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

$$
\begin{aligned}
t &::= p \mid \dot{\neg} t \mid t \mathbin{\dot\wedge} t \mid t \mathbin{\dot\vee} t \mid \Diamond \rho t \mid \Box \rho t \\
\rho &::= r \mid \rho^* \mid \rho ; \rho \mid \rho \cup \rho \mid t?
\end{aligned}
$$

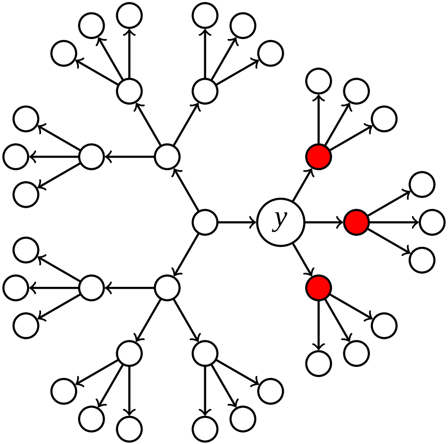
- Small Model Property [Fisher and Ladner, 1979]
- Robustly decidable [Giacomo and Massacci, 2000][Abate, Goré, and Widmann, 2009]

Mini-PDL

$$
\begin{aligned}
t &::= p \mid \dot{\neg} t \mid t \dot{\wedge} t \mid t \dot{\vee} t \mid \Diamond \rho t \mid \Box \rho t \\
\rho &::= r \mid r^*
\end{aligned}
$$

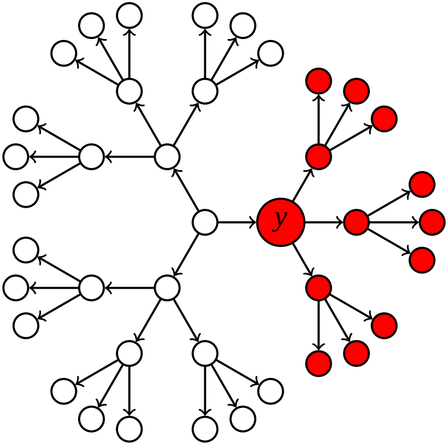
- Most important aspect covered: kleene star
- Thus still complex enough

Semantics



$\Box r p y$

Semantics



$\Box r^* p y$

Where do we want to go?

Complete and Terminating Tabelau 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.

$$\mathscr{R}_{\dot\neg} \ \frac{(\dot\neg p)x}{\bot} \ px \in A \qquad \mathscr{R}_{\dot\wedge} \ \frac{(t_1 \dot\wedge t_2)x}{t_1x\,,\,t_2x} \qquad \mathscr{R}_{\dot\vee} \ \frac{(t_1 \dot\vee t_2)x}{t_1x \mid t_2x}$$

$$\mathscr{R}_{\Box} \ \frac{\Box rtx}{ty} \ rxy \in \mathscr{N}A \qquad \mathscr{R}_{\Diamond} \ \frac{\Diamond rtx}{rxy\,,\,ty} \ y \notin \mathscr{N}A$$

- Add the following rules:

$$\mathscr{R}_{\Box^*} \ \frac{\Box r^* tx}{tx, \Box r(\Box r^* t)x} \qquad \mathscr{R}_{\Diamond^*} \ \frac{\Diamond r^* tx}{tx \mid \Diamond r(\Diamond r^* t)x}$$

Approach to a complete tableau system

- Start with tableaux system for K.

$$\mathscr{R}_{\dot\neg}\ \frac{(\dot\neg p)x}{\perp}\ px \in A \qquad \mathscr{R}_{\dot\wedge}\ \frac{(t_1 \dot\wedge t_2)x}{t_1x\,,\ t_2x} \qquad \mathscr{R}_{\dot\vee}\ \frac{(t_1 \dot\vee t_2)x}{t_1x \mid t_2x}$$

$$\mathscr{R}_{\Box}\ \frac{\Box rtx}{ty}\ rxy \in \mathscr{N}A \qquad \mathscr{R}_{\Diamond}\ \frac{\Diamond rtx}{rxy\,,\ ty}\ y \notin \mathscr{N}A$$

