Logik für Informatiker

Vorlesung 13: Prädikatenlogik

Babeş-Bolyai Universität, Department für Informatik, Cluj-Napoca
csacarea@cs.ubbcluj.ro

19. Januar 2017

Wiederholung

- Negationsnormalform
- Bereinigung
- Pränexnormalform
- Skolemnormalform

Skolem Normalform

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

- F ist in Pränexnormalform
- F enthält nur universelle Quantoren

Beispiele:

In Skolemnormalform

$$\forall x \forall y (p(x) \vee q(y))$$

Nicht in Skolemnormalform

$$\forall x\, p(x) \vee \forall y\, q(y)$$

$$\forall x \exists y\, (p(x) \vee q(y))$$

Skolemisierung

Skolemisierung: Transformation $\Rightarrow_S$:

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

wobei f/n ein neues Funktionssymbol (Skolemfunktion).

Skolemisierung: Beispiel

Gegeben:

$\forall w(\exists x(p(w,x) \vee \forall y\,(q(w,x,y) \wedge \exists z\, r(y,z))))$

Pränexnormalform:

$\forall w \exists x \forall y \exists z((p(w,x) \vee (q(w,x,y) \wedge r(y,z))))$

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

$\forall w \forall y((p(w, sk_x(w)) \vee (q(w, sk_x(w), y) \wedge r(y, sk_z(w,y)))))$

Skolemisierung

Zusammen:

$$F \overset{*}{\Rightarrow}_P \underbrace{G}_{\text{pränexe Form}} \overset{*}{\Rightarrow}_S \underbrace{H}_{\text{pränex, kein } \exists}$$

Theorem:
Seien F, G und H wie oben angenommen. Dann:

(1) F und G sind äquivalent.

(2) G erfüllbar gdw. H erfüllbar
(bzgl. Σ-Str) (bzgl. Σ'-Str)
wobei $\Sigma' = (\Omega \cup SKF, \Pi)$, wenn $\Sigma = (\Omega, \Pi)$.

Skolemisierung

Lemma. Sei $G = \forall x_1, \dots, x_n \exists y G_1$ und $H = \forall x_1, \dots, x_n G_1[f(x_1, \dots, x_n)/y]$, wobei f ein neues Funktionssymbol (Skolemfunktion) ist.

G erfüllbar (bezgl. Σ-Str.) genau dann, wenn H erfüllbar (bezgl. Σ'-Str.).

wobei: $\Sigma = (\Omega, \Pi)$ und $\Sigma' = (\Omega \cup \{f\}, \Pi)$.

Beweis: (1) G erfüllbar $\Rightarrow$ H erfüllbar

Sei $\mathcal{A}$ eine Σ-Struktur und $\beta : X \to U_\mathcal{A}$ mit $\mathcal{A}(\beta)(G) = 1$.

$$\begin{aligned} 1 = \mathcal{A}(\beta)(G) &= \min_{a_1,\dots,a_n \in U_\mathcal{A}} \mathcal{A}(\beta[x_1 \mapsto a_1, \dots, x_n \mapsto a_n])(\exists y G_1) \\ &= \min_{a_1,\dots,a_n \in U_\mathcal{A}} \max_{b \in U_\mathcal{A}} \mathcal{A}(\beta[x_1 \mapsto a_1, \dots, x_n \mapsto a_n, y \mapsto b])(G_1) \end{aligned}$$

d.h. für alle $a_1, \dots, a_n \in U_\mathcal{A}$ es gibt ein $b \in U_\mathcal{A}$ mit:
$\mathcal{A}(\beta[x_1 \mapsto a_1, \dots, x_n \mapsto a_n, y \mapsto b])(G_1) = 1$.

Wir definieren eine Σ'-struktur $\mathcal{A}'$, in der alle Funktionen und Prädikate in Σ wie in $\mathcal{A}$ definiert sind und in der wir für alle $a_1, \dots, a_n \in U_\mathcal{A}$, $f(a_1, \dots, a_n) := b$ definieren.

