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

Lösungen zu Übungsblatt 6

Dieses Übungsblatt wurde in der Übung am 11.12.2015 besprochen.

Aufgabe 1

Zeigen sie mit Hilfe des Hoare-Kalküls, dass folgendes Hoare-Tripel gültig ist:

$$\{\mathrm{i} \doteq a \wedge \mathrm{j} \doteq b\}\ \mathrm{k} := \mathrm{i};\ \mathrm{i} := \mathrm{j};\ \mathrm{j} := \mathrm{k}\ \{\mathrm{i} \doteq b \wedge \mathrm{j} \doteq a\}$$

Verwenden Sie dabei die folgenden Regeln: die aus der Vorlesung bekannte Zuweisungsregel (a), die Kompositionsregel (b), sowie die Konsequenzregel (c), die benötigt wird, da in der Vor- bzw. Nachbedingung die im Programm temporär verwendete Variable k nicht vorkommt, diese aber für den Beweis notwendig ist.

$$\frac{}{\{\{\mathrm{x/s}\}A\}\ \mathrm{x} := \mathrm{s}\ \{A\}} \qquad \frac{\{A\}\ \mathrm{P}\ \{B\}, \quad \{B\}\ \mathrm{Q}\ \{C\}}{\{A\}\ \mathrm{P};\ \mathrm{Q}\ \{C\}} \qquad \frac{B \to B' \quad \{B'\}\ \mathrm{Q}\ \{C\} \quad C \to C'}{\{B\}\ \mathrm{Q}\ \{C'\}}$$

(a) Zuweisungsregel (b) Kompositionsregel (c) Konsequenzregel

Lösung zu Aufgabe 1

Zu zeigen:

$$\{\underbrace{i \doteq a \wedge j \doteq b}_{P}\}\ \mathrm{k} := \mathrm{i};\ \mathrm{i} := \mathrm{j};\ \mathrm{j} := \mathrm{k}\ \{\underbrace{i \doteq b \wedge j \doteq a}_{Q}\}$$

$$\dfrac{\dfrac{P \to i \doteq a \wedge j \doteq b \wedge i \doteq i, \quad \{\mathbf{P} \wedge \mathbf{i} \doteq \mathbf{i}\}\ \mathrm{k} := \mathrm{i}\ \{\mathbf{P} \wedge \mathbf{k} \doteq \mathbf{i}\}, \quad P \wedge k \doteq i \to P \wedge k \doteq a}{\{\mathbf{P}\}\ \mathrm{k} := \mathrm{i}\ \{\mathbf{P} \wedge \mathbf{k} \doteq \mathbf{a}\}} \quad \dfrac{\{\mathbf{P} \wedge \mathbf{i} \doteq \mathbf{i}\}\ \mathrm{k} := \mathrm{i}\ \{\mathbf{P} \wedge \mathbf{k} \doteq \mathbf{i}\}}{}}{\{\mathbf{P}\}\ \mathrm{k} := \mathrm{i};\ \mathrm{i} := \mathrm{j};\ \mathrm{j} := \mathrm{k}\ \{\mathbf{Q}\}}\ H_1$$

H_1 :

$$\dfrac{\dfrac{P \wedge k \doteq a \to P \wedge k \doteq a, \quad \{\mathbf{P} \wedge \mathbf{k} \doteq \mathbf{a}\}\ \mathrm{i} := \mathrm{j};\ \mathrm{j} := \mathrm{k}\ \{\mathbf{Q} \wedge \mathbf{k} \doteq \mathbf{a}\}, \quad Q \wedge k \doteq a \to i \doteq b \wedge j \doteq a}{\{\mathbf{P} \wedge \mathbf{k} \doteq \mathbf{a}\}\ \mathrm{i} := \mathrm{j};\ \mathrm{j} := \mathrm{k}\ \{\mathbf{Q}\}} \quad \dfrac{\{\mathbf{P} \wedge \mathbf{k} \doteq \mathbf{a}\}\ \mathrm{i} := \mathrm{j}\ \{\mathbf{i} \doteq \mathbf{b} \wedge \mathbf{j} \doteq \mathbf{b} \wedge \mathbf{k} \doteq \mathbf{a}\} \quad \{\mathbf{i} \doteq \mathbf{b} \wedge \mathbf{j} \doteq \mathbf{b} \wedge \mathbf{k} \doteq \mathbf{a}\}\ \mathrm{j} := \mathrm{k}\ \{\mathbf{Q} \wedge \mathbf{k} \doteq \mathbf{a}\}}{}$$

Aufgabe 2

Gegeben sei folgendes Programm P zur Berechnung des Produkts der beiden Zahlen a und b. Geben Sie eine Invariante für die Schleife an, die ausreicht, um zu zeigen, dass das Hoare-Tripel

$$\{\mathrm{x} \doteq a \wedge \mathrm{y} \doteq b \wedge a \geq 0 \wedge b \geq 0\}\ \mathrm{P}\ \{\mathrm{z} \doteq a * b\}$$

gilt.

```
z := 0
while ¬(y ≐ 0) do
    if ((y/2) * 2 ≐ y) then
        x := 2 * x
        y := y/2
    else
        z := z + x
        x := 2 * x
        y := y/2
    end if
end while
```

Lösung zu Aufgabe 2

Der vorgestellte Algorithmus zur Multiplikation zweier Ganzzahlen entspricht der "Russischen Bauernmultiplikation" und funktioniert wie folgt:

Ist die Variable y ohne Rest durch zwei teilbar, gilt: $2\mathrm{x} \cdot \mathrm{y}/2 = \mathrm{x} \cdot \mathrm{y}$.

