Theoretical Computer Science 9 (1979) 67–72

INTUITIONISTIC PROPOSITIONAL LOGIC IS POLYNOMIAL-SPACE COMPLETE

Richard STATMAN

Department of Philosophy, The University of Michigan, Ann Arbor, MI 48109, U.S.A.

Communicated by A. Meyer
Received May 1977
Revised June 1978

Abstract. It is the purpose of this note to show that the question of whether a given propositional formula is intuitionistically valid (in Brouwer's sense, in Kripke's sense, or just provable by Heyting's rules, see Kreisel [7]) is p-space complete (see Stockmeyer [14]). Our result has the following consequences:

(a) There is a simple (i.e. polynomial time) translation of intuitionistic propositional logic into classical propositional logic if and only if NP $= p$-space.

(b) The problem of determining if a type of the typed λ-calculus is the type of a closed λ-term is p-space complete (this will be discussed below). Inhabitation problem

(c) There is a polynomial bounded intuitionistic proof system if and only if NP $= p$-space (see Cook and Reckhow [2]).

1. Reduction of B_ω to intuitionistic propositional logic

Let B_ω be classical second-order propositional logic (quantified Boolean formulae, see [14]). We shall define polynomial time translations $^*: B_\omega \to$ intuitionistic propositional logic, and $^\#$: intuitionistic propositional logic $\to$ intuitionistic implicational logic, satisfying, for prenex B_ω sentences A, that

A is true $\Leftrightarrow A^*$ is intuitionistically provable $\Leftrightarrow A^{*\#}$ is intuitionistically provable.

Our result follows from the existence of * and $^\#$, the completeness theorems of Kreisel and Kripke [8, 9], the results of Meyer and Stockmeyer [14] and Ladner [10], and a result of Tarski's [4].

The full language of intuitionistic propositional logic is built-up from propositional variables, $\perp$ (absurdity or falsehood), $\wedge$, $\vee$, $\rightarrow$ with $\neg A =_{\mathrm{df}} A \rightarrow \perp$. Let $A = Q_n x_n \cdots Q_1 x_1 B_0$ 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:

$$B_0^+ = \neg\neg B_0,$$

$$B_{k+1}^+ = (x_{k+1} \vee \neg x_{k+1}) \rightarrow B_k^+ \quad \text{if } Q_{k+1} = \forall$$

and

$$B^+_{k+1} = (x_{k+1} \to B^+_k) \vee (\neg x_{k+1} \to B^+_k) \quad \text{if } Q_{k+1} = \exists.$$

Select new variables $y_0 \cdots y_n$ and define $B^{\surd}_k$ by

$$B^{\surd}_0 = \neg\neg B_0 \leftrightarrow y_0,$$

$$B^{\surd}_{k+1} = ((x_{k+1} \vee \neg x_{k+1}) \to y_k) \leftrightarrow y_{k+1} \quad \text{if } Q_{k+1} = \forall$$

and

$$B^{\surd}_k = ((x_{k+1} \to y_k) \vee (\neg x_{k+1} \to y_k)) \leftrightarrow y_{k+1} \quad \text{if } Q_{k+1} = \exists.$$

Let $A^* = B^{\surd}_0 \to (\cdots (B^{\surd}_n \to y_n) \cdots)$; we shall show A is true $\Leftrightarrow A^+$ is intuitionistically provable $\Leftrightarrow A^*$ is intuitionistically provable. Clearly A^* can be obtained from A in polynomial time.

We shall take for our formulation of intuitionistic logic the natural deduction system of Prawitz [11, p.20]. If Γ is a finite set of formulae and A is a formula we write $\Gamma \vdash_{\mathrm{I}} A$ if there is a natural deduction of A from Γ. The following facts will be used below:

(1) If A is a classical consequence of Γ, then $\Gamma \vdash_{\mathrm{I}} \neg\neg A$ (Glivenko's theorem; see Kleene [7, p.492]).

(2) $\Gamma \vdash_{\mathrm{I}} A \to B \Leftrightarrow \Gamma \cup \{A\} \vdash_{\mathrm{I}} B$.

