On models for propositional dynamic logic

P.M.W. Knijnenburg and J. van Leeuwen

RUU-CS-89-3
February 1989

Rijksuniversiteit Utrecht

Vakgroep informatica

Padualaan 14 3584 CH Utrecht
Corr. adres: Postbus 80.089, 3508 TB Utrecht
Telefoon 030-531454
The Netherlands

On models for propositional dynamic logic

P.M.W. Knijnenburg and J. van Leeuwen

RUU-CS-89-3
February 1989

Rijksuniversiteit Utrecht

Vakgroep informatica

Padualaan 14 3584 CH Utrecht
Corr. adres: Postbus 80.089, 3508 TB Utrecht
Telefoon 030-531454
The Netherlands

On models for propositional dynamic logic

P.M.W. Knijnenburg and J. van Leeuwen

Technical Report RUU-CS-89-3
February 1989

Department of Computer Science
University of Utrecht
P.O.Box 80.089, 3508 TB Utrecht
The Netherlands

On Models for Propositional Dynamic Logic

P.M.W. Knijnenburg J. van Leeuwen

Department of Computer Science, University of Utrecht
Padualaan 14, 3584 CH Utrecht, The Netherlands

Abstract

In this paper we study some foundational aspects of the theory of **PDL**. We prove a claim made by Parikh [12], namely, the existence of a Kripke model $\mathcal{U}$ that is universal in the sense that every other Kripke model $\mathcal{M}$ can be isomorphically embedded in it. Using this model we give different and particularly easy proofs of the Completeness Theorem for the Segerberg axiomatization of **PDL** and the Small Model Theorem. We also give an infinitary axiomatization for **PDL** and prove it complete using a syntax model $\mathcal{A}$, by a technique that is well-known from Modal Logic. We prove that $\mathcal{U}$ and $\mathcal{A}$ are isomorphic. Finally, we briefly turn to Dynamic Algebras and show that the characteristic algebra of $\mathcal{U}$ is initial in the class of $\star$-continuous Dynamic Algebras.

1 Introduction

Logics of Programs are formal systems for reasoning about the behavior of computer programs. In these formal systems, computer programs are viewed as a means to enable certain logical formulae. The formulae may be propositional or first order, giving rise to propositional and first order program logics, respectively. Pratt [13] recognized the possibility of modeling program logics by means of Modal Logic. His idea was fully developed by Fischer and Ladner [3] and many other authors; see Harel [6] for a rather complete survey of results up to 1984. If we view a program to be defined by its *input/output* (or *before/after*) behavior then Modal Logic provides a natural framework in which we can develop a program logic. Each program α is associated its "own" modal operator $\Diamond_\alpha$, or $\langle\alpha\rangle$. For a propositional program logic we can take a set of primitive programs and rules that determine how more complex programs can be built. With each rule we can define how the modal operator for the more complex program relates to the modal operators of the building blocks. In this approach the modal operators for the primitive programs are parameters. See Goldblatt [4] for an introduction to Modal Logic and its connection with logics of programs.

In this paper, we focus attention on a propositional program logic, namely Propositional Dynamic Logic or **PDL** in short. In **PDL** programs are regular expressions over a set of primitive programs; in particular, there is a nondeterministic looping operator $\star$

for programs. In the **PDL** framework, programs can enable propositions by means of a *possibility operator* $\Diamond$. Thus, when α is a program and ϕ is a proposition, $\alpha\Diamond\phi$ states "program α can terminate with ϕ holding upon termination". We will write $\langle\alpha\rangle\phi$ instead of $\alpha\Diamond\phi$, as is common in **PDL**. In this paper we study some foundational aspects of the syntax and semantics of **PDL** and focus attention on the consequences of introducing the looping operator $\star$. In a way, we argue that *looping is inherently infinitary*, thus giving rise to an infinitary axiomatization. The argument is split in two major parts, outlined below.

The logic is interpreted over Kripke models and we will prove the existence of a Kripke model $\mathcal{U}$ that is universal in the sense that every other Kripke model $\mathcal{M}$ can be isomorphically embedded in it. In this we prove a claim of Parikh [12]. The model $\mathcal{U}$ also appears to be a powerful tool in the study of the logic. We give two applications. First, Segerberg gave an axiomatization for the logic that is sound and complete, *i.e.*, validity and derivability coincide (*c.f.* [10]). We give another proof of the completeness of the system using the model $\mathcal{U}$, which is particularly easy. Secondly, we prove the corectness of the construction of a Small Model satisfying a formula ϕ iff ϕ is satisfiable as given by Sherman and Harel [6, 16]. Again, the proof uses the model $\mathcal{U}$ and is particularly straightforward.

Next, we define an infinitary axiomatization for **PDL** that we prove complete using a technique that is well-known from Modal Logic (see [4]), namely, by constructing a syntax model $\mathcal{A}$ for the logic. The state space of $\mathcal{A}$ constists precisely of the set of all maximal consistent sets of formulae. As a rather immediate consequence we deduce that $\mathcal{U} \cong \mathcal{A}$. This infinitary system can be viewed as the propositional variant of the infinitary axiomatization for first-order Dynamic Logic [4, 6, 11]. We also show that we can use this technique to define a syntax model from the finitary Segerberg system which is universal in the class of non-standard Kripke models.

In the last section we briefly introduce Dynamic Algebras and $\star$-continuous Dynamic Algebras. Each Kripke model $\mathcal{M}$ is associated a characteristic Dynamic Algebra $\overline{\mathcal{M}}$. We show the algebra $\overline{\mathcal{U}}$ to be initial in the class of $\star$-continuous Dynamic Algebras.

2 Preliminaries

In this section we review the syntax and semantics of **PDL**. For a more detailed treatment, see Harel [6] or Kozen and Tiuryn [11].

2.1 Syntax

The syntax of **PDL** is based on two disjoint sets of primitive symbols, namely the set

$$\Phi_0 = \{p_0, p_1, \ldots\}$$

of primitive *predicate symbols*, and the set

$$\Pi_0 = \{a_0, a_1, \ldots\}$$

of primitive *program symbols*. From these base sets we recursively define the sets of **PDL** propositions Φ and programs Π:

1. $\Phi_0 \subseteq \Phi$;
2. if $\phi, \psi \in \Phi$ then $\phi \vee \psi, \neg\phi \in \Phi$;
3. if $\alpha \in \Pi$ and $\phi \in \Phi$ then $\langle\alpha\rangle\phi \in \Phi$;
4. $\Pi_0 \subseteq \Pi$;
5. if $\alpha, \beta \in \Pi$ then $\alpha \cup \beta, \alpha;\beta, \alpha^\star \in \Pi$;
6. if $\phi \in \Phi$ then $\phi? \in \Pi$.

We abbreviate $\neg(\neg\phi \vee \neg\psi)$ to $\phi \wedge \psi$; $\neg\phi \vee \psi$ to $\phi \rightarrow \psi$; $(\phi \rightarrow \psi) \wedge (\psi \rightarrow \phi)$ to $\phi \leftrightarrow \psi$. We further abbreviate $\neg\langle\alpha\rangle\neg\phi$ to $[\alpha]\phi$.

2.2 Semantics

First we give an informal semantics for the above construction. The meaning of the propositional connectives is exactly like in ordinary, classical propositional logic **CPC**. Therefore, **PDL** can be seen as an extension of **CPC**, *i.e.*, all tautologies of **CPC** are valid **PDL** formulae. Primitive programs are exactly what their name suggests: uninterpreted programs or *input/output relations*, which is essentially the way we view programs in general. That is, programs are black boxes and their input/output behavior completely characterizes their relevant aspects; two programs are equivalent if and only if they constitute the same input/output relation. The meaning of the operator ; is program concatenation; thus, $\alpha;\beta$ means "first execute program α and then execute β". $\cup$ means nondeterministic choice; $\alpha \cup \beta$ means "choose nondeterministically program α or β and execute it". The $\star$-operator is a nondeterministic looping operator and $\alpha^\star$ means "execute α a nondeterministically chosen number of times". In the sequel we often abbreviate $\alpha;\alpha;\cdots;\alpha$ (n times) to α^n. Thus $\alpha^\star$ can be viewed as "choose n nondeterministically and execute α^n". The operator ? is a testing operator and $\phi?$ means "test ϕ and proceed if true".

The operator $\Diamond$ is the usual modal operator and the meaning of $\langle\alpha\rangle\phi$ is "program α can be executed with ϕ holding upon termination". Its dual, $[\alpha]\phi$, therefore means "whenever program α terminates, ϕ holds".

Formally, **PDL** formulae are interpreted over Kripke models.

