The Decision Problem of Provability Logic with Only One Atom

Vítězslav Švejdar*†

Jan 19, 2003

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

Abstract

The decision problem for provability logic remains *PSPACE*-complete even if the number of propositional atoms is restricted to one.

In some cases the set of all tautologies of a modal logic is in *coNP*. An example of a logic like that is the well-known S5. However, most of the traditional modal systems, including S4 and T, have *PSPACE*-complete decision problem. So one can say that adding modalities to the language of classical propositional logic does increase algorithmic complexity — not a surprising paradigm. The methods for constructing a polynomial space decision procedure and for proving *PSPACE*-completeness of a modal logic can be learnt from R. Ladner's paper [Lad77]. Provability logic GL is not mentioned in [Lad77], but it is not difficult to verify that GL has *PSPACE*-complete decision problem as well. In this paper we go farther and use Ladner's methods to show that the decision problem of GL is *PSPACE*-complete even if the number of propositional atoms used to build modal formulas is restricted to one. This fact can be interpreted as saying that, in case of provability logic, allowing more than one atom does not increase the expressive power of the language.

The structure of the present paper is similar to that of our [Šve03] where an alternative simple proof of R. Statman's result concerning *PSPACE*-completeness of intuitionistic propositional logic is presented.

Modal formulas are built up from propositional atoms and the symbol $\bot$ for falsity using logical connectives and a unary symbol $\Box$ for necessity. We use $\Diamond A$ as a shorthand for $\neg\Box\neg A$. The formulas $\Box A$ and $\Diamond A$ are read "A is necessary" and "A is possible" respectively. Let Fm denote the set of all modal formulas.

*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.

A *Kripke model* for modal logic is a triple $\langle W, R, \Vdash \rangle$ where W is a non-empty set (of *nodes* or *possible worlds*), R is a relation on W and $\Vdash$ is a subset of $W \times \mathrm{Fm}$ respecting all logical connectives (i.e. satisfying $x \Vdash A \,\&\, B$ iff $x \Vdash A$ and $x \Vdash B$, etc.) and satisfying the well-known modal rule

$$x \Vdash \Box A \;\Leftrightarrow\; \forall y(x\ R\ y \;\Rightarrow\; y \Vdash A)$$

for all x in W and A (and B) in Fm. The pair $\langle W, R\rangle$ is called Kripke *frame*, R is called *accessibility relation*, whereas $\Vdash$ is the *forcing relation* (or *truth relation*) of a model $\langle W, R, \Vdash\rangle$. If $x \in W$ and $x \Vdash A$ then we say that A is *satisfied* in x. If A is satisfied in all $x \in W$ then A is *valid* in $\langle W, R, \Vdash\rangle$. If A is not valid in $\langle W, R, \Vdash\rangle$ then $\langle W, R, \Vdash\rangle$ is called a *counter-example* to A; if A is satisfied in some node of $\langle W, R, \Vdash\rangle$ then $\langle W, R, \Vdash\rangle$ is a *model of* A. For the symbol $\bot$ the stipulation that $\Vdash$ respects all logical connectives means that the formula $\bot$ is nowhere satisfied. This in turn means that the formula $\Box\bot$ is satisfied in x if and only if no y is accessible from x; so $\Box\bot$ is valid in every model $\langle W, R, \Vdash\rangle$ where R is empty, while its negation $\neg\Box\bot$ is valid e.g. in every model $\langle W, R, \Vdash\rangle$ where R is reflexive.

A model $\langle W, R, \Vdash\rangle$ is a Kripke model for *provability logic* GL if W is finite and R is transitive and irreflexive. A modal formula A is a *tautology of provability logic*, or a GL-*tautology*, if it is valid in every Kripke model for provability logic. Let GLTaut denote the set of all GL-tautologies. Some sources use G, L, or PRL instead of our GL; the letters G and L stand for Gödel and Löb.

From the point of view of graph theory, a Kripke model for provability logic is a directed acyclic (transitive) graph (not necessarily a tree). Let's call a node $x \in W$ a *root* of a model $K = \langle W, R, \Vdash\rangle$ if x is least in $\langle W, R\rangle$, i.e. if every $y \in W$, $y \neq x$ is accessible from x. A node $x \in W$ is a *leaf* in K if no $y \in W$ is accessible from x (i.e. if $x \Vdash \Box\bot$). It is evident that each model for provability logic has at most one root and at least one leaf. Also, some leaf is accessible from every x which is not a leaf itself. A consequence of this fact is that $\neg\Box\bot \to \neg\Box\neg\Box\bot$ is an example of a formula in GLTaut. Other examples are all instances of the scheme $\Box A \to \Box\Box A$. Formulas that are not GL-tautologies are e.g. $\Box\Box p \to \Box p$ and $\Box p \to p$.