(3) $\Gamma \cup \{A \vee B\} \vdash_{\mathrm{I}} C \Leftrightarrow \Gamma \cup \{A\} \vdash_{\mathrm{I}} C$ and $\Gamma \cup \{B\} \vdash_{\mathrm{I}} C$.

(4) $\Gamma \vdash_{\mathrm{I}} A$ or $\Gamma \vdash_{\mathrm{I}} B \Rightarrow \Gamma \vdash_{\mathrm{I}} A \vee B$.

(5) If Γ contains no formula containing $\vee$, then $\Gamma \vdash_{\mathrm{I}} A \vee B \Rightarrow \Gamma \vdash_{\mathrm{I}} A$ or $\Gamma \vdash_{\mathrm{I}} B$ (see Prawitz [11, p.55]).

Proposition 1. *Let A be a prenex B_ω sentence, then A is true $\Leftrightarrow A^+$ is intuitionistically provable.*

Proof. Set $A = Q_n x_n \cdots Q_1 x_1 B_0$ for B_0 quantifier-free and $Q_i = \forall$ or $\exists$ and set $B_{k+1} = Q_{k+1} x_{k+1} B_k$ as before. If Q_k is the jth $\exists$ from left to right we write $Q_k = \exists_j$. Suppose that there are $m \exists$ quantifiers in A.

First suppose that A is true, then there are connectives $C_1 \cdots C_m$ (for logicians Skolem functions) realizing the $\exists$ quantifiers in A (see [12, p.55]). If $Q_k = \exists_j$ it is convenient to take C_j as a function of $x_n \cdots x_{k+1}$. We write l_i ambiguously for x_i and $\neg x_i$, and define $C_j(l_n, \ldots, l_{k+1}) = l_k$ if setting $\nu_i = T$ when $l_i = x_i$ and $\nu_i = F$ when $l_i = \neg x_i$ we have $C_j(\nu_n, \ldots, \nu_{k+1}) = \nu_k$. Grow a tree $\mathcal{T}_1$ of statements of the form $\Gamma \vdash_{\mathrm{I}} C$ as follows: the root of $\mathcal{T}_1$ is $\vdash_{\mathrm{I}} A^+$. If $\{l_n, \ldots, l_{k+1}\} \vdash_{\mathrm{I}} B^+_k$ is a leaf, then from it grow new vertices

$$\begin{array}{c} \{l_n, \ldots, l_{k+1}\} \vdash_{\mathrm{I}} l_k \to B^+_{k-1} \\ | \\ \{l_n, \ldots, l_{k+1}, l_k\} \vdash_{\mathrm{I}} B^+_{k-1} \end{array}$$

if $Q_k = \exists_j$ and $C_j(l_n, \ldots, l_{k+1}) = l_k$ or new vertices

$$\begin{array}{ccc} & \{l_n, \ldots, l_{k+1} x_k \vee \neg x_k\} \vdash_{\mathrm{I}} B^+_{k-1} & \\ \swarrow & & \searrow \\ \{l_n, \ldots, l_{k+1}, x_k\} \vdash_{\mathrm{I}} B^+_{k-1} & & \{l_n, \ldots, l_{k+1} \neg x_k\} \vdash_{\mathrm{I}} B^+_{k-1} \end{array}$$

if $Q_k = \forall$.

It is easy to prove by induction on the structure of $\mathscr{T}_1$ that if $\{l_n, \ldots, l_{k+1}\} \vdash_{\mathrm{I}} B^+_k$ occurs in $\mathscr{T}_1$, then B_k is a classical consequence of $\{l_n, \ldots, l_{k+1}\}$. Thus by Glivenko's theorem each leaf is true and by (2), (3) and (4) each vertex of $\mathscr{T}_1$ is true. So $\vdash_{\mathrm{I}} A^+$.

