

Formale Modellierung
Vorlesung 11 vom 30.06.2014: Lineare Temporale Logik

Serge Autexier & Christoph Lüth

Universität Bremen

Sommersemester 2014

1 [14]

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

2 [14]

Tagesmenu: Lineare Temporale Logik

Logik	Programmbegriff	Beweisprinzip
HOL	Rekursive Funktion	Induktion
OCL ¹	Zustandsübergang	Vor/Nachbedingung
TL	Zustandsmaschine	Modelchecking

- ▶ Endliche Zustandsmaschinen
- ▶ Pfadausdrücke
- ▶ Ausdrücke über Pfaden: LTL

¹Und andere

3 [14]

Endliche Zustandsmaschine

Definition (Finite State Machine (FSM))

Eine FSM ist $\mathcal{M} = \langle \Sigma, \rightarrow \rangle$ mit

- ▶ Σ eine **endliche** Menge von **Zuständen**, und
- ▶ $\rightarrow \subseteq \Sigma \times \Sigma$ eine **Zustandsübergangsrelation**, mit \rightarrow linkstotal:

$$\forall s \in \Sigma. \exists s' \in \Sigma. s \rightarrow s'$$

- ▶ Varianten dieser Definition: Zustandsvariablen oder benannte Zustandsübergänge
- ▶ NB: Kein Endzustand, und keine Ein/Ausgabe (Unterschied zu **Automaten**)
- ▶ Wenn \rightarrow eine Funktion ist (rechtseindeutig), dann ist die FSM **deterministisch**, ansonsten **nicht-deterministisch**.
- ▶ Jede nicht-deterministische FSM kann durch die Power-State-Konstruktion deterministisch gemacht werden.

4 [14]

Ein Einfaches Beispiel

- ▶ Getränkemaschine für Kaffee
- ▶ Nimmt 10c oder 20c Münzen
- ▶ Kleiner Kaffee 10c, großer Kaffee 20c
- ▶ Nimmt nicht mehr als zwei Münzen
- ▶ Geldrückgabe

5 [14]

Linear Temporal Logic (LTL) and Pfade

- ▶ LTL ist die Logik über **Ausführungspfade** in einer FSM.
- ▶ Wir definieren erst Pfade, dann LTL-Formeln, dann eine Erfülltheitsrelation.

Definition (Pfade)

Für eine FSM $\mathcal{M} = \langle \Sigma, \rightarrow \rangle$ ist ein **Pfad** in \mathcal{M} eine (unendliche) Sequenz $\langle s_1, s_2, s_3, \dots \rangle$ mit $s_i \in \Sigma$ und $s_i \rightarrow s_{i+1}$ für alle i .

- ▶ Notation: Sei $p = \langle s_1, s_2, s_3, \dots \rangle$ ein Pfad, dann ist $p_i \stackrel{\text{def}}{=} s_i$ (Selektion) und $p^i \stackrel{\text{def}}{=} \langle s_i, s_{i+1}, \dots \rangle$ (Suffix ab Position i).

6 [14]

Lineare Temporale Logik (LTL)

$\phi ::= \top \mid \perp \mid q$	— True, false, atomar
$\mid \neg \phi \mid \phi_1 \wedge \phi_2 \mid \phi_1 \vee \phi_2 \mid \phi_1 \rightarrow \phi_2$	— Aussagenlog. Formeln
$\mid X \phi$	— Nächster Zustand
$\mid F \phi$	— Irgendwann
$\mid G \phi$	— Immer
$\mid \phi_1 U \phi_2$	— Bis

- ▶ Präzedenzen: unäre Operatoren; dann U ; dann \wedge, \vee ; dann \rightarrow .
- ▶ Eine atomare Formel p ist ein **Zustandsprädikat**. Andere (äquivalente) Möglichkeit: Zustände mit atomaren Prädikaten zu benennen.
- ▶ Andere Operatoren wie $\phi R \psi$ (release) oder $\phi W \psi$ (schwaches until).

7 [14]

Erfüllung und Modelle für LTL

Die **Erfüllbarkeitsrelation** für einen Pfad p und eine LTL-Formel ϕ ist induktiv wie folgt definiert:

$p \models \top$	$p \models \phi \wedge \psi$ gdw	$p \models \phi$ und $p \models \psi$
$p \not\models \perp$	$p \models \phi \vee \psi$ gdw	$p \models \phi$ oder $p \models \psi$
$p \models q$ gdw	$q(p_1)$	$p \models \phi \rightarrow \psi$ gdw
$p \models \neg \phi$ gdw	$p \not\models \phi$	wenn $p \models \phi$ dann $p \not\models \psi$

$p \models X \phi$ gdw	$p^2 \models \phi$
$p \models G \phi$ gdw	für alle i gilt $p^i \models \phi$
$p \models F \phi$ gdw	es gibt i mit $p^i \models \phi$
$p \models \phi U \psi$ gdw	es gibt i mit $p^i \models \psi$ und für $j = 1, \dots, i-1$, $p^j \models \phi$

Definition (Modell einer LTL-Formel)

Eine FSM \mathcal{M} erfüllt eine LTL formula ϕ , $\mathcal{M} \models \phi$, gdw. jeder Pfad p in \mathcal{M} erfüllt.

