Formale Grundlagen der Informatik 3
Kapitel 4
Prädikatenlogik
Resolution

Frank Heitmann
heitmann@informatik.uni-hamburg.de

30. November 2015

Eine besondere Formel

In der Aussagenlogik kann man Wahrheitstafeln aufmalen. In der Prädikatenlogik existieren unendlich viele Strukturen. Die Lage ist aber noch schlimmer:

Eine besondere Formel

Sei

$$\begin{aligned} F \quad = \quad & \forall x P(x, f(x)) \wedge \\ & \forall y \neg P(y, y) \wedge \\ & \forall u \forall v \forall w ((P(u, v) \wedge P(v, w)) \Rightarrow P(u, w)) \end{aligned}$$

Dann ist z.B. mit $\mathcal{A} = (U, I)$, wobei $U = \mathbb{N}$, $I(P) = \{(m, n) \mid m < n\}$ und $I(f)(n) = n + 1$ eine erfüllende Struktur gegeben.

Eine besondere Formel

In der Aussagenlogik kann man Wahrheitstafeln aufmalen. In der Prädikatenlogik existieren unendlich viele Strukturen. Die Lage ist aber noch schlimmer:

Eine besondere Formel

Sei

$$\begin{aligned} F \quad = \quad & \forall x P(x, f(x)) \wedge \\ & \forall y \neg P(y, y) \wedge \\ & \forall u \forall v \forall w ((P(u, v) \wedge P(v, w)) \Rightarrow P(u, w)) \end{aligned}$$

Dann ist z.B. mit $\mathcal{A} = (U, I)$, wobei $U = \mathbb{N}$, $I(P) = \{(m, n) \mid m < n\}$ und $I(f)(n) = n + 1$ eine erfüllende Struktur gegeben.

Eine besondere Formel

In der Aussagenlogik kann man Wahrheitstafeln aufmalen. In der Prädikatenlogik existieren unendlich viele Strukturen. Die Lage ist aber noch schlimmer:

Eine besondere Formel

Sei

$$\begin{aligned} F \quad = \quad & \forall x P(x, f(x)) \wedge \\ & \forall y \neg P(y, y) \wedge \\ & \forall u \forall v \forall w ((P(u, v) \wedge P(v, w)) \Rightarrow P(u, w)) \end{aligned}$$

Dann ist z.B. mit $\mathcal{A} = (U, I)$, wobei $U = \mathbb{N}$, $I(P) = \{(m, n) \mid m < n\}$ und $I(f)(n) = n + 1$ eine erfüllende Struktur gegeben.

Eine besondere Formel

Eine besondere Formel

Sei

$$\begin{aligned} F \quad = \quad & \forall x P(x, f(x)) \wedge \\ & \forall y \neg P(y, y) \wedge \\ & \forall u \forall v \forall w((P(u, v) \wedge P(v, w)) \Rightarrow P(u, w)) \end{aligned}$$

F hat aber kein endliches Modell, d.h. U kann nicht endlich sein!

Idee: Angenommen U wäre endlich, betrachte für ein beliebiges $m \in U$ eine Folge $m_0, m_1, m_2, \ldots$, wobei $m_0 = m$ und $m_{i+1} = I(f)(m_i)$. Dann muss sich in dieser Folge ein Wert m_x das erste Mal wiederholen. Aus dem ersten und dritten Konjunkt folgt dann $(m_x, m_x) \in I(P)$, was dem zweiten Konjunkt widerspricht.

Eine besondere Formel

Eine besondere Formel

Sei

$$\begin{aligned} F \quad = \quad & \forall x P(x, f(x)) \wedge \\ & \forall y \neg P(y, y) \wedge \\ & \forall u \forall v \forall w((P(u, v) \wedge P(v, w)) \Rightarrow P(u, w)) \end{aligned}$$

F hat aber kein endliches Modell, d.h. U kann nicht endlich sein!
Idee: Angenommen U wäre endlich, betrachte für ein beliebiges $m \in U$ eine Folge $m_0, m_1, m_2, \ldots$, wobei $m_0 = m$ und $m_{i+1} = I(f)(m_i)$. Dann muss sich in dieser Folge ein Wert m_x das erste Mal wiederholen. Aus dem ersten und dritten Konjunkt folgt dann $(m_x, m_x) \in I(P)$, was dem zweiten Konjunkt widerspricht.

Eine besondere Formel

Eine besondere Formel

Sei

$$\begin{aligned} F \quad = \quad & \forall x P(x, f(x)) \wedge \\ & \forall y \neg P(y, y) \wedge \\ & \forall u \forall v \forall w((P(u, v) \wedge P(v, w)) \Rightarrow P(u, w)) \end{aligned}$$

F hat aber kein endliches Modell, d.h. U kann nicht endlich sein!
Idee: Angenommen U wäre endlich, betrachte für ein beliebiges $m \in U$ eine Folge $m_0, m_1, m_2, \ldots$, wobei $m_0 = m$ und $m_{i+1} = I(f)(m_i)$. Dann muss sich in dieser Folge ein Wert m_x das erste Mal wiederholen. Aus dem ersten und dritten Konjunkt folgt dann $(m_x, m_x) \in I(P)$, was dem zweiten Konjunkt widerspricht.

Eine besondere Formel

Eine besondere Formel

Sei

$$\begin{aligned} F \quad = \quad & \forall x P(x, f(x)) \wedge \\ & \forall y \neg P(y, y) \wedge \\ & \forall u \forall v \forall w((P(u, v) \wedge P(v, w)) \Rightarrow P(u, w)) \end{aligned}$$

F hat aber kein endliches Modell, d.h. U kann nicht endlich sein!
Idee: Angenommen U wäre endlich, betrachte für ein beliebiges $m \in U$ eine Folge $m_0, m_1, m_2, \ldots$, wobei $m_0 = m$ und $m_{i+1} = I(f)(m_i)$. Dann muss sich in dieser Folge ein Wert m_x das erste Mal wiederholen. Aus dem ersten und dritten Konjunkt folgt dann $(m_x, m_x) \in I(P)$, was dem zweiten Konjunkt widerspricht.

Eine besondere Formel

Eine besondere Formel

Sei

$$\begin{aligned} F \quad = \quad & \forall x P(x, f(x)) \wedge \\ & \forall y \neg P(y, y) \wedge \\ & \forall u \forall v \forall w((P(u, v) \wedge P(v, w)) \Rightarrow P(u, w)) \end{aligned}$$

F hat aber kein endliches Modell, d.h. U kann nicht endlich sein!
Idee: Angenommen U wäre endlich, betrachte für ein beliebiges $m \in U$ eine Folge $m_0, m_1, m_2, \ldots$, wobei $m_0 = m$ und $m_{i+1} = I(f)(m_i)$. Dann muss sich in dieser Folge ein Wert m_x das erste Mal wiederholen. Aus dem ersten und dritten Konjunkt folgt dann $(m_x, m_x) \in I(P)$, was dem zweiten Konjunkt widerspricht.

Merke

Ergebnis

Es gibt nicht nur unendlich viele Strukturen, es gibt auch Formeln, für die eine (erfüllende) Struktur ein unendlich großes Universum benötigt.

Unentscheidbarkeit

Tatsächlich ist die Lage noch viel schlimmer:

Satz (Satz von Church)

Das Gültigkeitsproblem der Prädikatenlogik (also das Problem gegeben eine Formel $F \in \mathcal{L}_{PL}$, ist F eine Tautologie?) ist unentscheidbar.

Beweis.

Wir wollen den Beweis hier nicht im Detail führen. Zunächst zeigt man dass das sogenannte Postsche Korrespondenzproblem:
Gegeben: endliche Folge $(x_1, y_1), \ldots, (x_k, y_k)$ mit $x_i, y_i \in \{0,1\}^+$.
Gesucht: eine Folge von Indizes $i_1, \ldots, i_n \in \{1, \ldots, k\}$, $n \geq 1$ mit $x_{i_1} x_{i_2} \ldots x_{i_n} = y_{i_1} y_{i_2} \ldots y_{i_n}$.
unentscheidbar ist. Dann reduziert man dies auf das Gültigkeitsproblem der Prädikatenlogik. □

Unentscheidbarkeit

Tatsächlich ist die Lage noch viel schlimmer:

Satz (Satz von Church)

Das Gültigkeitsproblem der Prädikatenlogik (also das Problem gegeben eine Formel $F \in \mathcal{L}_{PL}$, ist F eine Tautologie?) ist unentscheidbar.

Beweis.

Wir wollen den Beweis hier nicht im Detail führen. Zunächst zeigt man dass das sogenannte Postsche Korrespondenzproblem:
Gegeben: endliche Folge $(x_1, y_1), \ldots, (x_k, y_k)$ mit $x_i, y_i \in \{0,1\}^+$.
Gesucht: eine Folge von Indizes $i_1, \ldots, i_n \in \{1, \ldots, k\}$, $n \geq 1$ mit $x_{i_1} x_{i_2} \ldots x_{i_n} = y_{i_1} y_{i_2} \ldots y_{i_n}$.
unentscheidbar ist. Dann reduziert man dies auf das Gültigkeitsproblem der Prädikatenlogik. □

Unentscheidbarkeit

Tatsächlich ist die Lage noch viel schlimmer:

Satz (Satz von Church)

Das Gültigkeitsproblem der Prädikatenlogik (also das Problem gegeben eine Formel $F \in \mathcal{L}_{PL}$, ist F eine Tautologie?) ist unentscheidbar.

Beweis.