- Add the following rules:

$$\mathscr{R}_{\Box^*}\ \frac{\Box r^* tx}{tx, \Box r(\Box r^* t)x} \qquad \mathscr{R}_{\Diamond^*}\ \frac{\Diamond r^* tx}{tx \mid \Diamond r(\Diamond r^* t)x}$$

An Infinite Derivation

$\Diamond r^* px$

$$\mathcal{R}_{\Diamond^*} \quad \frac{\Diamond r^* tx}{tx \mid \Diamond r(\Diamond r^* t)x}$$

$$\mathcal{R}_{\Diamond} \quad \frac{\Diamond rtx}{rxy\,,\, ty} \quad y \notin \mathcal{N}A$$

An Infinite Derivation

$$\Diamond r^* p x$$

$$\downarrow$$

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

$$\mathscr{R}_{\Diamond^*} \quad \frac{\Diamond r^* t x}{t x \mid \Diamond r(\Diamond r^* t) x}$$

$$\mathscr{R}_{\Diamond} \quad \frac{\Diamond r t x}{r x y\,,\, t y} \quad y \notin \mathscr{N} A$$

An Infinite Derivation

$$\begin{tikzcd} & \Diamond r^* p x \arrow[d] & \\ & \Diamond r(\Diamond r^* p)x \arrow[dl] \arrow[dr] & \\ rxy & & \Diamond r^* p y \end{tikzcd}$$

$$\mathscr{R}_{\Diamond^*} \quad \frac{\Diamond r^* t x}{tx \mid \Diamond r(\Diamond r^* t)x}$$

$$\mathscr{R}_{\Diamond} \quad \frac{\Diamond r t x}{rxy\,,\, ty} \quad y \notin \mathscr{N}A$$

An Infinite Derivation

$$\begin{tikzcd}[column sep=small]
 & \Diamond r^* p x \arrow[d] & \\
 & \Diamond r(\Diamond r^* p)x \arrow[dl] \arrow[dr] & \\
rxy & & \Diamond r^* p y \arrow[d] \\
 & & \Diamond r(\Diamond r^* p)y
\end{tikzcd}$$

$$\mathscr{R}_{\Diamond^*} \quad \frac{\Diamond r^* t x}{tx \mid \Diamond r(\Diamond r^* t)x}$$

$$\mathscr{R}_{\Diamond} \quad \frac{\Diamond r t x}{rxy\,,\, ty} \quad y \notin \mathscr{N}A$$

An Infinite Derivation

$$\begin{tikzcd}[column sep=small]
 & \Diamond r^* p x \arrow[d] & & \\
 & \Diamond r(\Diamond r^* p) x \arrow[dl] \arrow[dr] & & \\
r x y & & \Diamond r^* p y \arrow[d] & \\
 & & \Diamond r(\Diamond r^* p) y \arrow[dl] \arrow[dr] & \\
 & r y z & & \Diamond r^* p z \\
 & & & \ldots
\end{tikzcd}$$

$$\mathscr{R}_{\Diamond^*} \quad \frac{\Diamond r^* t x}{t x \mid \Diamond r(\Diamond r^* t) x}$$

$$\mathscr{R}_{\Diamond} \quad \frac{\Diamond r t x}{r x y \, , \, t y} \quad y \notin \mathscr{N}A$$

Pattern Based Blocking

$$\begin{tikzcd}
 & \Diamond r^* p x \arrow[d] & & \\
 & \Diamond r(\Diamond r^* p) x \arrow[dl] \arrow[dr] & & \\
rxy & & \Diamond r^* p y \arrow[d] & \\
 & & \Diamond r(\Diamond r^* p) y \arrow[dl] \arrow[dr] & \\
 & ryz & & \Diamond r^* p z \\
 & & & \dots
\end{tikzcd}$$

- The pattern $P_A^{\Diamond rtx}$ of a formula $\Diamond rtx \in A$ is defined as $\{\Diamond rt\} \cup \{\Box rt \mid \Box rtx \in A\}$.
- $P_A^{\Diamond r(\Diamond r^* p)x} = P_A^{\Diamond r(\Diamond r^* p)y} = \{\Diamond r(\Diamond r^* p)x\}$

