Theoretical Computer Science 14 (1981) 113–118
North-Holland Publishing Company

NOTE

AN ELEMENTARY PROOF OF THE COMPLETENESS OF PDL

Dexter KOZEN
IBM Thomas J. Watson Research Center, Yorktown Heights, NY 10598, U.S.A.

Rohit PARIKH*
Mathematics Department, Boston University, Boston, MA, 02215 and Laboratory for Computer Science, Massachusetts Institute of Technology, Cambridge, MA 02139, U.S.A.

Communicated by A. Meyer
Received April 1980

Abstract. We give an elementary proof of the completeness of the Segerberg axioms for Propositional Dynamic Logic.

Introduction

The completeness of Propositional Dynamic Logic (PDL) has been a source of considerable controversy. Several completeness proofs have been proposed independently [1, 3, 5–7, 9–11]. Some of these have been shown to contain subtle errors, and all are quite complicated.

In this note we provide a short, elementary completeness proof of the Segerberg axioms for PDL. The proof is essentially that of [7] but is much simpler, isolating the main ideas in three lemmas, each of which is proved by a simple induction on formula structure. The proof requires no knowledge of logic or model theory apart from basic familiarity with PDL and the propositional calculus.

First we give a brief review of PDL. The reader is referred to [2] for details and intuition.

Syntax

PDL has two types of objects: *programs* and *formulas*. There are primitive symbols $a, b, \ldots$ for programs and $P, Q, \ldots$ for formulas. Compound programs $\alpha, \beta, \gamma, \ldots$

* Research supported by NSF grant MCS7910261.

and formulas $W, X, Y, Z, \ldots$ are built up from these via the rules: if α, β are programs and X, Y are formulas, then $\alpha\beta$, $\alpha \cup \beta$, and α^* are programs and $X \vee Y$, $\neg X$, and $\langle\alpha\rangle X$ are formulas. $\neg\langle\alpha\rangle\neg X$ is abbreviated $[\alpha]X$. We omit the program operators $^-$ and ? for simplicity, although with some restructuring the proof can be extended to include them.

Semantics

PDL is interpreted over *Kripke models*. A Kripke model consists of a nonempty set S of *states*, an assignment $\models$ of a subset of S to each primitive formula, and an assignment $\rightarrow$ of a binary relation on S to each primitive program. We write $s \models P$ to indicate that state s is a member of the subset assigned to P and say *s satisfies P*. We write $s \rightarrow^a t$ to indicate that the pair of states (s, t) is a member of the binary relation assigned to a. The assignments $\models$ and $\rightarrow$ are extended to compound programs and formulas as follows:

$s \rightarrow^{\alpha\beta} t$ iff there is a u such that $s \rightarrow^\alpha u$ and $u \rightarrow^\beta t$,
$s \rightarrow^{\alpha\cup\beta} t$ iff $s \rightarrow^\alpha t$ or $s \rightarrow^\beta t$,
$s \rightarrow^{\alpha^*} t$ iff there are $s_1, \ldots, s_n$ such that $s = s_1 \rightarrow^\alpha s_2 \rightarrow^\alpha \cdots \rightarrow^\alpha s_n = t$,
$s \models X \vee Y$ iff $s \models X$ or $s \models Y$,
$s \models \neg X$ iff not $s \models X$,
$s \models \langle\alpha\rangle X$ iff there is a t such that $s \rightarrow^\alpha t$ and $t \models X$.

The Segerberg axioms

Segerberg [11] proposed the following axiom schemata and rules of inference for PDL:

(1) all propositional tautologies (or enough of them),
(2) $\langle\alpha\rangle\mathbf{false} \equiv \mathbf{false}$,
(3) $\langle\alpha \cup \beta\rangle X \equiv \langle\alpha\rangle X \vee \langle\beta\rangle X$,
(4) $\langle\alpha\rangle(X \vee Y) \equiv \langle\alpha\rangle X \vee \langle\alpha\rangle Y$,
(5) $\langle\alpha\beta\rangle X \equiv \langle\alpha\rangle\langle\beta\rangle X$,
(6) $\langle\alpha^*\rangle X \equiv X \vee \langle\alpha\rangle\langle\alpha^*\rangle X$,
(7) $\langle\alpha^*\rangle X \supset X \vee \langle\alpha^*\rangle(\neg X \wedge \langle\alpha\rangle X)$.

