

Formal Specification and Verification

Propositional Dynamic Logic (2)

7.02.2017

Viorica Sofronie-Stokkermans
e-mail: sofronie@uni-koblenz.de

Propositional Dynamic Logic

Propositional dynamic logic (PDL) is a multi-modal logic with structured modalities.

For each program α , there is:

- a box-modality $[\alpha]$ and
- a diamond modality $\langle \alpha \rangle$.

PDL was developed from first-order dynamic logic by Fischer-Ladner (1979) and has become popular recently.

Here we consider **regular** PDL.

Propositional Dynamic Logic

Syntax

Prog set of programs

$\text{Prog}_0 \subseteq \text{Prog}$: set of atomic programs

Π : set of propositional variables

The set of formulae $\mathbf{Fma}_{\text{Prog}, \Pi}^{PDL}$ of (regular) propositional dynamic logic and the set of programs \mathbf{Prog} are defined by simultaneous induction as follows:

PDL: Syntax

Formulae:

F, G, H	$::=$	\perp	(falsum)
		\top	(verum)
		p	$p \in \Pi$ (atomic formula)
		$\neg F$	(negation)
		$(F \wedge G)$	(conjunction)
		$(F \vee G)$	(disjunction)
		$(F \rightarrow G)$	(implication)
		$(F \leftrightarrow G)$	(equivalence)
		$[\alpha]F$	if $\alpha \in \text{Prog}$
		$\langle \alpha \rangle F$	if $\alpha \in \text{Prog}$

Programs:

α, β, γ	$::=$	α_0	$\alpha_0 \in \text{Prog}_0$ (atomic program)
		$F?$	F formula (test)
		$\alpha; \beta$	(sequential composition)
		$\alpha \cup \beta$	(non-deterministic choice)
		α^*	(non-deterministic repetition)

Semantics

A **PDL structure** $\mathcal{K} = (S, R(), I)$ is a multimodal Kripke structure with an accessibility relation for each atomic program. That is it consists of:

- a non-empty set S of states
- an interpretation $R() : \text{Prog}_0 \rightarrow S \times S$ of atomic programs that assigns a transition relation $R(\alpha)$ to each atomic program α
- an interpretation $I : \Pi \times S \rightarrow \{0, 1\}$

PDL: Semantics

The **interpretation** of PDL relative to a PDL structure $\mathcal{K} = (S, R(), I)$ is defined by extending $R()$ to Prog and extending I to $\text{Fma}_{\text{Prog}_0, \Pi}^{\text{PDL}}$ by the following simultaneously inductive definition:

Interpretation of formulae/programs

$$val_{\mathcal{K}}(p, s) = I(p, s) \quad \text{if } p \in \Pi$$

$$val_{\mathcal{K}}(\neg F, s) = \neg_{\text{Bool}} val_{\mathcal{K}}(F, s)$$

$$val_{\mathcal{K}}(F \wedge G, s) = val_{\mathcal{K}}(F, s) \wedge_{\text{Bool}} val_{\mathcal{K}}(G, s)$$

$$val_{\mathcal{K}}(F \vee G, s) = val_{\mathcal{K}}(F, s) \vee_{\text{Bool}} val_{\mathcal{K}}(G, s)$$

$$val_{\mathcal{K}}(F \rightarrow G, s) = val_{\mathcal{K}}(F, s) \rightarrow_{\text{Bool}} val_{\mathcal{K}}(G, s)$$

$$val_{\mathcal{K}}(F \leftrightarrow G, s) = val_{\mathcal{K}}(F, s) \leftrightarrow_{\text{Bool}} val_{\mathcal{K}}(G, s)$$

$$val_{\mathcal{K}}([\alpha]F, s) = 1 \text{ iff for all } t \in S \text{ with } (s, t) \in R(\alpha), val_{\mathcal{K}}(F, t) = 1$$

$$val_{\mathcal{K}}(\langle \alpha \rangle F, s) = 1 \text{ iff for some } t \in S \text{ with } (s, t) \in R(\alpha), val_{\mathcal{K}}(F, t) = 1$$

$$R([F?]) = \{(s, s) \mid val_{\mathcal{K}}(F, s) = 1\}$$

($F?$ means: if F then skip else do not terminate)

$$R(\alpha \cup \beta) = R(\alpha) \cup R(\beta)$$

$$R(\alpha; \beta) = \{(s, t) \mid \text{there exists } u \in S \text{ s.t. } (s, u) \in R(\alpha) \text{ and } (u, t) \in R(\beta)\}$$

