Formale Grundlagen der Informatik 3
Kapitel 6
Automatenbasiertes LTL Model Checking (Teil 2)

Frank Heitmann
heitmann@informatik.uni-hamburg.de

25. Januar 2016

Die Idee

Wie war noch gleich der Plan?!

Sei M ein LTS und ϕ eine LTL Formel.

- Zu $\neg\phi$ (der Negation der Spezifikation!) konstruieren wir einen (Büchi-)Automaten $A_{\neg\phi}$.
- $A_{\neg\phi}$ akzeptiert genau die Wörter w mit $w \models \neg\phi$.
- Bilde den "Produktautomaten" $M \cap A_{\neg\phi}$.
- Prüfe, ob die akzeptierte Sprache von $M \cap A_{\neg\phi}$ leer ist.

Das Vorgehen (Wiederholung)

1. Büchi-Automaten (und drumherum) (erledigt)
2. Eine alternative (aber äquivalente) Semantik für LTL
3. Damit dann die Konstruktion für $A_{\neg\phi}$
4. Den "Produktautomaten" (erledigt, aber ...)
5. Den Leerheitstest (erledigt)

LTL - alternative Definition

Sei $P = \{p_1, p_2, \ldots\}$ eine Menge von atomaren Formeln. Sei

$$\phi ::= p \mid \neg\phi \mid (\phi \vee \phi) \mid X\phi \mid \phi U \phi$$

und als Abkürzungen:

$$\begin{aligned} \phi R \psi &:= \neg(\neg\phi U \neg\psi) \\ F\phi &:= \top U \phi \\ G\phi &:= \neg F \neg\phi \end{aligned}$$

Dabei wird $\phi R \psi$ erfüllt, wenn entweder ψ immer gilt oder ψ bis zu einem Moment gilt, in dem sowohl ϕ als auch ψ gelten.

LTL - alternativ

Definition (LTL - alternativ)

Sei $w = a_0 a_1 \ldots \in (2^P)^\omega$. Die Semantik ist induktiv für alle $i \in \mathbb{N}$ definiert durch:

$w, i \models p$	gdw.	$p \in a_i$
$w, i \models \neg\phi$	gdw.	$w, i \not\models \phi$
$w, i \models \phi_1 \vee \phi_2$	gdw.	$w, i \models \phi_1$ *oder* $w, i \models \phi_2$
$w, i \models X\phi$	gdw.	$w, i+1 \models \phi$
$w, i \models \phi_1 U \phi_2$	gdw.	ein $k \geq i$ existiert mit $w, k \models \phi_2$ und für alle j mit $i \leq j < k$ gilt $w, j \models \phi_1$

Ein Wort entspricht dabei den Labels jener Zustand, die bei einem Lauf durch ein LTS besucht werden.

LTL - alternativ

Definition

Sei $\Sigma = (2^P)$, $v \in \Sigma^\omega$ und ϕ eine LTL-Formel. Es ist $v \models \phi$, falls $v, 0 \models \phi$ und $L(\phi) = \{u \mid u \models \phi\}$. Zwei Formeln ϕ und ψ sind äquivalent, $\phi \equiv \psi$, falls $L(\phi) = L(\psi)$ gilt.

Ist z.B. $P = \{C, D\}$, dann ist $\Sigma = \{\emptyset, \{C\}, \{D\}, \{C, D\}\}$. Will man nun an ein bestimmtes $a \in \Sigma$ herankommen, so kann man *charakteristische Formeln* χ_a verwenden:

$$\chi_a := (\bigwedge_{p \in a} p) \wedge (\bigwedge_{p \notin a} \neg p)$$

Will man z.B. eine Formel für die Sprache, die nur aus dem Wort $(\{C\}\{D\})^\omega$ besteht, so geht dies mit:

$$\chi_C \wedge G((\chi_C \Rightarrow X\chi_D) \wedge (\chi_D \Rightarrow X\chi_C))$$

Normalform

Definition (Positive Normalform)

Eine LTL-Formel ist in *positiver Normalform*, wenn sie nur aus Literalen $p, \neg p$ (für ein $p \in P$) und den Operatoren $\vee, \wedge, X, U$ und R aufgebaut ist.

