+1}^\checkmark = ((x_{k+1} \vee \neg x_{k+1}) \to y_k) \leftrightarrow y_{k+1}$ if $Q_{k+1} = \forall$,

$B^{\vee}_{k+1} = ((x_{k+1} \to y_k) \vee (\neg x_{k+1} \to y_k)) \leftrightarrow y_{k+1}$ if $Q_{k+1} = \exists$.
Set $A^* = B^{\vee}_0 \to (\ldots(B^{\vee}_n \to y_n)\ldots)$; clearly A^* can be obtained from A in polynomial time and A^* is intuitionistically provable $\iff$ A^+ is intuitionistically provable.

Proposition: A $\iff$ A^+ is intuitionistically provable.

Proof: Suppose A and let $C_1 \ldots C_m$ be the connectives (Skolem functions) realizing the $\exists$ quantifiers in A. If Q_k is the j^{th} $\exists$ quantifier we write $Q_k = \exists_j$ and take C_j as a function of $x_n \ldots x_{k+1}$ for convenience. We write e_i ambiguously for x_i and $\neg x_i$ and define $C_j(e_n,\ldots,e_{k+1}) = e_k$ if setting $\nu_i = T$ when $e_i = x_i$ and $\nu_i = \bot$ when $e_i = \neg x_i$ we have $C_j(\nu_n,\ldots,\nu_{k+1}) = \nu_k$.

Grow a tree of sequents as follows: T_1

$$\Longrightarrow \emptyset \to A^+$$

$$\{e_n \ldots e_{k+1}, e_k\} \to B^{\vee}_{k-1}$$

$$\{e_n \ldots e_{k+1}\} \to (e_k \to B^{\vee}_{k-1})$$

$$\{e_n \ldots e_{k+1}\} \to B^{\vee}_k \Longrightarrow \{e_n \ldots e_{k+1}\} \to B^{\vee}_k$$

if $Q_k = \exists_j$ and $C_j(e_n \ldots e_{k+1}) = e_k$

$$\{e_n \ldots e_{k+1}, x_k\} \to B_k \quad \{e_n \ldots e_{k+1}, \neg x_k\} \to B^{\vee}_{k-1}$$

$$\{e_n \ldots e_{k+1}, x_k \vee \neg x_k\} \to B^{\vee}_{k-1}$$

$$\{e_n \ldots e_{k+1}\} \to B^{\vee}_k \Longrightarrow \{e_n \ldots e_{k+1}\} \to B^{\vee}_k$$

if $Q_k = \forall$

$$\{e_n \ldots e_1\} \to B^{\vee}_0 \Longrightarrow \{e_n \ldots e_1\} \to B^{\vee}_0$$

Note that if $\{e_n \ldots e_{k+1}\} \to B^{\vee}_k$ occurs in T_1 then $e_n \wedge \ldots \wedge e_{k+1} \Longrightarrow B_k$. Moreover each leaf of T_1 has the form $\{e_n \ldots e_1\} \to \neg\neg B_0$ and thus is intuitionistically provable by Glivenko's theorem.(8) Hence A^+ is intuitionistically provable.

Suppose that A^+ is intuitionistically provable. Grow a tree of sequents as follows: T_2

$$\Longrightarrow \emptyset \to A^+$$

$$\{e_n \ldots e_{k+1}, e_k\} \to B^{\vee}_{k-1}$$

$$\{e_n \ldots e_{k+1}\} \to (e_k \to B^{\vee}_{k-1})$$

$$\{e_n \ldots e_{k+1}\} \to B^{\vee}_k \Longrightarrow \{e_n \ldots e_{k+1}\} \to B^{\vee}_k$$

if $Q_k = \exists$ and $e_n \wedge \ldots \wedge e_{k+1} \to (e_k \to B^{\vee}_{k-1})$ is intuitionistically provable.

$$\{e_n \ldots e_{k+1}, x_k\} \to B_{k-1} \quad \{e_n \ldots e_{k+1}, \neg x_k\} \to B^{\vee}_{k-1}$$

$$\{e_n \ldots e_{k+1}, x_k \vee \neg x_k\} \to B^{\vee}_{k-1}$$

$$\{e_n \ldots e_{k+1}\} \to B^{\vee}_k \Longrightarrow \{e_n \ldots e_{k+1}\} \to B^{\vee}_k$$

if $Q_k = \forall$

$$\{e_n \ldots e_1\} \to B^{\vee}_0 \Longrightarrow \{e_n \ldots e_1\} \to B^{\vee}_0 .$$

Note that if $\{e_n \ldots e_{k+1}\} \to B_k$ occurs in T_2 then $e_n \wedge \ldots \wedge e_{k+1} \to B_k$. Thus A.

