A Formal Completeness Proof for Test-free PDL

Final Bachelor Talk

Joachim Bard
Advisor: Christian Doczkal

February 17, 2017

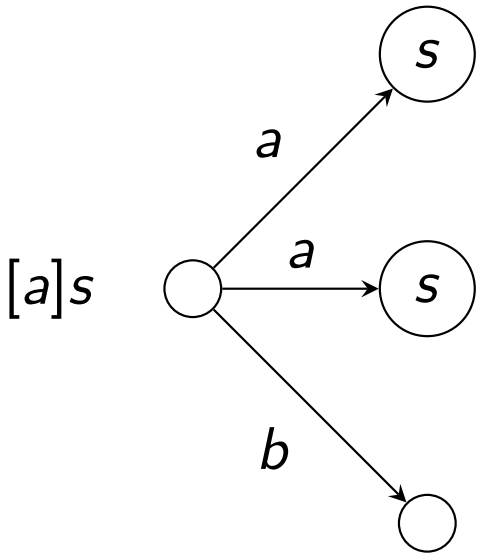
Outline

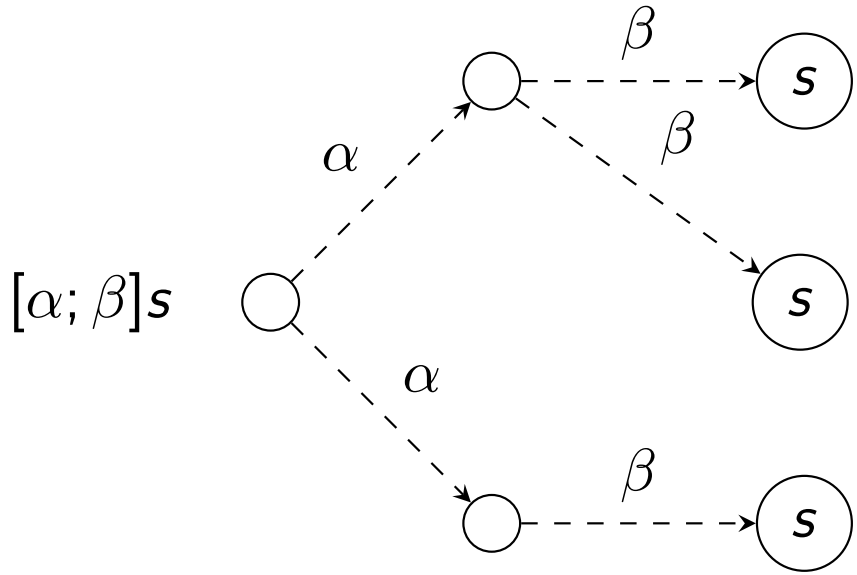
1. Test-free PDL
2. Demos
3. Pruning and Refutations
4. Hilbert Refutations
5. Conclusion

Test-free PDL

Definition

$$s, t ::= x \mid \bot \mid s \to t \mid [\alpha]s \qquad (x : \mathbb{N})$$
$$\alpha, \beta ::= a \mid \alpha; \beta \mid \alpha + \beta \mid \alpha^* \qquad (a : \mathbb{N})$$

