

Übungen zu Model Checking

Besprechung am 11.05.06

Aufgabe 1.1

In dieser Aufgabe sollen Sie die prädikaten-logischen Definitionen, welche den **LTL**-Operatoren zu Grunde liegen, wiederholen. Weiterhin wird der Release-Operator **R** eingeführt, von dem Sie zeigen werden, dass er als dualer Operator zu **U** aufgefasst werden kann.

Für $\mathbf{AP} \neq \emptyset$ sei $\Sigma = 2^{\mathbf{AP}}$. Wir fassen ein Wort $w \in \Sigma^\omega$ als Abbildung von \mathbb{N} nach Σ auf und schreiben $w(i)$ oder w_i für das i -te Zeichen in w und $w^i = w(i)w(i+1) \dots$ für den i -ten Suffix von w (mit $i = 0, 1, \dots$).

Der Release-Operator **R** ist für zwei **LTL**-Formeln ϕ, ϕ' und $w \in \Sigma^\omega$ dann durch

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

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

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

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 **U** und **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 $\exists j \in \mathbb{N} : (j < i \wedge \phi)$.
- (a)+(b) lassen sich direkt durch Umformen der Formeln herleiten. Bei (c) empfiehlt es sich allerdings eine Fallunterscheidung.

Aufgabe 1.2

In dieser Aufgabe wird die positive Normalform einer **LTL**-Formel eingeführt und darauf aufbauend untersucht, ob einer der Operatoren **U**, **G** oder **X** bezüglich dieser Normalform bereits durch die jeweils anderen beiden ausgedrückt werden kann.

Eine **LTL**-Formel ist in *positiver Normalform*, falls die Negation \neg nur direkt vor atomaren Propositionen $a \in \mathbf{AP}$ auftritt. Z.B. ist die Formel $\neg a \mathbf{U} \neg b$ in positiver 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 positiver Normalform zunächst nicht erklärt.

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

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

definiert. Entsprechend gelte

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

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

Mit **NF-LTL** sei dann die Menge aller **LTL**-Formeln in positiver Normalform bezeichnet (über den Operatoren **X**, **U**, **G**, \wedge , \vee , \neg).

- (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. (Aufgabe 1 nicht vergessen.)
- (b) Mit NF-**LTL** $_{\mathbf{G}}$ sei die Teilmenge von NF-**LTL**-Formeln bezeichnet, in welchen der Operator **G** *nicht* vorkommt, und sei ϕ eine solche 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.

- (c) Entsprechend sei nun NF-**LTL** $_{\mathbf{X}}$ die Menge aller NF-**LTL**-Formeln, in welchen **X** nicht auftritt. Zeigen Sie, dass eine NF-**LTL** $_{\mathbf{X}}$ -Formel ϕ nicht zwischen $w \in \Sigma^\omega$ und $D(w) := w_0 w_0 w_1 w_1 \dots$ unterscheiden kann, d.h., dass $(w \models \phi) \Leftrightarrow (D(w) \models \phi)$ gilt.

Aufgabe 1.3

In der Vorlesung wurde **LTL** nur bezüglich $w \in \Sigma^\omega$ definiert. In dieser Aufgabe werden Sie die Semantik von **LTL**-Formeln auf $\Sigma^\infty = \Sigma^* \cup \Sigma^\omega$ ausdehnen und die daraus entstehenden Unterschiede betrachten.

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. Σ^∞ kann also als eine Menge von sowohl partiellen als auch totalen Abbildungen von \mathbb{N} nach Σ aufgefasst werden. Für $w \in \Sigma^\infty$ sei

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

$Pos : \Sigma^\infty \rightarrow \mathbb{N} \cup \{\mathbb{N}\}$ gibt somit den Definitionsbereich (\sim Länge) einer „Funktion“ $w \in \Sigma^\infty$ wieder zurück. Hiermit wird die Semantik von **LTL**-Formeln folgendermaßen auf Wörter $w \in \Sigma^\infty$ ausgedehnt:

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

(Man mache sich klar, dass diese Definitionen für $w \in \Sigma^\omega$ mit den Definitionen aus der Vorlesung übereinstimmen.)

\wedge und **G** sind wieder durch $\phi \wedge \psi \equiv \neg(\neg\phi \vee \neg\psi)$ bzw. $\mathbf{G} \phi \equiv \neg(\mathbf{true} \mathbf{U} \neg\phi)$ erklärt. Für eine **LTL**-Formel φ sei dann $\llbracket \varphi \rrbracket_\infty$ die Menge $\{w \in \Sigma^\infty \mid w \models^\infty \varphi\}$.

- (a) Geben Sie für $\mathbf{AP} = \{a\}$ die Mengen $\llbracket \mathbf{X} \mathbf{G} a \rrbracket_\infty, \llbracket \mathbf{G} \mathbf{X} a \rrbracket_\infty, \llbracket \mathbf{G} \mathbf{X} a \rrbracket, \llbracket \mathbf{X} \mathbf{G} a \rrbracket$ an. Für eine **LTL**-Formel ist hierbei ist $\llbracket \phi \rrbracket$ die Semantik der Formel im Sinne der Vorlesung, während $\llbracket \phi \rrbracket_\infty$ die erweiterte Semantik ist.
- (b) Es sei $a \in \mathbf{AP}$. Geben Sie eine **LTL**-Formel an, welche bezüglich \models^∞ aussagt, dass a in $w \in \Sigma^\infty$ unendlich oft gilt.

Anmerkung: Man hätte auch $w \models^\infty \mathbf{X} \phi$ durch $(1 \in Pos(w)) \rightarrow (w^1 \models^\infty \phi)$ erklären können. Wäre dann (b) noch lösbar gewesen?