Pattern Based Blocking

$$\begin{tikzcd}
& \Diamond r^* p x \arrow[d] & & \\
& \Diamond r(\Diamond r^* p)x \arrow[dl] \arrow[dr] & & \\
rxy & & \Diamond r^* p y \arrow[d] & \\
& & \Diamond r(\Diamond r^* p)y \arrow[dl] \arrow[dr] & \\
& ryz & & \Diamond r^* p z \\
& & & \ldots
\end{tikzcd}$$

- The pattern $P_A^{\Diamond rtx}$ of a formula $\Diamond rtx \in A$ is defined as $\{\Diamond rt\} \cup \{\Box rt \mid \Box rtx \in A\}$.
- $P_A^{\Diamond r(\Diamond r^* p)x} = P_A^{\Diamond r(\Diamond r^* p)y} = \{\Diamond r(\Diamond r^* p)x\}$

Pattern Based Blocking

$$\begin{tikzcd}
 & \Diamond r^* p x \arrow[d] & & \\
 & \boxed{\Diamond r(\Diamond r^* p) x} \arrow[dl] \arrow[dr] & & \\
rxy & & \Diamond r^* p y \arrow[d] & \\
 & & \boxed{\Diamond r(\Diamond r^* p) y} \arrow[dl] \arrow[dr] & \\
 & ryz & & \Diamond r^* p z \\
 & & & \dots
\end{tikzcd}$$

- The pattern $P_A^{\Diamond rtx}$ of a formula $\Diamond rtx \in A$ is defined as $\{\Diamond rt\} \cup \{\Box rt \mid \Box rtx \in A\}$.
- $P_A^{\Diamond r(\Diamond r^* p)x} = P_A^{\Diamond r(\Diamond r^* p)y} = \{\Diamond r(\Diamond r^* p)x\}$

A Blocked Derivation

$$
\begin{array}{ccccc}
\Diamond r^* p x & & & & \\
\downarrow & & & & \\
\boxed{\Diamond r(\Diamond r^* p) x} & & & & \\
\swarrow \quad \searrow & & & & \\
rxy \qquad \Diamond r^* p y & & & & \\
\quad\quad\quad \downarrow & & & & \\
\quad\quad\quad \boxed{\Diamond r(\Diamond r^* p) y} & & & & \\
\quad\quad\quad \swarrow \quad \searrow & & & & \\
\quad\quad\quad ryz \qquad \Diamond r^* p z & & & & \\
\quad\quad\quad\quad\quad\quad \downarrow & & & & \\
\quad\quad\quad\quad\quad\quad pz & & & &
\end{array}
$$

Derivation is blocked *before* witness is generated.

A Blocked Derivation

$$
\begin{array}{ccccc}
 & \Diamond r^* p x & & & \\
 & \downarrow & & & \\
 & \boxed{\Diamond r(\Diamond r^* p) x} & & & \\
\swarrow & & \searrow & & \\
rxy & & \Diamond r^* p y & & \\
 & & \downarrow & & \\
 & & \boxed{\Diamond r(\Diamond r^* p) y} & & \\
 & \swarrow & & \searrow & \\
 & ryz & & \Diamond r^* p z & \\
 & & & \downarrow & \\
 & & & pz &
\end{array}
$$

Derivation is blocked *before* witness is generated.

A Blocked Derivation

$$\Diamond r^* p x$$

$$\downarrow$$

$$\boxed{\Diamond r(\Diamond r^* p) x}$$

$$\swarrow \qquad \searrow$$

$$rxy \qquad \Diamond r^* p y$$

$$\downarrow$$

$$\boxed{\Diamond r(\Diamond r^* p) y}$$

$$\swarrow \qquad \searrow$$

$$ryz \qquad \Diamond r^* p z$$

$$\downarrow$$

$$pz$$

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.

