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

Formale Systeme, WS 2014/2015

Übungsblatt 5

Dieses Übungsblatt wird in der Übung am 28.11.2014 besprochen.

Aufgabe 1

In dieser Aufgabe sollen Aussagen über Verwandtschaftsbeziehungen in Prädikatenlogik formalisiert werden. Die Signatur $\Sigma_{\text{Verwandtschaft}}$ enthalte die zweistelligen Prädikate *mutter* und *vater*. Formeln werden in Interpretationen ausgewertet, in denen das Universum eine Menge von Personen ist. Dabei bedeutet die Aussage $I(\mathit{mutter})(a, b)$ (bzw. $I(\mathit{vater})(a, b)$), dass a die Mutter (der Vater) von b ist. Formalisieren Sie in der Signatur $\Sigma_{\text{Verwandtschaft}}$:

(a) „Jede Person hat genau eine Mutter.“

(b) „Niemand kann ein Elternteil seiner eigenen Eltern sein.“

(c) „Dagobert ist der Onkel von Donald.“
Seien dazu *Donald* und *Dagobert* zwei Konstantensymbole in $\Sigma_{\text{Verwandtschaft}}$.

Lösung zu Aufgabe 1

(a) $\forall x \exists y (\mathit{mutter}(y, x)) \;\wedge\; \forall x \forall y \forall z (\mathit{mutter}(x, z) \wedge \mathit{mutter}(y, z) \to x \doteq y)$

Das erste Konjunkt besagt, dass jede Person x (mindestens) eine Mutter y hat. Das zweite sagt aus, dass jede Person *höchstens* eine Mutter hat: Wenn es zwei Mütter x und y von z gibt, so müssen diese gleich sein.

(b) $\forall x \forall y \big((\mathit{mutter}(x, y) \vee \mathit{vater}(x, y)) \to (\neg \mathit{mutter}(y, x) \wedge \neg \mathit{vater}(y, x))\big)$

Wenn x Mutter oder Vater von y ist, so kann y weder Mutter von x von Vater von x sein.

(c)
$$\begin{array}{ll} \exists x \exists y \; (& (\mathit{vater}(x, \mathit{Donald}) \vee \mathit{mutter}(x, \mathit{Donald})) \\ \wedge & (\mathit{vater}(y, x) \vee \mathit{mutter}(y, x)) \\ \wedge & (\mathit{vater}(y, \mathit{Dagobert}) \vee \mathit{mutter}(y, \mathit{Dagobert}) \;) \end{array}$$

Dagobert und Donald sind Onkel und Neffe, wenn es zwei Personen x und y gibt, so dass x Elternteil von Donald ist und y Elternteil von sowohl Dagobert als auch von x.

Die Formel unter den Quantoren wird wahr, wenn für x und y die die Verwandtschaft vermittelnden Personen (Elternteil und Großelternteil) gewählt werden.

Aufgabe 2

In der Vorlesung wurden die beiden Interpretationen $\mathcal{Z}$ und $\mathcal{Z}_{\text{Jint}}$ der Signatur, die $0, 1, +, *$ (Funktionssymbole) und $<$ (Prädikatsymbol) enthält, vorgestellt. Der Ausdruck 2 ist damit kein gültiger Term in der Signatur. Er steht hier als Abkürzung für den Term $(1 + 1)$.

Überprüfen Sie, ob die folgenden Formeln in $\mathcal{Z}$ und $\mathcal{Z}_{\text{Jint}}$ erfüllt sind oder nicht. Begründen Sie jeweils kurz.

(a) $\forall y(\exists k_1(2 * k_1 \doteq y) \rightarrow \exists k_2(2 * k_2 \doteq y + 2))$

(b) $\forall x(0 < x \rightarrow x < x + x)$

(c) $\exists x \forall y(x < y \vee x \doteq y)$

Lösung zu Aufgabe 2

Mit ψ_a, ψ_b, ψ_c werden die Formeln aus der Aufgabenstellung bezeichnet.

(a) in $\mathcal{Z}$: Die Auswertung von ψ_a in $\mathcal{Z}$ ergibt die Bedingung

Ist $y \in \mathbb{Z}$ gerade, dann ist auch $y + 2$ gerade

Dies ist in $\mathbb{Z}$ erfüllt, denn aus $y = 2k$ folgt, dass $y + 2 = 2(k + 1)$ trivialerweise auch gerade ist.

in $\mathcal{Z}_{\text{Jint}}$: Die Auswertung von ψ_a in $\mathcal{Z}$ ergibt die Bedingung

Gibt es für $y \in \mathbb{Z}_{\text{Jint}}$ ein $k_1 \in \mathbb{Z}_{\text{Jint}}$ mit $y = 2 \overset{J}{*} k_1$, so gibt es für $y \overset{J}{+} 2$ ein $k_2 \in \mathbb{Z}_{\text{Jint}}$ mit $y \overset{J}{+} 2 = 2 \overset{J}{*} k_2$.

