Ludwig-Maximilians-Universität München
Institut für Informatik
Dr. S. Merz

SS 2001
Begleitblatt 11

Temporale Logik

Zustandsübergangssysteme

Im folgenden stehe $\mathcal{L}_T$ immer für $\mathcal{L}_{PLTL}$, ggf. mit Erweiterungen.

PLTL-Theorien

Definition. Sei $TSIG$ eine temporale Signatur. Eine *PLTL-Theorie* $\mathcal{T} = (\mathcal{L}_T, \mathbb{A})$ ist gegeben durch:

- eine Sprache $\mathcal{L}_T$ über $TSIG$,
- eine Menge $\mathbb{A}$ von Formeln von $\mathcal{L}_T$ (*nicht-logische Axiome*)

Eine temporale Struktur $\mathbb{K}$ für $TSIG$ heißt *Modell* von $\mathcal{T}$, wenn jede Formel von $\mathbb{A}$ in der Struktur $\mathbb{K}$ gültig ist.

Sei $\mathcal{C}$ eine Klasse von temporalen Strukturen für $TSIG$. $\mathcal{T}$ heißt *$\mathcal{C}$-PLTL-Theorie*, wenn jede temporale Struktur in $\mathcal{C}$ Modell von $\mathcal{T}$ ist.

Zustandsübergangssysteme: grundlegende Definitionen

Definition. Gegeben sei eine Signatur $SIG = (S, F, P)$ und eine Struktur $\mathbb{S}$ für SIG. Ein *Zustandsübergangssystem (state transition system, STS)* $\Gamma = (X, V, Z, T)$ (bzgl. SIG und $\mathbb{S}$) ist gegeben durch:

- höchstens abzählbar unendliche Mengen X_s für jedes $s \in S$, schreibe $X = \bigcup_{s \in S} X_s$,
- eine höchstens abzählbar unendliche Menge V (die Elemente von $X \cup V$ heißen *Systemvariablen (Zustandsvariablen)*,
- eine Menge Z von *(System-)Zuständen*

$$\eta : \begin{cases} X_s \to |\mathbb{S}|_s & \text{für jedes } s \in S \\ V \to \{\mathbf{f}, \mathbf{t}\} \end{cases}$$

- eine (links-)totale Relation $T \subseteq Z \times Z$ (*Transitionsrelation*).

Ein *Ablauf* von Γ ist eine Folge $\mathbb{W} = (\eta_0, \eta_1, \ldots)$ von Systemzuständen mit $(\eta_i, \eta_{i+1}) \in T$ für alle $i \in \mathbb{N}_0$.

Γ heißt *(zustands-)endlich*, wenn Z endlich ist. Γ heißt *propositional*, wenn $X = \emptyset$ (dann SIG und $\mathbb{S}$ irrelevant).

Sei $\Gamma = (X, V, Z, T)$ ein STS bzgl. SIG, $\mathbb{S}$, dann ist $TSIG_\Gamma = (SIG, X, V)$. Die *Sprache $\mathcal{L}_{T\Gamma}$ der linearen temporalen Logik von* Γ ist die Sprache $\mathcal{L}_T(TSIG_\Gamma)$. Offenbar ist für jeden Ablauf $\mathbb{W}$ von Γ das Paar $\mathbb{K} = (\mathbb{S}, \mathbb{W})$ eine temporale Struktur für $TSIG_\Gamma$.

Die Signatur SIG^+ entstehe aus SIG, indem die Elemente von X zu den Konstanten und die Elemente von V zu den atomaren Aussagen hinzugenommen werden. Die *prädikatenlogische Sprache $\mathcal{L}_\Gamma$ von* Γ ist die Sprache $\mathcal{L}_{PL}(SIG^+)$. $\mathcal{L}_\Gamma$ ist der Kern $kern(\mathcal{L}_{T\Gamma})$ von $\mathcal{L}_{T\Gamma}$.

Definition. Zu einem Transitionssystem Γ (bzgl. SIG und $\mathbb{S}$) sei

$$\mathcal{C}_\Gamma = \{\ \mathbb{K} = (\mathbb{S}, \mathbb{W}) \ \mid\ \mathbb{W} \text{ Ablauf von } \Gamma\ \}$$

Eine Formel A von $\mathcal{L}_{T\Gamma}$ heißt Γ-*gültig* (in Zeichen $\models_\Gamma A$), wenn sie in jedem $\mathbb{K} \in \mathcal{C}_\Gamma$ gültig ist. Eine $\mathcal{C}_\Gamma$-PLTL-Theorie (kurz: Γ-*Theorie*) heißt *(axiomatische) PLTL-Spezifikation von* Γ.

