Lecture Notes on
Theory of Dynamic Logic

15-816: Modal Logic
André Platzer

Lecture 25
April 27, 2010

1 Introduction to This Lecture

In this lecture we study some parts of the theory of dynamic logics. We extend the study of decidability of propositional modal logics to obtain a decidability result about propositional dynamic logic.

2 Decidability of PDL

Recall propositional dynamic logic (PDL) from lecture 19. What we have not seen yet is why PDL is decidable. For this, we use filtration arguments from lecture 21, but we need to take care of the structured multi-modal operators of PDL. For simplicity we assume that PDL only uses the logical operators $\neg, \vee, \langle\cdot\rangle$, which can clearly be used to define all other operators of PDL.

Definition 1 (Fischer-Ladner closure) *Let F be a formula of PDL. The smallest set S of formulas with the following properties is called* Fischer-Ladner closure *of F:*

1. $F \in S$
2. $\neg G \in S$ *then* $G \in S$
3. $(G \vee H) \in S$ *then* $G, H \in S$
4. $\langle\alpha\rangle G \in S$ *then* $G \in S$

5. *$\langle ?H\rangle G \in S$ then $H \in S$ (and $G \in S$ by 4)*

6. *$\langle \alpha \cup \beta\rangle G \in S$ then $\langle\alpha\rangle G \in S$ and $\langle\beta\rangle G \in S$*

7. *$\langle \alpha ; \beta\rangle G \in S$ then $\langle\alpha\rangle\langle\beta\rangle G \in S$*

8. *$\langle \alpha^*\rangle G \in S$ then $\langle\alpha\rangle\langle\alpha^*\rangle G \in S$*

Definition 2 (Quotient) *Let $K = (W, \rho(), v)$ be a PDL structure and let S be any set of PDL formulas. We define an equivalence relation $\sim_S$ on W by*

$$s \sim_S t \quad \textit{iff} \quad \textit{for all } F \in S : \ K, s \models F \textit{ iff } K, t \models F$$

and consider equivalence classes $[s]$ of states s with respect to $\sim_S$. We define the quotient structure $K_S = (W_S, \rho_S(), \tau_S)$ as:

- *$W_S := \{[s] \ : \ s \in W_S\}$ (well-defined because $\sim_S$ is an equivalence relation)*
- *$\tau_S(q) := \{[s] \ : \ s \in \tau_S(q)\}$ when propositional letter $q \in S$ (well-defined because $\sim_S$ is an equivalence relation)*
- *$\tau_S(q)$ is arbitrary when propositional letter $q \notin S$*
- *For an atomic program $\pi \in \Pi_0$, $[s]\rho_S(\pi)[t]$ iff for all $\langle\pi\rangle G \in S$*

$$\textit{if } K, s \models \neg\langle\pi\rangle G \textit{ then } K, t \models \neg G$$

Lemma 3 (Filtration) *Let F be a formula of PDL and S its Fischer-Ladner closure. Let $K = (W, \rho(), v)$ be a PDL structure and $K_S = (W_S, \rho_S(), \tau_S)$ its quotient structure with respect to $\sim_S$. Then for all formulas $G \in S$ all programs $\alpha \in \Pi$*

1. *$[s]\rho_S(\alpha)[t]$ implies that for all $\langle\alpha\rangle G \in S$*

$$\textit{if } K, s \models \neg\langle\alpha\rangle G \textit{ then } K, t \models \neg G$$

2. *$s\rho(\alpha)t$ implies $[s]\rho_S(\alpha)[t]$*

3. *$K, s \models G$ iff $K_S, [s] \models G$.*

Proof: The proof is by simultaneous induction for all cases on the complexity of α and G. The base case of atomic programs is by construction.

Part 1: Consider induction step for $\langle\alpha;\beta\rangle G$. Let $([s],[t]) \in \rho_S(\alpha;\beta)$. Then there is a u such that $([s],[u]) \in \rho_S(\alpha)$ and $([u],[t]) \in \rho_S(\beta)$. By induction hypothesis, we know that for all $\langle\alpha\rangle A \in S$ and all $\langle\beta\rangle B \in S$:

$$\text{if } s \models \neg\langle\alpha\rangle A \text{ then } u \models \neg A \tag{1}$$

$$\text{if } u \models \neg\langle\beta\rangle B \text{ then } t \models \neg B \tag{2}$$

We need to show for any $\langle\alpha;\beta\rangle C \in S$ that

$$\text{if } s \models \neg\langle\alpha;\beta\rangle C \text{ then } t \models \neg C$$

Thus assume $[s] \models \neg\langle\alpha;\beta\rangle C$. By construction of the Fischer-Ladner closure we have $\langle\alpha\rangle\langle\beta\rangle C \in S$, thus $\langle\beta\rangle C \in S$. Consequently, $s \models \neg\langle\alpha\rangle\langle\beta\rangle C$ implies $u \models \neg\langle\beta\rangle C$ using (4). Thus (2) implies $t \models \neg C$.

