Dynamische Logik

Präsentiert von: Vitali Amann

Universität Hamburg - FGI 3 Seminar
(06.01.2010)

Index

- Motivation
- Dynamische Logik (DL)
- Propositionale Dynamische Logik (PDL)
  - Syntax
  - Semantik
  - Erfüllbarkeit/Gültigkeit
  - Vollständigkeit
- Erweiterungen von PDL

Motivation

- Formales System für Korrektheitsbeweise von Programmen
- Äquivalenz der Programme
- Mächtigkeit verschiedener Programmkonzepte

Konzept der Beweise

- Programm ist korrekt, wenn:
  - Spezifikation eines Programms erfüllt wird

- Problematik:
  - Spezifikation ist komplex
  - Fehler in der Spezifikation
  - Fehler im Programm
  - Fehler in Spezifikation und Programm

Dynamische Logik: Konzept

- Prädikatenlogik (1. Ordnung)
- Modallogik
- Algebra der regulären Ausdrücke

- Stärken sowohl in der Theorie als auch in Praxis

Dynamische Logik vs. Prädikatenlogik

- Prädikatenlogik:
  - Statische Wahrheitsaussagen
  - Hängt von Auswertung der freien Variablen
- Dynamische Logik:
  - Explizite Konstrukte (Programme)
  - Erlaubt Änderungen der Werte der Variablen
  - $x := x + 1$

Dynamische Logik: Ziele

- Analyse was ein Programm genau tut
- Ermittlung unerwarteter Fehler
- Isolation der Kernprobleme
- Prüfung ob Programm die Spezifikation erfüllt

Propositionale Dynamische Logik (PDL)

- PDL verhält sich zu DL genau wie Aussagenlogik zur Prädikatenlogik
- PDL beschreibt Eigenschaften und Verhalten bei der Interaktion zwischen Programmen und Aussagen
- Keine Domänen
  - Keine gebundenen Variablen

PDL: Syntax

Atomare Formeln:	$p \in \Phi_0$
Formeln:	$\varphi \in \Phi$
Atomare Programme:	$a \in \Pi_0$
Programme:	$\alpha \in \Pi$
Operatoren:	
Propositional:	$\rightarrow \quad 0$
Programm:	$; \quad \cup \quad *$
Gemischte:	$[] \quad ?$

PDL: Syntax

Implikation:	$\varphi \rightarrow \psi$
Kontradiktion:	0
Notwendigkeit:	$[\alpha]\varphi$
Sequenzieller Ablauf:	$\alpha;\beta$
Auswahl (nichtdeterm.):	$\alpha \cup \beta$
Wiederholung:	α^*
Test:	$\varphi?$

PDL: erweiterte Syntax

$$<\alpha>\varphi \overset{def}{=} \neg[\alpha]\neg\varphi$$

$$\text{skip} \overset{def}{=} 1?$$

$$\text{fail} \overset{def}{=} 0?$$

$$\text{if } \varphi \text{ then } \alpha \text{ else } \beta \overset{def}{=} \varphi?;\alpha \cup \neg\varphi?;\beta$$

$$\text{while } \varphi \text{ do } \alpha \overset{def}{=} (\varphi?;\alpha)^*;\neg\varphi?$$

$$\text{repeat } \alpha \text{ until } \varphi \overset{def}{=} \alpha;(\neg\varphi?;\alpha)^*;\varphi?$$

PDL: Semantik

- Kripke-Rahmen
  - Struktur zur Interpretation von Programmen und Propositionen
- Definition: $\kappa = (K, m_\kappa)$

K Menge der Zustände

m_κ Funktion, die Φ_0 und Π_0 eine Bedeutung zuweist

$$m_\kappa(p) \subseteq K, \qquad p \in \Phi_0$$

$$m_\kappa(a) \subseteq K \times K, \quad a \in \Pi_0$$

PDL: Kripke-Rahmen

- Allgemein für Formeln und Programme:

$$m_\kappa(\varphi) \subseteq K, \qquad \varphi \in \Phi$$

$$m_\kappa(\alpha) \subseteq K \times K, \quad \alpha \in \Pi$$

- $m_\kappa(\varphi)$ ist eine Menge aller Zustände, die die Aussage φ erfüllen
- $m_\kappa(\alpha)$ ist eine Menge der Eingabe- und Ausgabezustände des Programms α