Dann $\mathcal{A}'(\beta[x_1 \mapsto a_1, \dots, x_n \mapsto a_n])(G_1[f(x_1, \dots, x_n)/y]) = 1$.

Skolemisierung

Lemma. Sei $G = \forall x_1, \ldots, x_n \exists y G_1$ und $H = \forall x_1, \ldots, x_n G_1[f(x_1, \ldots, x_n)/y]$, wobei f ein neues Funktionssymbol (Skolemfunktion) ist.

G erfüllbar (bezgl. Σ-Str.) genau dann, wenn H erfüllbar (bezgl. Σ'-Str.).

wobei: $\Sigma = (\Omega, \Pi)$ und $\Sigma' = (\Omega \cup \{f\}, \Pi)$.

Beweis: (2) H erfüllbar $\Rightarrow$ G erfüllbar

Sei $\mathcal{A}'$ eine Σ'-Struktur und $\beta : X \to U_{\mathcal{A}'}$ mit $\mathcal{A}'(\beta)(H) = 1$.

$$\begin{aligned} 1 = \mathcal{A}'(\beta)(H) &= \min_{a_1,\ldots,a_n \in U_{\mathcal{A}'}} \mathcal{A}'(\beta[x_1 \mapsto a_1, \ldots, x_n \mapsto a_n])(G_1[f(x_1, \ldots, x_n)/y]) \\ &= \min_{a_1,\ldots,a_n \in U_{\mathcal{A}'}} (\beta[x_1 \mapsto a_1, \ldots, x_n \mapsto a_n, y \mapsto f_{\mathcal{A}'}(a_1, \ldots, a_n)])(G_1) \end{aligned}$$

d.h. für alle $a_1, \ldots, a_n \in U_{\mathcal{A}'}$ es gibt ein $b = f_{\mathcal{A}'}(a_1, \ldots, a_n) \in U_{\mathcal{A}'}$ mit: $\mathcal{A}(\beta[x_1 \mapsto a_1, \ldots, x_n \mapsto a_n, y \mapsto b])(G_1) = 1$.

$$\begin{aligned} \text{Dann gilt: } \mathcal{A}(\beta)(G) &= \min_{a_1,\ldots,a_n \in U_{\mathcal{A}}} \mathcal{A}(\beta[x_1 \mapsto a_1, \ldots, x_n \mapsto a_n])(\exists y G_1) \\ &= \min_{a_1,\ldots,a_n \in U_{\mathcal{A}}} \max_{b \in U_{\mathcal{A}}} \mathcal{A}(\beta[x_1 \mapsto a_1, \ldots, x_n \mapsto a_n, y \mapsto b])(G_1) = 1 \end{aligned}$$

wobei $\mathcal{A}$ ist $\mathcal{A}'$ ohne die Funktion f.

Skolemisierung

Theorem:

Seien F, G und H wie oben angenommen. Dann:

(1) F und G sind äquivalent.

(2) G erfüllbar (bzgl. Σ-Str) gdw. H erfüllbar (bzgl. Σ'-Str)

wobei $\Sigma' = (\Omega \cup SKF, \Pi)$, wenn $\Sigma = (\Omega, \Pi)$.

Klauselnormalform (konjunktive Normalform

Transformationsregeln $\Rightarrow_K$

(1)	$(F \leftrightarrow G)$	$\Rightarrow_K$	$(F \rightarrow G) \wedge (G \rightarrow F)$	
(2)	$(F \rightarrow G)$	$\Rightarrow_K$	$(\neg F \vee G)$	
(3)	$\neg(F \vee G)$	$\Rightarrow_K$	$(\neg F \wedge \neg G)$	
(4)	$\neg(F \wedge G)$	$\Rightarrow_K$	$(\neg F \vee \neg G)$	
(5)	$\neg\neg F$	$\Rightarrow_K$	F	
$(\neg\forall)$	$\neg\forall x F$	$\Rightarrow_K$	$\exists x \neg F$	
$(\neg\exists)$	$\neg\exists x F$	$\Rightarrow_K$	$\forall x \neg F$	(NNF)

