Prädikatenlogische Entscheidbarkeitsprobleme

Erfüllbarkeitsproblem:

Gegeben: prädikatenlogischer Ausdruck A über einer Signatur $\mathcal{S}$
Frage: Ist A erfüllbar ?

Gültigkeitsproblem:

Gegeben: prädikatenlogischer Ausdruck A über einer Signatur $\mathcal{S}$
Frage: Ist A allgemeingültig ?

Unerfüllbarkeitsproblem:

Gegeben: prädikatenlogischer Ausdruck A über einer Signatur $\mathcal{S}$
Frage: Ist A unerfüllbar ?

Algorithmus und Entscheidbarkeit

Ein *Algorithmus* überführt in endlicher Zeit die Eingabedaten in eine Antwort "ja" oder "nein" und besteht aus einer Folge von Anweisungen mit folgenden Eigenschaften:

- es gibt eine eindeutig festgelegte Anweisung, die als erste auszuführen ist,

- nach Abarbeitung einer Anweisung gibt es eine eindeutig festgelegte Anweisung, die als nächste abzuarbeiten ist, oder die Abarbeitung des Algorithmus ist beendet.

Ein Problem heißt *entscheidbar*, wenn es einen Algorithmus zu seiner Lösung gibt, d.h. einen Algorithmus, der auf die Frage die korrekte Antwort "ja" oder "nein" gibt. Falls kein Algorithmus zur Lösung existiert, heißt das Problem *unentscheidbar*.

Unentscheidbarkeit in der Prädikatenlogik

Satz:
Das Gültigkeitsproblem der Prädikatenlogik ist unentscheidbar, d.h. es gibt keinen Algorithmus, der für einen beliebigen prädikatenlogischen Ausdruck A feststellt, ob A eine Tautologie ist.

Satz:
Das Unerfüllbarkeitsproblem der Prädikatenlogik ist unentscheidbar, d.h. es gibt keinen Algorithmus, der für einen beliebigen prädikatenlogischen Ausdruck A feststellt, ob A unerfüllbar ist.

Satz:
Das Erfüllbarkeitsproblem der Prädikatenlogik ist unentscheidbar, d.h. es gibt keinen Algorithmus, der für einen beliebigen prädikatenlogischen Ausdruck A feststellt, ob A erfüllbar ist.

Semi-Algorithmus

Wir nennen ein Verfahren zur Entscheidung einer Eigenschaft E einen Semi-Algorithmus, wenn es

— auf einer Eingabe X mit Eigenschaft E nach einer endlichen Anzahl von Schritten antwortet, dass X die Eigenschaft E hat und

— auf einer Eingabe, die die Eigenschaft E nicht hat, keine Antwort gibt.

Herbrand-Universum – Definition

Definition:
Für einen prädikatenlogischen Ausdruck A in bereinigter Skolemform definieren das Herbrand-Universum $H(A)$ von A induktiv wie folgt:

- Alle in A vorkommenden Konstanten sind in $H(A)$. Falls A keine Konstante enthält, so ist $a \in H(A)$ (wobei a ein Symbol ist, das in A nicht vorkommt).

- Sind $t_1, t_2, \ldots, t_k$ in $H(A)$ und ist f ein k-stelliges Funktionssymbol in A, so ist $f(t_1, t_2, \ldots, t_k) \in H(A)$.

Herbrand-Erweiterung – Definition

Definition:
Für einen Ausdruck $A = \forall x_1 \forall x_2 \ldots \forall x_n A'$ in bereinigter Skolemform definieren wir die Herbrand-Erweiterung $E(A)$ als die Menge

$$\begin{aligned} E(A) \quad = \quad & \{sub(sub(\ldots(sub(sub(A', x_n, t_n), x_{n-1}, t_{n-1})\ldots), x_2, t_2), x_1, t_1) \mid \\ & \quad t_1, t_2, \ldots, t_n \in H(A)\} \end{aligned}$$

und setzen

$$\begin{aligned} E'(A) \quad = \quad & \{sub(\ldots(sub(sub(B, x_n, t_n), x_{n-1}, t_{n-1})\ldots), x_1, t_1) \mid \\ & \quad B \in B(A),\ t_1, t_2, \ldots, t_n \in H(A)\}\,. \end{aligned}$$