PDL: Beispiel

- Gegeben ist ein Kripke-Rahmen mit:

$$\kappa = (K, m_\kappa) \qquad m_\kappa(p) = \{u, v\}$$

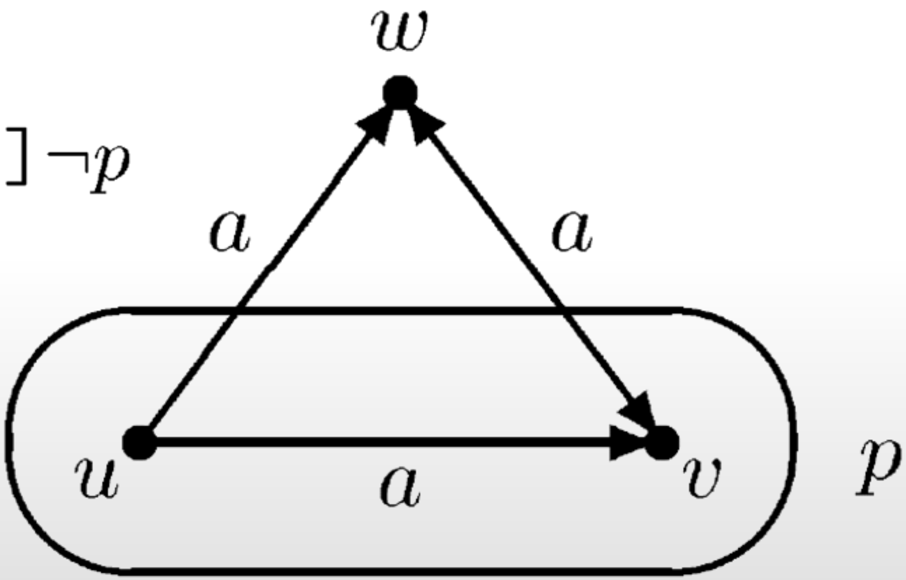
$$K = \{u, v, w\} \qquad m_\kappa(a) = \{(u,v), (u,w), (v,w), (w,v)\}$$

$$\langle a^* \rangle [(aa)^*] p \wedge \langle a^* \rangle [(aa)^*] \neg p$$

$$u \models \langle a \rangle \neg p \wedge \langle a \rangle p$$

$$v \models [a] \neg p$$

$$w \models [a] p$$



PDL: Erfüllbarkeit und Gültigkeit

- Definitionen aus Modallogik

- Gegeben:
  - Kripke-Rahmen $\kappa = (K, m_\kappa)$
  - Aussageformel φ

PDL: Erfüllbarkeit

- Wenn $\mathfrak{K}, u \vDash \varphi$ für ein beliebiges $u \in K$
  - ➢ φ ist in $\mathfrak{K}$ erfüllbar
- Wenn φ in einem beliebigen $\mathfrak{K}$ erfüllbar ist
  - ➢ φ ist erfüllbar

PDL: Erfüllbarkeit

- Wenn $\mathfrak{K}, u \models \varphi$ für ein beliebiges $u \in K$
  - φ ist in $\mathfrak{K}$ erfüllbar
- Wenn φ in einem beliebigen $\mathfrak{K}$ erfüllbar ist
  - φ ist erfüllbar

- Erfüllbarkeitsproblem für PDL hat exponentielle Komplexität $2^{|\varphi|}$

PDL: Gültigkeit

- Wenn $\mathfrak{K}, u \models \varphi$ für all $u \in K$
  - φ ist gültig in $\mathfrak{K}$
  - $\mathfrak{K} \models \varphi$
- Wenn $\mathfrak{K} \models \varphi$ in allen Kripke-Rahmen $\mathfrak{K}$ gütig ist
  - φ ist gültig
  - $\models \varphi$

PDL: Beispiel (1/2)

