15-812: Programming Language Semantics

Lecture Notes on Axiomatic Semantics

André Platzer

Carnegie Mellon University
Lecture 23

1 Introduction to This Lecture

In this lecture we study some parts of the theory of dynamic logics and how its axiomatic semantics agrees with its denotational semantics.

These lecture notes are based on [Pla10, Pla18, MS00, HKT00].

$$[\cdot]\ \ [\alpha]\phi \leftrightarrow \neg\langle\alpha\rangle\neg\phi$$

$$\langle:=\rangle\ \ \langle x:=\theta\rangle\phi(x) \leftrightarrow \phi(\theta)$$

$$\langle ?\rangle\ \ \langle ?H\rangle\phi \leftrightarrow (H \wedge \phi)$$

$$\langle\cup\rangle\ \ \langle\alpha\cup\beta\rangle\phi \leftrightarrow (\langle\alpha\rangle\phi \vee \langle\beta\rangle\phi)$$

$$\langle;\rangle\ \ \langle\alpha;\beta\rangle\phi \leftrightarrow \langle\alpha\rangle\langle\beta\rangle\phi$$

$$\langle^*\rangle\ \ \langle\alpha^*\rangle\phi \leftrightarrow \phi \vee \langle\alpha\rangle\langle\alpha^*\rangle\phi$$

Figure 1: Some differential dynamic logic axioms

2 Background: First-Order Logic

Soundness is the question whether all provable formulas are valid and is a minimal requirement for proper logics. Completeness studies the converse question whether all valid formulas are provable.

The first-order logic proof calculus can be shown to be both sound and complete, which is a result that originates from Gödel's PhD thesis [Göd30], albeit in a different form.

Theorem 1 (Soundness & completeness of first-order logic)**.** *First-order logic is* sound*, i.e.* $\vdash \subseteq \models$*, which means that* $\vdash \phi$ *implies* $\models \phi$ *for all first-order formulas* ϕ *(all provable formulas are valid). First-order logic is* complete*, i.e.* $\models \subseteq \vdash$*, which means that* $\models \phi$ *implies* $\vdash \phi$ *for all first-order formulas* ϕ *(all valid formulas are provable). In particular, the provability relation* $\vdash$ *and the validity relation* $\models$ *coincide for first-order logic:* $\vdash = \models$*. The same holds in the presence of a set of assumptions* Γ*, i.e.* $\Gamma \vdash \phi$ *iff* $\Gamma \models \phi$*, that is, a first-order formula* ϕ *is provable from a set of first-order assumptions* Γ *in first-order logic if and only if* ϕ *is a consequence of* Γ*, i.e. entailed by* Γ*, i.e. true in all models of* Γ*.*

Soundness and completeness together show that validity of a formula in the semantics coincide with provability of the formula from the axioms. While of independent significance, soundness and completeness also argue why the axioms could have been used to define the meaning of the operators, because, after all, the result coincides with the denotational semantics. This viewpoint is that of *axiomatic semantics*, where the meaning of an operator is given by the set of proof rules and axioms for it.

This lecture will not set out for a direct proof of Theorem 1, because the techniques used for those proofs are very interesting but would lead us too far astray. An indirect justification for what makes first-order logic so special that Theorem 1 can hold will be discussed later.

The following central result about compactness of first-order logic is of similar importance. Compactness is involved in most proofs of Theorem 1, but, once Theorem 1 has been proved, also easily follows from Theorem 1. Compactness means that if a formula A is a consequence of a set of formulas Γ, then it already is a consequence of finitely many formulas.

Theorem 2 (Compactness of first-order logic)**.** *First-order logic is* compact*, i.e.*

$$\Gamma \models A \iff E \models A \text{ for some finite } E \subseteq \Gamma \tag{1}$$

Proof. By Theorem 1, $\vdash = \models$. By completeness, the semantic compactness theorem (1) is equivalent to the syntactic compactness theorem:

$$\Gamma \vdash A \iff E \vdash A \text{ for some finite } E \subseteq \Gamma \tag{2}$$

Condition (2) is obvious, because provability implies that there is a proof, which can, by definition, only use finitely many assumptions $E \subseteq \Gamma$. □

Without compactness, proving cannot always work, because proofs are finite so can only use finitely many assumptions.