Now consider the induction step for $\langle\alpha^*\rangle G$. Let $([s],[t]) \in \rho_S(\alpha^*)$. Then there is a sequence of states $s_0, s_1, \ldots, s_n$ such that $[s_0] = [s], [s_n] = [t]$ and $([s_i],[s_{i+1}]) \in \rho_S(\alpha)$ for all $0 \leq i < n$. By induction hypothesis, we know that for all $\langle\alpha\rangle A \in S$ and all i:

$$\text{if } s_i \models \neg\langle\alpha\rangle A \text{ then } s_{i+1} \models \neg A \tag{3}$$

We need to show for any $\langle\alpha^*\rangle C \in S$ that

$$\text{if } s \models \neg\langle\alpha^*\rangle C \text{ then } t \models \neg C$$

It is easy to see that $\neg\langle\alpha^*\rangle C \leftrightarrow \neg C \land \neg\langle\alpha\rangle\langle\alpha^*\rangle C$ is a valid equivalence in PDL. We show by induction on i that $s_i \models \neg\langle\alpha^*\rangle C$ for $0 \leq i \leq n$.

0. $i = 0$ is what we assumed.

i+1. Assuming $s_i \models \neg\langle\alpha^* C\rangle$, we have that $s_i \models \neg\langle\alpha\rangle\langle\alpha^*\rangle C$ by the above equivalence. By construction of the Fischer-Ladner closure we know that $\neg\langle\alpha\rangle\langle\alpha^*\rangle C \in S$. Consequently, the induction hypothesis yields $s_{i+1} \models \neg\langle\alpha^*\rangle C$.

Thus from $s_n \models \neg\langle\alpha^*\rangle C$, the above equivalence implies $s_n \models \neg C$, which implies $s \models \neg C$, by step 3 (note that G is simpler), because $[s] = [s_n]$.

Consider the case for $\langle ?H\rangle G$, which uses part 3. Let $([s],[t]) \in \rho_S(?H)$. Then $[s] = [t]$ and $[s] \models H$. Assume $s \models \neg\langle ?H\rangle A$, which directly implies that $s \models \neg H \lor \neg A$ by the PDL semantics. Yet $[s] \models H$ implies $s \models H$ by part 3. We want to show $t \models \neg A$. Now by part 3 (H is simpler), $s \models \neg A$ implies $[s] \models \neg A$ and $[t] \models \neg A$ by $[s] = [t]$. Thus $t \models \neg A$, again by part 3.

Part 2: Let $s\rho(\alpha)t$. For proving $[s]\rho_S(\alpha)[t]$, consider any formula $\neg\langle\alpha\rangle A \in S$ with $K, s \models \neg\langle\alpha\rangle A$. This directly implies $K, t \models \neg A$, because $s\rho(\alpha)t$.

Part 3: Consider the most interesting case where G is $\langle\alpha\rangle A$. Assume $K, s \models \langle\alpha\rangle A$, then there is a t with $s\rho()t$ and $K, t \models A$. By induction hypothesis, this implies $K_S, [t] \models A$. By part 2, we have $[s]\rho_S()[t]$ and $K_S, [s] \models \langle\alpha\rangle A$. Conversely, assume $K_S, [s] \models \langle\alpha\rangle A$. Then there is a $[t]$ with $[s]\rho_S()[t]$ and $K_S, [t] \models A$. By induction hypothesis, this implies $K, t \models A$. Suppose we had $K, s \models \neg\langle\alpha\rangle A$, then part 1 would imply $K, t \models \neg A$, which is a contradiction. □

Also see [FL79, HKT00, Sch03] for details.

