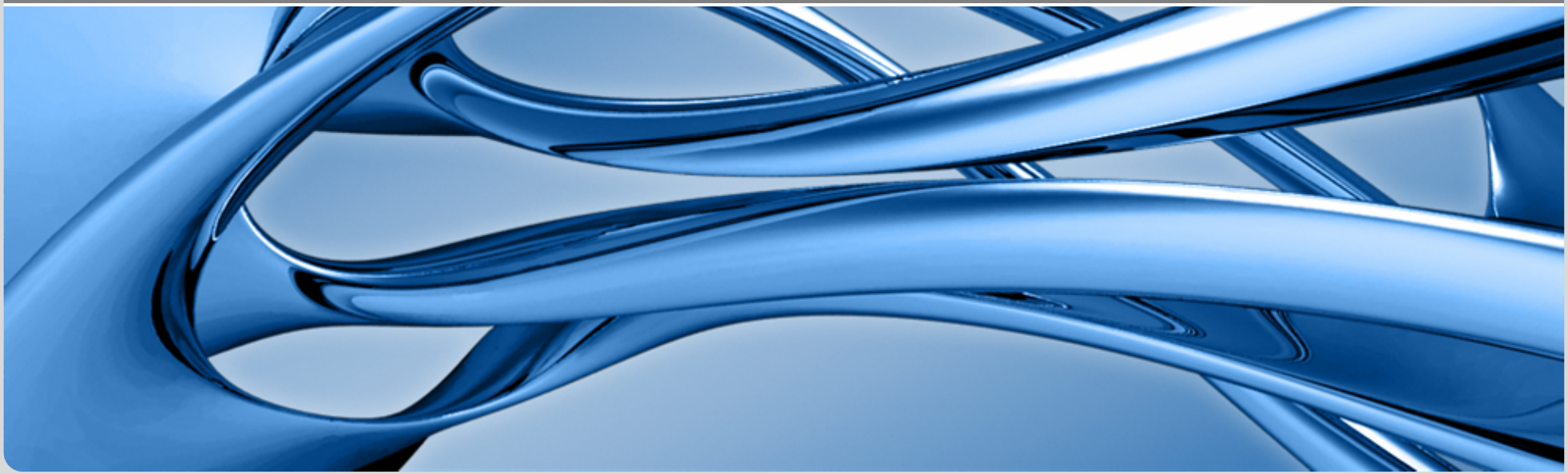
Karlsruher Institut für Technologie

Kombination von Entscheidungsverfahren

Entscheidungsverfahren mit Anwendungen in der Softwareverifikation

STEPHAN FALKE — INSTITUT FÜR THEORETISCHE INFORMATIK (ITI)



Inhalt

Motivation

- Oft möchte man Erfüllbarkeit von Formel untersuchen die in die Kombination mehrerer Theorien fallen
  - LIA und UF:

$$1 \leq x \wedge x \leq 2 \wedge f(x) \neq f(1) \wedge f(x) \neq f(2)$$

  - LIA und UF:

$$x + y = z \wedge f(x) \neq f(y)$$

  - LIA und Arrays:

$$x = \text{read}(\text{write}(v, i, e), j) \wedge y = \text{read}(v, j) \wedge x > e \wedge x > y$$

- Ziel: Methode, die Entscheidungsverfahren für zwei Theorien in ein Entscheidungsverfahren für die kombinierte Theorien zusammenführt

Beispiel

LIA und UF:

$$1 \leq x \wedge x \leq 2 \wedge f(x) \neq f(1) \wedge f(x) \neq f(2)$$

Variablenabstraktion:

$$\underbrace{1 \leq x \wedge x \leq 2 \wedge w_1 = 1 \wedge w_2 = 2}_{\text{LIA}} \wedge \underbrace{f(x) \neq f(w_1) \wedge f(x) \neq f(w_2)}_{\text{UF}}$$