Axiom 7 is the *induction axiom* and is probably better known in its dual form:

$$X \wedge [\alpha^*](X \supset [\alpha]X) \supset [\alpha^*]X.$$

The rules of inference are

$$\frac{X,\ X \supset Y}{Y}, \qquad \frac{X}{[\alpha]X}$$

called *modus ponens* and *generalization*, respectively.

We write $\vdash X$ if X is provable in this system. A formula X is *consistent* if not $\vdash \neg X$. We shall make several uses of the principle that if a disjunction $Y_1 \vee \cdots \vee Y_k$ is consistent, then some Y_i must be consistent. Also, we shall make several uses of the following substitution lemma:

Lemma. *If $\vdash X \equiv Y$, then $\vdash Z \equiv W$, where W is the result of substituting Y for an occurrence of X in Z.*

Proof. The proof is by a simple induction on formula structure and is left to the reader.

We write $X \leq Y$ if $\vdash X \supset Y$.

The completeness of the Segerberg system

Theorem. *The above deductive system for PDL is complete.*

Remark. The proof below constructs a finite model for any consistent formula W. The number of states in this model is exponential in the size of W. It follows immediately from the soundness of the above deductive system that any satisfiable formula W has a model of size exponential in the size of W. This is exactly the Small Model Theorem of [2], used there to obtain an upper bound on the complexity of PDL.

Proof. Let W be a consistent formula of PDL. We wish to construct a Kripke model $\mathcal{M}$ such that W is satisfied at some state of $\mathcal{M}$. $\mathcal{M}$ will be constructed from FL(W), the *Fischer/Ladner closure* of W [2, 7, 1, 10]. FL(W) is the smallest set of formulas containing W such that:

(1) if $X \vee Y \in \mathrm{FL}(W)$, then $X \in \mathrm{FL}(W)$ and $Y \in \mathrm{FL}(W)$,
(2) if $\neg X \in \mathrm{FL}(W)$, then $X \in \mathrm{FL}(W)$,
(3) if $\langle\alpha\rangle X \in \mathrm{FL}(W)$, then $X \in \mathrm{FL}(W)$,
(4) if $\langle\alpha \cup \beta\rangle X \in \mathrm{FL}(W)$, then $\langle\alpha\rangle X \in \mathrm{FL}(W)$ and $\langle\beta\rangle X \in \mathrm{FL}(W)$,
(5) if $\langle\alpha\beta\rangle X \in \mathrm{FL}(W)$, then $\langle\alpha\rangle\langle\beta\rangle X \in \mathrm{FL}(W)$,
(6) if $\langle\alpha^*\rangle X \in \mathrm{FL}(W)$, then $\langle\alpha\rangle X \in \mathrm{FL}(W)$ and $\langle\alpha\rangle\langle\alpha^*\rangle X \in \mathrm{FL}(W)$.

It is easy to see that FL(W) is finite, so let $\mathrm{FL}(W) = \{X_1, \ldots, X_n\}$. An *atom* of FL($W$) is any *consistent* conjunction $Y_1 \wedge \cdots \wedge Y_n$, where each Y_i is either X_i or $\neg X_i$. The symbols A, B, C, D, E always denote atoms of FL(W).[1] Note that for any $X \in \mathrm{FL}(W)$ and atom A, either $A \leq X$ or $A \leq \neg X$, since either X or $\neg X$ appears in the conjunction A. Since PDL contains the propositional calculus, it is easy to show that

[1] The term *atom* is from Boolean algebra: if $\mathcal{L}$ is the Boolean algebra of formulas of PDL modulo provable equivalence, then the $A, B, \ldots$ are atoms of the Boolean subalgebra of $\mathcal{L}$ generated by elements of the Fischer/Ladner closure.

any X in FL(W) is provably equivalent to the join of all $A \leq X$, and **true** is equivalent to the join of all atoms. It follows that there is at least one atom $A \leq W$, since W is consistent.

The Kripke model $\mathcal{M}$ is defined as follows: S is the set of atoms of FL(W). For primitive programs a, $A \rightarrow^a B$ iff $A \wedge \langle a \rangle B$ is consistent. For primitive formulas P, $A \vDash P$ iff $A \leq P$.

Lemma 1. *For any program α, if $A \wedge \langle \alpha \rangle B$ is consistent, then $A \rightarrow^\alpha B$.*

Remark. This is the only place where the induction axiom of PDL is used. The converse is false in general.