Now suppose $\vdash_{\mathrm{I}} A^+$. Grow a tree $\mathscr{T}_2$ as follows: The root of $\mathscr{T}_2$ is $\vdash_{\mathrm{I}} A^+$. If $\{l_n, \ldots, l_{k+1}\} \vdash_{\mathrm{I}} B^+_k$ is a leaf, then from it grow new vertices

$$\begin{array}{c} \{l_n, \ldots, l_{k+1}\} \vdash_{\mathrm{I}} l_k \rightarrow B^+_{k-1} \\ | \\ \{l_n, \ldots, l_{k+1} l_k\} \vdash_{\mathrm{I}} B^+_{k-1} \end{array}$$

if $Q_k = \exists$ and $\{l_n, \ldots, l_{k+1}\} \vdash_{\mathrm{I}} l_k \rightarrow B_{k-1}$ or new vertices

$$\begin{array}{ccc} & \{l_n, \ldots, l_{k+1} x_k \vee \neg x_k\} \vdash_{\mathrm{I}} B^+_{k-1} & \\ \swarrow & & \searrow \\ \{l_n, \ldots, l_{k+1} x_k\} \vdash_{\mathrm{I}} B^+_{k-1} & & \{l_n, \ldots, l_{k+1} x_k\} \vdash_{\mathrm{I}} B^+_{k-1} \end{array}$$

if $Q_k = \forall$.

It is easy to see by (2), (3), and (5) that if $\{l_n, \ldots, l_{k+1}\} \vdash_{\mathrm{I}} B^+_k$ occurs in $\mathscr{T}_2$, then it is true. In addition if $\{l_n, \ldots, l_{k+1}\} \vdash_{\mathrm{I}} B^+_k$ occurs in $\mathscr{T}_2$, then B_k is a classical consequence of $\{l_n, \ldots, l_{k+1}\}$. Thus A is true.

Proposition 2. $\vdash_{\mathrm{I}} A^+ \Leftrightarrow \vdash_{\mathrm{I}} A^*$.

Proof. Suppose $\vdash_{\mathrm{I}} A^+$. It is easy to prove by induction on k that $\{B^{\surd}_0, \ldots, B^{\surd}_n\} \vdash_{\mathrm{I}} y_k \leftrightarrow B^+_k$ so $\{B^{\surd}_0, \ldots, B^{\surd}_n\} \vdash_{\mathrm{I}} y_n$. Thus by (2) $\vdash_{\mathrm{I}} A^*$. Now suppose $\vdash_{\mathrm{I}} A^*$. By (2), $\{B^{\surd}_0, \ldots, B^{\surd}_n\} \vdash_{\mathrm{I}} y_n$. Take a natural deduction (alternative definition of Prawitz [11, p.29]) of y_n from $\{B^{\surd}_0, \ldots, B^{\surd}_n\}$ and for $1 \leqslant k \leqslant n$ substitute B^+_k for y_k. The result is a natural deduction of B^+_n $(=A^+)$ from $\{B^+_0 \leftrightarrow B^+_0 \cdots B^+_n \leftrightarrow B^+_n\}$ so $\vdash_{\mathrm{I}} A^+$.

2. Reduction of intuitionistic propositional logic to its implicational fragment

We shall now reduce intuitionistic logic to its implicational fragment. Let A be an arbitrary propositional formula; to each subformula B of A assign a new variable x_B. Define $\mathscr{F}_A$ to be the union of the following sets:

(1) $\{y \rightarrow x_y, x_y \rightarrow y \colon y \text{ in } A\}$,

(2) $\{x_\perp \rightarrow \perp, \perp \rightarrow x_\perp\}$,

(3) $\{x_\perp \to x_B \colon B \text{ in } A\}$,

(4) $\{x_B \to (x_{B_1} \to x_{B_2}),\ (x_{B_1} \to x_{B_2}) \to x_B \colon B = B_1 \to B_2 \text{ in } A\}$,

(5) $\{x_{B_1} \to (x_{B_2} \to x_B),\ x_B \to x_{B_1},\ x_B \to x_{B_2} \colon B = B_1 \wedge B_2 \text{ in } A\}$,

(6) $\{x_{B_1} \to x_B,\ x_{B_2} \to x_B,\ x_B \to ((x_{B_1} \to x_{B_3}) \to ((x_{B_2} \to x_{B_3}) \to x_{B_3})) \colon B = B_1 \vee B_2 \text{ in } A,\ B_3 \text{ in } A\}$.

