Terminating Tableaux for Mini-PDL

Sigurd Schneider

Bachelor’s Thesis Proposal Talk
Advisors: Mark Kaminski, Gert Smolka
Responsible Professor: Gert Smolka

April 30, 2009
Propositional Dynamic Logic

\[ t ::= p \mid \neg t \mid t \land t \mid t \lor t \mid \Diamond \rho t \mid \Box \rho t \]
\[ \rho ::= r \mid \rho^* \mid \rho ; \rho \mid \rho \cup \rho \mid t? \]

- Small Model Property [Fisher and Ladner, 1979]
- Robustly decidable [Giacomo and Massacci, 2000][Abate, Goré, and Widmann, 2009]
Mini-PDL

\[ t ::= p \mid \neg t \mid t \land t \mid t \lor t \mid \diamond \rho t \mid \Box \rho t \]
\[ \rho ::= r \mid r^* \]

- Most important aspect covered: kleene star
- Thus still complex enough
Semantics

Terminating Tableaux for Mini-PDL (Sigurd Schneider)
Semantics
Where do we want to go?

Complete and Terminating Tableau System for Mini-PDL incorporating
  - key ideas from literature
  - elegant proofs
  - pattern-based blocking
Approach to a complete tableau system

- Start with tableaux system for K.

\[
\begin{align*}
R\upharpoonright & \quad \frac{\neg p}{\bot} \quad px \in A \\
R\wedge & \quad \frac{t_1 \wedge t_2}{t_1x, t_2x} \\
R\lor & \quad \frac{t_1 \lor t_2}{t_1x \mid t_2x} \\
R\Box & \quad \frac{\Box rt}{ty} \quad rxy \in \mathcal{N}A \\
R\Diamond & \quad \frac{\Diamond rt}{rxy, ty} \quad y \notin \mathcal{N}A \\
R\Box^{*} & \quad \frac{\Box r^* t}{tx, \Box r(\Box r^* t)x} \\
R\Diamond^{*} & \quad \frac{\Diamond r^* t}{tx \mid \Diamond r(\Diamond r^* t)x}
\end{align*}
\]

- Add the following rules:
Approach to a complete tableau system

- Start with tableaux system for K.

\[
\begin{align*}
\mathcal{R}^- & \quad (\neg p)x \quad px \in A \\
\mathcal{R}^\wedge & \quad (t_1 \wedge t_2)x \quad t_1x, t_2x \\
\mathcal{R}^\vee & \quad (t_1 \vee t_2)x \quad t_1x | t_2x \\
\mathcal{R}^\boxdot & \quad \Box rt x \quad rxy \in \mathcal{N}A \\
\mathcal{R}^\blacklozenge & \quad \lozenge rt x \quad y \notin \mathcal{N}A \\
\mathcal{R}^\blacklozenge^* & \quad \lozenge r^* tx \quad tx | \lozenge r(\lozenge r^* t)x \\
\mathcal{R}^\boxdot^* & \quad \Box r^* tx \quad tx, \Box r(\Box r^* t)x 
\end{align*}
\]

- Add the following rules:
An Infinite Derivation

\[ \Diamond r^* px \]

\[ R \Diamond^* \quad \frac{\Diamond r^* tx}{tx \mid \Diamond r(\Diamond r^* t)x} \]

\[ R \Diamond \quad \frac{\Diamond rtx}{rxy, ty \ y \notin \mathcal{N}A} \]
An Infinite Derivation

\[ \diamond r^* px \]

\[ \downarrow \]

\[ \diamond r(\diamond r^* p)x \]

\[ \mathcal{R} \diamond^* \]

\[ \begin{array}{c}
\diamond r^* tx \\
\hline
\end{array} \]

\[ \begin{array}{c}
\mathcal{R}^* \\
\end{array} \]

\[ \begin{array}{c}
\diamond rtx \\
\hline
\end{array} \]

\[ \begin{array}{c}
\mathcal{R} \diamond \quad \diamond rtx \\
y \notin \mathcal{N}A \\
\end{array} \]

\[ \begin{array}{c}
\mathcal{R}^* \\
\hline
\end{array} \]

\[ \begin{array}{c}
\mathcal{R} \diamond \quad \diamond rt_\nu , ty \\
\end{array} \]

\[ x, y \notin \mathcal{N}A \]
An Infinite Derivation

\[
\begin{align*}
&\Diamond r^* px \\
\downarrow & \\
&\Diamond r(\Diamond r^* p)x \\
\downarrow & \\
rxy & \Diamond r^* py
\end{align*}
\]