- LIA: Jedes Modell erfüllt $x = 1 \vee x = 2$
- Falls Modell $x = 1$ erfüllt:
  LIA: $x = w_1$
  UF: Widerspruch zu $f(x) \neq f(w_1)$
- Falls Modell $x = 2$ erfüllt:
  LIA: $x = w_2$
  UF: Widerspruch zu $f(x) \neq f(w_2)$
- Formel ist daher unerfüllbar
- Aber: LIA-Teil und UF-Teil sind separat erfüllbar

Kombination von Theorien

Definition

Eine Theorie $T = \langle \Sigma, Ax \rangle$ besteht aus

- einer Signatur Σ bestehend aus Konstanten-, Funktions-, und Prädikatensymbolen
- einer Menge Ax von Axiomen (Sätze der Prädikatenlogik)

Definition

Seien $T_0 = \langle \Sigma_0, Ax_0 \rangle$ und $T_1 = \langle \Sigma_1, Ax_1 \rangle$ zwei Theorien.
Die kombiniert Theorie ist $T_0 \oplus T_1 = \langle \Sigma, Ax \rangle$ mit

- $\Sigma = \Sigma_0 \cup \Sigma_1$
- $Ax = Ax_0 \cup Ax_1$

Stably-Infinite Theorien

Definition

Eine Theorie T ist stably-infinite gdw. jede erfüllbare, quantoren-freie T-Formel ein Modell mit einem unendlichen Universum hat

Beispiel

- LIA, UF und die Theorie der Arrays sind stably-infinite
- Die Theorie $T = \langle \Sigma, Ax \rangle$ mit
  - $\Sigma = \{a, b\}$
  - $Ax = \{\forall x.\ x = a \vee x = b\}$

  ist nicht stably-infinite

Hauptresultat

Definition

Zwei Theorien $T_0 = \langle \Sigma_0, Ax_0 \rangle$ und $T_1 = \langle \Sigma_1, Ax_1 \rangle$ erfüllen die Nelson-Oppen-Bedingung falls

- $\Sigma_0 \cap \Sigma_1 = \{=\}$, und diese Prädikatensymbol ist in beiden Theorien als Gleichheit axiomatisiert
- T_0 und T_1 sind stably-infinite

Satz (Nelson-Oppen)

Seien T_0 und T_1 zwei Theorien so dass

- die quantorenfreien Fragmente von T_0 und T_1 entscheidbar sind
- T_0 und T_1 die Nelson-Oppen-Bedingung erfüllen

Dann ist auch das quantorenfreie Fragment von $T_0 \oplus T_1$ entscheidbar

Anmerkung 1: Im folgenden sind alle Formeln quantorenfreie Konjunktionen

Anmerkung 2: Formeln mit einer komplexeren Booleschen Struktur können dann mit Hilfe des DPLL(T)-Verfahrens entschieden werden

Nichtdeterministisches Nelson-Oppen Verfahren – Phase 1 (Variablenabstraktion)

- Ziel: Transformiere $T_0 \oplus T_1$-Formel φ in eine T_0-Formel φ_0 und eine T_1-Formel φ_1 so dass φ und $\varphi_0 \wedge \varphi_1$ äquivalent bzgl. $T_0 \oplus T_1$ sind
- Vorgehen: Wende die folgenden Transformationen an (w ist jeweils eine frische Variable)
  - $\varphi[f(\ldots, g(\ldots), \ldots)] \Longrightarrow \varphi[f(\ldots, w, \ldots)] \wedge w = g(\ldots)$ falls $f \in \Sigma_i$ und $g \in \Sigma_{1-i}$
  - $\varphi[p(\ldots, g(\ldots), \ldots)] \Longrightarrow \varphi[p(\ldots, w, \ldots)] \wedge w = g(\ldots)$ falls $p \in \Sigma_i$ und $g \in \Sigma_{1-i}$
  - $\varphi[f(\ldots) = g(\ldots)] \Longrightarrow \varphi[f(\ldots) = w] \wedge w = g(\ldots)$ falls $f \in \Sigma_i$ und $g \in \Sigma_{1-i}$
- Nach Anwendung dieser Transformationen:
  - Jedes Literal ist entweder ein T_0-Literal oder ein T_1-Literal
  - Ausnahme: Literal $(\neg)x = y$ für Variablen x, y sind T_0-Literale und T_1-Literale
- φ_i ist dann die Konjunktion von T_i-Literalen