If $K = \langle W, R, \Vdash\rangle$ is a Kripke model for provability logic and $a \in W$ then a *submodel generated by* a is the model $K_0 = \langle W_0, R_0, \Vdash_0\rangle$ where W_0 is the set $\{\ x \in W\ ;\ x = a \ \vee\ a\ R\ x\ \}$ and R_0 and $\Vdash_0$ are the obvious restrictions of R and $\Vdash$ to W_0. It is almost evident that if K and K_0 are as above, x an element of W_0 and A a modal formula then $x \Vdash A \;\Leftrightarrow\; x \Vdash_0 A$. So if K is a Kripke counter-example to A we can assume that K has a root a and that it is the root a where $a \not\Vdash A$.

If necessity is interpreted as provability then the formula $\neg\Box\bot \to \neg\Box\neg\Box\bot$ says if contradiction is not provable then the fact that contradiction is not provable is unprovable; so it is a modal version of Gödel's Second Incompleteness Theorem.

The connections of provability logic to metamathematics, however extremely important, are immaterial for the present paper. We refer the interested reader to various sources, e.g. [Sol76], [Smo85], or [Boo93].

We prove the *PSPACE*-completeness of our single-atom provability logic by constructing a reduction from QBF (*quantified Boolean formulae*, see [Pap94]). So 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 will write $B(\underline{p})$ or only B for $B(p_1, .., p_m)$.

First we generalize the fact that the formula $\Box\bot$ is satisfied exactly in leaves, i.e. exactly in nodes of *depth zero*. Let

$$\nabla_i = \Diamond^{(i)}\top \;\&\; \Box^{(i+1)}\bot$$

where the superscript indicates iteration, $\top$ is $\neg\bot$, and $\Diamond$, as already noted, is a shorthand for $\neg\Box\neg$. So for example ∇_1 is equivalent to $\neg\Box\bot\,\&\,\Box\Box\bot$. In general the formula ∇_i is satisfied in a node a of a Kripke model $\langle W, R, \Vdash\rangle$ if and only if there are no paths in $\langle W, R\rangle$ starting in a and having length $i+1$, but there are paths starting in a and having length i (further paths shorter than i not being excluded). Thus the informal reading of ∇_i could be the depth is exactly i. We will work with formulas ∇_i for $i \le m$. Let

$$\boxplus_i = \Box(\nabla_i \to q), \qquad \boxminus_i = \Box(\nabla_i \to \neg q),$$

where q is the (only) atom allowed in our paper for constructing modal formulas. The formulas $\boxplus_i$ and $\boxminus_i$ say that the atom q is positive (or negative, respectively) everywhere in depth i but they do not ensure the existence of nodes of depth i. The basic idea of our construction is to stand in a node (root of a model) of depth $2m$ and speak about what is observable in depth $m-j$ if the observation standpoint is moved to a place of depth $m+j-1$, where $1 \le j \le m$. Before we state and prove theorem 1 we may think of the formula A, the number m of its quantifiers, and its quantifier-free matrix B as fixed. However, we consider various truth evaluations of atoms $p_1, .., p_m$. If e is a truth evaluation of $p_{j+1}, .., p_m$ then we put

$$V(e,j) = \bigwedge_{\substack{j<i\le m,\\ e(i)=1}} \boxplus_{m-i} \;\&\; \bigwedge_{\substack{j<i\le m,\\ e(i)=0}} \boxminus_{m-i},$$

where $0 \le j \le m$. Now we are ready to construct a formula $C^\sharp$ for any subformula C of the formula B:

$$p_i^\sharp = \boxplus_{m-i},$$
$$(D \,\&\, E)^\sharp = D^\sharp \,\&\, E^\sharp, \qquad (\neg D)^\sharp = \neg D^\sharp, \qquad \text{etc.}$$

Note that no propositional quantifiers are involved so far. Let GLSat denote the set of all GL-satisfiable formulas, i.e. formulas satisfied in the root of some Kripke model for provability logic.

Lemma 1 *Let e be a truth evaluation of the atoms $p_1, \ldots, p_m$ and let C be a subformula of B. Then the following conditions are equivalent:*

(i) $e \models C$,

(ii) $\nabla_m \,\&\, V(e,0) \to C^\sharp \in \mathrm{GLTAUT}$,

(iii) $\nabla_m \,\&\, V(e,0) \,\&\, C^\sharp \in \mathrm{GLSAT}$.