Definition 2.1 *A* Kripke model *is a triple* $\mathcal{A} = (W^{\mathcal{A}}, \pi^{\mathcal{A}}, \rho^{\mathcal{A}})$ *where*

- $W^{\mathcal{A}}$ *is a set of states;*
- $\pi^{\mathcal{A}} : \Phi_0 \mapsto 2^{W^{\mathcal{A}}}$ *is an interpretation function for the primitive predicate symbols;*
- $\rho^{\mathcal{A}} : \Pi_0 \mapsto 2^{W^{\mathcal{A}} \times W^{\mathcal{A}}}$ *is an interpretation function for the primitive program symbols.*

Usually we write a Kripke model as $\mathcal{A} = (W, \pi, \rho)$ when no confusion can arise. We further use the terms "Kripke model", and "model" interchangeably. The interpretation functions extend to the whole sets Φ and Π:

- $\rho(\alpha \cup \beta) = \rho(\alpha) \cup \rho(\beta)$;
- $\rho(\alpha;\beta) = \rho(\alpha) \circ \rho(\beta)$, where $\circ$ is relation composition;
- $\rho(\alpha^*) = \bigcup_{i<\omega} \rho(\alpha^i)$, the reflexive transitive closure of $\rho(\alpha)$;
- $\rho(\phi?) = \{(s,s) \in W \times W \mid s \in \pi(\phi)\}$;
- $\pi(\phi \vee \psi) = \pi(\phi) \cup \pi(\psi)$;
- $\pi(\neg\phi) = W - \pi(\phi)$;
- $\pi(\langle\alpha\rangle\phi) = \{s \in W \mid \exists t \in W.((s,t) \in \rho(\alpha) \wedge t \in \pi(\phi))\}$;

We say that a proposition ϕ is *satisfiable* in a model $\mathcal{A}$ if and only if there exists a state s in $\mathcal{A}$ such that $s \in \pi(\phi)$ and we write $\mathcal{A}, s \models \phi$. We omit $\mathcal{A}$ when it is clear from the context. We say that ϕ is *$\mathcal{A}$-valid* and write $\mathcal{A} \models \phi$ if $\mathcal{A}, s \models \phi$ for each $s \in W$. We say that ϕ is *valid* and write $\models \phi$ if ϕ is $\mathcal{A}$-valid for every model $\mathcal{A}$. Clearly, ϕ is valid if and only if $\neg\phi$ is not satisfiable.

In the sequel of this paper we use $\phi, \psi, \ldots$ to denote propositions and $\alpha, \beta, \ldots$ to denote programs.

2.3 Axiomatization

We now present an axiomatization for **PDL** as proposed by Segerberg [17].

Definition 2.2 *The set of axioms AX for* **PDL** *contains*

1. *axioms for propositional logic;*
2. $\langle\alpha\rangle\phi \wedge [\alpha]\psi \rightarrow \langle\alpha\rangle(\phi \wedge \psi)$;
3. $\langle\alpha\rangle(\phi \vee \psi) \leftrightarrow \langle\alpha\rangle\phi \vee \langle\alpha\rangle\psi$;
4. $\langle\alpha \cup \beta\rangle\phi \leftrightarrow \langle\alpha\rangle\phi \vee \langle\beta\rangle\phi$;
5. $\langle\alpha;\beta\rangle\phi \leftrightarrow \langle\alpha\rangle\langle\beta\rangle\phi$;
6. $\langle\psi?\rangle\phi \leftrightarrow \psi \wedge \phi$;
7. $\phi \vee \langle\alpha\rangle\langle\alpha^*\rangle\phi \rightarrow \langle\alpha^*\rangle\phi$;
8. $\langle\alpha^*\rangle\phi \rightarrow \phi \vee \langle\alpha^*\rangle(\neg\phi \wedge \langle\alpha\rangle\phi)$.

In addition we have the following inference rules:

1. *modus ponens: from* ϕ, $\phi \to \psi$, *infer* ψ;

2. *modal generalization: from* ϕ, *infer* $[\alpha]\phi$, *for any* $\alpha \in \Pi$.

As usual, we define a *derivation* to be a finite sequence of well-formed formulae, each of which is an instance of an axiom or the conclusion of an inference rule whose premisses occur earlier in the derivation. The last formula occurring in the derivation is called the *conclusion of the derivation.* If, for any formula ϕ, there exists a derivation of which ϕ is the conclusion, we say that ϕ is *derivable* and write $\vdash \phi$.

Axioms 1–3 are not particular for **PDL** but hold in most modal systems. The dual of axiom 3 reads

$$[\alpha](\phi \to \psi) \to ([\alpha]\phi \to [\alpha]\psi)$$

which states that the logic is *normal* in the terminology of Modal Logic. Axiom 8 is called the *induction axiom,* and is better known in its dual form

$$\phi \wedge [\alpha^\star](\phi \to [\alpha]\phi) \to [\alpha^\star]\phi.$$

Note the resemblance between this axiom and the induction axiom in arithmetic. The intuition behind axiom 8 is that if a program $\alpha^\star$ enables a proposition ϕ, then the proposition is always true or there is a point in the looping of the program where the proposition becomes true for the first time.

Inspection of the system AX immediately gives us the next proposition.

Theorem 2.3 (Soundness Theorem) *If* $\vdash \phi$ *then* $\models \phi$.

A familiar fact of **PDL** is its lack of compactness. For an easy example, consider the infinite set Γ:

$$\begin{aligned} \Gamma &= \{\neg\phi, \neg\langle\alpha\rangle\phi, \neg\langle\alpha^2\rangle\phi, \ldots\} \cup \{\langle\alpha^\star\rangle\phi\} \\ &= \Delta \cup \{\langle\alpha^\star\rangle\phi\} \end{aligned}$$

Every finite subset $\Gamma' \subseteq \Gamma$ has a model: suppose $\langle\alpha^\star\rangle\phi \in \Gamma'$ and let i be the largest integer such that $\neg\langle\alpha^i\rangle\phi \in \Gamma'$. Then each model $\mathcal{M}$ that satisfies $\neg\langle\alpha^j\rangle\phi$ for $j \leq i$ and $\langle\alpha^{i+1}\rangle\phi$, satisfies Γ'. Yet the whole set Γ cannot have a model, for Δ is precisely the definition of $\neg\langle\alpha^\star\rangle\phi$. Note that this non-compactness property is essentially caused by the $\star$-operator.

3 A Universal Model Theorem for Kripke Models

In this section we establish a nontrivial property of Kripke models, namely the existence of an model $\mathcal{U}$ that is universal in the sense that every other model can be isomorphically embedded in it. In this, we prove a claim of Parikh [12], which seems not to have been developed in the literature. We also exhibit some immediate corollaries. We first establish some facts about models for **PDL**.

Definition 3.1 *For each model* $\mathcal{M}$ *the relation* $\equiv$ *on the state space* $W^{\mathcal{M}}$ *is defined by:*

$$s \equiv t \text{ iff } \mathcal{M}, s \models \phi \iff \mathcal{M}, t \models \phi.$$

For each model $\mathcal{M}$ we now define the *collapse of* $\mathcal{M}$ to be the model $\mathcal{M}_c = \mathcal{M}/\equiv$:

$$\begin{aligned} s_c &= \{t \mid s \equiv t\} \\ W^{\mathcal{M}_c} &= \{s_c \mid s \in W^{\mathcal{M}}\} \\ \pi^{\mathcal{M}_c}(p_i) &= \{s_c \mid s \in \pi^{\mathcal{M}}(p_i)\} \\ \rho^{\mathcal{M}_c}(a_j) &= \{(s_c, t_c) \mid (s,t) \in \rho^{\mathcal{M}}(a_j)\} \end{aligned}$$

The following lemma is immediate.

Lemma 3.2 *For each proposition* ϕ,

$$\mathcal{M}, s \models \phi \text{ iff } \mathcal{M}_c, s_c \models \phi.$$

The lemma in effect states that we only need to consider models of cardinality at most $\aleph_1$, that is, the cardinality of the power set of Φ.

Lemma 3.3 *For every model* $\mathcal{M}$ *and program* α,

1. *if* $(s,t) \in \rho(\alpha)$, *then* $\forall\phi.(\mathcal{M}, t \models \phi \Longrightarrow \mathcal{M}, s \models \langle\alpha\rangle\phi)$;
2. *if* $(s,t) \in \rho(\alpha)$, *then* $\forall\phi.(\mathcal{M}, s \models [\alpha]\phi \Longrightarrow \mathcal{M}, t \models \phi)$;
3. $\forall\phi.(\mathcal{M}, t \models \phi \Longrightarrow \mathcal{M}, s \models \langle\alpha\rangle\phi)$ *iff* $\forall\phi.(\mathcal{M}, s \models [\alpha]\phi \Longrightarrow \mathcal{M}, t \models \phi)$.

Proof.

Clauses (1) and (2) follow immediately from the definition of $\models$. For clause (3): $\forall\phi.(\mathcal{M}, s \models [\alpha]\phi \Longrightarrow \mathcal{M}, t \models \phi)$ iff $\forall\phi.(\mathcal{M}, t \not\models \phi \Longrightarrow \mathcal{M}, s \not\models [\alpha]\phi)$ iff $\forall\phi.(\mathcal{M}, t \models \neg\phi \Longrightarrow \mathcal{M}, s \models \neg\langle\alpha\rangle\neg\phi)$ iff $\forall\psi.(\mathcal{M}, t \models \psi \Longrightarrow \mathcal{M}, s \models \langle\alpha\rangle\psi)$. □

In the light of Lemma 3.3 we can define for each model $\mathcal{M}$ another model $\mathcal{M}_{ex}$, called the *extension of* $\mathcal{M}$, by:

$$\begin{aligned} W^{\mathcal{M}_{ex}} &= W^{\mathcal{M}}; \\ \pi^{\mathcal{M}_{ex}} &= \pi^{\mathcal{M}}; \\ \rho^{\mathcal{M}_{ex}}(a) &= \{(s,t) \mid \forall\phi(\mathcal{M}, s \models [a]\phi \Longrightarrow \mathcal{M}, t \models \phi)\} \text{ for } a \text{ primitive} \end{aligned}$$

By Lemma 3.3, $\rho^{\mathcal{M}}(a) \subseteq \rho^{\mathcal{M}_{ex}}(a)$ for each primitive program a. Note that $\rho^{\mathcal{M}}(a)$ need not equal $\rho^{\mathcal{M}_{ex}}(a)$. Consider for example the case in which $\mathcal{M}, s \models [a]\phi$ only if ϕ is valid. Then, for every $t \in W^{\mathcal{M}}$, $(s,t) \in \rho^{\mathcal{M}_{ex}}(a)$. Obviously, $\rho^{\mathcal{M}_{ex}}(a)$ can be substantially larger than $\rho^{\mathcal{M}}(a)$. We extend $\rho^{\mathcal{M}_{ex}}$ to the whole set Π in the usual way.

