Reaktive Systeme

Prof. Martin Wirsing

13.12.2002

Spezifikation von Transitionssystemen mit TLA

Temporale Logiken zur Beschreibung reaktiver Systeme und ihrer Eigenschaften wurden seit der 2. Hälfte der 1970er Jahre entwickelt (erste Veröffentlichungen 1977 von A. Pnueli und von F. Kröger).

Ab 1990 definierte L. Lamport die Temporal Logic of Actions (TLA), die sich durch folgende Charakteristika auszeichnet:

- natürliche Beschreibung von Transitionssystemen durch Formeln
- Charakterisierung von Begriffen wie (Parallel-)Komposition, Verfeinerung, Hiding durch einen möglichst kleinen Satz logischer Operatoren
- weitgehende Reduktion temporallogischer Verifikationsbedingungen auf prädikatenlogische Beweisverpflichtungen

Ziele

- TLA als Beschreibungssprache für reaktive Systeme
- unterschiedliche Spezifikationsstile, z.B. asynchrone vs. synchrone Kommunikation, Interleaving vs. echte Parallelität
- grundlegende Regeln zur Systemverifikation in TLA
- Komposition, Verfeinerung und Hiding
- Implementierungsbeweise durch Verfeinerungsabbildungen

Die Logik TLA

Example (Spezifikation einer Uhr mit Stunden- und Minutenanzeige):

$$
\begin{aligned}
IClk &\equiv hr \in \{0,\ldots,23\} \wedge min \in \{0,\ldots,59\} \\
Min &\equiv min < 59 \wedge min' = min + 1 \wedge hr' = hr \\
Hr &\equiv min = 59 \wedge min' = 0 \wedge hr' = (hr + 1) \bmod 24 \\
Tick &\equiv Min \vee Hr \\
Clock &\equiv IClk \wedge \Box[Tick]_{hr,min} \wedge \mathrm{WF}_{hr,min}(Tick)
\end{aligned}
$$

Üblicherweise haben Systemspezifikationen in TLA die Form

$$Init \wedge \Box[Next]_v \wedge L$$

Dabei ist

[$Init$:] eine prädikatenlogische Formel zur Beschreibung der Anfangszustände.

[$Next$:] eine Formel mit gestrichenen und ungestrichenen Variablen zur Beschreibung der erlaubten Zustandsübergänge. $Next$ hat meist die Form $A_1 \vee \ldots \vee A_n$, wobei die Formeln A_i die einzelnen Systemaktionen beschreiben.

[v :] ein Tupel aller Variablen, die vom System verändert werden können.

[L :] eine Konjunktion von Fairnessbedingungen $\mathrm{WF}_v(A_i)$ oder $\mathrm{SF}_v(A_i)$.

Man unterscheidet in TLA drei Klassen von Formeln:

- Zustandsformeln beschreiben Zustände,
- Aktionsformeln beschreiben Zustandsübergänge,
- temporallogische Formeln beschreiben Abläufe.

Zustandsformeln (state predicates)

Im folgenden sei eine (z.B. algebraisch beschriebene) Signatur Σ vorausgesetzt.

Prädikatenlogische (Σ-)Formeln heißen in TLA Zustandsformeln.

Beispiele: $n > 0$, $q =$ empty, $y = 0 \Leftrightarrow pc_1 =$ “g”, $\exists\, k : n = m + k$

Formal wird die Menge X der Variablen unterteilt in disjunkte Teilmengen

- X_f von flexiblen (zustandsabhängigen) Variablen und
- X_r von rigiden (zustandsunabhängigen) Variablen.

Die rigiden Variablen entsprechen den üblichen Variablen der Prädikatenlogik.

Die flexiblen Variablen modellieren Zustandskomponenten (z.B. Programmvariablen).

Die Syntax von Zustandsformeln entspricht der Definition von Σ-Formeln in Abschnitt 2.2 von Teil II der Vorlesung.

Interpretation von Zustandsformeln

Vorausgesetzt sei eine gegebene Σ-Algebra A.

Ein Zustand s ist eine (sortenrichtige) Belegung der flexiblen Variablen mit Werten.

Zustandsformeln werden interpretiert relativ zu einem Zustand s und einer Belegung ξ der rigiden Variablen.

