A Formal Completeness Proof for PDL

Second Bachelor Seminar Talk

Joachim Bard
Advisor: Christian Doczkal

September 9, 2016

Outline

Testfree-PDL

Definition

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

Definition

w state of LTS M

$$w \vDash x \qquad \text{given}$$
$$w \vDash \bot := \bot$$
$$w \vDash s \to t := w \vDash s \to w \vDash t$$
$$w \vDash [\alpha]s := \forall v.\, w \overset{\alpha}{\Rightarrow} v \to v \vDash s$$

Semantics

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

Definition

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

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

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

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

Support

- $s^+ \simeq s$, $s^- \simeq \neg s$
- clause C: finite set of signed formulas

$$C \rhd s^\sigma \leftrightarrow s^\sigma \in C \qquad (s \text{ literal: } x, \bot, [a]t)$$

$$C \rhd s \to t^+ \leftrightarrow C \rhd s^- \vee C \rhd t^+$$

$$C \rhd s \to t^- \leftrightarrow C \rhd s^+ \wedge C \rhd t^-$$

$$C \rhd [\alpha;\beta]s^\sigma \leftrightarrow C \rhd [\alpha][\beta]s^\sigma$$

$$C \rhd [\alpha+\beta]s^+ \leftrightarrow C \rhd [\alpha]s^+ \wedge C \rhd [\beta]s^+$$

$$C \rhd [\alpha+\beta]s^- \leftrightarrow C \rhd [\alpha]s^- \vee C \rhd [\beta]s^-$$

$$C \rhd [\alpha^*]s^+ \leftrightarrow C \rhd s^+ \wedge C \rhd [\alpha][\alpha^*]s^+$$

$$C \rhd [\alpha^*]s^- \leftrightarrow C \rhd s^- \vee C \rhd [\alpha][\alpha^*]s^-$$

Informative Completeness

Theorem (Informative Completeness)

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

- attempt to build canonical model

Results:

- completeness
- small model theorem
- several decidability results

Demo

given a finite set of clauses S:

Definition

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

- $s \to t^\sigma \in \mathcal{U} \to \{s^{\overline{\sigma}}, t^\sigma\} \subset \mathcal{U}$
- $[a]s^\sigma \in \mathcal{U} \to s^\sigma \in \mathcal{U}$
- $[\alpha;\beta]s^\sigma \in \mathcal{U} \to \{[\alpha][\beta]s^\sigma, [\beta]s^\sigma, s^\sigma\} \subset \mathcal{U}$
- $[\alpha+\beta]s^\sigma \in \mathcal{U} \to \{[\alpha]s^\sigma, [\beta]s^\sigma, s^\sigma\} \subset \mathcal{U}$
- $[\alpha^*]s^\sigma \in \mathcal{U} \to \{[\alpha][\alpha^*]s^\sigma, s^\sigma\} \subset \mathcal{U}$

Fischer-Ladner closure: $\mathcal{U}$ containing s

Reachability in a Set

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

Definition

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

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

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

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

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

- $C \overset{\alpha}{\rightsquigarrow}_S D \leftrightarrow C \overset{\alpha}{\Rightarrow} D$ given $C \overset{a}{\Rightarrow} D := C \overset{a}{\rightsquigarrow}_S D$

Demo

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

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

Lemma

$C \rhd s^\sigma \to C \vDash s^\sigma$

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

Pruning

- build a demo
- start with $S_0 := \{C \subset \mathcal{U} \mid C \text{ literal and locally consistent}\}$
- C locally consistent: $\bot^+ \notin C \wedge \{x^+, x^-\} \not\subset C$
- remove C iff C contradicts demo condition:
  $C \rhd [\alpha]s^- \in \mathcal{U} \to \exists D \in S.\, C \overset{\alpha}{\rightsquigarrow}_S D \wedge D \rhd s^-$
- results in a demo

Refutations

- give reasons for unsatisfiable clauses

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

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

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

- every removed clause is refutable
- demo is corefutable

Informative Completeness

Theorem (Informative Completeness)

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

build demo S

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

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

Hilbert Refutations

- translate refutations into the Hilbert system
- ref $C := \vdash C \to \bot$, read as $\vdash \bigwedge C \to \bot$