Satz

Zu jeder LTL-Formel ϕ gibt es eine äquivalente LTL-Formel ϕ' in positiver Normalform. Ferner ist $|\phi'| \leq 2 \cdot |\phi|$.

Beweis.

Zum Beweis betrachtet man jeden Operator in negierter und nicht-negierter Form und zeigt, dass man ihn wie angegeben ausdrücken kann. Z.B. ist
$Gp \equiv \neg F \neg p \equiv \neg(\top U \neg p) \equiv \neg(\neg\bot U \neg p) \equiv \bot R p$ und
$\neg(pRq) \equiv \neg\neg(\neg pU\neg q) \equiv (\neg pU\neg q)$. □

Abwicklung von U und R

Satz

Es gilt $pUq \equiv q \vee (p \wedge X(pUq))$.

Beweis.

Sei $w, i \models pUq$. Dann gibt es ein $k \geq i$ mit $w, k \models q$ und $w, j \models p$ für alle j mit $i \leq j < k$. Zwei Fälle:

1. $k = i$. Dann gilt $w, i \models q$.
2. $k > i$. Dann ist $w, i \models p$ und $w, i+1 \models pUq$ (Warum?) und daher $w, i \models X(pUq)$.

Damit gilt $w, i \models q \vee (p \wedge X(pUq))$. □

Abwicklung von U und R

Die Rückrichtung zeigt man analog. Ebenso wie die Abwicklung von R:

Satz

Es gilt $pRq \equiv q \wedge (p \vee X(pRq))$.

Beweis.

Zur Übung... □

Von LTL zum NBA - Die Idee

Wir konstruieren nun einen NBA, der genau die Menge aller Modelle für eine LTL Formel ϕ erkennt.

- Die Idee ist als Zustände Hintikka-Mengen zu benutzen. Diese enthalten gerade die (Unter-)Formeln, die an einer bestimmten Stelle im Modell gelten müssen.
- Diese werden in jedem Schritt nichtdeterministisch geraten.
- Durch die Konsistenz der Hintikka-Mengen wird ausgeschlossen, dass etwas geraten wird, was bereits der Aussagenlogik widerspricht.
- U und R Formeln werden entsprechend ihrer Abwicklung behandelt.
- Dass U nicht unendlich lange abgewickelt wird, wird durch die Akzeptanzbedingung sichergestellt.
- Der X Operator wird durch die Übergänge behandelt.

Von LTL zum NBA - Vorarbeiten

Definition (Fischer-Ladner-Abschluss)

Sei ϕ eine LTL-Formel in positiver Normalform. Der Fischer-Ladner-Abschluss von ϕ ist die kleinste Menge $FL(\phi)$, die ϕ enthält und für die folgendes gilt:

1. $p \vee q \in FL(\phi) \Rightarrow \{p, q\} \subseteq FL(\phi)$
2. $p \wedge q \in FL(\phi) \Rightarrow \{p, q\} \subseteq FL(\phi)$
3. $Xp \in FL(\phi) \Rightarrow p \in FL(\phi)$
4. $pUq \in FL(\phi) \Rightarrow \{p, q, q \vee (p \wedge X(pUq)), p \wedge X(pUq), X(pUq)\}$
5. $pRq \in FL(\phi) \Rightarrow \{p, q, q \wedge (p \vee X(pRq)), p \vee X(pRq), X(pRq)\}$

Von LTL zum NBA - Vorarbeiten

Definition (Hintikka-Mengen)

Sei ϕ eine LTL-Formel in positiver Normalform. Eine Hintikka-Menge für ϕ ist eine Menge $M \subseteq FL(\phi)$ mit

1. $p \vee q \in M \Rightarrow p \in M$ oder $q \in M$
2. $p \wedge q \in M \Rightarrow p \in M$ und $q \in M$
3. $pUq \in M \Rightarrow q \in M$ oder ($p \in M$ und $X(pUq) \in M$)
4. $pRq \in M \Rightarrow q \in M$ und ($p \in M$ oder $X(pRq) \in M$)

Von LTL zum NBA - Vorarbeiten

Definition (Hintikka-Mengen (Teil 2))

- Eine Hintikka-Menge M heißt konsistent, falls es kein $p \in P$ mit $\{p, \neg p\} \subseteq M$ gibt.
- Mit $H(\phi)$ wird die Menge aller konsistenten Hintikka-Mengen bezeichnet.
- Mit $P^+(M)$ wird die Menge aller atomaren Formeln bezeichnet, die als positives Literal in M auftreten (oder kurz: alle positiven Literale in M), also $P^+(M) = M \cap P$.
- Mit $P^-(M)$ wird die Menge aller atomaren Formeln bezeichnet, die als negatives Literal in M auftreten, also $P^-(M) = \{p \in P \mid \neg p \in M\}$.

