

Formale Modellierung

Vorlesung 12 vom 07.07.2014: Temporale Logik und Modellprüfung

Serge Autexier & Christoph Lüth

Universität Bremen

Sommersemester 2014

1 [15]

Organisatorisches

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

2 [15]

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

3 [15]

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

4 [15]

CTL

Die Formeln der CTL sind gegeben durch:

$\phi ::= \top \mid \perp \mid p$	— True, false, atomic
$\neg\phi \mid \phi_1 \wedge \phi_2 \mid \phi_1 \vee \phi_2 \mid \phi_1 \rightarrow \phi_2$	— Propositional formulae
$AX\phi \mid EX\phi$	— All or some next state
$AF\phi \mid EF\phi$	— All or some future states
$AG\phi \mid EG\phi$	— All or some global future
$A[\phi_1 U \phi_2] \mid E[\phi_1 U \phi_2]$	— Until all or some

5 [15]

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.

6 [15]

Erfüllbarkeit für CTL

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

$\mathcal{M}, s \models \top$	
$\mathcal{M}, s \not\models \perp$	
$\mathcal{M}, s \models p$	gdw $p(s)$
$\mathcal{M}, s \models \phi \wedge \psi$	gdw $\mathcal{M}, s \models \phi$ und $\mathcal{M}, s \models \psi$
$\mathcal{M}, s \models \phi \vee \psi$	gdw $\mathcal{M}, s \models \phi$ oder $\mathcal{M}, s \models \psi$
$\mathcal{M}, s \models \phi \rightarrow \psi$	gdw wenn $\mathcal{M}, s \models \phi$ dann $\mathcal{M}, s \models \psi$
...	

7 [15]

Erfüllbarkeit für CTL

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

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

8 [15]

Spezifikationsmuster

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

9 [15]

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 Pfaden, in denen p auftritt, tritt auch q auf.
- ▶ LTL: $F p \longrightarrow F q$
- ▶ CTL: **Weder** $AF p \longrightarrow AF q$ **noch** $AG(p \longrightarrow AF q)$
- ▶ Die Logik CTL^* kombiniert die Mächtigkeit von LTL and CTL.

10 [15]

Äquivalenzen

- ▶ Es gelten aussagenlogische Tautologien z.B. $\neg(\phi \vee \psi) \equiv \neg\phi \wedge \neg\psi$
 $\neg(AF \phi) \equiv EG(\neg\phi) \quad AF(\phi \vee \psi) \equiv AF \phi \vee AF \psi$
 $\neg(EF \phi) \equiv AG(\neg\phi) \quad AG(\phi \wedge \psi) \equiv AG \phi \wedge AG \psi$
 $A[\phi U \psi] \equiv \neg(E[\neg\psi U \neg\phi \wedge \neg\psi] \vee EG \neg\psi)$

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.

11 [15]

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 Ganzzahlvariable 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**

12 [15]

Skizze eines Model-Checking-Algorithmus für CTL

- ▶ Die **Denotation** einer CTL-Formel ϕ in einem Modell $\mathcal{M}$ ist definiert:
$$\llbracket \phi \rrbracket_{\mathcal{M}} \stackrel{\text{def}}{=} \{s \mid \mathcal{M}, s \models \phi\}$$
- ▶ Wir definieren $\llbracket \phi \rrbracket_{\mathcal{M}}$ durch Rekursion über ϕ :
 - ▶ Die aussagenlogischen Fälle sind einfach, z.B. $\llbracket \phi \vee \psi \rrbracket = \llbracket \phi \rrbracket \cup \llbracket \psi \rrbracket$
 - ▶ Die temporalen Operatoren werden durch die Äquivalenzen zu EX, EG, EU reduziert, z.B. $\llbracket AF \phi \rrbracket = \llbracket \neg EG \neg \phi \rrbracket$
- ▶ Für Menge von Zuständen $Y \subseteq S$, definiere:
$$pre_3(Y) = \{s \in S \mid \exists s'. (s \rightarrow s', s' \in Y)\}$$

und damit **rekursive Formulierung** für EG, EU:

$$\begin{aligned}\llbracket EX \phi \rrbracket &= pre_3(\llbracket \phi \rrbracket) \\ \llbracket EG \phi \rrbracket &= \llbracket \phi \rrbracket \cap pre_3(\llbracket EG \phi \rrbracket) \\ \llbracket E[\phi U \psi] \rrbracket &= \llbracket \psi \rrbracket \cup (\llbracket \phi \rrbracket \cap pre_3(\llbracket E[\phi U \psi] \rrbracket))\end{aligned}$$

- ▶ Basis für funktionale Implementation oder Korrektheitsbeweis.

13 [15]

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

14 [15]

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?

15 [15]