

## Semantik von Programmiersprachen – SS 2017

<http://pp.ipd.kit.edu/lehre/SS2017/semantik>

**Lösungen zu Blatt 7: Prozeduren**

Besprechung: 12.06.2017

### 1. Welche der folgenden Aussagen sind richtig, welche falsch? (H)

- (a)  $[(p, i := i * 1; \text{call } p)] \vdash \langle \text{call } p, \sigma \rangle \Downarrow \sigma$
- (b)  $[(p, \text{skip}), \text{call } q]$  ist ein Programm der Sprache  $\text{While}_{PROC}$ .
- (c)  $\langle \text{skip}, \sigma \rangle$  ist die einzige blockierte Konfiguration der Small-Step-Semantik für  $\text{While}_{PROC}$ .
- (d) Wenn  $P \vdash \langle c, \sigma \rangle \xrightarrow{\infty}_1$ , dann enthält  $c$  eine **while**-Schleife.
- (e) Sei  $P \equiv [(p, y, x := 4; \text{result} := 5 * y)]$ ,  $E_0 \equiv [x \mapsto 0, y \mapsto 1]$  und  $s \equiv [\text{next} \mapsto 2]$ .  
 Wenn  $P, E_0, E_0 \vdash \langle \{ \text{var } x = 3; y \leftarrow \text{call } p(x); y := y + x \}, s \rangle \Downarrow s'$ ,  
 dann  $s'(E_0(x)) = 4$  und  $s'(E_0(y)) = 18$ .
- (f) Wenn  $P, E_0, E \vdash \langle c, s \rangle \Downarrow s'$ , dann  $s'(\text{next}) = s(\text{next})$ .

#### Lösung:

- (1a) Falsch.  $p$  ist eine rekursive Prozedur, die *nie* abbricht. Wie bei unendlichen Schleifen gibt es für unendlich viele rekursive Aufrufe keine Ableitung.
- (1b) Richtig. Die Syntax überprüft nicht, ob eine aufgerufene Methode existiert.
- (1c) Falsch. Das Fortschrittslemma gilt *nicht* für  $\text{While}_{PROC}$ . Beispielsweise ist auch die Konfiguration  $\text{call } p$  blockiert, falls es keine Prozedur  $p$  in der Prozedurdeklarationsliste  $P$  gibt, d.h.,  $P \vdash \langle \text{call } p, \sigma \rangle \not\rightarrow_1$ .  
 Auch die Big-Step-Semantik blockiert, wenn eine Prozedur nicht vorhanden ist. Dies bedeutet, dass Nichtableitung nicht mehr mit Nichttermination gleichgesetzt werden kann.
- (1d) Falsch. Nichttermination ist auch durch Rekursion möglich.

$$[(p, \text{call } p)] \vdash \langle \text{call } p, \sigma \rangle \rightarrow_1 \langle \text{call } p, \sigma \rangle \rightarrow_1 \dots$$

- (1e) Richtig. Man zeichne einen Ableitungsbaum.
- (1f) Richtig. Beweis mittels Regelinduktion über die Big-Step-Semantik.
  - Fälle  $\text{SKIP}_{BS}^{P1}$ ,  $\text{ASS}_{BS}^{P1}$ ,  $\text{WHILEFF}_{BS}^{P1}$ : Trivial.
  - Fälle  $\text{SEQ}_{BS}^{P1}$ ,  $\text{IFTT}_{BS}^{P1}$ ,  $\text{IFFF}_{BS}^{P1}$ ,  $\text{WHILETT}_{BS}^{P1}$ :  
 Folgt direkt aus den Induktionsannahmen.
  - Fälle  $\text{BLOCK}_{BS}^{P1}$ ,  $\text{CALL}_{BS}^{P1}$ : Folgt direkt aus der Regel. □

### 2. Small-Step-Semantik für Prozeduren mit Parametern (H)

Für Prozeduren mit einem Parameter ( $\text{While}_{PROCP}$ ) gibt es folgende Vorschläge für eine Aufrufregel der Small-Step-Semantik:

$$(a) \frac{(p, x, c) \in P}{P \vdash \langle y \leftarrow \text{call } p(a), \sigma \rangle \rightarrow_1 \langle x := a; c; y := \text{result}, \sigma \rangle}$$

