FGI-2 – Formale Grundlagen der Informatik II

Modellierung und Analyse von Informatiksystemen

Musterlösung 4: LTL

Präsenzteil am 4./5. 11. – Abgabe am 11./12. 11. 2013

Präsenzaufgabe 4.1:

1. Betrachte das TS aus Abb. 2.8. Betrachte die ω-Sprache $L = y^\omega$ mit $y = (s_0 s_1 s_2 s_4)$. Gib die Ettikettensprache $E_S(L)$ an!

   Lösung: $E_S(L) = z^\omega$ mit $z = (\{\}\ \{\alpha_1\}\ \{\alpha_1, \alpha_2\}\ \{\})$

2. Betrachte das TS aus Abb. 2.8. Definiere die Aussagen α_4 = „In der Tasse ist Tee.“ und α_5 = „In der Tasse ist Kaffee.“. Modifiziere das TS so, dass diese beiden Aussagen sinnvoll integriert werden. Gib eine LTL-Formel an, die Folgendes beschreibt: Immer, wenn Kaffee ausgewählt wurde, befindet sich kurz danach auch Kaffee in der Tasse (und nicht etwa Tee!).

   Lösung: Zwischen s_4 und s_0 wird ein weiterer Zustand s_6 eingefügt, der über die Aktionen „Tee einfüllen“ erreicht und über eine neue Aktionen „Tasse entnehmen“ verlassen werden kann. Analog wird zwischen s_5 und s_0 ein Zustand s_7 eingefügt, der die Kaffee-Entnahme modelliert. Mit $E_S(s_6) = \{\alpha_4\}$ und $E_S(s_7) = \{\alpha_5\}$ sind die beiden Aussagen integriert.

   Zwei verschiedene Interpretationen der Aufgabenstellung könnten als LTL-Formeln folgendermaßen aussehen:

   $\square(\alpha_3 \implies (\neg\alpha_4\ \mathbf{U}\ \alpha_5))$ betont die Bedingung, dass zwischen dem Wählen von Kaffee und dem In-der-Tasse-Befinden des Kaffees sich auf keinen Fall Tee in der Tasse befinden darf.

   $\square(\alpha_3 \implies \circ\circ\alpha_5)$ betont das *kurz danach*, indem genau zwei Zustände später der Kaffee in der Tasse sein muss.

3. Sei $AP = \{\alpha_1, \alpha_2, \alpha_3\}$. Geben Sie die Menge $L^\omega(f)$ (vgl. Def. 3.3) für folgende LTL-Formeln an! (Beachten Sie, dass die Sprache $L^\omega(f)$ völlig unabhängig vom TS aus Abb. 2.8 ist.)

   (a) $f = \square\alpha_2$
   (b) $f = \diamond(\alpha_1 \wedge \circ\neg\alpha_2)$

   Sie können dabei die folgenden Mengen verwenden ($\alpha \in AP$ und $A \subseteq AP$):

   $$\begin{aligned} \text{Obermengen}(A) &:= \{X \subseteq AP \mid A \subseteq X\} \\ \text{Obermengen}(\alpha) &:= \text{Obermengen}(\{\alpha\}) \\ \text{Obermengen}(\neg\alpha) &:= \{X \subseteq AP \mid \alpha \notin X\} \end{aligned}$$

   Rechnen Sie die Mengen für die konkreten, von Ihnen benötigten α_i aus.

   Lösung: $L^\omega(f)$ ist hier eine unendliche Folgensprache über den logischen Atomen AP, d.h. eine Teilmenge von $\mathcal{P}(AP)^\omega$.