(P) Pränex Normalform

(S) Skolemisierung

(6)	$(F \wedge G) \vee H$	$\Rightarrow_K$	$(F \vee H) \wedge (G \vee H)$	
(7)	$(F \wedge \top)$	$\Rightarrow_K$	F	
(8)	$(F \wedge \bot)$	$\Rightarrow_K$	$\bot$	
(9)	$(F \vee \top)$	$\Rightarrow_K$	$\top$	
(10)	$(F \vee \bot)$	$\Rightarrow_K$	F	(KNF)

Übersicht

$$F \quad \overset{*}{\Rightarrow}_P \quad Q_1 y_1 \dots Q_n y_n \; G$$

(G quantorenfrei) Pränexnormalform

$$\overset{*}{\Rightarrow}_S \quad \forall x_1, \dots, x_m \; H$$

(H quantorenfrei) Skolemnormalform

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

Skolemnormalform mit Matrix in KNF

$N = \{C_1, \dots, C_k\}$ 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

$$F := \exists z\Big(\big(\forall x(p(u,z,x))\big) \rightarrow \big(\forall y(q(z,y) \wedge (\exists x r(y,x)))\big)\Big)$$

Beispiel

$$F := \exists z\Big((\forall x(p(u,z,x))) \rightarrow (\forall y(q(z,y) \wedge (\exists x r(y,x)))) \Big)$$

Pränexnormalform:

$$\begin{aligned}
F &\equiv \exists z\Big((\neg\forall x p(u,z,x)) \vee (\forall y(q(z,y) \wedge (\exists x r(y,x)))) \Big) & \\
&\equiv \exists z\Big((\exists x \neg p(u,z,x)) \vee (\forall y(q(z,y) \wedge (\exists x r(y,x)))) \Big) & \text{(NNF)} \\
&\equiv \exists z\Big((\exists x \neg p(u,z,x)) \vee (\forall y(q(z,y) \wedge (\exists x_1 r(y,x_1)))) \Big) & \text{(Bereinigung)} \\
&\equiv \exists z \exists x \forall y \exists x_1 (\neg p(u,z,x) \vee (q(z,y) \wedge r(y,x_1))) & \text{(Pränexnormalform)}
\end{aligned}$$

Beispiel

$$F := \exists z\Big((\forall x(p(u,z,x))) \to (\forall y(q(z,y) \wedge (\exists x r(y,x)))) \Big)$$

Pränexnormalform:

$$\begin{aligned}
F &\equiv \exists z\Big((\neg\forall x p(u,z,x)) \vee (\forall y(q(z,y) \wedge (\exists x r(y,x)))) \Big) & \\
&\equiv \exists z\Big((\exists x \neg p(u,z,x)) \vee (\forall y(q(z,y) \wedge (\exists x r(y,x)))) \Big) & \text{(NNF)} \\
&\equiv \exists z\Big((\exists x \neg p(u,z,x)) \vee (\forall y(q(z,y) \wedge (\exists x_1 r(y,x_1)))) \Big) & \text{(Bereinigung)} \\
&\equiv \exists z \exists x \forall y \exists x_1 (\neg p(u,z,x) \vee (q(z,y) \wedge r(y,x_1))) & \text{(Pränexnormalform)}
\end{aligned}$$

Skolemisierung $u \mapsto sk_u$, $z \mapsto sk_z$; $x \mapsto sk_x$; $x_1 \mapsto sk_{x_1}(y)$

$$\Rightarrow_S^* \ \forall y(\neg p(sk_u, sk_z, sk_x) \vee (q(sk_z, y) \wedge r(y, sk_{x_1}(y))))$$

(Erfüllbarkeitsäquivalente Formel in Skolemnormalform)