Wir wollen den Beweis hier nicht im Detail führen. Zunächst zeigt man dass das sogenannte Postsche Korrespondenzproblem:
Gegeben: endliche Folge $(x_1, y_1), \ldots, (x_k, y_k)$ mit $x_i, y_i \in \{0,1\}^+$.
Gesucht: eine Folge von Indizes $i_1, \ldots, i_n \in \{1, \ldots, k\}$, $n \geq 1$ mit $x_{i_1} x_{i_2} \ldots x_{i_n} = y_{i_1} y_{i_2} \ldots y_{i_n}$.
unentscheidbar ist. Dann reduziert man dies auf das Gültigkeitsproblem der Prädikatenlogik. □

Unentscheidbarkeit

Satz

Das Erfüllbarkeitsproblem der Prädikatenlogik (also der Problem gegeben eine Formel $F \in \mathcal{L}_{PL}$, ist F erfüllbar?) ist unentscheidbar.

Beweis.

F ist gültig genau dann, wenn $\neg F$ unerfüllbar ist. Könnten wir also Erfüllbarkeit entscheiden, so könnten wir das Verfahren auf $\neg F$ anwenden und damit entscheiden, ob F gültig ist. (Aus dem vorherigen Satz wissen wir aber, dass wir dies nicht entscheiden können, also auch Erfüllbarkeit nicht.) □

Unentscheidbarkeit

Satz

Das Erfüllbarkeitsproblem der Prädikatenlogik (also der Problem gegeben eine Formel $F \in \mathcal{L}_{PL}$, ist F erfüllbar?) ist unentscheidbar.

Beweis.

F ist gültig genau dann, wenn $\neg F$ unerfüllbar ist. Könnten wir also Erfüllbarkeit entscheiden, so könnten wir das Verfahren auf $\neg F$ anwenden und damit entscheiden, ob F gültig ist. (Aus dem vorherigen Satz wissen wir aber, dass wir dies nicht entscheiden können, also auch Erfüllbarkeit nicht.) □

Motivation

Ein bisschen Hoffnung ...

Auch wenn das Erfüllbarkeitsproblem unentscheidbar ist, heißt das nicht, dass es nicht sinnvolle Verfahren geben kann, um zu ermitteln, ob eine Formel F erfüllbar ist. Das Verfahren würde die Frage nur nicht entscheiden. Vielleicht gibt das Verfahren nicht immer die richtige Lösung aus, oder es terminiert nicht immer ...

Ein Problem ist nun, dass für U beliebige Mengen möglich sind. Kann man dies einschränken? Kann man Strukturen "griffiger" machen, so dass man sie auf bestimmte Art und Weise durchwandern kann? ...

Motivation

Ein bisschen Hoffnung ...

Auch wenn das Erfüllbarkeitsproblem unentscheidbar ist, heißt das nicht, dass es nicht sinnvolle Verfahren geben kann, um zu ermitteln, ob eine Formel F erfüllbar ist. Das Verfahren würde die Frage nur nicht entscheiden. Vielleicht gibt das Verfahren nicht immer die richtige Lösung aus, oder es terminiert nicht immer ...

Ein Problem ist nun, dass für U beliebige Mengen möglich sind. Kann man dies einschränken? Kann man Strukturen "griffiger" machen, so dass man sie auf bestimmte Art und Weise durchwandern kann? ...

Herbrand-Universum

Definition (Herbrand-Universum)

Sei F eine geschlossene Formel in Skolemform. Das Herbrand-Universum $D(F)$ wird wie folgt induktiv gebildet:

1. Alle in F vorkommenden Konstanten sind in $D(F)$. Enthält F keine Konstanten, so sei die neue Konstante a in $D(F)$.
2. Für jedes in F vorkommende k-stellige Funktionssymbol f und Terme $t_1, \ldots, t_k \in D(F)$ ist auch $f(t_1, \ldots, t_k) \in D(F)$.

Anmerkung

In $D(F)$ sind also alle variablenfreien Terme, die aus Bestandteilen von F gebildet werden können.

Herbrand-Universum

Definition (Herbrand-Universum)

Sei F eine geschlossene Formel in Skolemform. Das Herbrand-Universum $D(F)$ wird wie folgt induktiv gebildet:

1. Alle in F vorkommenden Konstanten sind in $D(F)$. Enthält F keine Konstanten, so sei die neue Konstante a in $D(F)$.
2. Für jedes in F vorkommende k-stellige Funktionssymbol f und Terme $t_1, \ldots, t_k \in D(F)$ ist auch $f(t_1, \ldots, t_k) \in D(F)$.

Anmerkung

In $D(F)$ sind also alle variablenfreien Terme, die aus Bestandteilen von F gebildet werden können.

Herbrand-Universum - Beispiel

Beispiel

Sei

$$\begin{aligned} F &= \forall x \forall y P(x, f(y), c) \\ G &= \forall x \forall y P(f(x), b, g(x, y)) \\ H &= \forall x P(f(x, x)) \end{aligned}$$

Dann ist

$$\begin{aligned} D(F) &= \{c, f(c), f(f(c)), f(f(f(c))), \ldots\} \\ D(G) &= \{b, f(b), g(b, b), f(f(b)), f(g(b, b)), \\ &\quad g(b, f(b)), g(f(b), b), g(b, g(b, b)), \\ &\quad g(g(b, b), b), g(f(b), g(b, b)), \ldots\} \\ D(H) &= \{a, f(a, a), \\ &= f(a, f(a, a)), f(f(a, a), a), f(f(a, a), f(a, a)), \ldots\} \end{aligned}$$

Herbrand-Universum - Beispiel

Beispiel

Sei

$$\begin{aligned} F &= \forall x \forall y P(x, f(y), c) \\ G &= \forall x \forall y P(f(x), b, g(x, y)) \\ H &= \forall x P(f(x, x)) \end{aligned}$$

Dann ist

$$\begin{aligned} D(F) &= \{c, f(c), f(f(c)), f(f(f(c))), \ldots\} \\ D(G) &= \{b, f(b), g(b, b), f(f(b)), f(g(b, b)), \\ &\quad g(b, f(b)), g(f(b), b), g(b, g(b, b)), \\ &\quad g(g(b, b), b), g(f(b), g(b, b)), \ldots\} \\ D(H) &= \{a, f(a, a), \\ &= f(a, f(a, a)), f(f(a, a), a), f(f(a, a), f(a, a)), \ldots\} \end{aligned}$$

Motivation

Anmerkung

$D(F)$ wird nun als 'Standard'-Grundbereich benutzt, um nach Modellen zu suchen. Dies reicht tatsächlich und hilft uns auf gewisse Art und Weise nach Modellen zu suchen.

Herbrand-Struktur und -Modell

Definition (Herbrand-Struktur und -Modell)

Sei F eine geschlossene Formel in Skolemform. Dann heißt $\mathcal{A} = (U, I)$ **Herbrand-Struktur** zu F, wenn:

1. $U = D(F)$
2. Für jedes in F auftretende k-stellige Funktionssymbol f und Terme $t_1, \ldots, t_k \in D(F)$ ist $I(f)(t_1, \ldots, t_k) = f(t_1, \ldots, t_k)$.

Ist eine Herbrand-Struktur $\mathcal{A}$ ein Modell für eine Formel F, so nennen wir $\mathcal{A}$ ein **Herbrand-Modell**.

Anmerkungen

Anmerkung

Zwei Anmerkungen:

1. Durch die Festlegung der Interpretation der Funktionssymbole wird Syntax und Semantik von Termen quasi gleichgeschaltet. Die Bedeutung (Semantik) eines Terms ist der Term (syntaktisch) selbst.
2. Die Definition der Herbrand-Struktur legt viel fest. Offen ist aber dann noch die Interpretation der Prädikatensymbole. Dies schränkt einen ein und hilft, die Suche nach erfüllenden Strukturen zu vereinfachen. (Das Erfüllbarkeitsproblem der Prädikatenlogik bleibt aber unentscheidbar!)

Anmerkungen

Anmerkung

Zwei Anmerkungen:

1. Durch die Festlegung der Interpretation der Funktionssymbole wird Syntax und Semantik von Termen quasi gleichgeschaltet. Die Bedeutung (Semantik) eines Terms ist der Term (syntaktisch) selbst.
2. Die Definition der Herbrand-Struktur legt viel fest. Offen ist aber dann noch die Interpretation der Prädikatensymbole. Dies schränkt einen ein und hilft, die Suche nach erfüllenden Strukturen zu vereinfachen. (Das Erfüllbarkeitsproblem der Prädikatenlogik bleibt aber unentscheidbar!)

Abzählbare Modelle

Man kann nun folgende Sätze zeigen:

Satz

Sei F eine geschlossene Formel in Skolemform. F ist genau dann erfüllbar, wenn F ein Herbrand-Modell besitzt.

Satz (Satz von Löwenheim-Skolem)

Jede erfüllbare Formel der Prädikatenlogik besitzt ein abzählbares Modell (eine Struktur mit abzählbarem Universum).

Beweis.

Folgt sofort aus obigem, da Herbrand-Modelle abzählbar sind. □

Abzählbare Modelle

Man kann nun folgende Sätze zeigen:

Satz

Sei F eine geschlossene Formel in Skolemform. F ist genau dann erfüllbar, wenn F ein Herbrand-Modell besitzt.

Satz (Satz von Löwenheim-Skolem)

Jede erfüllbare Formel der Prädikatenlogik besitzt ein abzählbares Modell (eine Struktur mit abzählbarem Universum).

Beweis.

Folgt sofort aus obigem, da Herbrand-Modelle abzählbar sind. □

Abzählbare Modelle

Wichtige Anmerkung

Wenn wir zu Anfang gezeigt haben, dass einige Formeln der Prädikatenlogik unendlich große Strukturen benötigen, so wissen wir nun immerhin, dass Strukturen mit abzählbar unendlichen Universen ausreichend sind!