**Tableau Rules**

\[
\begin{align*}
R & : \quad \frac{\Diamond r^* tx}{tx \mid \Diamond r(\Diamond r^* t)x} \\
R & : \quad \frac{\Diamond rt x}{rxy, ty \not\in NA}
\end{align*}
\]
An Infinite Derivation

\[ \diamond r^* px \]
\[ \downarrow \]
\[ \diamond r(\diamond r^* p)x \]
\[ \downarrow \]
\[ \diamond r(\diamond r^* p)y \]

\[ \mathcal{R}^* \quad \frac{\diamond r^* tx}{tx \mid \diamond r(\diamond r^* t)x} \]

\[ \mathcal{R} \quad \frac{\diamond rt x}{rxy, ty \quad y \notin \mathcal{N}A} \]
An Infinite Derivation

\[ \diamond r^* px \]
\[ \downarrow \]
\[ \diamond r(\diamond r^* p)x \]
\[ \downarrow \]
\[ \diamond r(\diamond r^* p)y \]
\[ \downarrow \]
\[ ryz \quad \diamond r^* pz \]
\[ \ldots \]

\[ R^* \quad \frac{\diamond r^* tx}{tx \mid \diamond r(\diamond r^* t)x} \]

\[ R \quad \frac{\diamond rtx}{rxy, ty \quad y \notin \mathcal{NA}} \]
The pattern $P_{A}^{\Diamond rt_{x}}$ of a formula $\Diamond rt_{x} \in A$ is defined as
\[ \{ \Diamond rt \} \cup \{ \Box rt \mid \Box rt_{x} \in A \}. \]

$P_{A}^{\Diamond r(\Diamond r^{*}p)x} = P_{A}^{\Diamond r(\Diamond r^{*}p)y} = \{ \Diamond r(\Diamond r^{*}p)x \}$
The pattern $P^r_{tx}$ of a formula $\diamond rtx \in A$ is defined as

$$\{\diamond rt\} \cup \{\Box rt \mid \Box rtx \in A\}.$$
The pattern $P_A^{\Diamond rt x}$ of a formula $\Diamond rt x \in A$ is defined as

$\{\Diamond rt \} \cup \{\Box rt \mid \Box rt x \in A\}$.

$$P_A^{\Diamond r(\Diamond r^* p)x} = P_A^{\Diamond r(\Diamond r^* p)y} = \{\Diamond r(\Diamond r^* p)x\}$$
A Blocked Derivation

\[ \Diamond r^* p x \]
\[ \downarrow \]
\[ \Diamond r (\Diamond r^* p) x \]
\[ \Diamond r^* p y \]
\[ \downarrow \]
\[ \Diamond r (\Diamond r^* p) y \]
\[ \Diamond r^* p z \]
\[ \downarrow \]
\[ p z \]

Derivation is blocked *before* witness is generated.
A Blocked Derivation

\[ \Box r^* p x \]
\[ \Downarrow \]
\[ \Box r(\Box r^* p)x \]
\[ \Downarrow \]
\[ r x y \quad \Box r^* p y \]
\[ \Downarrow \]
\[ \Box r(\Box r^* p)y \]
\[ \Downarrow \]
\[ r y z \quad \Box r^* p z \]
\[ \Downarrow \]
\[ p z \]

Derivation is blocked *before* witness is generated.
A Blocked Derivation

\[ \Diamond r^* p x \]
\[ \downarrow \]
\[ \Diamond r(\Diamond r^* p)x \]
\[ \downarrow \]
\[ r x y \]
\[ \Diamond r^* p y \]
\[ \downarrow \]
\[ \Diamond r(\Diamond r^* p)y \]
\[ \downarrow \]
\[ r y z \]
\[ \Diamond r^* p z \]
\[ \downarrow \]
\[ p z \]

Derivation is blocked before witness is generated.
Different Kinds of Maximal Branches

There are *three* kinds of maximal derivations:

- Verifying derivations that yield a model.
- Falsifying derivations that are inconsistent.
- Blocked derivations, that may or may not be extended to an verifying derivation.
There are *three* kinds of maximal derivations:

- **Verifying derivations** that yield a model.
- **Falsifying derivations** that are inconsistent.
- **Blocked derivations**, that may or may not be extended to an verifying derivation.
There are *three* kinds of maximal derivations:

- Verifying derivations that yield a model.
- Falsifying derivations that are inconsistent.
- Blocked derivations, that may or may not be extended to a verifying derivation.
Different Kinds of Maximal Branches

There are three kinds of maximal derivations:

- Verifying derivations that yield a model.
- Falsifying derivations that are inconsistent.
- Blocked derivations, that may or may not be extended to an verifying derivation.
Proof Strategy

Usually, a completeness proof for a tableaux system shows:

- System terminates.
- If system terminates and branch is consistent, we can construct a model.
- By refutation soundness, completeness follows.