- (b) 
$$\frac{(p, x, c) \in P}{P \vdash \langle y \leftarrow \text{call } p(a), \sigma \rangle \rightarrow_1}$$

$$\langle \{ \text{var result} = 0; \{ \text{var } x = a; c \}; y := \text{result} \}, \sigma \rangle$$
- (c) 
$$\frac{(p, x, c) \in P}{P \vdash \langle y \leftarrow \text{call } p(a), \sigma \rangle \rightarrow_1}$$

$$\langle \{ \text{var } x = a; \{ \text{var result} = 0; c; y := \text{result} \} \}, \sigma \rangle$$
- (d) 
$$\frac{(p, x, c) \in P \quad z \text{ nicht verwendet in } P \text{ und } a}{P \vdash \langle y \leftarrow \text{call } p(a), \sigma \rangle \rightarrow_1}$$

$$\langle \{ \text{var } z = 0; \{ \text{var } x = a; \{ \text{var result} = 0; c; z := \text{result} \} \}; y := z \}, \sigma \rangle$$

Untersuchen Sie, in wie weit diese Regeln call-by-value Prozedurparameter und Rückgabewerte korrekt abbilden. Begründen Sie Ihre Antwort; ggf. mit Beispielprogrammen, die entsprechende Defizite aufzeigen. Welche dieser Regeln modellieren statische Variablenbindung?

**Lösung:** Alle vorgestellten Regeln haben Probleme.

- (2a) Diese Regel ist nur die Erweiterung *dynamischer* Variablenbindung um einen Parameter.  
Mangel: Parameter- und Rückgabewert überhaupt nicht lokal, kein call-by-value.  
Beispiel:  $P \equiv [(p, x, x := 5; \text{result} := 1)]$ ,  
Aufruf:  $\{ \text{var result} = 0; x := 2; y \leftarrow \text{call } p(1); z := \text{result} \}$   
Nach dem Aufruf hat  $x$  den Wert 5, nicht 2;  $z$  den Wert 1, nicht 0.
- (2b) Parameter- und Rückgabewariable werden hier außerhalb des Aufrufs wegen der Blöcke nicht geändert.
- i. Die Reihenfolge der Blöcke ist schlecht gewählt.  $a$  kann **result** enthalten, das durch den umgebenden Block umgebunden wird.  
Beispiel:  $P \equiv [(p, x, \text{result} := x)]$ ,  
Aufruf:  $\text{result} := 1; y \leftarrow \text{call } p(\text{result})$   
Am Ende hat  $y$  den Wert 0, richtig wäre aber 1.  
Lösung dafür: Man initialisiert nicht  $x$  auf  $a$ , sondern auf  $\mathcal{N}^{-1} \llbracket \mathcal{A} \llbracket a \rrbracket \sigma \rrbracket$ . Dann vermischt man aber mehrere Schritte in einem, was dem Small-Step-Gedanken entgegenläuft.
  - ii. Wenn  $y$  **result** ist, ist das  $y$  an den neuen Block gebunden, damit geht der Rückgabewert verloren.  
Beispiel:  $P \equiv [(p, x, \text{result} := x)]$ ,  
Aufruf:  $\text{result} := 1; \text{result} \leftarrow \text{call } p(5)$   
Am Ende hat **result** noch immer den Wert 1, richtig wäre 5.
- (2c) Im Gegensatz zu (2b) ist hier Blockreihenfolge besser,  $a$  wird zu Blockbeginn korrekt ausgewertet, Problem (2b) i tritt nicht mehr auf. Dafür tritt das Problem (2b) ii. des verlorenen Rückgabewertes hier verstärkt auf, weil auch im (viel häufigeren) Fall  $y = x$  der Rückgabewert verloren geht. Beispiel wie vorher.
- (2d) Durch das Einführen einer neuen Zwischenspeichervariable  $z$ , die nicht in  $P$  oder  $a$  verwendet wird, verschwinden die Probleme mit versehentlichen Bindungen. Der Fall, dass  $x$  gleich **result** ist, bleibt weiterhin problematisch. In diesem Fall ist der Parameterwert nicht mehr zugreifbar. Das gleiche Problem hat übrigens auch die Big-Step-Semantik-Regel  $\text{CALL}_{\text{BS}}^1$ . Dort könnte man dies einfach lösen, indem das Speicherupdate für  $x$  nicht an der Stelle  $s(\text{next})$  durchgeführt wird, sondern nochmals über die neue Variablenbindung aufgelöst wird. Bei dieser Regel könnte man dies lösen, indem man die Blockreihenfolge  $z$ , **result** und  $x$  verwendet,  $z$  auf  $a$  und  $x$  auf  $z$  initialisiert – dann kann  $z$  auch in  $a$  vorkommen:

$$\frac{(p, x, c) \in P \quad z \text{ nicht verwendet in } P}{P \vdash \langle y \leftarrow \text{call } p(a), \sigma \rangle \rightarrow_1}$$

$$\langle \{ \text{var } z = a; \{ \text{var result} = 0; \{ \text{var } x = z; c; z := \text{result} \} \}; y := z \}, \sigma \rangle$$

