

Symbolische Modell-Überprüfung

Modell-Überprüfung mit Hilfe von BDDs:

Die grundlegende Idee ist, dass *alles* mit BDDs dargestellt und manipuliert wird.

“Symbolisch” bezieht sich auf die Tatsache, dass nicht einzelne Zustände, sondern Mengen von Zuständen symbolisch dargestellt werden – jeweils diejenige Menge von Zuständen, die eine bestimmte Formel erfüllen.

Zu repräsentieren sind:

- Zustände und Operationen auf Zuständen
- Transitionssysteme
- die Algorithmen

Symbolische Modell-Überprüfung (2)

Ansatz:

- Endliche Zustandsmengen können in Binär-Vektoren kodiert werden.
- Die gewünschten und nachzuweisenden Eigenschaften des modellierten Systems werden als Prädikate über den Zuständen ausgedrückt.
- Repräsentation all dieser Dinge als aussagenlosche Formeln.
- Überprüfung durch Konstruktion bzw. Vergleich von BDDs

Modell-Überprüfung mit OBBDs

Repräsentation endlicher Zustandsmengen und Teilmengen:

- Wahl eines “genügend großen” Binärvektors $\{0, 1\}^n$ zur Darstellung der Zustände
- Teilmenge $T \subseteq S$ repräsentiert durch charakteristische Funktionen

$$f_T : \{0, 1\}^n \rightarrow \{0, 1\}$$

- Für ein CTL-Modell $\mathcal{M} = (S, \rightarrow, L)$ bietet sich an, die Markierungsfunktion L zur Darstellung heranzuziehen:
 - Für die Atome wird eine feste Ordnung angenommen.
 - Jeder Zustand wird kodiert durch die Konjunktion der (positiven bzw. negativen) Werte der Atome
 - Es wird sichergestellt, daß genügend viele Atome vorhanden sind, um alle Zustände eindeutig und unterschiedlich kodieren zu können (keine Zustände mit derselben Markierung!).
 - Eine Teilmenge von Zuständen wird repräsentiert durch die Disjunktion der (Kodierungen der) Zustände, die zu ihr gehören.
- Die Mengenoperationen Durchschnitt, Vereinigung und Komplement werden mit Hilfe der entsprechenden logischen Operationen \wedge , \vee und \neg dargestellt.

Modell-Überprüfung mit OBBDs (2)

Repräsentation der Zustandsübergangsrelation:

- Transitionsrelation ist Teilmenge von $S \times S$
 - \rightsquigarrow 2 Kopien der Repräsentation von S werden benötigt
 - \rightsquigarrow für jedes Atom a eine Kopie a'
- Übergang $s \rightarrow s'$ repräsentiert durch Konjunktion der Repräsentationen von s (mit a -s) und s' (mit a' -s)
- Transitionsrelation dargestellt als Disjunktion aller einzelnen Transitionen

Bei der Berechnung von Vorgängern von Zuständen müssen Symbole geeignet umbenannt werden ($a \rightarrow a'$ usw.)

Darstellung der Berechnung von Fixpunkten ebenfalls möglich – soll hier nicht behandelt werden.

Modell-Überprüfung mit OBBDs (3)

Gewisse Eigenschaften (bzw. temporallogische Formeln) können als (kleinste oder größte) *Fixpunkte* ausgedrückt werden.

Beispiel: Erreichbarkeit eines Zustands, der ein Prädikat p erfüllt, über die Transitionsrelation R :

$$EX(p) := \lambda x. \exists y. R(x, y) \wedge p(y)$$

Erreichbarkeit bezgl. R :

$$\mu y. (p \vee EX(y))$$

Voraussetzung: Fixpunkt existiert.

Kann gezeigt werden durch Nachweis, daß das Funktional monoton ist.

Hinreichend hierfür: in logischer Formel kommen Variable nur positiv vor (d.h. im Wirkungsbereich einer geraden Anzahl von Negationen)

Alternative Temporallogiken

LTL: “*Linear Time Logic*”

Formeln beschreiben Eigenschaften einzelner Pfade – im Gegensatz zu Pfad-Verzweigungen wie in CTL

Stattdessen können Operatoren geschachtelt werden

Syntax von LTL:

$$\begin{aligned} \phi ::= & p \mid (\neg\phi) \mid (\phi \wedge \phi) \mid \\ & \mathbf{X} \phi \mid \mathbf{G} \phi \mid \mathbf{F} \phi \mid \phi \mathbf{U} \phi \end{aligned}$$

Semantik von LTL-Formeln relativ zu einem Pfad bzw. einer Pfadmenge (in letzterem Fall muß Formel für *jeden* Pfad in der Menge erfüllt sein).

Pfade π definiert relativ zu Zustandsübergangssystem $\mathcal{M} = (S, \rightarrow, L)$

$$\pi = s_1, s_2, \dots$$

$$\pi^i = s_i, s_{i+1}, \dots \quad \text{Endstück von } \pi \text{ beginnend mit } s_i$$

LTL – Semantik

- $\mathcal{M}, \pi \models p$ genau dann, wenn $p \in L(s_1)$
- $\mathcal{M}, \pi \models \neg\phi$ genau dann, wenn $\mathcal{M}, \pi \not\models \phi$
- $\mathcal{M}, \pi \models \phi_1 \wedge \phi_2$ genau dann, wenn
 $\mathcal{M}, \pi \models \phi_1$ und $\mathcal{M}, \pi \models \phi_2$
- $\mathcal{M}, \pi \models \mathbf{X} \phi$ genau dann, wenn $\mathcal{M}, \pi^2 \models \phi$
- $\mathcal{M}, \pi \models \mathbf{G} \phi$ genau dann, wenn $\mathcal{M}, \pi^i \models \phi$ für jedes $i \geq 1$.
- $\mathcal{M}, \pi \models \mathbf{F} \phi$ genau dann, wenn es ein $i \geq 1$ gibt, so daß $\mathcal{M}, \pi^i \models \phi$
- $\mathcal{M}, \pi \models \phi_1 \mathbf{U} \phi_2$ genau dann, wenn es ein $i \geq 1$ gibt, so daß $\mathcal{M}, \pi^i \models \phi_2$,
und $\mathcal{M}, \pi^j \models \phi_1$ für jedes $1 \leq j < i$

Für LTL gelten viele Äquivalenzen analog zu denen für CTL

Alternative Temporallogiken (2)

LTL und CTL sind in gewisser Weise unvergleichbar:

Es gibt LTL-Formeln, für die es keine äquivalente CTL-Formel gibt:

z.B. **FG** p (bzw. **A** (**FG** p)) – von einem bestimmten Punkt an gilt p immer –
und umgekehrt: z.B. **AG** (**EF** p)

Erweiterung:

CTL*: (syntaktische) Obermenge von CTL und LTL; insbesondere: temporallogische Operatoren können geschachtelt werden;

CTL* ist semantisch ausdrucksstärker als CTL und LTL; z.B.

E (**GF** p) – es gibt einen Pfad, auf dem p unendlich oft gilt.

Es gibt Systeme zur Modell-Überprüfung für alle diese Varianten temporaler Logik; einige Systeme erlauben die Benutzung mehrerer Logiken