Theorem 4 *PDL satisfiability is decidable.*

Proof: Consider any PDL formula F. Let S be the Fischer-Ladner closure of F. Let $n \in \mathbb{N}$ be the size of S, which is a finite set, say, of size n. We show that if F is satisfiable at all, it has a model of at most size 2^n. Let K be a PDL structure satisfying F. Then its quotient structure K_S has at most 2^n states and still satisfies F by Lemma 3. Thus, if F is satisfiable then it is satisfiable in models of bounded finite size and enumeration can be used to decide. □

But there is one thing we have forgotten! Why does the Fischer-Ladner closure always exist and is finite? Or why is Definition 1 actually a definition? Case 8 seems to demand that we keep on adding new formulas. Does that continue forever? We consider that next.

3 Fischer-Ladner Tableaux

We consider a tableau construction for the Fischer-Ladner closure. For a PDL formula F we define its *diamond closure* $\Diamond^{-*}F$ is the smallest set S of subformulas of F such that $F \in S$ and whenever $\langle\alpha\rangle G \in S$, we also have $G \in S$.

Definition 5 (Fischer-Ladner tableaux) *Let F be a PDL formula and let the set $\Diamond^{-*}F = \{F_1, \ldots, F_n\}$ be its diamond closure. A Fischer-Ladner tableau is formed by applying the rules in Fig. 1 from the initial tableau*

$$F_1 \quad F_2 \quad \ldots \quad F_i \quad \ldots \quad F_n$$

A Fischer-Ladner tableau stops *if no more rules are applicable. By $FLT(T)$ we denote the set of all formulas occurring in T.*

$$\begin{array}{llll}
\text{(FL1)} & \dfrac{\neg F}{F_1 \dots F_n}\,{}^{1} & \text{(FL4)} & \dfrac{\langle \alpha \cup \beta \rangle F}{\langle \alpha \rangle F \quad \langle \beta \rangle F} \\
\text{(FL2)} & \dfrac{F \vee G}{F_1 \dots F_n G_1 \dots G_m}\,{}^{1} & \text{(FL5)} & \dfrac{\langle \alpha ; \beta \rangle F}{\langle \alpha \rangle \langle \beta \rangle F \quad \langle \beta \rangle F} \\
\text{(FL3)} & \dfrac{\langle ?F \rangle G}{F_1 \dots F_n}\,{}^{1} & \text{(FL6)} & \dfrac{\langle \alpha^* \rangle F}{\langle \alpha \rangle \langle \alpha^* \rangle F}
\end{array}$$

[1] where $\Diamond^{-*}F = \{F_1, \dots, F_n\}$ and $\Diamond^{-*}G = \{G_1, \dots, G_m\}$

Figure 1: Fischer-Ladner closure tableaux

Lemma 6 *The Fischer-Ladner tableau procedure has the following properties:*

1. *The Fischer-Ladner tableau procedure terminates for every input F with a tableau of size $\leq |F|$, where $|F|$ is the number of symbols in F.*
2. *All Fischer-Ladner tableaus (stopped or not) with a node $\langle \alpha \rangle G$ also have a node G (diamond closure).*
3. *If T is a stopped Fischer-Ladner tableau then $FLT(T)$ is the Fischer-Ladner closure of F.*

Proof: 1. In rules FL1 and FL2, the number of propositional operators decreases strictly. Rule FL3 turns a modal formula $\langle \alpha \rangle F$ into formulas F_i that are strictly smaller than α. Rules FL4,FL5,FL6 turn a modal formula $\langle \alpha \rangle F$ into a set of formulas $\langle \alpha_i \rangle F_i$ for arbitrary F_i but strictly smaller α_i. Consequently, the number of symbols in the starting formula is an upper bound on the number of rule applications. Especially, no rules are applicable for formulas of the form $\langle \pi \rangle F$ with atomic program π, where the process stops.

2. Proof by induction on the tableau T. The property easily holds for the initial tableau by the definition of diamond closures.

FL1 The cases where tableau T' is obtained from tableau T by FL1, FL2, or FL3 are simple, because the extension is the full diamond closure.

FL4 T' is obtained from T by FL4. Then the extensions $\langle \alpha \rangle F$ and $\langle \beta \rangle F$ inherit the property from the induction hypothesis for $\langle \alpha \cup \beta \rangle F$, because the postcondition did not change.

FL5 T' is obtained from T by FL5. The left branch is easy. The second branch follows from $\Diamond^{-*}\langle \beta \rangle F = \Diamond^{-*}F \cup \{\langle \beta \rangle F\}$ and the fact that $\Diamond^{-*}F$ is on the tableau already by induction hypothesis.

