

Logik für Informatiker

3. Prädikatenlogik

Teil 6

2.07.2013

Viorica Sofronie-Stokkermans

Universität Koblenz-Landau

e-mail: sofronie@uni-koblenz.de

Bis jetzt

- Prädikatenlogische Signatur; Term, Atom, Formel
- Prädikatenlogisches Modell; Auswertung von Formeln in Modellen
- Erfüllbarkeit, Gültigkeit; Folgerung, Äquivalenz
- Wichtige Äquivalenzen
- Entscheidbarkeit der Erfüllbarkeit von Formeln

Ziel: Kalküle zur systematischen Überprüfung von Erfüllbarkeit (für Formeln und/oder Formelmengen)

- Normalformen, Skolemisierung

Pränexe Normalform

Definition: Pränexe Formeln sind von der Form $Q_1x_1 \dots Q_nx_n F$, wobei F quantorenfrei, $Q_i \in \{\forall, \exists\}$.

Hierbei heißt $Q_1x_1 \dots Q_nx_n$ der **Quantorenpräfix** und F die **Matrix** der Formel.

Theorem. Zu jeder Formel $F \in \text{For}_\Sigma$ gibt es eine äquivalente Formel in Pränexnormalform

Konstruktiver Beweis

(1) Formel in NNF transformieren

1. Elimination von \leftrightarrow
2. Elimination von \rightarrow
3. “Nach innen schieben” von \neg
 - aussagenlogische Umformungen (de Morgans Regeln; $\neg\neg A \equiv A$)
 - $\neg\forall xF(x) \equiv \exists x\neg F(x)$
 - $\neg\exists xF(x) \equiv \forall x\neg F(x)$

(2) Formel bereinigen

(3) Alle Quantoren nach vorne (Reihenfolge unverändert lassen)

Skolemnormalform

Definition. Eine Formel $F \in \text{For}_\Sigma$ ist in Skolemnormalform (SNF), falls:

- F ist in Pränexnormalform
- F enthält nur universelle Quantoren

Skolemisierung: Transformation \Rightarrow_S :

$$\forall x_1, \dots, x_n \exists y F \quad \Rightarrow_S \quad \forall x_1, \dots, x_n F[f(x_1, \dots, x_n)/y]$$

wobei f/n ein neues Funktionssymbol (**Skolemfunktion**).

Gesamtbild

$$F \xRightarrow{*}_P Q_1 y_1 \dots Q_n y_n G \quad (G \text{ quantorenfrei})$$

$$\xRightarrow{*}_S \forall x_1, \dots, x_m H \quad (H \text{ quantorenfrei})$$

$$\xRightarrow{*}_K \underbrace{\underbrace{\forall x_1, \dots, x_n}_{\text{weglassen}} \bigwedge_{i=1}^k \underbrace{\bigvee_{j=1}^{n_j} L_{ij}}_{\text{Klauseln } C_i}}_{F'}$$

$N = \{C_1, \dots, C_k\}$ heißt **Klausel(normal)form** (KNF) von F .

Merke: Die Variablen in Klauseln sind implizit allquantifiziert.

Falls F freie Variablen enthält, werden diese Variablen mit **Konstanten** ersetzt
 ($F(x)$ erfüllbar gdw. $\exists x F(x)$ erfüllbar)

Theorem: F ist erfüllbar, gdw. F' erfüllbar, gdw. N erfüllbar.

Viel **Optimierungspotential** vorhanden, wenn nur Erfüllbarkeit bewahrt werden muß und kann: Größenexplosion, **kleine Stelligkeit** von Skolemfunktionen.

Beispiel

$$F = \forall x((\forall yR(x, y)) \wedge (\exists z\neg S(x, z)))$$

• NNF; bereinigt

• Pränexnormalform: $\forall x\forall y\exists z(R(x, y) \wedge \neg S(x, z))$

• Skolemisierung: $z \mapsto sk_z(x, y)$

$$\forall x\forall y(R(x, y) \wedge \neg S(x, sk_z(x, y)))$$

Beispiel

$$F = \forall x((\forall yR(x, y)) \wedge (\exists z\neg S(x, z)))$$

• NNF; bereinigt

• Pränexnormalform: $\forall x\forall y\exists z(R(x, y) \wedge \neg S(x, z))$

• Skolemisierung: $z \mapsto sk_z(x, y)$

$$\forall x\forall y(R(x, y) \wedge \neg S(x, sk_z(x, y)))$$

Bemerkung:

$$\forall x((\forall yR(x, y)) \wedge (\exists z\neg S(x, z))) \equiv \forall x((\exists z\neg S(x, z)) \wedge (\forall yR(x, y)))$$

• Pränexnormalform: $\forall x\exists z\forall y(R(x, y) \wedge \neg S(x, z))$

• Skolemisierung: $z \mapsto sk'_z(x)$ (kleinere Stelligkeit der Skolemfunktion)

$$\forall x\forall y(R(x, y) \wedge \neg S(x, sk'_z(x)))$$

Kalküle

- Resolution
- Semantische Tableaux

Ab jetzt betrachten wir, falls nichts Anderes angegeben, immer nur **PL** ohne Gleichheit.

