Temporallogik

Ablaufverhalten von Programmen

- Programmabläufe: **Lineare Sequenzen** von
  - Programmzuständen
  - Ereignissen
  - Beobachtungen
- **Potentiell endlos**
  - Interaktive Programme (z.B. GUI-Anwendungen, Server)
  - Allgemein: Systeme ohne Terminierungsgarantie

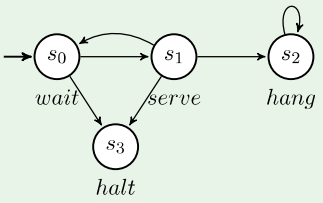
Temporallogik (Forts.)

Endliche Abläufe

- endliche Pfade $u \in S^*$, z. B. $s_0 s_1 s_0 s_1 s_3$
- Beschriftung: endliche Wörter, z.B. $\lambda(u) = wait\ serve\ wait\ serve\ halt \in \Sigma^*$

Beispiel (Transitionssystem T)

$T = (S, \to, \lambda)$ über $\Sigma = \{wait, serve, halt, hang\}$:



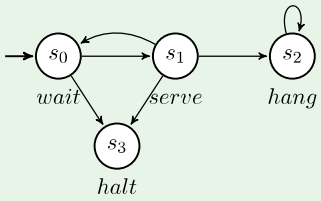
Temporallogik (Forts.)

Unendliche Abläufe

- unendliche Pfade, z. B. $s_0 s_1 s_0 s_1 s_0 s_1 \ldots$
- Beschriftung: unendliche Wörter, z. B. $w = wait\ serve\ wait\ serve\ wait\ serve\ \ldots$

Beispiel (Transitionssystem T)

$T = (S, \to, \lambda)$ über $\Sigma = \{wait, serve, halt, hang\}$:



Temporallogik (Forts.)

Unendliche Sequenzen

- A^ω beschreibt die Menge unendlicher Sequenzen aus Elementen der Menge A
- u^ω bezeichnet die unendliche Wiederholung einer endlichen Sequenz $u \in A^*$
- Beispiel: $(wait\ serve)^\omega$ ist die unendliche Sequenz $wait\ serve\ wait\ serve\ wait\ serve\ \ldots \in \Sigma^\omega$
- Begriffe: „ω-Wörter“ (Elemente $w \in \Sigma^\omega$) und „ω-Sprachen“ (Teilmengen $L \subseteq \Sigma^\omega$)

(Hintergrund: ω bezeichnet üblicherweise die kleinste nicht endliche Größe, z.B. bei Ordinalzahlen)

Temporallogik (Forts.)

Temporale Eigenschaften

Spezifizieren „zeitlicher“ Zusammenhänge, z.B:

- *davor, danach, als nächstes, irgendwann, nie, immer ...*
- Iteratoren: *„Direkt vor Aufruf der Methode* `next()`*, wird stets die Methode* `hasNext()` *benutzt.“*
- Programmzustände: *„Ein mit* `fail` *beschrifteter Zustand wird nie durchlaufen.“*
- *„Solange die Verbindung nicht geschlossen wird, erfolgt immer wieder eine Synchronisation.“*

Temporallogik (Forts.)

Mathematische Logiken:

- unmissverständliche Aussagen
- „Bedeutung“ klar definiert
- gut untersuchte Eigenschaften
- automatische Analysen

Temporallogik (Forts.)

Prädikatenlogik

„Ein mit `fail` beschrifteter Zustand wird nie durchlaufen."

- $\neg \exists i : Fail(i)$
- Universum U: Positionen in einem Wort w
- Prädikat $Fail \subseteq U$: Menge der Positionen in einem Wort w, die mit `fail` beschriftet sind
- Modelle: Wörter
- Modell für diese Formel: $w = wait\ serve\ halt$
- kein Modell: $w = wait\ serve\ wait\ serve\ fail\ serve\ wait$

Temporallogik (Forts.)

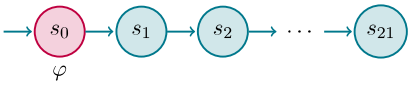
LTL: Linear-time temporal logic

- Formalismus zum (möglichst intuitiven) spezifizieren zeitlicher Zusammenhänge
- Aussagen werden über Wörtern (z.B. den Läufen eines Systems) ausgewertet

Temporallogik (Forts.)

Formel: φ

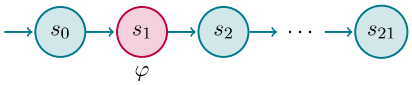
Die Formel φ hält für eine Ausführung, wenn φ in dem ersten Zustand s_0 der Ausführung hält.



Temporallogik (Forts.)

Next: $\mathcal{X}\,\varphi$

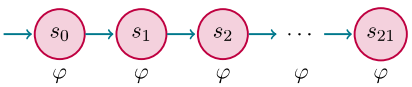
Die Formel $\mathcal{X}\,\varphi$ hält in dem Zustand s_i, wenn φ in dem Zustand s_{i+1} hält.



Temporallogik (Forts.)

Globally: $\mathcal{G}\,\varphi$

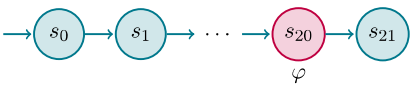
Die Formel $\mathcal{G}\,\varphi$ hält in dem Zustand s_i, wenn φ in allen Zuständen s_j für $j \geq i$ hält.



Temporallogik (Forts.)

Finally: $\mathcal{F}\,\varphi$

Die Formel $\mathcal{F}\,\varphi$ hält in dem Zustand s_i, wenn es einen Zustand s_j für $j \geq i$ gibt, in dem φ hält.



Temporallogik (Forts.)

