Propositional Dynamic Logic

Sigurd Schneider

Bachelor Seminar
Advisors: Mark Kaminski, Gert Smolka
Responsible Professor: Gert Smolka

30. Januar 2009

Syntax

$$t \ ::= \ p \mid \dot{\bot} \mid t \dot{\rightarrow} t \mid \Box \rho t \mid \dot{\top} \mid \dot{\neg} t \mid t \mathbin{\dot{\wedge}} t \mid t \mathbin{\dot{\vee}} t \mid \Diamond \rho t$$

$$\rho ::= r \mid \rho ; \rho \mid \rho \cup \rho \mid \rho^* \mid t?$$

Syntax

$$t \ ::= \ p \mid \dot{\bot} \mid t \dot{\rightarrow} t \mid \Box\rho t \mid \dot{\top} \mid \dot{\neg} t \mid t \dot{\wedge} t \mid t \dot{\vee} t \mid \Diamond\rho t$$

$$\rho ::= r \mid \rho;\rho \mid \rho \cup \rho \mid \rho^* \mid t?$$

$\Phi, (\Phi_0)$ denotes the set of all (atomic) predicates

$\Pi, (\Pi_0)$ denotes the set of all (atomic) programs

Semantics

$$\dot\bot = \lambda x.\bot \qquad \dot\bot : IB$$

$$\dot\to = \lambda pqx.\ px \to qx \qquad \dot\to : (IB)(IB)IB$$

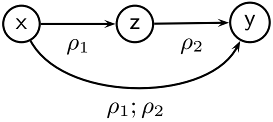
$$\Box = \lambda rpx.\ \forall y.\ rxy \to py \qquad \Box : (IIB)(IB)IB$$

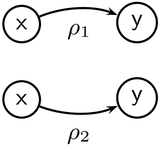
$$* = \lambda \rho xy.\ (x,y) \text{ in refl. transitive closure of } \rho \qquad * : (IIB)IIB$$

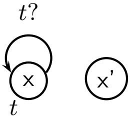
$$; = \lambda \rho_1 \rho_2 xy.\ \exists z.\ \rho_1 xz \wedge \rho_2 zy \qquad ; : (IIB)(IIB)IIB$$

$$\cup = \lambda \rho_1 \rho_2 xy.\ \rho_1 xy \vee \rho_2 xy \qquad \cup : (IIB)(IIB)IIB$$

$$? = \lambda txy.\ ty \wedge x = y \qquad ? : (IB)IIB$$







Interpretation

A modal interpretation $\mathcal{I}$ is an interpretation of simple type theory that interprets

- B as the set $\{0, 1\}$
- I as a nonempty set
- the logical constants as usual
- the modal constants according to their defining equations

Let $t \in \Phi,\ \rho \in \Pi,\ x, y \in I$. By abuse of notation, we define:

$$x \xrightarrow{\rho} y \iff \hat{\mathcal{I}}\rho x y = 1$$

$$tx \iff \hat{\mathcal{I}}tx = 1$$

$$\mathcal{L}x := \{t \mid \hat{\mathcal{I}}tx = 1\}$$

Some Properties

Dynamic Logic originates from Hoare Logic [Pratt, 1976]
Idea: reasoning in terms of input/output relations.
PDL is the propositional subset, it covers regular programs.

```
while t do
  ρ
end
```

$(t?; \rho)^*; \dot{\neg} t?$

PDL is not compact over the modal interpretations:

$$\{\Diamond \rho^* t, \dot{\neg} t, \Box \rho(\dot{\neg} t), \Box(\rho; \rho)(\dot{\neg} t), \dots\}$$

[Fischer and Ladner, 1977] showed decidability of PDL.

Overview

1. Motivation and definition the Fisher-Ladner Closure
2. Argument that the Fisher-Ladner Closure is finite
3. Defintion of Filtration
4. Finite Model Property

Motivation through Filtration

1. Filtration is a technique from Modal Logic, due to [Lemmon and Scott, approx. 1965].
2. Idea: Only finitely many formulas matter to satisfiability.
3. Consequence: Drop all other information and identify states that cannot be distinguished by those formulas.
4. In the case of PDL: Fischer-Ladner closure instead of subterm closure.