Spezielle Klassen von Zustandsübergangssystemen

Definition. Ein *STS mit Startzuständen (verwurzeltes STS, STS$_s$)* $\Gamma = (X, V, Z, T, \text{start}_\Gamma)$ ist ein STS $\Gamma' = (X, V, Z, T)$ zusammen mit einer Formel start_Γ von $\mathcal{L}_{\Gamma'}$ (*Anfangsbedingung*). Ein Ablauf von Γ ist ein Ablauf $(\eta_0, \eta_1, \ldots)$ von Γ' mit $\mathbb{S}^{(\xi,\eta_0)}(\text{start}_\Gamma) = \mathbf{t}$ für jede Variablenbelegung ξ.

Satz 5.1.1. Für jedes STS$_s$ Γ ist das folgende Axiom Γ-gültig.

(root) $\quad \textsf{init} \rightarrow \text{start}_\Gamma$

Definition. Ein *markiertes STS (MSTS)* Γ ist gegeben durch:

- eine endliche Menge $\mathcal{A}$ von *Aktionen*,
- ein STS (X, V, Z, T) mit
  - $\{\text{exec } \lambda \mid \lambda \in \mathcal{A}\} \subseteq V$,
  - Falls $(\eta, \eta') \in T$ und $\eta(\text{exec } \lambda) = \mathbf{f}$ für alle $\lambda \in \mathcal{A}$, so ist $\eta' = \eta$.

Für ein MSTS Γ mit Aktionen $\mathcal{A} = \{\lambda_1, \ldots, \lambda_n\}$ bezeichnet nil_Γ die Formel

$$\text{nil}_\Gamma \quad \equiv \quad \neg\text{exec } \lambda_1 \wedge \ldots \wedge \neg\text{exec } \lambda_n$$

Markierte STS mit Startzuständen (MSTS$_s$) werden analog definiert.

Satz 5.2.1. Für jedes MSTS$_{(s)}$ Γ ist das folgende Axiom Γ-gültig.

(nil) $\quad \text{nil}_\Gamma \wedge A \rightarrow \circ A \quad$ falls A Zustandsformel von Γ

Folgerung aus 5.2.1. Sei Γ ein MSTS$_{(s)}$. Die folgende abgeleitete Regel ist Γ-gültig:

(trans) $\quad \text{exec } \lambda \wedge A \rightarrow \circ B \quad$ für ale $\lambda \in \mathcal{A}_\Gamma$
$\quad\quad\quad\quad \text{nil}_\Gamma \wedge A \rightarrow B$
$\quad\quad\quad \vdash \; A \rightarrow \circ B \quad$ falls A und B Zustandsformeln von Γ

Definition. Ein *faires STS$_{(s)}$ (FSTS$_{(s)}$)* ist ein MSTS$_{(s)}$ $\Gamma = (X, V, Z, T, \mathcal{A}, (\text{start}))$ zusammen mit je einer Formel enabled_λ von $\mathcal{L}_\Gamma$ für jedes $\lambda \in \mathcal{A}$ *(Ausführbarkeitsbedingung, enabling condition)*. Ein Ablauf von Γ ist ein Ablauf $(\eta_0, \eta_1, \ldots)$ (im bisherigen Sinn) mit folgenden zusätzlichen Eigenschaften (ξ beliebig):

- Für alle $\lambda \in \mathcal{A}$ und $i \in \mathbb{N}_0$ gilt: Falls $\mathbb{S}_\Gamma^{(\xi,\eta_i)}(\text{exec } \lambda) = \mathbf{t}$, so auch $\mathbb{S}_\Gamma^{(\xi,\eta_i)}(\text{enabled}_\lambda) = \mathbf{t}$.
- Für alle $\lambda \in \mathcal{A}$ gilt: Falls $\mathbb{S}_\Gamma^{(\xi,\eta_k)}(\text{enabled}_\lambda) = \mathbf{t}$ für unendlich viele k, so ist $\mathbb{S}_\Gamma^{(\xi,\eta_k)}(\text{exec } \lambda) = \mathbf{t}$ für unendlich viele k (*fairer Ablauf*).

Satz 5.2.2. Für jedes FSTS$_{(s)}$ Γ sind die folgenden Axiome Γ-gültig:

(action) $\quad \text{exec } \lambda \rightarrow \text{enabled}_\lambda$
(fair) $\quad \Box\Diamond\text{enabled}_\lambda \rightarrow \Diamond\text{exec } \lambda$

Folgerung aus 5.2.2. Für jedes FSTS$_{(s)}$ Γ sind die folgende abgeleitete Formeln Γ-gültig:

(progress) $\quad \text{enabled}_\lambda \rightarrow \neg\text{nil}_\Gamma \quad$ für jedes $\lambda \in \mathcal{A}_\Gamma$