Sätze der Herbrand-Theorie

Satz: Ein Ausdruck A in bereinigter Skolemform ist genau dann erfüllbar, wenn die Menge $E(A)$ im aussagenlogischen Sinn erfüllbar ist (d.h., wenn es eine Belegung α von $E'(A)$ derart gibt, dass $w_\alpha(B) = 1$ für alle $B \in E(A)$ gilt).

Satz: Ein Ausdruck A in bereinigter Skolemform ist genau dann erfüllbar, wenn jede endliche Teilmenge von $E(A)$ erfüllbar ist.

Satz: Ein Ausdruck A in bereinigter Skolemform ist genau dann unerfüllbar, wenn es eine endliche Teilmenge von $E(A)$ gibt, die unerfüllbar ist.

Semi-Algorithmus (von GILMORE) für das Unerfüllbarkeitsproblem

Eingabe: prädikatenlogischer Ausdruck A in bereinigter Skolemform,
Aufzählung von $E(A) = \{A_1, A_2, A_3, \ldots\}$

$n = 1$; $F = A_1$;
`while` (F ist erfüllbar) $\{\ n = n + 1$; $F = F \wedge A_n;\}$
Gib "A ist unerfüllbar" aus (und stoppe);

Grundresolutionsalgorithmus zur Entscheidung der Unerfüllbarkeit eines prädikatenlogischen Ausdrucks

Eingabe: präd.log. Ausdruck $A = \forall x_1 \ldots \forall x_k A'$ in bereinigter Skolemform
A' in konjunktiver Normalform
Aufzählung von $E(A) = \{A_1, A_2, A_3, \ldots\}$
für $n \geq 1$ sei K_n die Klauselmenge zu A_n

$n = 1$; $M = \{K_1\}$; $M = res^*(M)$;
`while` $(\emptyset \notin M)$ $\{$ $n = n + 1$; $M = M \cup \{K_n\}$; $M = res^*(M)$; $\}$
Gib "A ist unerfüllbar" aus (und stoppe);

Unifikator

Definition:
i) Eine Substitution s heißt Unifikator der Menge $\mathcal{L} = \{L_1, L_2, \ldots L_r\}$ von Literalen, falls $s(L_1) = s(L_2) = \ldots = s(L_r)$ gelten.

ii) Eine Substitution s heißt allgemeinster Unifikator von $\mathcal{L}$, falls für jeden Unifikator s' von $\mathcal{L}$ eine Substitution s'' mit $s' = s \circ s''$ existiert.

Satz:
Jede unifizierbare Menge von Literalen besitzt einen allgemeinsten Unifikator.

Algorithmus für den allgemeinsten Unifikator

Eingabe: nichtleere Menge $\mathcal{L} = \{L_1, L_2, \ldots, L_r\}$ von Literalen

$s = id$;

`while` $(s(L_i) \neq s(L_j)$ für gewisse $1 \leq i < j \leq k)$

$\{$ Durchsuche die Literale von $s(L_i)$ und $s(L_j)$ von links nach rechts, bis erste Position a gefunden ist, an der sich mindestens zwei Literale unterscheiden;

`if` (keines der Zeichen ist eine Variable)

Stoppe mit "$\mathcal{L}$ ist nicht unifizierbar";

`else` $\{$ $x =$ Variable in a; $t =$ Term, der in a beginnt;

`if` (x kommt in t vor)

Stoppe mit "$\mathcal{L}$ ist nicht unifizierbar";

`else` $s = s \circ [x/t]$;

$\}$

$\}$

Gib s als allgemeinsten Unifikator aus

Unifikationsalgorithmus – Beispiel

Literale: $L_1 = \neg P(f(z, g(a, y)), h(z))$
$L_2 = \neg P(f(f(u, v), w), h(f(a, b)))$

