Karlsruher Institut für Technologie
Institut für Theoretische Informatik
Prof. Dr. Bernhard Beckert
Dr. Thorsten Bormer, Dr. Vladimir Klebanov, Dr. Mattias Ulbrich

Formale Systeme, WS 2015/2016

Übungsblatt 4

Dieses Übungsblatt wird in der Übung am 27.11.2015 besprochen.

Aufgabe 1

Tante Agathe wurde in ihrem Haus tot aufgefunden. Nach bisherigen Ermittlungen gilt Folgendes als sicher:

1. Im Haus lebten nur Agathe, ihr Butler und Onkel Charles.
2. Agathe wurde von einem Hausbewohner getötet.
3. Wer jemanden tötet, hasst sein Opfer.
4. Charles hasst niemanden, den Agathe hasste.
5. Der Täter ist niemals reicher als das Opfer.
6. Der Butler hasst alle, die nicht reicher als Agathe sind oder die Agathe hasste.
7. Kein Bewohner des Hauses hasst(e) alle Hausbewohner.

Gegeben ist ferner die prädikatenlogische Signatur $\Sigma_{Agathe} = (F, P, \alpha)$ mit

- $P = \{\text{kills}, \text{hates}, \text{richer}\}$
- $F = \{a, b, c\}$
- $\alpha(a) = \alpha(b) = \alpha(c) = 0, \qquad \alpha(\text{kills}) = \alpha(\text{hates}) = \alpha(\text{richer}) = 2$

Formalisieren Sie die Aussagen 1-7 in Prädikatenlogik mit dem Vokabular aus Σ_{Agathe}.

Lösung zu Aufgabe 1

1. $\forall x(x \doteq a \vee x \doteq b \vee x \doteq c)$
2. $\exists x(\text{kills}(x, a))$
   eigentlich gehört aber die Aussage 1. (Stichwort Hausbewohner) noch mit in die Kodierung, so dass die (in Kombination mit (1) äquivalente) Formel $\exists x(\text{kills}(x, a) \wedge (x \doteq a \vee x \doteq b \vee x \doteq c) \equiv \text{kills}(a, a) \vee \text{kills}(b, a) \vee \text{kills}(c, a)$ noch exakter formalisiert.
3. $\forall x \forall y(\text{kills}(x, y) \to \text{hates}(x, y))$
4. $\forall x(\text{hates}(a, x) \to \neg\text{hates}(c, x))$
5. $\forall x \forall y(\text{kills}(x, y) \to \neg\text{richer}(x, y))$

6. $\forall x((\neg \mathrm{richer}(x,a) \lor \mathrm{hates}(a,x)) \rightarrow \mathrm{hates}(b,x))$

7. $\neg \exists x \forall y(\mathrm{hates}(x,y))$

Aufgabe 2

(a) Betrachten Sie jeweils die folgenden Substitutionen σ und Formeln F. Falls σ für F kollisionsfrei ist, geben Sie $\sigma(F)$ an; andernfalls geben Sie an, wo eine Kollision auftritt.

(i)	$\sigma = \{x/c,\ y/f(c, g(x))\}$	$F = \forall x(p(g(x), f(x,y)) \lor q(x))$
(ii)	$\sigma = \{x/f(g(x), c)\}$	$F = \exists y(p(x,y) \lor \exists z \forall x(f(z,c) \doteq f(c,x)))$
(iii)	$\sigma = \{y/g(x),\ z/g(y)\}$	$F = p(x,y) \rightarrow \forall x(q(f(x,z)) \lor \exists y(q(f(x,y))))$

(b) Betrachten Sie jeweils die folgenden Formeln F und G. Geben Sie einen allgemeinsten Unifikator μ sowie das Ergebnis $\mu(F) = \mu(G)$ der Unifikation an, falls sie unifizierbar sind.

(Hierbei sind a, b Konstanten, f, g, h Funktionssymbole und v, x, y, z Variablen.)

(i)	$F = f(x,z,z)$	$G = f(g(a,y), h(v), h(y))$
(ii)	$F = f(g(x,z), z, h(b,x))$	$G = f(g(a,y), h(v,a), y)$
(iii)	$F = g(x,y)$	$G = g(f(y), f(x))$
(iv)	$F = f(g(y), h(y, g(y)))$	$G = f(z, h(g(x), g(g(x))))$

Lösung zu Aufgabe 2

(a) (i) Nicht kollisionsfrei, da

- x kommt in $\sigma(y)$ vor.
- y kommt im Wirkungsbereich des Quantors $\forall x$ vor.

