Ludwig-Maximilians-Universität München **SoSe 2015**
Institut für Informatik
Dr. M. Hölzl, C. Kroiß

Formale Techniken der Software-Entwicklung

Übungsblatt 9

Besprechung am 03.07.2015

Musterlösung

Aufgabe 1:

Gegeben sei das Transitionssystem $\mathcal{M}$ in Abbildung 1.

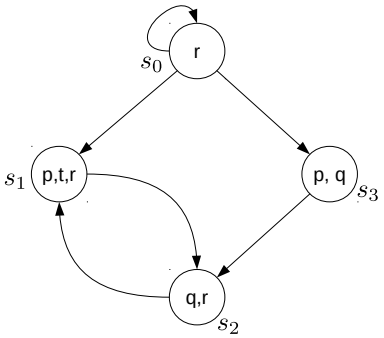
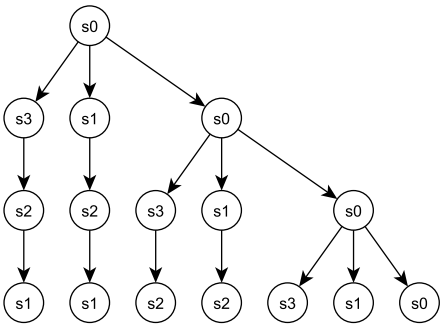


Abbildung 1: Transitionssystem

(a) Zeichnen Sie, beginnend bei Zustand s_0, die entfalteten *Ablauf-Pfade* des Transitionssystems $\mathcal{M}$ bis zu einer Pfadlänge von 4.

Lösung:



(b) Entscheiden Sie für die folgenden CTL- bzw. LTL-Formeln ϕ_1 bis ϕ_n, ob $\mathcal{M}, s_0 \models \phi_i$ und $\mathcal{M}, s_2 \models \phi_i$ gilt und begründen Sie Ihre Antwort.

(i) $\phi_1 := \neg p \implies r$
(ii) $\phi_2 := \mathbf{F}\, t$
(iii) $\phi_3 := \neg\, \mathbf{E}\, \mathbf{G}\, r$
(iv) $\phi_4 := \mathbf{E}(t\, \mathbf{U}\, q)$
(v) $\phi_5 := \mathbf{F}\, q$
(vi) $\phi_6 := \mathbf{E}\, \mathbf{F}\, q$
(vii) $\phi_7 := \mathbf{E}\, \mathbf{G}\, r$
(viii) $\phi_8 := \mathbf{G}(r \vee q)$

Lösung:

(i) ϕ_1 gilt in s_0 und s_2 weil in beiden r gilt.

(ii) ϕ_2 gilt nicht in s_0 weil es die Möglichkeit einer Endlosschleife gibt. ϕ_2 gilt in s_2, weil die Transition nach s_1 erfolgen muss.

(iii) ϕ_3 gilt weder in s_0 noch in s_2 weil von beiden aus einen Pfad gibt, auf dem immer r gilt.

(iv) ϕ_4 gilt weder in s_0 noch in s_2 weil t in beiden Zuständen nicht gilt.

(v) ϕ_5 gilt nicht in s_0 aber in s_2, siehe ii)

(vi) ϕ_6 gilt in s_0 und in s_2 weil von s_0 aus s_3 erreichbar ist und q sowieso in s_2 gilt.

(vii) ϕ_7 gilt in s_0 wegen der Endlosschleife und in s_2 weil r sowohl in s_2 als auch in s_1 gilt.

(viii) ϕ_8 gilt in in s_0 und in s_2.

Aufgabe 2:

Drücken Sie die folgenden Eigenschaften falls möglich in CTL und LTL aus. Wenn die Eigenschaft weder in CTL noch in LTL ausdrückbar ist, versuchen Sie es mit CTL*.

(a) Immer wenn auf p nach einer endlichen Anzahl von Schritten q folgt, dann tritt das System in eine Phase ein, während der kein r eintritt bevor schließlich t gilt.

Lösung:
CTL: $\mathbf{A}\, \mathbf{G}(p \implies \mathbf{A}\, \mathbf{X}\, \mathbf{A}\, \mathbf{G}(\neg q \vee \mathbf{A}[\neg r\, \mathbf{U}\, t]))$
LTL: $\mathbf{G}(p \implies \mathbf{X}\, \mathbf{G}(\neg q \vee \neg r\, \mathbf{U}\, t))$

(b) Ereignis p geht in allen Ablaufpfaden sowohl s als auch t voraus. **Hinweis:** Es kann hilfreich sein, zunächst die Negation dieser Eigenschaft zu formulieren.

Lösung:
CTL: $\neg(\mathbf{E}\,\neg p\,\mathbf{U}(s \vee t)) \equiv \mathbf{A}\,\neg(\neg p\,\mathbf{U}(s \vee t)) \equiv \mathbf{A}\,p\,\mathbf{R}\,\neg(s \vee t)$
LTL: $p\,\mathbf{R}\,\neg(s \vee t)$
Hierbei wurde die Äquivalenz $\neg(\phi\,\mathbf{U}\,\psi) \equiv \neg\phi\,\mathbf{R}\,\neg\psi$ verwendet.

(c) Für alle Ausführungspfade gilt: Nach p ist q niemals wahr.

Lösung:
LTL: $\mathbf{G}(p \implies \mathbf{G}\,\neg q)$
CTL: $\mathbf{A}\,\mathbf{G}(p \implies \mathbf{A}\,\mathbf{G}\,\neg q)$

(d) Zwischen den Ereignissen q und r is p niemals wahr.

Lösung:
LTL: $\mathbf{G}\,q \implies ((\neg p\,\mathbf{U}\,r) \vee \mathbf{G}\,\neg r)$

(e) Transitionen zu Zuständen, in denen p wahr ist, treten höchstens zweimal auf.

Lösung:
$\mathbf{G}((\neg p \wedge \mathbf{X}\,p) \implies \mathbf{G}((\neg p \wedge \mathbf{X}\,p) \implies \mathbf{G}\,\neg(p \wedge \mathbf{X}\,p)))$

(f) Es gibt einen Ausführungspfad, auf dem p in jedem zweiten Zustand wahr ist.

Lösung:
Wenn an die Aussage so versteht, dass p **genau** in jedem 2. Zustand wahr sein soll und annimmt, dass man mit dem 2. Schritt ausgehend vom Anfangszustand anfängt:
CTL*: $\mathbf{E}\,\neg p \wedge \mathbf{G}((\neg p \implies \mathbf{X}\,p) \wedge (p \implies \mathbf{X}\,\neg p))$