

Dynamische Logik

Simon Matthias Brodt

28.5.2008

Übersicht

- 1 Motivation – Programm Verifikation
- 2 PDL
- 3 Filtration und Entscheidbarkeit
- 4 Vollständigkeit

Problem – Fehlerhafte Programme

Ursache:

- Unpräzise Anforderungen
- „Intuitiv richtige“ Lösungen

Unklare Begriffe

- Korrektheit – Was bedeutet „korrekt“ bzw. „richtig“?
- Verifikation – Wann ist ein bestimmtes Programm „korrekt“?

Korrektheits-Spezifikation

Was ist das?

- Formale Beschreibung des gewünschten Verhaltens eines Programms
- Im Falle einer Berechnung z.B. durch Ein-/Ausgabe-Relation

Schwierigkeit

- Zunächst keine präzisen, formalen Anforderungen vorhanden
- Müssen meist durch den Programmierer selbst definiert werden

Verifikation

Wann ist ein Programm korrekt?

- Ein Programm ist korrekt bzgl. einer Spezifikation, wenn es sich wie erwartet verhält (die Spezifikation erfüllt)
- Im Fall einer Ein-/Ausgabe-Relation: Ein Programm ist korrekt, falls es für jede passende Eingabe, die spezifizierte Ausgabe liefert

Schwierigkeit

- Programmierung erfolgt meist nicht in einer anderen weniger formalen Sprache
- Passen Programm und Spezifikation nicht zusammen stellt sich die Frage: Ist das Programm oder die Spezifikation falsch?

Nutzen

- Klare Vorstellung dessen, was das Programm tun soll
- Entdecken unerwarteter Fälle
- Isolation des Kernproblems erleichtert die Implementierung
- Häufig einfacher anzugeben *Was* ein Programm tun soll, als zu sagen *Wie* es das tun soll.
- Die Verifikation ermöglicht es zu überprüfen, ob definiertes Ziel (Spezifikation) und vorgeschlagene Lösung (Programm) zusammenpassen

Syntax

Atomare Formeln: $p \in \Phi_0$

Atomare Programme: $a \in \Pi_0$

Formeln: $\phi \in \Phi$

Programme: $\alpha \in \Pi$

$\phi ::= p \mid \perp \mid \phi_1 \rightarrow \phi_2 \mid [\alpha] \phi$

$\alpha ::= a \mid \alpha_1; \alpha_2 \mid \alpha_1 \cup \alpha_2 \mid \alpha^* \mid \phi?$

Intuitive Bedeutung

$[\alpha]\phi$	nach α , ϕ
$\alpha_1; \alpha_2$	führe α_1 aus und danach α_2
$\alpha_1 \cup \alpha_2$	führe nicht-deterministisch α_1 oder α_2 aus
α^*	wiederhole α endlich oft (≥ 0)
$\phi?$	Fahre fort falls ϕ gilt, ansonsten scheitere

Abkürzungen

$\langle \alpha \rangle \phi$	ist	$\neg [\alpha] \neg \phi$
if ϕ then α else β	ist	$(\phi?; \alpha) \cup (\neg \phi?; \beta)$
while ϕ do α	ist	$(\phi?; \alpha)^*; \neg \phi?$
repeat α until ϕ	ist	$\alpha; (\neg \phi?; \alpha)^*$
skip	ist	$\top?$
abort	ist	$\perp?$
α^0	ist	skip
α^{n+1}	ist	$(\alpha; \alpha^n)$

Semantik für atomare Programme und Aussagen

Ein Kripke-Rahmen ist ein Paar

$$\mathcal{K} = (K, m_{\mathcal{K}})$$

,wobei K eine Menge von Zuständen darstellt und $m_{\mathcal{K}}$ eine Funktion, die jeder atomaren Aussage und jedem atomaren Programm eine Bedeutung zuweist, und zwar folgendermaßen:

$$\begin{array}{ll} m_{\mathcal{K}}(p) \subseteq K, & p \in \Phi_0 \\ m_{\mathcal{K}}(a) \subseteq K \times K, & a \in \Pi_0 \end{array}$$