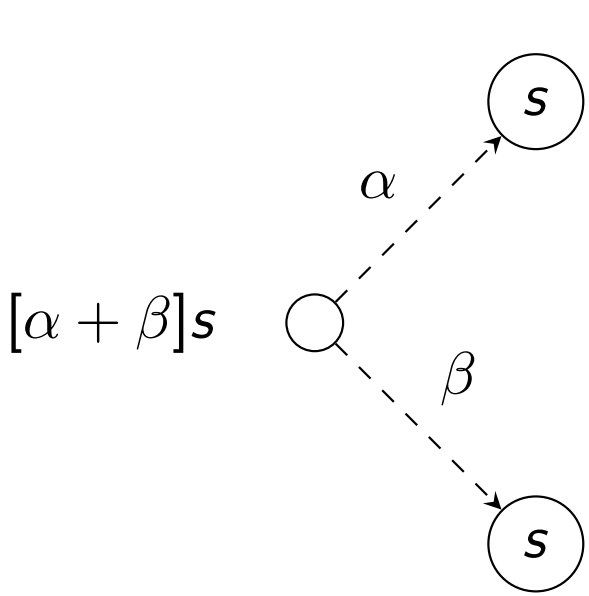


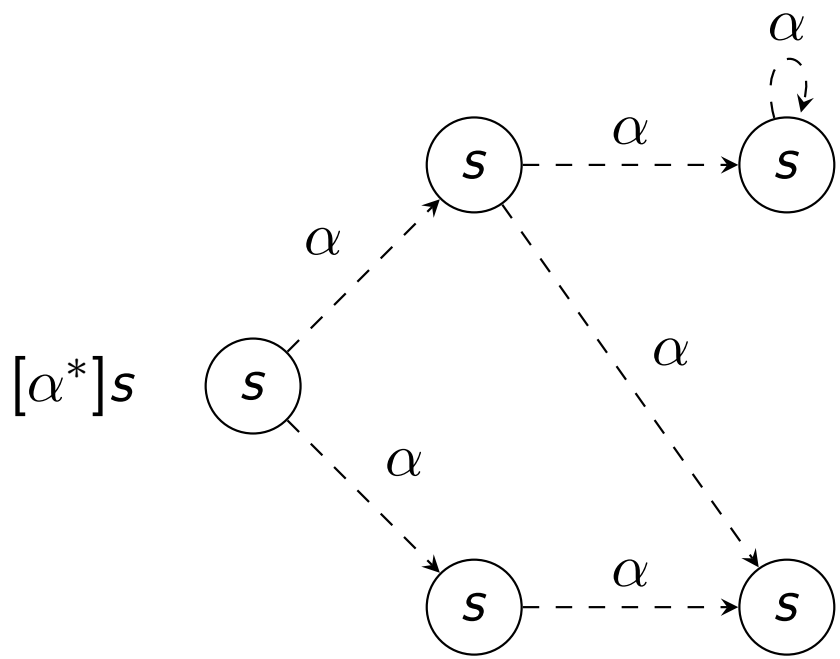


Test-free PDL

Definition

$$s, t ::= x \mid \bot \mid s \to t \mid [\alpha]s \qquad (x : \mathbb{N})$$
$$\alpha, \beta ::= a \mid \alpha; \beta \mid \alpha + \beta \mid \alpha^* \qquad (a : \mathbb{N})$$





Semantics

Definition (Models)

- Type of states
- $w \vDash x$ for all variables x
- $w \overset{a}{\Rightarrow} v$ for each atomic program a
- $w \vDash s \lor w \nvDash s$

Definition

w state of model $\mathcal{M}$

$$w \vDash \bot := \bot$$

$$w \vDash s \to t := w \vDash s \to w \vDash t$$

$$w \vDash [\alpha]s := \forall v.\, w \overset{\alpha}{\Rightarrow} v \to v \vDash s$$

Semantics

$$w \vDash [\alpha]s := \forall v.\, w \overset{\alpha}{\Rightarrow} v \to v \vDash s$$

Definition

w and v states of model $\mathcal{M}$

$$w \overset{a}{\Rightarrow} v \qquad \text{given}$$

$$w \overset{\alpha;\beta}{\Rightarrow} v := \exists u.\, w \overset{\alpha}{\Rightarrow} u \wedge u \overset{\beta}{\Rightarrow} v$$

$$w \overset{\alpha+\beta}{\Rightarrow} v := w \overset{\alpha}{\Rightarrow} v \vee w \overset{\beta}{\Rightarrow} v$$

