

Logik für Informatiker

3. Prädikatenlogik

Teil 8

7.07.2016

Viorica Sofronie-Stokkermans

Universität Koblenz-Landau

e-mail: sofronie@uni-koblenz.de

Bis jetzt

Syntax

- Prädikatenlogische Signatur
- Term, Atom, Formel

Semantik

- Prädikatenlogisches Modell
- Auswertung von Formeln in Modellen
- Erfüllbarkeit, Gültigkeit; Folgerung, Äquivalenz
- Eigenschaften von Quantoren (Vertauschbarkeit untereinander und mit \wedge, \vee)

Substitutionslemma

Unentschiedbarkeit der Erfüllbarkeit von Formeln

Bis jetzt

Normalformen

- NNF
- Pränexe Normalform
- Skolemnormalform
- Klauselnormalform

Kalküle

- Resolution
- Semantische Tableaux

Prädikatenlogische Resolution

Grundidee

Vor Resolutionsschritt durch geeignete Substitution komplementäres Paar von Literalen erzeugen

Möglichkeit für Resolutionsregel

$$\frac{C_1 \cup \{L\} \quad C_2 \cup \{\neg L'\}}{C_1\sigma \cup C_2\sigma}$$

wobei

- die Elternklauseln keine Variablen gemeinsam haben (bereinigt)
 \mapsto ggf. umbenennen
- $\sigma(L) = \sigma(L')$

Nachteil: Viel zu viele Substitutionen σ mit $\sigma(L) = \sigma(L')$

Idee: Wähle die “allgemeinste” Substitution, mit $\sigma(L) = \sigma(L')$

Unifikation

Sei $E = \{s_1 \stackrel{?}{=} t_1, \dots, s_n \stackrel{?}{=} t_n\}$ (s_i, t_i Terme oder Atome) eine Menge von Gleichheitsproblemen.

Definition: Eine Substitution σ heißt ein **Unifikator** von E g.d.w.

$$\forall 1 \leq i \leq n : s_i \sigma = t_i \sigma.$$

Existiert ein Unifikator, so heißt E **unifizierbar**.

Definition: σ heißt **allgemeiner** als τ

$$\sigma \leq \tau \iff \text{es gibt Subst. } \varrho : \sigma \circ \varrho = \tau$$

wobei $(\sigma \circ \varrho)(x) := \varrho(\sigma(x))$ die Komposition von σ und ϱ als Abbildungen.^a

^aIst wohldefiniert, weil $\sigma \circ \varrho$ einen endlichen Bereich hat.

Unifikation nach Martelli/Montanari

- (1) $t \stackrel{?}{=} t, E \Rightarrow_{MM} E$
- (2) $f(s_1, \dots, s_n) \stackrel{?}{=} f(t_1, \dots, t_n), E \Rightarrow_{MM} s_1 \stackrel{?}{=} t_1, \dots, s_n \stackrel{?}{=} t_n, E$
- (3) $f(\dots) \stackrel{?}{=} g(\dots), E \Rightarrow_{MM} \perp$
- (4) $x \stackrel{?}{=} t, E \Rightarrow_{MM} x \stackrel{?}{=} t, E[t/x]$
falls $x \in \text{var}(E), x \notin \text{var}(t)$
- (5) $x \stackrel{?}{=} t, E \Rightarrow_{MM} \perp$
falls $x \neq t, x \in \text{var}(t)$
- (6) $t \stackrel{?}{=} x, E \Rightarrow_{MM} x \stackrel{?}{=} t, E$
falls $t \notin X$

Unifikation: Haupteigenschaften

Definition. Eine Substitution σ heißt **idempotent**, wenn $\sigma \circ \sigma = \sigma$.

Lemma.

σ ist idempotent gdw. $dom(\sigma) \cap codom(\sigma) = \emptyset$.

Theorem.

1. $E \Rightarrow_{MM}^* \perp$ gdw. E nicht unfizierbar.
2. E unfizierbar gdw. $E \Rightarrow_{MM}^* x_1 \stackrel{?}{=} u_1, \dots, x_k \stackrel{?}{=} u_k$,
mit x_i pw. verschieden, $x_i \notin var(u_j), 1 \leq i, j \leq k$.
3. Falls $E \Rightarrow_{MM}^* x_1 \stackrel{?}{=} u_1, \dots, x_k \stackrel{?}{=} u_k$,
mit x_i pw. verschieden, $x_i \notin var(u_j)$ so
 $\sigma = [u_1/x_1, \dots, u_k/x_k]$ ist allgemeinsten Unifikator von E .