Resolution für Grundklauseln (Mengennotation)

Aussagenlogische Klauseln entsprechen Grundklauseln und umgekehrt.

Resolutionsregel:

$$\frac{C \cup \{A\} \quad \{\neg A\} \cup D}{C \cup D}$$

$C \cup D$: **Resolvente**

A : **resolviertes Atom**

Aussagenlogische Resolution ist **korrekt** und **vollständig**.

- Mengennotation: Resolutionsregel
- Klauselnotation: Resolutionsregel + Faktorisieren

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 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 $t \notin X$

Beispiele

$$\Sigma = \{\Omega, \Pi\} \quad \Omega = \{f/2, g/2, a/0, b/0\}, \Pi = \{p/2, q/1\}$$

$$x, y, z \in X$$

$$\begin{aligned} \{f(g(a, x), g(y, b)) \stackrel{?}{=} f(g(b, x), z)\} &\stackrel{(2)}{\Rightarrow}_{MM} \{g(a, x) \stackrel{?}{=} g(b, x), g(y, b) \stackrel{?}{=} z\} \\ &\stackrel{(2)}{\Rightarrow}_{MM} \{a \stackrel{?}{=} b, x \stackrel{?}{=} x, g(y, b) \stackrel{?}{=} z\} \\ &\stackrel{(3)}{\Rightarrow}_{MM} \perp \end{aligned}$$

Beispiele

$$\Sigma = \{\Omega, \Pi\} \quad \Omega = \{f/2, g/2, a/0, b/0\}, \Pi = \{p/2, q/1\}$$

$$x, y, z \in X$$

$$\begin{aligned} \{f(g(a, x), g(y, b)) \stackrel{?}{=} f(g(b, x), z)\} &\stackrel{(2)}{\Rightarrow}_{MM} \{g(a, x) \stackrel{?}{=} g(b, x), g(y, b) \stackrel{?}{=} z\} \\ &\stackrel{(2)}{\Rightarrow}_{MM} \{a \stackrel{?}{=} b, x \stackrel{?}{=} x, g(y, b) \stackrel{?}{=} z\} \\ &\stackrel{(3)}{\Rightarrow}_{MM} \perp \end{aligned}$$

$$\begin{aligned} \{f(g(a, x), g(y, b)) \stackrel{?}{=} f(g(a, y), x)\} &\stackrel{(2)}{\Rightarrow}_{MM} \{g(a, x) \stackrel{?}{=} g(a, y), g(y, b) \stackrel{?}{=} x\} \\ &\stackrel{(2)}{\Rightarrow}_{MM} \{a \stackrel{?}{=} a, x \stackrel{?}{=} y, g(y, b) \stackrel{?}{=} x\} \\ &\stackrel{(1)}{\Rightarrow}_{MM} \{x \stackrel{?}{=} y, g(y, b) \stackrel{?}{=} x\} \\ &\stackrel{(4)}{\Rightarrow}_{MM} \{x \stackrel{?}{=} y, g(y, b) \stackrel{?}{=} y\} \\ &\stackrel{(6)}{\Rightarrow}_{MM} \{x \stackrel{?}{=} y, y \stackrel{?}{=} g(y, b)\} \stackrel{(5)}{\Rightarrow}_{MM} \perp \end{aligned}$$

Beispiele

$$\Sigma = \{\Omega, \Pi\} \quad \Omega = \{f/2, g/2, a/0, b/0\}, \Pi = \{p/2, q/1\}$$

$$x, y, z \in X$$

$$\{p(g(x, a), g(f(x, b), y)) \stackrel{?}{=} q(g(f(x, b), y))\} \stackrel{(3)}{\Rightarrow} MM \perp \quad (\text{weil } p \neq q)$$

Beispiele

$$\Sigma = \{\Omega, \Pi\} \quad \Omega = \{f/2, g/2, a/0, b/0\}, \Pi = \{p/2, q/1\}, \quad x, y, z, u \in X$$

$$\{p(g(y, a), g(f(x, b), z)) \stackrel{?}{=} p(z, g(f(g(u, y), b), u), \quad q(a) \stackrel{?}{=} q(y))\}$$

$$\stackrel{(2)}{\Rightarrow}_{MM} \{g(y, a) \stackrel{?}{=} z, \quad g(f(x, b), z) \stackrel{?}{=} g(f(g(u, y), b), u), \quad q(a) \stackrel{?}{=} q(y)\}$$

$$\stackrel{(6,2)}{\Rightarrow}_{MM} \{z \stackrel{?}{=} g(y, a), \quad f(x, b) \stackrel{?}{=} f(g(u, y), b), \quad z \stackrel{?}{=} u, \quad q(a) \stackrel{?}{=} q(y)\}$$

$$\stackrel{(4)}{\Rightarrow}_{MM} \{z \stackrel{?}{=} g(y, a), \quad f(x, b) \stackrel{?}{=} f(g(u, y), b), \quad g(y, a) \stackrel{?}{=} u, \quad q(a) \stackrel{?}{=} q(y)\}$$