Unterschied an der sechsten Position: Substitution $s_1 = [z/f(u, v)]$
$s_1(L_1) = \neg P(f(f(u, v), g(a, y)), h(f(u, v)))$
$s_1(L_2) = \neg P(f(f(u, v), w), h(f(a, b)))$

Unterschied an der elften Position: Substitution $s_2 = [w/g(a, y)]$
$s_2(s_1(L_1)) = \neg P(f(f(u, v), g(a, y)), h(f(u, v)))$
$s_2(s_1(L_2)) = \neg P(f(f(u, v), g(a, y)), h(f(a, b)))$

Unifikationsalgorithmus – Beispiel – Fortsetzung

Literale: $s_2(s_1(L_1)) = \neg P(f(f(u,v),g(a,y)),h(f(u,v)))$
$s_2(s_1(L_2)) = \neg P(f(f(u,v),g(a,y)),h(f(a,b)))$

Unterschied bei sechstletzten Buchstaben: Substitution $s_3 = [u/a]$
$s_3(s_2(s_1(L_1))) = \neg P(f(f(a,v),g(a,y)),h(f(a,v)))$
$s_3(s_2(s_1(L_2))) = \neg P(f(f(a,v),g(a,y)),h(f(a,b)))$

Unterschied bei viertletzten Buchstaben: Substitution $s_4 = [v/b]$
$s_4(s_3(s_2(s_1(L_1)))) = \neg P(f(f(a,b),g(a,y)),h(f(a,b)))$
$s_4(s_3(s_2(s_1(L_2)))) = \neg P(f(f(a,b),g(a,y)),h(f(a,b)))$

allgemeinsten Unifikator von L_1 und L_2:
$s_1 \circ s_2 \circ s_3 \circ s_4 = [z/f(u,v)] \circ [w/g(a,y)] \circ [u/a] \circ [v/b]$

Prädikatenlogische Resolution – Definition I

Definition:
Es seien $\mathcal{K}_1$, $\mathcal{K}_2$ und $\mathcal{R}$ Mengen von prädikatenlogischen Literalen. Dann heißt $\mathcal{R}$ prädikatenlogische Resolvente von $\mathcal{K}_1$ und $\mathcal{K}_2$, falls folgende Bedingungen erfüllt sind:

- Es gibt Substitutionen s_1 und s_2, die nur Variablenumbenennugen sind, so dass $s_1(\mathcal{K}_1)$ und $s_2(\mathcal{K}_2)$ keine gemeinsamen Variablen haben.

- Es gibt Literale $L_1, \ldots, L_m \in s_1(\mathcal{K}_1)$, $m \geq 1$, und $L'_1, \ldots, L'_n \in s_2(\mathcal{K}_2)$, $n \geq 1$, so dass die Menge $\mathcal{L} = \{\neg L_1, \neg L_2, \ldots, \neg L_m, L'_1, L'_2, \ldots, L'_n\}$ unifizierbar ist.
  s sei der allgemeinste Unifikator von $\mathcal{L}$.

- Es gilt $\mathcal{R} = s((s_1(\mathcal{K}_1) \setminus \{L_1, L_2, \ldots, L_m\}) \cup (s_2(\mathcal{K}_2) \setminus \{L'_1, L'_2, \ldots, L'_n\}))$

Prädikatenlogische Resolution – Definition II

Definition:
Für eine Menge $\mathcal{F}$ von Mengen von Literalen setzen wir

$$\begin{aligned}
Res(\mathcal{F}) &= \mathcal{F} \cup \{\mathcal{R} \mid \mathcal{R} \text{ ist Resolvente gewisser } \mathcal{K} \in \mathcal{F} \text{ und } \mathcal{K}' \in \mathcal{F}\}\,, \\
Res^0(\mathcal{F}) &= \mathcal{F}\,, \\
Res^n(\mathcal{F}) &= Res(Res^{n-1}(\mathcal{F})) \text{ für } n \geq 1 \text{ und} \\
Res^*(\mathcal{F}) &= \bigcup_{n \geq 0} Res^n(\mathcal{F})\,.
\end{aligned}$$