Unifikation: Haupteigenschaften

Theorem.

E unifizierbar g.d.w. es gibt allgemeinsten Unifikator σ von E , so dass:

- (1) σ idempotent und
- (2) $dom(\sigma) \cup codom(\sigma) \subseteq var(E)$.

Notation: $\sigma = mgu(E)$ („most general unifier“)

Beweisideen

- Falls $E \Rightarrow_{MM} E'$, dann σ Unifikator von E gdw. σ Unifikator von E' . (\perp habe keinen Unifikator.)
- Bzgl. \Rightarrow_{MM} irreduzible E sind trivialerweise nicht unifizierbar ($E = \perp$) oder haben die Form einer idempotenten Substitution. In diesem Fall ist die Substitution der allgemeinste Unifikator.
- \Rightarrow_{MM} “terminiert”. Eine geeignete lexikographische Ordnung auf Gleichungsmengen E (mit \perp minimal und kleiner als alle Gleichungsmengen) zeigt dieses. Man vergleiche in dieser Reihenfolge:
 1. Anzahl der definierten Variablen (d.h. Variablen x in Gleichung $x \stackrel{?}{=} t$ mit $x \notin \text{var}(t)$), die auch außerhalb ihrer Definition in E vorkommen
 2. Mengenordnung induziert von (i) der Größe (Anzahl der Symbole) einer Gleichung; (ii) bei gleicher Größe betrachten wir $x \stackrel{?}{=} t$ kleiner als $t \stackrel{?}{=} x$, falls $t \notin X$.
- σ ist idempotent wegen der Substitution in Regel 4. $\text{dom}(\sigma) \subseteq \text{var}(E)$, weil keine neuen Variablen eingeführt werden.

Unifikation

Problem: exponentielles Anwachsen der Terme möglich.

Beispiel:

$$E = \{x_1 \stackrel{?}{=} f(x_0, x_0), x_2 \stackrel{?}{=} f(x_1, x_1), \dots, x_n \stackrel{?}{=} f(x_{n-1}, x_{n-1})\}$$

m.g.u. $[x_1 \mapsto f(x_0, x_0), x_2 \mapsto f(f(x_0, x_0), f(x_0, x_0)), \dots]$

$x_i \mapsto$ kompletter binärer Baum der Höhe i Zeit/Raum: exponentiell

Idee: Terme: azyklische Termgraphen

Prädikatenlogische Resolution

Grundidee

Vor Resolutionsschritt durch geeignete Substitution komplementäres Paar von Literalen erzeugen

Möglichkeit für Resolutionsregel

$$\frac{C_1 \cup \{L\} \quad C_2 \cup \{\neg L'\}}{C_1\sigma \cup C_2\sigma}$$

wobei

- die Elternklauseln keine Variablen gemeinsam haben (bereinigt)
↳ ggf. umbenennen
- $\sigma = \text{mgu}(L, L')$

Beispiel

$$\{L\} \cup C_1 = \{\underbrace{p(a, x), p(x, x)}_L\}$$

$$\{\neg L'\} \cup C_2 = \{\neg \underbrace{p(y, y)}_{L'}\}$$

Beispiel

$$\{L\} \cup C_1 = \underbrace{\{p(a, x), p(x, x)\}}_L$$

$$\{\neg L'\} \cup C_2 = \underbrace{\{\neg p(y, y)\}}_{L'}$$

Allgemeinster Unifikator von L, L' :

$$\begin{aligned} \{p(a, x) \stackrel{?}{=} p(y, y)\} &\Rightarrow_{MM} \{a \stackrel{?}{=} y, x \stackrel{?}{=} y\} \\ &\Rightarrow_{MM} \{y \stackrel{?}{=} a, x \stackrel{?}{=} a\} \end{aligned}$$

$$\text{mgu}(L, L'): \quad \sigma = [a/y, a/x]$$

Beispiel

$$\{L\} \cup C_1 = \underbrace{\{p(a, x), p(x, x)\}}_L \qquad \{\neg L'\} \cup C_2 = \underbrace{\{\neg p(y, y)\}}_{L'}$$