Terme:

$$[\![x]\!]_{s,\xi} = \xi(x) \qquad \text{für rigide Variablen } x \in X_r$$
$$[\![v]\!]_{s,\xi} = s(v) \qquad \text{für flexible Variablen } v \in X_f$$
$$[\![f(t_1,\ldots,t_n)]\!]_{s,\xi} = f^A([\![t_1]\!]_{s,\xi},\ldots,[\![t_n]\!]_{s,\xi})$$

Formeln:

$$[\![p(t_1,\ldots,t_n)]\!]_{s,\xi} = \mathrm{T} \quad \text{gdw.} \quad ([\![t_1]\!]_{s,\xi},\ldots,[\![t_n]\!]_{s,\xi}) \in p^A$$
$$[\![\neg\, P]\!]_{s,\xi} = \mathrm{T} \quad \text{gdw.} \quad [\![P]\!]_{s,\xi} = \mathrm{F}$$
$$[\![P \wedge Q]\!]_{s,\xi} = \mathrm{T} \quad \text{gdw.} \quad [\![P]\!]_{s,\xi} = \mathrm{T} \text{ und } [\![Q]\!]_{s,\xi} = \mathrm{T}$$
$$[\![\exists\, x : P]\!]_{s,\xi} = \mathrm{T} \quad \text{gdw.} \quad [\![P]\!]_{s,\eta} = \mathrm{T} \text{ für ein } \eta \text{ mit } \eta(y) = \xi(y) \text{ für alle } y \in X_r \setminus \{x\}$$
$$[\![\exists\, v : P]\!]_{s,\xi} = \mathrm{T} \quad \text{gdw.} \quad [\![P]\!]_{t,\xi} = \mathrm{T} \text{ für ein } t \text{ mit } t(w) = s(w) \text{ für alle } w \in X_f \setminus \{v\}$$

Für eine gegebene Belegung ξ beschreiben Zustandsformeln also Mengen von Zuständen, z.B. die möglichen Anfangszustände eines Transitionssystems.

Aktionsformeln (actions, transition predicates)

Aktionsformeln sind prädikatenlogische Formeln, die gestrichene und ungestrichene Variablen enthalten dürfen.

Beispiele: $n' = n + 1, \quad q' = \text{cons}(i', q), \quad \exists x : n = x + m'$

Formal sei $X_f' = \{v' \mid v \in X_f\}$ eine Kopie von X_f.

Aktionsformeln sind prädikatenlogische (Σ-)Formeln mit Variablen aus $X_r \cup X_f \cup X_f'$.

Semantik.

Aktionsformeln werden interpretiert relativ zu einem Paar (s, t) von Zuständen und einer Belegung ξ von X_r.

Dabei ist
$$[\![v]\!]_{s,t,\xi} = s(v) \quad \text{für } v \in X_f$$
$$[\![v']\!]_{s,t,\xi} = t(v) \quad \text{für } v' \in X_f'$$
$$[\![x]\!]_{s,t,\xi} = \xi(x) \quad \text{für } x \in X_r$$

Wie bei Operationsschemata in Z werden gestrichene Variablen im Nachfolgerzustand interpretiert.

Für eine gegebene Belegung ξ von X_r beschreiben Aktionsformeln eine Menge von Zustandspaaren, z.B. die erlaubten Übergänge eines Transitionssystems.

Abkürzende Schreibweisen

- Für einen Term t bzw. eine Zustandsformel P bezeichnen t' und P' das Ergebnis der Ersetzung der freien Variablen $v \in X_f$ durch die entsprechenden Variablen $v' \in X'_f$. Dabei werden gebundene Variablen ggf. umbenannt, um Namenskonflikte zu vermeiden.

  Beispiele:
  $$\begin{aligned} (v+1)' &\equiv v'+1 \\ (\exists\, x : n = x + m)' &\equiv \exists\, x : n' = x + m' \\ (\exists\, n' : n = n' + m)' &\equiv \exists\, n1 : n' = n1 + m' \end{aligned}$$

- Für eine Aktionsformel A und Terme $t_1, \ldots, t_n$ (ohne gestrichene Variablen):

$$\begin{aligned} [A]_{t_1,\ldots,t_n} &\equiv A \vee (t'_1 = t_1 \wedge \ldots \wedge t'_n = t_n) \\ \langle A \rangle_{t_1,\ldots,t_n} &\equiv A \wedge \neg\, (t'_1 = t_1 \wedge \ldots \wedge t'_n = t_n) \end{aligned}$$

Ein Paar (s,t) von Zuständen erfüllt die Formel $[A]_{t_1,\ldots,t_n}$, wenn es A erfüllt oder wenn die Werte aller Terme $t_1, \ldots, t_n$ unverändert bleiben.

Ein Paar (s,t) von Zuständen erfüllt die Formel $\langle A \rangle_{t_1,\ldots,t_n}$, wenn es A erfüllt und wenn sich der Wert mindestens eines Terms $t_1, \ldots, t_n$ ändert.