Different Kinds of Maximal Branches

$$
\begin{tikzcd}
 & \Diamond r^* px \arrow[d] & \\
 & \boxed{\Diamond r(\Diamond r^* p)x} \arrow[dl] \arrow[dr] & \\
rxy & & \Diamond r^* py \arrow[d] \\
 & & py
\end{tikzcd}
$$

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.

Different Kinds of Maximal Branches

$$\begin{tikzcd} px \arrow[dr] & & \dot{\neg} px \arrow[dl] \\ & \dot{\perp} & \end{tikzcd}$$

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.

Different Kinds of Maximal Branches

$$\Diamond r^* p x$$
$$\downarrow$$
$$\boxed{\Diamond r(\Diamond r^* p) x}$$
$$\swarrow \qquad \searrow$$
$$rxy \qquad \Diamond r^* p y$$
$$\downarrow$$
$$\boxed{\Diamond r(\Diamond r^* p) y}$$
$$\swarrow \qquad \searrow$$
$$ryz \qquad \Diamond r^* p z$$
$$\downarrow$$
$$pz$$

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

$$
\begin{tikzcd}
 & \Diamond r^* p x \arrow[d] & & \\
 & \boxed{\Diamond r(\Diamond r^* p) x} \arrow[dl] \arrow[dr] & & \\
rxy & & \Diamond r^* p y \arrow[d] & \\
 & & \boxed{\Diamond r(\Diamond r^* p) y} \arrow[dl] \arrow[dr] & \\
 & ryz & & \Diamond r^* p z \arrow[d] \\
 & & & pz
\end{tikzcd}
$$

$$
\begin{tikzcd}
 & \Diamond r^* p x \arrow[d] & \\
 & \boxed{\Diamond r(\Diamond r^* p) x} \arrow[dl] \arrow[dr] & \\
rxy & & \Diamond r^* p y \arrow[d] \\
 & & py
\end{tikzcd}
$$

Minimal Derivation

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

Minimal Derivations

$$\Diamond r^* p x$$
$$\downarrow$$
$$\boxed{\Diamond r(\Diamond r^* p) x}$$
$$\swarrow \qquad \searrow$$
$$rxy \qquad \Diamond r^* p y$$
$$\downarrow$$
$$\boxed{\Diamond r(\Diamond r^* p) y}$$
$$\swarrow \qquad \searrow$$
$$ryz \qquad \Diamond r^* p z$$
$$\downarrow$$
$$pz$$

$$\Diamond r^* p x$$
$$\downarrow$$
$$\Diamond r(\Diamond r^* p) x$$
$$\swarrow \qquad \searrow$$
$$rxy \qquad \Diamond r^* p y$$
$$\downarrow$$
$$py$$

Minimal Derivation

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

Minimal Derivations

$$\begin{tikzcd}[column sep=small]
 & \Diamond r^* p x \arrow[d] & & \\
 & \boxed{\Diamond r(\Diamond r^* p) x} \arrow[dl] \arrow[dr] & & \\
r x y & & \Diamond r^* p y \arrow[d] & \\
 & & \boxed{\Diamond r(\Diamond r^* p) y} \arrow[dl] \arrow[dr] & \\
 & r y z & & \Diamond r^* p z \arrow[d] \\
 & & & p z
\end{tikzcd}$$

$$\begin{tikzcd}[column sep=small]
 & \Diamond r^* p x \arrow[d] & \\
 & \boxed{\Diamond r(\Diamond r^* p) x} \arrow[dl] \arrow[dr] & \\
r x y & & \Diamond r^* p y \arrow[d] \\
 & & p y
\end{tikzcd}$$

Minimal Derivation

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

Minimal Derivations

$$
\begin{array}{ccc}
 & \Diamond r^* p x & \\
 & \downarrow & \\
 & \boxed{\Diamond r(\Diamond r^* p) x} & \\
 \swarrow & & \searrow \\
 rxy & & \Diamond r^* p y \\
 & & \downarrow \\
 & & \boxed{\Diamond r(\Diamond r^* p) y} \\
 & \swarrow & & \searrow \\
 & ryz & & \Diamond r^* p z \\
 & & & \downarrow \\
 & & & pz
\end{array}
$$

$$
\begin{array}{ccc}
 & \Diamond r^* p x & \\
 & \downarrow & \\
 & \boxed{\Diamond r(\Diamond r^* p) x} & \\
 \swarrow & & \searrow \\
 rxy & & \Diamond r^* p y \\
 & & \downarrow \\
 & & py
\end{array}
$$