Herbrand-Expansion - Motivation

Nächstes Ziel

Man kann dies nun nutzen, um ein Verfahren zu entwickeln, dass systematisch alle Strukturen (bzw. bestimmte Strukturen) durchgeht und irgendwann eine erfüllende findet, sofern denn eine existiert.

Dies widerspricht nicht der Unentscheidbarkeit der Prädikatenlogik!
Das gleich vorgestellte Verfahren muss nämlich nicht terminieren!

Herbrand-Expansion - Motivation

Nächstes Ziel

Man kann dies nun nutzen, um ein Verfahren zu entwickeln, dass systematisch alle Strukturen (bzw. bestimmte Strukturen) durchgeht und irgendwann eine erfüllende findet, sofern denn eine existiert.

Dies widerspricht nicht der Unentscheidbarkeit der Prädikatenlogik!
Das gleich vorgestellte Verfahren muss nämlich nicht terminieren!

Herbrand-Expansion - Motivation

Nächstes Ziel

Man kann dies nun nutzen, um ein Verfahren zu entwickeln, dass systematisch alle Strukturen (bzw. bestimmte Strukturen) durchgeht und irgendwann eine erfüllende findet, sofern denn eine existiert.

Dies widerspricht nicht der Unentscheidbarkeit der Prädikatenlogik! Das gleich vorgestellte Verfahren muss nämlich nicht terminieren!

Herbrand-Expansion

Definition (Herbrand-Expansion)

Sei $F = \forall y_1 \ldots \forall y_k F^*$ eine Aussagen in Skolemform (F^* ist die Matrix). Dann ist

$$E(F) := \{F^*[y_1/t_1][y_2/t_2]\ldots[y_k/t_k] \mid t_1, \ldots, t_k \in D(F)\}$$

die **Herbrand-Expansion** von F.

Anmerkung

Die Formeln in $E(F)$ sind quasi wie aussagenlogische Formeln!

Herbrand-Expansion

Definition (Herbrand-Expansion)

Sei $F = \forall y_1 \ldots \forall y_k F^*$ eine Aussagen in Skolemform (F^* ist die Matrix). Dann ist

$$E(F) := \{F^*[y_1/t_1][y_2/t_2]\ldots[y_k/t_k] \mid t_1, \ldots, t_k \in D(F)\}$$

die **Herbrand-Expansion** von F.

Anmerkung

Die Formeln in $E(F)$ sind quasi wie aussagenlogische Formeln!

Ein Satz

Satz (Gödel-Herbrand-Skolem)

Für jede geschlossene Formel in Skolemform F gilt: F ist genau dann erfüllbar, wenn die Formelmenge $E(F)$ im aussagenlogischen Sinne erfüllbar ist.

Anmerkung

Der Satz besagt quasi, dass eine prädikatenlogische Formel durch (i.A.) unendlich viele aussagenlogische Formeln approximiert werden kann.

Ein Satz

Satz (Gödel-Herbrand-Skolem)

Für jede geschlossene Formel in Skolemform F gilt: F ist genau dann erfüllbar, wenn die Formelmenge $E(F)$ im aussagenlogischen Sinne erfüllbar ist.

Anmerkung

Der Satz besagt quasi, dass eine prädikatenlogische Formel durch (i.A.) unendlich viele aussagenlogische Formeln approximiert werden kann.

Noch ein Satz

In Kombination mit dem Endlichkeitssatz der Aussagenlogik:

Satz (Endlichkeitssatz (der Aussagenlogik))

Eine Menge M von Formeln ist genau dann erfüllbar, wenn jede endliche Teilmenge von M erfüllbar ist.

ergibt dies den folgenden Satz von Herbrand:

Satz (Herbrand)

Eine Aussage F in Skolemform ist genau dann unerfüllbar, wenn es eine endliche Teilmenge von $E(F)$ gibt, die (im aussagenlogischen Sinne) unerfüllbar ist.

Noch ein Satz

In Kombination mit dem Endlichkeitssatz der Aussagenlogik:

Satz (Endlichkeitssatz (der Aussagenlogik))

Eine Menge M von Formeln ist genau dann erfüllbar, wenn jede endliche Teilmenge von M erfüllbar ist.

ergibt dies den folgenden Satz von Herbrand:

Satz (Herbrand)

Eine Aussage F in Skolemform ist genau dann unerfüllbar, wenn es eine endliche Teilmenge von $E(F)$ gibt, die (im aussagenlogischen Sinne) unerfüllbar ist.

Zum Algorithmus von Gilmore

Aus dem Satz von Herbrand lässt sich ein Algorithmus entwickeln, der überprüft, ob eine prädikatenlogische Formel unerfüllbar ist.

ABER: Prädikatenlogik ist unentscheidbar, also hat der Algorithmus irgendeinen Haken. In diesem Fall: Er terminiert nicht zwingend!

Anmerkung

Man spricht hier von einem Semi-Entscheidungsverfahren. Auf den 'Ja'-Instanzen halten wir nach endlicher Zeit mit der korrekten Antwort an. (Bei den 'Nein'-Instanzen wissen wir aber immer nicht, ob das 'Ja' noch kommt oder ob diese eine 'Nein'-Instanz ist...)

Zum Algorithmus von Gilmore

Aus dem Satz von Herbrand lässt sich ein Algorithmus entwickeln, der überprüft, ob eine prädikatenlogische Formel unerfüllbar ist.

ABER: Prädikatenlogik ist unentscheidbar, also hat der Algorithmus irgendeinen Haken. In diesem Fall: Er terminiert nicht zwingend!

Anmerkung

Man spricht hier von einem Semi-Entscheidungsverfahren. Auf den 'Ja'-Instanzen halten wir nach endlicher Zeit mit der korrekten Antwort an. (Bei den 'Nein'-Instanzen wissen wir aber immer nicht, ob das 'Ja' noch kommt oder ob diese eine 'Nein'-Instanz ist...)

Der Algorithmus von Gilmore

Der Algorithmus von Gilmore arbeitet wie folgt:

1. Sei $F_1, F_2, F_3, \ldots$ eine Aufzählung von $E(F)$.
2. Eingabe ist eine prädikatenlogische Formel F in Skolemform.
3. $n = 0$
4. $n = n + 1$
5. Prüfe, ob $(F_1 \wedge F_2 \wedge \ldots \wedge F_n)$ unerfüllbar ist (z.B. mit Wahrheitstafeln der Aussagenlogik).
6. Falls ja, stoppe und gib 'unerfüllbar' aus. Falls nein, gehe zu Schritt 4.

Folgerungen aus dem Algorithmus

Wir haben damit ein Semi-Entscheidungsverfahren

- für das Unerfüllbarkeitsproblem
- für das Gültigkeitsproblem

Ferner könnte man systematisch endliche Modelle durchgehen und hätte dann auch ein Semi-Entscheidungsverfahren für

- erfüllbare Formeln mit endlichen Modellen

Die erfüllbaren, aber nicht gültigen Formeln mit unendlichen Modellen bleiben einem aber verwehrt! Und bei den obigen Verfahren weiß man bei Nicht-Termination immer nicht, ob noch eine Antwort kommt oder ob dies eine 'Nein'-Instanz ist!

Folgerungen aus dem Algorithmus

Wir haben damit ein Semi-Entscheidungsverfahren

- für das Unerfüllbarkeitsproblem
- für das Gültigkeitsproblem

Ferner könnte man systematisch endliche Modelle durchgehen und hätte dann auch ein Semi-Entscheidungsverfahren für

- erfüllbare Formeln mit endlichen Modellen

Die erfüllbaren, aber nicht gültigen Formeln mit unendlichen Modellen bleiben einem aber verwehrt! Und bei den obigen Verfahren weiß man bei Nicht-Termination immer nicht, ob noch eine Antwort kommt oder ob dies eine 'Nein'-Instanz ist!

Folgerungen aus dem Algorithmus

Wir haben damit ein Semi-Entscheidungsverfahren

- für das Unerfüllbarkeitsproblem
- für das Gültigkeitsproblem

Ferner könnte man systematisch endliche Modelle durchgehen und hätte dann auch ein Semi-Entscheidungsverfahren für

- erfüllbare Formeln mit endlichen Modellen

Die erfüllbaren, aber nicht gültigen Formeln mit unendlichen Modellen bleiben einem aber verwehrt! Und bei den obigen Verfahren weiß man bei Nicht-Termination immer nicht, ob noch eine Antwort kommt oder ob dies eine 'Nein'-Instanz ist!

Motivation

Statt wie im Algorithmus eben angedeutet Wahrheitstafeln für den Unerfüllbarkeitstest zu benutzen, können wir auch auf **(aussagenlogische) Resolution** zurückgreifen. Die Matrix muss dafür in KNF gebracht werden, aber das können wir ja ....

Grundresolutionsalgorithmus

Es sei wieder $F_1, F_2, \ldots$ eine Aufzählung von $E(F)$. Der **Grundresolutionsalgorithmus** arbeitet wie folgt:

1. Eingabe ist eine Aussage F in Skolemform mit der Matrix F^* in KNF.
2. $i = 0$
3. $M = \emptyset$
4. Wiederhole:
   - $i = i + 1$
   - $M = M \cup \{F_i\}$
   - $M = Res^*(M)$

   bis $\square \in M$.
5. Gib 'unerfüllbar' aus und stoppe.

Begriffe

Die Bezeichnung **Grundresolutionsalgorithmus** kommt von folgenden Begriffen:

Definition

Sei F eine Formel in Skolemform mit Matrix F^*.