$$R(\alpha^*) = R(\alpha)^*$$

$$= \{(s, t) \mid \text{there exist } n \geq 0 \text{ and } u_0, \dots, u_n \in S \text{ with}$$

$$s = u_0, t = u_n, (u_0, u_1), \dots, (u_{n-1}, u_n) \in R(\alpha)\}$$

Interpretation of formulae/programs

- (\mathcal{K}, s) **satisfies** F (notation $(\mathcal{K}, s) \models F$) iff $val_{\mathcal{K}}(F, s) = 1$.
- F is **valid in** \mathcal{K} (notation $\mathcal{K} \models F$) iff $(\mathcal{K}, s) \models F$ for all $s \in S$.
- F is **valid** (notation $\models F$) iff $\mathcal{K} \models F$ for all PDL-structures \mathcal{K} .

Hilbert-style axiom system for PDL

Axioms

- (D1) All propositional logic tautologies
- (D2) $[\alpha](A \rightarrow B) \rightarrow ([\alpha]A \rightarrow [\alpha]B)$
- (D3) $[\alpha](A \wedge B) \leftrightarrow [\alpha]A \wedge [\alpha]B$
- (D4) $[\alpha; \beta]A \leftrightarrow [\alpha][\beta]A$
- (D5) $[\alpha \cup \beta]A \leftrightarrow [\alpha]A \wedge [\beta]A$
- (D6) $[A?]B \leftrightarrow (A \rightarrow B)$
- (D7) $[\alpha^*]A \leftrightarrow A \wedge [\alpha][\alpha^*]A,$
- (D8) $[\alpha^*](A \rightarrow [\alpha]A) \rightarrow (A \rightarrow [\alpha^*]A)$

Inference rules

$$\begin{array}{l} MP \quad \frac{F \quad F \rightarrow G}{G} \\ \\ Gen \quad \frac{F}{[\alpha]F} \end{array}$$

We will show that PDL is determined by PDL structures, and has the finite model property.

Soundness of PDL

Theorem. If the formula F is provable in the inference system for PDL then F is valid in all PDL structures.

Proof: Induction of the length of the proof, using the following facts:

1. The axioms are valid in every PDL structure. Easy computation.
2. If the premises of an inference rule are valid in a structure \mathcal{K} , the conclusion is also valid in \mathcal{K} .

(MP) If $\mathcal{K} \models F, \mathcal{K} \models F \rightarrow G$ then $\mathcal{K} \models G$ (follows from the fact that for every state s of \mathcal{K} if $(\mathcal{K}, s) \models F, (\mathcal{K}, s) \models F \rightarrow G$ then $(\mathcal{K}, s) \models G$)

(Gen) Assume that $\mathcal{K} \models F$. Then $(\mathcal{K}, s) \models F$ for every state s of \mathcal{K} .

Let t be a state of \mathcal{K} . $(\mathcal{K}, t) \models [\alpha]F$ if for all t' with $(t, t') \in R(\alpha)$ we have $(\mathcal{K}, t') \models F$. But under the assumption that $\mathcal{K} \models F$ the latter is always the case. This shows that $(\mathcal{K}, t) \models [\alpha]F$ for all t .

Completeness of PDL

Theorem. If the formula F is valid in all PDL structures then F is provable in the inference system for PDL.

Proof

Idea:

Assume that F is not provable in the inference system for PDL.

We show that:

- (1) $\neg F$ is consistent with the set L of all theorems of PDL
- (2) We can construct a “canonical” PDL structure \mathcal{K}_L and a state w in this PDL structure such that $(\mathcal{K}_L, w) \models \neg F$.

Contradiction!

(Details of the proof in the lecture “Non-Classical Logics”; written proof included on the website of the lecture)

Decidability of PDL

Theorem. Assume that the formula F in PDL is not valid, i.e. there exists a Kripke model \mathcal{K} and a state s of \mathcal{K} with $(\mathcal{K}, s) \models \neg F$. Then $\neg F$ has a finite model, of size bounded by 2^n , where n is the number of subformulae of F .

Idea of the proof:

Fix a model $\mathcal{K} = (S, R, I)$ and a set $\Gamma \subseteq Fma_\Sigma$ that is closed under subformulae, i.e. $B \in \Gamma$ implies $\text{Subformulae}(B) \subseteq \Gamma$.