Filtration takes a model for $t \in \Phi$ and yields a finite model for t.

Fischer-Ladner Closure: Definition

The Fisher-Ladner Closure of a term $t \in \Phi$ is denoted by $[t]$.

$$FL_{\dot{\rightarrow}} \quad \frac{t_1 \dot{\rightarrow} t_2}{t_1, t_2} \qquad FL_{\Box} \quad \frac{\Box \rho t}{t} \qquad FL_{?} \quad \frac{\Box t_1 ?\, t_2}{t_1}$$

$$FL_{\cup} \quad \frac{\Box(\rho_1 \cup \rho_2)t}{\Box \rho_1 t, \Box \rho_2 t}$$

$$FL_{;} \quad \frac{\Box(\rho_1 ; \rho_2)t}{\Box \rho_1 (\Box \rho_2 t)} \qquad FL_{*} \quad \frac{\Box \rho^* t}{\Box \rho (\Box \rho^* t)}$$

$$\Box \rho^* t \iff t \wedge \Box \rho (\Box \rho^* t)$$

Fischer-Ladner Closure: Example

$$FL_\Box \ \frac{\Box\rho t}{t} \qquad FL_; \ \frac{\Box(\rho_1;\rho_2)t}{\Box\rho_1(\Box\rho_2 t)} \qquad FL_* \ \frac{\Box\rho^* t}{\Box\rho(\Box\rho^* t)}$$

Let p be an atomic propositions and α, β atomic programs.

$\Box(\alpha;\beta)^* p$	initial term
p	$FL_\Box$
$\Box(\alpha;\beta)(\Box(\alpha;\beta)^* p)$	FL_*
$\Box\alpha(\Box\beta(\Box(\alpha;\beta)^* p))$	$FL_;$
$\Box\beta(\Box(\alpha;\beta)^* p)$	$FL_\Box$

Fischer-Ladner Closure: Finiteness

$d(\rho)$ denotes the depth of the program $\rho \in \Pi$
$|f|$ denotes the number of symbols in $f \in \Phi \cup \Pi$ (modulo parentheses).
$l(t)$ limits the size of the longest term derivable from $t \in \Phi$.

$$l(\dot{\bot}) = l(p) = l(r) = 0 \qquad p, r \text{ atomic}$$
$$l(t_1 \dot{\rightarrow} t_2) = \max\{l(t_1), l(t_2)\}$$
$$l(\Box\rho t) = \max\{\underbrace{d(\rho)}_{\text{times}} * \underbrace{|\rho|}_{\text{extension}} + \underbrace{|\Box\rho t|}_{\text{tail}},\ l(t),\ l(\rho)\}$$
$$l(t?) = l(t)$$
$$l(\rho_1; \rho_2) = l(\rho_1 \cup \rho_2) = \max\{l(\rho_1), l(\rho_2)\}$$
$$l(\rho^*) = l(\rho)$$

Filtration

Let t be a PDL proposition, $\mathcal{I}$ be an interpretation and $x, y \in I$.

$$\begin{aligned} x \equiv y &\iff \mathcal{L}x \cap [t] = \mathcal{L}y \cap [t] \\ &\iff \mathcal{L}x =_{[t]} \mathcal{L}y \end{aligned}$$

The *filtration* with respect to t of $\mathcal{I}$ is the interpretation $\mathcal{I}_t$ defined as follows:

$$\begin{aligned} [x] &:= \{y \in \mathcal{I}I \mid y \equiv x\} \\ \mathcal{I}_t I &:= \{[x] \mid x \in \mathcal{I}I\} \\ \mathcal{I}_t p[x] &:= \begin{cases} \mathcal{I}px & \text{if } p \in [t] \\ 0 & otherwise \end{cases} && p \text{ atomic} \\ \mathcal{I}_t rXY &:= \exists x \in X, y \in Y : \mathcal{I}rxy && r \text{ atomic} \end{aligned}$$

$\mathcal{I}_t p[x]$ is well defined for the definition of $[\cdot]$ and $\equiv$.