Lemma 3.4 *For each proposition* ϕ,

$$\mathcal{M}_{ex}, s \models \phi \text{ iff } \mathcal{M}, s \models \phi.$$

Proof.

($\Longleftarrow$) Since $\rho^{\mathcal{M}}(a) \subseteq \rho^{\mathcal{M}_{ex}}(a)$ for each primitive program a, it is easy to see that for each $\alpha \in \Pi$, $\rho^{\mathcal{M}}(\alpha) \subseteq \rho^{\mathcal{M}_{ex}}(\alpha)$. The proof proceeds by induction on the complexity of ϕ. The only non-trivial case is $\phi = \langle\alpha\rangle\psi$, which follows from the inclusion given above.

($\Longrightarrow$) Let $\mathcal{M}_{ex}, s \models \phi$. We define the mapping $R : \Pi \mapsto 2^{W^{\mathcal{M}} \times W^{\mathcal{M}}}$ by:

$$\begin{aligned} R(\alpha) &= \{(s,t) \mid \forall\psi.(\mathcal{M}, s \models [\alpha]\psi \Longrightarrow \mathcal{M}, t \models \psi)\} \\ &= \{(s,t) \mid \forall\psi.(\mathcal{M}, t \models \psi \Longrightarrow \mathcal{M}, s \models \langle\alpha\rangle\psi\} \end{aligned}$$

for $\alpha \in \Pi$. Note that, by Lemma 3.3(3), we may use both conditions interchangeably in the definition of R.

Claim 1. $\mathcal{M}, s \models \phi$ iff $\mathcal{M}, s \models_R \phi$, where $\models_R$ is defined as the relation $\models$ except that we use $R(\alpha)$ instead of $\rho(\alpha)$.

Proof of claim. Induction on the structure of ϕ. The only non-trivial case is $\phi = \langle\alpha\rangle\psi$. Let $\mathcal{M}, s \models \langle\alpha\rangle\psi$. Then there exists a state t such that $\mathcal{M}, t \models \psi$ and $(s,t) \in \rho(\alpha)$. But then $(s,t) \in R(\alpha)$ by the construction of R and $\mathcal{M}, s \models_R \langle\alpha\rangle\psi$. Conversely, let $\mathcal{M}, s \models_R \langle\alpha\rangle\psi$; then there is a state t such that $(s,t) \in R(\alpha)$ and $t \models \psi$. Suppose that there exists no state t such that $(s,t) \in \rho(\alpha)$ and $\mathcal{M}, t \models \psi$. Then $\mathcal{M}, s \models [\alpha]\neg\psi$ and, by the definition of R, if $(s,t) \in R(\alpha)$, then $t \models \neg\psi$. Contradiction.

Claim 2. For each $\alpha \in \Pi$, $\rho^{\mathcal{M}_{ex}}(\alpha) \subseteq R(\alpha)$.

Proof of claim. Induction on the complexity of α. For α primitive, the claim holds by definition. Next we consider more complex programs α.

Case 1: $\alpha = \beta \cup \gamma$.

Clearly, $\rho(\beta \cup \gamma) = \rho(\beta) \cup \rho(\gamma) \subseteq R(\beta) \cup R(\gamma)$. The last union equals:

$$\{(s,t) \mid \forall\phi.(t \models \phi \Longrightarrow s \models \langle\beta\rangle\phi) \vee \forall\phi.(t \models \phi \Longrightarrow s \models \langle\gamma\rangle\phi)\}$$

It is easy to see that this set is contained in:

$$\{(s,t) \mid \forall\phi.(t \models \phi \Longrightarrow s \models \langle\beta\rangle\phi \vee s \models \langle\gamma\rangle\phi)\}$$

which is $R(\beta \cup \gamma)$.

Case 2: $\alpha = \beta;\gamma$.

$\rho(\beta;\gamma) = \rho(\beta) \circ \rho(\gamma) \subseteq R(\beta) \circ R(\gamma)$. Now,

$$R(\beta) \circ R(\gamma) = \{(s,t) \mid \exists u.((s,u) \in R(\beta) \wedge (u,t) \in R(\gamma))\}$$

Let $(s,t) \in R(\beta) \circ R(\gamma)$. Then, for each ϕ,

$$t \models \phi \Longrightarrow s \models \langle\beta\rangle\langle\gamma\rangle\phi$$

hence $(s,t) \in R(\beta;\gamma)$ and $R(\beta) \circ R(\gamma) \subseteq R(\beta;\gamma)$.

Case 3: $\alpha = \beta^\star$.
By the former argument we get

$$\rho(\beta^n) \subseteq R(\beta^n)$$

for each $n < \omega$. We further have, for each $n < \omega$,

$$R(\beta^n) \subseteq R(\beta^\star)$$

Suppose $(s,t) \in R(\beta^n)$; then $t \vDash \psi \Longrightarrow s \vDash \langle\beta^n\rangle\psi$ for all ψ. Surely $t \vDash \psi \Longrightarrow s \vDash \langle\beta^\star\rangle\psi$ for all ψ, by the definition of $\rho(\beta^\star)$. Hence $(s,t) \in R(\beta^\star)$. Hence, by induction on n,

$$\rho(\beta^\star) = \bigcup_{i<\omega} \rho(\beta^i) \subseteq \bigcup_{i<\omega} R(\beta^i) \subseteq R(\beta^\star).$$

Note that this is the place where we use the infinitary properties of $\beta^\star$.
Case 4: $\alpha = \psi?$.
Clearly, $\rho(\psi?) = R(\psi?)$ follows immediately by the definitions of ρ and R.

The proof of the lemma now follows by induction on the structure of ϕ. Again, the only non-trivial case is $\phi = \langle\alpha\rangle\psi$. If $\mathcal{M}_{ex}, s \vDash \langle\alpha\rangle\psi$ then, by claim 2, $\mathcal{M}, s \vDash_R \langle\alpha\rangle\psi$ and hence, by claim 1, $\mathcal{M}, s \vDash \langle\alpha\rangle\psi$. □

Next we define, for each model $\mathcal{M}$, the model $\widetilde{\mathcal{M}}$ by replacing every state in $W^{\mathcal{M}}$ by the set of propositions that hold at that state. We denote the state in $W^{\widetilde{\mathcal{M}}}$ corresponding to s by $\tilde{s}$. It is easy to see that

$$\mathcal{M}, s \vDash \phi \Longleftrightarrow \widetilde{\mathcal{M}}, \tilde{s} \vDash \phi \Longleftrightarrow \phi \in \tilde{s}$$

for each proposition $\phi \in \Phi$.

Definition 3.5 *For each model $\mathcal{M}$, the* canonical model for $\mathcal{M}$ *is* $[\mathcal{M}] = (\widetilde{\mathcal{M}_c})_{ex}$.

Theorem 3.6 *For each proposition ϕ and each model $\mathcal{M}$, $\mathcal{M}, s \vDash \phi$ iff $[\mathcal{M}], [s] \vDash \phi$.*

Proof.

Immediate from Lemma 3.2 and Lemma 3.4. □

We can now define a universal Kripke model $\mathcal{U}$. Consider the class $\mathcal{K}$ of all Kripke models. For each $\mathcal{M} \in \mathcal{K}$ we define the mapping $\theta_{\mathcal{M}} : W^{\mathcal{M}} \mapsto W^{\mathcal{U}}$ by:

$$\theta_{\mathcal{M}}(s) = \{\phi \mid \mathcal{M}, s \vDash \phi\}.$$

We let the set of states $W^{\mathcal{U}}$ of the universal model be exactly the set of all subsets of Φ that can be obtained this way (when $\mathcal{M}$ ranges over all Kripke models). That is, for $\Psi \subseteq \Phi$, $\Psi \in W^{\mathcal{U}}$ iff $\Psi = \theta_{\mathcal{M}}(s)$ for some model $\mathcal{M}$ and state $s \in W^{\mathcal{M}}$. We define $\pi^{\mathcal{U}}$ by:

$$\pi^{\mathcal{U}}(p_i) = \{s \in W^{\mathcal{U}} \mid p_i \in s\}$$

for $0 \leq i < \omega$. The interpretation for the primitive programs is defined as:

$$\rho^{\mathcal{U}}(a_j) = \{(s,t) \in W^{\mathcal{U}} \times W^{\mathcal{U}} \mid \forall \phi.([a_j]\phi \in s \Longrightarrow \phi \in t)\}$$

for $0 \leq j < \omega$. Note that the states of $\mathcal{U}$ consist of all semantically consistent complete sets of formulae.

We can also describe the Universal Model as the model which results from "pasting together" all canonical models $[\mathcal{M}]$ for all Kripke models $\mathcal{M}$. All states in $\mathcal{U}$ are "copies" of states in some canonical model $[\mathcal{M}]$.