**New strategy**

- Show that if a set of formulas is satisfiable, there exists a verifying derivation in the blocked system.
Minimal Derivations

On every path from the root over a diamond-star formula to its witness, no pattern occurs twice.
Minimal Derivations

On every path from the root over a diamond-star formula to its witness, no pattern occurs twice.
Minimal Derivations

On every path from the root over a diamond-star formula to its witness, no pattern occurs twice.
Minimal Derivations

Minimal Derivation

On every path from the root over a diamond-star formula to its witness, no pattern occurs twice.
Existence of Minimal Derivations

**Desired Theorem**

Let $A$ be a set of Mini-PDL formulas. For every verifying derivation starting from $A$, there is a minimal verifying derivation starting from $A$ which is obtained by shortening.

**Proof Idea:**

\[
\begin{aligned}
&\Diamond r^* px \\ &\rightarrow \Diamond r (\Diamond r^* p)x \\ &\rightarrow \Diamond r^* py \\ &\rightarrow \Diamond r (\Diamond r^* p)y \\ &\rightarrow r (\Diamond r^* p)y \\ &\rightarrow r (\Diamond r^* p)y \\ &\rightarrow ryz \\ &\rightarrow rxy \\ &\rightarrow \Diamond r^* pz \\ &\rightarrow pz
\end{aligned}
\]
Existence of Minimal Derivations

**Desired Theorem**

Let $A$ be a set of Mini-PDL formulas. For every verifying derivation starting from $A$, there is a minimal verifying derivation starting from $A$ which is obtained by shortening.

*Proof Idea:*

\[
\Diamond r^* px \rightarrow \Diamond r(\Diamond r^* p)x \rightarrow \Diamond r^* py \rightarrow py
\]

\[
rxy
\]
Roadmap and Open Problems

- Proving completeness of unconstrained system.
- Formalizing derivations as graphs.

$$\begin{align*}
\text{tx}, \Box r(\Box r^* t)x & \quad \rightarrow \\
\Box r^* tx & \\
\Box r^* tx & \quad \rightarrow \\
tx & \\
\Box r(\Box r^* t)x & 
\end{align*}$$

- Proving minimal derivation existence theorem using derivation graphs.
  - If that does not work, prove existence for every satisfiable set and analyse confluency of derivation relation.
- Does the approach scale to PDL?
References

David Harel and Dexter Kozen and Jerzy Tiuryn

*Dynamic Logic*
MIT Press, 2000

Fischer, M.J. and R. E. Ladner (1979)

*Propositional dynamic logic of regular programs.*


*An On-the-fly Tableau-based Decision Procedure for PDL-satisfiability.*


*Combining deduction and model checking into Tableaux and algorithms for converse-PDL.*
Does it work for full PDL?

\[ \diamond r(\diamond (r; r)^* p)x \]
\[ \downarrow \]
\[ rxy \]
\[ \diamond (r; r)^* py \]
\[ \downarrow \]
\[ \diamond (r; r)(\diamond (r; r)^* p)y \]
\[ \downarrow \]
\[ \diamond r(\diamond r(\diamond (r; r)^* p))y \]
\[ \downarrow \]
\[ ryz \]
\[ \diamond r(\diamond (r; r)^* p)z \]
\[ \downarrow \]
\[ rza \]
\[ \diamond (r; r)^* pa \]
\[ \downarrow \]
\[ pa \]

\[ \diamond (r; r)^* px \]
\[ \downarrow \]
\[ \diamond (r; r)(\diamond (r; r)^* p)x \]
\[ \downarrow \]
\[ \diamond r(\diamond r(\diamond (r; r)^* p))x \]
\[ \downarrow \]
\[ rxy' \]
\[ \diamond r(\diamond (r; r)^* p)y' \]
\[ \downarrow \]
\[ ry'z' \]
\[ \diamond (r; r)^* pz' \]
\[ \downarrow \]
\[ pz' \]
Does it work for full PDL?

