On the Polynomial-Space Completeness of Intuitionistic Propositional Logic

Vítězslav Švejdar*†

Jan 19, 2003

The original publication is available at www.springerlink.com.

Abstract

We present an alternative, purely semantical and relatively simple, proof of the Statman's result that both intuitionistic propositional logic and its implicational fragment are *PSPACE*-complete.

1 Introduction

R. Ladner in his 1977 paper [Lad77] presented a polynomial-space decision procedures for the most common modal logics like S4 and T, and proved that the decision problems in question are *PSPACE*-complete. The proofs in [Lad77] are purely semantical in the sense that modal logics are defined via their Kripke semantics; no properties of logical calculi are exploited or even mentioned. Later Statman [Sta79] showed that the intuitionistic propositional logic, along with its implicational fragment where all logical connectives except implication $\rightarrow$ are forbidden, also has a *PSPACE*-complete decision problem. The proofs in [Sta79] use proof-theoretic methods.

The purpose of this paper is to present proofs of Statman's results which are in the spirit of Ladner's [Lad77] and which may be found a little bit simpler than those in [Sta79]. We will not use any particular property of intuitionistic logic, like finite model property, soundness, completeness, or cut-eliminability. However, we will concentrate on only the construction of the reduction from a known *PSPACE*-complete problem, namely the QBF problem. The positive part of the story, i.e. the fact that intuitionistic propositional logic *is* decidable in *PSPACE*, we take as granted. It can be proved using methods from [Lad77].

I thank Albert Visser for an interest and stimulating remarks.

*This paper was supported by grant 401/01/0218 of the Grant Agency of the Czech Republic.

†Charles University, Prague, vitezslavdotsvejdaratcunidotcz, http://www1.cuni.cz/~svejdar/. Palachovo nám. 2, 116 38 Praha 1, Czech Republic.

2 Preliminaries

Propositional formulas are built up from propositional atoms and the nulary symbol $\bot$ for falsity using the usual binary connectives $\to$, $\&$, and $\vee$. Formulas $\neg A$ and $A \equiv B$ are shorthands for $A \to \bot$ and $(A \to B) \,\&\, (B \to A)$ respectively. In syntax analysis, implication $\to$ has lower priority than conjunction $\&$ and disjunction $\vee$, but higher than equivalence $\equiv$.

A *Kripke frame* for intuitionistic logic is a pair $\langle W, \leq \rangle$ where $W \neq \emptyset$ and $\leq$ is a reflexive and transitive relation on W. The elements of W are *nodes*; if $a \leq b$ then the node b is said to be *accessible* from a. A relation $\Vdash$ between nodes of a Kripke frame $\langle W, \leq \rangle$ and propositional formulas is a *truth relation* on $\langle W, \leq \rangle$ if, for any two nodes $a, b \in W$, any propositional atom p and any two propositional formulas A and B, it satisfies the following conditions:

- if $a \leq b$ and $a \Vdash p$ then $b \Vdash p$,
- $a \nVdash \bot$, $a \Vdash A \& B$ iff $a \Vdash A$ and $a \Vdash B$, $a \Vdash A \vee B$ iff $a \Vdash A$ or $a \Vdash B$,
- $a \Vdash A \to B$ iff $\forall b \geq a (b \Vdash A \Rightarrow b \Vdash B)$.

A triple $\langle W, \leq, \Vdash \rangle$ where $\Vdash$ is a truth relation on a Kripke frame $\langle W, \leq \rangle$ is called *Kripke model* for intuitionistic propositional logic. The first condition in the definition of truth relation is called *persistency condition*. A straightforward induction shows that the persistency condition holds for all formulas, not just for atoms. We read $a \Vdash A$ as "A is satisfied in a".

An example of a Kripke model is shown in Fig. 1. Its frame has three nodes a, b, and c, where b and c are accessible from a. We have $b \Vdash p$ and $c \Vdash q$. It is understood that p is not satisfied in a and c, that q is not satisfied in a and b, and that each of the nodes a, b, and c is accessible from itself. One can easily verify that $a \nVdash p \to q$, $a \nVdash q \to p$, and thus $a \nVdash (p \to q) \vee (q \to p)$.

A formula A is *valid* in a model $K = \langle W, \leq, \Vdash \rangle$ if it is satisfied in all nodes $a \in W$. A model K is a *(Kripke) counter-example* to a formula A if A is not valid in K. A formula A is an *intuitionistic tautology* if A is valid in all Kripke models, i.e. if A has no counter-example. The set of all intuitionistic tautologies is denoted IntTaut. Since classical tautologies are exactly those formulas which are valid in all one-element Kripke models, we have IntTaut $\subseteq$ Taut, where Taut is the set of all classical tautologies. Examples

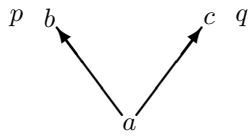

Figure 1: Example Kripke model for intuitionistic logic

of formulas in Taut $-$ IntTaut are $(p \to q) \vee (q \to p)$, $\neg\neg p \to p$, or $p \vee \neg p$. Examples of formulas in IntTaut are all instances of schemes $A \to \neg\neg A$, $\neg\neg\neg A \to \neg A$, or $A \vee B \to D \equiv (A \to D) \,\&\, (B \to D)$.