Allgemeinster Unifikator von L, L' :

$$\begin{aligned} \{p(a, x) \stackrel{?}{=} p(y, y)\} &\Rightarrow_{MM} \{a \stackrel{?}{=} y, x \stackrel{?}{=} y\} \\ &\Rightarrow_{MM} \{y \stackrel{?}{=} a, x \stackrel{?}{=} a\} \end{aligned}$$

$$\text{mgu}(L, L'): \quad \sigma = [a/y, a/x]$$

$$\frac{C_1 \cup \{L\} \quad C_2 \cup \{\neg L'\}}{C_1\sigma \cup C_2\sigma}$$

$$R := \{p(x, x)\}\sigma \cup \{\}\sigma = \{p(a, a)\}$$

Beispiel

$$\{L\} \cup C_1 = \underbrace{\{p(a, x), p(x, x)\}}_L \qquad \{\neg L'\} \cup C_2 = \underbrace{\{\neg p(y, y)\}}_{L'}$$

Allgemeinster Unifikator von L, L' :

$$\begin{aligned} \{p(a, x) \stackrel{?}{=} p(y, y)\} &\Rightarrow_{MM} \{a \stackrel{?}{=} y, x \stackrel{?}{=} y\} \\ &\Rightarrow_{MM} \{y \stackrel{?}{=} a, x \stackrel{?}{=} a\} \end{aligned}$$

$$\text{mgu}(L, L'): \quad \sigma = [a/y, a/x]$$

$$\frac{C_1 \cup \{L\} \quad C_2 \cup \{\neg L'\}}{C_1\sigma \cup C_2\sigma}$$

$$R := \{p(x, x)\}\sigma \cup \{\}\sigma = \{p(a, a)\}$$

$$\frac{\{p(a, x), p(x, x)\} \quad \{\neg p(y, y)\}}{\{p(a, a)\}}$$

Prädikatenlogische Resolution

Resolutionsregel in dieser Form alleine unvollständig für Prädikatenlogik

Beispiel:

$\{\{p(x), p(y)\}, \{\neg p(u), \neg p(v)\}\}$

- unerfüllbar
- aber nur Resolventen der Länge 2

Prädikatenlogische Resolution

Faktorisierung

$$\frac{\{L_1, \dots, L_n\} \cup C}{(\{L_1, \dots, L_n\} \cup C)\sigma}$$

wobei

- σ allgemeinsten Unifikator (MGU) von $\{L_1, \dots, L_n\}$ ist

$(\{L_1, \dots, L_n\} \cup C)\sigma$ heißt Faktor von $\{L_1, \dots, L_n\} \cup C$

Beispiel für Faktorisierung

$$\frac{\{p(x), p(y), r(y, z)\}}{\{p(x), r(x, z)\}}$$

$$\text{mgu}(p(x), p(y)) = [x/y]$$

Beispiel für Faktorisierung

$$\frac{\{p(x), p(y), r(y, z)\}}{\{p(x), r(x, z)\}}$$

$$\text{mgu}(p(x), p(y)) = [x/y]$$

$$\frac{\{p(x), p(y), p(a), r(y, z)\}}{\{p(a), r(a, z)\}}$$

$$\text{mgu}(p(x), p(y), p(a)) = [a/x, a/y]$$

Beispiel für Faktorisierung

$$\frac{\{p(x), p(y), r(y, z)\}}{\{p(x), r(x, z)\}}$$

$$\text{mgu}(p(x), p(y)) = [x/y]$$

$$\frac{\{p(x), p(y), p(a), r(y, z)\}}{\{p(a), r(a, z)\}}$$

$$\text{mgu}(p(x), p(y), p(a)) = [a/x, a/y]$$

$$\frac{\{p(b), p(y), p(a), r(y, z)\}}{\{p(b), p(a), r(b, z)\}}$$

$$\text{mgu}(p(b), p(y)) = [b/y]$$

$$\frac{\{p(b), p(y), p(a), r(y, z)\}}{\{p(b), p(a), r(a, z)\}}$$

$$\text{mgu}(p(y), p(a)) = [a/y]$$

Resolutionskalkül *Res* für allgemeine Klauseln (Mengennotation)

$$\frac{C \cup \{A_1\} \quad D \cup \{\neg A_2\}}{(C \cup D)\sigma} \quad \text{falls } \sigma = \text{mgu}(A_1, A_2) \quad [\text{Resolution}]$$

$$\frac{C \cup \{L_1, L_2\}}{(C \cup \{L_1\})\sigma} \quad \text{falls } \sigma = \text{mgu}(L_1, L_2) \quad [\text{Faktorisierung}]$$