Beispiel

LIA und UF:

$$f(x) = x + y \ \wedge \ x \leq y + z \ \wedge \ x + z \leq y \ \wedge \ y = 1 \ \wedge \ f(x) \neq f(2)$$

- $f \in \text{UF}, + \in \text{LIA}$:

$$f(x) = w_1 \ \wedge \ w_1 = x + y \ \wedge \ x \leq y + z \ \wedge \ x + z \leq y \ \wedge \ y = 1 \ \wedge \ f(x) \neq f(2)$$

- $f \in \text{UF}, 2 \in \text{LIA}$:

$$f(x) = w_1 \ \wedge \ w_1 = x + y \ \wedge \ x \leq y + z \ \wedge \ x + z \leq y \ \wedge \ y = 1 \ \wedge \ f(x) \neq f(w_2) \ \wedge \ w_2 = 2$$

- Aufteilung

$$\text{LIA} : w_1 = x + y \ \wedge \ x \leq y + z \ \wedge \ x + z \leq y \wedge y = 1 \wedge w_2 = 2$$
$$\text{UF} : f(x) = w_1 \ \wedge \ f(x) \neq f(w_2)$$

Nichtdeterministisches Nelson-Oppen Verfahren – Phase 2 (Rate-und-Prüfe)

- Sei $V = V(\varphi_0) \cap V(\varphi_1)$ die Menge der gemeinsamen Variablen
- Rate eine Äquivalenzrelation E auf V
- Definiere die Formel

$$\alpha(V,E): \bigwedge_{u,v \in V,(u,v) \in E} u = v \quad \wedge \quad \bigwedge_{u,v \in V,(u,v) \notin E} u \neq v$$

- Falls
  - $\varphi_0 \wedge \alpha(V,E)$ ist T_0-erfüllbar
  - $\varphi_1 \wedge \alpha(V,E)$ ist T_1-erfüllbar

  so gib `erfüllbar` aus

Beispiel

$$\text{LIA} : w_1 = x + y \ \wedge \ x \leq y + z \ \wedge \ x + z \leq y \wedge y = 1 \wedge w_2 = 2$$

$$\text{UF} : f(x) = w_1 \ \wedge \ f(x) \neq f(w_2)$$

- $V = \{x, w_1, w_2\}$
- Rate die leere Äquivalenzrelation E gegeben durch die Partitionierung $\{ \{x\}, \{w_1\}, \{w_2\} \}$
- Definiere die Formel (optimiert!)

$$\alpha(V, E) : x \neq w_1 \wedge x \neq w_2 \wedge w_1 \neq w_2$$

- Prüfe Erfüllbarkeit:

$$\text{LIA} : w_1 = x + y \ \wedge \ x \leq y + z \ \wedge \ x + z \leq y \wedge y = 1 \wedge w_2 = 2 \ \wedge \ \alpha(V, E)$$

erfüllbar, $x \mapsto 0, y \mapsto 1, z \mapsto 1, w_1 \mapsto 1, w_2 \mapsto 2$

$$\text{UF} : f(x) = w_1 \ \wedge \ f(x) \neq f(w_2) \ \wedge \ \alpha(V, E)$$

erfüllbar

- Gib `erfüllbar` aus

Beispiel

$$\underbrace{1 \leq x \wedge x \leq 2 \wedge w_1 = 1 \wedge w_2 = 2}_{\text{LIA}} \wedge \underbrace{f(x) \neq f(w_1) \wedge f(x) \neq f(w_2)}_{\text{UF}}$$