   (a) Es ist $L^\omega(\square\alpha_2) = \text{Obermengen}(\alpha_2)^\omega = (\{\{\alpha_2\}, \{\alpha_2, \alpha_1\}, \{\alpha_2, \alpha_3\}, \{\alpha_2, \alpha_1, \alpha_3\}\})^\omega$. (Der Lösungsansatz steht auch auf der letzten Vorlesungsfolie des LTL-Abschnitts.)
   (b) Es ist $L^\omega(\diamond(\alpha_1 \wedge \circ\neg\alpha_2)) = \mathcal{P}(AP)^* \cdot \text{Obermengen}(\alpha_1) \cdot \text{Obermengen}(\neg\alpha_2) \cdot \mathcal{P}(AP)^\omega$
   $= (\{\{\}, \{\alpha_1\}, \{\alpha_2\}, \{\alpha_3\}, \{\alpha_1, \alpha_2\}, \{\alpha_1, \alpha_3\}, \{\alpha_2, \alpha_3\}, \{\alpha_1, \alpha_2, \alpha_3\}\})^*$
   $\cdot\{\{\alpha_1\}, \{\alpha_1, \alpha_2\}, \{\alpha_1, \alpha_3\}, \{\alpha_1, \alpha_2, \alpha_3\}\} \cdot \{\{\}, \{\alpha_1\}, \{\alpha_3\}, \{\alpha_1, \alpha_3\}\}$
   $\cdot(\{\{\}, \{\alpha_1\}, \{\alpha_2\}, \{\alpha_3\}, \{\alpha_1, \alpha_2\}, \{\alpha_1, \alpha_3\}, \{\alpha_2, \alpha_3\}, \{\alpha_1, \alpha_2, \alpha_3\}\})^\omega$

Präsenzaufgabe 4.2: Beweisen Sie die Äquivalenzen in LTL:

$$\begin{array}{rcl} \mathbf{F}f & \equiv & \mathit{True}\,\mathbf{U}f \\ \mathbf{G}f & \equiv & \neg(\mathbf{F}\neg f) \end{array}$$

Lösung: Mit Definition 3.3 (S. 35) gilt:

$$\begin{array}{lll} & \alpha \models \mathbf{F}f & \text{Def. 3.3.8} \\ \Leftrightarrow & \exists k \geq 0 : \alpha^k \models f & g \equiv (g \wedge \top) \\ \Leftrightarrow & \exists k \geq 0 : ((\alpha^k \models f) \wedge \top) & \top \equiv (\forall 0 \leq j < k : \alpha^j \models \top) \\ \Leftrightarrow & \exists k \geq 0 : ((\alpha^k \models f) \wedge (\forall 0 \leq j < k : \alpha^j \models \top)) & \text{Def. 3.3.10} \\ \Leftrightarrow & \alpha \models \top \mathbf{U} f & \end{array}$$

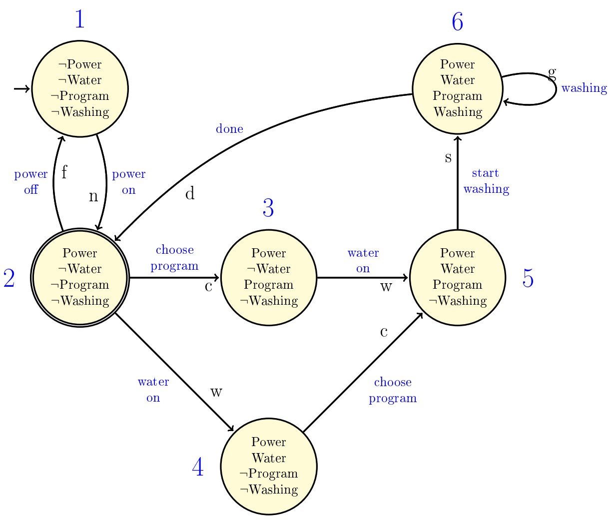
und:

$$\begin{array}{lll} & \alpha \models \mathbf{G}f & \text{Def. 3.3.9} \\ \Leftrightarrow & \forall k \geq 0 : \alpha^k \models f & g \equiv \neg\neg g \\ \Leftrightarrow & \neg\neg(\forall k \geq 0 : \alpha^k \models f) & \neg\forall g \equiv \exists \neg g \\ \Leftrightarrow & \neg(\exists k \geq 0 : \alpha^k \not\models f) & \text{Def. 3.3.4} \\ \Leftrightarrow & \neg(\exists k \geq 0 : \alpha^k \models \neg f) & \text{Def. 3.3.8} \\ \Leftrightarrow & \alpha \not\models \mathbf{F}\neg f & \text{Def. 3.3.4} \\ \Leftrightarrow & \alpha \models \neg \mathbf{F} \neg f & \end{array}$$

Beachten Sie, dass einige der auf der rechten Seite angegebenen benutzten Äquivalenzen sich nicht auf die LTL Formel beziehen, sondern sozusagen auf die Metaebene. So bezieht sich bspw. die im zweiten Schritt bei der zweiten Formel benutzte Äquivalenz $g \equiv \neg\neg g$ darauf, dass die ganze Formel $\forall k \geq 0 : \alpha^k \models f$ wahr oder falsch sein kann und somit als aussagenlogische Formel interpretiert werden kann. Für diese gilt dann die Äquivalenz.