Lemma 3.7 *For each canonical model* $[\mathcal{M}]$ *and* $\alpha \in \Pi$, $\rho^{[\mathcal{M}]}(\alpha) \subseteq \rho^{\mathcal{U}}(\alpha)$.

Proof.

It follows immediately from the definitions of $\rho^{[\mathcal{M}]}$ and $\rho^{\mathcal{U}}$ that, for primitive a, $\rho^{[\mathcal{M}]}(a) \subseteq \rho^{\mathcal{U}}(a)$. The lemma follows. □

Lemma 3.8 *Consider the universal model* $\mathcal{U}$.

1. *For each* $\phi \in \Phi$ *and* $\alpha \in \Pi$,

$$\langle\alpha\rangle\phi \in s \Longleftrightarrow \exists t.(s,t) \in \rho(\alpha) \wedge \phi \in t.$$

2. *For each* $\phi \in \Phi$,

$$\mathcal{U}, s \vDash \phi \text{ if and only if } \phi \in s.$$

Proof.

1. ($\Longrightarrow$) Let $\langle\alpha\rangle\phi \in s$. Then there exists a canonical model $[\mathcal{M}]$ and a state $[s] \in W^{[\mathcal{M}]}$ such that $\langle\alpha\rangle\phi \in [s]$. Then there exists a $[t] \in W^{\mathcal{M}]}$ such that $([s],[t]) \in \rho^{\mathcal{M}}(\alpha)$ and $\phi \in [t]$. Hence, by Lemma 3.7, $(s,t) \in \rho^{\mathcal{U}}(\alpha)$ and $\phi \in t$.

   ($\Longleftarrow$) Again define the function $R : \Pi \mapsto 2^{W \times W}$ as in Theorem 3.4 except that we use $\in$ instead of $\vDash$. By the proof of that theorem, $\rho(\alpha) \subseteq R(\alpha)$. Hence, if $(s,t) \in \rho(\alpha)$ and $\phi \in t$, then $(s,t) \in R(\alpha)$ and by the definition of R, $\langle\alpha\rangle\phi \in s$.

2. The proof is by induction on the structure of ϕ. For ϕ primitive, the lemma holds by definition.

   Case 1: $(\phi = \psi \vee \chi)$

   $s \vDash \psi \vee \chi$ iff $s \vDash \psi$ or $s \vDash \chi$ iff, by the induction hypothesis, $\psi \in s$ or $\chi \in s$ iff $\psi \vee \chi \in s$ by the maximality of s.

   Case 2: $(\phi = \neg\psi)$

   Similar.

   Case 3: $(\phi = \langle\alpha\rangle\psi)$

   $s \vDash \langle\alpha\rangle\psi$ iff there is a state $t \in W$ such that $(s,t) \in \rho(\alpha)$ and $t \vDash \psi$ iff $\psi \in t$ by the induction hypothesis and $\langle\alpha\rangle\phi \in s$ by the first part of the lemma.

The following theorem is an immediate consequence of the lemma.

Theorem 3.9 *There exists a universal Kripke model $\mathcal{U} = (W^{\mathcal{U}}, \pi^{\mathcal{U}}, \rho^{\mathcal{U}})$ such that for each Kripke model $\mathcal{M} = (W^{\mathcal{M}}, \pi^{\mathcal{M}}, \rho^{\mathcal{M}})$ there exists an embedding $\theta_{\mathcal{M}} : W^{\mathcal{M}} \mapsto W^{\mathcal{U}}$ such that $\mathcal{M}, s \models \phi$ iff $\mathcal{U}, \theta_{\mathcal{M}}(s) \models \phi$ for each well-formed formula ϕ.*

Proof.

The model $\mathcal{U}$ constructed above and mappings $\theta_{\mathcal{M}}$ for each $\mathcal{M}$ are the required model and mappings. □

We give two immediate consequences of Theorem 3.9 which will be instrumental for obtaining the results of the next section.

Lemma 3.10 *1. For all propositions ϕ, ϕ is satisfiable if and only if ϕ is $\mathcal{U}$-satisfiable.*

2. For all propositions ϕ, ϕ is valid if and only if ϕ is $\mathcal{U}$-valid.

4 Applications

In this section we prove the completeness of the system AX and the correctness of a construction for a Small Model using the Universal Model $\mathcal{U}$.

4.1 Completeness of AX

To prove completeness of AX we adapt the Lindenbaum construction [1] to PDL: We impose a Boolean algebra structure on the state space $W^{\mathcal{U}}$ of $\mathcal{U}$. With each proposition ϕ we associate the set of states that satisfy ϕ:

$$|\phi| = \{s \in W \mid s \models \phi\}.$$

Let P be the set of all such $|\phi|$. We define a partial ordering $\leqslant$ on P:

$$|\phi| \leqslant |\psi| \text{ iff } \vdash \phi \rightarrow \psi.$$

Lemma 4.1 *$\mathcal{B} = \langle P, \leqslant \rangle$ is a complemented distributive lattice, that is, a Boolean algebra.*

Proof.

By propositional reasoning we have

$$\vdash \psi \rightarrow \mathit{true}$$

$$\vdash \mathit{false} \rightarrow \psi$$

for all propositions ψ. Hence we can take $|\mathit{true}| = 1$ and $|\mathit{false}| = 0$ in $\mathcal{B}$.

Let $|\phi| \in P$. Then its complement, $|\phi|^c$, is defined as:

$$\begin{aligned} |\phi|^c &= \{s \mid s \vDash \phi\}^c \\ &= \{s \mid s \nvDash \phi\} \\ &= \{s \mid s \vDash \neg\phi\} \\ &= |\neg\phi| \end{aligned}$$

and $|\neg\phi| \in P$.

Let $|\phi|, |\psi| \in P$. Then:

$$\begin{aligned} |\phi| \cap |\psi| &= \{s \mid s \vDash \phi\} \cap \{s \mid s \vDash \psi\} \\ &= \{s \mid s \vDash \phi \wedge s \vDash \psi\} \\ &= \{s \mid s \vDash \phi \wedge \psi\} \\ &= |\phi \wedge \psi| \end{aligned}$$

Hence $|\phi| \cap |\psi| \in P$. By propositional reasoning,

$$\vdash (\phi \wedge \psi) \rightarrow \phi \text{ and } \vdash (\phi \wedge \psi) \rightarrow \psi.$$

Hence $|\phi \wedge \psi|$ is a lower bound for $\{|\phi|, |\psi|\}$. Suppose $|\chi|$ is a lower bound too. Then $\vdash \chi \rightarrow \phi$ and $\vdash \chi \rightarrow \psi$. Hence $\vdash \chi \rightarrow (\phi \wedge \psi)$. This shows that $|\phi \wedge \psi|$ is the greatest lower bound, *i.e.* the infimum of $\{|\phi|, |\psi|\}$. Similarly, $|\phi \vee \psi|$ is the supremum of $\{|\phi|, |\psi|\}$. Thus $\mathcal{B}$ is a lattice.

Let $|\phi|, |\psi|, |\chi| \in P$. Then $|(\phi \wedge \psi) \vee \chi| \in P$ and because

$$\vdash ((\phi \wedge \psi) \vee \chi) \leftrightarrow ((\phi \vee \chi) \wedge (\psi \vee \chi))$$

we get from the Soundness Theorem,

$$|(\phi \wedge \psi) \vee \chi| = |(\phi \vee \chi) \wedge (\psi \vee \chi)|.$$

This shows that $\mathcal{B}$ is a complemented distributive lattice. □

Lemma 4.2 *In the Boolean algebra $\mathcal{B}$,*

1. $|\phi| = 1$ *if and only if* $\vdash \phi$;
2. $|\psi| = 0$ *if and only if* $\vdash \neg\psi$.

Proof.

1. Let $|\phi| = 1$. Then for each $|\psi| \in P$, $|\psi| \leqslant |\phi|$. Hence, for each $|\psi|$, $\vdash \psi \rightarrow \phi$. Choose ψ so that $\vdash \psi$, then , by modus ponens, $\vdash \phi$. Conversely, suppose $\vdash \phi$. Then, for each ψ, $\vdash \psi \rightarrow \phi$. Hence, for each ψ, $|\psi| \leqslant |\phi|$, so $|\phi| = 1$ in $\mathcal{B}$.
2. Similar. □

Lemma 4.3 *For all proposition ϕ, if $\mathcal{U} \vDash \phi$ then $\vdash \phi$.*

Proof.

Suppose that ϕ is not provable in the system AX. Then, by lemma 4.2, in the Lindenbaum algebra $\mathcal{B}$, $|\phi| \neq 1$ and so $|\neg\phi| \neq 0$. Hence there exists a state $s \in |\neg\phi|$ such that $\mathcal{U}, s \models \neg\phi$. Hence ϕ is not $\mathcal{U}$-valid. □

Theorem 4.4 (Completeness Theorem) $\models \phi$ *if and only if* $\vdash \phi$.

Proof. One direction is the Soundness Theorem. The other direction follows from Lemmas 3.10 and 4.3. □

4.2 The Small Model theorem

We find another application of Theorem 3.9 in a different proof of the Small Model theorem. This theorem is one of the basic results of the theory of **PDL** and was first discovered by Fischer and Ladner [3]. It states that every proposition ϕ that is satisfiable, is satisfiable in a model with $2^{|\phi|}$ states. This fact immediately gives rise to a naïve doubly-exponential time decision procedure for the validity problem for **PDL**: to check whether ϕ is valid, generate all models with $2^{|\neg\phi|}$ states and cycle through them in search for a model that satisfies $\neg\phi$. If such a model doesn't exists, then ϕ is valid. Sherman and Harel [6, 16] proved the existence of a singly-exponential time procedure by constructing a model $\mathcal{A}_\phi$ that satisfies ϕ iff ϕ is satisfiable, following an idea of Pratt [14]. Thus one can construct a model in polynomial time and check whether this model satisfies $\neg\phi$ in exponential time.