- $V = \{x, w_1, w_2\}$
- Es gibt 5 Äquivalenzrelationen auf V
  1. $\{ \{x, w_1, w_2\} \}$
  2. $\{ \{x, w_1\}, \{w_2\} \}$
  3. $\{ \{x, w_2\}, \{w_1\} \}$
  4. $\{ \{x\}, \{w_1, w_2\} \}$
  5. $\{ \{x\}, \{w_1\}, \{w_2\} \}$
- Für 1, 2, und 3 ist UF $\wedge\, \alpha(V, E)$ unerfüllbar
- Für 4 und 5 ist LIA $\wedge\, \alpha(V, E)$ unerfüllbar
- Die Formel ist daher unerfüllbar

Nichtdeterministisches Nelson-Oppen Verfahren – Komplexität

Satz (Nelson-Oppen)
Seien T_0 und T_1 zwei Theorien so dass

- die quantorenfreien Fragmente von T_0 und T_1 in $\mathcal{NP}$ entscheidbar sind
- T_0 und T_1 die Nelson-Oppen-Bedingung erfüllen

Dann ist auch das quantorenfreie Fragment von $T_0 \oplus T_1$ in $\mathcal{NP}$ entscheidbar

Problem: Nicht praktikabel de es exponentiell viele Äquivalenzrelationen gibt

$\lvert V\rvert$	# Äquivalenzrelationen	$\lvert V\rvert$	# Äquivalenzrelationen
1	1	7	877
2	2	8	4.140
3	5	9	21.147
4	15	10	115.975
5	52	11	678.570
6	203	12	4.213.597

Nichtdeterministisches Nelson-Oppen Verfahren – Korrektheit 1

Satz

Seien T_0 und T_1 Theorien so dass $\Sigma_0 \cap \Sigma_1 = \{=\}$. Sei Φ_0 eine Menge von (allgemeinen) T_0-Formeln und sei Φ_1 eine Menge von (allgemeinen) T_1-Formeln.
Dann ist $\Phi_0 \cup \Phi_1$ erfüllbar gdw. es ein Modell $\mathcal{A}$ von Φ_0 und ein Modell $\mathcal{B}$ von Φ_1 gibt so dass

1. $|A| = |B|$
2. $x^{\mathcal{A}} = y^{\mathcal{A}}$ gdw. $x^{\mathcal{B}} = y^{\mathcal{B}}$ für alle Variablen $x, y \in V(\Phi_0) \cap V(\Phi_1)$

Für den Beweis siehe z.B.

Zohar Manna, Calogero G. Zarba: *Combining Decision Procedures*. 10th Anniversary Colloquium of UNU/IIST, p. 381-422, 2002

Nichtdeterministisches Nelson-Oppen Verfahren – Korrektheit 2

Satz

Seien T_0 und T_1 Theorien die Nelson-Oppen-Bedingung erfüllen. Sei φ_0 eine T_0-Formel und φ_1 eine T_1-Formel.
$\varphi_0 \wedge \varphi_1$ ist $T_0 \oplus T_1$-erfüllbar gdw. es eine Äquivalenzrelation E auf $V(\varphi_0) \cap V(\varphi_1)$ gibt so dass $\varphi_i \wedge \alpha(V, E)$ erfüllbar in T_i ist für $i = 0, 1$

Beweis.

"$(\Rightarrow)$" Jedes $T_0 \oplus T_1$-Modell von $\varphi_0 \wedge \varphi_1$ definiert eine "passende" Äquivalenzrelation

"$(\Leftarrow)$" Da T_0 und T_1 stably-infinite sind, gibt es unendliche Modelle von $\varphi_i \wedge \alpha(V, E)$ für $i = 0, 1$. Mit Hilfe des Satzes von Löwenheim und Skolem gibt es Modelle $\mathcal{A}_i$ von $\varphi_i \wedge \alpha(V, E)$ für $i = 0, 1$ mit der selben Kardinalität, d.h., $|A_0| = |A_1|$.
Da $\mathcal{A}_i$ für $i = 0, 1$ ein Modell von $\alpha(V, E)$ ist, gilt $x^{\mathcal{A}_0} = y^{\mathcal{A}_0}$ gdw. $x^{\mathcal{A}_1} = y^{\mathcal{A}_1}$ für alle Variablen $x, y \in V(\varphi_0) \cap V(\varphi_1)$. Aufgrund des Satzes von der vorherigen Folien ist $\varphi_0 \wedge \varphi_1$ dann $T_0 \oplus T_1$-erfüllbar. □

Warum Stably-Infinite Theorien?