Semantik für zusammengesetzte Programme und Aussagen

$$m_{\mathcal{H}}(\phi \rightarrow \psi) := (K - m_{\mathcal{H}}(\phi)) \cup m_{\mathcal{H}}(\psi)$$

$$m_{\mathcal{H}}(\perp) := \emptyset$$

$$\begin{aligned} m_{\mathcal{H}}([\alpha]\phi) &:= K - (m_{\mathcal{H}}(\alpha) \circ (K - m_{\mathcal{H}}(\phi))) \\ &= \{u \mid \forall v \in K : \text{falls } (u, v) \in m_{\mathcal{H}}(\alpha) \text{ dann } v \in m_{\mathcal{H}}(\phi)\} \end{aligned}$$

$$\begin{aligned} m_{\mathcal{H}}(\alpha; \beta) &:= m_{\mathcal{H}}(\alpha) \circ m_{\mathcal{H}}(\beta) \\ &= \{(u, v) \mid \exists w \in K : (u, w) \in m_{\mathcal{H}}(\alpha) \text{ und } (w, v) \in m_{\mathcal{H}}(\beta)\} \end{aligned}$$

Semantik für zusammengesetzte Programme und Aussagen

$$m_{\mathcal{K}}(\alpha \cup \beta) := m_{\mathcal{K}}(\alpha) \cup m_{\mathcal{K}}(\beta)$$

$$m_{\mathcal{K}}(\alpha^*) := m_{\mathcal{K}}(\alpha)^* = \bigcup_{n \geq 0} m_{\mathcal{K}}(\alpha)^n$$

$$m_{\mathcal{K}}(\phi?) := \{(u, v) \mid u \in m_{\mathcal{K}}(\phi)\}$$

Gültigkeit und Erfüllbarkeit

Schreibweise

$$\mathcal{K}, u \models \phi :\Leftrightarrow u \in m_{\mathcal{K}}(\phi)$$

Erfüllbarkeit

- ϕ heißt erfüllbar in $\mathcal{K}$, falls $\mathcal{K}, u \models \phi$ für ein $u \in \mathcal{K}$
- ϕ heißt erfüllbar, falls es ein $\mathcal{K}$ gibt in dem ϕ erfüllbar ist

Gültigkeit

- ϕ heißt gültig in $\mathcal{K}$, falls $\mathcal{K}, u \models \phi$ für alle $u \in \mathcal{K}$
Geschrieben: $\mathcal{K} \models \phi$
- ϕ heißt gültig, falls ϕ in gültig ist in jedem Kripke-Rahmen $\mathcal{K}$.
Geschrieben: $\models \phi$

Beispiel

Im Kripke-Rahmen

$$\mathcal{K} = (K, m_{\mathcal{K}})$$

$$K = \{u, v, w\}$$

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

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

gilt dann z.B.:

$$u \in m_{\mathcal{K}}(\langle \alpha \rangle \neg p \wedge \langle \alpha \rangle p), \quad (\Leftrightarrow u \models \langle \alpha \rangle \neg p \wedge \langle \alpha \rangle p)$$

$$v \in m_{\mathcal{K}}([a] \neg p), \quad (\Leftrightarrow v \models [a] \neg p)$$

$$w \in m_{\mathcal{K}}([a] p), \quad (\Leftrightarrow w \models [a] p)$$

Semantik von Abkürzungen

$\langle \alpha \rangle \phi$

$$\begin{aligned} m_{\mathcal{K}}(\langle \alpha \rangle \phi) &:= m_{\mathcal{K}}(\alpha) \circ m_{\mathcal{K}}(\phi) \\ &= \{u \mid \exists v \in K : (u, v) \in m_{\mathcal{K}}(\alpha) \text{ und } v \in m_{\mathcal{K}}(\phi)\} \end{aligned}$$

while ϕ do α

$$(u, v) \in m_{\mathcal{K}}(\text{while } \phi \text{ do } \alpha)$$

$\Leftrightarrow$

$\exists u_0, u_1, \dots, u_n, n \geq 0$ mit $u = u_0, v = u_n,$

$u_i \in m_{\mathcal{K}}(\phi), (u_i, u_{i+1}) \in m_{\mathcal{K}}(\alpha)$ für $0 \leq i < n$, und

$u_n \notin m_{\mathcal{K}}(\phi)$

Nonstandard-Kripke-Rahmen

Ein *Nonstandard-Kripke-Rahmen* ist eine Struktur $\mathcal{N} = (N, m_{\mathcal{N}})$ mit allen Eigenschaften eines Standard-Kripke-Rahmens, mit folgender Ausnahme:

$m_{\mathcal{N}}(\alpha^*)$ ist lediglich eine reflexive und transitive Relation die $m_{\mathcal{N}}(\alpha)$ umfasst und die PDL Axiome für $*$ erfüllt.

