

## Übungen zur Vorlesung Formale Spezifikation und Verifikation

Blatt 10

**Aufgabe 10-1** Geben Sie jeweils konkrete  $\tau$  und  $\varpi$  an, so dass die folgenden Urteile im Typsystem mit Referenzen herleitbar sind.

- a)  $r: \text{ref}_{\Pi} \text{int} \vdash \text{fn}_{\pi} x \Rightarrow (r:=x) : \tau \ \& \ \varpi$
- b)  $\emptyset \vdash \text{let } x = \text{ref}_A 0 \text{ in } \text{fn}_{\pi} f \Rightarrow (f (x:=!x + 1)) : \tau \ \& \ \varpi$
- c)  $\emptyset \vdash \text{fn}_{\pi} x \Rightarrow \text{if } !x < 10 \text{ then } (x:=!x + 1) \text{ else } 10 : \tau \ \& \ \varpi$
- d)  $y: \text{ref}_{\{A,B\}} \text{int} \vdash \text{fun}_{\pi} f x \Rightarrow \text{if } x > 0 \text{ then } (y:=!y * 2); f (x - 1) \text{ else } !y : \tau \ \& \ \varpi$

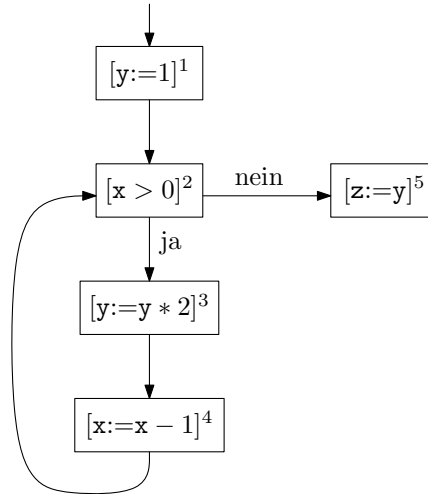
**Aufgabe 10-2** Geben Sie  $\sigma$  und  $\varpi$  an, so dass das folgenden Urteil im Typsystem mit Exceptions herleitbar ist:

$$\emptyset \vdash \text{fn } f \Rightarrow \text{fn } g \Rightarrow \text{fn } x \Rightarrow g (f x) : \sigma \ \& \ \varpi$$

Das Typschema  $\tau$  soll nur Effektausdrücke enthalten, die von der Grammatik  $\varphi ::= \varphi_1 \cup \varphi_2 \mid \varepsilon$  erzeugt werden, d.h. keinen Ausdruck der Form  $\{s\}$  für eine konkrete Exception  $s$ .

**Aufgabe 10-3** Für das Typsystem mit Exceptions sind auf Folie 229 die Regeln der operationellen Semantik für Applikations-Terme angegeben. Geben Sie Regeln für die operationelle Semantik für `fun`, `let` und `op` an.

**Aufgabe 10-4** Gegeben sei folgender Kontrollflussgraph.



Vervollständigen Sie die folgenden Gleichungen, so dass eine Lösung für die Datenflussinklu- sionen für Hoare-Logik entsteht.

$$HL_{entry}(1) =$$

$$HL_{exit}(1) =$$

$$HL_{entry}(2) = \{(\sigma_{init}, \sigma) \mid \sigma(y) = 2^{\sigma_{init}(x) - \sigma(x)}, \sigma(x) \geq 0\} = \llbracket (y = 2^{x_{init} - x}) \wedge (x \geq 0) \rrbracket$$

$$HL_{exit}(2) =$$

$$HL_{entry}(3) =$$

$$HL_{exit}(3) =$$

$$HL_{entry}(4) =$$

$$HL_{exit}(4) =$$

$$HL_{entry}(5) =$$

$$HL_{exit}(5) = \{(\sigma_{init}, \sigma) \mid \sigma(z) = 2^{\sigma_{init}(x)}\} = \llbracket (z = 2^{x_{init}}) \rrbracket$$

Folgern Sie, dass das Hoare-Tripel  $\{x \geq 0\} P \{z = 2^{x_{init}}\}$  gültig ist, wobei  $P$  das durch den Kontrollflussgraphen gegebene Programm ist.