Now let A be an arbitrary propositional formula of intuitionistic logic; to each subformula B of A assign a new variable x_B. Define F_A = $\{y \to x_y,\ x_y \to y : y \text{ in } A\} \cup \{x_\bot \to \bot,\ \bot \to x_\bot\} \cup \{x_B \to (x_{B_1} \to x_{B_2}),\ (x_{B_1} \to x_{B_2}) \to x_B : B = B_1 \to B_2 \text{ in } A\} \cup \{x_{B_1} \to (x_{B_2} \to x_B),\ x_B \to x_{B_1},\ x_B \to x_{B_2} : B = B_1 \wedge B_2 \text{ in } A\} \cup \{x_\bot \to x_B : B \text{ in } A\} \cup \{x_{B_1} \to x_B,\ x_{B_2} \to x_B,\ x_B \to ((x_{B_1} \to x_{B_3}) \to ((x_{B_2} \to x_{B_3}) \to x_{B_3})) : B = B_1 \vee B_2 \text{ in } A, B_3 \text{ in } A\}$. Let $F_A = \{F_1 \ldots F_n\}$ and define $A^{\#} = F_1 \to (\ldots(F_n \to x_A)\ldots)$.

Proposition: A is intuitionistically provable $\iff$ $A^{\#}$ is intuitionistically provable.

Proof: Suppose $A^{\#}$ is intuitionistically provable, then so is $F_A \Longrightarrow x_A$.
Let θ be the substitution defined by $\theta x_B = B$; $\theta'' F_A \Longrightarrow A$ is intuitionistically provable. It is easy to see that $B \in \theta'' F_A \Longrightarrow B$ is intuitionistically provable; thus A is intuitionistically provable.

Suppose A is intuitionistically provable. By the normal-form theorem(4) there is a natural deduction of A, with the subformula property, D. Replace each B in D by x_B and replace the resulting inferences as follows:

$$\frac{x_\bot}{x_B} \Longrightarrow \frac{x_\bot \to x_B \quad x_\bot}{x_B}$$

$$\frac{\begin{array}{c}[x_{B_1}]\\ x_{B_2}\end{array}}{x_B} \quad B = B_1 \to B_2 \Longrightarrow \frac{(x_{B_1} \to x_{B_2}) \to x_B \quad \begin{array}{c}[x_{B_1}]\\ x_{B_1} \to x_{B_2}\end{array}}{x_B}$$

$$\frac{x_B \quad x_{B_1}}{x_{B_2}} \quad B = B_1 \to B_2 \Longrightarrow \frac{x_B \to (x_{B_1} \to x_{B_2}) \quad x_B \qquad x_{B_1} \to x_{B_2} \quad x_{B_1}}{x_{B_2}}$$

$$\frac{x_{B_1} \quad x_{B_2}}{x_B} \quad B = B_1 \wedge B_2 \Longrightarrow \frac{x_{B_1} \to (x_{B_2} \to x_B) \quad x_{B_1} \qquad x_{B_2} \to x_B \quad x_{B_2}}{x_B}$$

$$\frac{x_B}{x_{B_i}} \quad B = B_1 \wedge B_2 \Longrightarrow \frac{x_B \to x_{B_i} \quad x_B}{x_{B_i}}$$

$$\frac{x_{B_i}}{x_B} \quad B = B_1 \vee B_2 \Longrightarrow \frac{x_{B_i} \to x_B \quad x_{B_i}}{x_B}$$

$$\frac{x_B \quad x_{B_3} \quad x_{B_3}}{x_{B_3}} \quad B = B_1 \vee B_2 \Longrightarrow$$

$$\frac{\begin{array}{c}[x_{B_1}]\\ x_B \to ((x_{B_1} \to x_{B_3}) \to ((x_{B_2} \to x_{B_3}) \to x_{B_3}))\end{array} \quad x_B \qquad x_{B_3} \quad [x_{B_1}]}{(x_{B_1} \to x_{B_3}) \to ((x_{B_2} \to x_{B_3}) \to x_{B_3})} \qquad \frac{x_{B_1} \to x_{B_3} \quad \begin{array}{c}[x_{B_2}]\\ x_{B_2} \to x_{B_3}\end{array}}{(x_{B_2} \to x_{B_3}) \to x_{B_3}}$$

$$x_{B_3}$$

The result is a natural deduction of x_A from F_A; thus $A^{\#}$ is intuitionistically provable.