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:

$$
\begin{tikzcd}
 & & & & \Diamond r^* pz \arrow[r] & pz \\
 & & \Diamond r^* py \arrow[r] & \boxed{\Diamond r(\Diamond r^* p) y} \arrow[ur] \arrow[dr] & & \\
\Diamond r^* px \arrow[r] & \boxed{\Diamond r(\Diamond r^* p) x} \arrow[ur] \arrow[dr] & & & ryz & \\
 & & rxy & & &
\end{tikzcd}
$$

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:

$$\begin{tikzcd}
 & & \Diamond r^* p y \arrow[r] & p y \\
\Diamond r^* p x \arrow[r] & \boxed{\Diamond r(\Diamond r^* p) x} \arrow[ur] \arrow[dr] & & \\
 & & r x y &
\end{tikzcd}$$

Roadmap and Open Problems

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

$$\mathscr{R}_{\square^*} \quad \frac{\square r^* tx}{tx, \square r(\square r^* t)x}$$

$$\begin{array}{ccc} & \square r^* tx & \\ \swarrow & & \searrow \\ tx & & \square r(\square r^* t)x \end{array}$$

- 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

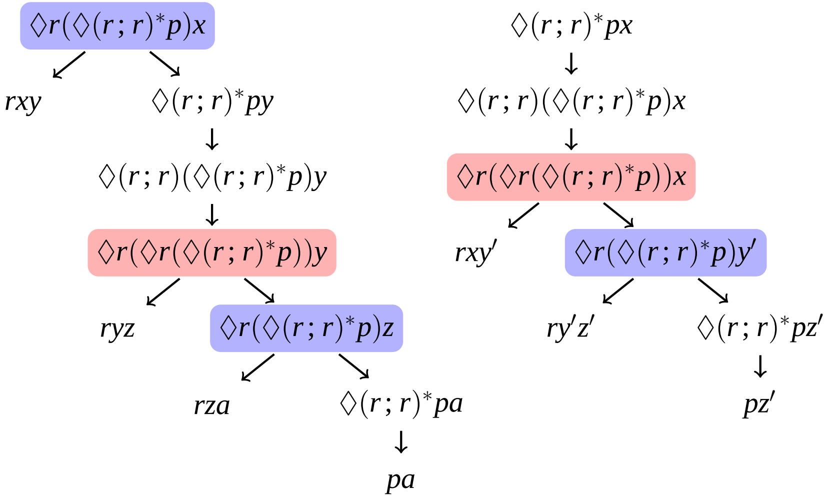
David Harel and Dexter Kozen and Jerzy Tiuryn
Dynamic Logic
MIT Press, 2000

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

Abate, P., Goré, R., and Widmann, F. (2009)
An On-the-fly Tableau-based Decision Procedure for PDL-satisfiability.
Electron. Notes Theor. Comput. Sci. 231 (Mar. 2009), 191-209.

de Giacomo, G. and Massacci, F. (2000)
Combining deduction and model checking into Tableaux and algorithms for converse-PDL.
Inf. Comput. 162, 1/2 (Oct. 2000), 117-137.

Does it work for full PDL?



Does it work for full PDL?