Until: $\varphi \mathcal{U} \psi$

Die Formel $\varphi \mathcal{U} \psi$ hält in dem Zustand s_i, wenn es einen Zustand s_j für $j \geq i$ gibt, in dem ψ hält und φ in allen Zuständen s_k für $i \leq k < j$ hält.

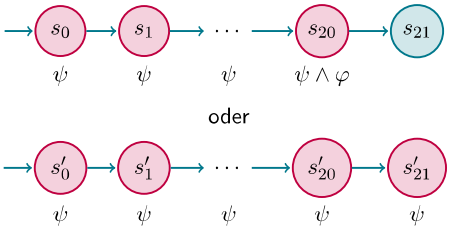
Achtung: Es muss nicht unbedingt einen Zustand geben, in dem φ hält.

Temporallogik (Forts.)

Release: $\varphi \mathcal{R} \psi$

Die Formel $\varphi \mathcal{R} \psi$ hält in dem Zustand s_i, wenn es einen Zustand s_j für $j \geq i$ gibt, in dem φ hält und ψ in allen Zuständen s_k für $i \leq k \leq j$ hält.

Wenn es keinen solchen Zustand s_j gibt, dann hält $\varphi \mathcal{R} \psi$, wenn ψ in allen Zuständen s_k für $k \geq i$ hält.

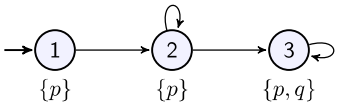


Temporallogik (Forts.)

Propositionen in Transitionssystemen

Transitionssystem $T = (S, \rightarrow, s_1, \lambda)$ über $\Sigma = 2^{AP}$ mit:

- $AP = \{p, q\}$,
- $S = \{s_1, s_2, s_3\}$,
- $\rightarrow = \{(s_1, s_2), (s_2, s_2), (s_2, s_3), (s_3, s_3)\}$,
- $\lambda : \{s_1 \mapsto \{p\}, s_2 \mapsto \{p\}, s_3 \mapsto \{p, q\}\}$



Gibt es einen Pfad in T, auf dem niemals q gilt?

Temporallogik (Forts.)

Für ein ω-Wort $w = w_0 w_1 ... \in \Sigma^\omega$ ($w_i \in \Sigma$) ist die Modell-Relation $\models$ induktiv definiert:

$w \models$ True		
$w \models p$	falls	$p \in w_0$
$w \models \varphi_1 \vee \varphi_2$	falls	$w \models \varphi_1$ oder $w \models \varphi_2$
$w \models \neg\varphi$	falls	nicht $w \models \varphi$
$w \models \mathcal{X} \varphi$	falls	$w^{(1)} \models \varphi$
$w \models \varphi_1 \ \mathcal{U} \varphi_2$	falls	$\exists_i : w^{(i)} \models \varphi_2$ und $\forall_{j, 0 \leq j < i} : w^{(j)} \models \varphi_1$

Dabei bezeichnet $w^{(n)}$ das Suffix $w_n w_{n+1} w_{n+2} ...$ von w ab der Position n.

Temporallogik (Forts.)

Alle weiteren Operatoren können wie folgt als syntaktische Abkürzungen betrachtet werden:

$\varphi_1 \wedge \varphi_2$	$:\equiv$	$\neg(\neg\varphi_1 \vee \neg\varphi_2)$	
$\varphi_1 \rightarrow \varphi_2$	$:\equiv$	$\neg\varphi_1 \vee \varphi_2$	
$\varphi_1 \leftrightarrow \varphi_2$	$:\equiv$	$(\varphi_1 \rightarrow \varphi_2) \wedge (\varphi_2 \rightarrow \varphi_1)$	
$\mathcal{F} \varphi$	$:\equiv$	True $\mathcal{U} \varphi$	„finally φ“
$\mathcal{G} \varphi$	$:\equiv$	$\neg \mathcal{F} \neg\varphi$	„globally φ“
$\varphi_1 \ \mathcal{R} \varphi_2$	$:\equiv$	$\neg(\neg\varphi_1 \ \mathcal{U} \neg\varphi_2)$	„φ_1 releases φ_2“

Temporallogik (Forts.)

Praktische Beispiele

In den folgenden Beispielen betrachten wir diese Bereiche:

- **immer:** alle Zustände
- **vor ψ:** alle Zustände vor dem ersten in dem ψ hält (wenn es einen solchen Zustand gibt)
- **nach ψ:** alle Zustände nach dem ersten (inkl.) in dem ψ hält (wenn es einen solchen Zustand gibt)

Temporallogik (Forts.)

Beispiel (Abwesenheit)

Die Formel φ hält

immer: $\mathcal{G}\,\neg\,\varphi$

vor ψ**:** $(\mathcal{F}\,\psi)\rightarrow(\neg\,\varphi\,\mathcal{U}\,\psi)$

nach ψ**:** $\mathcal{G}(\psi\rightarrow(\mathcal{G}\,\neg\,\varphi))$

nicht

Temporallogik (Forts.)

Beispiel (Existenz)

Die Formel φ hält in der Zukunft

immer: $\mathcal{F}\,\varphi$

vor ψ**:** $\mathcal{G}\,\neg\,\psi\vee\neg\,\psi\,\mathcal{U}(\varphi\wedge\neg\,\psi)$

nach ψ**:** $\mathcal{G}\,\neg\,\psi\vee\mathcal{F}(\psi\wedge\mathcal{F}\,\varphi)$

Temporallogik (Forts.)

Beispiel (Universalität)

Die Formel φ hält

immer: $\mathcal{G}\,\varphi$

vor ψ**:** $(\mathcal{F}\,\psi)\rightarrow(\varphi\,\mathcal{U}\,\psi)$

nach ψ**:** $\mathcal{G}(\psi\rightarrow\mathcal{G}\,\varphi)$