We shall call the least element of a model K (if it exists) a *root* of K. If $K = \langle W, \leq, \Vdash \rangle$ and $a_0 \in W$ then *submodel generated by* a_0 is the model $K_0 = \langle W_0, \leq_0, \Vdash_0 \rangle$ where $W_0 = \{\, x \in W \,;\, a_0 \leq x \,\}$ and $\leq_0$ and $\Vdash_0$ are the restrictions of $\leq$ and $\Vdash$ to W_0. It can be easily shown that if A is a propositional formula and $a \in W_0$ then $a \Vdash A \Leftrightarrow a \Vdash_0 A$. So in the sequel we can assume that if K is a counter-example to A then K has a root a and that it is the root a where $a \nVdash A$.

More about Kripke models can be found in various sources, e.g. in [vD86], [dJV88], or in [Tak75]. For the notions from theoretical computer science, like QBF, I recommend e.g. [Pap94].

3 The reduction

A key step in *PSPACE*-completeness proofs in [Lad77] is the construction of a sequence of propositional formulas such that the size of the formulas grows only polynomially, all have Kripke counter-example, but the size of the minimal counter-example grows exponentially. One can easily check that if the formulas D_n are defined by $D_0 = \bot$, $D_{n+1} = (p_{n+1} \to D_n) \vee (\neg p_{n+1} \to D_n)$ then each formula D_n has a Kripke counter-example and that each counter-example to D_{n+1} contains two disjoint counter-examples to D_n: one in which p_{n+1} is everywhere positive and another in which it is everywhere negative. So indeed the size of the minimal counter-example to D_n grows exponentially with n. This construction, however, does not work because, due to *two* occurrences of D_n in D_{n+1}, the size of D_n also grows exponentially. What works is this construction of E_n by recursion:

$$E_0 = \bot, \qquad E_{n+1} = (E_n \to q_{n+1}) \to (p_{n+1} \to q_{n+1}) \vee (\neg p_{n+1} \to q_{n+1})$$

where the intended meaning of the atom q_{n+1} is to be a shorthand for E_n. This is an explanation of the role of atoms q_j in our construction below. We will employ further auxiliary atoms s_j whose role is to avoid the use of disjunction in our formulas.

Let a quantified Boolean formula A be given. We may assume that A has the form $Q_m p_m \,..\, Q_1 p_1 B(p_1, .., p_m)$ where B contains no propositional quantifiers and no atoms except $p_1, .., p_m$. We construct the formulas $A_0^*, .., A_m^*$ by recursion. Let A_0^* be $B(\underline{p})$ where $\underline{p}$ stands for the m-tuple $p_1, .., p_m$. If $j > 0$ and $Q_j = \exists$ then A_j^* is

$$(A_{j-1}^* \to q_j) \,\&\, ((p_j \to q_j) \to s_j) \,\&\, ((\neg p_j \to q_j) \to s_j) \to s_j,$$

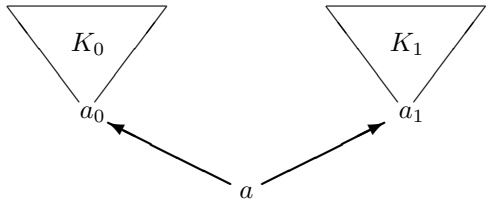

Figure 2: Amalgamating two models into one

whereas if $Q_j = \forall$ then A^*_j is

$$(A^*_{j-1} \to q_j) \,\&\, ((p_j \to q_j) \,\&\, (\neg p_j \to q_j) \to q_j) \to q_j.$$

Note that A^*_j is built up from $p_1, .., p_m$, $q_1, .., q_j$, and $s_1, .., s_j$. More precisely, s_i for $i \leq j$ occurs in A^*_j if and only if Q_i is existential. Finally let A^* be A^*_m.

Lemma 1 *Let $0 \leq j \leq m$ and let e be an evaluation of atoms $p_{j+1}, .., p_m$. Then $e \not\models Q_j p_j .. Q_1 p_1 B(\underline{p})$ if and only if A^*_j has a Kripke counter-example in which each atom p_i, for $i > j$, is evaluated according to e (equally in all nodes).*

Proof by induction on j. If e is an evaluation of $p_1, .., p_m$ and $e \not\models B(\underline{p})$ then the one-element model in which all $p_1, .., p_m$ are evaluated according to e is the required counter-example to A^*_0. Let, on the other hand, K be a counter-example to A^*_0, i.e. to $B(\underline{p})$, in which all $p_1, .., p_m$ are evaluated according to e. A straightforward induction shows that each subformula of $B(\underline{p})$ has the same value everywhere in K, namely the value assigned to it by e. So $e \not\models B(\underline{p})$.