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

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

Hilbert Refutations

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

- induction on α
- focus on $\alpha;\beta$ and α^*

Hilbert Refutations

$$\frac{C \rhd [\alpha][\beta]s^- \qquad \text{coref } S \qquad \nexists D \in S.\, D \rhd s^- \wedge \exists C' \in S.C \overset{\alpha}{\rightsquigarrow}_S C' \wedge C' \overset{\beta}{\rightsquigarrow}_S D}{\text{ref } C}$$

- $\nexists C' \in S.C \overset{\alpha}{\rightsquigarrow}_S C' \wedge C' \rhd [\beta]s^-$
  - use induction hypothesis for α
- $\exists C' \in S.C \overset{\alpha}{\rightsquigarrow}_S C' \wedge C' \rhd [\beta]s^-$
  - we can refute C' but not C
  - idea: order pruning
  - C' satisfies pruning condition for $[\beta]s^-$
  - $\exists D.C' \overset{\beta}{\rightsquigarrow}_S D \wedge D \rhd s^-$

Hilbert Refutations

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

- $\vdash C \to [\alpha^*]s \to \bot$
- $\vdash C \to [\alpha^*]s$
  - $\vdash C \to u$
  - $\vdash u \to s$
  - $\vdash u \to [\alpha]u$
- $I := \{D \in S \mid C \overset{\alpha^*}{\rightsquigarrow}_S D\}$, $u := \bigvee I$
- $I := \{D \in S \mid \nexists D' \in S. D \overset{\alpha^*}{\rightsquigarrow}_S D' \wedge D' \rhd s^-\}$, $u := \bigvee I$
  - $C \in I$
  - $\forall D \in I. D \not\rhd s^-$

Ideas

- $\vdash C \to \bigvee\{D \in S \mid D \triangleright C\}$
- prune by β before α if $\beta < \alpha$
- $C \triangleright s^\sigma \to \vdash C \to s^\sigma$
- change S_0: $\forall C \in S_0.C \triangleright s^+ \vee C \triangleright s^-$
- find u: $\vdash u \to [\alpha]u$
- $\mathcal{R}_\alpha\, C := \{s^+ \mid C \triangleright [\alpha]s^+ \in \mathcal{U}\}$
- $D \triangleright \mathcal{R}_\alpha\, C \to C \overset{\alpha}{\rightsquigarrow}_S D$

References


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


Mark Kaminski. *Incremental Decision Procedures for Modal Logics with Nominals and Eventualities*. PhD thesis, Saarland University, Feb 2012.


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.

Thanks for your attention!
Questions?

Subformula Closure

Definition

$$\begin{aligned}
\mathsf{sub}\, s^\sigma &:= \{s^\sigma\} \\
\mathsf{sub}\, s \to t^\sigma &:= \{s \to t^\sigma\} \cup \mathsf{sub}\, s^{\overline{\sigma}} \cup \mathsf{sub}\, t^\sigma \\
\mathsf{sub}\, [\alpha]s^\sigma &:= \{[\alpha]s^\sigma\} \cup \mathsf{sub}_\Box\, [\alpha]s^\sigma
\end{aligned}$$

Definition

$$\begin{aligned}
\mathsf{sub}_\Box\, [a]s^\sigma &:= \{[a]s^\sigma\} \\
\mathsf{sub}_\Box\, [\alpha^*]s^\sigma &:= \{[\alpha^*]s^\sigma\} \cup \mathsf{sub}_\Box\, [\alpha][\alpha^*]s^\sigma \\
\mathsf{sub}_\Box\, [\alpha;\beta]s^\sigma &:= \{[\alpha;\beta]s^\sigma\} \cup \mathsf{sub}_\Box\, [\alpha][\beta]s^\sigma \cup \mathsf{sub}_\Box\, [\beta]s^\sigma \\
\mathsf{sub}_\Box\, [\alpha+\beta]s^\sigma &:= \{[\alpha+\beta]s^\sigma\} \cup \mathsf{sub}_\Box\, [\alpha]s^\sigma \cup \mathsf{sub}_\Box\, [\beta]s^\sigma
\end{aligned}$$

Hilbert System

Definition

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

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

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

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

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

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

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