Beispiel

$$F := \exists z\Big((\forall x(p(u,z,x))) \rightarrow (\forall y(q(z,y) \wedge (\exists x r(y,x)))) \Big)$$

Pränexnormalform:

$$\begin{aligned}
F &\equiv \exists z\Big((\neg\forall x p(u,z,x)) \vee (\forall y(q(z,y) \wedge (\exists x r(y,x)))) \Big) \\
&\equiv \exists z\Big((\exists x \neg p(u,z,x)) \vee (\forall y(q(z,y) \wedge (\exists x r(y,x)))) \Big) && \text{(NNF)} \\
&\equiv \exists z\Big((\exists x \neg p(u,z,x)) \vee (\forall y(q(z,y) \wedge (\exists x_1 r(y,x_1)))) \Big) && \text{(Bereinigung)} \\
&\equiv \exists z \exists x \forall y \exists x_1 (\neg p(u,z,x) \vee (q(z,y) \wedge r(y,x_1))) && \text{(Pränexnormalform)}
\end{aligned}$$

Skolemisierung $u \mapsto sk_u,\ z \mapsto sk_z;\ x \mapsto sk_x;\ x_1 \mapsto sk_{x_1}(y)$

$$\Rightarrow^*_S \ \forall y(\neg p(sk_u, sk_z, sk_x) \vee (q(sk_z, y) \wedge r(y, sk_{x_1}(y))))$$

(Erfüllbarkeitsäquivalente Formel in Skolemnormalform)

Skolemnormalform mit Matrix in KNF:

$$\Rightarrow^*_K \ \forall y((\neg p(sk_u, sk_z, sk_x) \vee q(sk_z, y)) \wedge (\neg p(sk_u, sk_z, sk_x) \vee r(y, sk_{x_1}(y))))$$

Klauselmenge: $N = \{\{\neg p(sk_u, sk_z, sk_x), q(sk_z, y)\}, \{\neg p(sk_u, sk_z, sk_x), r(y, sk_{x_1}(y))\}\}$

Resolution für Grundklauseln

Aussagenlogische Klauseln entsprechen Grundklauseln und umgekehrt.

Resolutionsregel:

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

$C \cup D$: Resolvente

A: resolviertes Atom

Beispiel

1.	$\{\neg P(f(a)),\quad Q(b)\}$	(gegeben)
2.	$\{P(f(a)),\quad Q(b)\}$	(gegeben)
3.	$\{\neg P(g(b,a)),\quad \neg Q(b)\}$	(gegeben)
4.	$\{P(g(b,a))\}$	(gegeben)
5.	$\{Q(b)\}$	(Res. 2. in 1.)
6.	$\{\neg P(g(b,a))\}$	(Res. 5. in 3.)
8.	$\perp$	(Res. 4. in 6.)

Resolution für Grundklauseln

Resolutionsregel:

$$\frac{C \lor A \qquad \neg A \lor D}{C \lor D}$$

$C \lor D$: Resolvente

A: resolviertes Atom

Faktorisieren:

$$\frac{C \lor L \lor L}{C \lor L}$$

„$\lor$“ wird in Klauseln als assoziativ und kommutativ aufgefaßt.

Beispiel

1.	$\neg P(f(a)) \vee \neg P(f(a)) \vee Q(b)$	(gegeben)
2.	$P(f(a)) \vee Q(b)$	(gegeben)
3.	$\neg P(g(b,a)) \vee \neg Q(b)$	(gegeben)
4.	$P(g(b,a))$	(gegeben)
5.	$\neg P(f(a)) \vee Q(b) \vee Q(b)$	(Res. 2. in 1.)
6.	$\neg P(f(a)) \vee Q(b)$	(Fakt. 5.)
7.	$Q(b) \vee Q(b)$	(Res. 2. in 6.)
8.	$Q(b)$	(Fakt. 7.)
9.	$\neg P(g(b,a))$	(Res. 8. in 3.)
10.	$\perp$	(Res. 4. in 9.)