$$w \overset{\alpha^*}{\Rightarrow} v := w(\overset{\alpha}{\Rightarrow})^* v$$

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

Hilbert System

Definition

$$\vdash s \to t \to s \qquad \vdash (u \to s \to t) \to (u \to s) \to u \to t$$

$$\vdash \neg\neg s \to s \qquad \frac{\vdash s \to t \qquad \vdash s}{\vdash t}$$

$$\vdash [\alpha](s \to t) \to [\alpha]s \to [\alpha]t \qquad \frac{\vdash s}{\vdash [\alpha]s}$$

$$\vdash [\alpha][\beta]s \to [\alpha;\beta]s \qquad \vdash [\alpha;\beta]s \to [\alpha][\beta]s$$

$$\vdash [\alpha]s \to [\beta]s \to [\alpha+\beta]s \qquad \vdash [\alpha+\beta]s \to [\alpha]s$$

$$\vdash [\alpha+\beta]s \to [\beta]s \qquad \vdash [\alpha^*]s \to s \qquad \vdash [\alpha^*]s \to [\alpha][\alpha^*]s$$

$$\frac{\vdash u \to [\alpha]u \qquad \vdash u \to s}{\vdash u \to [\alpha^*]s}$$

Theorem (Soundness)

$\vdash s \to \forall \mathcal{M}\, w.\, w \vDash s$

Informative Completeness

Theorem (Informative Completeness)

$\{\vdash \neg s\} + \{\exists \mathcal{M}.\, |\mathcal{M}| \leq 2^{2|s|} \wedge \exists w.\, w \vDash s\}$

Results:

- Completeness: $(\forall \mathcal{M}\, w.\, w \vDash s) \to \vdash s$
- Small model theorem: $(\exists \mathcal{M}\, w.\, w \vDash s) \to \exists \mathcal{M}\, w.\, w \vDash s \wedge |\mathcal{M}| \leq 2^{2|s|}$
- Decidability of:
  - Validity: $\forall \mathcal{M}\, w.\, w \vDash s$
  - Satisfiability: $\exists \mathcal{M}\, w.\, w \vDash s$
  - $\vdash s$

Proof idea:

- Attempt to build canonical model

Hintikka Sets

- $\lfloor s^+ \rfloor := s$, $\lfloor s^- \rfloor := \neg s$
- Clause C: finite set of signed formulas

Definition

$$\bot^+ \notin C$$

$$s^\sigma \in C \to s^{\overline{\sigma}} \notin C$$

$$s \to t^+ \in C \to s^- \in C \vee t^+ \in C$$

$$s \to t^- \in C \to s^+ \in C \wedge t^- \in C$$

$$[\alpha;\beta]s^\sigma \in C \to [\alpha][\beta]s^\sigma \in C$$

$$[\alpha+\beta]s^+ \in C \to [\alpha]s^+ \in C \wedge [\beta]s^+ \in C$$

$$[\alpha+\beta]s^- \in C \to [\alpha]s^- \in C \vee [\beta]s^- \in C$$

$$[\alpha^*]s^+ \in C \to s^+ \in C \wedge [\alpha][\alpha^*]s^+ \in C$$

$$[\alpha^*]s^- \in C \to s^- \in C \vee [\alpha][\alpha^*]s^- \in C$$

Demo

- Finite set of maximal Hintikka clauses S
- C maximal: $\forall s \in F.\, s^+ \in C \vee s^- \in C$

Definition

$\mathcal{R}_a\, C := \{s^+ \mid [a]s^+ \in C\}$

$$C \overset{a}{\rightsquigarrow}_S D := \mathcal{R}_a\, C \subseteq D$$

$$C \overset{\alpha;\beta}{\rightsquigarrow}_S D := \exists E \in S.\, C \overset{\alpha}{\rightsquigarrow}_S E \wedge E \overset{\beta}{\rightsquigarrow}_S D$$

$$C \overset{\alpha+\beta}{\rightsquigarrow}_S D := C \overset{\alpha}{\rightsquigarrow}_S D \vee C \overset{\beta}{\rightsquigarrow}_S D$$

$$C \overset{\alpha^*}{\rightsquigarrow}_S D := C(\overset{\alpha}{\rightsquigarrow}_S)^* D$$

