Formale Modellierung
Vorlesung 12 vom 07.07.2014: Temporale Logik und Modellprüfung

Serge Autexier & Christoph Lüth

Universität Bremen

Sommersemester 2014

Organisatorisches

- Übung am Donnerstag kann verspätet anfangen (ca. 14:30).

Fahrplan

- Teil I: Formale Logik
- Teil II: Spezifikation und Verifikation
  - Formale Modellierung mit der UML und OCL
  - Lineare Temporale Logik
  - Temporale Logik und Modellprüfung
  - Hybride Systeme
  - Zusammenfassung, Rückblick, Ausblick

Computational Tree Logic (CTL)

- Grenzen der LTL: Quantifikation über Pfaden
  - z.B. Existenz eines Pfades mit einer bestimmten Eigenschaft
- Computational Tree Logic (CTL): Erweiterung der LTL um existentielle/universelle Quantoren über modalen Pfadoperatoren.
  - Modale Operatoren: die Zustandsübergänge betreffend
- Name: Pfade im Berechnungsbaum durch Auffalten der FSM.
  - Beispiel Berechnungsbäume für die Getränkemaschine

CTL

Die Formeln der CTL sind gegeben durch:

$$
\begin{array}{rll}
\phi ::= & \top \mid \bot \mid p & \text{— True, false, atomic} \\
\mid & \neg\phi \mid \phi_1 \wedge \phi_2 \mid \phi_1 \vee \phi_2 \mid \phi_1 \longrightarrow \phi_2 & \text{— Propositional formulae} \\
\mid & \mathsf{AX}\,\phi \mid \mathsf{EX}\,\phi & \text{— All or some next state} \\
\mid & \mathsf{AF}\,\phi \mid \mathsf{EF}\,\phi & \text{— All or some future states} \\
\mid & \mathsf{AG}\,\phi \mid \mathsf{EG}\,\phi & \text{— All or some global future} \\
\mid & \mathsf{A}[\phi_1\ U\ \phi_2] \mid \mathsf{E}[\phi_1\ U\ \phi_2] & \text{— Until all or some}
\end{array}
$$

Erfüllbarkeit

- CTL-Formeln: wie LTL, aber mit Quantoren (A or E) über den Temporaloperatoren.
- Ganz grob: A heißt Temporaloperator gilt für alle Pfade von hier; E bedeutet, Temporaloperator gilt für mindestens ein Pfad von hier.
  - Nicht ganz: Temporaloperatoren sind wieder CTL-Formeln, deshalb Rekursion
- In conclusio: Erfüllbarkeitsrelation nicht für einzelne Pfade p oder Bäume t, sondern immer in Bezug auf bestimmten Zustand der FSM.

Erfüllbarkeit für CTL

Für eine FSM $\mathcal{M} = \langle \Sigma, \rightarrow \rangle$, $s \in \Sigma$ und eine CTL-Formel ϕ, die Erfüllbarkeitsrelation $\mathcal{M}, s \models \phi$ ist induktiv wie folgt definiert:

$$
\begin{array}{lll}
\mathcal{M}, s \models \top & & \\
\mathcal{M}, s \not\models \bot & & \\
\mathcal{M}, s \models p & \text{gdw} & p(s) \\
\mathcal{M}, s \models \phi \wedge \psi & \text{gdw} & \mathcal{M}, s \models \phi \text{ und } \mathcal{M}, s \models \psi \\
\mathcal{M}, s \models \phi \vee \psi & \text{gdw} & \mathcal{M}, s \models \phi \text{ oder } \mathcal{M}, s \models \psi \\
\mathcal{M}, s \models \phi \longrightarrow \psi & \text{gdw} & \text{wenn } \mathcal{M}, s \models \phi \text{ dann } \mathcal{M}, s \models \psi \\
\ldots &&
\end{array}
$$

Erfüllbarkeit für CTL

Für eine FSM $\mathcal{M} = \langle \Sigma, \rightarrow \rangle$, $s \in \Sigma$ und eine CTL-Formel ϕ, die Erfüllbarkeitsrelation $\mathcal{M}, s \models \phi$ ist induktiv wie folgt definiert:

$\ldots$

$\mathcal{M}, s \models \mathsf{AX}\,\phi$ gdw für alle s_1 mit $s \rightarrow s_1$ gibt es $\mathcal{M}, s_1 \models \phi$

$\mathcal{M}, s \models \mathsf{EX}\,\phi$ gdw es gibt s_1 mit $s \rightarrow s_1$ und $\mathcal{M}, s_1 \models \phi$

Erfüllbarkeit für CTL

Für eine FSM $\mathcal{M} = \langle \Sigma, \rightarrow \rangle$, $s \in \Sigma$ und eine CTL-Formel ϕ, die Erfüllbarkeitsrelation $\mathcal{M}, s \models \phi$ ist induktiv wie folgt definiert:

$\ldots$

$\mathcal{M}, s \models \mathsf{AX}\,\phi$	gdw	für alle s_1 mit $s \rightarrow s_1$ gibt es $\mathcal{M}, s_1 \models \phi$
$\mathcal{M}, s \models \mathsf{EX}\,\phi$	gdw	es gibt s_1 mit $s \rightarrow s_1$ und $\mathcal{M}, s_1 \models \phi$
$\mathcal{M}, s \models \mathsf{AG}\,\phi$	gdw	für alle Pfade p mit $p_1 = s$ gilt $\mathcal{M}, p_i \models \phi$ für alle $i \geq 2$
$\mathcal{M}, s \models \mathsf{EG}\,\phi$	gdw	es gibt einen Pfad p mit $p_1 = s$ und $\mathcal{M}, p_i \models \phi$ für alle $i \geq 2$

Erfüllbarkeit für CTL

Für eine FSM $\mathcal{M} = \langle \Sigma, \rightarrow \rangle$, $s \in \Sigma$ und eine CTL-Formel ϕ, die Erfüllbarkeitsrelation $\mathcal{M}, s \models \phi$ ist induktiv wie folgt definiert:

$\ldots$

$\mathcal{M}, s \models \mathsf{AX}\,\phi$	gdw	für alle s_1 mit $s \rightarrow s_1$ gibt es $\mathcal{M}, s_1 \models \phi$
$\mathcal{M}, s \models \mathsf{EX}\,\phi$	gdw	es gibt s_1 mit $s \rightarrow s_1$ und $\mathcal{M}, s_1 \models \phi$
$\mathcal{M}, s \models \mathsf{AG}\,\phi$	gdw	für alle Pfade p mit $p_1 = s$ gilt $\mathcal{M}, p_i \models \phi$ für alle $i \geq 2$
$\mathcal{M}, s \models \mathsf{EG}\,\phi$	gdw	es gibt einen Pfad p mit $p_1 = s$ und $\mathcal{M}, p_i \models \phi$ für alle $i \geq 2$
$\mathcal{M}, s \models \mathsf{AF}\,\phi$	gdw	für alle Pfade p mit $p_1 = s$ gilt $\mathcal{M}, p_i \models \phi$ für ein i
$\mathcal{M}, s \models \mathsf{EF}\,\phi$	gdw	es gibt einen Pfad p mit $p_1 = s$ und $\mathcal{M}, p_i \models \phi$ für ein i

Erfüllbarkeit für CTL

Für eine FSM $\mathcal{M} = \langle \Sigma, \rightarrow \rangle$, $s \in \Sigma$ und eine CTL-Formel ϕ, die Erfüllbarkeitsrelation $\mathcal{M}, s \models \phi$ ist induktiv wie folgt definiert:

$\ldots$

$\mathcal{M}, s \models \mathsf{AX}\,\phi$	gdw	für alle s_1 mit $s \rightarrow s_1$ gibt es $\mathcal{M}, s_1 \models \phi$
$\mathcal{M}, s \models \mathsf{EX}\,\phi$	gdw	es gibt s_1 mit $s \rightarrow s_1$ und $\mathcal{M}, s_1 \models \phi$
$\mathcal{M}, s \models \mathsf{AG}\,\phi$	gdw	für alle Pfade p mit $p_1 = s$ gilt $\mathcal{M}, p_i \models \phi$ für alle $i \geq 2$
$\mathcal{M}, s \models \mathsf{EG}\,\phi$	gdw	es gibt einen Pfad p mit $p_1 = s$ und $\mathcal{M}, p_i \models \phi$ für alle $i \geq 2$
$\mathcal{M}, s \models \mathsf{AF}\,\phi$	gdw	für alle Pfade p mit $p_1 = s$ gilt $\mathcal{M}, p_i \models \phi$ für ein i
$\mathcal{M}, s \models \mathsf{EF}\,\phi$	gdw	es gibt einen Pfad p mit $p_1 = s$ und $\mathcal{M}, p_i \models \phi$ für ein i
$\mathcal{M}, s \models \mathsf{A}[\phi\ U\ \psi]$	gdw	für alle Pfade p mit $p_1 = s$ gibt es i mit $\mathcal{M}, p_i \models \psi$ und für alle $j < i$, $\mathcal{M}, p_j \models \phi$
$\mathcal{M}, s \models \mathsf{E}[\phi\ U\ \psi]$	gdw	es gibt einen Pfad p mit $p_1 = s$ und es gibt i mit $\mathcal{M}, p_i \models \psi$ und für alle $j < i$, $\mathcal{M}, p_j \models \phi$

Spezifikationsmuster

- Etwas schlechtes (p) darf nicht auftreten: $\mathrm{AG}\,\neg p$ (Sicherheit)
- p tritt unendlich oft auf: $\mathrm{AG}(\mathrm{AF}\,p)$
- p tritt irgendwann auf: $\mathrm{AF}\,p$ (Verfügbarkeit)
- In der Zukunft, p wird irgenwann für immer gelten: $\mathrm{AF}\,\mathrm{AG}\,p$
- Wann immer p gilt, wird q irgendwann auch gelten: $\mathrm{AG}(p \longrightarrow \mathrm{AF}\,q)$
- In allen Zuständen ist p immer eine Möglichkeit: $\mathrm{AG}(\mathrm{EF}\,p)$

LTL und CTL

- CTL ist ausdrucksstärker als LTL, aber das gilt auch anders herum!
  - D.h. es gibt Eigenschaften, die in LTL ausgedrückt werden können, aber nicht in CTL.
- Beispiel: in allen Pfade, in denen p auftritt, tritt auch q auf.
- LTL: $\mathsf{F}\, p \longrightarrow \mathsf{F}\, q$
- CTL: Weder $\mathsf{AF}\, p \longrightarrow \mathsf{AF}\, q$ noch $\mathsf{AG}(p \longrightarrow \mathsf{AF}\, q)$
- Die Logik CTL^* kombiniert die Mächtigkeit von LTL and CTL.

Äquivalenzen

- Es gelten aussagenlogische Tautologien z.B. $\neg(\phi \vee \psi) \equiv \neg\phi \wedge \neg\psi$

$$\begin{array}{lcllcl} \neg(\mathsf{AF}\,\phi) & \equiv & \mathsf{EG}(\neg\phi) & \mathsf{AF}(\phi \vee \psi) & \equiv & \mathsf{AF}\,\phi \vee \mathsf{AF}\,\psi \\ \neg(\mathsf{EF}\,\phi) & \equiv & \mathsf{AG}(\neg\phi) & \mathsf{AG}(\phi \wedge \psi) & \equiv & \mathsf{AG}\,\phi \wedge \mathsf{AG}\,\psi \end{array}$$

$$\mathsf{A}[\phi\ U\ \psi] \equiv \neg(\mathsf{E}[\neg\psi\ U\ \neg\phi \wedge \neg\psi] \vee \mathsf{EG}\,\neg\psi)$$

Theorem (Funktionale Vollständigkeit von CTL)

Eine Menge von CTL-Operatoren ist funktional vollständig für CTL gdw. sie mind. jeweils einen der folgenden Mengen enthält: AX *oder* EX*;* EG, AF *oder* AU*; und* EU*.*

Modellprüfung (Model-Checking)

- Das Model-Checking Problem:

  Gegeben Modell $\mathcal{M}$ und Eigenschaft ϕ, gilt $\mathcal{M} \models \phi$?