(ii) Kollisionsfrei, das zweite Auftreten von x (dort gebundene Variable!) wird nicht ersetzt.

$$\sigma(F) = \exists y(p(y, f(g(x), c)) \lor \forall x \exists z(f(z,c) \doteq f(c,x)))$$

(iii) Kollisionsfrei (das zweite Vorkommen von y wird nicht ersetzt)

$$\sigma(F) = p(x, g(x)) \rightarrow \forall x(q(f(x, g(y))) \lor \exists y(q(f(x,y))))$$

(b) (i) unifizierbar. Robinson ergibt:

$\mu_0 = id$	$\mu_0(F) = f(\boxed{x}, z, z)$	$\mu_0(G) = f(\boxed{g(a,y)}, h(v), h(y))$
$\mu_1 = \{x/g(a,y)\}$	$\mu_1(F) = f(g(a,y), \boxed{z}, z)$	$\mu_1(G) = f(g(a,y), \boxed{h(v)}, h(y))$
$\mu_2 = \{x/g(a,y), z/h(v)\}$	$\mu_2(F) = f(g(a,y), h(v), h(\boxed{v}))$	$\mu_2(G) = f(g(a,y), h(v), h(\boxed{y}))$
$\mu_3 = \{x/g(a,y), z/h(y), v/y\}$	$\mu_3(F) = \mu_3(G) = f(g(a,y), h(y), h(y))$	

Man muss beachten, dass man weitere Ersetzungen nicht einfach zur Menge hinzunehmen kann, sondern auch auf die darin enthaltenen Terme anwenden muss.
Beispielsweise: $\mu_3 = \{x/g(a,y), z/h(\boldsymbol{v})\} \circ \{v/\boldsymbol{y}\} = \{x/g(a,y), z/h(\boldsymbol{y}), v/y\}$

(ii) unifizierbar. Robinson ergibt:

$$\begin{array}{ll}
\mu_0 = id & \mu_0(F) = f(g(\boxed{x}, z), z, h(b, x)) \\
 & \mu_0(G) = f(g(\boxed{a}, y), h(v, a), y) \\
\mu_1 = \{x/a\} & \mu_1(F) = f(g(a, \boxed{z}), z, h(b, a)) \\
 & \mu_1(G) = f(g(a, \boxed{y}), h(v, a), y) \\
\mu_2 = \{x/a, z/y\} & \mu_2(F) = f(g(a, y), \boxed{y}, h(b, a)) \\
 & \mu_2(G) = f(g(a, y), \boxed{h(v, a)}, y) \\
\mu_3 = \{x/a, z/h(v, a), y/h(v, a)\} & \mu_3(F) = f(g(a, h(v, a)), h(v, a), h(\boxed{b}, a)) \\
 & \mu_3(G) = f(g(a, h(v, a)), h(v, a), h(\boxed{v}, a)) \\
\mu_4 = \{x/a, z/h(b, a), y/h(b, a), v/b\} & \mu_4(F) = \mu_4(G) = f(g(a, h(b, a)), h(b, a), h(b, a))
\end{array}$$

(iii) Im ersten Schritt des Robinsonalgorithmus erhält man:

$$\begin{array}{rcl}
\mu_1 & = & \{x/f(y)\} \\
\mu_1(F) & = & g(f(y), y) \\
\mu_1(G) & = & g(f(y), f(f(y)))
\end{array}$$

Nun aber muss der Algorithmus abbrechen, weil $D(\{\mu_1(F), \mu_1(G)\}) = \{y, f(f(y))\}$ und die sind nicht unifizierbar, weil y eine Variable ist und in $f(f(y))$ auftritt.

(iv) unifizierbar. Der Robinsonalgorithmus mit Zwischenergebnissen:

$$\begin{array}{lll}
\mu_0 = id & \mu_0(F) = f(\boxed{g(y)}, h(y, g(y))) & \mu_0(G) = f(\boxed{z}, h(g(x), g(g(x)))) \\
\mu_1 = \{z/g(y)\} & \mu_1(F) = f(g(y), h(\boxed{y}, g(y))) & \mu_1(G) = f(g(y), h(\boxed{g(x)}, g(g(x)))) \\
\mu_2 = \{z/g(g(x)), y/g(x)\} & \multicolumn{2}{c}{\mu_2(F) = \mu_2(G) = f(g(g(x)), h(g(x), g(g(x))))}
\end{array}$$

Aufgabe 3

Geben Sie eine Folge

$$(s_1, t_1),\ (s_2, t_2),\ (s_3, t_3),\ \ldots$$

von Termpaaren an, so daß:

- Für alle $n \in \mathbb{N}$ sind s_n und t_n unifizierbar.
- Die Größe der Terme s_n und t_n wächst (höchstens) linear in n.
- Die Größe des Ergebnisses $\sigma_n(s_n)$ bzw. $\sigma_n(t_n)$ der Unifikation (σ_n ist ein allgemeinster Unifikator von s_n und t_n) wächst exponentiell in n.