Übungsaufgabe 4.3: Betrachten Sie die Kripkestruktur $TS_{Waschmaschine}$, welches eine Systembeschreibung einer Waschmaschine darstellt. Die Transitionsbezeichner und negierten Aussagen in den Etiketten sind optional und dienen nur der Verdeutlichung.

von
6



$TS_{Waschmaschine}$

1. Betrachten Sie $TS_{Waschmaschine}$ ohne Etiketten als Büchi-Automat mit 2 als einzigem Endzustand und Alphabet $\Sigma = \{c, d, f, g, n, s, w\}$. Geben Sie die Mengen $L(TS_{Waschmaschine})$ bzw. $L^\omega(TS_{Waschmaschine})$ als regulären bzw. ω-regulären Ausdruck an. Hinweis: Wie oft,

kann es hilfreich sein, zuerst einen Pfad vom Anfangs- zum Endzustand zu betrachten und dann alle möglichen Zyklen anzufügen.

Lösung: $L(TS_{Waschmaschine}) = n(fn + (cw + wc)sg^*d)^*$ und
$L^\omega(TS_{Waschmaschine}) = n(fn + (cw + wc)sg^*d)^\omega$

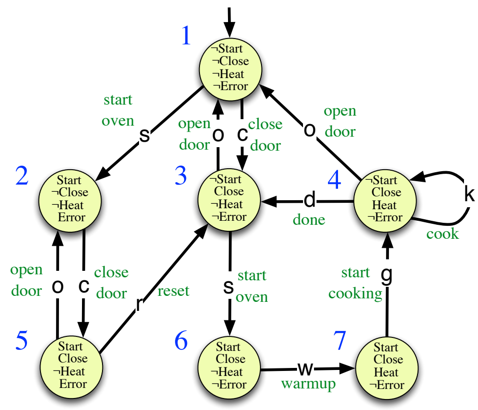
2. Betrachten Sie $TS_{Waschmaschine}$ mit Etiketten als Kripke-Struktur M. Bestimmen Sie die Menge $SS(M)$ aller Pfade (Def. 2.18) als ω-regulären Ausdruck. Das Alphabet dieses Ausdrucks ist also $\{1, 2, 3, 4, 5, 6\}$.

   Lösung: $SS(M) = 12(12 + (3 + 4)56^+2)^\omega$

3. Bestimmen Sie die Etikettensprache $E_S(SS(M))$ (Def. 2.18) als ω-regulären Ausdruck. Das Alphabet dieses Ausdrucks besteht also aus den Etiketten der Zustände. Da alle Zustände verschiedene Etikette haben, können Sie abkürzend die Zustandsbezeichner als Bezeichner der Etikette wählen.

   Lösung: $E_S(SS(M)) = SS(M)$, da alle Zustände verschiedene Etikette haben.

4. Betrachten Sie jetzt die vollständige Kripkestruktur M_{ofen} des Mikrowellen-Ofens:



M_{ofen}

   Für eine Formel α sei $Sat(\alpha)$ die Menge der Zustände, in denen α gilt. Bestimmen Sie $Sat(Start \wedge Error)$ sowie $Sat(Heat)$. Prüfen Sie dann, ob die LTL-Formel

$$\mathbf{GF}(Start \wedge Error \;\Rightarrow\; \mathbf{F}Heat)$$

   im Anfangszustend 1 gilt und beweisen Sie Ihre Behauptung, d.h. entweder die Gültigkeit beweisen oder eine Rechnung als Gegenbeispiel angeben.

   Lösung: $Sat(Start \wedge Error) = \{2, 5\}$ und $Sat(Heat) = \{4, 7\}$. Die LTL-Formel gilt nicht im Anfangszustand 1. Wenn M_{ofen} im Zustand 2 oder 5 ist, ist die Prämisse der Implikation erfüllt. Damit aber auch die Konklusion erfüllt wird, müsste später auch Zustand 4 oder 7 eingenommen werden. Dies ist aber für den Pfad $\pi = 1(25)^\omega$ nicht der Fall. Und da $\pi \in SS(M_{ofen})$ gilt, gilt die Formel nicht im Anfangszustand 1.

