A Canonical Model Construction for Iteration-Free PDL with Intersection

Florian Bruse   Daniel Kernberger   Martin Lange

University of Kassel, Germany

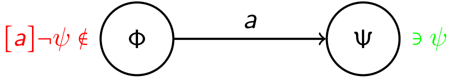
September 22, 2016

Canonical Models

Tool to show completeness of proof calculus (for e.g., ML)

Idea:

- take set of maximally consistent sets of formulas (mcs) as underlying set of structure
- atomic propositions via membership
- $\Phi \xrightarrow{a} \Psi$ iff $[a]\neg\psi \in \Phi$ for no $\psi \in \Psi$



→ (via induction): φ true at Φ iff $\varphi \in \Phi$.

yields satisfiability of any consistent set of formulas, i.e., completeness.

NB: presence of edge depends only on endpoints.

Iteration-Free PDL with Intersection (PDL_0)

fix propositions $\{P, Q, \dots\} = \mathcal{P}$, atomic programs $\{a, b, \dots\} = \mathcal{R}$

Syntax:

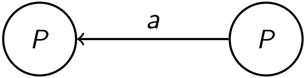
formulas: $\varphi ::= P \mid \varphi \vee \varphi \mid \varphi \wedge \varphi \mid \neg\varphi \mid \langle\alpha\rangle\varphi \mid [\alpha]\varphi$

programs: $\alpha ::= a \mid \alpha;\alpha \mid \alpha \cap \alpha \mid \alpha \cup \alpha \mid \varphi?$

Semantics (sketch) over LTS $\mathcal{T}$:

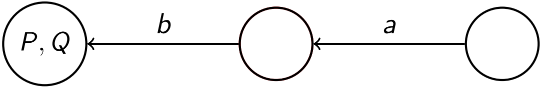
- $\langle\alpha\rangle\varphi$ true at s iff ex. t with $s \xrightarrow{\alpha} t$ and φ true at t
- $s \xrightarrow{a} t$ iff $(s, t) \in a^{\mathcal{T}}$
- $s \xrightarrow{\alpha_1;\alpha_2} t$ iff ex. u with $s \xrightarrow{\alpha_1} u$ and $u \xrightarrow{\alpha_2} t$
- $s \xrightarrow{\alpha_1\cap\alpha_2} t$ iff $s \xrightarrow{\alpha_1} t$ and $s \xrightarrow{\alpha_2} t$
- $s \xrightarrow{\varphi?} t$ iff $s = t$ and φ true at s

$\mathbf{PDL_0}$ in action



$\models P \wedge \langle a \rangle P \wedge [a \cap \top?]\bot$

→ no tree model property



$\not\models \langle a; [b; P?]\neg Q?; b \rangle (P \wedge Q)$

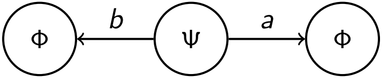
→ convoluted and nested programs hard to conquer inductively

More complications

Consider sat. set Φ (e.g. theory of dead end world)

$\Psi = \bigcup_{\varphi \in \Phi} \{\langle a \rangle \varphi, [a]\varphi, \langle b \rangle \varphi, [b]\varphi\} \cup \{[a \cap b]\bot\}$

Ψ has model:



But no model with only one instance of Φ

→ canonical model needs adaption

Existing constructions not convincing enough

A Proof Calculus for PDL_0

Standard style proof system with derivation rules

$$(\mathtt{MP})\ \frac{\varphi \qquad \varphi \rightarrow \psi}{\psi} \qquad (\mathtt{Gen})\ \frac{\varphi}{[\alpha]\varphi} \qquad (\mathtt{USub})\ \frac{\varphi}{\varphi\ulcorner\psi/p\urcorner}$$

$$(\mathtt{PSub})\ \frac{\varphi \qquad \alpha \Rightarrow \alpha'}{\varphi\ulcorner\langle\alpha'\rangle/\langle\alpha\rangle\urcorner}(pos)$$

and axioms and axiom schemes:

$\alpha \cap \beta \Rightarrow \alpha$

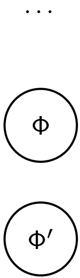
$(p?;\alpha) \cap \beta \Leftrightarrow p?;(\alpha \cap \beta)$

...