We first need a notion of the "subformulae" of a **PDL** formula ϕ. This concept is captured by the Fischer-Ladner closure of ϕ [3].

Definition 4.5 *Let $\phi \in \Phi$ be a* **PDL** *formula. The* Fischer-Ladner closure of ϕ, *denoted by $FL(\phi)$, is the smallest set S of formulae containing ϕ and satisfying the following closure rules for all $a \in \Pi_0$, $\alpha, \beta \in \Pi$ and $\psi, \chi \in \Phi$:*

$$\begin{aligned}
\neg\psi \in S &\implies \psi \in S \\
\psi \vee \chi \in S &\implies \psi, \chi \in S \\
\langle a \rangle \psi \in S &\implies \psi \in S \\
\langle \alpha\beta \rangle \psi \in S &\implies \langle \alpha \rangle \langle \beta \rangle \psi \in S \\
\langle \alpha \cup \beta \rangle \psi \in S &\implies \langle \alpha \rangle \psi, \langle \beta \rangle \psi \in S \\
\langle \alpha^* \rangle \psi \in S &\implies \psi, \langle \alpha \rangle \langle \alpha^* \rangle \psi \in S \\
\langle \psi? \rangle \chi \in S &\implies \psi, \chi \in S
\end{aligned}$$

The Fischer-Ladner closure of ϕ is the set of all "subformulae" that are relevant for the meaning of ϕ. The set $FL(\phi)$ induces an equivalence relation $\equiv_\phi$ on the state space W of any model $\mathcal{M}$:

$$s \equiv_\phi t \text{ iff } \forall \psi \in FL(\phi).(s \models \psi \iff t \models \psi)$$

In other words, we "collapse" s and t if they are not distinguishable by any formula of $FL(\phi)$. We now define the quotient model $\mathcal{M}/FL(\phi)$:

$$[s] \;=\; \{t \mid s \equiv_\phi t\}$$

$$
\begin{aligned}
W^{\mathcal{M}/FL(\phi)} &= \{[s] \mid s \in W^{\mathcal{M}}\} \\
\pi^{\mathcal{M}/FL(\phi)}(p_i) &= \{[s] \mid s \in \pi^{\mathcal{M}}(p_i)\} \text{ for all } p_i \in \Phi_0 \\
\rho^{\mathcal{M}/FL(\phi)}(a_j) &= \{([s],[t]) \mid (s,t) \in \rho^{\mathcal{M}}(a_j)\} \text{ for all } a_j \in \Pi_0
\end{aligned}
$$

$\pi^{\mathcal{M}/FL(\phi)}$ and $\rho^{\mathcal{M}/FL(\phi)}$ are extended inductively to Π and Φ in the usual way. The following lemma, called the *Filtration Lemma*, is crucial for the theorem:

Lemma 4.6 (Filtration Lemma) *For all $\psi \in FL(\phi)$:*

1. *if $\psi = \langle\alpha\rangle\chi$ then $\forall s,t \in W^{\mathcal{M}}\{(s,t) \in \rho^{\mathcal{M}}(\alpha) \Longrightarrow ([s],[t]) \in \rho^{\mathcal{M}/FL(\phi)}(\alpha)\}$;*
2. *for all states s: $\mathcal{M}, s \models \psi \Longleftrightarrow \mathcal{M}/FL(\phi), [s] \models \psi$.*

Proof.

Tedious but straightforward induction on the structure of ψ; see [3, 4] for details. □

We now consider the quotient model $\mathcal{U}/FL(\phi)$.

Lemma 4.7 *For each $\psi \in FL(\phi)$*

$$\psi \text{ is satisfiable iff } \psi \text{ is } \mathcal{U}/FL(\phi)\text{-satisfiable.}$$

Proof. The lemma follows from Lemma 3.10 and the Filtration Lemma. □

Next we give another representation for the states of the quotient model $\mathcal{U}/FL(\phi)$: for each $[s] \in W^{\mathcal{U}/FL(\phi)}$, let $\tilde{s}$ be the set

$$\tilde{s} = \{\psi \mid [s] \models \psi \text{ and } \psi \in FL(\phi)\} \cup \{\neg\psi \mid [s] \models \neg\psi \text{ and } \psi \in FL(\phi)\}$$

That is, $\tilde{s}$ is the set of formulae from $FL(\phi)$ that hold at $[s]$ together with the negations of the formulae from $FL(\phi)$ that don't hold. We define the model $\mathcal{U}_\phi$ by mapping in the filtration model $\mathcal{U}/FL(\phi)$ each state $[s]$ onto $\tilde{s}$. The interpretation functions are adapted in the obvious way. From this construction we immediately get the following lemma.

Lemma 4.8 *For each formula $\psi \in FL(\phi)$ and $[s] \in W^{\mathcal{U}/FL(\phi)}$,*

$$\mathcal{U}/FL(\phi), [s] \models \psi \text{ iff } \mathcal{U}_\phi, \tilde{s} \models \psi \text{ iff } \psi \in \tilde{s}.$$

Theorem 4.9 *For each formula $\psi \in FL(\phi)$,*

$$\psi \text{ is satisfiable iff } \psi \in \tilde{s}$$

for some state $\tilde{s} \in \mathcal{U}_\phi$.

Proof.

Immediate from Lemmas 4.7 and 4.8. □

The sets of formulae $\tilde{s}$ are called *atoms of $FL(\phi)$* and play a crucial role in the definition of the model $\mathcal{A}_\phi$. For the definition of $\mathcal{A}_\phi$ we follow the exposition in [6].

Definition 4.10 *Let Z be the set of* **PDL** *formulae in which all formulae of $FL(\phi)$ and their negations occur. Then an* atom of $FL(\phi)$ *is defined to be a subset $A \subseteq Z$ such that for every $\alpha, \beta \in \Pi$ and $\psi, \chi \in \Phi$:*

if $\neg\psi \in Z$, then $\psi \in A$ iff $\neg\psi \notin A$
if $\psi \vee \chi \in Z$, then $\psi \vee \chi \in A$ iff $\psi \in A$ or $\chi \in A$
if $\langle\alpha\beta\rangle\psi \in Z$, then $\langle\alpha\beta\rangle\psi \in A$ iff $\langle\alpha\rangle\langle\beta\rangle\psi \in A$
if $\langle\alpha \cup \beta\rangle\psi \in Z$, then $\langle\alpha \cup \beta\rangle\psi \in A$ iff $\langle\alpha\rangle\psi \in A$ or $\langle\beta\rangle\psi \in A$
if $\langle\alpha^*\rangle\psi \in Z$, then $\langle\alpha^*\rangle\psi \in A$ iff $\psi \in A$ or $\langle\alpha\rangle\langle\alpha^*\rangle\psi \in A$
if $\langle\psi?\rangle\chi \in Z$, then $\langle\psi?\rangle\chi \in A$ iff $\psi \in A$ and $\chi \in A$.

Note that for all $\psi \in FL(\phi)$, either ψ or $\neg\psi$ is contained in each atom. Denote the set of all atoms of $FL(\phi)$ by $At(\phi)$. From the definition of atoms it follows that an $A \in At(\phi)$ is free of "obvious" or internal contradictions. In the construction of the model $\mathcal{A}_\phi$ we will eliminate the "nonobvious" or external contradictions also. This model will be constructed in phases. For the definition of the interpretation functions π and ρ we limit ourself, without loss of generality, to the primitive predicate and program symbols occurring in ϕ.

$\mathcal{A}_0 = (W_0, \pi_0, \rho_0)$ is defined by:

- $W_0 = At(\phi)$;
- $\pi_0 : \Phi_0 \mapsto 2^{W_0}$ by $A \in \pi_0(p)$ iff $p \in A$;
- $\rho_0 : \Pi_0 \mapsto 2^{W_0 \times W_0}$ by $(A, B) \in \rho_0(a)$ iff
  1. there is a $\langle a\rangle\psi \in A$ with $\psi \in B$, and
  2. for every $[a]\psi \in A$, $\psi \in B$.

For $i > 0$, $\mathcal{A}_{i+1} = (W_{i+1}, \pi_{i+1}, \rho_{i+1})$ is defined by

- $W_{i+1} = \{A \mid A \in W_i$, and for every $\langle\alpha\rangle\psi \in A$, there is $B \in W_i$ with $(A, B) \in \rho'_i(\alpha)$ and $\psi \in B\}$;
- $\pi_{i+1}(p) = \pi_i(p) \cap W_{i+1}$;
- $\rho_{i+1}(a) = \rho_i(a) \cap (W_{i+1} \times W_{i+1})$.

Here ρ'_i is the ordinary extension of ρ_i to Π, except that for $\psi \in Z$ we define $\rho'_i(\psi?) = \{(A, A) \mid \psi \in A\}$. The unprimed ρ is the usual extension.

It follows from the finiteness of $At(\phi)$ and the fact that $W_{i+1} \subseteq W_i$ that there is a j for which the construction closes up; *i.e.* $\mathcal{A}_i = \mathcal{A}_j$ for each $i > j$. Accordingly, set $\mathcal{A}_\phi = \mathcal{A}_j$.