Proof The implication (ii) $\Rightarrow$ (iii) is evident since the formula $\nabla_m \,\&\, V(e,0)$ is GL-satisfiable for each e. So it is sufficient to prove (i) $\Rightarrow$ (ii) and $\neg$(i) $\Rightarrow$ $\neg$(iii). This is done by simultaneous induction on complexity of the formula C. If C is an atom p_i and $e \models C$ then $C^\sharp$ (i.e. $p_i^\sharp$, i.e. $\boxplus_{m-i}$) appears as a conjunct in $V(e,0)$. Hence $V(e,0) \to C^\sharp$ is in GLTAUT. If, on the other hand, $e \not\models C$ then $\boxminus_{m-i}$ appears among the conjuncts. Then (iii) fails because the formulas $\boxplus_{m-i}$ and $\boxminus_{m-i}$ cannot be simultaneously satisfied in a node of depth m. The induction step is straightforward. Note that $\neg$(ii) for a formula C is the same as (iii) for $\neg C$, while $\neg$(iii) for C is (ii) for $\neg C$. ∎

Now we use recursion to construct formulas $A_0^*, \ldots, A_m^*$. The formula A_0^* is $\nabla_m \,\&\, B^\sharp$. If $j > 0$ and $Q_j = \forall$ then A_j^* is

$$\Diamond(\nabla_{m+j-1} \,\&\, \boxplus_{m-j}) \,\&\, \Diamond(\nabla_{m+j-1} \,\&\, \boxminus_{m-j}) \,\&\, \Box(\nabla_{m+j-1} \to A_{j-1}^*),$$

whereas if $j > 0$ and $Q_j = \exists$ then A_j^* is

$$\Diamond((\boxplus_{m-j} \vee \boxminus_{m-j}) \,\&\, A_{j-1}^*).$$

Note that an important point here is that A_{j-1}^* appears only once as a subformula of A_j^*.

Lemma 2 *Let $0 \le j \le m$ and let e be a truth evaluation of $p_{j+1}, \ldots, p_m$. Then $e \models Q_j p_j \ldots Q_1 p_1 B(\underline{p})$ if and only if the formula $V(e,j) \,\&\, A_j^*$ is* GL*-satisfiable.*

Proof We proceed by induction on j, verifying simultaneously that if A_j^* has a model then it also has a model of depth exactly $m+j$. For $j = 0$ the statements follow from lemma 1 for $C = B$.

Assume $j > 0$ and $Q_j = \forall$. Let $K = \langle W, R, \Vdash \rangle$ be a model with root a such that $a \Vdash V(e,j) \,\&\, A_j^*$. By the definition of A_j^* we have (i) $a \Vdash \Diamond(\nabla_{m+j-1} \,\&\, \boxplus_{m-j})$, (ii) $a \Vdash \Diamond(\nabla_{m+j-1} \,\&\, \boxminus_{m-j})$, and (iii) $a \Vdash \Box(\nabla_{m+j-1} \to A_{j-1}^*)$. By (i) there is a node a_1 accessible from a and satisfying the formula $\nabla_{m+j-1} \,\&\, \boxplus_{m-j}$, by (ii) there is a node a_0 accessible from a and satisfying the formula $\nabla_{m+j-1} \,\&\, \boxminus_{m-j}$. One may think that the model K looks like that in Fig. 1. The numbers in the left indicate depth. The two parts circumscribed by thinner curves must be disjoint because all nodes in the left one can only see nodes satisfying $\neg q$ when