Anders ausgedrückt, wird die Definition

$$m_{\mathcal{N}}(\alpha^*) := m_{\mathcal{N}}(\alpha)^* = \bigcup_{n \geq 0} m_{\mathcal{N}}(\alpha)^n$$

durch folgende (schwächere) Forderung ersetzt:

$$\begin{aligned} m_{\mathcal{N}}([\alpha^*]\phi) &= m_{\mathcal{N}}(\phi \wedge [\alpha][\alpha^*]\phi) \\ m_{\mathcal{N}}([\alpha^*]\phi) &= m_{\mathcal{N}}(\phi \wedge [\alpha^*](\phi \rightarrow [\alpha]\phi)) \end{aligned}$$

Axiome

Axiome der Aussagenlogik

...

Modallogische Axiome

$$\begin{aligned} [\alpha] (\phi \rightarrow \psi) &\rightarrow ([\alpha] \phi \rightarrow [\alpha] \psi) \\ [\alpha] (\phi \wedge \psi) &\leftrightarrow ([\alpha] \phi \wedge [\alpha] \psi) \end{aligned}$$

Axiome

Spezielle Axiome

$$\begin{array}{ll}\text{Alt:} & [\alpha \cup \beta] \phi \leftrightarrow [\alpha] \phi \wedge [\beta] \phi \\ \text{Comp:} & [\alpha; \beta] \phi \leftrightarrow [\alpha] [\beta] \phi \\ \text{Test:} & [\phi?] \psi \leftrightarrow (\phi \rightarrow \psi) \\ \text{Mix:} & \phi \wedge [\alpha] [\alpha^*] \phi \leftrightarrow [\alpha^*] \phi \\ \text{Ind:} & \phi \wedge [\alpha^*] (\phi \rightarrow [\alpha] \phi) \rightarrow [\alpha^*] \phi\end{array}$$

Schlussregeln

$$\begin{array}{l}\phi, \phi \rightarrow \psi \vdash \psi \\ \phi \vdash [\alpha]\end{array}$$

Induktions-Axiom

Ähnlichkeit zum Induktionsaxiom der Peano-Arithmetik

$$\begin{array}{l} \phi \wedge [\alpha^*](\phi \rightarrow [\alpha]\phi) \rightarrow [\alpha^*]\phi \\ \phi(0) \wedge \forall n(\phi(n) \rightarrow \phi(n+1)) \rightarrow \forall n \phi(n) \end{array}$$

Korrektheit

Logische Folgerung

- ψ heißt logische Folgerung aus Σ , falls $\mathcal{K} \models \Sigma \Rightarrow \mathcal{K} \models \psi$.
- Geschrieben: $\Sigma \models \psi$

Korrektheit

Eine Schlussregel $\phi_1, \dots, \phi_n \vdash \phi$ heißt *korrekt*, falls $\{\phi_1, \dots, \phi_n\} \models \phi$

Die vorherigen Axiome und Schlussregeln sind korrekt.

Fischer-Ladner Abschluss

Wir definieren zwei Funktionen:

$$\begin{aligned} FL : & \Phi \rightarrow 2^\Phi \\ FL^\square : & \{[\alpha]\phi \mid \alpha \in \Pi, \phi \in \Phi\} \rightarrow 2^\Phi \end{aligned}$$

$$\begin{aligned} FL(p) &:= \{p\}, p \text{ eine atomare Aussage} \\ FL(\phi \rightarrow \psi) &:= \{\phi \rightarrow \psi\} \cup FL(\phi) \cup FL(\psi) \\ FL(\perp) &:= \{\perp\} \\ FL([\alpha]\phi) &:= FL^\square([\alpha]\phi) \cup FL(\phi) \end{aligned}$$