Von LTL zum NBA - Der Satz

Satz

Zu jeder LTL-Formel θ in positiver Normalform kann ein NBA A_θ konstruiert werden mit $L(A_\theta) = L(\theta)$. Ferner ist $|A_\theta| \leq 2^{4|\theta|}$.

Korollar

Zu jeder LTL-Formel θ kann ein NBA A_θ konstruiert werden mit $L(A_\theta) = L(\theta)$. Ferner ist $|A_\theta| \leq 2^{O(|\theta|)}$.

Nebenbemerkung

Im Satz oben steht im Exponenten $4|\theta|$. Im Buch ist dort der Faktor 2. Ich meine, 2 kann man widerlegen, mit 4 klappt es und ich glaube man kann sogar $2,5 \cdot |\theta| - 1,5$ zeigen (aber nicht weniger). Nachfolgend ist das nicht ganz so wichtig. Es genügt sich die Grenze aus dem Korrollar zu merken, also $|A_\theta| \leq 2^{O(|\theta|)}$.

Von LTL zum NBA - Die Konstruktion

Seien $p_1 U q_1, p_2 U q_2, \ldots, p_k U q_k$ alle in $FL(\theta)$ vorkommenden U-Formeln. Wir definieren

$$A := (H(\theta), \Sigma, \delta, Z_{start}, Z^1_{end}, \ldots, Z^k_{end})$$

wobei:

$$\begin{aligned} Z_{start} &:= \{M \mid \theta \in M\} \\ Z^i_{end} &:= \{M \mid p_i U q_i \in M \Rightarrow q_i \in M\} \end{aligned}$$

Ferner ist

$$\delta(M, a) := \{M' \mid \forall Xq \in M : q \in M'\}$$

im Fall $P^+(M) \subseteq a$ und $P^-(M) \cap a = \emptyset$ und sonst

$$\delta(M, a) := \emptyset.$$

Von LTL zum NBA - Die Konstruktion

Hinweise

1. Das Alphabet ist $\Sigma = 2^P$, wobei P die Menge der atomaren Formeln ist.
2. Im Spezialfall, dass in θ gar keine U-Formeln auftreten, gibt es nur eine Endzustandsmenge

$$Z_{end} := H(\theta)$$

   (alle Zustände sind also Endzustände).
3. Ist $\delta(M, a) := \emptyset$, so bedeutet dies, dass der Zustand M keine a-Kante hat (es bedeutet *nicht*, dass der Zustand $\emptyset$ der Nachfolgezustand ist).

Von LTL zum NBA - Korrektheit

Satz

Zu jeder LTL-Formel θ in positiver Normalform kann ein NBA A_θ konstruiert werden mit $L(A_\theta) = L(\theta)$. Ferner ist $|A_\theta| \leq 2^{4 \cdot |\theta|}$.

Beweis.

Zu zeigen ist $L(A_\theta) \subseteq L(\theta)$, $L(A_\theta) \supseteq L(\theta)$ und die Schranke.

Für die Schranke kann man mittels Induktion

$$|FL(\theta)| \leq 4|\theta|$$

zeigen (wobei wir für $|\theta|$ die Atome und Junktoren zählen und beachten, dass z.B. $|FL(\phi U \psi)| = |FL(\phi)| + |FL(\psi)| + 4$ gilt). Damit gilt dann $|H(\theta)| \leq 2^{4|\theta|}$ (maximale Anzahl der Teilmengen von $FL(\theta)$).

Seien nachfolgend $\phi_1 U \psi_1, \ldots, \phi_k U \psi_k$ alle U-Formeln in $FL(\theta)$.

Beweis.