The following lemma is the main technical lemma we need for our final result.

Lemma 4.11 *For every $A \in W^{\mathcal{A}_\phi}$,*

1. *for each* $\langle\alpha\rangle\psi \in FL(\phi)$,
   $\langle\alpha\rangle\psi \in A$ *iff there exists a* $B \in W^{\mathcal{A}_\phi}$ *with* $(A, B) \in \rho(\alpha)$ *and* $\psi \in B$;

2. *for each* $\psi \in FL(\phi)$,
   $\psi \in A$ *iff* $\mathcal{A}_\phi, A \models \psi$.

Proof.

The proof proceeds by simultaneous induction on the structure of α in (1) and the structure of ψ in (2). See [16] for details. □

Theorem 4.12 (Small Model Theorem) *For all* $\psi \in FL(\phi)$, ψ *is satisfiable iff* $\psi \in A$ *for some* $A \in W^{\mathcal{A}_\phi}$.

Proof.

In the light of Theorem 4.9, we only need to prove that $W^{\mathcal{U}_\phi} = W^{\mathcal{A}_\phi}$, from which the theorem follows.

- $W^{\mathcal{A}_\phi} \subseteq W^{\mathcal{U}_\phi}$: immediate from the construction of $\mathcal{U}_\phi$;
- suppose there exists an atom $A \in W^{\mathcal{U}_\phi}$ and $A \notin W^{\mathcal{A}_\phi}$. As we have started from the set of all atoms in W_0, there exists a phase i in which the first such atom is removed from W_{i+1}. Inspection of the algorithm shows that this can only happen if there exists a formula $\langle\alpha\rangle\psi \in A$ such that there exists no $B \in W_i$ with $(A, B) \in \rho_i'(\alpha)$ and $\psi \in B$. But $A \in W^{\mathcal{U}_\phi}$ and hence there exists a state $B \in W^{\mathcal{U}_\phi}$ with $(A, B) \in \rho(\alpha)$ and $\psi \in B$. Because A is the first state to be removes, $B \in W_i$. Contradiction. □

5 An infinitary axiom system

Intuitively, the nature of the $\star$-operator requires an *infinitary* axiom system. We define the system AX_∞ as such an infinitary system. The induction axiom is replaced by an inference rule with an infinite set of premisses.

Definition 5.1 *The infinitary axiom system* AX_∞ *contains the following axioms.*

1. *All* **PDL** *axioms, except the Induction Axiom;*
2. $[\alpha^\star]\phi \rightarrow [\alpha^i]\phi$, *for each* $i < \omega$;

In addition, we have the following inference rules:

1. *modus ponens: from* ϕ, $\phi \rightarrow \psi$, *infer* ψ;
2. *modal generalization: from* ϕ, *infer* $[\alpha]\phi$, *for any* $\alpha \in \Pi$;
3. ∞*-rule: from* $\{\psi \rightarrow [\beta; \alpha^i]\phi\}_{i<\omega}$, *infer* $\psi \rightarrow [\beta; \alpha^\star]\phi$.

In a way, we treat $[\alpha^*]\phi$ as an "abbreviation" for $\bigwedge_{i<\omega}[\alpha^i]\phi$. By contraposition, we have, for each $i < \omega$,

$$\langle\alpha^i\rangle\phi \to \langle\alpha^*\rangle\phi.$$

We define a derivation in AX_∞ to be a countable sequence of well-formed formulae, each of which is either an instance of an axiom or the conclusion of an inference rule whose premisses occur earlier in the sequence. The last formula in the sequence is called the conclusion of the derivation and any formula ϕ for which such a derivation exists is called derivable or provable and we write $\vdash_\infty \phi$.

From the Soundness Theorem for AX, we immediately get a Soundness Theorem for AX_∞.

Theorem 5.2 (Soundness Theorem) *If $\vdash_\infty \phi$, then $\models \phi$.*

In both systems, AX and AX_∞, derivability of formulae of the form $[\alpha^*]\phi$ is closely related, as the following theorem shows; a proof of the theorem can be found in [7].

Theorem 5.3 1. *In the infinitary system AX_∞, the induction axiom is derivable.*

2. *In the Segerberg system AX, $\vdash [\alpha^*](\phi \to [\alpha]\phi) \to (\phi \to [\alpha^n]\phi)$ for each $n < \omega$.*

We next give some definitions. Let $\mathrm{Pr}(AX_\infty) = \{\phi \mid \vdash_\infty \phi\}$ be the set of all provable formulas of the axiom system AX_∞. For any subset $\Sigma \subseteq \Phi$, let $\overline{\Sigma}$ be the union $\Sigma \cup \mathrm{Pr}(AX_\infty)$ closed under modus ponens and ∞-rule. Σ is a *theory* if $\Sigma = \overline{\Sigma}$. Intuitively, $\overline{\Sigma}$ contains all immediate consequences of Σ; in particular, if $\{[\alpha^i]\phi \mid i < \omega\} \subseteq \Sigma$, then $[\alpha^*]\phi \in \overline{\Sigma}$.

Definition 5.4 *Let Σ be a set of formulae and ϕ a formula.*

1. *$\Sigma \vdash_\infty \phi$ if and only if ϕ belongs to every theory that contains Σ.*
2. *We say that Σ is* inconsistent *iff $\Sigma \vdash_\infty$ false.*
3. *We say that Σ is* consistent *iff Σ is not inconsistent.*
4. *Σ is* maximally consistent *iff Σ is consistent and for each $\phi \in \Phi$, either ϕ or $\neg\phi \in \Sigma$.*

We give some useful lemmas.

Lemma 5.5 *Let Σ be a maximally consistent theory. Then $\langle\alpha^*\rangle\phi \in \Sigma$ implies $\langle\alpha^m\rangle\phi \in \Sigma$ for some $m < \omega$.*

Lemma 5.6 *Let Σ be a theory. Then $\Sigma \vdash_\infty \phi$ iff $\phi \in \Sigma$.*

Theorem 5.7 *$\Sigma \cup \{\phi\} \vdash_\infty \psi$ if and only if $\Sigma \vdash_\infty \phi \to \psi$.*

Proof.

Suppose that $\Sigma \cup \{\phi\} \vdash_\infty \psi$. Let

$$\Delta = \{\psi' \mid \Sigma \vdash_\infty \phi \to \psi'\}$$

We will show that Δ is a theory containing $\Sigma \cup \{\phi\}$. Since $\psi' \to (\phi \to \psi')$ is a tautology, $\psi' \in \Delta$ in case $\psi' \in \Sigma$ or $\vdash_\infty \psi'$. Since $\phi \to \phi$ is a tautology, $\phi \in \Delta$. Hence $\Sigma \cup \{\phi\} \subseteq \Delta$.

From the tautology

$$(\phi \to \phi_1 \to ((\phi \to (\phi_1 \to \phi_2)) \to (\phi \to \phi_2)$$

we deduce that Δ is closed under modus ponens.

Finally, suppose that

$$\{\phi_1 \to [\beta;\alpha^n]\phi_2 \mid n < \omega\} \subseteq \Delta.$$

From the assumption we can deduce, using the ∞-rule and propositional reasoning, that

$$\Sigma \vdash_\infty \phi \wedge \phi_1 \to [\beta;\alpha^*]\phi_2$$

Hence Δ is closed under the ∞-rule. This proves one direction; the other direction is trivial. □

Corollary 5.8 *$\Sigma \cup \{\phi\}$ is consistent iff $\Sigma \not\vdash_\infty \neg\phi$.*

We now define a model $\mathcal{A}$ by:

- $W^{\mathcal{A}} = \{s \subseteq \Phi \mid \mathrm{Pr}(AX_\infty) \subseteq s$ and s is maximally consistent $\}$;
- $\pi^{\mathcal{A}}(p) = \{s \mid p \in s\}$ for primitive predicate p;
- $\rho^{\mathcal{A}}(a) = \{(s,t) \mid \forall\psi.([a]\psi \in s \Longrightarrow \psi \in t)\}$ for primitive program a.

Lemma 5.9 *For each proposition ϕ,*

$$\mathcal{A}, s \models \phi \text{ iff } \phi \in s.$$

Proof.

We proceed by induction on the complexity of ϕ. For ϕ a primitive predicate, the theorem holds by definition.

($\phi = \psi \vee \chi$). $\mathcal{A}, s \models \psi \vee \chi$ iff $\mathcal{A}, s \models \psi$ or $\mathcal{A}, s \models \chi$ iff, by induction hypothesis, $\psi \in s$ or $\chi \in s$ iff $\psi \vee \chi \in s$, by construction.

($\phi = \neg\psi$). $\mathcal{A}, s \models \neg\psi$ iff $\mathcal{A}, s \not\models \psi$ iff $\psi \notin s$ iff $\neg\psi \in s$.

($\phi = \langle\alpha\rangle\psi$). The only nontrivial case. We prove this case by induction on the structure of α.