Desired Result

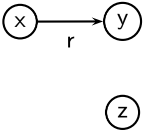
$$\mathcal{L}(x) =_{[t]} \mathcal{L}_t([x])$$

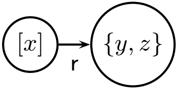
x satisfies the same subset of $[t]$ as $[x]$

$$\hat{\mathcal{I}}\rho x y \iff \hat{\mathcal{I}}_t \rho [x][y]$$

The filtration allows the same transitions.

Contradiction to second assumption for filtration $[\Diamond r \dot{\top}]$: $[x][\xrightarrow{r}][z]$





Filtration Lemma

Lemma

Let $\mathcal{I}$ be a modal interpretation and let $x, y \in I$.

1. $\mathcal{L}(x) =_{[t]} \mathcal{L}_t([x])$
   x *satisfies the same subset of* $[t]$ *as* $[x]$
2. $\forall\ \Box\rho u \in [t]$:
   1. $x \xrightarrow{\rho} y \Longrightarrow [x][\xrightarrow{\rho}][y]$
      No transition gets lost.
   2. $[x][\xrightarrow{\rho}][y]\ \wedge\ \Box\rho u \in \mathcal{L}x \Longrightarrow u \in \mathcal{L}y$
      If transitions are added, they are consitent.

Filtration Lemma: Part of the Proof

Simultaneous induction on the well-founded subexpression relation. We show for all $\Box\rho t' \in [t]$ with $\rho = \phi^*$ that $[x][\xrightarrow{\rho}][y]$ and $\Box\rho t' x$ implies $t'y$.

- Let $[x][\xrightarrow{\phi^*}][y]$ and $\Box\phi^* t' x$. Then there exist $z_1, \dots, z_n$ s.t. $x = z_1$, $y = z_n$ s.t. $[x][\xrightarrow{\phi}][z_2] \dots [z_i][\xrightarrow{\phi}][z_{i+1}] \dots [z_{n-1}][\xrightarrow{\phi}][y]$.
- Observe that $\Box\phi^* t' z_i$ implies $\Box\phi(\Box\phi^* t') z_i$, for all z_i. By the IH for $\Box\phi(\Box\phi^* t') \in [t]$ we get $\Box\phi^* t' z_{i+1}$.
- Continuing for n steps, we get $\Box\phi^* t' z_n$, which entails $t' z_n$. Since $z_n = y$, we are done.

Small Model Theorem

Theorem

Let t be a satisfiable formula of PDL. Then t is satisfied by an interpretation which interprets I as a finite set.

Proof.

1. If t is satisfiable, then there is an interpretation $\mathcal{I}$ and $x \in I$ with $\mathcal{I}tx = 1$.
2. By the Filtration Lemma $\mathcal{I}_t t[x] = 1$.
3. Moreover, $\mathcal{I}_t I$ has no more states than the powerset of $[t]$, which is finite.

□

References

V.G. Pratt.
Semantical considerations on Floyd-Hoare logic.
Massachusetts Institute of Technology, 1976.

Fischer, Michael J. and Ladner, Richard E.
Propositional modal logic of programs
STOC '77: Proceedings of the ninth annual ACM symposium on Theory of computing, 1977

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

E.J. Lemmon and D.S. Scott
The Lemmon Notes: An introduction to Modal Logic
Blackwell, 1977

Fischer-Ladner Closure: Proof

Claim: $l(s)$ is invariant under application of the FL-Rules. Case analysis.

- $s = p, s = \dot{\bot}, s = r$: No rules applicable.
- $s = t_1 \dot{\rightarrow} t_2$: $\max\{l(t_1), l(t_2)\} \geq l(t_i)$.
- $s = \Box rt$: $FL_\Box$ applicable. $\max\{\dots, l(t), l(r)\} \geq l(t)$.
- $s = \Box t_1?t_2$: $FL_?$ and $FL_\Box$ applicable. $\max\{\dots, l(t_1), l(t_2?)\} \geq l(t_i)$ since $l(t_2?) = l(t_2)$.
- $s = \Box(\rho_1 \cup \rho_2)t$: $FL_\Box$ and $FL_\cup$ applicable.
  - $\max\{\dots,\ l(t),\ l(\rho_1 \cup \rho_2)\} \geq \max\{l(t),\ l(\rho_i)\}$ since $l(\rho_1 \cup \rho_2) = \max\{l(\rho_1), l(\rho_2)\}$
  - $d(\rho_1 \cup \rho_2) * |\rho_1 \cup \rho_2| + |\Box(\rho_1 \cup \rho_2)t| \geq d(\rho_i) * |\rho_i| + |\Box\rho_i t|$

