VI.Übungsblatt zur Vorlesung
"Semantik von Programmiersprachen" SS 97

Prof. Gert Smolka und Martin Müller

Ausgabe: 26.5.1997 Abgabe: 5.6.1997

Aufgabe VI.1(Hoare-Regeln, 2 Punkte) Zeigen Sie oder widerlegen Sie, daß für alle c, A, B, I und σ immer *genau eine* der folgenden zwei Aussagen gilt:

$$\sigma \models^I \{A\}c\{B\} \qquad \text{oder} \qquad \sigma \models^I \{A\}c\{\neg B\}$$

Aufgabe VI.2(Verifikationsbedingungen, 4 Punkte) Zeigen Sie mit struktureller Induktion für alle annotierte Anweisungen $\{A\}c\{B\}$: Falls alle Assertionen $vc(\{A\}c\{B\})$ gültig sind, dann ist auch $\{A\}c\{B\}$ gültig. (Siehe auch Aufgabe 7.11 im Winskel.)

In den folgenden zwei Aufgaben sollen Programme verifiziert werden. Lösen Sie diese Aufgaben mit dem in der Vorlesung vorgestellten Verifikationsschema (siehe Winskel 7.4):

1. Annotieren Sie Ihr Programm vollständig mit den notwendigen Assertionen.
2. Führen Sie für die Assertionen Namen ein, insbesondere A und B für Vor- bzw. Nachbedingung, sowie I für die Schleifeninvariante.
3. Geben Sie die Verifikationsbedingungen (wie in Winskel 7.4) unter Verwendung der Namen für die Assertionen an.
4. Zeigen Sie, daß alle Verifikationsbedingungen gültig sind.

Aufgabe VI.3(Verifikation, 4 Punkte) Geben Sie eine Anweisung c an, so daß das Hoare-Tripel

$$\{Y = i\}c\{X = 2^i\}$$

gültig ist und verifizieren Sie es wie oben beschrieben.

Aufgabe VI.4(Verifikation, 4 Punkte) Sei c die Anweisung

$$\textbf{while}\ \neg M = N\ \textbf{do}\ (\textbf{if}\ M \leq N\ \textbf{then}\ N := N - M\ \textbf{else}\ M := M - N)$$

Verifizieren Sie mit dem obigen Schema, daß das Hoare-Tripel

$$\{N = n \wedge M = m \wedge 1 \leq n \wedge 1 \leq m\}c\{N = M = ggT(n,m)\}$$

gültig ist, wobei $ggT(n,m)$ den größten gemeinsamen Teiler von n und m bezeichne. Sie dürfen dabei ausnutzen, daß für alle n, m die folgenden Eigenschaften gelten:

1. $n > m \Rightarrow ggT(n,m) = ggT(n-m,m)$
2. $ggT(n,m) = ggT(m,n)$

3. $ggT(n, n) = n$

Aufgabe VI.5(Invarianten, 2 Punkte) Es sei eine Kanne mit schwarzen und weißen Kaffeebohnen gegeben, und der folgende Prozeß sei bis zur Terminierung zu wiederholen.

- Nimm zwei beliebige Kaffeebohnen aus der Kanne.
- Falls diese die gleiche Farbe haben, ersetze sie durch eine neue schwarze Kaffeebohne. (Es seien dazu genügend zusätzliche schwarze Bohnen vorhanden.)
- Falls sie verschiedenen Farben haben, lege die weiße zurück in die Kanne und die schwarze beiseite.

1. Dieser Prozeß terminiert immer, und zwar genau dann, wenn die Kanne noch genau eine Bohne enthält. Warum?
2. Was kann man bestenfalls über die Farbe der letzten Kaffebohne sagen und warum? Hinweis: Die Aufgabe wird einfach, wenn Sie die richtige Invariante des beschriebenen Prozesses angeben können.

Aufgabe VI.6(Berechenbarkeit, 2 Punkte) *Auf das nächste Übungsblatt verschoben. Der Setzer.*

Aufgabe VI.7(Gödels β-Prädikat (4 Zusatzpunkte))

1. Sei $n_0, \ldots, n_k$ eine Folge von natürlichen Zahlen und $m = (max\{k, n_0, \ldots, n_k\})!$. Zeigen Sie, daß die Zahlen
$$p_i = 1 + (1 + i) * m \qquad (0 \leq i \leq k)$$
teilerfremd sind ($ggT(p_i, p_j) = 1$ für $i \neq j$), und daß $n_i < p_i$ für alle $0 \leq i \leq k$ gilt.
2. Wir definieren Zahlen $c_i = p_0 * \ldots * p_k / p_i$ für $0 \leq i \leq k$. Zeigen Sie, daß für alle $0 \leq i \leq k$ genau ein $0 \leq d_i < p_i$ existiert mit
$$(c_i * d_i) \ \mathbf{mod}\ p_i = 1 \ .$$
3. Sei weiterhin
$$n = \Sigma_{i=0}^{k} c_i * d_i * n_i \ .$$
Weisen Sie $n_i = n \ \mathbf{mod}\ p_i$ für alle $1 \leq i \leq k$ nach.
4. Sei $\beta(m_1, m_2, i, x)$ das in Vorlesung eingeführte Prädikat, d.h.
$$\beta(m_1, m_2, i, x) \quad gdw. \quad x = m_1 \ \mathbf{mod}\ (1 + (1 + i) * m_2) \ .$$
Zeigen Sie: Für jede Folge $n_0, \ldots, n_k$ von natürlichen Zahlen gibt es natürliche Zahlen m_1 und m_2, so daß für alle $0 \leq i \leq k$ gilt:
$$\beta(m_1, m_2, i, x) \quad gdw. \quad x = n_i \ .$$