9. Übungsblatt zu Logik, Semantik und Verifikation SS 2001

Prof. Dr. Gert Smolka, Dr. Christian Schulte
www.ps.uni-sb.de/courses/prog-lsv01/

Abgabe: 11. Juni in der Vorlesungspause

Aufgabe 9.1: Formalisierung in *Assn* (8) Geben Sie jeweils eine Formel von *Assn* an, die genau dann gültig ist, wenn:

(a) Z das Maximum von X und Y ist.

(b) X eine Quadratzahl ist.

(c) $X \in \mathbb{N}$, $Y \in \mathbb{N}^+$ und $Z = X \mod Y$.

(d) $X, Y \in \mathbb{N}^+$ und Z ist der größte gemeinsame Teiler von X und Y.

Verwenden Sie dabei nur die im Skript für *Assn* angegebenen Konstrukte und Abkürzungen.
Die Formulierung der Aufgabe vertraut etwas auf Ihre Intuition. Formaler kann man (a) wie folgt formulieren: Geben Sie eine Formel $A \in Assn$ an mit:

(1) $\forall \sigma \in \Sigma : \ \sigma \models A \iff \sigma(Z)$ ist das Maximum von $\sigma(Y)$ und $\sigma(Z)$

(2) X, Y, Z sind drei paarweise verschiedene Variablen.

Aufgabe 9.2: Verifikation (8) Sei $I \in Assn$. Betrachten Sie die folgende Korrektheitsaussage:

$\{ N \geq 1 \}$
```
P:=0; C:=1;
```
$\{ I \}$
```
while C≤N do
   P:=P+M; C:=C+1;
```
$\{ P = M * N \}$

(a) Geben Sie die Verifikationsbedingungen an (in möglichst expliziter Form).

(b) Geben Sie eine Invariante I an, für die alle Verifikationsbedingungen gelten.

Aufgabe 9.3: Programmkonstruktion (22) Ein mit Schleifeninvarianten annotiertes Kommando c *erfüllt* eine Spezifikation (A, B) genau dann, wenn gilt:

(1) Alle Verifikationsbedingungen für $\{A\}\ c\ \{B\}$ sind erfüllt.

(2) c weist nur Variablen zu, die in A nicht vorkommen.

(3) c terminiert für jeden Zustand, der A erfüllt.

Geben Sie annotierte Kommandos an, die die folgenden Spezifikationen erfüllen:

(a) $(X \geq 0,\ X + Y = 0)$

(b) $(X \geq 0 \wedge Y \geq 0,\ Y + Z = X)$

(c) $(X \geq 0 \wedge Y \geq 1,\ Z \geq 0 \wedge Z < Y \wedge \exists K\ (X = K * Y + Z))$
Hinweis: Berechnen Sie zuerst $-Y$.

Aufgabe 9.4: Hoare-Regeln (6)

(a) Geben Sie eine Hoare-Regel für Until-Schleifen an (siehe voriges Übungsblatt).

(b) Viele Anfänger glauben, dass die Hoare-Regel für Zuweisungen so aussehen sollte:

$$\frac{}{\{B\}\ X := a\ \{B[a/X]\}}$$

Zeigen Sie mit einem Gegenbeispiel, dass die obige Regel nicht korrekt ist (also unter Umständen ungültige Hoare-Tripel liefert).

Aufgabe 9.5: Bindungsstruktur und Umbenennung (6) Seien:

- $A_1 \stackrel{\text{def}}{=} \exists X\ (X \leq Y \wedge \exists Y\ (Z \leq Y) \wedge Y \leq X)$
- $A_2 \stackrel{\text{def}}{=} \exists X\ \exists Y\ (X \leq Z \wedge \exists X\ (Y \leq X) \wedge \exists Y\ (X \leq Y) \wedge Y \leq Z)$
- $A_3 \stackrel{\text{def}}{=} \exists X\ (X \leq Z \wedge \exists Z\ (Z \leq Y)) \wedge \exists Z\ (X \leq Z) \wedge \exists Y\ (Z \leq X)$

(a) Machen Sie die Bindungsstruktur von A_1, A_2, A_3 durch Annotationen (überstreichen und indizieren von definierenden Auftreten, indizieren von benutzenden Auftreten) explizit.

(b) Geben Sie die freien Variablen von A_1, A_2, A_3 an.

(c) Geben Sie Formeln A_i' mit $A_i' \sim A_i$ ($i \in \{1, 2, 3\}$) an, sodass in A_i' keine Variable sowohl gebunden als auch frei vorkommt ($A \sim B$ gilt genau dann, wenn A und B bis auf konsistente Umbenennung von gebundenen Variablen gleich sind; siehe Vorlesungsnotizen).

(d) Geben Sie Formeln A_i' mit $A_i' \sim A_i[X/Y][Z/X]$ ($i \in \{1, 2, 3\}$) an.