Beispiel

- Die Theorie $T = \langle \Sigma, Ax \rangle$ mit
  - $\Sigma = \{a, b\}$
  - $Ax = \{\forall x.\ x = a \vee x = b\}$

  ist nicht stably-infinite
- T und UF:

$$\underbrace{a = b}_{T} \wedge \underbrace{f(x) \neq f(y)}_{\text{UF}}$$

- $V = \emptyset$, daher nur eine Äquivalenzrelation
- Prüfe Erfüllbarkeit:

$$T : a = b \qquad \text{UF} : f(x) \neq f(y)$$

erfüllbar erfüllbar

- Aber: $a = b \wedge f(x) \neq f(y)$ ist $T \oplus$ UF-unerfüllbar
  da $T \cup \{a = b\}$ impliziert dass $\forall x, y.\ x = y$ wahr ist

Deterministisches Nelson-Oppen Verfahren

- Idee: Benutze die Entscheidungsverfahren für T_0 und T_1 um die Äquivalenzrelation “on-the-fly” zu erzeugen
  - Falls das Entscheidungsverfahren für T_i feststellt dass

$$x = y$$

für $x, y \in V(\varphi_0) \cap V(\varphi_1)$ gelten muss, so teilt es dieses dem Entscheidungsverfahren für T_{1-i} mit

Definition (Konvexe Theorie)
Eine Theorie T ist konvex wenn für jede T-gültige Formel der Form (für Variablen u_i, v_i)

$$\varphi \rightarrow \bigvee_{i=1}^{n} u_i = v_i$$

ein $i \in \{1, \ldots, n\}$ existiert so dass bereits

$$\varphi \rightarrow u_i = v_i$$

T-gültig ist

Konvexe Theorien

- LIA ist nicht konvex

$$[1 \leq x \wedge x \leq 2 \wedge w_1 = 1 \wedge w_2 = 2] \rightarrow [x = w_1 \vee x = w_2] \quad \text{ist gültig}$$
$$[1 \leq x \wedge x \leq 2 \wedge w_1 = 1 \wedge w_2 = 2] \rightarrow [x = w_1] \quad \text{ist nicht gültig}$$
$$[1 \leq x \wedge x \leq 2 \wedge w_1 = 1 \wedge w_2 = 2] \rightarrow [x = w_2] \quad \text{ist nicht gültig}$$

- Linear Arithmetik über $\mathbb{Q}$ oder $\mathbb{R}$ ist konvex
- Die Theorie der Arrays ist nicht konvex

$$[\text{read}(\text{write}(a, i, v), j) = v)] \rightarrow [i = j \vee \text{read}(a, j) = v] \quad \text{ist gültig}$$
$$[\text{read}(\text{write}(a, i, v), j) = v)] \rightarrow [i = j] \quad \text{ist nicht gültig}$$
$$[\text{read}(\text{write}(a, i, v), j) = v)] \rightarrow [\text{read}(a, j) = v] \quad \text{ist nicht gültig}$$

- UF ist konvex

Deterministisches Nelson-Oppen Verfahren für konvexe Theorien

Algorithmus

- $T_0 \oplus T_1$-Formel φ für konvexe, die Nelson-Oppen-Bedingung erfüllende T_0, T_1
- Ausgabe: `erfüllbar` oder `unerfüllbar`
- Schritte:

1. Führe Variablenabstraktion durch, erhalte φ_0 und φ_1
2. Falls φ_i für ein i unerfüllbar in T_i ist, gib `unerfüllbar` aus
3. Falls es $u, v \in V(\varphi_0) \cap V(\varphi_1)$ und ein i gibt so dass

$$\varphi_i \rightarrow u = v$$

T_i-gültig und

$$\varphi_{1-i} \rightarrow u = v$$

nicht T_{1-i}-gültig ist, so setze

$$\varphi_{1-i} := \varphi_{1-i} \wedge u = v$$

und gehe zu Schritt 2

4. Andernfalls, gib `erfüllbar` aus

Beispiel

LRA und UF:

$$x_2 \geq x_1 \ \wedge \ x_1 - x_3 \geq x_2 \ \wedge \ x_3 \geq 0 \ \wedge \ f(f(x_1) - f(x_2)) \neq f(x_3)$$

LRA	UF
$x_2 \geq x_1$	$f(a_1) \neq f(x_3)$
$x_1 - x_3 \geq x_2$	$a_2 = f(x_1)$
$x_3 \geq 0$	$a_3 = f(x_2)$
$a_1 = a_2 - a_3$	
$(x_3 = 0)$	
$x_1 = x_2$	$\hookrightarrow x_1 = x_2$
$a_2 = a_3$	$\hookleftarrow a_2 = a_3$
$(a_1 = 0)$	
$a_1 = x_3$	$\hookrightarrow a_1 = x_3$
	`unerfüllbar`

Beispiel (inkorrekt!)

LIA und UF:

$$1 \leq x \wedge x \leq 2 \wedge f(x) \neq f(1) \wedge f(x) \neq f(2)$$

LIA	UF
$1 \leq x$ $x \leq 2$ $w_1 = 1$ $w_2 = 2$	$f(x) \neq f(w_1)$ $f(x) \neq f(w_2)$
keine implizierten Gleichheiten `erfüllbar`	keine implizierten Gleichheiten `erfüllbar`

Ergebnis ist inkorrekt da LIA nicht konvex ist!

Deterministisches Nelson-Oppen Verfahren für nicht-konvexe Theorien

Algorithmus

- $T_0 \oplus T_1$-Formel φ für die Nelson-Oppen-Bedingung erfüllende T_0, T_1
- Ausgabe: `erfüllbar` oder `unerfüllbar`
- Schritte:

1. Führe Variablenabstraktion durch, erhalte φ_0 und φ_1
2. Falls φ_i für ein i unerfüllbar in T_i ist, gib `unerfüllbar` aus
3. Falls es $u_k, v_k \in V(\varphi_0) \cap V(\varphi_1)$ und ein i gibt so dass

$$\varphi_i \rightarrow \bigvee_{l=1}^{n} u_l = v_l$$

T_i-gültig und

$$\varphi_{1-i} \rightarrow u_l = v_l$$

nicht T_{1-i}-gültig ist für alle $1 \leq l \leq n$, so rufe dich n-mal selber mit

$$\varphi_0 \wedge \varphi_1 \wedge x_1 = y_1, \ldots, \varphi_0 \wedge \varphi_1 \wedge x_n = y_n$$

und gib `erfüllbar` aus falls einer der rekursiven Aufrufe `erfüllbar` ausgibt

4. Andernfalls, gib `erfüllbar` aus

Beispiel

LIA und UF: $1 \leq x \wedge x \leq 2 \wedge f(x) \neq f(1) \wedge f(x) \neq f(2)$

LIA	UF
$1 \leq x$	$f(x) \neq f(w_1)$
$x \leq 2$	$f(x) \neq f(w_2)$
$w_1 = 1$	
$w_2 = 2$	
$x = w_1 \vee x = w_2$	

Aufspaltung in zwei rekursive Aufrufe

LIA	UF
$1 \leq x$	$f(x) \neq f(w_1)$
$x \leq 2$	$f(x) \neq f(w_2)$
$w_1 = 1$	
$w_2 = 2$	
$x = w_1 \hookrightarrow x = w_1$	`unerfüllbar`

LIA	UF
$1 \leq x$	$f(x) \neq f(w_1)$
$x \leq 2$	$f(x) \neq f(w_2)$
$w_1 = 1$	
$w_2 = 2$	
$x = w_2 \hookrightarrow x = w_2$	`unerfüllbar`