Auszug Pruefung vom 23.10.09
Program Verification

donPromillo

13. November 2009

1 Aufgabenstellung 3

Consider the following generalisation of the repeat- and while-loop. The program statement

$$\text{loop } S_1 \text{ exit-on } B \; S_2 \text{ endloop}$$

executes the statements S_1 and S_2 in an alternating sequence: S_1 is followed by S_2, and S_2 is again followed by S_1, repeating the cycle. After each execution of S_1 the condition B is testet. If it is true, the loop stops and execution continues with the statement immediately following endloop. If the condition is false, the loop cycles once more.
Define the syntax, semantics, and a verification rule for the loop-statement, without referring to while- or repeat-statements. (For the construction of the rules you may use these statements as intermediate steps.)

2 Loesungsweg

2.1 Definiere Syntax

Erweitere P mit folgender Syntax (S_1, S_2 dienen als Platzhalter fuer eine Syntax aus P, B steht fuer eine Bedingung ξ) : loop P exit-on ξ P endloop

$$P ::= \ldots | \text{loop } P \text{ exit-on } \xi \; P \text{ endloop} \tag{1}$$

2.2 Definiere Semantik

Laut Programmbeschreibung wird S1 ausgefuehrt und im Anschluss erfolgt sofort die ueberpruefung von B auf true oder false. Ergibt diese ueberpruefung `false`, so wird S2, gefolgt von S1 mit erneuter ueberpruefung ausgefuehrt. In diesem `false`-Zweig erkennt man das Verhalten einer `while`-Schleife. Im `true`-Zweig wird nichts weiter ausgefuehrt.

2.2.1 Pseudocode

```
 p;
while not-e do
q;
p;
od
```

2.2.2 Semantik

$$\underbrace{[loop\ p\ exit\text{-}on\ e\ p\ endloop]\sigma}_{[while\ \neg e\ do\ q\ ;\ p\ od][p]\sigma} = \begin{cases} [loop\ p\ exit\text{-}on\ e\ p\ endloop][q][p]\sigma & \text{if[e][p]}\sigma = false \\ [p]\sigma & \text{if[e][p]}\sigma = true \end{cases} \quad (2)$$

Zur Herleitung einer Verifikationsregel waere es hilfreich die vorgegangene *loop*-Semantik in eine *while*-Semantik umzufuehren.

$$[while\ \neg e\ do\ q\ ;\ p\ od][\text{p}]\sigma = \begin{cases} [while\ \neg e\ do\ q\ ;\ p\ od][p][q][p]\sigma & \text{if}[\neg\text{e}][\text{p}]\sigma = true \\ [p]\sigma & \text{if}[\neg\text{e}][\text{p}]\sigma = false \end{cases}$$

2.3 Definiere Verifikation

2.3.1 Herleitung

$$\dfrac{\{F\}\ \text{p}\ \{G\}_{G\Rightarrow\{Inv\}} \qquad \dfrac{\{Inv\wedge\neg e\}\ \text{q; p}\ \{Inv\}}{\{Inv\}\ \text{while}\ \neg e\ \text{do q; p od}\ \{Inv\wedge\neg e\}}\ \text{(wh.)}}{\{F\}\ \underbrace{\text{p; while}\ \neg e\ \text{do q; p od}}_{\text{loop p exit-on } e \text{ q endloop}}\{Inv\wedge\neg e\}}\ \text{(sc.)}$$

2.3.2 Abgeleitete Regel

$$\dfrac{\{F\}p\{Inv\} \qquad \{Inv\wedge\neg e\}\ \text{q; p}\ \{Inv\}}{\{F\}\text{loop p exit-on } e \text{ q endloop}\{Inv\wedge\neg e\}} \quad (3)$$