

Übungen zu Model Checking

Besprechung am 28.04.05

Aufgabe 1.1

Für $\mathbf{AP} \neq \emptyset$ sei $\Sigma = 2^{\mathbf{AP}}$. Der *Release*-Operator \mathbf{R} ist für zwei **LTL**-Formeln ϕ, ϕ' und $w \in \Sigma^\omega$ durch

$$w \models \phi \mathbf{R} \phi' \stackrel{\text{DEF}}{\iff} \forall i \in \mathbb{N} : \left((\forall j < i : w^j \not\models \phi) \rightarrow w^i \models \phi' \right)$$

definiert. Beweisen Sie formal für beliebiges $w \in \Sigma^\omega$ und beliebige **LTL**-Formeln ϕ, ϕ' die folgenden Aussagen:

- (a) $w \models \neg(\phi \mathbf{U} \phi')$ genau dann, wenn $w \models \neg\phi \mathbf{R} \neg\phi'$
- (b) $w \models \mathbf{G} \phi$ genau dann, wenn $\forall i \in \mathbb{N} : w^i \models \phi$
- (c) $w \models \neg(\phi \mathbf{U} \phi')$ genau dann, wenn $w \models (\mathbf{G} \neg\phi') \vee (\neg\phi' \mathbf{U} (\neg\phi \wedge \neg\phi'))$

Hinweise:

$\mathbf{G} \phi$ ist in der Vorlesung nur als Abkürzung für $\neg(\mathbf{true} \mathbf{U} \neg\phi)$ erklärt worden.

Die Definition der Semantik von \mathbf{U} und \mathbf{R} verwendet „ $\forall j < i$ “. Für $i \in \mathbb{N}$ ist dabei $\forall j < i : \phi$ durch $\forall j \in \mathbb{N} : (j < i \rightarrow \phi)$ definiert. Entsprechend steht $\exists j < i : \phi$ abkürzend für $\exists j \in \mathbb{N} : (j < i \wedge \phi)$.

Aufgabe 1.2

Eine **LTL**-Formel ist in *negierter Normalform*, falls die Negation \neg einzig direkt vor atomaren Propositionen $a \in \mathbf{AP}$ auftritt. Z.B. ist die Formel $\neg a \mathbf{U} \neg b$ in negierter Normalform, jedoch nicht $\neg(a \mathbf{U} b)$.

In der Vorlesung wurden die Formeln $\phi \wedge \psi$ und $\mathbf{G} \phi$ als Abkürzungen von $\neg(\neg\phi \vee \neg\psi)$ bzw. $\neg(\mathbf{true} \mathbf{U} \neg\phi)$ definiert. Diese sind somit für Formeln in negierter Normalform zunächst nicht erklärt.

Hierfür sei die Semantik von $\mathbf{G} \phi$ direkt mittels

$$w \models \mathbf{G} \phi \stackrel{\text{DEF}}{\iff} \forall i \in \mathbb{N} : w^i \models \phi$$

definiert. Entsprechend gelte

$$w \models \phi \wedge \phi' \stackrel{\text{DEF}}{\iff} (w \models \phi) \wedge (w \models \phi').$$

Aus obiger Aufgabe wissen Sie, dass hierdurch die Semantik unverändert bleibt.

Mit **NF-LTL** sei dann die Menge aller **LTL**-Formeln in negierter Normalform bezeichnet, welche einzig die Operatoren $\{\mathbf{X}, \mathbf{U}, \mathbf{G}, \wedge, \vee, \neg\}$ verwenden.

- (a) Zeigen Sie mittels Induktion über den Formelaufbau einer **LTL**-Formel, dass für jede **LTL**-Formel ϕ eine **NF-LTL**-Formel ϕ' mit $\phi \equiv \phi'$ existiert.

- (b) Mit $\text{NF-LTL}_{\mathbf{G}}$ sei die Teilmenge von NF-LTL -Formeln bezeichnet, in welchen der Operator \mathbf{G} *nicht* vorkommt, und sei ϕ eine solche $\text{NF-LTL}_{\mathbf{G}}$ -Formel.