Sei die Funktion $\text{mod}_J : \mathbb{Z} \rightarrow \mathbb{Z}_{\text{Jint}}$ gegeben durch $\text{mod}_J(x) \equiv x \pmod{2^{32}}$ mit $\mathsf{int\_MIN} \leq \text{mod}_J(x) \leq \mathsf{int\_MAX}$ die Normalisierungsfunktion für Java-Integer. Nach Definition gilt für die Operationen in $\mathcal{Z}_{\text{Jint}}$:

$$\begin{aligned}
2 \overset{J}{*} k_1 \overset{J}{+} 2 &= \text{mod}_J(2 \overset{\mathbb{Z}}{*} k_1) \overset{J}{+} 2 \\
&= \text{mod}_J(2 \overset{\mathbb{Z}}{*} k_1 \overset{\mathbb{Z}}{+} 2) \\
&= \text{mod}_J(2 \overset{\mathbb{Z}}{*} (k_1 \overset{\mathbb{Z}}{+} 1)) \\
&= 2 \overset{J}{*} \text{mod}_J(k_1 \overset{\mathbb{Z}}{+} 1) = 2 \overset{J}{*} (k_1 \overset{J}{+} 1)
\end{aligned}$$

Für $k_2 := k_1 \overset{J}{+} 1$ gilt also die Behauptung.

(b) in $\mathcal{Z}$: Die Auswertung von ψ_b in $\mathcal{Z}$ ergibt die Bedingung:

Für alle $x \in \mathbb{Z}$ mit $x > 0$ gilt $2 \overset{\mathbb{Z}}{*} x > x$.

Wegen der der Verträglichkeit von $\overset{\mathbb{Z}}{*}$ mit der Addition in $\mathbb{Z}$ folgt aus $x > 0$, dass $x \overset{\mathbb{Z}}{+} x > x \overset{\mathbb{Z}}{+} 0$. Damit gilt ψ_b in $\mathcal{Z}$.

in $\mathcal{Z}_{\text{Jint}}$: Die Auswertung von ψ_b in $\mathcal{Z}$ ergibt die Bedingung

Für alle $\mathbb{Z}_{\text{Jint}} \ni x > 0$ gilt $x \overset{J}{+} x > x$

Für $x = \mathsf{int\_MAX}$ gilt $x \overset{J}{+} x = \text{mod}_J((2^{31} - 1) \overset{\mathbb{Z}}{+} (2^{31} - 1)) = \text{mod}_J(2^{32} - 2) = -2$.
Also ist $x \overset{J}{+} x = -2 \not> x$, ψ_b ist also nicht erfüllt in $\mathcal{Z}_{\text{Jint}}$.

(c) in $\mathcal{Z}$: Die Auswertung von ψ_c in $\mathcal{Z}$ ergibt die Bedingung

Es gibt ein $x \in \mathbb{Z}$, so dass für alle $y \in \mathbb{Z}$ gilt $x \leq y$.

Zu einem beliebigen $x \in \mathbb{Z}$ ist aber $x - 1$ eine ganze Zahl und echt kleiner als x. Somit ist ψ_c in $\mathcal{Z}$ nicht erfüllt.

in $\mathcal{Z}_{\text{Jint}}$: Die Auswertung von ψ_c in $\mathcal{Z}_{\text{Jint}}$ ergibt die Bedingung

$$\text{Es gibt ein } x \in \mathbb{Z}_{\text{Jint}}, \text{ so dass für alle } y \in \mathbb{Z}_{\text{Jint}} \text{ gilt } x \leq y.$$

$x = \mathsf{int\_MIN}$ ist das minimale Element, das dies erfüllt.

Aufgabe 3

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 3

(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 für eine strikte Halbordnung p 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 $z_1 \xrightarrow{I(p)} z_2 \xrightarrow{I(p)} \ldots \xrightarrow{I(p)} z_r \xrightarrow{I(p)} z_1$, so würde wegen der Transitiviät auch $z_1 \xrightarrow{I(p)} z_1$ 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.

Aufgabe 4

Geben Sie für jede der folgenden Formeln an, ob sie erfüllbar, allgemeingültig, unerfüllbar oder keine Formel der Prädikatenlogik erster Stufe ist. Begründen Sie Ihre Entscheidungen.

(a) $\phi_a = \exists x \neg(\forall x(f(x) \doteq f(x)))$

(b) $\phi_b = \forall x(f(x) \doteq c) \rightarrow f(f(f(c))) \doteq c$

(c) $\phi_c = \forall x(\forall y(p(x) \vee \neg p(y)))$

(d) $\phi_d = \forall x((p(x) \doteq \mathbf{1} \wedge p(x) \doteq q(x)) \rightarrow q(x) \doteq \mathbf{1})$

(e) $\phi_e = ((r \rightarrow s) \rightarrow r) \rightarrow (r \rightarrow (s \rightarrow r))$

Bemerkung: p, q, r, s sind Prädikatssymbole, f, g Funktionssymbole (jeweils mit der richtigen Stelligkeit), c ein Konstantensymbol (nullstelliges Funktionssymbol) und x, y sind Variablen. Eine Formel kann mehr als eine der genannten Eigenschaften haben.