Es wird immer implizit angenommen, dass die Variablen in einer der beiden Prämissen der Resolutionsregel ggfs. (bijektiv) umbenannt werden, so dass sie disjunkt mit denen der anderen Prämisse sind.

Dieses implizite Umbenennen werden wir nicht formalisieren.

Welche Variablennamen man verwendet ist egal.

Beispielsweise könnte man sich vorstellen, dass am Anfang alle Klauseln paarweise variablendisjunkt sind und das Unifikatoren so gewählt werden, dass in ihrem Wertebereich nur neue Variablen vorkommen.

Beispiel

1. $\{P(x), P(f(x)), \neg Q(x)\}$ [Gegeben]
2. $\{\neg P(y)\}$ [Gegeben]
3. $\{P(g(x', x)), Q(x)\}$ [Gegeben]

Beispiel

1. $\{P(x), P(f(x)), \neg Q(x)\}$ [Gegeben]
2. $\{\neg P(y)\}$ [Gegeben]
3. $\{P(g(x', x'')), Q(x'')\}$ [Gegeben; Bereinigt]
4. $\{P(f(x)), \neg Q(x)\}$ [Res. 1, 2], $\text{mgu}(P(x), P(y)) = [x/y]$
5. $\{\neg Q(x)\}$ [Res. 4, 2], $\text{mgu}(P(y), P(f(x))) = [f(x)/y]$
6. $\{Q(x'')\}$ [Res. 3, 2], $\text{mgu}(P(y), P(g(x', x''))) = [g(x', x'')/y]$
7. \perp [Res. 5, 6], $\text{mgu}(Q(x), Q(x'')) = [x/x'']$

Resolutionskalkül *Res* für allgemeine Klauseln (Klauselnotation)

$$\frac{C \vee A_1 \quad D \vee \neg A_2}{(C \vee D)\sigma} \quad \text{falls } \sigma = \text{mgu}(A_1, A_2) \quad [\text{Resolution}]$$

$$\frac{C \vee L_1 \vee L_2}{(C \vee L_1)\sigma} \quad \text{falls } \sigma = \text{mgu}(L_1, L_2) \quad [\text{Faktorisierung}]$$

Es wird immer implizit angenommen, dass die Variablen in einer der beiden Prämissen der Resolutionsregel ggfs. (bijektiv) umbenannt werden, so dass sie disjunkt mit denen der anderen Prämisse sind.

Dieses implizite Umbenennen werden wir nicht formalisieren.

Welche Variablennamen man verwendet ist egal.

Beispielsweise könnte man sich vorstellen, dass am Anfang alle Klauseln paarweise variablendisjunkt sind und das Unifikatoren so gewählt werden, dass in ihrem Wertebereich nur neue Variablen vorkommen.

Beispiel

1. $P(x) \vee P(f(x)) \vee \neg Q(x)$ [Gegeben]
2. $\neg P(y)$ [Gegeben]
3. $P(g(x', x)) \vee Q(x)$ [Gegeben]

Beispiel

1. $P(x) \vee P(f(x)) \vee \neg Q(x)$ [Gegeben]
2. $\neg P(y)$ [Gegeben]
3. $P(g(x', x'')) \vee Q(x'')$ [Gegeben; Bereinigt]
4. $P(f(x)) \vee \neg Q(x)$ [Res. 1, 2], $\text{mgu}(P(x), P(y)) = [x/y]$
5. $\neg Q(x)$ [Res. 4, 2], $\text{mgu}(P(y), P(f(x))) = [f(x)/y]$
6. $Q(x'')$ [Res. 3, 2], $\text{mgu}(P(y), P(g(x', x''))) = [g(x', x'')/y]$
7. \perp [Res. 5, 6], $\text{mgu}(Q(x), Q(x'')) = [x/x'']$

Wichtig: Häufige Fehlerquellen

- Das Bereinigen (Umbenennen) nicht vergessen!
- Das Faktorisierungen (falls möglich) nicht vergessen!
- Selbstresolution ist möglich!