For each $s \in S$, define

$$\Gamma_s = \{B \in \Gamma \mid (\mathcal{K}, s) \models B\}$$

and put $s \sim_\Gamma t$ iff $\Gamma_s = \Gamma_t$,

Then $s \sim_\Gamma t$ iff for all $B \in \Gamma$, $(\mathcal{K}, s) \models B$ iff $(\mathcal{K}, t) \models B$.

Fact: \sim_Γ is an equivalence relation on S .

Decidability

Let $[s] = \{t \mid s \sim_{\Gamma} t\}$ be the \sim_{Γ} -equivalence class of s .

Let $S_{\Gamma} := \{[s] \mid s \in S\}$ be the set of all such equivalence classes.

Goal: $(\mathcal{K}, s) \models A \mapsto (\mathcal{K}', s') \models A, \quad \mathcal{K}' = (S', R', I'), \quad S' \text{ finite.}$

Step 1: $S' := S_{\Gamma}$, where $\Gamma = \text{Subformulae}(A)$

Step 2: $I' : (\Pi \cap \Gamma) \times S' \rightarrow \{0, 1\}$ def. by $I'(P, [s]) = I(P, s)$

Step 3: $R'(\alpha)$ def. e.g. by: $([s], [t]) \in R'(\alpha)$ iff $\exists s' \in [s], \exists t' \in [t]: (s', t') \in R(\alpha)$

Theorem: \mathcal{K}' is a PDL structure (a filtration of \mathcal{K}).

Since $(\mathcal{K}, s) \models \neg F$ it can easily be seen that $(\mathcal{K}', [s]) \models \neg F$.

Lemma. If Γ is finite, then S_{Γ} is finite and has at most 2^n elements, where n is the number of elements of Γ . \mapsto decidability

Conclusions

PDL is decidable (it has the finite model property).

Proof calculi for PDL exist (e.g. sequent calculi, tableau calculi)

For really reasoning about programs, often *first order dynamic logic* is needed (undecidable)

Nevertheless, many systems used for verification use sequent or tableau calculi also for first order dynamic logic.

Sequent calculi

In what follows we illustrate a way of designing sequent calculi for propositional dynamic logic.

We do not give here any completeness results; for a sound and complete sequent calculus we refer e.g. to:

- Vaughan R. Pratt: A Practical Decision Method for Propositional Dynamic Logic: Preliminary Report STOC 1978: 326-337
<http://dl.acm.org/citation.cfm?doid=800133.804362>

For a sound and complete tableau calculus we refer e.g. to:

- Rajeev Goré, Florian Widmann: An Optimal On-the-Fly Tableau-Based Decision Procedure for PDL-Satisfiability. CADE 2009: 437-452

A sequent calculus for PDL

Reminder (Classical propositional logic)

Sequent Calculus based on notion of sequent

$$\underbrace{\psi_1, \dots, \psi_m}_{\text{Antecedent}} \Rightarrow \underbrace{\phi_1, \dots, \phi_n}_{\text{Succedent}}$$

Has same semantics as

$$\models \psi_1 \wedge \dots \wedge \psi_m \rightarrow (\phi_1 \vee \dots \vee \phi_n)$$

$$\{\psi_1, \dots, \psi_m\} \models \phi_1 \vee \dots \vee \phi_n$$

Notation for Sequents

$$\underbrace{\psi_1, \dots, \psi_m}_{\text{Antecedent}} \Rightarrow \underbrace{\phi_1, \dots, \phi_n}_{\text{Succedent}}$$

Consider antecedent/succedent as sets of formulas, may be empty

Schema Variables:

ϕ, ψ, \dots match formulas, Γ, Δ, \dots match sets of formulas

Characterize infinitely many sequents with a single schematic sequent:

Example: $\Gamma \Rightarrow \Delta, \phi \wedge \psi$

Matches any sequent with occurrence of conjunction in succedent

We call $\phi \wedge \psi$ **main formula** and Γ, Δ **side formulae** of sequent.