Demo

Definition (Demo)

$[\alpha]s^- \in C \in S \to \exists D \in S.\, C \overset{\alpha}{\rightsquigarrow}_S D \wedge s^- \in D$

- $C \vDash x := x^+ \in C$
- $C \overset{a}{\Rightarrow} D := C \overset{a}{\rightsquigarrow}_S D$
- $C \overset{\alpha}{\rightsquigarrow}_S D \leftrightarrow C \overset{\alpha}{\Rightarrow} D$

Lemma

$s^\sigma \in C \to C \vDash \lfloor s^\sigma \rfloor$

- $[\alpha]s^+ \in C \to C \vDash [\alpha]s$ by construction of $\overset{\alpha}{\rightsquigarrow}$
- $[\alpha]s^- \in C \to C \vDash \neg[\alpha]s$ by demo condition

- Demo is the desired canonical model

Pruning

- Build a demo
- Start with $S_0 := \{C \subseteq \mathcal{U} \mid \text{maximal Hintikka clause } C\}$

Subformula Closure

Definition (Fischer-Ladner closure)

$$
\begin{aligned}
\operatorname{sub} x &:= \{x\} \\
\operatorname{sub} \bot &:= \{\bot\} \\
\operatorname{sub} s \to t &:= \{s \to t\} \cup \operatorname{sub} s \cup \operatorname{sub} t \\
\operatorname{sub} [\alpha]s &:= \operatorname{sub} s \cup \operatorname{sub}_\Box [\alpha]s \\
\operatorname{sub}_\Box [a]s &:= \{[a]s\} \\
\operatorname{sub}_\Box [\alpha;\beta]s &:= \{[\alpha;\beta]s\} \cup \operatorname{sub}_\Box [\alpha][\beta]s \cup \operatorname{sub}_\Box [\beta]s \\
\operatorname{sub}_\Box [\alpha+\beta]s &:= \{[\alpha+\beta]s\} \cup \operatorname{sub}_\Box [\alpha]s \cup \operatorname{sub}_\Box [\beta]s \\
\operatorname{sub}_\Box [\alpha^*]s &:= \{[\alpha^*]s\} \cup \operatorname{sub}_\Box [\alpha][\alpha^*]s
\end{aligned}
$$

$$
\mathcal{U} := \bigcup_{t \in \operatorname{sub} s} \{t^+, t^-\}
$$

Pruning

- Build a demo
- Start with $S_0 := \{C \subseteq \mathcal{U} \mid \text{maximal Hintikka clause } C\}$
- Remove C iff C contradicts demo condition:
  $[\alpha]s^- \in C \in S \to \exists D \in S.\, C \overset{\alpha}{\rightsquigarrow}_S D \wedge s^- \in D$
- Reachability changes
- Check again the demo condition ...
- Results in a demo

Vaughan R. Pratt. Models of program logics. In *20th Annual Symposium on Foundations of Computer Science*, pages 115-122, 1979.

Refutations

- Give reasons for unsatisfiable clauses

Definition

coref $S := \forall C \in S_0 \setminus S.\ \text{ref}\ C$

$$\frac{C \subseteq \mathcal{U} \qquad \text{coref}\ S \qquad \nexists D \in S.\ C \subseteq D}{\text{ref}\ C}$$

$$\frac{[\alpha]s^- \in C \qquad S \subseteq S_0 \qquad \text{coref}\ S \qquad \nexists D \in S.\ C \overset{\alpha}{\rightsquigarrow}_S D \wedge s^- \in D}{\text{ref}\ C}$$