Notation

Sei N eine Klauselmengende und

$$\text{Res}(N) = N \cup \{R \mid R \text{ ist eine Resolvente zweier Klauseln aus } N$$

oder Resultat der Faktorisierung einer Klausel aus $N\}$

$$\text{Res}^0(N) = N$$

$$\text{Res}^{n+1}(N) = \text{Res}(\text{Res}^n(N))$$

$$\text{Res}^*(N) = \bigcup_{n \in \mathbb{N}} \text{Res}^n(N)$$

(bezeichnet die Vereinigung der Ergebnisse aus aller möglichen Resolutions- und Faktorisierungsschritten auf N)

Resolution: Korrektheit

Theorem

Für eine Menge N von Klauseln gilt: Falls $\perp \in \text{Res}^*(N)$, so N unerfüllbar.

Beweis (Idee):

Wie bei Aussagenlogik.

Einzelne Regelanwendung erhält die Erfüllbarkeit der Klauselmenge.

Auch dies einfach zu beweisen wie in Aussagenlogik (beachte dabei: Variablen in Klauseln sind universell quantifiziert).

Resolution: Korrektheit

Theorem

Für eine Menge N von Klauseln gilt: Falls $\perp \in \text{Res}^*(N)$, so N unerfüllbar.

Beweis:

Annahme: $\mathcal{A} \models C_1 \vee L_1$, $\mathcal{A} \models C_2 \vee \neg L_2$ (d.h. $\mathcal{A} \models \forall x(C_1 \vee L_1)$, $\mathcal{A} \models \forall x(C_2 \vee \neg L_2)$)

Sei $\sigma = \text{mgu}(L_1, L_2)$.

Zu zeigen: $\mathcal{A} \models \forall x(C_1 \vee C_2)\sigma$.

Sei β beliebig.

$\mathcal{A}(\beta)((C_1 \vee C_2)\sigma) = \mathcal{A}(\beta \circ \sigma)(C_1 \vee C_2)$ (Substitution-Lemma)

- Fall 1: $\mathcal{A}(\beta \circ \sigma)(C_1) = 1$. Dann $\mathcal{A}(\beta)((C_1 \vee C_2)\sigma) = 1$.
- Fall 2: $\mathcal{A}(\beta \circ \sigma)(C_1) = 0$. Laut Annahme, $\mathcal{A}(\beta \circ \sigma)(C_1 \vee L_1) = 1$, so $\mathcal{A}(\beta \circ \sigma)(L_1) = 1$. Dann: $\mathcal{A}(\beta \circ \sigma)(L_2) = \mathcal{A}(\beta)(L_2\sigma) = \mathcal{A}(\beta)(L_1\sigma) = \mathcal{A}(\beta \circ \sigma)(L_1) = 1$. Also: $\mathcal{A}(\beta \circ \sigma)(\neg L_2) = 0$.

Aber $\mathcal{A}(\beta \circ \sigma)(C_2 \vee \neg L_2) = 1$, so $\mathcal{A}(\beta \circ \sigma)(C_2) = 1$. Dann $\mathcal{A}(\beta)((C_1 \vee C_2)\sigma) = 1$.

Resolution: Vollständigkeit

Theorem

Für eine Menge N von Klauseln gilt: Falls N unerfüllbar, so $\perp \in \text{Res}^*(N)$.

Idee: Reduktion auf Vollständigkeit der Resolution für Grundklauseln (also Aussagenlogischer Resolution).

↳ Herbrandinterpretationen

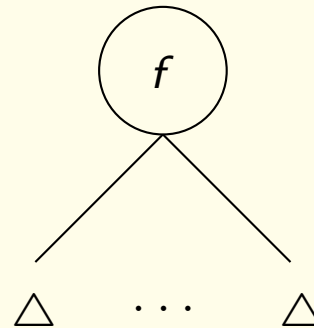
Herbrand-Interpretationen

Ω enthalte immer mindestens ein Konstantensymbol.

