Übungen zu Model-Checking

Sommersemester 2008 / Blatt 1

Wir besprechen die Beispiele gemeinsam am 8.5.
Bei Fragen zum Übungsbetrieb oder den Beispielen, schicken Sie mir bitte eine email (`schalla@in.tum.de`).

Beispiel 1.1: Spezifikationen mit LTL

Finden Sie geeignete atomare Propositionen und spezifizieren Sie die untenstehenden Eigenschaften in **LTL**:

a. Der Prozeß wird terminieren.

b. Der Prozeß erfüllt eine bestimmte Invariante.

c. Der Prozeß sendet unendlich viele Nachrichten.

d. Jeder Request wird irgendwann durch ein Acknowledge beantwortet.

e. Nachdem der Prozess terminierte, sendet er keine Nachrichten mehr.

f. Das static initialization fiasco in C++: Vor dem Eintritt in die `main` Routine wird kein Thread erzeugt.

Geben Sie für jede der obigen Eigenschaften jeweils eine erfüllende und nicht-erfüllende Belegungssequenz an. Für welche Eigenschaften brauchen gibt es endliche/unendliche erfüllende/nicht-erfüllende Belegungssequenzen? Wie sehen entsprechende Kripke-Strukturen aus?

Beispiel 1.2: Weitere Temporaloperatoren

In der Vorlesung wurden folgende abkürzende Schreibweisen eingeführt:

- *Globally:* $w \models \mathbf{G}\phi \quad \Leftrightarrow \quad w \models \neg(\mathbf{true}\,\mathbf{U}\,\neg\phi)$
- *Release:* $w \models \phi\,\mathbf{R}\,\psi \quad \Leftrightarrow \quad w \models \neg(\neg\phi\,\mathbf{U}\,\neg\psi)$

Sei nun $\Sigma = 2^{\mathbf{AP}}$ mit $AP \neq \emptyset$, dann schreiben wir ein Wort $w \in \Sigma^\omega$ als $w = w_0 w_1 \ldots$ und definieren das i-te Suffix w^i mit $w^i = w_i w_{i+1} \ldots$ Zeigen Sie damit die folgenden Zusammenhänge:

a. $w \models \mathbf{G}\phi \quad \Leftrightarrow \quad \forall i \in \mathbb{N}\ w^i \models \phi$
b. $w \models \phi\,\mathbf{R}\,\psi \quad \Leftrightarrow \quad \forall i \in \mathbb{N}\ \ (\forall j < i\ \ w^j \not\models \phi) \rightarrow w^i \models \psi$
c. $w \models \neg(\phi\,\mathbf{U}\,\psi) \quad \Leftrightarrow \quad w \models \neg\phi\,\mathbf{R}\,\neg\psi$
d. $w \models \phi\,\mathbf{U}\,\psi \quad \Leftrightarrow \quad w \models \psi \vee (\phi \wedge \mathbf{X}(\phi\,\mathbf{U}\,\psi))$
e. $w \models \phi\,\mathbf{R}\,\psi \quad \Leftrightarrow \quad w \models \mathbf{G}\psi \vee (\psi\,\mathbf{U}\,(\phi \wedge \psi))$

Beispiel 1.3: Positive Normalform

Eine Formel ϕ über den Propositionen $\mathbf{AP}$ ist in *positiver Normalform*, wenn Negationszeichen $\neg$ in ϕ nur direkt vor den Propositionen $a \in \mathbf{AP}$ vorkommen. Zum Beispiel ist $\neg\mathbf{G}a$ nicht in positiver Normalform, wohingegen die äquivalente Formel $\mathbf{true}\,\mathbf{U}\,\neg a$ in positiver Normalform ist.

Wir bezeichnen die Menge der in positiver Normalform angegebenen Formeln über den Operatoren $\mathbf{X}$, $\mathbf{U}$, $\mathbf{G}$, $\wedge$, $\vee$ und $\neg$ als **NF-LTL**.

a. Zeigen Sie mittels Induktion über den Formelaufbau, dass sich jede **LTL**-Formel ϕ eine äquivalente Formel ψ in **NF-LTL** existiert. Nützen Sie dazu die Äquivalenzen aus Aufgabe 1.2.

b. Sei $\mathbf{NF} - \mathbf{LTL}_{-\mathbf{G}}$ die Menge aller **NF-LTL** Formeln, in denen der Operator $\mathbf{G}$ nicht vorkommt. Zeigen Sie für jede beliebige Formel $\phi \in \mathbf{NF} - \mathbf{LTL}_{-\mathbf{G}}$ mittels Induktion über den Formelaufbau, dass für jedes Wort $w = w_0 w_1 \cdots \in \Sigma^\omega$ mit $w \models \phi$ eine Zahl $N_\phi(w) \in \mathbb{N}$ existiert, so dass bereits mit den ersten $N_\phi(w) + 1$ Symbolen $w_0 \dots w_{N_\phi(w)}$ dieses Wortes entschieden werden kann, ob $w \models \phi$ gilt oder nicht. Mit anderen Worten, für jede beliebige Fortsetzung $w' \in \Sigma^\omega$ gilt

$$w \models \phi \;\Leftrightarrow\; w_0 \dots w_{N_\phi(w)} w' \models \phi$$

c. Sei $\mathbf{NF} - \mathbf{LTL}_{-\mathbf{X}}$ die Menge aller **NF-LTL** Formeln, in denen der Operator $\mathbf{X}$ nicht vorkommt. Zeigen Sie, dass eine Formel $\phi \in \mathbf{NF} - \mathbf{LTL}_{-\mathbf{X}}$ nicht zwischen $w = w_0 w_1 \cdots \in \Sigma^\omega$ und $D(w) = w_0 w_0 w_1 w_1 \dots$ unterscheiden kann, das heißt,

$$w \models \phi \;\Leftrightarrow\; D(w) \models \phi$$

gilt für alle $\phi \in \mathbf{NF} - \mathbf{LTL}_{-\mathbf{X}}$ und $w \in \Sigma^\omega$.

1.4: Mehr oder weniger Verhalten?

Seien $K_1 = (S, \to_1, r, \mathbf{AP}, v)$ und $K_2 = (S, \to_2, r, \mathbf{AP}, v)$ zwei Kripke-Strukturen mit denselben Zuständen S, demselben Startzustand r und dergleichen Interpretation v über den Propositionen $\mathbf{AP}$. Wir schreiben nun $K_1 \leq K_2$, wenn die Transitionsrelation $\to_2 \subseteq S \times S$ mehr Verhalten erlaubt als die Transitionsrelation $\to_1 \subseteq S \times S$, das heißt, wenn $\to_1 \subseteq \to_2$ gilt.

Zeigen Sie, dass für $K_1 \leq K_2$ der folgende Zusammenhang für jede **LTL** Formel ϕ gilt:

$$K_2 \models \phi \;\Rightarrow\; K_1 \models \phi$$