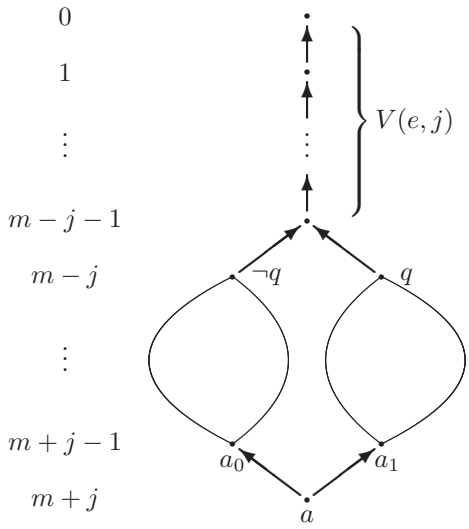

Figure 1: Observing nodes having depth $m-j$

observing depth $m-j$, while all nodes in the right one can only see nodes satisfying q when observing depth $m-j$. Let K_0 and K_1 be the (not necessarily disjoint) submodels of K generated by a_0 and a_1 respectively. From $a_0 \Vdash \nabla_{m+j-1}$ and (iii) we have $a_0 \Vdash A^*_{j-1}$. The formula $V(e,j)$ is persistent in the sense that if it is satisfied in some node x then it is also satisfied in any node y accessible from x. So $a_0 \Vdash V(e,j)$. Note that $V(0^\frown e, j-1)$, where $0^\frown e$ is the extension of e sending j to 0, is the conjunction $\boxminus_{m-j} \& V(e,j)$. So the condition $a_0 \Vdash \boxminus_{m-j}$ yields $a_0 \Vdash V(0^\frown e, j-1)$. Thus K_0 is a model of $V(0^\frown e, j-1) \,\&\, A^*_{j-1}$. So, by the induction hypothesis, $0^\frown e \models Q_{j-1}p_{j-1}..Q_1p_1B(\underline{p})$. Analogical reasoning about K_1 and a_1 shows $1^\frown e \models Q_{j-1}p_{j-1}..Q_1p_1B(\underline{p})$. By the definition of propositional quantifiers we have $e \models \forall p_j Q_{j-1}p_{j-1}..Q_1p_1B(\underline{p})$.

If, on the other hand, both truth evaluations $0^\frown e$ and $1^\frown e$ satisfy the formula $Q_{j-1}p_{j-1}..Q_1p_1B(\underline{p})$ then the induction hypothesis yields two models K_0 and K_1 the roots a_0 and a_1 of which satisfy the formula $V(e,j) \,\&\, A^*_{j-1}$ and such that $a_0 \Vdash \boxminus_{m-j}$ and $a_1 \Vdash \boxplus_{m-j}$. We may assume that both K_0 and K_1 have depth exactly $m+j-1$. Then the model K is constructed from K_0 and K_1 by amalgamation, i.e. by appending a new root a and stipulating that a_0 and a_1 are the only immediate successors of a. The formula $V(e,j)$ is not necessarily backward persistent, but the facts that it is satisfied in all immediate successors of a *and* that all immediate successors of a have depth at least m ensure that $a \Vdash V(e,j)$.

If $Q_j = \exists$ and a is such that $a \Vdash \Diamond((\boxplus_{m-j} \vee \boxminus_{m-j}) \,\&\, A^*_{j-1})$ and $a \Vdash V(e,j)$

then some of the nodes accessible from a generates a submodel the root of which satisfies A^*_{j-1} and one of the formulas $V(0^\frown e, j-1)$ and $V(1^\frown e, j-1)$. The rest of the proof is left to the reader. ∎

For $j = m$ the lemma says that the formula $Q_m p_m \,..\, Q_1 p_1 B(p_1, .., p_m)$, i.e. the formula A, is true in the sense of quantified Boolean formulas if and only if the modal formula A^*_m is GL-satisfiable. The formula A^*_m can be constructed from A in logarithmic space. Thus the function $A \mapsto \neg A^*_m$ is a reduction from $\overline{\text{QBF}}$, the complement of QBF, to GLTAUT. The problem $\overline{\text{QBF}}$, as well as QBF, is *PSPACE*-complete. The formula $\neg A^*_m$ contains no atoms except q. So the following theorem is proved.

Theorem 1 *The set of all* GL*-tautologies built up from only one given propositional atom is* *PSPACE*-*complete.*

Remark (added in January 2002[1]) This result was obtained in 1998 and was presented on several occasions, e.g. at the conference Logica 99 in Liblice, organized by the Philosophical institute of the Czech Academy of Sciences. The same and other related results are also in [CR02].

References

[Boo93] G. Boolos. *The Logic of Provability.* Cambridge University Press, 1993.

[CR02] A. V. Chagrov and M. N. Rybakov. How many variables does one need to prove PSPACE-hardness of modal logics. In Philippe Balbiani, Nobu-Yuki Suzuki, Frank Wolter, and Michael Zakharyaschev, editors, *Advances in Modal Logic 4 (AiML'02)*, pages 71–82, Toulouse, France, October 2002. King's College Publications, 2003.

[Hem01] E. Hemaspaandra. The complexity of poor man's logic. *Journal of Logic and Computation*, 11(4):609–622, 2001.

[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.

[Smo85] C. Smoryński. *Self-Reference and Modal Logic.* Springer, New-York, 1985.

[1] This is a misprint inserted during the proofreading process: should be "added in January 2003".

[Sol76] R. M. Solovay. Provability interpretations of modal logic. *Israel J. Math.*, 25:287–304, 1976.

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

[Šve00] V. Švejdar. On provability logic. *Nordic J. Philosophical Logic*, 4(2):95–116, 2000.

[Šve03] V. Švejdar. On the polynomial-space completeness of intuitionistic propositional logic. *Archive for Math. Logic*, 42(7):711–716, 2003.