Sei $w \in L(\theta)$ (wir wollen $w \in L(A_\theta)$ zeigen). Sei

$$M_i := \{\psi \in FL(\theta) \mid w, i \models \psi\} \text{ für jedes } i \in \mathbb{N}$$

Wir bemerken:

1. $M_i \in H(\theta)$ (die Menge der Formeln muss eine Hintikka-Menge bilden)
   - Die Sequenz der M_i ist eine Folge von Zuständen in A_θ
2. $\theta \in M_0$ (wegen $w \in L(\theta)$)
   - Sequenz beginnt in einem Startzustand
3. Ist $X\psi \in M_i$, dann gilt $\psi \in M_{i+1}$
4. Ist der i-te Buchstabe von w ein a, so ist $M_i \cap P = a$
   - Sequenz ist eine korrekte, unendliche(!) Rechnung
5. Ist $\phi_j U \psi_j \in M_i$, dann gibt es ein $i' \geq i$ mit $\psi_j \in M_{i'}$
   - Rechnung ist akzeptierend (gibt es keine U-Formeln genügt bereits obiges)

Beweis.

Sei nun $w \in L(A_\theta)$ ($w \in L(\theta)$ ist zu zeigen). Es gibt einen akzeptierenden Lauf $M_0, M_1, \ldots$ von A_θ auf $w = w_0 w_1 \ldots$. Wir zeigen

$$\text{Wenn } \psi \in M_i, \text{ dann } w, i \models \psi$$

für alle $i \in \mathbb{N}$ und alle $\psi \in FL(\phi)$ mittels **Induktion über den Formelaufbau**.

Induktionsanfang: Ist $\psi = p \in P$, dann ist $p \in M_i$ und der Übergang in A_θ von M_i nach M_{i+1} geht nur, wenn $p \in w_i$ ist und damit gilt $w, i \models p$. Analog zeigt man für $\psi = \neg p$, dass $p \notin w_i$ sein muss und damit $w, i \models \neg p$.

Wenn $\psi \in M_i$, dann $w, i \models \psi$

Beweis.

Induktionsschritt. Für $\psi = \phi_1 \wedge \phi_2$ folgt dies schnell aus $\phi_1 \in M_i$ und $\phi_2 \in M_i$ (wegen $\psi \in M_i$ und da M_i eine Hintikka-Menge ist) und dann aus der Induktionsannahme und der Definition von $\models$. (Analog für $\vee$.)

Für $\psi = X\phi$ folgt dies, da mit $\psi \in M_i$ dann nach Konstruktion des Automaten (insb. der Übergangsrelation δ) dann $\phi \in M_{i+1}$ ist. Aufgrund der Induktionsannahme wissen wir dann $w, i+1 \models \phi$ und damit $w, i \models \psi$ (nach Definition von $\models$).

Wenn $\psi \in M_i$, dann $w, i \models \psi$

Beweis.

Der spannende Fall $\phi_j U \psi_j \in M_i$. Zwei Fälle:

- $\psi_j \in M_i$. Dann sind wir mit der Induktionsannahme (und der Definition von $\models$) sofort fertig.
- $\phi_j \in M_i$ und $X(\phi_j U \psi_j) \in M_i$. Dann ist nach der Definition von δ $\phi_j U \psi_j \in M_{i+1}$, was man iterieren kann, woraus $w, i' \models \phi_j$ (mit Induktionsannahme) und $\phi_j U \psi_j \in M'_i$ für $i' = i, i+1, i+2, \ldots$ folgt.
  Es muss nun ein $k > i$ mit $\psi_j \in M_k$ geben (sonst wird kein Endzustand besucht). Mit der Induktionsannahme folgt $w, k \models \psi_j$ und (wegen obigem) $w, h \models \phi_j$ für $i \leq h < k$.
  Daraus folgt (Definition von $\models$) $w, i \models \phi_j U \psi_j$.

Der Fall für R geht analog ($\Rightarrow$ Übung!) und wir sind fertig! $\square$

Von LTL zum NBA - Korrektheit

Hinweis

Die Konstruktion und der Beweis klappt auch ohne U-Formeln. Man muss sich dann bewusst machen, dass es nur eine Endzustandsmenge gibt (und diese aus genau allen Zuständen besteht) und dass dann also jede unendliche Rechnung akzeptiert wird. Der Automat ist aber so konstruiert, dass er bei Rechnungen, die nicht akzeptiert werden sollen, dann blockiert, weil es keinen Übergang gibt. (Siehe auch im Beweis die erste Richtung und da die ersten vier Beobachtungen; die fünfte trifft dann ja nicht zu!)