First let $\alpha = a$ be a primitive program. $\mathcal{A}, s \models \langle a\rangle\psi$ iff there exists a state t such that $(s,t) \in \rho(a)$ and $\mathcal{A}, t \models \psi$. By induction hypothesis, $\psi \in t$ and by the definition of $\rho(a)$, $\langle a\rangle\psi \in s$. Conversely, suppose $\langle a\rangle\psi \in s$. Consider the set

$$\Gamma = \{\phi \mid [a]\phi \in s\}.$$

Claim 1 Γ is a theory.
Proof of claim 1 $\Pr(AX_\infty) \subseteq \Gamma$, by the definition of s. Suppose ϕ, $\phi \to \psi \in \Gamma$, then $\psi \in \Gamma$ since the logic is normal. Suppose $\psi \to [\delta;\beta^i]\phi \in \Gamma$ for all $i < \omega$, then $[a](\psi \to [\delta;\beta^i]\phi) \in s$ for all $i < \omega$ hence $[a]\psi \to [a][\delta;\beta^*]\phi \in s$ by the maximality of s. We argue that $[a](\psi \to [\delta;\beta^*]\phi) \in s$. Suppose not. Then $\neg[a](\psi \to [\delta;\beta^*]\phi) \in s$ or

$$\langle a\rangle(\psi \wedge \langle\delta;\beta^*\rangle\neg\phi) \in s$$

and, by Lemma 5.5,

$$\langle a\rangle(\psi \wedge \langle\delta;\beta^m\rangle\neg\phi) \in s$$

for some $m < \omega$. Contradiction. Hence Γ is closed under the ∞-rule and is a theory.

Extend Γ to the set $\Gamma' = \Gamma \cup \{\psi\}$.

Claim 2 Γ' is consistent.
Proof of claim 2 Suppose Γ' is inconsistent. Then, by Corollary 5.8, $\Gamma \vdash_\infty \neg\psi$. By Lemma 5.6, $\neg\psi \in \Gamma$ or $[a]\neg\psi \in s$. But $\langle a\rangle\psi \in s$ by assumption. Contradiction.

Hence Γ' can be extended to a maximally consistent set t. By the definition of ρ, $(s,t) \in \rho(a)$ and by induction hypothesis, $\mathcal{A}, t \vDash \psi$. Hence, $\mathcal{A}, s \vDash \langle a\rangle\psi$. The case α is primitive, is proved. The other cases follow easily.

$\mathcal{A}, s \vDash \langle\chi?\rangle\psi$ iff $\mathcal{A}, s \vDash \chi \wedge \psi$ iff, by induction hypothesis, $\chi \wedge \psi \in s$ iff $\langle\chi?\rangle\psi \in s$.

$\mathcal{A}, s \vDash \langle\alpha \cup \beta\rangle\psi$ iff $\mathcal{A}, s \vDash \langle\alpha\rangle\psi \vee \langle\beta\rangle\psi$ iff $\langle\alpha\rangle\psi \vee \langle\beta\rangle\psi \in s$ iff $\langle\alpha \cup \beta\rangle\psi \in s$.

$\mathcal{A}, s \vDash \langle\alpha;\beta\rangle\psi$ iff $\mathcal{A}, s \vDash \langle\alpha\rangle\langle\beta\rangle\psi$ iff $\langle\alpha\rangle\langle\beta\rangle\psi \in s$ iff $\langle\alpha;\beta\rangle\psi \in s$.

Dually we prove $[\alpha^*]\psi \in s$ iff $\mathcal{A}, s \vDash [\alpha^*]\psi$. $\mathcal{A}, s \vDash [\alpha^*]\psi$ iff, by definition of Kripke models, $\mathcal{A}, s \vDash [\alpha^n]\psi$ for each $n < \omega$, iff, by induction hypothesis, $[\alpha^n]\psi \in s$ for each $n < \omega$, iff, by the ∞-rule, $[\alpha^*]\psi \in s$. □

With Lemma 5.9 we can easily prove the completeness of the system AX_∞:

Theorem 5.10 (Completeness Theorem) *For each* **PDL** *formula* ϕ, $\vdash_\infty \phi$ *iff* $\vDash \phi$.

Proof.

One direction is the Soundness Theorem; for the other direction: let ϕ be such that $\nvdash_\infty \phi$. Then $\Pr(AX_\infty) \cup \{\neg\phi\}$ is consistent and can be extended to a maximally consistent set s by Lindenbaum's Theorem. Hence, $s \in W^{\mathcal{A}}$ and $\mathcal{A}, s \vDash \neg\phi$ by Lemma 5.9, which implies that ϕ is not valid or $\nvDash \phi$. □

Since the Segerberg axiomatization is complete for **PDL**, we have the following corollary.

Corollary 5.11 *For all* $\phi \in \Phi$,

$$\vdash \phi \text{ iff} \vDash \phi \text{ iff} \vdash_\infty \phi.$$

Let $\mathcal{U}$ be the model as defined in the previous section. An immediate observation leads to the next lemma.

Lemma 5.12 $W^{\mathcal{A}} = W^{\mathcal{U}}$.

Proof.

By Soundness, each $s \in W^{\mathcal{U}}$ is maximally consistent and $\Pr(AX_\infty) \subseteq s$ so $W^{\mathcal{U}} \subseteq W^{\mathcal{A}}$. Conversely, $W^{\mathcal{A}} \subseteq W^{\mathcal{U}}$ by Completeness. □

By the lemma and the constructions of $\mathcal{U}$ and $\mathcal{A}$ we get:

Theorem 5.13 $\mathcal{U} \cong \mathcal{A}$.

In fact we may say that $\mathcal{U}$ and $\mathcal{A}$ are only two different names for the same model and conclude that $\mathcal{U} = \mathcal{A}$.

6 Non-standard Models

We have introduced a completeness technique for PDL which is based on an infinitary axiom system. One might ask whether this technique is applicable to the "normal" axiomatization as well. The answer to this question is "No". The difficulty in proving a lemma such as Lemma 5.9 lies in the case $\phi = [\alpha^*]\psi$. Let us see what happens when we try to prove the case. We can prove that $\mathcal{A}, s \vDash [\alpha^*]\psi$ implies $[\alpha^n]\psi \in s$ for each $n < \omega$, but we may not infer then that $[\alpha^*]\psi \in s$. In fact, we can prove the following theorem.

Theorem 6.1 *Let*

$$\begin{aligned} \Gamma &= \Pr(AX) \cup \{\phi, [a]\phi, [a^2]\phi, \ldots\} \cup \{\neg[a^*]\phi\} \\ &= \Pr(AX) \cup \Delta \cup \{\neg[a^*]\psi\} \end{aligned}$$

Then Γ *is consistent.*

Proof.

Suppose Γ inconsistent. Then for some *finite* subset $\Gamma' = \{\phi_0, \phi_1, \ldots, \phi_n\} \subseteq \Gamma$,

$$\Gamma' \vdash \mathit{false}.$$

Or

$$\vdash \phi_0 \wedge \cdots \wedge \phi_n \rightarrow \mathit{false}.$$

Without loss of generality, we may assume that $\phi_n = \neg[a^*]\psi$ and the other $\phi_j \in \Delta$. By Soundness, then, for all models $\mathcal{M}$ and states $s \in W^{\mathcal{M}}$, $\mathcal{M}, s \vDash \phi_0 \wedge \cdots \wedge \phi_{n-1} \rightarrow [\alpha^*]\phi$. But counterexamples are easily found. Hence Γ is consistent. □

Essentially, this is the same argument as we used for proving incompactness. There we saw that an infinite, semantically inconsistent set could not be proved to be inconsistent, by proving inconsistency of each of its finite subsets. In fact, each of its finite subsets was consistent. For exactly the same reason, namely syntactic consistency of each of the finite subsets of Γ, we must conclude that Γ itself is syntactically consistent. Yet it

surely is *not* semantically consistent in standard Kripke models. We therefore conclude that *syntactic* and *semantic* consequence are two different notions in the case of the axiom system AX and standard models.

As has been noted in [4, 11], we can construct a syntax model $\mathcal{A}'$ from the Segerberg axiomatization that is a *non-standard* model in the following sense.

Definition 6.2 *A* non-standard Kripke model *is any model $\mathcal{M}$ that is a Kripke model according to Definition 2.1, except that $\rho^{\mathcal{M}}(\alpha^*)$ need not be the reflexive transitive closure of $\rho^{\mathcal{M}}(\alpha)$, but only a reflexive transitive relation containing $\rho^{\mathcal{M}}(\alpha)$ and satisfying the induction axiom.*

In a way we might view this relaxation as a means to "compactify" the logic: the set Γ from Theorem 6.1 is satisfiable in a non-standard model. In non-standard models the set $\rho(\alpha^*)$ is simply larger than in standard models.

The construction of $\mathcal{A}'$ proceeds as follows. Let consistency for $\vdash$ be defined in the usual way (*c.f.* [11]).

- $W^{\mathcal{A}'} = \{s \subseteq \Phi \mid \Pr(AX) \subseteq s \text{ and } s \text{ is maximally consistent}\}$;
- $\pi^{\mathcal{A}'}(p) = \{s \mid p \in s\}$ for primitive p;
- $\rho^{\mathcal{A}'}(\alpha) = \{(s,t) \mid \forall \phi.([\alpha]\phi \in s \Longrightarrow \phi \in t)\}$.

Note the definition of $\rho^{\mathcal{A}'}$ which is defined for *all* programs, rather than only for primitive one's.

Theorem 6.3 *Let $\mathcal{A}'$ be the syntax model constructed from the Segerberg axiom system as indicated above. Then*

1. *$\mathcal{A}'$ is non-standard;*
2. *$\mathcal{A}'$ is universal in the class of non-standard models.*

Proof.

For (1), see [4, 11]. For (2), it is sufficient to prove

$$\mathcal{A}', s \vDash \phi \text{ iff } \phi \in s.$$

To prove this claim we can adapt the proof of Lemma 5.9, or see [2]. □

Corollary 6.4 *The Segerberg system AX is complete for* PDL *with respect to non-standard models.*

Note that the infinitary system is not complete with respect to these models.