Korrektheit und Vollständigkeit

- Aussagenlogische Resolution ist korrekt und vollständig.
- Mengennotation: Resolutionsregel
- Klauselnotation: Resolutionsregel + Faktorisieren

Prädikatenlogische Resolution

Grundidee

- Vor Resolutionsschritt durch geeignete Substitution komplementäres Paar von Literalen erzeugen

Prädikatenlogische Resolution

Möglichkeit für Resolutionsregel

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

wobei

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

Prädikatenlogische Resolution

Grundidee

Vor Resolutionsschritt durch geeignete Substitution komplementäres Paar von Literalen erzeugen

Möglichkeit für Resolutionsregel

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

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 $\sigma(L) = \sigma(L')$

Beispiel

$$\frac{\{p(x,f(x)), q(f(x))\} \qquad \{\neg r(f(y)), \neg q(y)\}}{\{p(x,f(x))\sigma, \neg r(f(y))\sigma\}}$$

$L = q(f(x)),\ L' = q(y)$

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

σ_1	$\sigma_1(x) = a,\ \sigma_1(y) = f(a)$
σ_1	$\sigma_1(x) = f(a),\ \sigma_1(y) = f(f(a))$
...	

Beispiel

$$\frac{\{p(x,f(x)), q(f(x))\} \qquad \{\neg r(f(y)), \neg q(y)\}}{\{p(x,f(x))\sigma, \neg r(f(y))\sigma\}}$$

$L = q(f(x)),\, L' = q(y)$

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

σ_1	$\sigma_1(x) = a,\ \sigma_1(y) = f(a)$
σ_1	$\sigma_1(x) = f(a),\ \sigma_1(y) = f(f(a))$
$\ldots$	

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

$q(f(x)) \stackrel{?}{=} q(y) \quad \Rightarrow \quad f(x) \stackrel{?}{=} y \quad \Rightarrow \quad y \stackrel{?}{=} f(x)$

$\sigma = [f(x)/y] \qquad \sigma(y) = f(x),\ \sigma(z) = z$ for $z \neq y$.

Unifikation

Sei $E = \{s_1 \stackrel{?}{=} t_1, \ldots, s_n \stackrel{?}{=} t_n\}$ (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

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

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

[a] Ist wohldefiniert, weil $\sigma \circ \varrho$ einen endlichen Bereich hat.

Beispiel

$E = \{q(f(x)) \stackrel{?}{=} q(y)\}$

$\sigma_1 = [a/x, f(a)/y]$ ist ein Unifikator von E

$\sigma_2 = [f(a)/x, f(f(a))/y]$ ist ein Unifikator von E

$\sigma = [f(x)/y]$ ist ein Unifikator von E

σ ist allgemeiner als σ_1 und als σ_2:

$\sigma_1 = \sigma \circ [a/x]$

$$\sigma \circ [a/x](y) = \sigma(y)[a/x] = f(x)[a/x] = f(a)$$
$$\sigma \circ [a/x](x) = \sigma(x)[a/x] = x[a/x] = a$$

$\sigma_2 = \sigma \circ [f(a)/x]$

$$\sigma \circ [f(a)/x](y) = \sigma(y)[f(a)/x] = f(x)[f(a)/x] = f(f(a))$$
$$\sigma \circ [f(a)/x](x) = \sigma(x)[f(a)/x] = x[f(a)/x] = f(a)$$

Fakten

- Jeder Term ist mit sich selbst unifizierbar (mittels id)
- Terme der Gestalt $f(s_1, \ldots, s_n)$, $f(t_1, \ldots, t_n)$ sind unifizierbar g.d.w. si und t_i unifizierbar für $1 \leq i \leq n$
- Atome der Gestalt $p(s_1, \ldots, s_n)$, $p(t_1, \ldots, t_n)$ sind unifizierbar g.d.w. si und t_i unifizierbar für $1 \leq i \leq n$
- Terme der Gestalt $f(s_1, \ldots, s_n)$, $g(t_1, \ldots, t_m)$ sind niemals unifb.
- Atome der Gestalt $p(s_1, \ldots, s_n)$, $q(t_1, \ldots, t_n)$ sind niemals unifb.
- Eine Variable x und ein Term t, der x nicht enthält, sind immer unifb. (mittels $[t/x]$)
- Eine Variable x und ein Term $t \neq x$, der x enthält, sind niemals unifizierbar