Ist y ungerade, so gilt mit Ganzzahldivision: $\mathrm{y}/2 = (\mathrm{y}-1)/2$ und damit ergibt sich das Produkt der Variablen x und y zu: $2\mathrm{x} \cdot (\mathrm{y}-1)/2 + x = \mathrm{x} \cdot \mathrm{y} - \mathrm{x} + \mathrm{x} = \mathrm{x} \cdot \mathrm{y}$.

Dieser zusätzliche Summand x wird im else-Teil der Bedingung in der Schleife zur Variablen z hinzuaddiert, sodass folgende Beziehung über alle Schleifeniterationen erhalten bleibt und damit die Invariante der Schleife bildet: $\mathrm{x} * \mathrm{y} + \mathrm{z} \doteq a * b$

Aufgabe 3

Gegeben sei die Signatur $\Sigma = (F_\Sigma, P_\Sigma, \alpha_\Sigma)$ mit

- $F_\Sigma = \{b, f\}$,
- $P_\Sigma = \{p\}$ und
- $\alpha_\Sigma(b) = 0, \alpha_\Sigma(f) = 1, \alpha_\Sigma(p) = 1$.

(a) Wieviele verschiedene Herbrand-Interpretationen über Σ gibt es?

(b) Wieviele verschiedene Herbrand-Modelle besitzt die Formel

$$p(f(f(b))) \wedge \forall x(p(x) \rightarrow p(f(x))) \ ? \tag{1}$$

Zählen Sie sie auf.

(c) Jedes Herbrand-Modell über Σ der Formel (1) ist auch Modell der Formel

$$\forall x(p(f(f(x)))) \ . \tag{2}$$

Geben Sie eine (Nicht-Herbrand-)Interpretation an, die Modell von (1) aber nicht von (2) ist.

Begründen Sie, warum die Existenz eines Modells für $\underbrace{p(f(f(b))) \wedge \forall x(p(x) \rightarrow p(f(x)))}_{(1)} \wedge \underbrace{\neg\forall x(p(f(f(x))))}_{\text{Negation von (2)}}$, zusammen mit dem Satz von Herbrand und der Tatsache, dass jedes Herbrand-Modell (über Σ) der Formel (1) ein Modell der Formel (2) ist, nicht zu einem Widerspruch führt.

Lösung zu Aufgabe 3

Das Herbrand-Universum ist $D_H = \{\underbrace{f(f(\ldots f(}_{n} b)\ldots)) \mid n \in \mathbb{N}\}$

(a) Unendlich[1] viele. Für $I(p)$ kann jede beliebige Teilmenge der (unendlich großen) Menge D_H gewählt werden. $I(f)$ ist nicht veränderbar.

(b) 3, nämlich (D, I_0), (D, I_1) und (D, I_2) mit

$$\begin{array}{lllll} I_0(p) = \{ & b, & f(b), & f(f(b)), & f(f(f(b))), \ldots\} = D_H \\ I_1(p) = \{ & & f(b), & f(f(b)), & f(f(f(b))), \ldots\} = D_H \setminus \{b\} \\ I_2(p) = \{ & & & f(f(b)), & f(f(f(b))), \ldots\} = D_H \setminus \{b, f(b)\} \end{array}$$

(c) Um das gewünschte Resultat zu erzielen, muss man ein Universum wählen, in dem nicht jedes Element durch f und b dargestellt werden kann.

Sei also $D = D_H \cup \{c\}$. Es gibt keinen Grundterm t, für den $\text{val}(t) = c$ in Herbrand-Interpretationen gelten kann. Ist nun $I(p) = D_H$ (also ohne c) und $I(f)(c) = c$ und I identisch zu I_H, wo letzteres definiert ist, so gilt offensichtlich (1), da diese Formel keine Bedingungen an c stellt. (2) gilt jedoch nicht, da $\text{val}_{I,\beta}(p(f(f(x)))) = F$ für $\beta(x) = c$ ist.

Alternative Lösung: Wähle (D, I) mit $D = \mathbb{Z}$, $I(f) : x \mapsto x+1$, $I(b) = 0$, und $I(p) = \{x \in \mathbb{Z} \mid x \geq 0\}$. Auch dann ist (1) erfüllt, nicht aber (2).

[1] sogar überabzählbar unendlich

Die Existenz eines Modells für die Formel $F = p(f(f(b))) \wedge \forall x(p(x) \rightarrow p(f(x))) \wedge \neg\forall x(p(f(f(x))))$, steht deshalb nicht im Widerspruch zum Satz von Herbrand, da dieser Satz nur Aussagen über *allquantifizierte* Formeln macht. In unserem Fall folgt aus der Existenz eines Modells für obige Formel *nicht*, dass es ein Herbrandmodell über der Signatur Σ gibt. Überführt man die Formel F für die Anwendbarkeit des Satzes von Herbrand in Skolem-Normalform, muss die Signatur um ein neues nullstelliges Funktionszeichen erweitert werden – über dieser *neuen* Signatur existiert dann ein Herbrand-Modell für F.