Construction of the Canonical Model

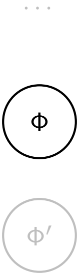
Idea: build “free” structure, i.e., maximally tree-like, no unnecessary connections

Construction of the Canonical Model

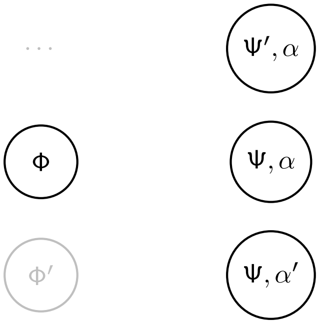


start with mcs, no edges → atomic and box formulas satisfied (generation 0)

Construction of the Canonical Model

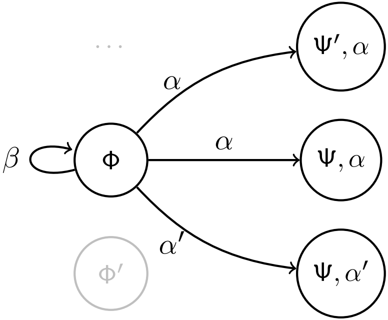


Construction of the Canonical Model



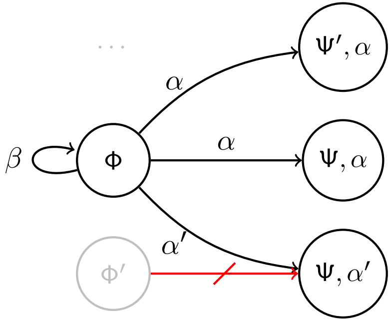
add witnesses for missing diamonds

Construction of the Canonical Model



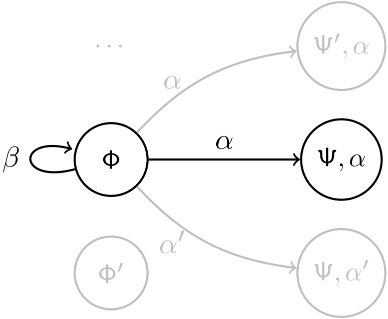
add witnesses for missing diamonds, connect with abstract edges

Construction of the Canonical Model

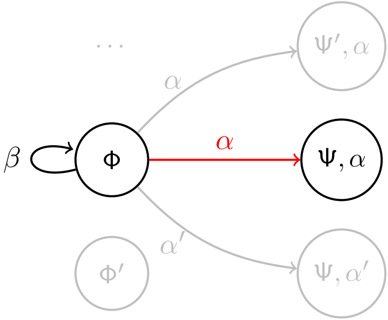


add witnesses for missing diamonds, connect with abstract edges in disjoint fashion