Let $\mathcal{F}_A = \{F_1, \ldots, F_n\}$ and set $A^\# = F_1 \to (\cdots (F_n \to x_A) \cdots)$.

Clearly $A^\#$ can be obtained from A in polynomial time.

Proposition 3. $\vdash_{\mathrm{I}} A \Leftrightarrow \vdash_{\mathrm{I}} A^\#$.

Proof. Suppose $\vdash_{\mathrm{I}} A^\#$. By (2), $\mathcal{F}_A \vdash_{\mathrm{I}} x_A$. Take a natural deduction of x_A from $\mathcal{F}_A$ and substitute B for x_B for each B in A (also for $B = \perp$). Let $\mathcal{G}$ result from $\mathcal{F}_A$ by applying these substitutions to each member of $\mathcal{F}_A$. We now have a deduction of A from $\mathcal{G}$. It is easy to see that $B \in \mathcal{G} \Rightarrow \vdash_{\mathrm{I}} B$; thus $\vdash_{\mathrm{I}} A$.

Now suppose $\vdash_{\mathrm{I}} A$. By the normal form theorem for natural deductions (see Prawitz [11, p.50]) there is a natural deduction D of A containing only subformulae of A (see Prawitz [11, p.53, Corollary 1]). Replace each B in D by x_B and replace the resulting inferences as follows:

$$\dfrac{x_\perp}{x_B} \quad \Longrightarrow \quad \dfrac{x_\perp \to x_B \qquad x_\perp}{x_B}$$

$$\dfrac{\begin{array}{c}[x_{B_1}]\\ x_{B_2}\end{array}}{x_B} \quad \xRightarrow{\text{for } B = B_1 \to B_2} \quad \dfrac{(x_{B_1} \to x_{B_2}) \to x_B \qquad \dfrac{\begin{array}{c}[x_{B_1}]\\ x_{B_2}\end{array}}{x_{B_1} \to x_{B_2}}}{x_B}$$

$$\dfrac{x_B \qquad x_{B_1}}{x_{B_2}} \quad \xRightarrow{\text{for } B = B_1 \to B_2} \quad \dfrac{\dfrac{x_B \to (x_{B_1} \to x_{B_2}) \qquad x_B}{x_{B_1} \to x_{B_2}} \qquad x_{B_1}}{x_{B_2}}$$

$$\dfrac{x_{B_1} \qquad x_{B_2}}{x_B} \quad \xRightarrow{\text{for } B = B_1 \wedge B_2} \quad \dfrac{\dfrac{x_{B_1} \to (x_{B_2} \to x_B) \qquad x_{B_1}}{x_{B_2} \to x_B} \qquad x_{B_2}}{x_B}$$

$$\dfrac{x_B}{x_{B_i}} \quad \xRightarrow{\text{for } B = B_1 \wedge B_2} \quad \dfrac{x_B \to x_{B_i} \qquad x_B}{x_{B_i}}$$

$$\dfrac{x_{B_i}}{x_B} \quad \xRightarrow{\text{for } B = B_1 \vee B_2} \quad \dfrac{x_{B_i} \to x_B \qquad x_{B_i}}{x_B}$$

and

$$\dfrac{x_B \qquad \begin{matrix}[x_{B_1}]\\ x_{B_3}\end{matrix} \qquad \begin{matrix}[x_{B_2}]\\ x_{B_2}\end{matrix}}{x_{B_3}} \quad \xRightarrow{\text{for } B=B_1\vee B_2}$$

$$\dfrac{\dfrac{\dfrac{x_B\to((x_{B_1}\to x_{B_3})\to((x_{B_2}\to x_{B_3})\to x_{B_3})) \qquad x_B}{(x_{B_1}\to x_{B_3})\to((x_{B_2}\to x_{B_3})\to x_{B_3})} \qquad \dfrac{\begin{matrix}[x_{B_1}]\\ x_{B_3}\end{matrix}}{x_{B_1}\to x_{B_3}}}{(x_{B_2}\to x_{B_3})\to x_{B_3}} \qquad \dfrac{\begin{matrix}[x_{B_2}]\\ x_{B_3}\end{matrix}}{x_{B_2}\to x_{B_3}}}{x_{B_3}}$$

The result is a natural deduction of x_A from $\mathscr{F}_A$, so by (2) $\vdash_{\mathrm{I}} A^{\#}$.