UNIFIKATIONSALGORITHMUS VON MARTELLI/MONTANARI

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

Beispiel 1

$$\{f(g(a,x),g(y,b)) \stackrel{?}{=} f(x,g(v,w)), f(x,g(v,w)) \stackrel{?}{=} f(g(x,a),g(v,b))\}$$

$$\stackrel{(2)}{\Rightarrow}_{MM} \quad \{g(a,x) \stackrel{?}{=} x, g(y,b) \stackrel{?}{=} g(v,w), x \stackrel{?}{=} g(x,a), g(v,w) \stackrel{?}{=} g(v,b)\}$$

$$\stackrel{(5)}{\Rightarrow}_{MM} \quad \perp$$

Beispiel 2

$$\{f(g(a,x),g(y,b)) \stackrel{?}{=} g(x,g(v,w)), f(x,g(v,w)) \stackrel{?}{=} f(g(x,a),g(v,b))\}$$

$$\stackrel{(3)}{\Rightarrow}_{MM} \quad \perp$$

BEISPIEL 3

$$\{f(g(a,x),g(y,b)) \stackrel{?}{=} f(z,g(v,w)), f(z,g(v,w)) \stackrel{?}{=} f(g(x,a),g(v,b)\}$$

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

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

Beispiel 3

$$\{f(g(a,x),g(y,b)) \stackrel{?}{=} f(z,g(v,w)), f(z,g(v,w)) \stackrel{?}{=} f(g(x,a),g(v,b)\}$$

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

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

$$\Rightarrow^{*}_{MM} \quad \{z \stackrel{?}{=} g(a,x), y \stackrel{?}{=} v, b \stackrel{?}{=} w, a \stackrel{?}{=} x, x \stackrel{?}{=} a, v \stackrel{?}{=} v, w \stackrel{?}{=} b\}$$

Beispiel 3

$$\{f(g(a,x),g(y,b)) \stackrel{?}{=} f(z,g(v,w)), f(z,g(v,w)) \stackrel{?}{=} f(g(x,a),g(v,b)\}$$

$$\begin{aligned}
&\stackrel{(2)}{\Rightarrow}_{MM} && \{g(a,x) \stackrel{?}{=} z, g(y,b) \stackrel{?}{=} g(v,w), z \stackrel{?}{=} g(x,a), g(v,w) \stackrel{?}{=} g(v,b)\} \\
&\stackrel{(4)}{\Rightarrow}_{MM} && \{z \stackrel{?}{=} g(a,x), g(y,b) \stackrel{?}{=} g(v,w), g(a,x) \stackrel{?}{=} g(x,a), g(v,w) \stackrel{?}{=} g(v,b)\} \\
&\Rightarrow^*_{MM} && \{z \stackrel{?}{=} g(a,x), y \stackrel{?}{=} v, b \stackrel{?}{=} w, a \stackrel{?}{=} x, x \stackrel{?}{=} a, v \stackrel{?}{=} v, w \stackrel{?}{=} b\} \\
&\Rightarrow^*_{MM} && \{z \stackrel{?}{=} g(a,x), y \stackrel{?}{=} v, b \stackrel{?}{=} w, a \stackrel{?}{=} x, x \stackrel{?}{=} a, w \stackrel{?}{=} b\}
\end{aligned}$$

Beispiel 3

$$\{f(g(a,x),g(y,b)) \stackrel{?}{=} f(z,g(v,w)), f(z,g(v,w)) \stackrel{?}{=} f(g(x,a),g(v,b)\}$$