Der Schluss...

Wir nähern uns dem Ende. Das System wird eher mit einem Transitionssystem modelliert (oder mit einem Formalismus, der in dieses übersetzt wird). Daher brauchen wir dafür einen "Produktautomaten". Zur Wiederholung ...

Transitionssysteme (Wiederholung)

Definition (Transitionssystem)

Ein *labelled transition system* (LTS) ist ein Tupel $TS = (S, s_0, R, L)$mit

- einer endlichen Menge von Zuständen S,
- einem Startzustand $s_0 \in S$,
- einer links-totalen Übergangsrelation $R \subseteq S \times S$ und
- einer labelling function $L : S \to 2^P$, die jedem Zustand s die Menge der atomaren Formeln $L(s) \subseteq P$ zuweist, die in s gelten.

Transitionssysteme (Wiederholung)

Definition (Pfad im LTS)

- Ein *Pfad* π in einem LTS $TS = (S, s_0, R, L)$ ist eine unendliche Sequenz von Zuständen

$$\pi = s_1 s_2 s_3 \ldots$$

derart, dass $(s_i, s_{i+1}) \in R$ für alle $i \geq 1$.

- Ein *Lauf* in TS ist ein unendliches Wort $a_0 a_1 \ldots \in (2^P)^\omega$, so dass ein Pfad $s_0 s_1 \ldots$ existiert mit $a_i = L(s_i)$ für alle i. Mit $L(TS)$ wird die Menge der Läufe von TS bezeichnet.

Ein weiterer Produktautomat

Definition

Sei $TS = (S, s_0, R, L)$ ein LTS über P und $A = (Z, 2^P, \delta, z_0, Z_{end})$ ein NBA. Wir definieren deren *Produkt* als NBA $C := (S \times Z, \{\bullet\}, \Delta, (s_0, z_0), S \times Z_{end})$, wobei

$$\Delta((s,z),\bullet) = \{(s',z') \mid (s,s') \in R \wedge z' \in \delta(z, L(s))\}$$

Satz

Ist TS ein LTS, A ein NBA und C der aus obiger Definition hervorgegangener NBA. Es gilt $L(C) = \emptyset$ gdw. $L(TS) \cap L(A) = \emptyset$.

Beweis.

Zur Übung... □

Finale!

Satz

Das Model-Checking-Problem mit LTS TS und LTL-Formel ϕ lässt sich in Zeit $|TS| \cdot 2^{O(|\phi|)}$ entscheiden.

Beweis.

1. Betrachte $\neg\phi$ und konstruiere NBA $A_{\neg\phi}$ mit $L(A_{\neg\phi}) = L(\neg\phi) = \overline{L(A_\phi)}$. Es ist $|A_{\neg\phi}| = 2^{O(|\phi|)}$.
2. Bilde das Produkt C aus LTS TS und $A_{\neg\phi}$. Nach obigem ist $|C| = |TS| \cdot 2^{O(|\phi|)}$.
3. Nun ist nach dem vorherigen Satz $L(C) = \emptyset$ gdw. $L(TS) \cap L(A) = \emptyset$ und wir können das Leerheitsproblem in linearer Zeit, d.h. hier in $O(|TS| \cdot 2^{O(|\phi|)})$ lösen.

□

Zur Lektüre

Literaturhinweis

Der Inhalt der letzte beiden Vorlesungen ist aus *Automatentheorie und Logik* von Martin Hofmann und Martin Lange. Erschienen im Springer-Verlag, 2011.
Dort

- Kapitel 5 (komplett) für Büchi-Automaten
- Satz 9.4 und Korollar 9.5 aus Kapitel 9 zum Leerheitsproblem
- Kapitel 11 (ohne 11.3) für LTL, die Konvertierung zu NBAs und letztendlich für das Model-Checking-Problem für LTL.

Zusammenfassung

- Aussagenlogik
  - Syntax & Semantik
  - Normalform
  - **Resolution**
  - **Natürliche Deduktion**
- Prädikatenlogik
  - Syntax & Semantik
  - Normalform
  - **Resolution**
- LTL, CTL und CTL*
  - Syntax & Semantik
  - Das Model Checking Problem
  - **Automatenbasiertes LTL Model Checking**

Ende ...

Ende