7 Dynamic Algebras

In this section we introduce the notion of *Dynamic Algebras* [8, 9, 15] and study the relationship between these algebras and Kripke models.

Dynamic algebras were introduced by Kozen [8, 9] and Pratt [15] to give PDL a more algebraic interpretation, in much the same way as Boolean algebras give an interpretation for propositional logic.

A *dynamic algebra* is a two-sorted algebra $D = (K, B, \Diamond)$ where K is a Kleene or relational algebra and B is a Boolean algebra, for which a scalar multiplication $\Diamond : K \times B \mapsto B$ is defined. The basic operators for the Boolean algebra are $\wedge$, $\vee$ and $\neg$; the operators for the Kleene algebra are $;$, $\cup$ and $\star$. The defining axioms for the Boolean algebra are standard. However we do not have equality for the Kleene elements. Instead we axiomatize the meaning of $\Diamond$. As we have seen, there exist two axiomatizations for PDL that are sound and complete; Pratt used the Segerberg system and Kozen the infinitary sytem to axiomatize his versions of Dynamic algebras. We concentrate on the version of Kozen, which is called $\star$-*continuous*. Hence we have as axioms:

1. the axioms for Boolean algebras;
2. $\langle\alpha\rangle 0 = 0$;
3. $\langle\alpha\rangle(\phi \vee \psi) = \langle\alpha\rangle\phi \vee \langle\alpha\rangle\psi$;
4. $\langle\alpha;\beta\rangle\phi = \langle\alpha\rangle\langle\beta\rangle\phi$;
5. $\langle\alpha \cup \beta\rangle\phi = \langle\alpha\rangle\phi \vee \langle\beta\rangle\phi$;
6. $\langle\alpha^\star\rangle\phi = \bigvee_{i<\omega}\langle\alpha^i\rangle\phi$.

Here we have used ϕ, ψ to denote the Boolean elements and α, β to denote the Kleene elements. Let Φ_0 and Π_0 be the sets of names for (primitive) propositions and programs as defined in section 2. These names act as names for constants in these algebras. Let $\mathcal{D}$ be the class of all $\star$-continuous dynamic algebras with sets of constants Φ_0 and Π_0. $\mathcal{D}$ is equationally defined and thus has an initial algebra $\mathcal{I}$. We construct $\mathcal{I}$ as follows. Let T be the *term algebra* generated over Φ_0 and Π_0. Then $T = (\Phi, \Pi, \Diamond)$ and $\mathcal{I} = (\Phi/=, \Pi, \Diamond)$. Let D be any member of $\mathcal{D}$; then every assignment of elements of D to the sets Φ_0 and Π_0 extends to a homomorphism of $\mathcal{I}$ into D. An immediate observation is

$$\mathcal{I} \models \phi = \psi \text{ iff } \vdash_\infty \phi \leftrightarrow \psi.$$

With every Kripke model $\mathcal{M}$ we can easily associate a dynamic algebra $\overline{\mathcal{M}}$. With every $\phi \in \Phi$ we associate the subset $|\phi| \subseteq W$ where $|\phi|$ is defined by:

$$|\phi| = \{s \mid \mathcal{M}, s \models \phi\}$$

Denote the set of all such subsets $|\phi|$ by $|\Phi|^{\mathcal{M}}$. Similary, with every $\alpha \in \Pi$ we associate the function $|\alpha|$ defined by:

$$\langle|\alpha|\rangle|\phi| = |\langle\alpha\rangle\phi|$$

Denote the set of all such functions $|\alpha|$ by $|\Pi|^{\mathcal{M}}$. We let $\overline{\mathcal{M}} = (|\Phi|^{\mathcal{M}}, |\Pi|^{\mathcal{M}}, \Diamond)$.

Lemma 7.1 *For every Kripke model $\mathcal{M}$, $\overline{\mathcal{M}}$ is well-defined.*

Proof.

We have already proven that $|\Phi|^{\mathcal{M}}$ is a Boolean algebra. For the Kleene part of $\overline{\mathcal{M}}$: let $\tilde{\alpha} \in |\Pi|^{\mathcal{M}}$. Then

($\tilde{\alpha} = |\alpha|$) Immediate.

($\tilde{\alpha} = |\alpha|;|\beta|$)

$$\begin{aligned} \langle|\alpha|;|\beta|\rangle|\phi| &= \langle|\alpha|\rangle\langle|\beta|\rangle|\phi| \\ &= \langle|\alpha|\rangle|\langle\beta\rangle\phi| \\ &= |\langle\alpha;\beta\rangle\phi| \end{aligned}$$

($\tilde{\alpha} = |\alpha| \cup |\beta|$) Similar.

($\tilde{\alpha} = |\alpha|^*$)

$$\begin{aligned} \langle|\alpha|^*\rangle|\phi| &= \bigvee_n \langle|\alpha|^n\rangle|\phi| \\ &= \bigvee_n |\langle\alpha^n\rangle\phi| \\ &= |\bigvee_n \langle\alpha^n\rangle\phi| \\ &= |\langle\alpha^*\rangle\phi| \end{aligned}$$

□

Next we consider the algebra $\overline{\mathcal{U}}$. A first observation is that every (associated) algebra $\overline{\mathcal{M}}$ is a subalgebra of $\overline{\mathcal{U}}$: the embedding $\theta_{\mathcal{M}}$ of $W^{\mathcal{M}}$ into $W^{\mathcal{U}}$ extends to an embedding of $\overline{\mathcal{M}}$ into $\overline{\mathcal{U}}$. The main result of this section is now immediate.

Theorem 7.2 $\overline{\mathcal{U}} \cong \mathcal{I}$

Proof.

Consider the mapping $f : \overline{\mathcal{U}} \mapsto \mathcal{I}$ defined by:

- $f(|\phi|) = \phi$;
- $f(|\alpha|) = \alpha$.

f is clearly surjective. f is injective as well:

$$\begin{aligned} \overline{\mathcal{U}} \vDash |\phi| \neq |\psi| &\iff \mathcal{U} \nvDash \phi \leftrightarrow \psi \\ &\iff \nvdash_\infty \phi \leftrightarrow \psi \\ &\iff \mathcal{I} \nvDash \phi = \psi \\ &\iff \mathcal{I} \vDash \phi \neq \psi \end{aligned}$$

Finally, by Lemma 7.1, f is a homomorphism. □

References

[1] Bell, J.L. and A.B. Slomson, *Models and Ultraproducts*, North Holland, Amsterdam, 1979.

[2] Berman, F., "A Completeness Technique for D-Axiomatizable Semantics", *Proc. 11th ACM Symp. Theory of Comput.*, 1979, 160–166.

[3] Fischer, M.J. and R.E. Ladner, "Propositional Dynamic Logic of Regular Programs",*J. Comput. Syst. Sci.* 18:2 (1979), 194–211.

[4] Goldblatt, R., *Logics of Time and Computation*, Lecture Notes 7, CSLI, Stanford, 1987.

[5] Harel, D., *First Order Dynamic Logic*, LNCS 68, Springer-Verlag, Berlin etc., 1979.

[6] Harel, D., "Dynamic Logic", in: Gabbay and Guenthner (eds.), *Handbook of Philosophical Logic II: Extensions of Classical Logic*, D. Reidel, Boston, 1984, 497–604.

[7] Knijnenburg, P.M.W., "On Axiomatizations for Propositional Logics of Programs", Tech. Rep. RUU-CS-88-34, Univ. of Utrecht.

[8] Kozen, D., "A Representation Theorem for Models of $\star$–Free PDL", *Proc. 7th Int. Colloq. Automata Lang. Prog.*, LNCS 85, Springer-Verlag, Berlin etc., 1982, 348–359.

[9] Kozen, D., "On Induction vs. $\star$–Continuity", in: D. Kozen (ed.), *Proc. Workshop on Logics of Programs*, LNCS 131, Springer-Verlag, Berlin etc., 1981, 167–176.

[10] Kozen, D. and R. Parikh, "An Elementary Proof of the Completeness of PDL", *Theor. Comput. Sci.*, 14 (1981), 113–118.

[11] Kozen, D. and J. Tiuryn, "Logics of Programs", to appear in: J. van Leeuwen (ed.), *Handbook of Theoretical Computer Science*, North Holland, Amsterdam.

[12] Parikh, R., "Propositional Dynamic Logic of Programs: A Survey", in: E. Engeler (ed.), *Proc. Workshop on Logic of Programs*, LNCS 125, Springer-Verlag, Berlin etc., 1981, 102–144.

[13] Pratt, V.R., "Semantical Considerations on Floyd-Hoare Logic", *Proc. 17th IEEE Symp. Found. Comput. Sci.* 1976, 326–337.

[14] Pratt, V.R., "Models of Program Logics", *Proc. 20th IEEE Symp. Found. Comput. Sci.*, 1979, 115–122.

[15] Pratt, V.R., "Dynamic Algebras and the Nature of Induction", *Proc. 12th ACM Symp. Theory Comput.*, 1980, 22–28.

[16] Sherman, R. and D. Harel, "A Combined Proof of one-exponentional Decidability and Completeness for PDL", *Proc. 1st Int. Workshop on Found. Theor. Comput. Sci., GTI*, Paderborn, 1982.

[17] Segerberg, K., "A Completeness Theorem in the Modal Logic of Programs (Preliminary Report)", *Not. Amer. Math. Soc.*, 24:6, A–552, 1979.