Lösung zu Aufgabe 4

(a)

	$\exists x \neg(\forall x(f(x) \doteq f(x)))$	$a \doteq a$ ist für jeden Term a immer wahr
$\equiv$	$\exists x \neg(\forall x(\mathbf{1}))$	die gebundene Variable x tritt nicht auf
$\equiv$	$\exists x \neg(\mathbf{1})$	die gebundene Variable x tritt nicht auf
$\equiv$	$\neg \mathbf{1} \equiv \mathbf{0}$	Die Formel ist also **unerfüllbar**

(b) Sei (D, I) eine beliebige Interpretation und β eine beliebige Variablenbelegung.

$$\begin{array}{ll} & \mathrm{val}_{I,\beta}(\forall x(f(x) \doteq c)) = W \\ \iff & \text{Für alle } d \in D \text{ gilt } \mathrm{val}_{I,\beta_x^d}(f(x) \doteq c) = W \\ \implies & \mathrm{val}_{I,\beta_x^{val_I(f(c))}}(f(x) \doteq c) = W \\ \iff & I(f)(val_{I,\beta}(f(c))) = I(c) \\ \iff & \mathrm{val}_{I,\beta}(f(f(c)) \doteq c) = W \end{array}$$

also

$$\begin{array}{ll} & \mathrm{val}_{I,\beta}(\forall x(f(x) \doteq c)) = W \implies \mathrm{val}_{I,\beta}(f(f(c)) \doteq c) = W \\ \iff & \mathrm{val}_{I,\beta}(\phi_b) = W \end{array}$$

Also ist ϕ_b *allgemeingültig*. Jede allgmeingültige Formel ist aber auch insbesondere *erfüllbar*.

(c) Da in ϕ_c die gebundenen Variablen nur in jeweils einem der Operanden der Disjunktion auftreten, gilt nach Satz 4.47:

$$\phi_c \equiv (\forall x\ p(x)) \vee (\forall y\ \neg p(y)) =: \phi'_c$$

Wir zeigen zunächst die Erfüllbarkeit von ϕ'_c. Sei $D = \{d_1\}$ ein einelementiges Universum und $I(p) = \{d_1\}$. Die einzig mögliche Variablenbelegung β ist dann $\beta(v) = d_1$ für alle $v \in Var$ und damit

$$\begin{array}{ll} & d_1 \in I(p) \\ \implies & \mathrm{val}_{I,\beta}(p(x)) = W \\ \implies & \mathrm{val}_{I,\beta}(\forall x\ p(x)) = W \text{ weil das die einzig mögliche Var-Belegung ist} \\ \implies & \mathrm{val}_{I,\beta}(\forall x\ p(x) \vee \forall y\ \neg p(y)) = W \\ \implies & \mathrm{val}_{I,\beta}(\phi'_c) = W \end{array}$$

Damit ist gezeigt, dass ϕ_c in (D, I) erfüllt ist.

Umgekehrt gilt für $D' = \{d_1, d_2\}$, $I'(p) = \{d_1\}$, und β' eine beliebige Var-Belegung, dass

$$\begin{array}{ll} & d_2 \notin I(p) \text{ und } d_1 \in I(p) \\ \implies & \mathrm{val}_{I,\beta}(\forall x\ p(x)) = F \text{ und } \mathrm{val}_{I,\beta}(\forall y\ \neg p(y)) = F \\ \implies & \mathrm{val}_{I,\beta}(\phi'_c) = F \end{array}$$

Damit ist gezeigt, dass ϕ'_c in (D', I') nicht erfüllt ist. ϕ_c ist also erfüllbar, aber nicht allgemeingültig.

(d) Dies ist keine prädikatenlogische Formel nach unserer Definition. Links und rechts des Gleichheitszeichens $\doteq$ müssen bei uns Terme und nicht Formeln stehen. Das „Gleichheitszeichen“ für Formeln ist $\leftrightarrow$.

Bemerkung: Die modifizierte Formel $\forall x(((p(x) \leftrightarrow \mathbf{1}) \wedge (p(x) \leftrightarrow q(x))) \rightarrow (q(x) \leftrightarrow \mathbf{1}))$ ist dann allgemeingültig.

(e) Da r und s nullstellige Prädikate – also aussagenlogische Variablen – sind, handelt es sich auch um eine AL-Formel (AL ist in PL enthalten!). Diese Formel lässt sich also mit den Mitteln, die wir in der AL verwendet haben, untersuchen, z.B. einer Wertetabelle.

Man kann auch eine geschickte Fallunterscheidung machen. Wenn $I(r) = W$ gewählt wird, so kann man die rechte Seite zu $\mathbf{1}$ vereinfachen. Die Formel ϕ_e ist also wahr, wenn r wahr ist. Wenn man $I(r) = F$ wählt, so stellt man fest, dass die linke Seite zu $\mathbf{0}$ vereinfacht werden kann. Die Formel ϕ_e ist also auch wahr, wenn r falsch ist.

Dies zeigt, dass die Formel aussagenlogisch allgemeingültig ist, also eine **Tautologie** ist. (Damit ist sie auch erfüllbar.)