- Every removed clause is refutable
- Demo is corefutable

Pruning Completeness

Theorem (Pruning Completeness)

$$C \subseteq \mathcal{U} \to \{\mathit{ref}\ C\} + \{\exists \mathcal{M}.\, |\mathcal{M}| \leq 2^{|\mathcal{U}|} \wedge \exists w.\, \forall s^\sigma \in C.\, w \vDash \lfloor s^\sigma \rfloor\}$$

Build demo S

- $\exists D \in S.\, C \subseteq D$: D satisfies C
- $\nexists D \in S.\, C \subseteq D$: C is refutable by definition

$$\frac{C \subseteq \mathcal{U} \qquad \mathrm{coref}\ S \qquad \nexists D \in S.\, C \subseteq D}{\mathrm{ref}\ C}$$

Theorem (Informative Completeness)

$$\{\vdash \neg s\} + \{\exists \mathcal{M}.\, |\mathcal{M}| \leq 2^{2|s|} \wedge \exists w.\, w \vDash s\}$$

- Translate refutations into the Hilbert system

Hilbert Refutations

- Translate refutations into the Hilbert system
- ref $C := \vdash \neg C$, read C as $\bigwedge_{s^\sigma \in C} \lfloor s^\sigma \rfloor$
- coref $S = \ \forall C \in S_0 \setminus S.\ \vdash \neg C$

Lemma

$$\frac{C \subseteq \mathcal{U} \qquad \mathit{coref}\ S \qquad \nexists D \in S.\, C \subseteq D}{\vdash \neg C}$$

- $\vdash C \to \bigvee \{D \in S \mid C \subseteq D\}$
- $\{D \in S \mid C \subseteq D\} = \emptyset$
- $\vdash C \to \bot$

Hilbert Refutations

Lemma

$$\frac{[\alpha]s^- \in C \qquad S \subseteq S_0 \qquad \mathit{coref}\ S \qquad \nexists D \in S.\, C \overset{\alpha}{\rightsquigarrow}_S D \wedge s^- \in D}{\vdash \neg C}$$

- $X := \{D \in S \mid s^- \in D\}$
- $\vdash C \to \neg[\alpha]\neg \bigvee_{D \in X} D$
- $\vdash C \to [\alpha] \bigwedge_{D \in X} \neg D$, proven using a lemma
- $\vdash \neg C$