Compactness is equivalent to the finiteness property, which, for that reason, is usually simply referred to as compactness. The finiteness property says that a set of formulas Γ has a model if and only if all its finite subsets of formulas have a model.

Corollary 3 (Finiteness). *First-order logic satisfies the* finiteness property*, i.e.*

$$\Gamma \textit{ has a model} \iff \textit{all finite } E \subseteq \Gamma \textit{ have a model} \tag{3}$$

Proof. Compactness (Theorem 2) implies the finiteness property. The key observation is that Γ has no model iff $\Gamma \vDash \mathit{false}$, because if Γ has no model, then false holds in all models of Γ of which there are none. Conversely, the only chance for false to hold in all models of Γ is if there are no such models, since false never holds. By Theorem 2,

$$\Gamma \vDash \mathit{false} \iff \exists \text{finite } E \subseteq \Gamma \;\; E \vDash \mathit{false}$$

Hence,

$$\Gamma \text{ has a model} \iff \Gamma \nvDash \mathit{false} \iff \forall \text{finite } E \subseteq \Gamma \;\; E \nvDash \mathit{false} \iff \text{all finite } E \subseteq \Gamma \text{ have a model}$$

It is worth noting that, conversely, the finiteness property implies compactness.

$$\begin{aligned} \Gamma \vDash A &\iff \Gamma \cup \{\neg A\} \text{ has no model} \\ &\iff \text{some finite } E \subseteq \Gamma \cup \{\neg A\} \text{ has no model} \qquad \text{by finiteness} \\ &\iff E \vDash A \text{ for some finite } E \subseteq \Gamma \end{aligned}$$

The last equivalence uses that we might as well include $\neg A$ in E, because if E has no model then neither does $E \cup \{\neg A\}$. □

3 Axiomatic Semantics

Propositional dynamic logic is decidable but of limited expressive power. Propositional dynamic logic is the variable-free fragment of dynamic logic, so it really only has predicate symbols $p()$ without arguments and atomic programs a, b, c without any fixed interpretation. So for example,

$$q() \vee [a^*]p() \to q() \vee [a \cup a; a^*]p()$$

As in the rest of the course, we consider first-order dynamic logic where variables are allowed 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], hybrid systems verification [Pla12b], distributed hybrid systems verification [Pla12a] and, indirectly, for network systems [AFG+14].

The axioms and proof rules that dynamic logic provides are in a strong sense aligned with its denotational semantics. With a suitable reading, the axioms tell us the meaning of the operators as well. Yet, there are some challenges along the way of making it formally precise how the axiomatic and denotational semantics of dynamic logic agree. They do agree in terms of soundness, i.e. every provable formula is valid, so the axioms never justify something that is not backed up by the denotational semantics. The

converse question of completeness is more subtle, because we immediately hit a bump in the road.

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 by Rice's theorem [Ric53] and nuisances such as the Entscheidungsproblem and halting problem [Chu36, Tur37]. We show a very simple standalone proof of incompleteness.

Theorem 4 (Incompleteness)**.** *(First-order) Dynamic logic of programs has no effective sound and complete calculus.*

Proof. We first show that the compactness theorem does not hold in DL [MS00]. 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:

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

Suppose there was an effective sound and complete calculus for DL. Consider a set Φ of formulas that has no model in which all finite subsets have a model. Then $\Phi \vDash q \wedge \neg q$ is valid, thus provable by completeness. But this effective proof can only use finitely many assumptions $\Phi_0 \subset \Phi$. Thus $\Phi_0 \vDash q \wedge \neg q$ 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, Coo78]. These are very interesting results but their proofs also too complicated for today's lecture. So we will first settle on answering the story for a fragment. Recall that the computation sequence semantics assigns to each program α the set of all ;-separated sequences of assignments and tests that the program α could run.