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

$$\swarrow \qquad \searrow$$

$$rxy \qquad \Diamond(r;r)^* py$$

$$\downarrow$$

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

$$\downarrow$$

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

$$\swarrow \qquad \searrow$$

$$ryz \qquad \Diamond r(\Diamond(r;r)^* p)z$$

$$\swarrow \qquad \searrow$$

$$rza \qquad \Diamond(r;r)^* pa$$

$$\downarrow$$

$$pa$$

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

$$\downarrow$$

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

$$\downarrow$$

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

$$\swarrow \qquad \searrow$$

$$rxy' \qquad \Diamond r(\Diamond(r;r)^* p)y'$$

$$\swarrow \qquad \searrow$$

$$ry'z' \qquad \Diamond(r;r)^* pz'$$

$$\downarrow$$

$$pz'$$

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
        - $\Diamond r(\Diamond(r;r)^{*}p)z$
          - rza
          - $\Diamond(r;r)^{*}pa$
            - pa

- $\Diamond(r;r)^{*}px$
  - $\Diamond(r;r)(\Diamond(r;r)^{*}p)x$
    - $\Diamond r(\Diamond r(\Diamond(r;r)^{*}p))x$
      - rxy'
      - $\Diamond r(\Diamond(r;r)^{*}p)y'$
        - $ry'z'$
        - $\Diamond(r;r)^{*}pz'$
          - pz'

Semantics

$$
\begin{array}{lll}
\dot{\neg} = \lambda px.\neg px & \dot{\neg} : (IB)IB & \\
\dot{\wedge} = \lambda pqx.\ px \wedge qx & \dot{\wedge} : (IB)(IB)IB & \\
\dot{\vee} = \lambda pqx.\ px \vee qx & \dot{\vee} : (IB)(IB)IB & \\
\Diamond = \lambda rpx.\ \exists y.\ rxy \wedge py & \Diamond : (IIB)(IB)IB & \\
\Box = \lambda rpx.\ \forall y.\ rxy \Longrightarrow py & \Box : (IIB)(IB)IB & \\
{}^{0} = \lambda rxy.\ x = y & {}^{0} : (IIB)IIB & \\
{}^{n} = \lambda rxy.\ \exists z.\ rxz \ \wedge \ r^{n-1}zy & {}^{n} : (IIB)IIB & n \in \mathbb{N}, n > 0 \\
{}^{*} = \lambda rxy.\ \exists n \in \mathbb{N}. r^{n}xy & {}^{*} : (IIB)IIB &
\end{array}
$$

A derivation with a box

$$
\begin{tikzcd}
 & \Box r^*(\Diamond rp)x \arrow[dl] \arrow[dr] & & \\
\Box r(\Box r^*(\Diamond rp))x \arrow[ddr, bend right] & & \Diamond rpx \arrow[dl] \arrow[dr] & \\
 & rxy \arrow[d] & & py \\
 & \Box r^*(\Diamond rp)y \arrow[dl] \arrow[dr] & & \\
\Box r(\Box r^*(\Diamond rp))y \arrow[ddr, bend right] & & \Diamond r^*py \arrow[dl] \arrow[dr] & \\
 & ryz \arrow[d] & & pz \\
 & \Box r^*(\Diamond rp)z & & \\
 & \ldots & &
\end{tikzcd}
$$

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 everthing beyond off. Examine every section between duplicate patterns:
  - If there is no witness path running over the second occurence, cut the direct witness off.
  - If there is a witness path running over the second occurence, shorten the derivation.
- Patterns occuring on a processed path can be cut off instantly. The stock of patterns is finite.

Tableau Rules

$$\mathscr{R}_{\dot\neg} \quad \frac{(\dot\neg p)x}{\perp} \quad px \in A \qquad \mathscr{R}_{\dot\wedge} \quad \frac{(t_1 \dot\wedge t_2)x}{t_1x\,,\, t_2x} \qquad \mathscr{R}_{\dot\vee} \quad \frac{(t_1 \dot\vee t_2)x}{t_1x \mid t_2x}$$

$$\mathscr{R}_{\Diamond^*} \quad \frac{\Diamond r^* tx}{tx \mid \Diamond r(\Diamond r^* t)x} \qquad \mathscr{R}_{\Box^*} \quad \frac{\Box r^* tx}{tx, \Box r(\Box r^* t)x}$$

$$\mathscr{R}_{\Diamond} \quad \frac{\Diamond rtx}{rxy\,,\, ty} \quad y \notin \mathscr{N}A \qquad \mathscr{R}_{\Box} \quad \frac{\Box rtx}{ty} \quad rxy \in \mathscr{N}A$$