Karlsruher Institut für Technologie
Institut für Theoretische Informatik
Prof. Dr. B. Beckert
Thorsten Bormer

Formale Systeme, WS 2010/2011

Lösungen zu Übungsblatt 6

Dieses Blatt wurde in der Übung am 10.12.2010 besprochen.

Zu Aufgabe 1

(a) Wenn jeder arme Mensch einen reichen Vater hat, dann gibt es einen reichen Menschen, der einen reichen Großvater hat.

Lösung:

Die Signatur besteht hier aus den einstelligen Funktionssymbolen *vater*, *mutter* sowie dem einstelligen Prädikatsymbol *reich* mit der ihres Namens entsprechenden Bedeutung. Die Bedeutung von *arm* ist in diesem Kontext als Negation des Prädikats *reich* definiert. Damit ergibt sich als Formalisierung der obigen Aussage:

$$\forall x\ (\neg reich(x) \to reich(vater(x))) \to \exists x\ (reich(x) \wedge (reich(vater(vater(x))) \vee reich(vater(mutter(x)))))$$

(b) In einer Bar gibt es stets eine Person P, so daß, falls P etwas trinkt, alle anwesenden Personen etwas trinken.

Lösung:

Diese Aussage ist auch als Trinker-Paradoxon bekannt und wird durch folgende allgemeingültige Formel beschrieben:

$$\exists x\ (trinkt(x) \to \forall y\ trinkt(y))$$

(c) Jeder Barbier rasiert alle Personen, außer denen, die sich selbst rasieren.

Lösung:

Die wörtliche Übersetzung liefert hier die erfüllbare Formel:

$$\forall x\ (barbier(x) \to \forall y\ \neg rasiert(y, y) \leftrightarrow rasiert(x, y))$$

In der Literatur ist eine andere Version dieser Aussage als Barbier-Paradoxon bekannt und lautet als Rätsel etwa wie folgt:

> Der Barbier zeichnet sich dadurch aus, dass er genau diejenigen rasiert, die sich nicht selbst rasieren. Rasiert der Barbier sich selbst?

Diese Formulierung fordert, im Gegensatz zur Aufgabenstellung, die Existenz eines solchen Barbiers, so dass sich nun als Formalisierung des Rätsels die unerfüllbare Formel

$$\forall y\ \neg rasiert(y, y) \leftrightarrow rasiert(b, y)$$

ergibt. Dabei ist b eine Konstante, die den Barbier bezeichnet.

Eine alternative Formalisierung ist auch:

$$\exists z\ barbier(z) \wedge \forall x\ (barbier(x) \to \forall y\ \neg rasiert(y, y) \leftrightarrow rasiert(x, y))$$

Zu Aufgabe 2

Gegeben sei die Struktur $I = \langle U, A \rangle$ folgendermaßen:

$$U = \mathbb{R},$$
$$p^I = \{z \mid z \geq 0\},$$
$$q^I = \{(x, y) \mid x = y\},$$
$$f^I(z) = z^2,$$
$$g^I(x, y) = x + y,$$
$$x^I = \sqrt{2},$$
$$y^I = -1$$

In der Aufgabenstellung wurde die Notation x^I, sowie y^I analog zur Angabe der Interpretation der Funktions- und Prädikatsymbole verwendet. Da x und y Variablen sind, wäre jedoch die Angabe einer Variablenbelegung β stattdessen die formal korrekte Vorgehensweise (also: $\beta(x) = \sqrt{2}$, sowie $\beta(y) = -1$).

Der Übersichtlichkeit wegen ist im Folgenden die nicht ganz korrekte, informelle Schreibweise der Variablenbelegung als x^I etc. beibehalten.

Bestimmen Sie den Wert folgender Terme und Formeln:

1. $I(g(f(x), f(y)))$

   Lösung:

$$\begin{aligned} I(g(f(x), f(y))) &= g^I(I(f(x)), I(f(y))) \\ &= f^I(I(x)) + f^I(I(y)) \\ &= (x^I)^2 + (y^I)^2 \\ &= (\sqrt{2})^2 + (-1)^2 \\ &= 2 + 1 \\ &= 3 \end{aligned}$$

2. $I(\forall x\ p(f(x)))$

   Lösung:
   Betrachten wir zunächst $I(p(f(x)))$:

$$I(p(f(x))) = p^I(f^I(x^I))$$

   $p^I(f^I(x^I))$ hat genau denn den Wert true, wenn $(x^I)^2 \geq 0$ ist. Da dies für jede Belegung von x mit Elementen aus U gilt, gilt auch $I_{x/d}(p(f(x))) = true$ für alle $d \in U$. Daraus folgt $I(\forall x\ p(f(x))) = true$