First-order properties of computation sequences are expressible in first-order logic:

Lemma 5 (First-order rendition)**.** *There is an effective mapping $^\flat$ that assigns to any formula of the form $\langle\sigma\rangle G$ for a computation sequence σ and a first-order formula G a first-order formula $(\langle\sigma\rangle G)^\flat$ that is equivalent, i.e.*

$$\vDash \langle\sigma\rangle G \leftrightarrow (\langle\sigma\rangle G)^\flat$$

Proof. The proof is by structural induction on σ (for arbitrary first-order formulas G).

- $\vDash \langle x := \theta\rangle G \leftrightarrow (\langle x := \theta\rangle G)^\flat$ when defining $(\langle x := \theta\rangle G)^\flat$ as G_x^θ, which is a formula in first-order logic. Note that the substitution never clashes after bound variable renaming of the quantifiers.
- $\vDash \langle ?H\rangle G \leftrightarrow (\langle ?H\rangle G)^\flat$ when defining $(\langle ?H\rangle G)^\flat$ as $H \wedge G$, which is a formula in first-order logic.

- $\models \langle\alpha;\beta\rangle G \leftrightarrow (\langle\alpha;\beta\rangle G)^\flat$ when defining $(\langle\alpha;\beta\rangle G)^\flat$ as $\Big(\langle\alpha\rangle(\langle\beta\rangle G)^\flat\Big)^\flat$ since $\models \langle\beta\rangle G \leftrightarrow (\langle\beta\rangle G)^\flat$ by induction hypothesis since β is smaller than $\alpha;\beta$ and so $\models \langle\alpha\rangle(\langle\beta\rangle G)^\flat \leftrightarrow \Big(\langle\alpha\rangle(\langle\beta\rangle G)^\flat\Big)^\flat$ by induction hypothesis, since α is smaller than $\alpha;\beta$ and since $(\langle\beta\rangle G)^\flat$ is a first-order formula even if possibly a bigger one. □

Termination assertions are valid if and only if they are provable:

Theorem 6 (Completeness of termination in uninterpreted case). *In the uninterpreted case, i.e., with arbitrary interpretations and no built-in arithmetic, the dynamic logic calculus is complete for termination assertions with first-order formulas F, G:*

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

Proof. The soundness direction (from right to left) has been proved already in a previous lecture. The completeness direction (from left to right) is by structural induction on α.

- $\models F \to \langle x := \theta\rangle G$ then $\models F \to G_x^\theta$, e.g. by soundness of $\langle:=\rangle$. This formula is first-order, hence, provable by Theorem 1: $\vdash F \to G_x^\theta$. This proof can be continued to a proof of $\vdash F \to \langle x := \theta\rangle G$ using $\langle:=\rangle$.
- $\models F \to \langle\alpha;\beta\rangle G$ then $\models F \to \langle\alpha\rangle\langle\beta\rangle G$, e.g. by soundness of $\langle;\rangle$. Thus, there is a computation sequence $\sigma \in \mathrm{CS}(\beta)$ such that $\models F \to \langle\alpha\rangle\langle\sigma\rangle G$. Now Lemma 5 implies, $\models F \to \langle\alpha\rangle(\langle\sigma\rangle G)^\flat$, which, by induction hypothesis, is provable $\vdash F \to \langle\alpha\rangle(\langle\sigma\rangle G)^\flat$ because α is smaller than $\alpha;\beta$ and $(\langle\sigma\rangle G)^\flat$ is first-order. By Lemma 5 and $\sigma \in \mathrm{CS}(\beta)$, $\models (\langle\sigma\rangle G)^\flat \to \langle\beta\rangle G$, which, by induction hypothesis, is provable $\vdash (\langle\sigma\rangle G)^\flat \to \langle\beta\rangle G$ because β is smaller than $\alpha;\beta$ and $(\langle\sigma\rangle G)^\flat$ is first-order. This implies $\vdash \langle\alpha\rangle(\langle\sigma\rangle G)^\flat \to \langle\alpha\rangle\langle\beta\rangle G$ using, e.g. the generalization proof rule[1]. Combining both proofs $\vdash F \to \langle\alpha\rangle(\langle\sigma\rangle G)^\flat$ and $\vdash \langle\alpha\rangle(\langle\sigma\rangle G)^\flat \to \langle\alpha\rangle\langle\beta\rangle G$ yields $\vdash F \to \langle\alpha\rangle\langle\beta\rangle G$ by modus ponens, from which $\langle;\rangle$ derives $\vdash F \to \langle\alpha;\beta\rangle G$.
- $\models F \to \langle\alpha\cup\beta\rangle G$. The approach of the above cases does not work here unless $\models F \to \langle\alpha\rangle G$ or $\models F \to \langle\beta\rangle G$, which cannot generally be expected, because it may be the case that in some states only α leads to G while only β leads to G in others. Let $\Omega = \mathrm{CS}(\alpha\cup\beta) = \mathrm{CS}(\alpha)\cup\mathrm{CS}(\beta)$ 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 $\bigvee_{\sigma\in\Omega}\langle\sigma\rangle G$, except that this one is an infinitely big formula. Still, $\models F \to \langle\alpha\cup\beta\rangle G$ implies that the following set of DL formulas is unsatisfiable:

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

  For each computation sequence $\sigma \in \Omega$, $\models \langle\sigma\rangle G \leftrightarrow (\langle\sigma\rangle G)^\flat$. Hence, the following set of first-order formulas is unsatisfiable

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

[1] If $\vdash A \to B$ then $\vdash \langle\alpha\rangle A \to \langle\alpha\rangle B$.

Thus, Corollary 3 implies that there is a finite subset of $\Omega_0 \subseteq \Omega$ for which the following 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

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

where $A = \Omega_0 \cap \mathrm{CS}(\alpha)$ and $B = \Omega_0 \cap \mathrm{CS}(\beta)$. By Theorem 1, the latter first-order formula is provable in first-order logic (thus in DL). As A and B are sets of computation sequences of α and β respectively:

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

These formulas involve smaller programs, so are provable by induction hypothesis. Combining these proofs with the provability of (4) proves

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

from which $\langle\cup\rangle$ proves

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

- $\vDash F \to \langle\alpha^*\rangle G$. Let $\Omega = \mathrm{CS}(\alpha^*)$ the set of all computation sequences of α^*. In an infinitary logic, we could say that $\langle\alpha^*\rangle G$ is equivalent to the infinitary formula $\bigvee_{\sigma\in\Omega} \langle\sigma\rangle G$, except that this one is an infinitely big formula. Still, the following set of formulas is unsatisfiable:

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

  For each computation sequence $\sigma \in \Omega$, $\vDash \langle\sigma\rangle G \leftrightarrow (\langle\sigma\rangle G)^\flat$. Hence, the following set of first-order formulas is unsatisfiable

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

  Thus, Corollary 3 implies that there is a finite subset of $\Omega_0 \subseteq \Omega$ for which the following finite subset is unsatisfiable

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

  Thus

  $$\vDash F \to \bigvee_{\sigma\in\Omega_0} (\langle\sigma\rangle G)^\flat \tag{5}$$

By Theorem 1, this first-order formula is provable in first-order logic (thus in DL). For $\sigma \in \Omega_0$, let n be the iteration count for the loop explaining σ, i.e. let $\sigma \in \text{CS}(\alpha^n)$, in which case

$$\vDash (\langle\sigma\rangle G)^\flat \to \langle\alpha^n\rangle G$$

This formula has a program α^n of smaller structural complexity than α^*, so it is provable by induction hypothesis

$$\vdash (\langle\sigma\rangle G)^\flat \to \langle\alpha^n\rangle G \tag{6}$$

For any natural number $n \in \mathbb{N}$, the following formula is provable by n uses of $\langle^*\rangle$:

$$\vdash \langle\alpha^n\rangle G \to \langle\alpha^*\rangle G \tag{7}$$

Combining the proofs of (5), (6) and (7) leads to a proof of

$$\vdash F \to \bigvee_{\sigma\in\Omega_0} \langle\alpha^*\rangle G$$

from which the desired conclusion proves easily since σ no longer occurs:

$$\vdash F \to \langle\alpha^*\rangle G \qquad \square$$

Consequently, for this fragment of uninterpreted termination assertions, the axiomatic semantics of dynamic logic is equivalent to its denotational semantics.

With some relaxations of working relative to a data logic such as the underlying first-order logic of integer arithmetic, completeness can be lifted to general dynamic logic formulas [HKT00].