Prädikatenlogische Resolution – Resultate

Lemma: (Lifting-Lemma) Seien K_1 und K_2 zwei prädikatenlogische Klauseln und K_1' und K_2' zugehörige (beliebige) Grundinstanzen. Ferner sei R' eine (aussagenlogische) Resolvente von K_1' und K_2'. Dann gibt es eine prädikatenlogische Resolvente R von K_1 und K_2 so, dass R' Grundinstanz von R ist.

$$\begin{tikzcd}
K_1 \arrow[d] & & K_2 \arrow[d] \\
K_1' \arrow[dr] & & K_2' \arrow[dl] \\
& R' &
\end{tikzcd}
\qquad
\begin{tikzcd}
K_1 \arrow[dr] & & K_2 \arrow[dl] \\
& R \arrow[d] & \\
& R' &
\end{tikzcd}$$

Satz: Ein prädikatenlogischer Ausdruck $A = \forall x_1 \forall x_2 \ldots \forall x_n A'$ in bereinigter Skolemform, bei dem A' in konjunktiver Normalform vorliegt, ist A genau dann unerfüllbar, wenn die leere Menge in $Res^*(A)$ liegt.

Lineare Resolutionen I

Definition: Die Resolution einer Klausel R aus einer Klauselmenge $\mathcal{K}$ heißt linear, falls es Klauseln $R_0, R_1, R_2, \ldots, R_n$ so gibt, dass

$$\begin{aligned} R_0 &\in \mathcal{K}, \\ R_i &\in res(R_{i-1}, C_{i-1}) \\ &\qquad \text{mit } C_{i-1} \in \mathcal{K} \cup \{R_1, R_2, \ldots, R_{i-1}\},\ 1 \leq i \leq n \end{aligned}$$

gelten.

Satz: Sei $A = \forall x_1 \forall x_2 \ldots \forall x_n A'$ ein prädikatenlogischer Ausdruck in bereinigter Skolemform, bei dem A' in konjunktiver Normalform vorliegt. Dann ist A genau dann unerfüllbar, wenn es eine lineare Resolution für die leere Menge aus der Klauselmenge zu A' gibt.

Lineare Resolutionen II

Definition: Eine Klauselmenge $\mathcal{K}$ heißt minimal unerfüllbar, wenn sie unerfüllbar ist und für jede Klausel $K \in \mathcal{K}$ die Menge $\mathcal{K} \setminus \{K\}$ erfüllbar ist.

Satz: Sei $A = \forall x_1 \forall x_2 \ldots \forall x_n A'$ ein prädikatenlogischer Ausdruck in bereinigter Skolemform, bei dem A' in konjunktiver Normalform vorliegt. Ferner sei die zu A' gehörende Klauselmenge minimal unerfüllbar. Dann gibt es für jede Klausel K von A' eine lineare Resolution für die leere Menge aus der Klauselmenge zu A', bei der $R_0 = K$ gilt.

SDL-Resolutionen

Definition: i) Wir sagen, dass eine Klausel negativ ist, wenn alle Literale negierte Basisausdrücke sind. Eine Klausel heißt definit, wenn genau ein Literal ein nichtnegierter Basisausdruck ist.

ii) Eine lineare Resolution heißt SLD–Resolution, falls R_0 eine negative Klausel ist und C_{i-1} für $1 \leq i \leq n$ eine definite Klausel ist.

Definition: Ein quantorenfreier prädikatenlogischer Ausdruck A' in konjunktiver Normalform heißt Hornausdruck, falls jede Alternative höchstens einen nichtnegierten Basisausdruck enthält.

Satz: Sei $A = \forall x_1 \forall x_2 \dots \forall x_n A'$ ein prädikatenlogischer Ausdruck in bereinigter Skolemform, bei dem A' ein Hornausdruck ist. Dann ist A genau dann unerfüllbar, wenn es eine SLD-Resolution für die leere Menge aus der Klauselmenge zu A' gibt.