Fischer-Ladner Abschluss

$FL^{\square}([a]\phi) := \{[a]\phi\}$, a ein atomares Programm

$FL^{\square}([\alpha \cup \beta]\phi) := \{[\alpha \cup \beta]\phi\} \cup FL^{\square}([\alpha]\phi) \cup FL^{\square}([\beta]\phi)$

$FL^{\square}([\alpha; \beta]\phi) := \{[\alpha; \beta]\phi\} \cup FL^{\square}([\alpha][\beta]\phi) \cup FL^{\square}([\beta]\phi)$

$FL^{\square}([\alpha^*]\phi) := \{[\alpha^*]\phi\} \cup FL^{\square}([\alpha][\alpha^*]\phi)$

$FL^{\square}([\psi?]\phi) := \{[\psi?]\phi\} \cup FL(\psi)$

Fischer-Ladner Abschluss

Lemma

Falls $\sigma \in FL(\phi)$, dann gilt $FL(\sigma) \subseteq FL(\phi)$.

Falls $\sigma \in FL^\square([\alpha]\phi)$, dann gilt $FL(\sigma) \subseteq FL^\square([\alpha]\phi) \cup FL(\phi)$.

Lemma

Für jede Formel ϕ , $|FL(\phi)| \leq |\phi|$.

Für jede Formel $[\alpha]\phi$, $|FL^\square([\alpha]\phi)| \leq |\alpha|$

Filtration

Sei eine PDL Aussage ϕ und ein Kripke-Rahmen $\mathcal{K} = (K, m_{\mathcal{K}})$ gegeben. Wir definieren einen neuen Rahmen, die „Filtration von $\mathcal{K}$ durch $FL(\phi)$ “, folgendermaßen:

$$u \equiv v :\Leftrightarrow \text{Für alle } \psi \in FL(\phi) (u \in m_{\mathcal{K}}(\psi) \Leftrightarrow v \in m_{\mathcal{K}}(\psi))$$

Informell:

Zwei Zustände u und v fallen zusammen, falls sie sich durch eine Formel aus $FL(\phi)$ nicht unterscheiden lassen.

Filtration

$$[u] := \{v \mid v \equiv u\}$$

$$K/FL(\phi) := \{[u] \mid u \in K\}$$

$$m_{\mathcal{K}/FL(\phi)}(p) := \{[u] \mid u \in m_{\mathcal{K}}(p)\}, p \text{ eine atomare Aussage}$$

$$m_{\mathcal{K}/FL(\phi)}(a) := \{([u], [v]) \mid (u, v) \in m_{\mathcal{K}}(a)\}, a \text{ ein atomares Programm}$$

$m_{\mathcal{K}/FL(\phi)}$ wird induktiv auf zusammengesetzte Aussagen und Programme fortgesetzt.

Filtrations-Lemma

Sei $\mathcal{K}$ ein Kripke-Rahmen und seien u, v Zustände von $\mathcal{K}$.

- Für alle $\psi \in FL(\phi)$, $u \in m_{\mathcal{K}}(\psi) \Leftrightarrow [u] \in m_{\mathcal{K}/FL(\phi)}(\psi)$
- Für alle $[\alpha]\psi \in FL(\phi)$,
 - Falls $(u, v) \in m_{\mathcal{K}}(\alpha)$ dann $([u], [v]) \in m_{\mathcal{K}/FL(\phi)}(\alpha)$
 - Falls $([u], [v]) \in m_{\mathcal{K}/FL(\phi)}(\alpha)$ und $u \in m_{\mathcal{K}}([\alpha]\psi)$, dann $v \in m_{\mathcal{K}}(\psi)$

Satz von den Kleinen Modellen

Satz

Sei ϕ eine erfüllbare PDL Formel. Dann ist ϕ in einem Kripke-Rahmen mit höchstens $2^{|\phi|}$ Zuständen erfüllbar.

Beweis.

Wenn ϕ erfüllbar ist, dann gibt es einen Kripke-Rahmen $\mathcal{K}$ und einen Zustand $u \in \mathcal{K}$ mit $u \in m_{\mathcal{K}}(\phi)$.