$$\stackrel{(2,6)}{\Rightarrow}_{MM} \{z \stackrel{?}{=} g(y, a), \quad x \stackrel{?}{=} g(u, y), \quad b \stackrel{?}{=} b, \quad u \stackrel{?}{=} g(y, a), \quad q(a) \stackrel{?}{=} q(y)\}$$

$$\stackrel{(1)}{\Rightarrow}_{MM} \{z \stackrel{?}{=} g(y, a), \quad x \stackrel{?}{=} g(u, y), \quad u \stackrel{?}{=} g(y, a), \quad q(a) \stackrel{?}{=} q(y)\}$$

$$\stackrel{(4)}{\Rightarrow}_{MM} \{z \stackrel{?}{=} g(y, a), \quad x \stackrel{?}{=} g(g(y, a), y), \quad u \stackrel{?}{=} g(y, a), \quad g(a) \stackrel{?}{=} g(y)\}$$

$$\stackrel{(2)}{\Rightarrow}_{MM} \{z \stackrel{?}{=} g(y, a), \quad x \stackrel{?}{=} g(g(y, a), y), \quad u \stackrel{?}{=} g(y, a), \quad a \stackrel{?}{=} y\}$$

$$\stackrel{(6)}{\Rightarrow}_{MM} \{z \stackrel{?}{=} g(y, a), \quad x \stackrel{?}{=} g(g(y, a), y), \quad u \stackrel{?}{=} g(y, a), \quad y \stackrel{?}{=} a\}$$

$$\stackrel{(4)}{\Rightarrow}_{MM} \{z \stackrel{?}{=} g(a, a), \quad x \stackrel{?}{=} g(g(a, a), a), \quad u \stackrel{?}{=} g(a, a), \quad y \stackrel{?}{=} a\}$$

Allgemeinster Unifikator (mgu): $[g(a, a)/z, \quad g(g(a, a), a)/x, \quad g(a, a)/u, \quad a/y]$

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 unifizierbar.
2. E unifizierbar 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)
 \mapsto ggf. umbenennen
- $\sigma = \text{mgu}(L, L')$

Beispiel

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

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

Beispiel

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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], $\text{mgu}(Q(x), Q(x'')) = [x/x'']$

Resolutionskalkül *Res* für allgemeine Klauseln

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

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

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 die Unifikatoren so gewählt werden, dass in ihrem Wertebereich nur neue Variablen vorkommen.

Wichtig: Häufige Fehlerquellen

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

Notation

Sei N eine Klauselmengue 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 Faktorisierungsschritte auf N)

Resolution: Korrektheit

Theorem

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

Resolution: Korrektheit

Theorem

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

Beweis: 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: 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

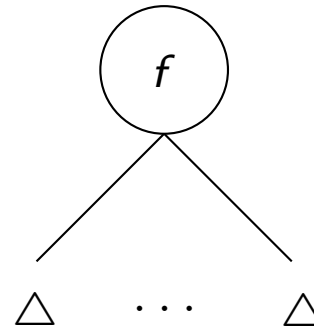
Herbrand-Interpretationen

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

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

Beispiel

$$\Sigma = (\Omega, \Pi), \Omega = \{a/0, b/0, f/1, g/2\}, \Pi = \{p/2, q/1\}$$

Herbrand Interpretation:

$$\mathcal{A} = (T_\Sigma, \{a_{\mathcal{A}}, b_{\mathcal{A}}, f_{\mathcal{A}}, g_{\mathcal{A}}\}, \{p_{\mathcal{A}}, q_{\mathcal{A}}\})$$

- Herbrand Universum: T_Σ , Menge der Grundterme

Beispiele von Elemente in T_Σ :

$$a, b, f(a), f(b), f(f(a)), f(f(b)), \underbrace{f(f(\dots f(a)))}_{n \text{ Mal}}, \underbrace{f(f(\dots f(b)))}_{n \text{ Mal}}, \dots,$$

$$g(a, a), g(a, b), \dots, \underbrace{g(f(f(\dots f(a))))}_{n \text{ Mal}}, \underbrace{f(f(\dots f(b)))}_{k \text{ Mal}}, \dots$$

- $a_{\mathcal{A}} = a \in T_\Sigma, \quad b_{\mathcal{A}} = b \in T_\Sigma$

$$f_{\mathcal{A}} : T_\Sigma \rightarrow T_\Sigma, f_{\mathcal{A}}(t) = f(t) \in T_\Sigma$$

Beispiel: $f_{\mathcal{A}}(g(b, a)) = f(g(b, a))$

$$g_{\mathcal{A}} : T_\Sigma \times T_\Sigma \rightarrow T_\Sigma, g_{\mathcal{A}}(t_1, t_2) = g(t_1, t_2) \in T_\Sigma$$

Beispiel: $g_{\mathcal{A}}(f(a), g(b, a)) = g(f(a), (g(b, a)))$

- $p_{\mathcal{A}} \subseteq T_\Sigma \times T_\Sigma,$

$$q_{\mathcal{A}} \subseteq T_\Sigma$$

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:

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

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

Herbrand-Interpretationen als Mengen von Grundatomen

Beispiel:

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

Herbrand-Interpretation über Σ_{Pres}

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

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.]