Fischer-Ladner Closure: Proof II

$s = \Box(\rho_1;\rho_2)t$: $FL_\Box$ and $FL_;$ applicable, $FL_\Box$ obvious.
To show: $\max\{d(\rho_1;\rho_2) * |\rho_1;\rho_2| + |\Box(\rho_1;\rho_2)t|, l(t), l(\rho_1;\rho_2)\} \geq \max\{d(\rho_1) * |\rho_1| + |\Box\rho_1(\Box\rho_2 t)|, l(\Box\rho_2 t), d(\rho_1)\}$

- $\max\{\ldots,\ l(\rho_1;\rho_2)\} \geq \max\{\ l(\rho_1)\}$ since $l(\rho_1;\rho_2) = \max\{l(\rho_1), l(\rho_2)\}$.

$$
\begin{aligned}
& d(\rho_1;\rho_2) * |\rho_1;\rho_2| + |\Box(\rho_1;\rho_2)t| & \\
\geq\ & d(\rho_1) * |\rho_1;\rho_2| + |\Box(\rho_1;\rho_2)t| & d(\rho_1;\rho_2) \geq d(\rho_1) \\
\geq\ & d(\rho_1) * |\rho_1| + |\Box(\rho_1;\rho_2)t| & |\rho_1;\rho_2| \geq |\rho_1| \\
=\ & d(\rho_1) * |\rho_1| + |\Box\rho_1(\Box\rho_2 t)| & |\Box| = |;|
\end{aligned}
$$

- $d(\rho_1;\rho_2) * |\rho_1;\rho_2| + |\Box(\rho_1;\rho_2)t| \geq d(\rho_2) * |\rho_2| + |\Box\rho_2 t|$ is similar.

Fischer-Ladner Closure: Proof III

$s = \Box(\rho^*)t$ $\quad FL_*$ and $FL_\Box$ applicable.

- $FL_\Box$: $\max\{\dots, l(t)\} \geq l(t)$.
- FL_* : t.s: $l(\Box\rho^* t) = \max\{d(\rho^*) * |\rho^*| + |\Box\rho^* t|, l(t), l(\rho^*)\} \geq \max\{d(\rho) * |\rho| + |\Box\rho(\Box\rho^* t)|, l(\Box\rho^* t), l(\rho)\}$

$$\begin{aligned}
& d(\rho^*) * |\rho^*| + |\Box\rho^* t| \\
= \; & (d(\rho)+1) * |\rho^*| + |\Box\rho^* t| && d(\rho^*) = d(\rho) + 1 \\
= \; & d(\rho) * |\rho^*| + |\rho^*| + |\Box\rho^* t| \\
\geq \; & d(\rho) * |\rho| + |\rho^*| + |\Box\rho^* t| \\
= \; & d(\rho) * |\rho| + |\Box\rho(\Box\rho^* t)| && |\rho^*| = |\Box\rho|
\end{aligned}$$

Reflexive Transitive Closure

$$
\begin{aligned}
T &= \lambda r.\ \forall xyz.\ rxy \wedge ryz \Longrightarrow rxz && T : (IIB)B \\
R &= \lambda r.\ \forall x.\ rxx && T : (IIB)B \\
\subseteq &= \lambda rr'.\ \forall xy.\ rxy \Longrightarrow r'xy && TR : (IIB)(IIB)I \\
C^{TR} &= \lambda rxy.\ \exists r' \colon\ Tr' \ \wedge\ Rr' \wedge\ r \subseteq r' \\
&\quad \wedge\ \forall \rho \colon (T\rho\ \wedge\ R\rho\ \wedge\ \rho \subseteq r' \Longrightarrow \rho = r') \\
&\quad \wedge\ r'xy && C^{TR} : (IIB)IIB
\end{aligned}
$$