8 [14]

Äquivalenzen

Definition (Äquivalenz)

Zwei Formeln sind äquivalent, $\phi \equiv \psi$ gdw. für alle FSM \mathcal{M} und Pfade p in \mathcal{M} , $p \models \phi \leftrightarrow p \models \psi$

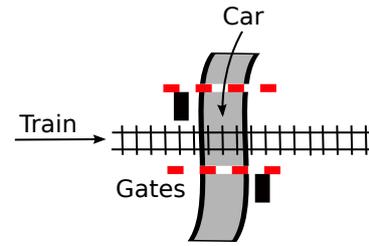
- ▶ Es gelten aussagenlogische Tautologien z.B. $\neg(\phi \vee \psi) \equiv \neg\phi \wedge \neg\psi$

$$\begin{aligned} F(\phi \vee \psi) &\equiv F\phi \vee F\psi & \neg F\phi &\equiv G(\neg\phi) & FGF\phi &\equiv GF\phi \\ G(\phi \wedge \psi) &\equiv G\phi \wedge G\psi & \neg G\phi &\equiv F(\neg\phi) & GFG\phi &\equiv FG\phi \\ & & \neg X\phi &\equiv X(\neg\phi) & & \end{aligned}$$

$$\begin{aligned} XF\phi &\equiv FX\phi & F\phi &\equiv \phi \vee XF\phi \\ XG\phi &\equiv GX\phi & G\phi &\equiv \phi \wedge XG\phi \\ X(\phi U \psi) &\equiv X\phi U X\psi & \phi U \psi &\equiv \psi \vee (\phi \wedge X(\phi U \psi)) \end{aligned}$$

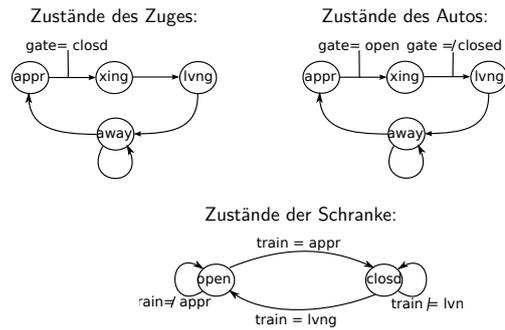
9 [14]

Längeres Beispiel: der Bahnübergang



10 [14]

Modellierung des Bahnübergangs



11 [14]

Die FSM

- ▶ Zustände sind eine endliche Abbildung der Variablen Car , $Train$, $Gate$ auf Wertebereiche:

$$\begin{aligned} \Sigma_{Car} &= \{\text{appr}, \text{xing}, \text{lvng}, \text{away}\} \\ \Sigma_{Train} &= \{\text{appr}, \text{xing}, \text{lvng}, \text{away}\} \\ \Sigma_{Gate} &= \{\text{open}, \text{clsd}\} \end{aligned}$$

oder ein Tripel $S \in \Sigma = \Sigma_{Car} \times \Sigma_{Train} \times \Sigma_{Gate}$.

- ▶ Zustandsübergang **komponentenweise**, bspw:

$$\begin{aligned} \langle \text{away}, \text{open}, \text{away} \rangle &\rightarrow \langle \text{appr}, \text{open}, \text{away} \rangle \\ \langle \text{appr}, \text{open}, \text{away} \rangle &\rightarrow \langle \text{xing}, \text{open}, \text{away} \rangle \\ &\dots \end{aligned}$$

12 [14]

Bahnübergang — Formalisierung von Eigenschaften

- ▶ Bahn und Auto überqueren den Übergang nie zur selben Zeit:

$$G \neg(\text{car} = \text{xing} \wedge \text{train} = \text{xing})$$

- ▶ Ein Auto kann den Übergang immer wieder verlassen:

$$G(\text{car} = \text{xing} \rightarrow F(\text{car} = \text{lvng}))$$

- ▶ Ein annähernder Zug darf irgendwann den Bahnübergang passieren:

$$G(\text{train} = \text{appr} \rightarrow F(\text{train} = \text{xing}))$$

- ▶ Es gibt Autos, die den Bahnübergang passieren:

$$F(\text{car} = \text{xing}) \text{ ist etwas anderes!}$$

- ▶ Nicht in LTL auszudrücken!

13 [14]

Zusammenfassung

- ▶ LTL: Logik über **Pfade** in **Zustandsautomaten**
- ▶ Aussagenlogik plus modale Operatoren (X, G, F, U)
- ▶ Man kann eine Axiomatisierung und Schlussregeln angeben
 - ▶ Dann ist LTL konsistent und vollständig.
- ▶ In der Praxis wird LTL über Modellprüfung (**model checking**) bewiesen.
 - ▶ Modellierung des Systems als FSM \mathcal{M} , Eigenschaften als LTL-Formel ϕ , Überprüfung ob $\mathcal{M} \models \phi$.
- ▶ LTL ist für **Sicherheitseigenschaften**, keine **Verfügbarkeit**.
- ▶ Dazu mehr in der **nächsten Vorlesung**

14 [14]