FL6 T' is obtained from T by FL6. For the new formula $\langle\alpha\rangle\langle\alpha^*\rangle G$ we need to show that $\Diamond^{-*}\langle\alpha^*\rangle F = \Diamond^{-*}F \cup \{\langle\alpha^*\rangle F\}$ occur on T' already. Clearly $\Diamond^{-*}F$ is in T by induction hypothesis and $\langle\alpha^*\rangle F$ is the premiss.

3. It is easy to see that $FLT(T)$ satisfies the conditions for the Fischer-Ladner closure just by looking at the rules:

1. $F \in S$: holds from the initial tableau and the fact that $F \in \Diamond^{-*}F$.
2. $\neg G \in S$ then $G \in S$: by FL1 and $F \in \Diamond^{-*}F$.
3. $(G \vee H) \in S$ then $G, H \in S$: by FL2 and $F \in \Diamond^{-*}F, G \in \Diamond^{-*}G$.
4. $\langle\alpha\rangle G \in S$ then $G \in S$: By part 2
5. $\langle ?F\rangle G \in S$ then $F \in S$: By FL3 and $F \in \Diamond^{-*}F$.
6. $\langle\alpha \cup \beta\rangle G \in S$ then $\langle\alpha\rangle G \in S$ and $\langle\beta\rangle G \in S$: By FL4 and $F \in \Diamond^{-*}F$.
7. $\langle\alpha;\beta\rangle G \in S$ then $\langle\alpha\rangle\langle\beta\rangle G \in S$: By FL5 and $F \in \Diamond^{-*}F$.
8. $\langle\alpha^*\rangle G \in S$ then $\langle\alpha\rangle\langle\alpha^*\rangle G \in S$: By FL6 and $F \in \Diamond^{-*}F$.

The converse direction is also easy to see: $FLT(T) \subseteq S$ for any set S satisfying the conditions of the Fischer-Ladner closure. □

4 Some Dynamic Logic Meta-Theory

Propositional dynamic logic is decidable but of limited expressive power. We consider first-order dynamic logic from lecture 19 and study a few simple meta properties. Dynamic logic has a rich theory [HKT00] and practical applications, e.g., in program verification [HLS$^+$96, BHS07], probabilistic systems [Koz85], and hybrid systems verification [Pla08].

As one example we show how easy it is to see that dynamic logic does not have a sound and complete effective calculus. Given that (first-order) dynamic logic talks about properties of programs, undecidability is not surprising. We show a very simple standalone proof of incompleteness.

Theorem 7 (Incompleteness) *(First-order) Dynamic logic has no effective sound and complete calculus.*

Proof: We first show that the compactness theorem does not hold in DL. It is easy to see that there is a set of formulas that has no model even though all finite subsets have a model, consider:

$$\{\langle (x := f(x))^*;\ ?p(x)\rangle \mathit{true}\} \cup \{\neg p(f^n(x)) \ :\ n \in \mathbb{N}\}$$

Suppose there was an effective sound and complete calculus for DL. Consider an set Φ of formulas that has no model in which all finite subsets have a model. Then $\Phi \vDash q \land \neg q$ is valid, thus provable by completeness. But this effective proof can only use finitely many assumptions $\Phi_0 \subset \Phi$. Thus $\Phi_0 \vDash q \land \neg q$ by soundness. But then the finite set Φ_0 has no model, which is a contradiction. □

Sound and complete infinitary axiomatizations of DL still exist [HKT00]. Also relative completeness proofs exist and arithmetical completeness has been shown [HKT00, Har79].

The set of computation sequences of a regular program is defined as

$$\begin{aligned}
CS(\pi) &:= \{\pi\} && \text{for atomic program } \pi\\
CS(?\phi) &:= \{?\phi\}\\
CS(\alpha \cup \beta) &:= CS(\alpha) \cup CS(\beta)\\
CS(\alpha;\beta) &:= \{\sigma\tau \ :\ \sigma \in CS(\alpha), \tau \in CS(\beta)\}\\
CS(\alpha^*) &:= \bigcup_{n\in\mathbb{N}} CS(\alpha^n)
\end{aligned}$$

Theorem 8 (Completeness of termination in uninterpreted case) *In the uninterpreted case, i.e., in the class of arbitrary Kripke structures, the dynamic logic calculus is complete for termination assertions with first-order formulas F, G:*

$$\vDash F \to \langle\alpha\rangle G \quad \textit{iff} \quad \vdash F \to \langle\alpha\rangle G$$