Definition. Herbrand-Interpretationen (über Σ) sind Σ -Strukturen \mathcal{A} mit:

1. $U_{\mathcal{A}} = T_{\Sigma}$ Menge der Grundterme, d.h. variablenfreien Terme über Σ
($U_{\mathcal{A}}$: Herbrand-Universum)
2. $f_{\mathcal{A}} : (s_1, \dots, s_n) \mapsto f(s_1, \dots, s_n)$, $f/n \in \Omega$

$$f_{\mathcal{A}}(\Delta, \dots, \Delta) =$$



d.h. vorgegeben sind Terme als Daten und Funktionen als **Termkonstruktoren**.

Variabel sind nur die Interpretationen der Prädikatensymbole

$$p_{\mathcal{A}} \subseteq T_{\Sigma}^m, p_m \in \Pi$$

Herbrand-Interpretationen als Mengen von Grundatomen

Satz.

Jede Menge von Grundatomen I identifiziert genau eine Herbrand-Interpretation \mathcal{A} durch

$$(s_1, \dots, s_n) \in p_{\mathcal{A}} \text{ genau dann, wenn } p(s_1, \dots, s_n) \in I$$

Im folgenden werden wir daher nicht zwischen Herbrand-Interpretationen (über Σ) und Mengen von Σ -Grundatomen unterscheiden.

Herbrand-Interpretationen als Mengen von Grundatomen

Beispiel:

- Sei \mathcal{A} eine Herbrand Interpretation mit:

$$p_{\mathcal{A}} = \{(a, b), (f(a), f(b)), (f(f(a)), f(f(b)))\} \text{ und}$$

$$q_{\mathcal{A}} = \{a, f(a), f(f(a)), f(f(f(a))), \dots\}$$

Dann sind folgende Grundatome wahr in \mathcal{A} :

$$p(a, b), \quad p(f(a), f(b)), \quad p(f(f(a)), f(f(b))),$$

$$q(a), \quad q(f(a)), \quad q(f(f(a))), \quad q(f(f(f(a)))) , \dots$$

Sei I die Menge dieser Grundatome. I identifiziert \mathcal{A} .

- Sei $I' = \{p(a, b), p(b, a), q(b), q(f(b)), q(f(f(b)))\}$.

I' identifiziert die Herbrand interpretation \mathcal{A}' mit:

$$p_{\mathcal{A}'} = \{(a, b), (b, a)\} \text{ und}$$

$$q_{\mathcal{A}'} = \{b, f(b), f(f(b))\}.$$

Existenz von Herbrand-Modellen

Definition. Eine Herbrand-Interpretation I heißt **Herbrand-Modell** von F , falls $I \models F$.

Theorem [Herbrand] Sei N eine Menge von Σ -Klauseln.

N erfüllbar g.d.w. N hat Herbrand-Modell (über Σ)

 g.d.w. $G_\Sigma(N)$ hat Herbrand-Modell (über Σ)

wobei

$$G_\Sigma(N) = \{C\sigma \text{ Grundklausel} \mid C \in N, \sigma : X \rightarrow T_\Sigma\}$$

die Menge der **Grundinstanzen** von N ist.

[Beweis später im Zusammenhang mit dem Vollständigkeitsbeweis für Resolution.]

Herbrand-Interpretationen als Mengen von Grundatomen

Beispiel:

$$\Sigma_{Pres} = (\{0/0, s/1, +/2\}, \{</2, \leq /2\})$$

Herbrand-Interpretation über Σ_{Pres}

$$I = \{ \begin{array}{l} 0 \leq 0, 0 \leq s(0), 0 \leq s(s(0)), \dots, \\ 0 + 0 \leq 0, 0 + 0 \leq s(0), \dots, \\ \dots, (s(0) + 0) + s(0) \leq s(0) + (s(0) + s(0)) \\ \dots \\ s(0) + 0 < s(0) + 0 + 0 + s(0) \\ \dots \end{array} \}$$

Beispiel für G_Σ

Bzgl. Σ_{Pres} erhält man für

$$C = (x < y) \vee (y \leq s(x))$$

folgende Grundinstanzen:

$$(0 < 0) \vee (0 \leq s(0))$$

$$(s(0) < 0) \vee (0 \leq s(s(0)))$$

...

$$(s(0) + s(0) < s(0) + 0) \vee (s(0) + 0 \leq s(s(0) + s(0)))$$

...