Hilbert Refutations

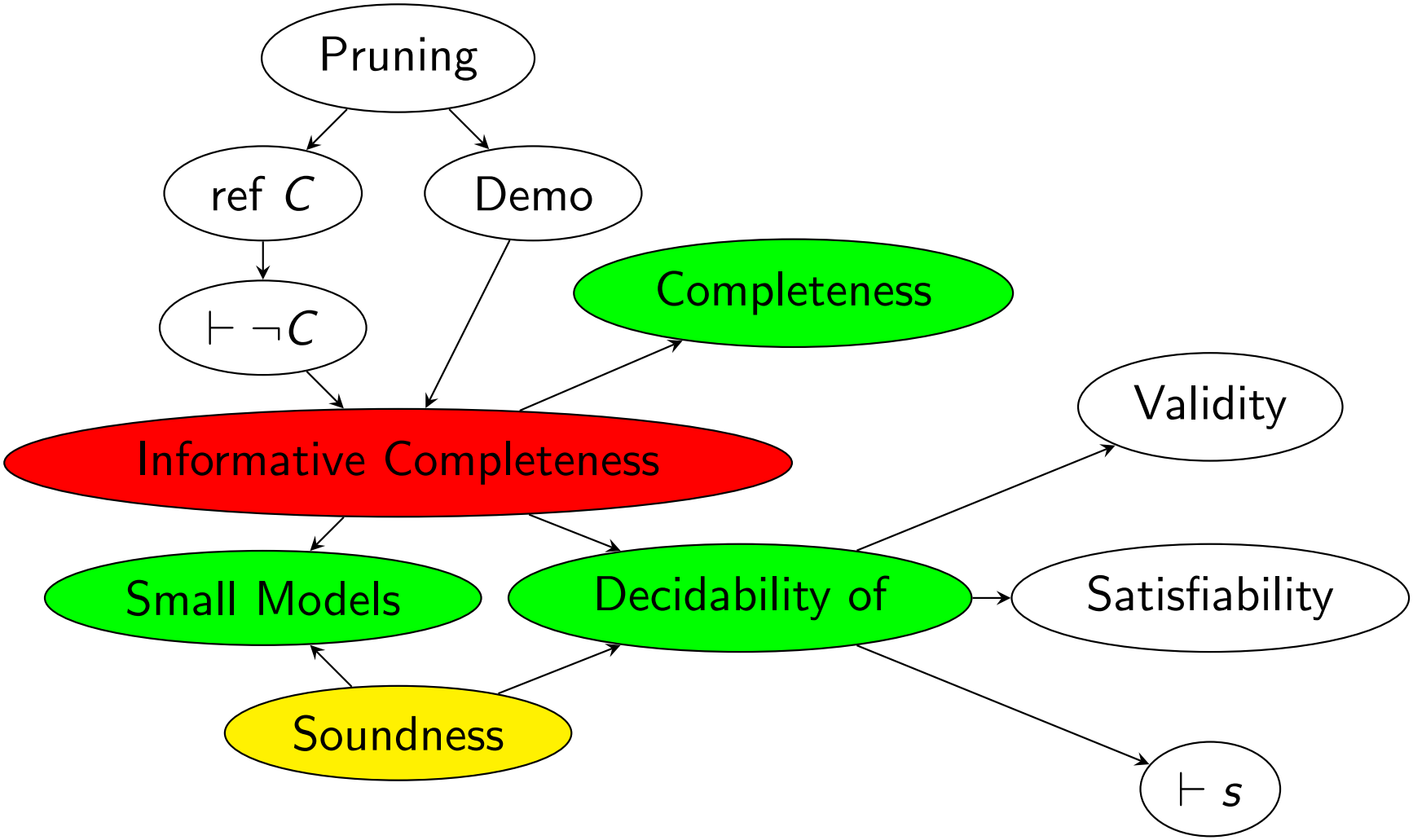
Lemma

Let $S \subseteq S_0$ *be corefutable. If* $C, D \in S$ *and* $C \overset{\alpha}{\not\mapsto}_S D$, *then* $\vdash C \to [\alpha]\neg D$

- Induction on α
- Dualized version of Kozen's and Parikh's "Lemma 1"

Dexter Kozen and Rohit Parikh. An elementary proof of the completeness of PDL. *Theor. Comput. Sci.*, 14:113-118, 1981.

Conclusion



- $\sim$1000 lines of Coq code
- Reusing Christian's libraries for finite sets and Hilbert proofs
- Can be extended to PDL with tests

References


Christian Doczkal. *A Machine-Checked Constructive Metatheory of Computation Tree Logic*. PhD thesis, Saarland University, Mar 2016.


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


David Harel, Dexter Kozen, and Jerzy Tiuryn. *Dynamic Logic*. The MIT Press, 2000.


Dexter Kozen and Rohit Parikh. An elementary proof of the completeness of PDL. *Theor. Comput. Sci.*, 14:113–118, 1981.


Vaughan R. Pratt. Models of program logics. In *20th Annual Symposium on Foundations of Computer Science, San Juan, Puerto Rico, 29-31 October 1979*, pages 115–122, 1979.

Thanks for your attention!
Questions?

Subformula Closure

- If $s \to t \in F$, then $\{s, t\} \subseteq F$.
- If $[a]s \in F$, then $s \in F$.
- If $[\alpha;\beta]s \in F$, then $\{[\alpha][\beta]s, [\beta]s, s\} \subseteq F$.
- If $[\alpha + \beta]s \in F$, then $\{[\alpha]s, [\beta]s, s\} \subseteq F$.
- If $[\alpha^*]s \in F$, then $\{[\alpha][\alpha^*]s, s\} \subseteq F$.