Theorem. *The problem of determining if an arbitrary implicational formula is intuitionistically valid (valid in all Kripke models) is p-space complete.*

Proof. By Kreisel's completeness theorem [8] A is intuitionistically valid $\Leftrightarrow \vdash_{\mathrm{I}} A$ and by Kripke's completeness theorem [9] A is valid in all Kripke models $\Leftrightarrow \vdash_{\mathrm{I}} A$. If A is a prenex B_ω sentence by the previous propositions A is true $\Leftrightarrow \vdash_{\mathrm{I}} A^{*\#}$ so by the theorem of Meyer and Stockmeyer [14, p.12] the problem is p-space hard.

There is a polynomial time translation of intuitionistic logic into the modal logic S4 due to Tarski (see Fitting [4, p.43]). Ladner [10] shows that S4 can be decided in p-space, so the problem is p-space complete.

3. Typed λ-calculus

In this section we consider the typed λ-calculus (as in Friedman [5]) with infinitely many ground types $0_1, \ldots, 0_n, \ldots$ and the problem of whether an arbitrary type is the type of a closed (i.e. without free variables) term.

Associate, bijectively, to each ground type a propositional variable. Such an association induces a bijection $*$ of types to implicational formulae satisfying $(\sigma, \tau)^* = \sigma^* \to \tau^*$.

Fact (Howard [6], Curry [3]): There is a closed term of type $\sigma \Leftrightarrow \vdash_{\mathrm{I}} \sigma^*$. We obtain as a corollary to our theorem the

Proposition 4. *The problem of determining whether an arbitrary type is the type of a closed term is p-space complete.*

We note in closing that the following problem can be solved in polynomial time:

Given a term M and a type σ is σ the type of M?

References

[1] S.A. Cook, Feasibly constructive proofs and the propositional calculus, in: *Proc. of the 7th Annual Symp. on Theory of Computing* (A.C.M., May 1975).

[2] S.A. Cook and R.A. Reckhow, On the length of proofs in the propositional calculus, in: *Proc. Sixth A.C.M. Symp. on Theory of Computing* (A.C.M., May 1974).

[3] H.B. Curry and R. Feys, *Combinatory Logic, Vol. 1* (North-Holland, Amsterdam, 1968).

[4] M. Fitting, *Intuitionistic Logic, Modal Theory and Forcing* (North-Holland, Amsterdam, 1969).

[5] H. Friedman, Equality between functionals, in: R. Parikh, ed., *Lecture Notes in Math. 453* (Springer-Verlag, Berlin, 1974).

[6] W. Howard, The formulae-as-types notion of construction, mimeographed (1969).

[7] S.C. Kleene, *Introduction to Mathematics* (Van Nostrand, New York, 1952).

[8] G. Kreisel, A remark on free choice sequences and topological completeness proofs, *J. Symbolic Logic* **23** (1958) 378.

[9] S. Kripke, Semantical analysis of intuitionistic logic I, in: J. Crossley and M. Dummett, eds., *Formal Systems and Recursive Functions* (North-Holland, Amsterdam, 1965).

[10] R.E. Ladner, The computational complexity of provability in systems of model propositional logic, *SIAM J. Comput.* **6** (3) (Sept. 1977).

[11] D. Prawitz, *Natural Deduction, Stockholm Studies in Philosophy 3* (Almqvist and Wiksell, 1965).

[12] J.R. Shoenfield, *Mathematical Logic* (Addison-Wesley, Reading, MA, 1967).

[13] R. Statman, The typed λ-calculus is not elementary recursive, *Theoret. Comput. Sci.* **9** (1979) 73–81.

[14] L. V. Stockmeyer, The polynomial-time hierarchy, *Theoret. Comput. Sci.* **3** (1976) 1–22.