Resolution: Vollständigkeit

Theorem (**Vollständigkeit**)

Für eine Menge N von Klauseln gilt: Falls N unerfüllbar, so $\perp \in \text{Res}^*(N)$.

Beweisplan:

1. Sei N eine unter Res saturierte Menge allgemeiner Klauseln, d.h. $\text{Res}(N) \subseteq N$. Dann ist auch $G_\Sigma(N)$ saturiert.

Beweis: “Lifting-Lemma”

2. Sei N eine Menge von Σ -Klauseln.
 N erfüllbar g.d.w. N besitzt Herbrand-Modell über Σ .
3. Sei N Menge allgemeiner Klauseln mit $\text{Res}(N) \subseteq N$. Dann
 $N \models \perp$ genau dann, wenn $\perp \in N$.

Resolution: Vollständigkeit

Theorem (**Vollständigkeit**)

Für eine Menge N von Klauseln gilt: Falls N unerfüllbar, so $\perp \in \text{Res}^*(N)$.

Beweisplan:

1. Sei N eine unter Res saturierte Menge allgemeiner Klauseln, d.h. $\text{Res}(N) \subseteq N$. Dann ist auch $G_\Sigma(N)$ saturiert.

Beweis: "Lifting-Lemma"

2. Sei N eine Menge von Σ -Klauseln.
 N erfüllbar g.d.w. N besitzt Herbrand-Modell über Σ .
3. Sei N Menge allgemeiner Klauseln mit $\text{Res}(N) \subseteq N$. Dann
 $N \models \perp$ genau dann, wenn $\perp \in N$.

Lifting-Lemma

Lemma. Falls

$$\frac{C\sigma \quad D\sigma}{C'} \quad [\text{aussagenlogische Resolution}]$$

dann gibt es τ , so dass

$$\frac{C \quad D}{C''} \quad [\text{allgemeine Resolution}]$$

und $C' = C''\tau$.

Entsprechend für Faktorisieren.

Lifting-Lemma: Beweis

Beweis (Idee)

Sei $C = C_1 \vee L_1$, $D = C_2 \vee \neg L_2$.

$C\sigma = C_1\sigma \vee L_1\sigma$, $D\sigma = C_2\sigma \vee \neg L_2\sigma$.

$L_1\sigma = L_2\sigma$ und $C' = (C_1 \vee C_2)\sigma$.

L_1, L_2 unifizierbar. Sei $\rho = mgu(L_1, L_2)$.

Die Resolvente C'' ist dann $(C_1 \vee C_2)\rho$.

ρ ist allgemeiner als σ , d.h. es gibt eine Substitution τ mit $\sigma(x) = \tau(\rho(x))$ für alle $x \in X$.

$C''\tau = (C_1 \vee C_2)\rho\tau = (C_1 \vee C_2)\sigma = C'$.

Saturiertheit von Mengen allgemeiner Klauseln

Sei N eine Klauselmenge und

$$\text{Res}(N) = N \cup \{R \mid R \text{ ist eine Resolvente zweier Klauseln aus } N$$

oder Resultat der Faktorisierung einer Klausel aus $N\}$

$$\text{Res}^0(N) = N$$

$$\text{Res}^{n+1}(N) = \text{Res}(\text{Res}^n(N))$$

$$\text{Res}^*(N) = \bigcup_{n \in \mathbb{N}} \text{Res}^n(N)$$

(bezeichnet die Vereinigung der Resolventen aus aller möglichen Resolutionsschritte auf N)

Saturiertheit von Mengen allgemeiner Klauseln

Theorem.

Sei N eine unter Res saturierte Menge allgemeiner Klauseln, d.h. $\text{Res}(N) \subseteq N$. Dann ist auch $G_{\Sigma}(N)$ saturiert, d.h.

$$\text{Res}(G_{\Sigma}(N)) \subseteq G_{\Sigma}(N).$$

Saturiertheit von Mengen allgemeiner Klauseln

Theorem.