5. Prüfen Sie ebenso, ob die LTL-Formel

$$f = \mathbf{FG}(Error \wedge Start)$$

   im Anfangszustend 1 gilt und beweisen Sie Ihre Behauptung, d.h. entweder die Gültigkeit beweisen oder eine Rechnung als Gegenbeispiel angeben. Geben Sie zudem einen Pfad π an, für den diese Formel gilt, d.h. für den $M_{ofen}, \pi \models f$ gilt.

Lösung: Die Formel gilt nicht, da immer Zyklen im rechten Teil durchlaufen werden können, auf denen es keinen Zustand gibt, der sowohl $Start$ als auch $Error$ erfüllt. Ein Gegenbeispiel ist also die Folge in der Menge $(13674)^\omega$ oder $1(3674)^\omega$. Die Formel f kann nur von Pfaden erfüllt werden, die sich auf den Zyklus im linken Teil beschränken, da nur in Zustand 2 und 5 $(Error \wedge Start)$ gilt. Damit π also die Formel f erfüllen kann, muss der Pfad demnach mit $(25)^\omega$ enden. So gilt zum Beispiel $M_{ofen}, \pi \models f$ für $\pi = 1(25)^\omega$.

Übungsaufgabe 4.4: Betrachten Sie die Kripkestruktur M_{ofen} aus Aufgabe 4.3. und den unendlichen Zustandspfad $\pi = s_0 s_{i_1} s_{i_2} \ldots$ aus der Menge $13(125253)^\omega$.

von
6

Geben Sie an, ob für die folgenden LTL-Formeln f jeweils $M_{ofen}, \pi \models f$ und allgemeiner $M_{ofen} \models f$ gilt.

Anmerkung: Wie im Skript werden hier die temporalen Operatoren in der Form $\circ, \diamond$ und $\square$ benutzt, da Sie auf beide Formen auch in der Literatur treffen werden.

Lösung:

f	$M_{ofen}, \pi \models f$	$M_{ofen} \models f$
$\circ\neg(Start \wedge Heat)$	Ja	Ja
$\square\neg Start$	Nein	Nein
$\square(Start \Longrightarrow Close)$	Nein	Nein
$\square\diamond(Heat \vee Error \vee \neg Start)$	Ja	Ja
$\diamond((Start \wedge Close \wedge \neg Error)\ \mathbf{U}\ Heat)$	Nein	Nein
$\square((Close \wedge \neg Heat \wedge Start) \Longrightarrow \circ\circ\neg Heat)$	Ja	Nein

Die Richtigkeit der Lösungen in der Spalte $M_{ofen}, \pi \models f$ kann man stets direkt am Pfad π ablesen. Zur Begründung der Spalte $M_{ofen} \models f$:

1. Jeder mögliche Pfad aus dem Startzustand hat als zweiten Zustand entweder die 2 oder 3, beide erfüllen $\neg(Start \wedge Heat)$, somit ist die Formel für jeden Pfad erfüllt.
2. Klar, da schon auf π nicht erfüllt.
3. Klar, da schon auf π nicht erfüllt.
4. Der interessante Zustand ist 6 (in allen anderen ist die Disjunktion ohnehin erfüllt). Wird dieser jedoch auf einem Pfad eingenommen, so muss man nachfolgend in den Zustand 4 gelangen, in dem bspw. $Heat$ gilt. In 6 gilt somit $\diamond(Heat \vee Error \vee \neg Start)$ und damit gilt die angegebene Formel stets.
5. Klar, da schon auf π nicht erfüllt.
6. Die Prämisse $(Close \wedge \neg Heat \wedge Start)$ der Implikation wird nur von den Zuständen 5 und 6 erfüllt, von Interesse sind also nur Pfade, die 5 oder 6 enthalten, da ansonsten die Implikation automatisch erfüllt wird. So erfüllt beispielsweise der Pfad $(13674)^\omega$ die Formel nicht, da der übernächste Zustand von 6 die 4 ist, welcher aber die Konklusion $\neg Heat$ nicht erfüllt.

Bisher erreichbare Punktzahl: 48