Hinweis: Betrachten Sie die Terme $g(x_1, x_2)$ und $g(c, f(x_1, x_1))$, und verallgemeinern Sie.

Lösung zu Aufgabe 3

$$\begin{array}{rcl}
s_n & := & g(x_1, x_2, \ldots, x_{n-1}, x_n) \\
t_n & := & g(c, f(x_1, x_1), f(x_2, x_2), \ldots, f(x_{n-1}, x_{n-1}))
\end{array}$$

Die Länge $|s_n|$ von s_n ist $n + 1$ und $|t_n|$ ist $3n - 1$, also linear in n (Klammern und Kommata nicht gezählt). Der allgemeinste Unifikator instantiiert x_1 mit c und x_{i+1} mit $f(x_i, x_i)$ $(1 \leq i < n)$. Darum gilt

$$\begin{array}{rcll}
|\sigma(x_1)| & = & 1 & \\
|\sigma(x_i + 1)| & = & 1 + 2 \cdot |\sigma(x_i)| & \text{für } 1 \leq i < n
\end{array}$$

und also

$$|\sigma(x_i)| = 2^i - 1 \qquad \text{für } 1 \le i \le n$$

Schließlich

$$\begin{aligned} |\sigma(s_n)| = |\sigma(t_n)| &= 1 + \sum_{i=1}^{n}(2^i - 1) \\ &= 2^{n+1} - n + 1 \end{aligned}$$

Die Länge von $\sigma_n(s_n) = \sigma(t_n)$ ist also exponentiell in n.

Aufgabe 4

Sei Σ eine prädikatenlogische Signatur mit einem zweistelligen Prädikatensymbol p.

(a) Geben Sie eine prädikatenlogische Formel F über Σ an, so dass gilt: Eine Interpretation (D, I) ist genau dann Modell von F, wenn die Relation $I(p)$ eine *strikte Halbordnung* (also transitiv und irreflexiv) auf D ist.

(b) Geben Sie eine erfüllbare prädikatenlogische Formel G über Σ an, so dass gilt: Wenn eine Interpretation (D, I) Modell von G ist, dann ist D unendlich.

Lösung zu Aufgabe 4

(a) Axiomatisiere p als strikte Halbordnung

- p ist transitiv: $\forall x \forall y \forall z(p(x, y) \wedge p(y, z) \rightarrow p(x, z))$
- p ist irreflexiv: $\forall x \neg p(x, x)$

Also insgesamt: $F = (\forall x \forall y \forall z(p(x, y) \wedge p(y, z) \rightarrow p(x, z))) \wedge (\forall x \neg p(x, x))$

(b) Die Unendlichkeit eines Modells kann erzwungen werden, wenn man im Universum eine unendlich aufsteigende Kette fordern kann.

Dies kann durch

$$U = \forall x \exists y(p(x, y))$$

gemacht werden. Setze also

$$G = U \wedge F \ .$$

Sei (D, I) ein beliebiges Modell von G. Dann ist die Relation $I(p) \subseteq D \times D$ zyklenfrei. Hätte sie einen Zyklus $z_1 \xrightarrow{I(p)} z_2 \xrightarrow{I(p)} \ldots \xrightarrow{I(p)} z_r$, so würde wegen der Transitiviät auch $z_0 \xrightarrow{I(p)} z_0$ gelten und es ein Element geben, das reflexiv bzgl. $I(p)$ ist. Das widerspräche aber der axiomatisierten Irreflexitivität.

Sei (D, I) ein beliebiges Modell und $d_0 \in D$ beliebiges Element. Dann gibt es eine unendliche Kette $(d_0 \xrightarrow{I(p)} d_1 \xrightarrow{I(p)} \ldots)$ mit $d_i \in D$ und $(d_i, d_{i+1}) \in I(p)$. Die Existenz eines Nachfolgers wird durch U sichergestellt.

Da die Folge keinen Zyklus enthalten darf, müssen die d_i paarweise verschieden sein und damit die Menge D unendlich.