- Eine Substitution, die alle freien Variablen in F durch variablenfreie Terme ersetzt wird **Grundsubstitution** genannt. (Die Substitutionen in der Definition von $E(F)$ sind also Grundsubstitutionen.)
- Wenn alle freien Variablen in F^* durch eine Grundsubstitution ersetzt werden, nennen wir das Resultat eine **Grundinstanz** von F^*.
- Werden die freien Variablen in F^* durch eine Substitution ersetzt, so nennen wir das Resultat eine **Instanz** von F^*.

Begriffe

Die Bezeichnung **Grundresolutionsalgorithmus** kommt von folgenden Begriffen:

Definition

Sei F eine Formel in Skolemform mit Matrix F^*.

- Eine Substitution, die alle freien Variablen in F durch variablenfreie Terme ersetzt wird **Grundsubstitution** genannt. (Die Substitutionen in der Definition von $E(F)$ sind also Grundsubstitutionen.)
- Wenn alle freien Variablen in F^* durch eine Grundsubstitution ersetzt werden, nennen wir das Resultat eine **Grundinstanz** von F^*.
- Werden die freien Variablen in F^* durch eine Substitution ersetzt, so nennen wir das Resultat eine **Instanz** von F^*.

Begriffe

Die Bezeichnung **Grundresolutionsalgorithmus** kommt von folgenden Begriffen:

Definition

Sei F eine Formel in Skolemform mit Matrix F^*.

- Eine Substitution, die alle freien Variablen in F durch variablenfreie Terme ersetzt wird **Grundsubstitution** genannt. (Die Substitutionen in der Definition von $E(F)$ sind also Grundsubstitutionen.)
- Wenn alle freien Variablen in F^* durch eine Grundsubstitution ersetzt werden, nennen wir das Resultat eine **Grundinstanz** von F^*.
- Werden die freien Variablen in F^* durch eine Substitution ersetzt, so nennen wir das Resultat eine **Instanz** von F^*.

Zum Grundresolutionsalgorithmus

Satz

Bei Eingabe einer Aussage F in Skolemform mit Matrix F^* in KNF stoppt der Grundresolutionsalgorithmus genau dann nach endlich vielen Schritten mit der Ausgabe 'unerfüllbar', wenn F unerfüllbar ist.

Anmerkung

Der Algorithmus erzeugt meist viel mehr Elemente in M als nötig. Bei der Darstellung eines Beweises für die Unerfüllbarkeit genügt es geeignete Grundinstanzen der Klauseln in F^* anzugeben und diese dann in einem Resolutionsgraphen zur leeren Klausel zu resolvieren.

Zum Grundresolutionsalgorithmus

Satz

Bei Eingabe einer Aussage F in Skolemform mit Matrix F^* in KNF stoppt der Grundresolutionsalgorithmus genau dann nach endlich vielen Schritten mit der Ausgabe 'unerfüllbar', wenn F unerfüllbar ist.

Anmerkung

Der Algorithmus erzeugt meist viel mehr Elemente in M als nötig. Bei der Darstellung eines Beweises für die Unerfüllbarkeit genügt es geeignete Grundinstanzen der Klauseln in F^* anzugeben und diese dann in einem Resolutionsgraphen zur leeren Klausel zu resolvieren.

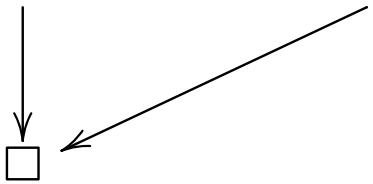
Beispiel

Zur Formel

$$F = \forall x(P(x) \wedge \neg P(f(x)))$$

genügen bereits die Substitutionen $[x/a]$ und $[x/f(a)]$ um zu einer unerfüllbaren Klauselmenge zu kommen:

$\{P(a)\}$ $\{\neg P(f(a))\}$ $\{P(f(a))\}$ $\{\neg P(f(f(a)))\}$



Anmerkung

Genauer gengügt es sogar für jede Klausel in F^* individuell geeignete Substitutionen zu finden, die dann auf diese Klausel aber nicht auf die ganze Klauselmenge F^* angewendet werden.

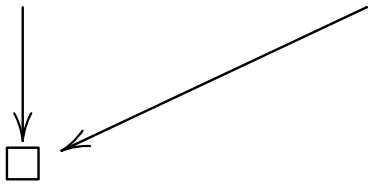
Beispiel

Zur Formel

$$F = \forall x(P(x) \wedge \neg P(f(x)))$$

genügen bereits die Substitutionen $[x/a]$ und $[x/f(a)]$ um zu einer unerfüllbaren Klauselmenge zu kommen:

$\{P(a)\}$ $\{\neg P(f(a))\}$ $\{P(f(a))\}$ $\{\neg P(f(f(a)))\}$



Anmerkung

Genauer gengügt es sogar für jede Klausel in F^* individuell geeignete Substitutionen zu finden, die dann auf diese Klausel aber nicht auf die ganze Klauselmenge F^* angewendet werden.

Motivation

Motivation

Wenn man einige Grundsubstitutionen macht, merkt man recht schnell, dass man sich oft durch eine (Grund-)Substitution zu schnell einschränkt (und dadurch zu vorausschauend arbeiten muss). Ziel ist es daher in einer Weise zu substituieren, dass man nicht mehr als nötig substitutiert und insb. nicht mehr als nötig geschlossene Terme einführt.

Hat man z.B. $\{P(x), \neg Q(g(x))\}$ und $\{\neg P(f(y))\}$, so würde die Substitution $[x/f(y)]$ genügen, um zu $\{\neg Q(g(f(y)))\}$ zu resolvieren. Mit dem bisherigen geht das aber nicht. In der prädikatenlogischen Resolution will man genau dies erlauben. Um die formal auszudrücken brauchen wir noch den Begriff der Unifikation...

Motivation

Motivation

Wenn man einige Grundsubstitutionen macht, merkt man recht schnell, dass man sich oft durch eine (Grund-)Substitution zu schnell einschränkt (und dadurch zu vorausschauend arbeiten muss). Ziel ist es daher in einer Weise zu substituieren, dass man nicht mehr als nötig substitutiert und insb. nicht mehr als nötig geschlossene Terme einführt.
Hat man z.B. $\{P(x), \neg Q(g(x))\}$ und $\{\neg P(f(y))\}$, so würde die Substitution $[x/f(y)]$ genügen, um zu $\{\neg Q(g(f(y)))\}$ zu resolvieren. Mit dem bisherigen geht das aber nicht. In der prädikatenlogischen Resolution will man genau dies erlauben. Um die formal auszudrücken brauchen wir noch den Begriff der Unifikation...

Motivation

Motivation

Wenn man einige Grundsubstitutionen macht, merkt man recht schnell, dass man sich oft durch eine (Grund-)Substitution zu schnell einschränkt (und dadurch zu vorausschauend arbeiten muss). Ziel ist es daher in einer Weise zu substituieren, dass man nicht mehr als nötig substitutiert und insb. nicht mehr als nötig geschlossene Terme einführt.
Hat man z.B. $\{P(x), \neg Q(g(x))\}$ und $\{\neg P(f(y))\}$, so würde die Substitution $[x/f(y)]$ genügen, um zu $\{\neg Q(g(f(y)))\}$ zu resolvieren. Mit dem bisherigen geht das aber nicht. In der prädikatenlogischen Resolution will man genau dies erlauben. Um die formal auszudrücken brauchen wir noch den Begriff der Unifikation...

Unifikator

Definition (Unifikator)

Eine Substitution σ ist ein **Unifikator** einer endlichen Menge von Literalen $L = \{L_1, \ldots, L_k\}$, wenn $L_1\sigma = \ldots = L_k\sigma$, wenn also $|L\sigma| = 1$. Wir sagen dann, dass L unifizierbar ist.

σ heißt **allgemeinster Unifikator** von L, falls für jeden Unifikator σ' von L gilt, dass es eine Substitution *sub* gibt mit $\sigma' = \sigma sub$, d.h. wenn für jede Formel F $F\sigma' = F\sigma sub$ gilt.

Unifikator

Definition (Unifikator)

Eine Substitution σ ist ein **Unifikator** einer endlichen Menge von Literalen $L = \{L_1, \ldots, L_k\}$, wenn $L_1\sigma = \ldots = L_k\sigma$, wenn also $|L\sigma| = 1$. Wir sagen dann, dass L unifizierbar ist.
σ heißt **allgemeinster Unifikator** von L, falls für jeden Unifikator σ' von L gilt, dass es eine Substitution sub gibt mit $\sigma' = \sigma sub$, d.h. wenn für jede Formel F $F\sigma' = F\sigma sub$ gilt.

Unifikationsalgorithmus

Satz (Unifikationssatz)

Jede unifizierbare Menge von Literalen besitzt auch einen allgemeinsten Unifikator.

Beweis.

Der nachfolgende Unifikationsalgorithmus ermittelt einen allgemeinsten Unifikator sofern einer existiert und gibt sonst aus, dass die Menge nicht unifizierbar ist.
Einen detaillierten Korrektheitsbeweis findet man im Buch von Schöning. □

Unifikationsalgorithmus

Eingabe: nicht-leere Literalmenge L.