Let $j > 0$ and $Q_j = \exists$ and assume $e \not\models \exists p_j Q_{j-1} p_{j-1} .. Q_1 p_1 B(\underline{p})$. By the definition of propositional quantifiers, none of the two extensions $0^\frown e$ and $1^\frown e$ of e to atom p_j satisfies the formula $Q_{j-1} p_{j-1} .. Q_1 p_1 B(\underline{p})$. So the induction hypothesis yields two Kripke counter-examples to A^*_{j-1}: K_0 with a root a_0 in which $p_{j+1}, .., p_m$ are evaluated everywhere according to e and in which p_j is everywhere negative, and K_1 with a root a_1 in which $p_{j+1}, .., p_m$ are also evaluated according to e and in which p_j is everywhere positive. Note that $a_0 \Vdash \neg p_j$ and $a_1 \Vdash p_j$. Let K be the model depicted in Fig. 2, with a new root a. To complete the definition of K, we must specify the values of the new atoms q_j and s_j everywhere in K and also the values of all atoms $p_1, .., p_m$, $q_1, .., q_j$, and $s_1, .., s_j$ in the new node a. This is done as follows:

- in a, atoms $p_{j+1}, .., p_m$ have the truth values assigned by e,
- $p_1, .., p_j$, $q_1, .., q_{j-1}$, and $s_1, .., s_{j-1}$ are negative in a,
- q_j has everywhere the same truth value as the formula A^*_{j-1},
- s_j has everywhere the same truth value as $(p_j \to q_j) \vee (\neg p_j \to q_j)$.

Note that the only thing we had to ensure was the persistency condition, which we did. We have $a \Vdash A^*_{j-1} \to q_j$. Since the formula

$$((p_j \to q_j) \to s_j) \,\&\, ((\neg p_j \to q_j) \to s_j)$$

is intuitionistically equivalent to $(p_j \to q_j) \vee (\neg p_j \to q_j) \to s_j$, it is everywhere satisfied. We also have $a_0 \not\Vdash \neg p_j \to q_j$ and $a_1 \not\Vdash p_j \to q_j$. Persistency yields $a \not\Vdash (p_j \to q_j) \vee (\neg p_j \to q_j)$. So $a \not\Vdash s_j$ and K is a counter-example to A^*_j.

Assume, on the other hand, that $j > 0$, $Q_j = \exists$ and K is a counter-example to A^*_j. We may assume that K has a root a and that $a \not\Vdash A^*_j$. So $a \not\Vdash s_j$. Since $a \Vdash (\neg p_j \to q_j) \to s_j$, we have $a \not\Vdash \neg p_j \to q_j$. So there exists a node $a_0 \geq a$ such that $a_0 \Vdash \neg p_j$ and $a_0 \not\Vdash q_j$. From $a \Vdash A^*_{j-1} \to q_j$ we have $a_0 \not\Vdash A^*_{j-1}$. So the submodel generated by a_0 is a counter-example to A^*_{j-1} in which p_j is everywhere negative. For analogical reasons, there exists a node a_1 such that the submodel generated by a_1 is a counter-example to A^*_{j-1} in which p_j is everywhere positive. The induction hypothesis says $0^\frown e \not\models Q_{j-1} p_{j-1} .. Q_1 p_1 B(\underline{p})$ and $1^\frown e \not\models Q_{j-1} p_{j-1} .. Q_1 p_1 B(\underline{p})$. So $e \not\models \exists p_j Q_{j-1} p_{j-1} .. Q_1 p_1 B(\underline{p})$.

The reasoning in the case where $j > 0$ and $Q_j = \forall$ is similar. If K is a model with root a and $a \Vdash A^*_j$ then K has an node a_0 such that $a_0 \Vdash p_j \vee \neg p_j$ and the submodel K_0 generated by a_0 is a counter-example to A^*_{j-1}. Since p_j does not change value in K_0, the induction hypothesis is applicable to K_0. Details and the proof of the reverse implication are left to the reader. ∎

One can check that if the possibility of avoiding the connectives &, $\vee$, $\bot$ were not an issue, a simpler definition of A^* would do: A^*_j is $(A^*_{j-1} \to q_j) \to ((p_j \to q_j) \vee (\neg p_j \to q_j))$ or $p_j \vee \neg p_j \to A^*_{j-1}$ according to whether Q_j is $\exists$ or $\forall$ respectively.