Ist nun $FL(\phi)$ der Fischer-Ladner Abschluss von ϕ , so gilt nach dem Filtrations-Lemma: $[u] \in m_{\mathcal{K}/FL(\phi)}(\phi)$.

Desweiteren hat $\mathcal{K}/FL(\phi)$ höchstens so viele Zustände wie es konsistente Teilmengen von $FL(\phi)$ gibt. Nach einem vorangegangenen Lemma sind das aber höchstens $2^{|\phi|}$ viele. □

Entscheidbarkeit

Satz

Das Erfüllbarkeitsproblem für PDL ist entscheidbar.

Beweis.

Die Aussage folgt unmittelbar aus dem vorangegangenen Satz von den kleinen Modellen:

Es gibt nur endlich viele Kripke-Rahmen mit maximal $2^{|\phi|}$ vielen Zuständen und es ist möglich in polynomieller Zeit zu prüfen, ob eine gegebene Formel in einem bestimmten Rahmen und einem bestimmten Zustand erfüllt ist. □

Filtration von Nonstandard-Kripke-Rahmen

Axiome und Regeln von PDL

- Gelten auch in Nonstandard-Kripke-Rahmen
- Alle in diesem System hergeleiteten Sätze und Regeln gelten ebenfalls auch über Nonstandard-Kripke-Rahmen

Filtration von Nonstandard-Kripke-Rahmen

- $\mathcal{N} / FL(\phi)$ ist ein *Standard*-Kripke-Rahmen
- höchstens $2^{|\phi|}$ viele Zustände

Filtrations-Lemma

- Gilt auch für Nonstandard-Kripke-Rahmen
- Beweis muss nur in den Fällen die * betreffen angepasst werden

Konsistenz und maximal konsistente Formelmengen

- Eine Formelmenge Σ heißt konsistent, falls $\Sigma \not\vdash \perp$.
- Sie heißt maximal konsistent, falls für alle Formeln ϕ gilt:
 $\phi \in \Sigma$ oder $\Sigma \cup \{\phi\} \vdash \perp$.

Konstruktion eines Nonstandard-Kripke-Rahmen

$$\mathcal{N} = (N, m_{\mathcal{N}})$$

$$N := \{\text{maximal konsistente PDL Formelmengen}\}$$

$$m_{\mathcal{N}}(\phi) := \{s \mid \phi \in s\}$$

$$m_{\mathcal{N}}(\alpha) := \{(s, t) \mid \text{Für alle } \phi, \text{ falls } [\alpha]\phi \in s, \text{ dann } \phi \in t\}$$

- Beachte:
Die Definitionen von $m_{\mathcal{N}}(\phi)$ und $m_{\mathcal{N}}(\alpha)$ beziehen sich auf *alle* Formeln und Programme.
- Die so definierte Struktur ist ein Nonstandard-Kripke-Rahmen.

Vollständigkeit von PDL

Satz

Falls $\models \phi$, dann $\vdash \phi$.

Beweis.

Es ist gleichbedeutend zu zeigen, dass es falls ϕ konsistent ist einen erfüllenden Standard-Kripke-Rahmen gibt.

Da ϕ konsistent ist gibt es eine maximal konsistente Formelmenge u die ϕ enthält. u ist ein Zustand des zuvor konstruierten Nonstandard-Kripke-Rahmen $\mathcal{N}$.

Das Filtrations-Lemma (für Nonstandard-Standard-Kripke-Rahmen) liefert uns, dass ϕ im Zustand $[u]$ des endlichen *Standard*-Kripke-Rahmens $\mathcal{N} / FL(\phi)$ erfüllt ist. □

Alternative Schreibweise für Semantik

$$\mathcal{K}, u \models p :\Leftrightarrow u \in m_{\mathcal{K}}(p) \text{ , für } p \in \Phi_0$$

$$\mathcal{K}, u \models \phi \rightarrow \psi :\Leftrightarrow \mathcal{K}, u \models \phi \Rightarrow \mathcal{K}, u \models \psi$$

$$\mathcal{K}, u \not\models \perp$$

$$\mathcal{K}, u \models [\alpha] \phi :\Leftrightarrow \forall v \in K : \text{ falls } (u, v) \in m_{\mathcal{K}}(\alpha) \text{ dann } \mathcal{K}, v \models \phi$$