- sub = []
- Wiederhole so lange $|Lsub| > 1$:
  - Wandere von links nach rechts durch die Literale in $Lsub$ bis die erste Position gefunden wird an der sich mindestens zwei Literale unterscheiden
  - Ist keines der beiden eine Variable brich mit 'nicht unifizierbar' ab.
  - sonst sei x die Variable t der Term
  - Kommt x in t vor, brich mit 'nicht unifizierbar' ab.
  - sonst setze $sub = sub[x/t]$ und fahre fort
- Gib sub aus

Unifikation - Beispiel

Beispiel

Sei

$$L = \{P(x, y), P(f(a), g(x)), P(f(z), g(f(z)))\}$$

dann

1. erster Unterschied bei x und $f(a)$, also $sub_1 = [x/f(a)]$ (oder x und $f(z)$ dann $sub = [x/f(z)]$)
   - $Lsub_1 = \{P(f(a), y), P(f(a), g(f(a))), P(f(z), g(f(z)))\}$
2. nächster Unterschied bei z und a, also $sub_2 = sub_1[z/a]$
   - $Lsub_2 = \{P(f(a), y), P(f(a), g(f(a)))\}$
3. nächster Unterschied bei y und $g(f(a))$, also $sub_3 = sub_2[y/g(f(a))]$
   - $Lsub_3 = \{P(f(a), g(f(a)))\}$

   und wir sind fertig!

Der allgemeinste Unifikator ist $\sigma = [x/f(a)][z/a][y/g(f(a))]$.

Unifikation - Beispiel

Beispiel

Sei

$$L = \{P(x, y), P(f(a), g(x)), P(f(z), g(f(z)))\}$$

dann

1. erster Unterschied bei x und $f(a)$, also $sub_1 = [x/f(a)]$ (oder x und $f(z)$ dann $sub = [x/f(z)]$)
   - $Lsub_1 = \{P(f(a), y), P(f(a), g(f(a))), P(f(z), g(f(z)))\}$
2. nächster Unterschied bei z und a, also $sub_2 = sub_1[z/a]$
   - $Lsub_2 = \{P(f(a), y), P(f(a), g(f(a)))\}$
3. nächster Unterschied bei y und $g(f(a))$, also $sub_3 = sub_2[y/g(f(a))]$
   - $Lsub_3 = \{P(f(a), g(f(a)))\}$

   und wir sind fertig!

Der allgemeinste Unifikator ist $\sigma = [x/f(a)][z/a][y/g(f(a))]$.

Unifikation - Beispiel

Beispiel

Sei

$$L = \{P(x, y), P(f(a), g(x)), P(f(z), g(f(z)))\}$$

dann

1. erster Unterschied bei x und $f(a)$, also $sub_1 = [x/f(a)]$ (oder x und $f(z)$ dann $sub = [x/f(z)]$)
   - $Lsub_1 = \{P(f(a), y), P(f(a), g(f(a))), P(f(z), g(f(z)))\}$
2. nächster Unterschied bei z und a, also $sub_2 = sub_1[z/a]$
   - $Lsub_2 = \{P(f(a), y), P(f(a), g(f(a)))\}$
3. nächster Unterschied bei y und $g(f(a))$, also $sub_3 = sub_2[y/g(f(a))]$
   - $Lsub_3 = \{P(f(a), g(f(a)))\}$

   und wir sind fertig!

Der allgemeinste Unifikator ist $\sigma = [x/f(a)][z/a][y/g(f(a))]$.

Unifikation - Beispiel

Beispiel

Sei

$$L = \{P(x, y), P(f(a), g(x)), P(f(z), g(f(z)))\}$$

dann

1. erster Unterschied bei x und $f(a)$, also $sub_1 = [x/f(a)]$ (oder x und $f(z)$ dann $sub = [x/f(z)]$)
   - $Lsub_1 = \{P(f(a), y), P(f(a), g(f(a))), P(f(z), g(f(z)))\}$
2. nächster Unterschied bei z und a, also $sub_2 = sub_1[z/a]$
   - $Lsub_2 = \{P(f(a), y), P(f(a), g(f(a)))\}$
3. nächster Unterschied bei y und $g(f(a))$, also $sub_3 = sub_2[y/g(f(a))]$
   - $Lsub_3 = \{P(f(a), g(f(a)))\}$

   und wir sind fertig!

Der allgemeinste Unifikator ist $\sigma = [x/f(a)][z/a][y/g(f(a))]$.

Unifikation - Beispiel

Beispiel

Sei

$$L = \{P(x, y), P(f(a), g(x)), P(f(z), g(f(z)))\}$$

dann

1. erster Unterschied bei x und $f(a)$, also $sub_1 = [x/f(a)]$ (oder x und $f(z)$ dann $sub = [x/f(z)]$)
   - $Lsub_1 = \{P(f(a), y), P(f(a), g(f(a))), P(f(z), g(f(z)))\}$
2. nächster Unterschied bei z und a, also $sub_2 = sub_1[z/a]$
   - $Lsub_2 = \{P(f(a), y), P(f(a), g(f(a)))\}$
3. nächster Unterschied bei y und $g(f(a))$, also $sub_3 = sub_2[y/g(f(a))]$
   - $Lsub_3 = \{P(f(a), g(f(a)))\}$

   und wir sind fertig!

Der allgemeinste Unifikator ist $\sigma = [x/f(a)][z/a][y/g(f(a))]$.

Motivation

Mit der Unifikation können wir nun unser Ziel der 'zurückhaltenden' Resolution erreichen und die prädikatenlogische Resolution formulieren ...

Resolution

Definition (Prädikatenlogische Resolution)

Seien K_1, K_2 und R prädikatenlogische Klauseln. Dann ist R eine prädikatenlogische **Resolvente** von K_1 und K_2, falls folgendes gilt:

1. Es gibt Substitutionen s_1 und s_2, die Variablenumbenennungen sind, so dass $K_1 s_1$ und $K_2 s_2$ keine gemeinsamen Variablen enthalten.
2. Es gibt eine Menge von Literalen $L_1, \ldots, L_m \in K_1 s_1$ und $L'_1, \ldots, L'_n \in K_2 s_2$ (wobei $n, m \geq 1$), so dass $L = \{\overline{L_1}, \ldots, \overline{L_m}, L'_1, \ldots, L'_n\}$ unifizierbar ist. Sei sub der allgemeinste Unifikator von L.
3. R hat die Form

$$R = ((K_1 s_1 - \{L_1, \ldots, L_m\}) \cup (K_2 s_2 - \{L'_1, \ldots, L'_n\}))sub$$

Resolution

Definition (Prädikatenlogische Resolution)

Seien K_1, K_2 und R prädikatenlogische Klauseln. Dann ist R eine prädikatenlogische **Resolvente** von K_1 und K_2, falls folgendes gilt:

1. Es gibt Substitutionen s_1 und s_2, die Variablenumbenennungen sind, so dass $K_1 s_1$ und $K_2 s_2$ keine gemeinsamen Variablen enthalten.
2. Es gibt eine Menge von Literalen $L_1, \ldots, L_m \in K_1 s_1$ und $L'_1, \ldots, L'_n \in K_2 s_2$ (wobei $n, m \geq 1$), so dass $L = \{\overline{L_1}, \ldots, \overline{L_m}, L'_1, \ldots, L'_n\}$ unifizierbar ist. Sei *sub* der allgemeinste Unifikator von L.
3. R hat die Form

$$R = ((K_1 s_1 - \{L_1, \ldots, L_m\}) \cup (K_2 s_2 - \{L'_1, \ldots, L'_n\}))sub$$

Resolution

Definition (Prädikatenlogische Resolution)

Seien K_1, K_2 und R prädikatenlogische Klauseln. Dann ist R eine prädikatenlogische **Resolvente** von K_1 und K_2, falls folgendes gilt:

1. Es gibt Substitutionen s_1 und s_2, die Variablenumbenennungen sind, so dass $K_1 s_1$ und $K_2 s_2$ keine gemeinsamen Variablen enthalten.
2. Es gibt eine Menge von Literalen $L_1, \ldots, L_m \in K_1 s_1$ und $L'_1, \ldots, L'_n \in K_2 s_2$ (wobei $n, m \geq 1$), so dass $L = \{\overline{L_1}, \ldots, \overline{L_m}, L'_1, \ldots, L'_n\}$ unifizierbar ist. Sei *sub* der allgemeinste Unifikator von L.
3. R hat die Form

$$R = ((K_1 s_1 - \{L_1, \ldots, L_m\}) \cup (K_2 s_2 - \{L'_1, \ldots, L'_n\}))sub$$

Resolution

Definition (Prädikatenlogische Resolution)

Seien K_1, K_2 und R prädikatenlogische Klauseln. Dann ist R eine prädikatenlogische **Resolvente** von K_1 und K_2, falls folgendes gilt:

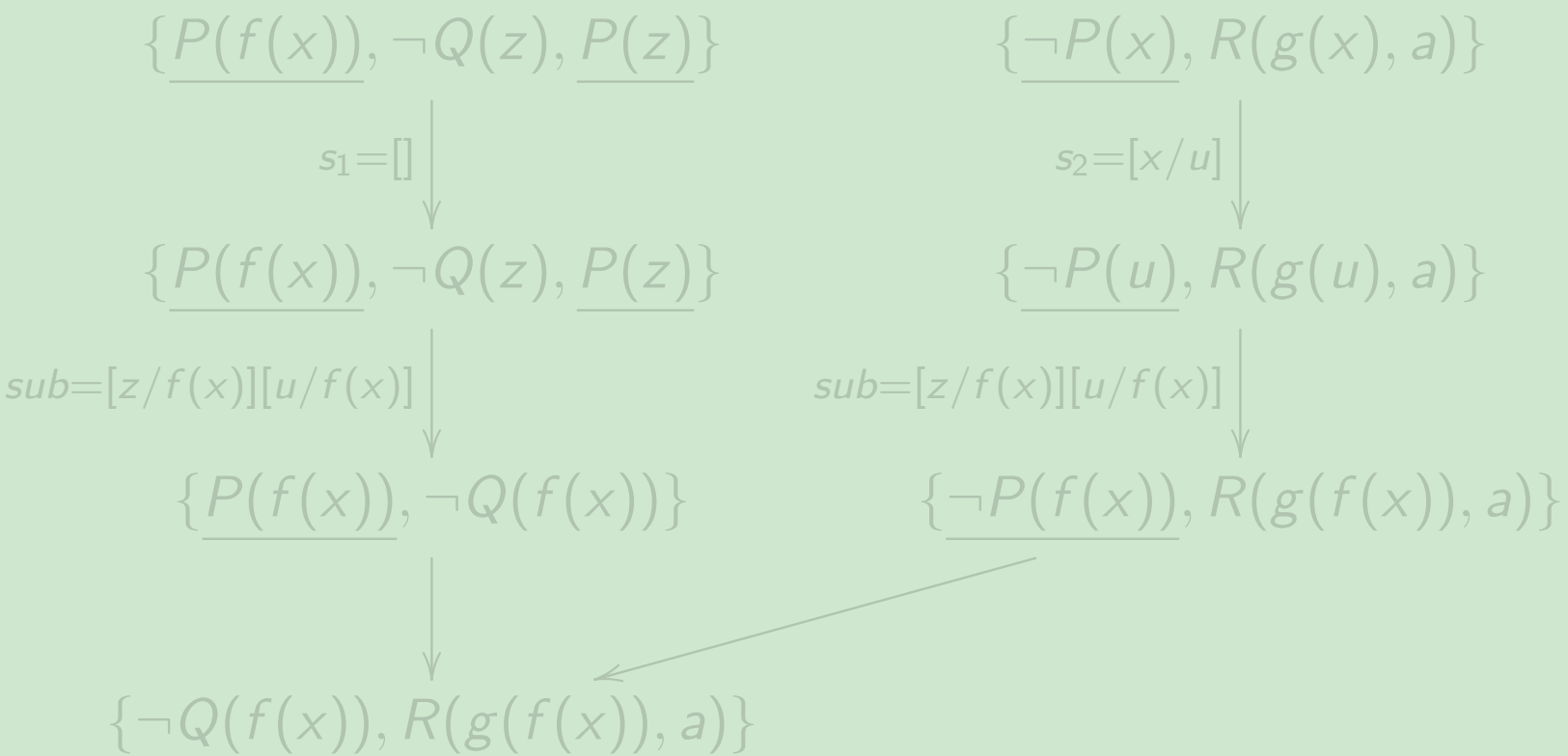
1. Es gibt Substitutionen s_1 und s_2, die Variablenumbenennungen sind, so dass $K_1 s_1$ und $K_2 s_2$ keine gemeinsamen Variablen enthalten.
2. Es gibt eine Menge von Literalen $L_1, \ldots, L_m \in K_1 s_1$ und $L'_1, \ldots, L'_n \in K_2 s_2$ (wobei $n, m \geq 1$), so dass $L = \{\overline{L_1}, \ldots, \overline{L_m}, L'_1, \ldots, L'_n\}$ unifizierbar ist. Sei sub der allgemeinste Unifikator von L.
3. R hat die Form

$$R = ((K_1 s_1 - \{L_1, \ldots, L_m\}) \cup (K_2 s_2 - \{L'_1, \ldots, L'_n\}))sub$$

Resolution - Beispiel 1

Beispiel

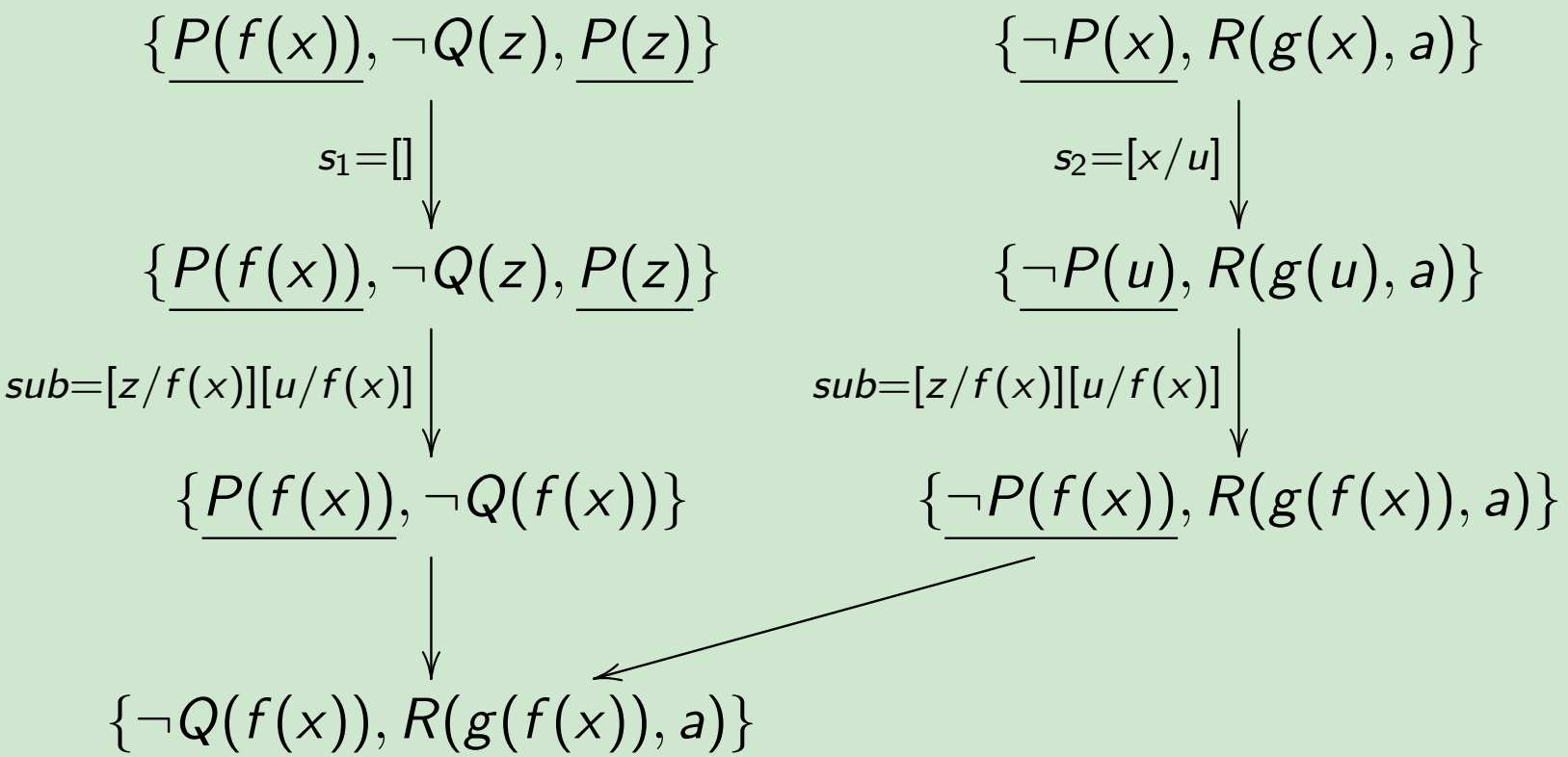
Sei $K_1 = \{P(f(x)), \neg Q(z), P(z)\}$ und $K_2 = \{\neg P(x), R(g(x), a)\}$
Wir wählen $P(f(x)), P(z) \in K_1$ und $\neg P(x) \in K_2$ zur Resolution aus. Damit:



Resolution - Beispiel 1

Beispiel

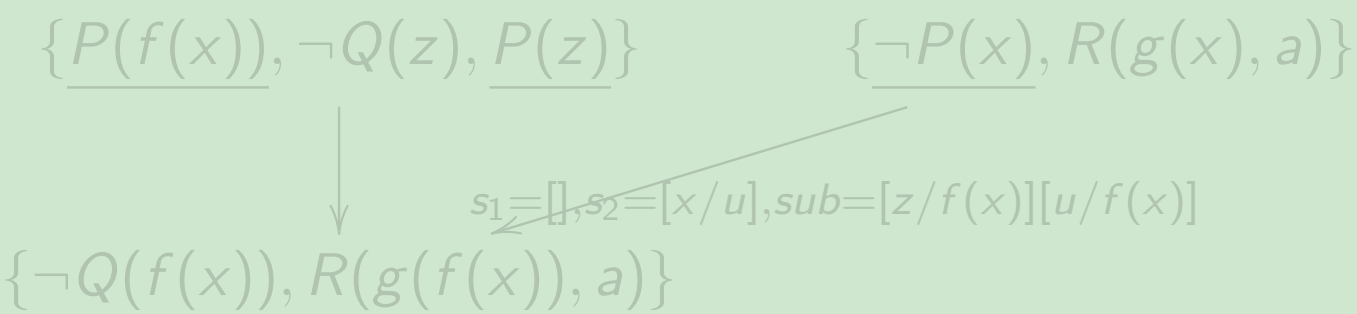
Sei $K_1 = \{P(f(x)), \neg Q(z), P(z)\}$ und $K_2 = \{\neg P(x), R(g(x), a)\}$
Wir wählen $P(f(x)), P(z) \in K_1$ und $\neg P(x) \in K_2$ zur Resolution aus. Damit:



Resolution - Beispiel 1 (kürzer)

Beispiel

Das Beispiel von eben kürzer:
Sei $K_1 = \{P(f(x)), \neg Q(z), P(z)\}$ und $K_2 = \{\neg P(x), R(g(x), a)\}$
Wir wählen $P(f(x)), P(z) \in K_1$ und $\neg P(x) \in K_2$ zur Resolution aus. Damit:



Resolution - Beispiel 1 (kürzer)