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

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

$$\Rightarrow^*_{MM} \quad \{z \stackrel{?}{=} g(a,x), y \stackrel{?}{=} v, b \stackrel{?}{=} w, a \stackrel{?}{=} x, x \stackrel{?}{=} a, v \stackrel{?}{=} v, w \stackrel{?}{=} b\}$$

$$\Rightarrow^*_{MM} \quad \{z \stackrel{?}{=} g(a,x), y \stackrel{?}{=} v, b \stackrel{?}{=} w, a \stackrel{?}{=} x, x \stackrel{?}{=} a, w \stackrel{?}{=} b\}$$

$$\Rightarrow^*_{MM} \quad \{z \stackrel{?}{=} g(a,a), y \stackrel{?}{=} v, b \stackrel{?}{=} b, a \stackrel{?}{=} a, x \stackrel{?}{=} a, w \stackrel{?}{=} b\}$$

$$\Rightarrow^*_{MM} \quad \{z \stackrel{?}{=} g(a,a), y \stackrel{?}{=} v, x \stackrel{?}{=} a, w \stackrel{?}{=} b\}$$

Beispiel 3

$$\{f(g(a,x),g(y,b)) \stackrel{?}{=} f(z,g(v,w)), f(z,g(v,w)) \stackrel{?}{=} f(g(x,a),g(v,b))\}$$

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

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

$$\Rightarrow^*_{MM} \quad \{z \stackrel{?}{=} g(a,x), y \stackrel{?}{=} v, b \stackrel{?}{=} w, a \stackrel{?}{=} x, x \stackrel{?}{=} a, v \stackrel{?}{=} v, w \stackrel{?}{=} b\}$$

$$\Rightarrow^*_{MM} \quad \{z \stackrel{?}{=} g(a,x), y \stackrel{?}{=} v, b \stackrel{?}{=} w, a \stackrel{?}{=} x, x \stackrel{?}{=} a, w \stackrel{?}{=} b\}$$

$$\Rightarrow^*_{MM} \quad \{z \stackrel{?}{=} g(a,a), y \stackrel{?}{=} v, b \stackrel{?}{=} b, a \stackrel{?}{=} a, x \stackrel{?}{=} a, w \stackrel{?}{=} b\}$$

$$\Rightarrow^*_{MM} \quad \{z \stackrel{?}{=} g(a,a), y \stackrel{?}{=} v, x \stackrel{?}{=} a, w \stackrel{?}{=} b\}$$

Allgemeinster Unifikator:

$$[g(a,a)/z, v/y, a/x, b/w]$$

Vorsicht: a, b sind Konstanten. $[g(a,a)/z, v/y, x/a, w/b]$ ist keine Substitution!

