9. Übungsblatt zu Logik, Semantik und Verifikation SS 2002

Prof. Dr. Gert Smolka, Dipl.-Inform. Tim Priesnitz
www.ps.uni-sb.de/courses/prog-lsv02/

Abgabe: 10. Juni in der Vorlesungspause

Diesmal geht es hauptsächlich um rekursive Definitionen und induktive Beweise, mit Anwendungen bei der Semantik von IMP. Lesen Sie dazu Abschnitt 1.8 über wohlfundierte Induktion, Abschnitt 5.4 über rekursive Definition von Mengen, und Kapitel 6 über IMP.

Aufgabe 9.1: Regelinduktion (8) Sei $X = \mathbb{Z}\times\mathbb{Z}\times\mathbb{Z}$ und sei die Menge $M \subseteq X$ durch die folgenden Inferenzregeln definiert:

$$\frac{i \in \mathbb{N}}{(i,0,i) \in M} \qquad \frac{i \in \mathbb{N}}{(0,i,i) \in M} \qquad \frac{(i,j,k) \in M}{(i+1,\, j+1,\, k+1) \in M}$$

(a) Geben Sie die durch die Regeln definierte Grundregelmenge an.

(b) Sei $P = \{\, (k,m,n) \in X \mid n = \max\{k,m\}\,\}$. Beweisen Sie $M \subseteq P$ durch Regelinduktion.

(c) Beweisen Sie durch Induktion über n:

$$\forall n \in \mathbb{N}\ \forall m \in \mathbb{N}\colon\ (n, m, \max\{n,m\}) \in M$$

Aufgabe 9.2: Operationale Semantik (8) In Abschnitt 6.2 wird die operationale Semantik von IMP definiert. Die angebenen Inferenzregeln beschreiben ein Menge von Grundregeln wie in Abschnitt 5.4 beschrieben.

(a) Geben Sie die Grundmenge X an.

(b) Geben Sie die durch die Regel für Zuweisungen beschriebene Grundregelmenge an.

(c) Geben Sie die durch die erste Regel für Konditionale beschriebene Grundregelmenge an.

(d) Beschreiben Sie die durch die operationale Semantik definierte Menge $I_R \subseteq X$ mithilfe der Denotationsfunktion $\mathcal{C}$.

Aufgabe 9.3: Regelinduktion (5) Regelinduktion wird durch Proposition 5.4.3 unter Bezugnahme auf zwei Mengen X und P formuliert. Geben Sie das passende X und P für den Beweis von Proposition 6.3.1 an.

Aufgabe 9.4: Strukturelle Induktion (5) Strukturelle Induktion ist ein Spezialfall von wohlfundierter Induktion, bei der die wohlfundierte Relation durch die Konstituentenbeziehung $\rhd$ gegeben ist. Wohlfundierte Induktion wird durch Proposition 1.8.2 unter Bezugnahme auf zwei Mengen X und P formuliert. Geben Sie das passende X und P für den Beweis von Proposition 6.3.2 an.

Aufgabe 9.5: Until-Schleifen (8) Wir erweitern IMP um Until-Schleifen der Form

$$\textsf{do } c \textsf{ until } b$$

Die Semantik von Until-Schleifen spezifizieren wir dadurch, dass wir sagen, dass das obige Kommando für alle c und b dasselbe Ergebnis liefern soll wie

$$c \ ; \ \textsf{if } b \textsf{ then skip else do } c \textsf{ until } b$$

(a) Erweitern Sie die operationale Semantik von IMP um passende Regeln für Until-Schleifen.

(b) Erweitern Sie die denotationale Semantik von IMP um eine passende Gleichung für Until-Schleifen. Verwenden Sie dabei eine Hilfsfunktion Γ, die das Tripel $(\mathcal{B}(b), \mathcal{C}(c))$ als Argument bekommt.

Aufgabe 9.6: For-Schleifen (8) Wir erweitern IMP um For-Schleifen der Form

$$\textsf{for } X \textsf{ to } a \textsf{ do } c$$

Die Semantik von For-Schleifen spezifizieren wir dadurch, dass wir sagen, dass das obige Kommando für alle X, a und c dasselbe Ergebnis liefern soll wie

$$\textsf{if } X \leq a \textsf{ then } c \ ; \ X := X + 1 \ ; \ \textsf{for } X \textsf{ to } a \textsf{ do } c \textsf{ else skip}$$

(a) Geben Sie mithilfe einer For-Schleife ein Kommando ohne While-Schleife an, dass für jeden Anfangszustand divergiert.

(b) Erweitern Sie die operationale Semantik von IMP um passende Regeln für For-Schleifen.

(c) Erweitern Sie die denotationale Semantik von IMP um eine passende Gleichung für For-Schleifen. Verwenden Sie dabei eine Hilfsfunktion Γ, die das Tripel $(X, \mathcal{A}(a), \mathcal{C}(c))$ als Argument bekommt.

Aufgabe 9.7: Formalisierung in ASSN (8) Geben Sie jeweils eine Formel von *Assn* an, die genau dann gültig ist, wenn:

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

(b) X eine durch 7 teilbare Zahl ist.

(c) $X \in \mathbb{N}$, $Y \in \mathbb{N}^+$ und Z ist das Ergebnis der ganzahligen Division von X durch Y ($X \operatorname{div} Y$).

(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 Minimum von $\sigma(Y)$ und $\sigma(Z)$

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