Proof. The proof is by induction on the complexity of α. The basis $\alpha = a$ is by definition of $\rightarrow^a$. There are three other cases: (1) $\alpha = \beta \cup \gamma$, (2) $\alpha = \beta\gamma$, and (3) $\alpha = \beta^*$.

(1) If $A \wedge \langle \beta \cup \gamma \rangle B$ is consistent, then so is $(A \wedge \langle \beta \rangle B) \vee (A \wedge \langle \gamma \rangle B)$, by Axiom (3). Then either $A \wedge \langle \beta \rangle B$ or $A \wedge \langle \gamma \rangle B$ is consistent, so by the induction hypothesis either $A \rightarrow^\beta B$ or $A \rightarrow^\gamma B$, therefore $A \rightarrow^{\beta \cup \gamma} B$.

(2) If $A \wedge \langle \beta\gamma \rangle B$ is consistent, then so is $A \wedge \langle \beta \rangle \langle \gamma \rangle B$, by Axiom (5). Using Axiom (4), this is provably equivalent to $\bigvee (A \wedge \langle \beta \rangle (C \wedge \langle \gamma \rangle B))$, where the join is taken over all atoms C. Thus for some C, $A \wedge \langle \beta \rangle (C \wedge \langle \gamma \rangle B))$ must be consistent. By Axiom (4) and the generalization rule, $A \wedge \langle \beta \rangle C$ is consistent; by Axiom (2), $C \wedge \langle \gamma \rangle B$ is consistent. By the induction hypothesis, $A \rightarrow^\beta C \rightarrow^\gamma B$, and therefore $A \rightarrow^{\beta\gamma} B$.

(3) Suppose $A \wedge \langle \beta^* \rangle B$ is consistent. Let $\boldsymbol{G}$ be the smallest set of atoms containing A such that if $C \in \boldsymbol{G}$ and $C \wedge \langle \beta \rangle D$ is consistent, then $D \in \boldsymbol{G}$. By the induction hypothesis, if $C \wedge \langle \beta \rangle D$ is consistent, then $C \rightarrow^\beta D$, so by the definition of $\boldsymbol{G}$, $A \rightarrow^{\beta^*} C$ for all $C \in \boldsymbol{G}$. Thus we need only show that $B \in \boldsymbol{G}$. Let $Y = \bigvee \boldsymbol{G}$. Then $Y \wedge \langle \beta \rangle \neg Y$ is inconsistent, because by Axiom (4) it is equivalent to $\bigvee (C \wedge \langle \beta \rangle D)$, where the join is taken over all $C \in \boldsymbol{G}$ and $D \notin \boldsymbol{G}$, and each such $C \wedge \langle \beta \rangle D$ is inconsistent by the construction of $\boldsymbol{G}$. Thus $\vdash Y \supset [\beta] Y$, and by the generalization rule, $\vdash [\beta^*](Y \supset [\beta] Y)$, and $\vdash A \supset [\beta^*](Y \supset [\beta] Y)$. Also $\vdash A \supset Y$, so by the induction axiom, $\vdash A \supset [\beta^*] Y$, or in other words $A \wedge \langle \beta^* \rangle \neg Y$ is inconsistent. Thus $B \leq Y$ and $B \in \boldsymbol{G}$, as desired.

Lemma 2. *For any $\langle \alpha \rangle X \in$ FL(W) and atom A,*

$$A \leq \langle \alpha \rangle X \text{ iff there exists a } B \text{ such that } A \leftarrow^\alpha B \text{ and } B \leq X.$$

Proof. ($\rightarrow$) By Axiom (4), if $A \leq \langle \alpha \rangle X$, then $A \wedge \langle \alpha \rangle B$ is consistent for some $B \leq X$, and the result follows from Lemma 1.

($\leftarrow$) Suppose $A \rightarrow^\alpha B$ and $B \leq X$. The proof proceeds by induction on the complexity of α. If $\alpha = a$, then $A \wedge \langle a \rangle B$ is consistent, therefore so is $A \wedge \langle a \rangle X$, and thus $A \leq \langle a \rangle X$. This leaves the three induction cases: (1) $\alpha = \beta \cup \gamma$, (2) $\alpha = \beta\gamma$, and (3) $\alpha = \beta^*$.