Es gilt: $\langle A \rangle_{t_1,\ldots,t_n} \Leftrightarrow \neg\, [\neg\, A]_{t_1,\ldots,t_n}$ und $[A]_{t_1,\ldots,t_n} \Leftrightarrow \neg\, \langle \neg\, A \rangle_{t_1,\ldots,t_n}$

- Für eine Aktionsformel A definieren wir

$$\text{ENABLED}\, A \;\equiv\; \exists\, v_1', \ldots, v_n' : A$$

wobei $\{v_1', \ldots, v_n'\}$ die Menge der freien gestrichenen Variablen ($\in X_f'$) ist.

Die Zustandsformel ENABLED A gilt in einem Zustand s genau dann, wenn es einen Zustand t gibt, so dass A im Zustandspaar (s, t) erfüllt ist.

Example:

$$\text{ENABLED}(n' = n + 1) \;\equiv\; \exists\, n' : n' = n + 1$$

$$\text{ENABLED}(q = \mathsf{cons}(o', q')) \;\equiv\; \exists\, o', q' : q = \mathsf{cons}(o', q')$$

$$\text{ENABLED}(\exists\, z' : w = v' + z') \;\equiv\; \exists\, v', z' : w = v' + z'$$

$$(\text{ENABLED}(q = \mathsf{cons}(o', q')))' \;\equiv\; \exists\, o1, q1 : q' = \mathsf{cons}(o1, q1)$$

Temporallogische Formeln (temporal formulas) werden (zunächst) induktiv folgendermaßen definiert:

Definition:

- Jede Zustandsformel P ist eine temporale Formel.
- Ist A Aktionsformel und sind $t_1, \ldots, t_m$ Terme, so ist $\Box[A]_{t_1,\ldots,t_m}$ temporale Formel.
- Ist F temporale Formel, so ist $\Box F$ ("always F") temporale Formel.
- Aussagenlogische Kombinationen temporaler Formeln sind temporale Formeln.

Semantik temporaler Formeln definiert über Folgen $\sigma = s_0 s_1 \ldots$ von Zuständen

$$
\begin{aligned}
[\![P]\!]_{\sigma,\xi} = \mathrm{T} \quad &\text{gdw.} \quad [\![P]\!]_{s_0,\xi} = \mathrm{T} \qquad (P \text{ Zustandsformel}) \\
[\![\Box[A]_t]\!]_{\sigma,\xi} = \mathrm{T} \quad &\text{gdw.} \quad [\![[A]_t]\!]_{s_n,s_{n+1},\xi} = \mathrm{T} \text{ für alle } n \in \mathbb{N} \\
[\![\Box F]\!]_{\sigma,\xi} = \mathrm{T} \quad &\text{gdw.} \quad [\![F]\!]_{\sigma[n..],\xi} = \mathrm{T} \text{ für alle } n \in \mathbb{N} \\
[\![\neg F]\!]_{\sigma,\xi} = \mathrm{T} \quad &\text{gdw.} \quad [\![F]\!]_{\sigma,\xi} = \mathrm{F} \\
[\![F \wedge G]\!]_{\sigma,\xi} = \mathrm{T} \quad &\text{gdw.} \quad [\![F]\!]_{\sigma,\xi} = \mathrm{T} \text{ und } [\![G]\!]_{\sigma,\xi} = \mathrm{T}
\end{aligned}
$$

Dabei bezeichnet $\sigma[n..]$ den Suffix $s_n s_{n+1} \ldots$ von σ.

Abkürzende Schreibweisen für temporale Formeln

- Ist F temporale Formel, so steht $\Diamond F$ ("eventually F", "finally F") für die Formel

$$\Diamond F \quad \equiv \quad \neg\, \Box \neg\, F$$

  Es ist $[\![\Diamond F]\!]_{\sigma,\xi} = \mathrm{T}$ gdw. $[\![F]\!]_{\sigma[n..],\xi} = \mathrm{T}$ für ein $n \in \mathbb{N}$.

- Analog schreiben wir

$$\Diamond \langle A \rangle_{t_1,\ldots,t_m} \quad \equiv \quad \neg\, \Box [\neg\, A]_{t_1,\ldots,t_m}$$

  Die Zustandsfolge σ erfüllt $\Diamond \langle A \rangle_t$, wenn mindestens ein Paar aufeinanderfolgender Zustände die Formel A erfüllt und t verändert.

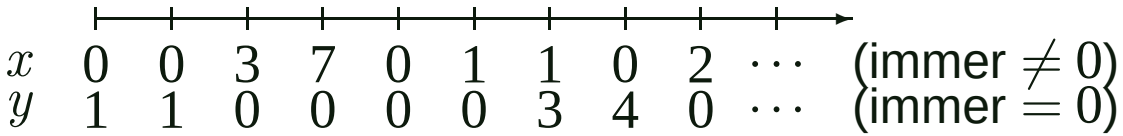
- Für temporale Formeln F, G definieren wir $F \rightsquigarrow G$ ("F leadsto G") durch

$$F \rightsquigarrow G \quad \equiv \quad \Box(F \Rightarrow \Diamond G)$$

  Die Formel $F \rightsquigarrow G$ ist wahr in σ, wenn für jeden Suffix $\sigma[n..]$, der F erfüllt, ein Suffix $\sigma[m..]$ mit $m \geq n$ existiert, der G erfüllt.