Sequent Calculus Rules of Propositional Logic

Write syntactic transformation schema for sequents that reflects semantics of connectives as closely as possible

$$\text{Rule Name} \quad \frac{\overbrace{\Gamma_1 \Rightarrow \Delta_1 \dots \Gamma_n \Rightarrow \Delta_n}^{\text{premises}}}{\underbrace{\Gamma \Rightarrow \Delta}_{\text{conclusion}}} .$$

Example:

$$\text{andRight} \quad \frac{\Gamma \Rightarrow \phi, \Delta \quad \Gamma \Rightarrow \psi, \Delta}{\Gamma \Rightarrow \phi \wedge \psi, \Delta} .$$

Informal meaning:

In order to prove that Γ entails $(\phi \wedge \psi) \vee \Delta$ we need to prove that:

Γ entails $\phi \vee \Delta$ and

Γ entails $\psi \vee \Delta$

Sequent Calculus Rules of Propositional Logic

Write syntactic transformation schema for sequents that reflects semantics of connectives as closely as possible

$$\text{Rule Name} \quad \frac{\overbrace{\Gamma_1 \Rightarrow \Delta_1 \dots \Gamma_n \Rightarrow \Delta_n}^{\text{premises}}}{\underbrace{\Gamma \Rightarrow \Delta}_{\text{conclusion}}} .$$

Example:

$$\text{andRight} \quad \frac{\Gamma \Rightarrow \phi, \Delta \quad \Gamma \Rightarrow \psi, \Delta}{\Gamma \Rightarrow \phi \wedge \psi, \Delta} .$$

Sound rule (essential): If $\models (\Gamma_1 \rightarrow \Delta_1)$ and \dots and $\models (\Gamma_n \rightarrow \Delta_n)$ then $\models (\Gamma \rightarrow \Delta)$

Complete rule (desirable): If $\models (\Gamma \rightarrow \Delta)$ then $\models (\Gamma_1 \rightarrow \Delta_1), \dots \models (\Gamma_n \rightarrow \Delta_n)$

Rules of Propositional Sequent Calculus

main	left side (antecedent)	right side (succedent)
not	$\frac{\Gamma \Rightarrow \phi, \Delta}{\Gamma, \neg \phi \Rightarrow \Delta}$	$\frac{\Gamma, \phi \Rightarrow \Delta}{\Gamma \Rightarrow \neg \phi, \Delta}$
and	$\frac{\Gamma, \phi, \psi \Rightarrow \Delta}{\Gamma, \phi \wedge \psi \Rightarrow \Delta}$	$\frac{\Gamma \Rightarrow \phi, \Delta \quad \Gamma \Rightarrow \psi, \Delta}{\Gamma \Rightarrow \phi \wedge \psi, \Delta}$
or	$\frac{\Gamma, \phi \Rightarrow \Delta \quad \Gamma, \psi \Rightarrow \Delta}{\Gamma, \phi \vee \psi \Rightarrow \Delta}$	$\frac{\Gamma \Rightarrow \phi, \psi, \Delta}{\Gamma \Rightarrow \phi \vee \psi, \Delta}$
imp	$\frac{\Gamma \Rightarrow \phi, \Delta \quad \Gamma, \psi \Rightarrow \Delta}{\Gamma, \phi \rightarrow \psi \Rightarrow \Delta}$	$\frac{\Gamma, \phi \Rightarrow \psi, \Delta}{\Gamma \Rightarrow \phi \rightarrow \psi, \Delta}$

close $\overline{\Gamma, \phi \Rightarrow \phi, \Delta}$
 true $\overline{\Gamma \Rightarrow \text{true}, \Delta}$
 false $\overline{\Gamma, \text{false} \Rightarrow \Delta}$

Example: Part of a sequent calculus for PDL

In addition to the classical propositional rules we can consider:

main	left side (antecedent)	right side (succedent)
$[\alpha]$	$\frac{\Gamma, [\alpha]\phi, [\alpha]\psi \Rightarrow \Delta}{\Gamma, [\alpha](\phi \wedge \psi) \Rightarrow \Delta}$	$\frac{\Gamma \Rightarrow \Delta, [\alpha]\phi \quad \Gamma \Rightarrow \Delta, [\alpha]\psi}{\Gamma \Rightarrow \Delta, [\alpha](\phi \wedge \psi)}$
$\langle \alpha \rangle$	$\frac{\Gamma, \langle \alpha \rangle \phi \Rightarrow \Delta \quad \Gamma, \langle \alpha \rangle \psi \Rightarrow \Delta}{\Gamma, \langle \alpha \rangle (\phi \vee \psi) \Rightarrow \Delta}$	$\frac{\Gamma \Rightarrow \Delta, \langle \alpha \rangle \phi, \langle \alpha \rangle \psi}{\Gamma \Rightarrow \Delta, \langle \alpha \rangle (\phi \vee \psi)}$
$[\alpha^*]$	$\frac{\Gamma, [\alpha][\alpha^*]\phi, \phi \Rightarrow \Delta}{\Gamma, [\alpha^*]\phi \Rightarrow \Delta}$	$\frac{\Gamma \Rightarrow \phi, \Delta \quad \Gamma \Rightarrow [\alpha][\alpha^*]\phi, \Delta}{\Gamma \Rightarrow \Delta, [\alpha^*]\phi}$
$[\phi?]$	$\frac{\Gamma \Rightarrow \phi, \Delta \quad \Gamma, \psi \Rightarrow \Delta}{\Gamma, [\phi?]\psi \Rightarrow \Delta}$	$\frac{\Gamma, \phi \Rightarrow \psi, \Delta}{\Gamma \Rightarrow [\phi?]\psi, \Delta}$
$\langle \phi? \rangle$	$\frac{\Gamma, \phi, \psi \Rightarrow \Delta}{\Gamma, \langle \phi? \rangle \psi \Rightarrow \Delta}$	$\frac{\Gamma, \Rightarrow \phi, \Delta \quad \Gamma, \Rightarrow \psi, \Delta}{\Gamma \Rightarrow \langle \phi? \rangle \psi, \Delta}$
$\alpha \cup \beta$	$\frac{\Gamma, [\alpha]\phi, [\beta]\phi \Rightarrow \Delta}{\Gamma, [\alpha \cup \beta]\phi \Rightarrow \Delta}$	$\frac{\Gamma \Rightarrow [\alpha]\phi, \Delta \quad \Gamma \Rightarrow [\beta]\phi, \Delta}{\Gamma \Rightarrow [\alpha \cup \beta]\phi, \Delta}$
$\alpha; \beta$	$\frac{\Gamma, [\alpha][\beta]\phi \Rightarrow \Delta}{\Gamma, [\alpha; \beta]\phi \Rightarrow \Delta}$	$\frac{\Gamma \Rightarrow [\alpha][\beta]\phi, \Delta}{\Gamma \Rightarrow [\alpha; \beta]\phi, \Delta}$

Example: Part of a sequent calculus for PDL

We also use:

$$\frac{\Gamma \Rightarrow [\alpha](\phi \rightarrow \psi), \Delta}{\Gamma \Rightarrow ([\alpha]\phi \rightarrow [\alpha]\psi), \Delta}$$

$$\frac{\Gamma, [\alpha]\neg\phi \Rightarrow \Delta}{\Gamma \Rightarrow \langle\alpha\rangle\phi, \Delta}$$

$$\frac{\Gamma, \phi \Rightarrow \Delta, \psi}{\Gamma, \langle\alpha\rangle\phi \Rightarrow \Delta, \langle\alpha\rangle\psi}$$

Example

Prove $\langle \alpha^* \rangle \phi \rightarrow \phi \vee \langle \alpha \rangle \langle \alpha^* \rangle \phi$ using the sequent calculus.

Example

Prove $\langle \alpha^* \rangle \phi \rightarrow \phi \vee \langle \alpha \rangle \langle \alpha^* \rangle \phi$ using the sequent calculus.

close	close	
$[\alpha][\alpha^*]\neg\phi, \neg\phi \Rightarrow \neg\phi$	$[\alpha][\alpha^*]\neg\phi, \neg\phi \Rightarrow [\alpha][\alpha^*]\neg\phi$	$([\alpha^*], \text{right})$
$[\alpha][\alpha^*]\neg\phi, \neg\phi \Rightarrow [\alpha^*]\neg\phi$		(not)
$[\alpha][\alpha^*]\neg\phi \Rightarrow [\alpha^*]\neg\phi, \phi$		(not + $\langle \alpha \rangle$)
$\langle \alpha^* \rangle \phi \Rightarrow \phi, \langle \alpha \rangle \langle \alpha^* \rangle \phi$		or, right
$\langle \alpha^* \rangle \phi \Rightarrow \phi \vee \langle \alpha \rangle \langle \alpha^* \rangle \phi$		(imp, right)
$\Rightarrow \langle \alpha^* \rangle \phi \rightarrow \phi \vee \langle \alpha \rangle \langle \alpha^* \rangle \phi$		

Summary

Dynamic logic

- Syntax and semantics
- Axiom system
- Soundness and completeness
- Sequent calculus