- Das Grundproblem beim Model-Checking ist Zustandsexplosion.
  - Eine typische 32-Bit Ganzzahlvariabele hat über 4 Mrd. Zustände!
- Die Theorie bietet wenig Anlass zu Hoffnung:

Theorem (Komplexität von Modellprüfung)

(i) *Model-Checking für LTL ohne U ist NP-vollständig.*

(ii) *Model-Checking für LTL ist PSPACE-vollständig.*

(iii) *Model-Checking für CTL ist EXPTIME-vollständig.*

- Gute Nachricht: wenigstens entscheidbar
  - Schlüsseltechnik: Zustandsabstraktion und Zustandskompression

Skizze eines Model-Checking-Algorithmus für CTL

- Die Denotation einer CTL-Formel ϕ in einem Modell $\mathcal{M}$ ist definiert:
$$[\![\phi]\!]_{\mathcal{M}} \stackrel{def}{=} \{s \mid \mathcal{M}, s \models \phi\}$$
- Wir definieren $[\![\phi]\!]_{\mathcal{M}}$ durch Rekursion über ϕ:
  - Die aussagenlogischen Fälle sind einfach, z.B. $[\![\phi \vee \psi]\!] = [\![\phi]\!] \cup [\![\psi]\!]$
  - Die temporalen Operatoren werden durch die Äquivalenzen zu EX, EG, EU reduziert, z.B. $[\![\mathsf{AF}\,\phi]\!] = [\![\neg\,\mathsf{EG}\,\neg\phi]\!]$
- Für Menge von Zuständen $Y \subseteq S$, definiere:
$$pre_{\exists}(Y) \quad = \quad \{s \in S \mid \exists s'.(s \to s', s' \in Y)\}$$
und damit rekursive Formulierung für EG, EU:

$$\begin{aligned} [\![\mathsf{EX}\,\phi]\!] &= pre_{\exists}([\![\phi]\!]) \\ [\![\mathsf{EG}\,\phi]\!] &= [\![\phi]\!] \cap pre_{\exists}([\![\mathsf{EG}\,\phi]\!]) \\ [\![\mathsf{E}[\phi\ U\ \psi]]\!] &= [\![\psi]\!] \cup ([\![\phi]\!] \cap pre_{\exists}([\![\mathsf{E}[\phi\ U\ \psi]]\!])) \end{aligned}$$

- Basis für funktionale Implementation oder Korrektheitsbeweis.

Model-Checking Werkzeuge

- NuSMV2 (Edmund Clarke, Ken McMillan)
  - Web Seite: `http://nusmv.fbk.eu/`
- Spin (Gerard Holzmann)
  - Web Seite: `http://spinroot.com/`
- NuSMV vs. Spin:
  - Spin (Promela) ist näher an einer Programmiersprache
  - NuSMV unterstützt auch CTL

Zusammenfassung

- LTL und CTL sind temporale Logiken, die Aussagen über das Verhalten eines als FSM modellierten Systems erlauben.
  - Unterschiedliche Mächtigkeiten
  - LTL für Sicherheitseigenschaften, CTL für Verfügbarkeit.
- Modellprüfung (Model-Checking):
  - Entscheidbar, aber mit hoher Komplexität (Zustandsexplosion)
  - Zustandsabstraktion und Zustandskompression machen Model-Checking handhabbar.
- Model-Checker wie NuSMV entscheiden das Model-Checking-Problem.
  - Bei negativer Antwort Gegenbeispiel.
  - Vertrauenswürdigkeit: bei positiver Antwort? Wie gut ist das Modell?