Beispiel 4

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

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

Beispiel 4

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

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

$$\begin{array}{llllll}
\stackrel{(2)}{\Rightarrow}_{MM} & \{g(y,a) \stackrel{?}{=} z, & g(f(x,b), z) \stackrel{?}{=} g(f(g(u,y), b), u), & & & q(a) \stackrel{?}{=} q(y)\} \\
\stackrel{(6,2)}{\Rightarrow}_{MM} & \{z \stackrel{?}{=} g(y,a), & f(x,b) \stackrel{?}{=} f(g(u,y), b), & z \stackrel{?}{=} u, & & q(a) \stackrel{?}{=} q(y)\} \\
\stackrel{(4)}{\Rightarrow}_{MM} & \{z \stackrel{?}{=} g(y,a), & f(x,b) \stackrel{?}{=} f(g(u,y), b), & g(y,a) \stackrel{?}{=} u, & & q(a) \stackrel{?}{=} q(y)\} \\
\stackrel{(2,6)}{\Rightarrow}_{MM} & \{z \stackrel{?}{=} g(y,a), & x \stackrel{?}{=} g(u,y), b \stackrel{?}{=} b, & u \stackrel{?}{=} g(y,a), & & q(a) \stackrel{?}{=} q(y)\} \\
\stackrel{(1)}{\Rightarrow}_{MM} & \{z \stackrel{?}{=} g(y,a), & x \stackrel{?}{=} g(u,y), & u \stackrel{?}{=} g(y,a), & & q(a) \stackrel{?}{=} q(y)\} \\
\stackrel{(4)}{\Rightarrow}_{MM} & \{z \stackrel{?}{=} g(y,a), & x \stackrel{?}{=} g(g(y,a), y), & u \stackrel{?}{=} g(y,a), & & g(a) \stackrel{?}{=} g(y)\} \\
\stackrel{(2)}{\Rightarrow}_{MM} & \{z \stackrel{?}{=} g(y,a), & x \stackrel{?}{=} g(g(y,a), y), & u \stackrel{?}{=} g(y,a), & & a \stackrel{?}{=} y\} \\
\stackrel{(6)}{\Rightarrow}_{MM} & \{z \stackrel{?}{=} g(y,a), & x \stackrel{?}{=} g(g(y,a), y), & u \stackrel{?}{=} g(y,a), & & y \stackrel{?}{=} a\} \\
\stackrel{(4)}{\Rightarrow}_{MM} & \{z \stackrel{?}{=} g(a,a), & x \stackrel{?}{=} g(g(a,a), a), & u \stackrel{?}{=} g(a,a), & & y \stackrel{?}{=} a\}
\end{array}$$

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 Substitition 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 unifizierbar gdw. $E \Rightarrow^*_{MM} x_1 \stackrel{?}{=} u_1, \ldots, x_k \stackrel{?}{=} u_k$,
   mit x_i pw. verschieden, $x_i \notin var(u_j), 1 \leq i, j \leq k$.
3. Falls $E \Rightarrow^*_{MM} x_1 \stackrel{?}{=} u_1, \ldots, x_k \stackrel{?}{=} u_k$,
   mit x_i pw. verschieden, $x_i \notin var(u_j)$ so
   $\sigma = [u_1/x_1, \ldots, u_k/x_k]$ ist allgemeinster 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: $\sigma = \mathrm{mgu}(E)$ („most general unifier“)

Prädikatenlogische Resolution

Grundidee

Vor Resolutionsschritt durch geeignete Substitution komplementäres Paar von Literalen erzeugen

Möglichkeit für Resolutionsregel

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

wobei

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

Beispiel

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

Allgemeinster Unifikator von L, L':

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

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

Beispiel

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

Allgemeinster Unifikator von L, L':

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

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

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

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

Beispiel

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

Allgemeinster Unifikator von L, L':

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

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

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

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

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

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

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

wobei

- σ allgemeinster Unifikator (MGU) von $\{L_1, \ldots, L_n\}$ ist

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

Beispiel für Faktorisierung

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

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

$$\frac{\{p(b),p(y),p(a),r(y,z)\}}{\{p(b),p(a),r(b,z)\}} \qquad \text{mgu}(p(b), p(y)) = [b/y]$$

$$\frac{\{p(b),p(y),p(a),r(y,z)\}}{\{p(b),p(a),r(a,z)\}} \qquad \text{mgu}(p(y), p(a)) = [a/y]$$

RESOLUTIONSKALKÜL RES FÜR ALLGEMEINE KLAUSELN

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

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

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

Notation

Sei N eine Klauselmenge und

$$\begin{aligned}\text{Res}(N) = N \cup \{R \mid\ & R \text{ ist eine Resolvente zweier Klauseln aus } N \\ & \text{oder Resultat der Faktorisierung einer Klausel aus } N\}\end{aligned}$$

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

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

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

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

Anwendungen

- Logische Programmierung (Prolog, Answer Set Programming)
- Industrielle Anwendungen
- SAT Solver
- Theorem Prover
- Software Verifikation

Last but not least

Nicht vergessen Spass zu haben!