(1) If $A \to^{\beta \cup \gamma} B$, then either $A \to^{\beta} B$ or $A \to^{\gamma} B$, so we can assume the former without loss of generality. By Fischer/Ladner rule (4), $\langle\beta\rangle X \in \mathrm{FL}(W)$, so we can apply the induction hypothesis to obtain $A \leqslant \langle\beta\rangle X$. Since $\langle\beta\rangle X \leqslant \langle\beta \cup \gamma\rangle X$, we have that $A \leqslant \langle\beta \cup \gamma\rangle X$.

(2) If $A \to^{\beta\gamma} B$, then there must exist a C such that $A \to^{\beta} C \to^{\gamma} B$. By the induction hypothesis, $C \leqslant \langle\gamma\rangle X$. By Fischer/Ladner rules (5) and (3), $\langle\gamma\rangle X \in \mathrm{FL}(W)$, so again by the induction hypothesis, $A \leqslant \langle\beta\rangle\langle\gamma\rangle X$. Thus $A \leqslant \langle\beta\gamma\rangle X$ by Axiom (5).

(3) There must be $A_1, \ldots, A_n$ such that

$$A = A_1 \to^{\beta} A_2 \to^{\beta} \cdots \to^{\beta} A_n = B.$$

Since $A_n = B \leqslant X$ and $X \leqslant \langle\beta^*\rangle X$ by Axiom (6), $A_n \leqslant \langle\beta^*\rangle X$. By Fischer/Ladner rule (6), $\langle\beta\rangle\langle\beta^*\rangle X \in \mathrm{FL}(W)$, and so by the induction hypothesis, $A_{n-1} \leqslant \langle\beta\rangle\langle\beta^*\rangle X$, and thus $A_{n-1} \leqslant \langle\beta^*\rangle X$ by Axiom (6). Continuing in this fashion we get $A = A_1 \leqslant \langle\beta^*\rangle X$.

Lemma 3. *For any $X \in \mathrm{FL}(W)$ and atom A,*

$$A \vDash X \text{ iff } A \leqslant X.$$

Proof. The proof is by induction on the complexity of X. The basis $X = P$ is immediate from the definition of $\vDash$. This leaves the three induction cases: (1) $X = Y \vee Z$, (2) $X = \neg Y$, (3) $X = \langle\alpha\rangle Y$. Case (1) is trivial and Case (2) is immediate from the observation that for any $X \in \mathrm{FL}(W)$ and atom A, either $A \leqslant X$ or $A \leqslant \neg X$. These two cases use the Fischer/Ladner rules (1) and (2).

(3) $A \leqslant \langle\alpha\rangle Y$ iff (by Lemma 2) $\exists B \leqslant Y\, A \to^{\alpha} B$, iff (by induction hypothesis) $\exists B$ $A \to^{\alpha} B$ and $B \vDash Y$, iff $A \vDash \langle\alpha\rangle Y$.

Since W is consistent, there is an atom $A \leqslant W$, and A is a state of $\mathcal{M}$. By Lemma 3, $A \vDash W$. This completes the proof of the theorem.

References

[1] F. Berman, A completeness technique for D-axiomatizable semantics, *Proc. 11th ACM Symp on Theory of Comp* (May 1979) 160–166.

[2] M.J. Fischer and R.E. Ladner, Propositional dynamic logic of regular programs, *J. Comput. System Sci* **18** (2) (1979) 194–211.

[3] D. Gabbay, Axiomatizations of logics of programs, unpublished manuscript (1977).

[4] J. Halpern, unpublished manuscript (1980).

[5] G. Mirkowska, Model existence theorem in algorithmic logic with nondeterministic programs, University of Warsaw, unpublished manuscript.

[6] H. Nishimura, Sequential method in propositional dynamic logic, *Acta Informatic.* **12** (1979) 377–400.

[7] R. Parikh, The completeness of Propositional Dynamic Logic, *Proc. 7th Symp. on Math. Found. of Comp. Sci.*, Zakopane, Poland (Sept. 1978) 403–415.

[8] R. Parikh, Propositional logics of programs, *Proc. 7th ACM Symp. on Principles of Programming Languages* (Jan. 1980) 186–192.

[9] V.R. Pratt, A practical decision method for Propositional Dynamic Logic, *Proc. 10th ACM Symp. on Theory of Computing* (May 1978) 326–337.

[10] V.R. Pratt, Models of program logics, *Proc. 20th IEEE Symp. on Foundations of Computer Science* (Oct. 1979) 115–122.

[11] K. Segerberg, A completeness theorem in the modal logic of programs, *Notices AMS* 24(6) (1977) A-522.