Sei N eine unter Res saturierte Menge allgemeiner Klauseln, d.h. $Res(N) \subseteq N$. Dann ist auch $G_{\Sigma}(N)$ saturiert, d.h.

$$Res(G_{\Sigma}(N)) \subseteq G_{\Sigma}(N).$$

Beweis. Sei $C' \in Res(G_{\Sigma}(N))$. D.h. es gibt: (i) Grundinstanzen C_{σ} und $D_{\sigma'}$ von N mit Resolvente C' , oder (ii) Grundinstanz C_{σ} s.d. C' durch Faktorisierung abgeleitet.

(i) Ist C' Resolvente, so können wir o.B.d.A. annehmen, dass $\sigma = \sigma'$.

(Nur wenn C und D nicht variablen-disjunkt wären, könnte dies schiefgehen. Dann aber dürfen und müssen wir die Variablen in einer Klausel umbenennen.)

Wegen des Lifting-Lemmas sind C und D resolvierbar mit einer Resolvente C'' so dass $C''\tau = C'$, für eine geeignete Substitution τ . Weil $C'' \in N$ nach Voraussetzung, ist $C' \in G_{\Sigma}(N)$.

(ii) Analog für den Fall, dass C' durch Faktorisierung abgeleitet wurde.

Satz von Herbrand

Theorem (Herbrand)

Sei N eine Menge von Σ -Klauseln.

N erfüllbar g.d.w. N besitzt Herbrand-Modell über Σ

Beweis:

“ \Leftarrow ” trivial

“ \Rightarrow ”

$N \not\models \perp \Rightarrow \perp \notin Res^*(N)$ (Res. korrekt)
 $\Rightarrow \perp \notin G_\Sigma(Res^*(N))$
 $\Rightarrow G_\Sigma(Res^*(N))$ hat ein ('aussagenlogisches') Modell
 $\Rightarrow G_\Sigma(Res^*(N))$ hat ein Herbrand Modell I
 $\Rightarrow I \models Res^*(N)$ (I Herbrand-Modell)
 $\Rightarrow I \models N$ ($N \subseteq Res^*(N)$)

Korrektheit und Vollständigkeit der allgemeinen Resolution

Theorem

Sei N Menge allgemeiner Klauseln mit $Res(N) \subseteq N$. Dann:

$N \models \perp$ genau dann, wenn $\perp \in N$

Korrektheit und Vollständigkeit der allgemeinen Resolution

Theorem

Sei N Menge allgemeiner Klauseln mit $Res(N) \subseteq N$. Dann:

$$N \models \perp \text{ genau dann, wenn } \perp \in N$$

Proof: " \Leftarrow " trivial

" \Rightarrow :" Sei N Klauselmenge mit $Res(N) \subseteq N$.

Dann $Res(G_\Sigma(N)) \subseteq G_\Sigma(N)$ (Theorem Seite 43)

Annahme: $N \models \perp$. Dann $G_\Sigma(N) \models \perp$ (Wir haben gezeigt, dass $G_\Sigma(N) \not\models \perp \Rightarrow G_\Sigma(N)$ hat Herbrand Modell I und $I \models N$)

Aber $G_\Sigma(N) \models \perp$ gdw. $\perp \in G_\Sigma(N)$ (aussag.log. Resol. vollständig + korrekt).

Es ist leicht zu sehen, dass $\perp \in G_\Sigma(N)$ gdw. $\perp \in N$.

Resolution: Vollständigkeit

Theorem (**Vollständigkeit**)

Für eine Menge N von Klauseln gilt: Falls N unerfüllbar, so $\perp \in \text{Res}^*(N)$.

Beweis:

Sei $M = \text{Res}^*(N)$. Dann $\text{Res}(M) \subseteq M$. So: $M \models \perp$ gdw. $\perp \in M$.

Widerspruchsbeweis:

Annahme: $\perp \notin \text{Res}^*(N)$. Dann $\text{Res}^*(N) \not\models \perp$, d.h. $\text{Res}^*(N)$ hat ein Modell \mathcal{A} .

Da $N \subseteq \text{Res}^*(N)$, $\mathcal{A} \models N$, d.h. $N \not\models \perp$.