Proof: The calculus needs axiom schemata for instances of all valid PDL formulas, of all valid first-order formulas, modus ponens and the following axiom for all first-order formulas ϕ:

$$\phi_x^\theta \leftrightarrow \langle x := \theta\rangle\phi$$

Soundness is simple. Completeness can be proven by induction on the structure of α. Consider the case $\vDash F \to \langle\alpha \cup \beta\rangle G$. Let Ω be the set of all computation sequences of $\alpha \cup \beta$. In an infinitary logic, we could say that $\langle\alpha\cup\beta\rangle G$ is equivalent to the infinitary formula $\bigvee_{\sigma\in\Omega}\langle\sigma\rangle G$. Hence

$\vDash F \to \langle \alpha \cup \beta \rangle G$ implies that the following set of DL formulas is unsatisfiable:

$$\{F\} \cup \{\neg\langle\sigma\rangle G \ : \ \sigma \in \Omega\}$$

For each computation sequence σ it is easy to see that there is a first-order formula $(\langle\sigma\rangle G)^\flat$ that is equivalent to $\langle\sigma\rangle G$. Thus the following set of first-order formulas is unsatisfiable

$$\{F\} \cup \{\neg(\langle\sigma\rangle G)^\flat \ : \ \sigma \in \Omega\}$$

Thus compactness of first-order logic implies that there is a finite subset of $\Omega_0 \subseteq \Omega$ such that the finite subset is unsatisfiable

$$\{F\} \cup \{\neg(\langle\sigma\rangle G)^\flat \ : \ \sigma \in \Omega_0\}$$

Thus

$$\vDash F \to \bigvee_{\sigma\in\Omega_0} (\langle\sigma\rangle G)^\flat$$

which can be rewritten in the form

$$\vDash F \to \left(\bigvee_{\sigma\in A} (\langle\sigma\rangle G)^\flat \lor \bigvee_{\sigma\in B} (\langle\sigma\rangle G)^\flat \right) \tag{4}$$

for finite subsets A and B of the computation sequences of α and β respectively. By completeness of first-order logic the latter first-order formula is provable in first-order logic (thus in DL). Because A and B are computation sequences of α and β respectively we have

$$\vDash \bigvee_{\sigma\in A} (\langle\sigma\rangle G)^\flat \to \langle\alpha\rangle G \quad \text{and} \quad \vDash \bigvee_{\sigma\in B} (\langle\sigma\rangle G)^\flat \to \langle\beta\rangle G$$

Thus these simpler formulas are provable by induction hypothesis. Combining this with the provability of (4) gives

$$\vdash F \to \langle\alpha\rangle G \lor \langle\beta\rangle G$$

Now the PDL axiom $\langle\alpha\rangle G \lor \langle\beta\rangle G \leftrightarrow \langle\alpha \cup \beta\rangle G$ yields

$$\vdash F \to \langle\alpha \cup \beta\rangle G$$

□

References

[BHS07] Bernhard Beckert, Reiner Hähnle, and Peter H. Schmitt, editors. *Verification of Object-Oriented Software: The KeY Approach*, volume 4334 of *LNCS*. Springer, 2007.

[FL79] Michael J. Fischer and Richard E. Ladner. Propositional dynamic logic of regular programs. *J. Comput. Syst. Sci.*, 18(2):194–211, 1979.

[Har79] David Harel. *First-Order Dynamic Logic*. Springer, New York, 1979.

[HKT00] David Harel, Dexter Kozen, and Jerzy Tiuryn. *Dynamic logic*. MIT Press, Cambridge, 2000.

[HLS$^+$96] Dieter Hutter, Bruno Langenstein, Claus Sengler, Jörg H. Siekmann, Werner Stephan, and Andreas Wolpers. Deduction in the verification support environment (VSE). In Marie-Claude Gaudel and Jim Woodcock, editors, *FME*, volume 1051 of *LNCS*, pages 268–286. Springer, 1996.

[Koz85] Dexter Kozen. A probabilistic PDL. *J. Comput. Syst. Sci.*, 30(2):162–178, 1985.

[Pla08] André Platzer. Differential dynamic logic for hybrid systems. *J Autom Reas*, 41(2):143–189, 2008.

[Sch03] Peter H. Schmitt. Nichtklassische Logiken. Vorlesungsskriptum Fakultät für Informatik , Universität Karlsruhe, 2003.