Theorem: The problem of determining if an arbitrary implicational formula is intuitionistically valid is p-space complete.

Proof: That the problem is p-space hard follows from the preceding propositions. That the problem can be solved in p-space follows from the familiar Tarski translation into the modal logic S4 (6d) and a result of Ladner.

References

Aho, Hopcroft and Ullman — The Design and Analysis of Computer Algorithms, Addison Wesley, 1974

Church — The Calculi of Lambda-Conversion, Annals of Math. Studies No. 6

Friedman — "Equality between Functionals" Springer Lecture Notes in Math., 453

Hindley, Lercher, and Seldin — Introduction to Combinatory Logic, London Math. Soc. Lecture Note No. 7

Huet — "A Unification Algorithm for Typed λ-calculus" This journal, no. 1, 1975

Kreisel — "A Remark on Free Choice Sequences and Topological Completeness Proofs" J.S.L. 23, 1958

Ladner — "The Computational Complexity of Validity in T, S4 and S5" Unpublished manuscript

Lauchli — "An abstract notion of realizability for which the intuitionistic predicate calculus is complete" Intuitionism and proof theory, Kino, Myhill and Vesley, eds. North Holland, 1968

Mann — "The connection between equivalence of proofs and cartesian closed categories" Proc. London Math. Soc. (3), 31, no. 3, 1975

Meyer — "The Inherent Computational Complexity of Theories of Ordered Sets" Proc. of the Int. Cong. of Math., 1974

Montague — "The proper treatment of quantification in ordinary English" Approaches to Natural Language, Reidel, 1973

Prawitz — "Ideas and results in proof theory" Proc. of the Second Scand. Logic Symp. North Holland, 1971

Schwichtenberg — "Definiebare Functionen im λ-Kalkul mit Typen" Arch. Math. Logik 17, no. 3-4, 1975-76

Stockmeyer — "The Polynomial-Time Hierarchy" This journal, no. 3, 1977

Notes

(1) [unification] Of course, this can be viewed as a special case of unification. In addition, let t be a normal term and s an arbitrary term of type σ. For each "redex" $(\lambda x s_1)^{\tau_1 \to \tau_2} s_2^{\tau_1}$ in s select a new variable $z^{(\tau_1 \to \tau_2) \to (\tau_1 \to \tau_2)}$ and replace the redex by $z(\lambda x s_1)s_2$. Let s' be the result and $z_1 \ldots z_n$ the new variables. Let $s_i = \lambda u_i v_i (z_i u_i) v_i$ and $t_i = \lambda u_i v_i (u_i v_i)$ for u_i, v_i of appropriate type; put $s^+ = \lambda y \cdot y s' s_1 \ldots s_n$ and $t^+ = \lambda y \cdot y t t_1 \ldots t_n$ for y of appropriate type. We have s β-conv. t $\Leftrightarrow \{s^+, t^+\}$ is unifiable. Thus, by our principal result (see below), the problem of determining for normal terms s,t with t closed whether {s,t} is unifiable is not elementary recursive.

(2) The question is certainly decidable. For a proof see Prawitz, IV.2.

(3) Equivalently, whether a given formula in the → fragment of intuitionistic propositional logic is valid (this is discussed in Prawitz, IV.2). In particular, we shall show that this problem is p-space complete.

(4) The problem of determining if an arbitrary Ω-sentence is true is decidable. This can be proved by eliminating quantifiers from Ω (see for example, "The consistency of the simple theory of types," The Collected Papers of Gerhard Gentzen, Szabo (ed.), North Holland (1969).

(5) More generally, iff σ contains a closed term and a positive occurrence of a subtype of the form $\sigma_1 \to (\sigma_2 \to \sigma_3)$. However, the proof of this requires the model mentioned parenthetically below and is not included. See III.3, paragraph 3, for a definition of 'consistent extension'.

(6) This observation already establishes that the normal form algorithm requires non-elementary time.

(7) Here we give a non-deterministic algorithm. The tree is grown from sequents $\Gamma \Rightarrow A$ with a dot over the sequential arrow, and the dot is passed up the branches until termination.

(8) See Kleene, Introduction to Metamathematics, Van Nostrand (1952), p. 492.

(9) See Prawitz, II.3.5.

(10) See McKinsey and Tarski, "Some theorems about the sentential calculi of Lewis and Heyting," J.S.L. 13, 1-15, 1948.