- Gegeben ist ein Kripke-Rahmen mit:

$$\kappa = (K, m_\kappa)$$

$$K = \{s, t, u, v\}$$

$$m_\kappa(p) = \{u, v\}$$

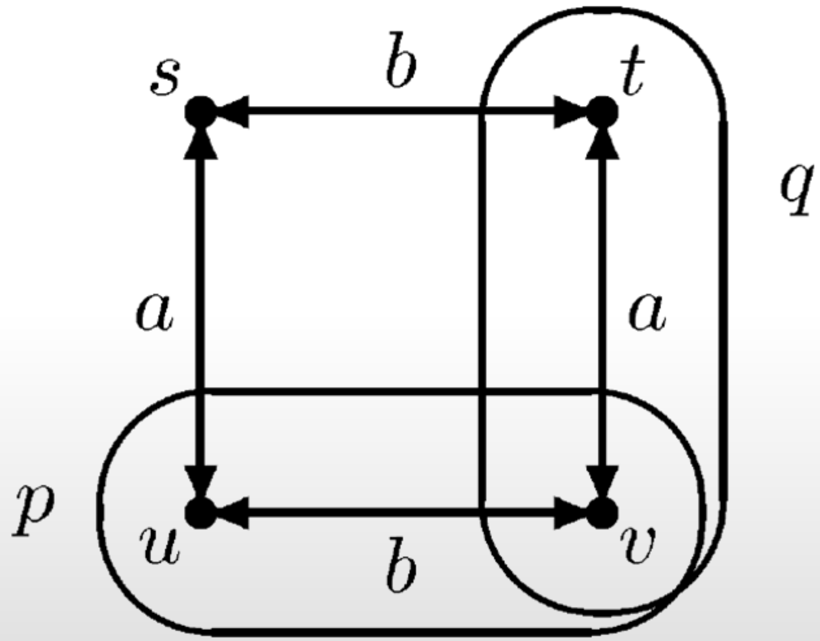
$$m_\kappa(q) = \{t, v\}$$

$$m_\kappa(a) = \{(t,v), (v,t), (s,u), (u,s)\}$$

$$m_\kappa(b) = \{(u,v), (v,u), (s,t), (t,s)\}$$

PDL: Beispiel (2/2)

- Gültige Formeln in $\mathfrak{K}$:
  - $p \leftrightarrow [(ab^*a)^*]p$
  - $q \leftrightarrow [(ba^*b)^*]q$



PDL: Umkehrungsoperator

- Erlaub das Programm rückwärts laufen zu lassen

$$m_\kappa(\alpha^-) = m_\kappa(\alpha)^- = \{(v,u) \mid (u,v) \in m_\kappa(\alpha)\}$$

- Eingabe von α ist die Ausgabe von α^- und
- Ausgabe von α ist die Eingabe von α^-

PDL: Folgerungsregeln

- Modale Generalisierung (GEN): $$\frac{\varphi}{[\alpha]\varphi}$$
- Monotonie von <α>: $$\frac{\varphi \to \psi}{<\alpha>\varphi \to <\alpha>\psi}$$
- Monotonie von [α]: $$\frac{\varphi \to \psi}{[\alpha]\varphi \to [\alpha]\psi}$$

PDL: Vollständigkeit

- Ergibt sich aus der Gültigkeit einer Formel
- Falls $\models \varphi$, dann $\vdash \varphi$

Erweiterungen von PDL

- DPDL (deterministische PDL):
  - Interpretation nur über deterministische Strukturen
- SPDL (strikte PDL):
  - erlaubt ausschließlich deterministische **while**-Programme
- SDPDL (strikte deterministische PDL):
  - Mischung aus DPDL und SPDL, wo beide Einschränkungen gelten

Deterministische Programme

- Kripke-Rahmen wird angepasst
  - Alle atomaren Programme sind in der Semantik deterministisch
- Deterministische **while**-Programme (DWP)
  - Operatoren $\cup$, ?, und $*$ nur in bedingten Tests, while loop, skip, fail
  - In bedingten Tests und while loop keine <> und [] Operatoren

Erfüllbarkeit und Gültigkeit

- Definition wie bei PDL mit Bezug zum Determinismus
- φ gültig in PDL, dann auch gültig in DPDL
  - Nicht umgekehrt!
  - Beispiel: $< a > \varphi \rightarrow [a]\varphi$
- SPDL und SDPDL weniger Aussagekraft
  - Beispiel: $< (a \cup b)^* > \varphi$

Fragen?