Hoare Logic vs. PDL

Floyd-Hoare logic: $\{t_1\}\alpha\{t_2\}$. (pre and post conditions)
Same in PDL: $t_1 \dot{\rightarrow} \Box\alpha t_2$

$$\textit{Composition} \quad \frac{\{t_1\}\alpha\{t_2\},\ \{t_2\}\beta\{t_3\}}{\{t_1\}\alpha;\beta\{t_2\}}$$

$$\textit{Conditional} \quad \frac{\{t_1 \wedge t_2\}\alpha\{s\},\ \{\dot{\neg} t_1 \wedge t_2\}\beta\{s\}}{\{t_2\}\ \text{if}\ t_1\ \text{then}\ \alpha\ \text{else}\ \beta\ \{s\}}$$

$$\textit{While} \quad \frac{\{t_1 \wedge t_2\}\alpha\{t_2\}}{\{t_2\}\ \text{while}\ t_1\ \text{do}\ \alpha\ \{\dot{\neg} t_1 \wedge t_2\}}$$

$$\textit{Weakening} \quad \frac{t_1 \dot{\rightarrow} t_2,\ \{t_2\}\alpha\{s_1\},\ s_1 \dot{\rightarrow} s_2}{\{t_1\}\alpha\{s_2\}}$$

Filtration Lemma: Part of the Proof II

Simultaneous induction on the well-founded subexpression relation. We show for all $\Box\rho t' \in [t]$ with $\rho = \phi^*$ that $x \xrightarrow{\rho} y \Longrightarrow [x][\xrightarrow{\rho}][y]$.

- We have $\Box\phi\Box(\phi^*)t' \in [t]$, and since ϕ is a proper subterm of ϕ^* the IH holds for all $\Box\phi s \in [t]$. Thus we know $u \xrightarrow{\phi} v \Longrightarrow [u][\xrightarrow{\phi}][v]$.
- If $x \xrightarrow{\phi^*} y$ there exist $z_1, \ldots, z_n$ s.t. $x = z_1$, $y = z_n$ and $x \xrightarrow{\phi} z_2 \ldots z_i \xrightarrow{\phi} z_{i+1} \ldots z_{n-1} \xrightarrow{\phi} y$.
- This implies $[x][\xrightarrow{\phi}][z_2] \ldots [z_i][\xrightarrow{\phi}][z_{i+1}] \ldots [z_{n-1}][\xrightarrow{\phi}][y]$, which yields $[x][\xrightarrow{\phi^*}][y]$.

Compact models for PDL

Allow diamond satisfaction to be infinitley prolonged.

$$\Box\rho^* t \iff t \wedge \Box\rho(\Box\rho^* t)$$
$$\Box\rho^* t \iff t \wedge \Box\rho^*(t \dot{\rightarrow} \Box\rho t)$$

$$\Diamond\rho^* t \iff t \vee \Diamond\rho(\Diamond\rho^* t) \quad (1)$$
$$\Diamond\rho^* t \iff t \vee \Diamond\rho^*(\dot{\neg} t \wedge \Diamond\rho t) \quad (2)$$
$$(3)$$

Forumla (1) captures reflexivity, transitivity and the containment of the subrelation.

Translation of the relations without *

$$
\begin{aligned}
\Diamond(\rho_1;\rho_2)tx &= \Diamond\rho_1(\Diamond\rho_2 t)x \\
\Box(\rho_1;\rho_2)tx &= \Box\rho_1(\Box\rho_2 t)x \\
\Diamond(\rho_1 \cup \rho_2)tx &= \Diamond\rho_1 tx \lor \Diamond\rho_2 tx \\
\Box(\rho_1 \cup \rho_2)tx &= \Box\rho_1 tx \lor \Box\rho_2 tx \\
\Box(t?)ux &= (t \dot{\rightarrow} u)x \\
\Diamond(t?)ux &= (t \land u)x
\end{aligned}
$$