- Klammerersparnis: $\Box$ und $\Diamond$ binden stärker als binäre aussagenlogische Operatoren. Z.B. steht $\Box F \wedge \Diamond G$ für $(\Box F) \wedge (\Diamond G)$.

Example (Semantik temporaler Formeln):



Welche der folgenden Formeln gelten in diesem Ablauf?

$\Box\neg\,(x = 0 \wedge y = 0)$

$\Box[x = 0 \Rightarrow y' = 0]_{x,y}$

$\Diamond(x = 7 \wedge y = 0)$

$\Diamond\langle y = 0 \wedge x' = 0\rangle_y$

$\Box\Diamond(y \neq 0)$

$\Diamond\Box(x = 0 \Rightarrow y \neq 0)$

$\Diamond\Box[\mathbf{false}]_y$

“Unendlich oft” und “irgendwann immer”

Es gilt: $[\![\Box\Diamond F]\!]_{\sigma,\xi} = \mathrm{T}$ gdw. für alle $m \in \mathbb{N}$ gibt es $n \geq m$ mit $[\![F]\!]_{\sigma[n..],\xi} = \mathrm{T}$.
Die Formel $\Box\Diamond F$ fordert also, dass F in der Zustandsfolge σ unendlich oft gilt.

Analog verlangt die Formel $\Box\Diamond\langle A\rangle_t$, dass die Aktion $\langle A\rangle_t$ unendlich oft ausgeführt wird.

Dagegen ist $[\![\Diamond\Box F]\!]_{\sigma,\xi} = \mathrm{T}$ gdw. ein $m \in \mathbb{N}$ existiert, so dass für alle $n \geq m$ gilt: $[\![F]\!]_{\sigma[n..],\xi} = \mathrm{T}$.
Die Formel $\Diamond\Box F$ fordert also, dass F in σ ab einem gewissen Zeitpunkt immer gilt.

Analog verlangt die Formel $\Diamond\Box[A]_t$, dass schließlich nur noch die Aktion $[A]_t$ stattfindet.

Für eine erfüllbare Zustandsformel P sind $\Box\Diamond P$ und $\Diamond\Box P$ Lebendigkeitseigenschaften.

Umformungsregeln: Es gelten

$$\neg\,\Box\Diamond F \Leftrightarrow \Diamond\Box\neg\, F \qquad \Diamond\Box\Diamond F \Leftrightarrow \Box\Diamond F$$
$$\neg\,\Diamond\Box F \Leftrightarrow \Box\Diamond\neg\, F \qquad \Box\Diamond\Box F \Leftrightarrow \Diamond\Box F$$

Fairness in TLA

Im Abschnitt über Fainess hatten wir definiert:

- Ein Ablauf ist schwach fair bezüglich A, falls gilt: Ist A ab einem gewissen Zeitpunkt immer ausführbar,
  so wird A unendlich oft ausgeführt.
- Ein Ablauf ist stark fair bezüglich A, falls gilt: Ist A unendlich oft ausführbar, so wird A unendlich oft ausgeführt.

Für Aktionen der Form $\langle A \rangle_t$ können wir dies durch TLA-Formeln ausdrücken:

$$\begin{aligned} \mathrm{WF}_t(A) &\equiv \Diamond\Box\,\mathsf{ENABLED}\langle A\rangle_t \Rightarrow \Box\Diamond\langle A\rangle_t \\ \mathrm{SF}_t(A) &\equiv \Box\Diamond\,\mathsf{ENABLED}\langle A\rangle_t \Rightarrow \Box\Diamond\langle A\rangle_t \end{aligned}$$

Äquivalente Formulierungen sind:

$$\mathrm{WF}_t(A) \equiv \Box\Diamond\neg\,\mathsf{ENABLED}\langle A\rangle_t \vee \Box\Diamond\langle A\rangle_t \qquad \mathrm{SF}_t(A) \equiv \Diamond\Box\neg\,\mathsf{ENABLED}\langle A\rangle_t \vee \Box\Diamond\langle A\rangle_t$$

$$\mathrm{WF}_t(A) \equiv \Box\Diamond(\mathsf{ENABLED}\langle A\rangle_t \Rightarrow \Diamond\langle A\rangle_t) \qquad \mathrm{SF}_t(A) \equiv \Diamond\Box(\mathsf{ENABLED}\langle A\rangle_t \Rightarrow \Diamond\langle A\rangle_t)$$