Zeigen Sie mittels Induktion über den Formelaufbau von ϕ , dass es dann für jedes Wort $w \in \Sigma^\omega$ mit $w \models \phi$ ein $N_\phi \in \mathbb{N}$ gibt, so dass auch alle Wörter der Form $w_0 w_1 \dots w_{N_\phi} (2^{\mathbf{AP}})^\omega$ die Formel ϕ erfüllen. D.h., bereits ein *endlicher* Präfix von w entscheidet darüber, ob w die Formel ϕ erfüllt oder nicht.

Geben Sie nun eine NF-LTL -Formel an, für welche keine semantisch äquivalente $\text{NF-LTL}_{\mathbf{G}}$ -Formel existiert.

Aufgabe 1.3

Es sei $\mathbf{AP} \neq \emptyset$ eine endliche Menge von atomaren Propositionen und $\Sigma = 2^{\mathbf{AP}}$. Mit $\Sigma^\infty = \Sigma^* \cup \Sigma^\omega$ wird die Menge der *abzählbaren* Wörter über Σ bezeichnet. Für $w \in \Sigma^\infty$ sei

$$\text{Pos}(w) = \begin{cases} \emptyset & \text{falls } w = \varepsilon \\ \{0, 1, \dots, n\} & \text{falls } w = w_0 w_1 \dots w_n \in \Sigma^+ \quad (w_i \in \Sigma) \\ \mathbb{N} & \text{falls } w = w_0 w_1 \dots \in \Sigma^\omega \quad (w_i \in \Sigma) \end{cases}$$

Hiermit wird die Semantik von LTL -Formeln folgendermaßen auf Wörter $w \in \Sigma^\infty$ ausgedehnt:

$$\begin{aligned} w \models^\infty a & \stackrel{\text{DEF}}{\iff} (0 \in \text{Pos}(w)) \wedge (a \in w_0) & (a \in \mathbf{AP}) \\ w \models^\infty \phi \vee \phi' & \stackrel{\text{DEF}}{\iff} (w \models^\infty \phi) \vee (w \models^\infty \phi') \\ w \models^\infty \neg \phi & \stackrel{\text{DEF}}{\iff} w \not\models^\infty \phi \\ w \models^\infty \mathbf{X} \phi & \stackrel{\text{DEF}}{\iff} (1 \in \text{Pos}(w)) \wedge (w^1 \models^\infty \phi) \\ w \models^\infty \phi \mathbf{U} \phi' & \stackrel{\text{DEF}}{\iff} \exists i \in \text{Pos}(w) : (w^i \models^\infty \phi' \wedge \forall j < i : w^j \models^\infty \phi) \\ w \in \llbracket \phi \rrbracket_\infty & \stackrel{\text{DEF}}{\iff} w \models^\infty \phi \end{aligned}$$

\wedge und \mathbf{G} seien entsprechend dem Skript als Abkürzungen definiert.

- (a) Geben Sie für $\mathbf{AP} = \{a\}$ die Mengen $\llbracket \mathbf{XG} a \rrbracket_\infty$, $\llbracket \mathbf{GX} a \rrbracket_\infty$, $\llbracket \mathbf{GX} a \rrbracket$, $\llbracket \mathbf{XG} a \rrbracket$ an.
- (b) Es sei $a \in \mathbf{AP}$. Geben Sie bezüglich \models^∞ eine LTL -Formel an, welche aussagt, dass a in $w \in \Sigma^\infty$ unendlich oft gilt.

Aufgabe 1.4

Formulieren Sie folgende Sprichwörter in LTL unter Verwendung geeigneter atomarer Propositionen.

- „Nach dem Sturm ist vor dem Sturm.“
- „Ohne Fleiß kein Preis.“
- „Wer A sagt, muss auch B sagen.“
- „Wer im Glashaus sitzt, sollte (darf) nicht mit Steinen werfen.“
- „Der Apfel fällt nicht weit vom Stamm.“
- „Hegel bemerkte irgendwo, dass alle großen weltgeschichtlichen Tatsachen und Personen sich sozusagen zweimal ereignen. Er hat vergessen, hinzuzufügen: das eine Mal als Tragödie, das andere Mal als Farce.“