Theorem 7 (Relative completeness)**.** *Dynamic logic is complete relative to the underlying first-order logic of integer arithmetic* $\text{FOL}_\mathbb{Z}$*. That is, if DL formula* ϕ *is valid, then it is provable in the DL calculus from a set of tautologies of* $\text{FOL}_\mathbb{Z}$*:*

$$\vDash \phi \text{ implies } \text{FOL}_\mathbb{Z} \vdash \phi$$

For the proof, see [Pla17, Theorem 40] and a more general discussion around [Pla15, Theorem 4.5], which contain additional complications about differential equations that are unnecessary in our context and can be safely ignored here. The remaining question to complete the proof from [Pla17, Theorem 40] for the particular case of Theorem 7 is to show that modal formulas of loops such as $[\alpha^*]G$ have a first-order rendition $([\alpha^*]G)^\flat$in $\text{FOL}_\mathbb{Z}$, which follows similar to Lemma 5 using Gödel's definable pairing bijections $p : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ to encode intermediate states of loops. Gödel's pairing function, in turn, is based on the unique prime factorization in natural numbers so that this function is an injection

$$\mathbb{N} \times \mathbb{N} \to \mathbb{N}; (a, b) \mapsto 2^a 3^b$$

References

[AFG+14] Carolyn Jane Anderson, Nate Foster, Arjun Guha, Jean-Baptiste Jeannin, Dexter Kozen, Cole Schlesinger, and David Walker. NetKAT: semantic foundations for networks. In Suresh Jagannathan and Peter Sewell, editors, *The 41st Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages, POPL '14, San Diego, CA, USA, January 20-21, 2014*, pages 113–126. ACM, 2014. URL: http://dl.acm.org/citation.cfm?id=2535838, doi:10.1145/2535838.2535862.

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

[Chu36] Alonzo Church. A note on the Entscheidungsproblem. *J. Symb. Log.*, 1(1):40–41, 1936.

[Coo78] Stephen A. Cook. Soundness and completeness of an axiom system for program verification. *SIAM J. Comput.*, 7(1):70–90, 1978.

[Göd30] Kurt Gödel. Die Vollständigkeit der Axiome des logischen Funktionenkalküls. *Monatshefte Math. Phys.*, 37:349–360, 1930. doi:10.1007/BF01696781.

[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.

[MS00] Wolfram Menzel and Peter H. Schmitt. Formale Systeme. Vorlesungsskriptum Fakultät für Informatik , Universität Karlsruhe, 2000.

[Pla10] André Platzer. Modal logic. Lecture Notes 15-816 Modal Logic, Carnegie Mellon University, 2010. URL: http://www.cs.cmu.edu/~fp/courses/15816-s10/.

[Pla12a] André Platzer. A complete axiomatization of quantified differential dynamic logic for distributed hybrid systems. *Log. Meth. Comput. Sci.*, 8(4:17):1–44, 2012. Special issue for selected papers from CSL'10. doi:10.2168/LMCS-8(4:17)2012.

[Pla12b] André Platzer. Logics of dynamical systems. In *LICS*, pages 13–24, Los Alamitos, 2012. IEEE. doi:10.1109/LICS.2012.13.

[Pla15] André Platzer. Differential game logic. *ACM Trans. Comput. Log.*, 17(1):1:1–1:51, 2015. doi:10.1145/2817824.

[Pla17] André Platzer. A complete uniform substitution calculus for differential dynamic logic. *J. Autom. Reas.*, 59(2):219–265, 2017. doi:10.1007/s10817-016-9385-1.

[Pla18] André Platzer. *Logical Foundations of Cyber-Physical Systems*. Springer, Switzerland, 2018. URL: http://www.springer.com/978-3-319-63587-3.

[Ric53] H. Gordon Rice. Classes of recursively enumerable sets and their decision problems. *Trans. AMS*, 74(2):358–366, 1953. doi:10.2307/1990888.

[Tur37] Alan M. Turing. On computable numbers, with an application to the Entscheidungsproblem. *Proc. Lond. Math. Soc.*, 42(1):230–265, 1937. doi:10.1112/plms/s2-42.1.230.