\[ \Diamond r(\Diamond (r; r)^p)x \]

\[ rxy \]

\[ \Diamond r(\Diamond (r; r)^p)z \]

\[ rza \]

\[ (r; r)^p y \]

\[ \Diamond (r; r)^p y \]

\[ rxy' \]

\[ \Diamond (r; r)(\Diamond (r; r)^p)x \]

\[ \Diamond r(\Diamond (r; r)^p)x \]

\[ ryz \]

\[ \Diamond r(\Diamond (r; r)^p)y \]

\[ ryz' \]

\[ \Diamond r(\Diamond (r; r)^p)z \]

\[ rya' \]

\[ (r; r)^p z' \]

\[ \Diamond (r; r)^p z' \]

\[ pz' \]
Does it work for full PDL?

\( \Diamond r(\Diamond (r; r)^* p)x \)

\( rxy \)

\( \Diamond (r; r)^* py \)

\( \Diamond (r; r)(\Diamond (r; r)^* p)y \)

\( \Diamond r(\Diamond r(\Diamond (r; r)^* p))y \)

\( ryz \)

\( \Diamond r(\Diamond (r; r)^* p)z \)

\( rz\alpha \)

\( \Diamond (r; r)^* pa \)

\( pa \)

\( \Diamond (r; r)^* px \)

\( \Diamond (r; r)^* py \)

\( \Diamond (r; r)(\Diamond (r; r)^* p)x \)

\( \Diamond r(\Diamond r(\Diamond (r; r)^* p))x \)

\( rxy' \)

\( \Diamond r(\Diamond (r; r)^* p)y' \)

\( ry'z' \)

\( \Diamond (r; r)^* pz' \)

\( pz' \)
Semantics

\[ \vdash = \lambda px. \neg px \quad \vdash : (IB)IB \]
\[ \hat{\wedge} = \lambda pqx. px \land qx \quad \hat{\wedge} : (IB)(IB)IB \]
\[ \hat{\vee} = \lambda pqx. px \lor qx \quad \hat{\vee} : (IB)(IB)IB \]
\[ \lozenge = \lambda rp x. \exists y. rxy \land py \quad \lozenge : (IIB)(IB)IB \]
\[ \Box = \lambda rp x. \forall y. rxy \implies py \quad \Box : (IIB)(IB)IB \]
\[ 0 = \lambda rxy. x = y \quad 0 : (IIB)IIB \]
\[ n = \lambda rxy. \exists z. rxz \land r^{n-1}zy \quad n : (IIB)IIB \quad n \in \mathbb{N}, n > 0 \]
\[ * = \lambda rxy. \exists n \in \mathbb{N}. r^n xy \quad * : (IIB)IIB \]
A derivation with a box

\[ \square r^* (\Diamond rp) x \]

\[ \square r (\square r^* (\Diamond rp)) x \quad \Diamond rpx \]

\[ rxy \quad py \]

\[ \square r^* (\Diamond rp) y \]

\[ \square r (\square r^* (\Diamond rp)) y \quad \Diamond r^* py \]

\[ ryz \quad pz \]

\[ \square r^* (\Diamond rp) z \]

\[ \ldots \]
Why does the construction of a minimal derivation terminate?

- Scan through each path from the root in some order.
- If a processed pattern occurs, cut everything beyond off. Examine every section between duplicate patterns:
  - If there is no witness path running over the second occurrence, cut the direct witness off.
  - If there is a witness path running over the second occurrence, shorten the derivation.
- Patterns occurring on a processed path can be cut off instantly. The stock of patterns is finite.
Tableau Rules

\[
\begin{align*}
\mathcal{R}_\neg & \quad \frac{(\neg p)x}{\perp} \quad px \in A \\
\mathcal{R}_\land & \quad \frac{(t_1 \land t_2)x}{t_1x, t_2x} \\
\mathcal{R}_\lor & \quad \frac{(t_1 \lor t_2)x}{t_1x \mid t_2x} \\
\mathcal{R}_\Box & \quad \frac{\Box r^* tx}{tx, \Box r(\Box r^* t)x} \\
\mathcal{R}_\Diamond & \quad \frac{\Diamond r^* tx}{tx \mid \Diamond r(\Diamond r^* t)x} \\
\mathcal{R}_\Diamond & \quad \frac{\Diamond rtx}{rxy, ty} \quad y \notin \mathcal{N}A \\
\mathcal{R}_\Box & \quad \frac{\Box rtx}{ty} \quad rxy \in \mathcal{N}A
\end{align*}
\]