Construction of the Canonical Model



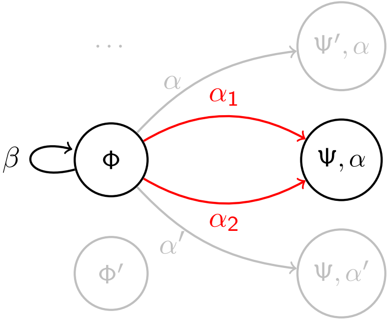
Construction of the Canonical Model



refine iteratively

$\alpha = \alpha_1 \cap \alpha_2$

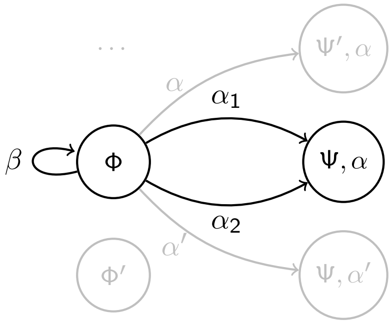
Construction of the Canonical Model



refine iteratively

$\alpha = \alpha_1 \cap \alpha_2$

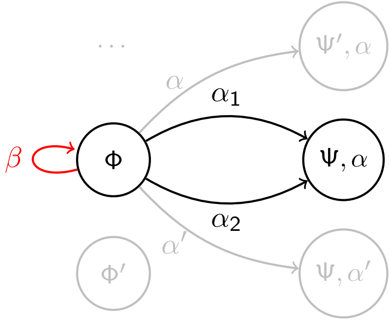
Construction of the Canonical Model



refine iteratively

$\alpha = \alpha_1 \cap \alpha_2$

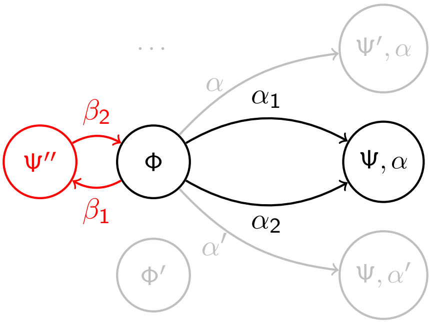
Construction of the Canonical Model



refine iteratively, add intermediate nodes if necessary

$\alpha = \alpha_1 \cap \alpha_2 \qquad \beta = \beta_1 ; \beta_2$

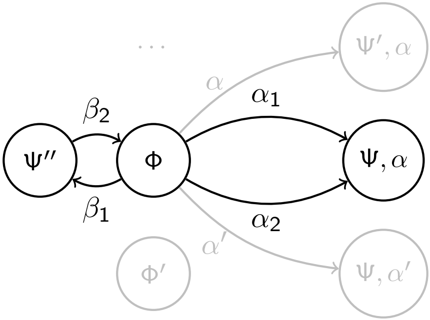
Construction of the Canonical Model



refine iteratively, add intermediate nodes if necessary

$\alpha = \alpha_1 \cap \alpha_2 \qquad \beta = \beta_1 ; \beta_2$

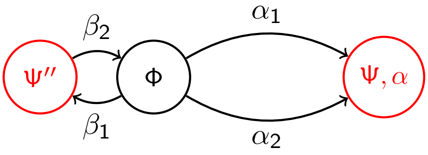
Construction of the Canonical Model



continue inductively until abstract programs converted to concrete programs

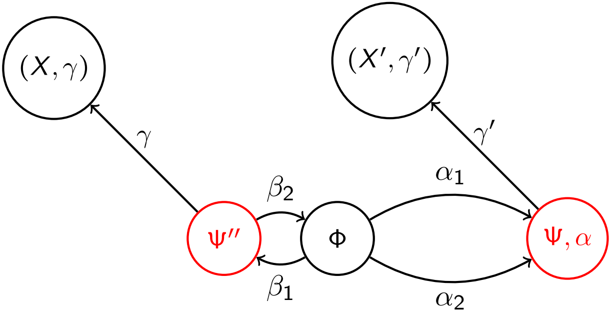
$\alpha = \alpha_1 \cap \alpha_2 \qquad \beta = \beta_1 ; \beta_2$

Construction of the Canonical Model



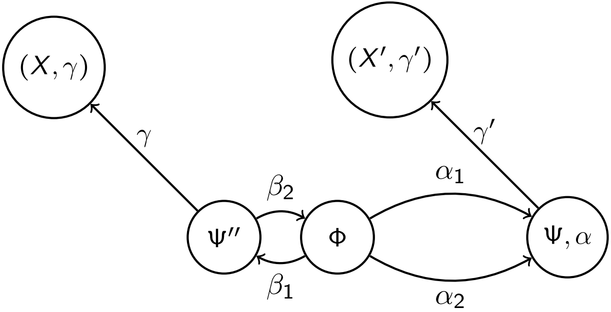
Problem: New unsatisfied diamonds in generation 1 nodes

Construction of the Canonical Model



Repeat Process: Add witnesses (generation 2), refine

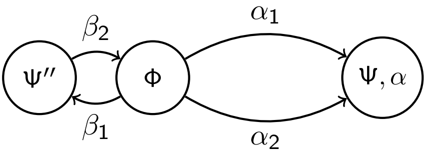
Construction of the Canonical Model



Repeat Process: Add witnesses (generation 2), refine

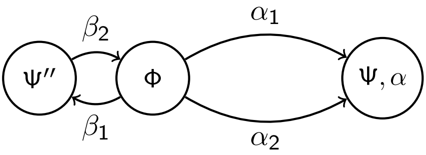
All diamonds satified in limit (generation ω)

Correctness of the Construction



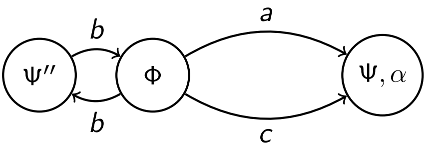
Need to show: φ true at node labelled Φ iff $\varphi \in \Phi$

Correctness of the Construction



In particular:
If $[\alpha]\neg\psi \in \Psi''$ and $\Psi'' \xrightarrow{\alpha} \Psi$, then $\psi \notin \Psi$

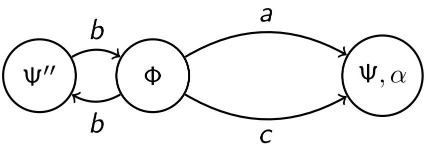
Correctness of the Construction



In particular:

If $[(b;a) \cap (b;c)]\neg P \in \Psi''$ and $\Psi'' \xrightarrow{(b;a)\cap(b;c)} \Psi$, then $P \notin \Psi$

Correctness of the Construction

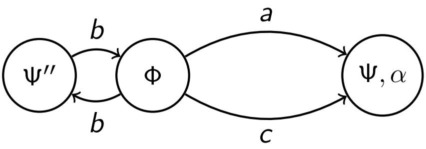


In particular:

If $[(b;a) \cap (b;c)]\neg P \in \Psi''$ and $\Psi'' \xrightarrow{(b;a)\cap(b;c)} \Psi$, then $P \notin \Psi$

Problem: Program unplanned: structure constructed for $b;(a \cap c)$

Correctness of the Construction



In particular:

If $[(b;a) \cap (b;c)]\neg P \in \Psi''$ and $\Psi'' \xrightarrow{(b;a)\cap(b;c)} \Psi$, then $P \notin \Psi$

Problem: Program unplanned: structure constructed for $b;(a \cap c)$
Can rewrite: $[(b;a) \cap (b;c)]\neg P \to [b;(a \cap c)]\neg P$
Correctness of construction provable

End of Talk

Further work:

- Extend to full PDL with intersection, i.e., with Kleene star (weak completeness only)
- Compare present work to existing constructions more thoroughly

Thanks for listening!