3. $I(\exists z \forall x \forall y\ q(g(x, y), z))$

   Lösung:
   Wir betrachten $I(q(g(x, y), z))$:

$$I(q(g(x, y), z)) = q^I(g^I(x^I, y^I))$$

   $q^I(g^I(x^I, y^I), z^I))$ ist genau dann wahr, wenn $x^I + y^I = z^I$ ist. Es gibt jedoch kein $z \in \mathbb{R}$, so dass für alle $x, y \in \mathbb{R}$ gilt: $x + y = z$
   Daraus folgt $I(\exists z\ \forall x\ \forall y\ q(g(x, y), z)) = false$

4. $I(\forall y (q(f(x), y) \to p(g(x, y))))$

Lösung:
In $\forall y\ (q(f(x), y) \to p(g(x, y)))$ kommt x frei vor und y gebunden. Daher ist $x^I = \sqrt{2}$. Außerdem ist:

$$I(q(f(x), y) \to p(g(x, y))) = q^I(f^I(x^I, y^I) \to p^I(g^I(x^I, y^I))$$

und $q^I(f^I(x^I, y^I) \to p^I(g^I(x^I, y^I))$ ist genau dann wahr, wenn

$$((x^I)^2 = y) \to ((x^I + y^I) \geq 0)$$
$$((\sqrt{2})^2 = y) \to ((\sqrt{2} + y^I) \geq 0)$$

ist. Betrachten wir nun den Wahrheitswert von

$$\forall y(((\sqrt{2})^2 = y) \to ((\sqrt{2} + y) \geq 0)))$$

Die Prämisse $((\sqrt{2})^2 = y)$ ist genau dann wahr, wenn y den Wert 2 hat. Für $y = 2$ ist jedoch auch die Konklusion $\sqrt{2} + 2 \geq 0$ wahr. Daraus folgt:

$$I(\forall y\ (q(f(x), y) \to p(g(x, y)))) = true$$

Zu Aufgabe 3

Seien p und q Prädikate über den natürlichen Zahlen. Die Semantik von p und q sei gegeben durch:

- $p(x, y)$ gilt genau dann, wenn x die Zahl y teilt und
- $q(x, y)$ gilt genau dann, wenn $x \leq y$ ist.

Für alle Interpretationen I, deren Universum die natürlichen Zahlen sind und für die gilt, dass

$$p^I = \{(x, y) \mid x \text{ teilt } y\} \text{ und}$$
$$q^I = \{(x, y) \mid x \leq y\}$$

ist, muss z.B. für die im Aufgabenteil (a) gebildete Formel F gelten, dass F^I genau dann wahr ist, wenn y^I eine Primzahl ist.

Analog zu Aufgabe 2 ist hier für Variablenbelegungen die Notation y^I verwendet worden. Formal korrekt müsste die Aufgabenstellung also lauten:

> ... ist, muss z.B. für die im Aufgabenteil (a) gebildete Formel F gelten, dass $val_{I,\beta}(F) = W$ gdw. $\beta(y)$ eine Primzahl ist.

Des Weiteren wurden in der Aufgabenstellung keine Angaben über zu verwendende Konstanten aus den natürlichen Zahlen gemacht. Eine Lösungsmöglichkeit besteht darin, diese Konstanten zu definieren und deren Interpretation festzulegen, also:

$$1^I = 1, \text{ sowie } 2^I = 2$$

Die hier vorgestellte Lösung formalisiert die Eigenschaften der benötigten Elemente aus der Menge der natürlichen Zahlen – so etwa für die Zahl 1:

$$y \doteq 1 \equiv \forall z\ (q(y, z))\ .$$

Die Konstante 2 lässt sich formalisieren als:

$$y \doteq 2 \equiv \overbrace{\forall z\ (q(y,z) \vee \underbrace{\forall v\ (q(z,v))}_{z \doteq 1})}^{y \doteq 1 \vee y \doteq 2} \wedge \underbrace{\neg \forall w\ (q(y,w))}_{y \neq 1}$$

Formalisieren Sie mit Hilfe der Prädikatenlogik:

1. y ist eine Primzahl
   Lösung:
   $\forall x(p(x,y) \rightarrow \forall z\ (q(x,z)) \vee (x \doteq y)) \wedge \neg \forall z\ (q(y,z))$
2. y ist eine gerade Zahl
   Lösung:
   $\forall x \forall z\ (\overbrace{(q(x,z) \vee \forall v\ (q(z,v))) \wedge \neg \forall w\ (q(x,w))}^{x \doteq 2} \rightarrow p(x,y))$
3. ggt ist der größte gemeinsame Teiler der beiden Zahlen x und y
   Lösung:
   $p(ggt,x) \wedge p(ggt,y) \wedge \forall z(p(z,y) \wedge p(z,x) \rightarrow q(z,ggt))$

   Hierbei sind x, y und ggt freie Variablen.
4. kgV ist das kleinste gemeinsame Vielfache der beiden Zahlen x und y
   Lösung:
   $p(x,kgV) \wedge p(y,kgV) \wedge \forall z(p(y,z) \wedge p(x,z) \rightarrow q(kgV,z))$

   Mit den freien Variablen x, y und kgV.
5. x und y sind teilerfremde Zahlen
   Lösung:
   $\neg \exists z(p(z,x) \wedge p(z,y) \wedge \neg(\forall z\ (q(y,z))))$
6. zwischen zwei verschiedenen natürlichen Zahlen liegt stets eine natürliche Zahl
   Lösung:
   $\forall x \forall y\ (\neg(x \doteq y) \rightarrow \exists z\ (\neg(x \doteq z) \wedge \neg(y \doteq z) \wedge ((q(x,z) \wedge q(z,y)) \vee ((q(y,z) \wedge q(z,x))))))$

Zu Aufgabe 4

Zusätzlich zur Kompositions- und Zuweisungsregel benötigen wir für den Beweis der Gültigkeit des Hoare-Tripels noch folgende Konsequenzregel:

$$\frac{B' \rightarrow B \quad \{B'\}\ \mathrm{Q}\ \{C\} \quad C \rightarrow C'}{\{B\}\ \mathrm{Q}\ \{C'\}}$$

Diese Regel wird benötigt, da in der Vor- bzw. Nachbedingung die im Programm temporär verwendete Variable k nicht vorkommt, diese aber für den Beweis notwendig ist.

$$\dfrac{\dfrac{i \doteq a \wedge j \doteq b \rightarrow i \doteq a \wedge j \doteq b \wedge i \doteq i, \quad \dfrac{}{\{i \doteq a \wedge j \doteq b \wedge i \doteq i\}\ \mathrm{k := i}\ \{i \doteq a \wedge j \doteq b \wedge k \doteq i\}}, \quad i \doteq a \wedge j \doteq b \wedge k \doteq i \rightarrow i \doteq a \wedge j \doteq b \wedge k \doteq a}{\{i \doteq a \wedge j \doteq b\}\ \mathrm{k := i}\ \{i \doteq a \wedge j \doteq b \wedge k \doteq a\}} \qquad H_1}{\{i \doteq a \wedge j \doteq b\}\ \mathrm{k := i;\ i := j;\ j := k}\ \{i \doteq b \wedge j \doteq a\}}$$

H_1 :

$$\dfrac{\dfrac{\dfrac{}{\{i \doteq a \wedge j \doteq b \wedge k \doteq a\}\ \mathrm{i := j}\ \{i \doteq b \wedge j \doteq b \wedge k \doteq a\}} \qquad \dfrac{}{\{i \doteq b \wedge j \doteq b \wedge k \doteq a\}\ \mathrm{j := k}\ \{i \doteq b \wedge j \doteq a \wedge k \doteq a\}}}{\{i \doteq a \wedge j \doteq b \wedge k \doteq a\}\ \mathrm{i := j;\ j := k}\ \{i \doteq b \wedge j \doteq a \wedge k \doteq a\}, \quad i \doteq b \wedge j \doteq a \wedge k \doteq a \rightarrow i \doteq b \wedge j \doteq a}}{\{i \doteq a \wedge j \doteq b \wedge k \doteq a\}\ \mathrm{i := j;\ j := k}\ \{i \doteq b \wedge j \doteq a\}}$$

Zu Aufgabe 5

(a) Axiomatisiere p als strikte Halbordnung

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

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

(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

$$G = U \land F \ .$$

Sei (D, I) ein beliebiges Modell von G. Dann ist die Relation $I(p) \subseteq D \times D$ zyklenfrei. Hätte sie einen Zyklus $z_1 \xrightarrow{I(p)} z_2 \xrightarrow{I(p)} \dots \xrightarrow{I(p)} z_r$, 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 $(d_0 \xrightarrow{I(p)} d_1 \xrightarrow{I(p)} \dots)$ 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.