Beispiel

Das Beispiel von eben kürzer:
Sei $K_1 = \{P(f(x)), \neg Q(z), P(z)\}$ und $K_2 = \{\neg P(x), R(g(x), a)\}$
Wir wählen $P(f(x)), P(z) \in K_1$ und $\neg P(x) \in K_2$ zur Resolution aus. Damit:

$$\{\underline{P(f(x))}, \neg Q(z), \underline{P(z)}\} \qquad \{\underline{\neg P(x)}, R(g(x), a)\}$$

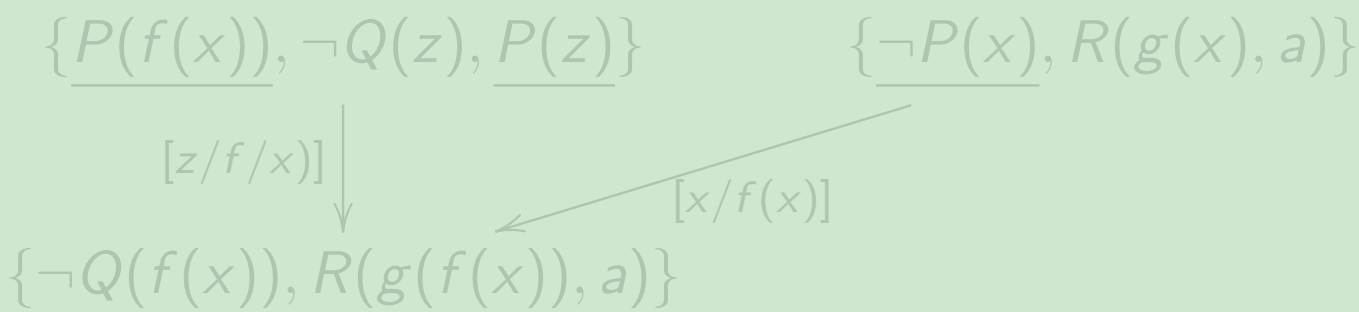
$$\downarrow \qquad s_1{=}[],s_2{=}[x/u],sub{=}[z/f(x)][u/f(x)]$$

$$\{\neg Q(f(x)), R(g(f(x)), a)\}$$

Resolution - Beispiel 1 (noch kürzer)

Beispiel

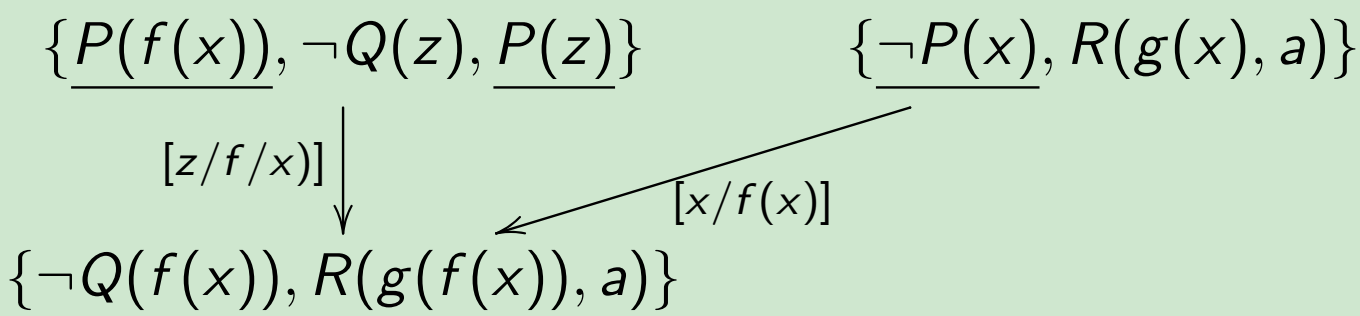
Das Beispiel von eben noch kompakter:
Sei $K_1 = \{P(f(x)), \neg Q(z), P(z)\}$ und $K_2 = \{\neg P(x), R(g(x), a)\}$
Wir wählen $P(f(x)), P(z) \in K_1$ und $\neg P(x) \in K_2$ zur Resolution aus. Damit:



Resolution - Beispiel 1 (noch kürzer)

Beispiel

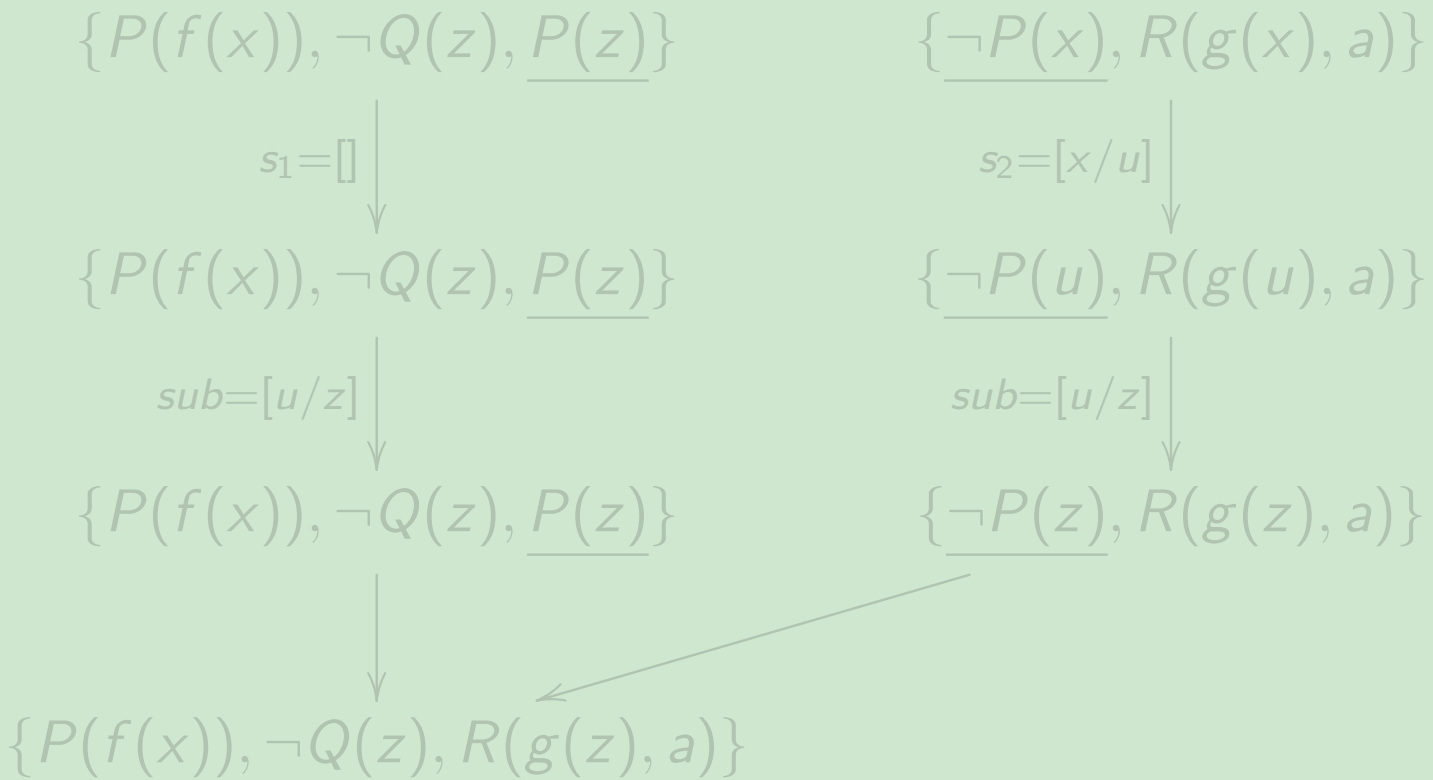
Das Beispiel von eben noch kompakter:
Sei $K_1 = \{P(f(x)), \neg Q(z), P(z)\}$ und $K_2 = \{\neg P(x), R(g(x), a)\}$
Wir wählen $P(f(x)), P(z) \in K_1$ und $\neg P(x) \in K_2$ zur Resolution aus. Damit:



Resolution - Beispiel 2

Beispiel

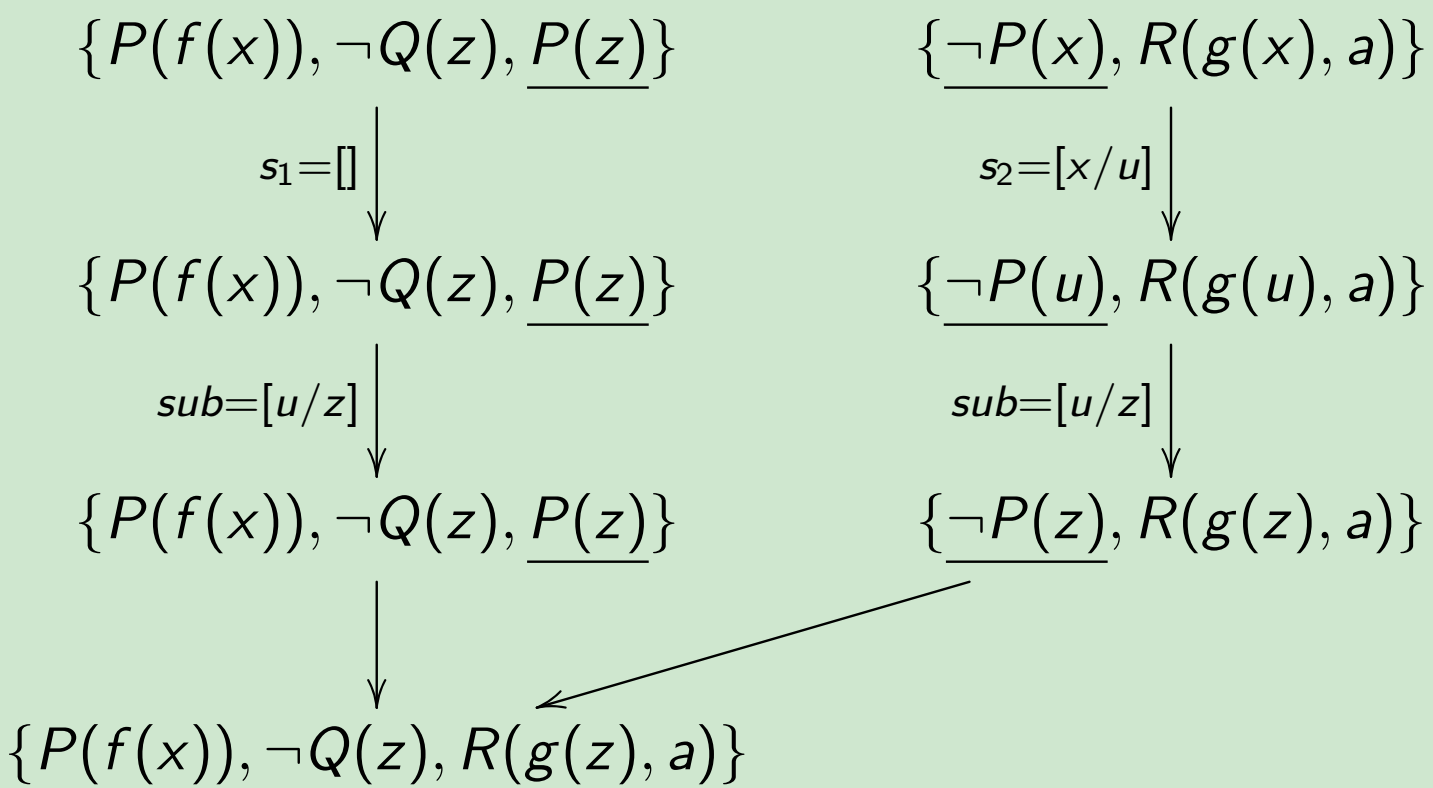
Sei $K_1 = \{P(f(x)), \neg Q(z), P(z)\}$ und $K_2 = \{\neg P(x), R(g(x), a)\}$
Wir wählen $P(z) \in K_1$ und $\neg P(x) \in K_2$ zur Resolution aus. Damit:



Resolution - Beispiel 2

Beispiel

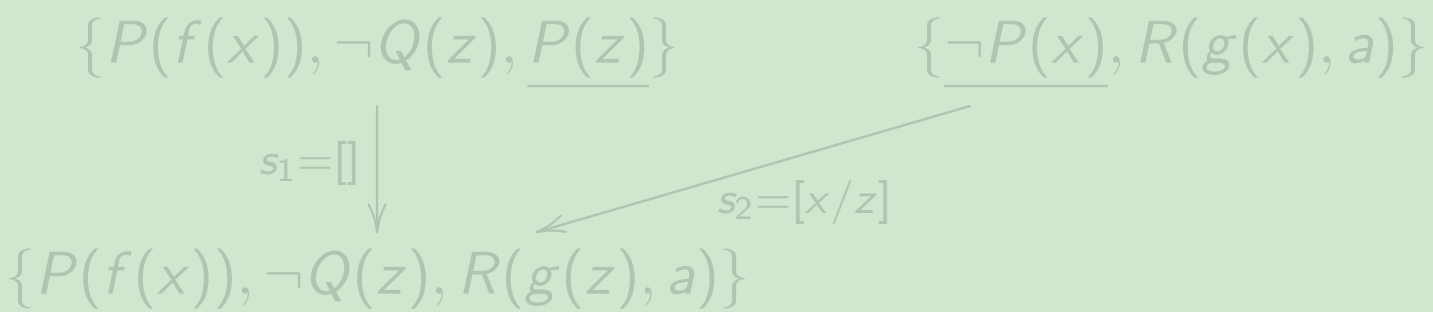
Sei $K_1 = \{P(f(x)), \neg Q(z), P(z)\}$ und $K_2 = \{\neg P(x), R(g(x), a)\}$
Wir wählen $P(z) \in K_1$ und $\neg P(x) \in K_2$ zur Resolution aus. Damit:



Resolution - Beispiel 2 (kürzer)

Beispiel

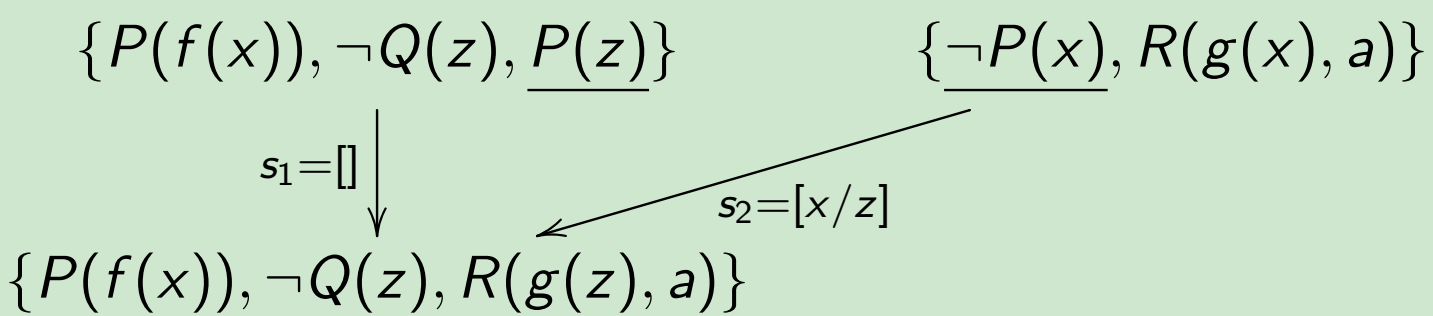
Oder in kompakter Schreibweise:
Sei $K_1 = \{P(f(x)), \neg Q(z), P(z)\}$ und $K_2 = \{\neg P(x), R(g(x), a)\}$
Wir wählen $P(z) \in K_1$ und $\neg P(x) \in K_2$ zur Resolution aus. Damit:



Resolution - Beispiel 2 (kürzer)

Beispiel

Oder in kompakter Schreibweise:
Sei $K_1 = \{P(f(x)), \neg Q(z), P(z)\}$ und $K_2 = \{\neg P(x), R(g(x), a)\}$
Wir wählen $P(z) \in K_1$ und $\neg P(x) \in K_2$ zur Resolution aus. Damit:



Resolutionssatz

Satz (Resolutionssatz der Prädikatenlogik)

Sei F eine Aussage in Skolemform mit der Matrix F^* in KNF. Dann gilt: F ist genau dann unerfüllbar, wenn $\square \in Res^*(F^*)$.

Beweis.

Es ist wieder die Korrektheit und die Vollständigkeit des Verfahrens zu zeigen. Im Beweis wird auf die Grundresolution zurückgegriffen. Dafür wird das folgende Lifting-Lemma benötigt. $\square$

Satz (Lifting-Lemma)

Seien K_1, K_2 zwei prädikatenlogische Klauseln, K_1', K_2' Grundinstanzen von ihnen mit Resolvente R'. Dann gibt es eine prädikatenlogische Resolvente R von K_1 und K_2, so dass R' Grundinstanz von R ist.

Zusammenfassung

Wir haben heute:

- Formeln gesehen, die unendlich große Modell benötigen
- die **Unentscheidbarkeit der Prädikatenlogik** gesehen
- mit Herbrand-Universum, -Struktur und -Modell gesehen, wie Syntax und Semantik "gleich" gemacht werden und damit gesehen, dass immerhin abzählbare Strukturen genügen.
- mit der Herbrand-Expansion und den Sätzen von Gödel-Herbrand-Skolem und Herbrand den Übergang zum Algorithmus von Gilmore bzw. zum Grundresolutionsalgorithmus geschafft (und damit zurück zur Aussagenlogik)
- die **Prädikatenlogische Resolution** eingeführt, wozu noch der **Unifikationsalgorithmus** benötig wurde.

Ausblick (1/2)

Satz

Sei F eine geschlossene Formel in Skolemform. F ist genau dann erfüllbar, wenn F ein Herbrand-Modell besitzt.

Satz (Gödel-Herbrand-Skolem)

Für jede geschlossene Formel in Skolemform F gilt: F ist genau dann erfüllbar, wenn die Formelmenge $E(F)$ im aussagenlogischen Sinne erfüllbar ist.

Ausblick (2/2)

Satz (Unifikationssatz)

Jede unifizierbare Menge von Literalen besitzt auch einen allgemeinsten Unifikator.

Satz (Lifting-Lemma)

Seien K_1, K_2 zwei prädikatenlogische Klauseln, K_1', K_2' Grundinstanzen von ihnen mit Resolvente R'. Dann gibt es eine prädikatenlogische Resolvente R von K_1 und K_2, so dass R' Grundinstanz von R ist.

Satz (Resolutionssatz der Prädikatenlogik)

Sei F eine Aussage in Skolemform mit der Matrix F^* in KNF. Dann gilt: F ist genau dann unerfüllbar, wenn $\square \in Res^*(F^*)$.

Hausaufgabe

Zur Übung

1. Die heutige Vorlesung in der Vogelperspektive noch einmal nachvollziehen. Was geschieht wo? Was wird wo benötigt?
2. Versucht die obigen fünf Sätze zu beweisen. Bei Bedarf schaut in die Literatur (siehe unten).

Literatur

Die heutige Vorlesung orientiert sich stark an den Kapiteln 2.4 und 2.5 aus dem Buch *Logik für Informatiker* von Uwe Schöning.