Lemma 2 *Let A be a formula and r an atom having no occurrences in A. Let further $A^\flat$ be the result of substitution of r for all occurrence of $\bot$ in A, and let $\Sigma(A)$ be the conjunction of all formulas $r \to p$ where p is an atom in A. Then A has a counter-example if and only if $\Sigma(A) \to A^\flat$ has a counter-example.*

Proof If K is a counter-example to A then we can obtain a counter-example H to $\Sigma(A) \to A^\flat$ simply by evaluating the new atom r negatively everywhere in K.

Assume that $H = \langle W, \leq, \Vdash \rangle$ is a model with root a and $a \not\Vdash \Sigma(A) \to A^\flat$. An easy induction on complexity of B shows that *each implication $r \to B^\flat$, where B is a subformula of A, is valid in H*. Let K be $\langle W_1, \leq_1, \Vdash_1 \rangle$, where $W_1 = \{ x \in W ; x \not\Vdash r \}$ and $\leq_1$ and $\Vdash_1$ are the obvious restrictions of $\leq$ and $\Vdash$. From $a \Vdash r \to A^\flat$ and $a \not\Vdash A^\flat$ we have $a \in W_1$. We claim that for each $x \in W_1$ and each subformula B of A we have $x \Vdash B^\flat \Leftrightarrow x \Vdash_1 B^\flat$. For if, for instance, $x \Vdash_1 C^\flat \to D^\flat$ and $x \not\Vdash C^\flat \to D^\flat$ then for some $y \geq x$ where $y \in W - W_1$ we have $y \Vdash C^\flat$ and $y \not\Vdash D^\flat$. But $y \not\Vdash D^\flat$ and $y \Vdash r$ is a contradiction with the

statement typeset in italics above. Thus K is a counter-example to $A^\flat$ in which r is everywhere negative. So indeed A has a counter-example. ∎

Theorem 1 IntTaut *is a* PSPACE*-complete set. Its purely implicational fragment, i.e. the set of all intuitionistic tautologies built up from propositional atoms using implication as the only connective, also is* PSPACE*-complete.*

Proof For $j = m$ Lemma 1 says that $Q_m p_m \,..\, Q_1 p_1 B(\underline{p})$ (i.e. A) is false in the sense of quantified Boolean formulae if and only if A^*_m (i.e. A^*) has a Kripke counter-example. So the function $A \mapsto A^*$ is a reduction from QBF to IntTaut. This function is computable in polynomial time or even in logarithmic space. We agreed that the membership of IntTaut in PSPACE we take as granted. To obtain a reduction to the implicational fragment, first replace the subformula $B(\underline{p})$ of A^* by a (classically) equivalent formula built up using only $\to$ and $\bot$. Then use Lemma 2 to get rid of the symbol $\bot$. The resulting formula contains none of the symbols $\vee$ and $\bot$ and the statement of Lemma 2 and an inspection of our construction of formulas A^*_j make it clear that it contains conjunctions only in subformulas of the form $C_1 \,\&\, .. \,\&\, C_k \to D$. This last formula is intuitionistically equivalent to $C_1 \to (C_2 \to (\,.. \to (C_k \to D)\,..)$. ∎

Remark 1 The reader of Statman's proof in [Sta79] may be not quite sure whether the symbol $\bot$ is also avoidable when constructing the PSPACE-reduction. So our theorem and Lemma 2 perhaps clarify this point.

Remark 2 Note that if a formula is satisfied in some node of some Kripke model then it is valid in some (one-element) Kripke model. This fact says that the set of all intuitionistically *satisfiable* formulas equals the set Sat of all classically satisfiable formulas. Or better, this fact shows that the satisfiability problem has not a good sense for intuitionistic propositional logic.

References

[dJV88] D. H. J. de Jongh and F. Veltman. Intensional Logic. Lecture notes, Philosophy Department, University of Amsterdam, Amsterdam, 1988.

[Lad77] R. Ladner. The computational complexity of provability in systems of modal logic. *SIAM Journal on Computing*, 6(3):467–480, 1977.

[Pap94] C. H. Papadimitriou. *Computational Complexity.* Addison-Wesley, 1994.

[Spa93] E. Spaan. *Complexity of Modal Logics.* Dissertation, Faculty of Mathematics and Informatics, University of Amsterdam, Amsterdam, 1993.

[Sta79] R. Statman. Intuitionistic propositional logic is polynomial-space complete. *Theoretical Comput. Sci.*, 9:67–72, 1979.

[Tak75] G. Takeuti. *Proof Theory.* North-Holland, Amsterdam, 1975.

[vD86] D. van Dalen. Intuitionistic logic. In D. Gabbay and F. Guenthner, editors, *Handbook of Philosophical Logic*, number 164–167 in Synthese Library, chapter III.4, pages 225–340. Kluwer, Dordrecht, 1986.