Wesentlicher Nachteil dieser Regel ist, dass sie die Einzelschritt-Semantik mehrdeutig macht – die Wahl von  $z$  ist nicht eindeutig. Die so entstehenden Programme sind aber semantisch alle äquivalent, nur der Determinismusbeweis wird wesentlich komplizierter. Da die Menge der Variablen in  $P$  endlich ist, kann auch leicht eine deterministische Auswahlfunktion angegeben werden.

Keine der Regeln eignet sich für statische Variablenbindung, da alle die Prozeduraufrufe textuell ersetzen und dabei keine Variablenumbenennung vornehmen (können). Da Funktionsaufrufe auch nur strukturierte `gotos` sind, können wir für echte statische Bindung die Continuation-Semantik aus dem letzten Übungsblatt wiederverwenden. Wir könnten sie mit der Speicherverwaltung aus der Bigstep-Semantik kombinieren, aber zur Abwechslung verwenden wir stattdessen die abstraktere Darstellung über einen expliziten Stack von lokalen, partiellen Zustandsfunktionen  $\bar{\sigma} \in \text{Var} \rightarrow \mathbb{Z}$ . Es befinden sich stets so viele lokale Zustandsfunktionen wie Continuations auf den Stacks. Der ursprüngliche Zustand  $\sigma$  wird nur noch für globale Variablen verwendet.

Ein Call legt das Unterprogramm, einen neuen Zustand, der nur den Parameterwert enthält, sowie die Rückgabevariable auf die Stacks. Zusätzlich merken wir uns mit der “Stack-Instruktion”  $y \leftarrow \text{POP}$ , dass wir am Ende den lokalen Zustand vom Stack nehmen und  $y$  zuweisen müssen.

$$\text{CALL}_{\text{PSS}}: \frac{(p, x, c) \in P}{P \vdash \langle y \leftarrow \text{call } p(a) \cdot cs, \bar{\sigma} \cdot st, \sigma \rangle \rightarrow_1 \langle c \cdot cs, [x \mapsto \mathcal{A}[[a]] \sigma[\bar{\sigma}]] \cdot y \leftarrow \text{POP} \cdot \bar{\sigma} \cdot st, \sigma \rangle}$$

Das Update  $\sigma[\bar{\sigma}]$  ist dabei definiert als

$$\sigma[\bar{\sigma}](x) = \begin{cases} y & \text{falls } \bar{\sigma}(x) = y \\ \sigma(x) & \text{falls } \bar{\sigma}(x) = \perp \end{cases}$$

Auch die Sequenz erstellt wie gehabt eine Continuation, allerdings ohne Rückgabevariable oder Änderung des lokalen Zustands.

$$\text{SEQ}_{\text{PSS}}: P \vdash \langle c_0; c_1 \cdot cs, st, \sigma \rangle \rightarrow_1 \langle c_0 \cdot c_1 \cdot cs, st, \sigma \rangle$$

Wir können die bisher notwendige Codeerzeugung in der Blockregel umgehen, indem wir stattdessen einen neuen lokalen Zustand sowie eine Instruktion, um ihn am Schluss wieder zu entfernen, pushen.

$$\text{BLOCK}_{\text{PSS}}: P \vdash \langle \{ \text{var } x = a; c \} \cdot cs, \bar{\sigma} \cdot st, \sigma \rangle \rightarrow_1 \langle c \cdot cs, \bar{\sigma}[x \mapsto \mathcal{A}[[a]] \sigma[\bar{\sigma}]] \cdot \text{POP} \cdot \bar{\sigma} \cdot st, \sigma \rangle$$

Die Stack-Instruktionen werden durch die Skip-Regel ausgewertet.

$$\text{SKIP}_{\text{PSS}}: P \vdash \langle \text{skip} \cdot cs, \bar{\sigma} \cdot \bar{\sigma}' \cdot st, \sigma \rangle \rightarrow_1 \langle cs, \bar{\sigma} \cdot \bar{\sigma}' \cdot st, \sigma \rangle$$

$$\text{SKIPPOP}_{\text{PSS}}: P \vdash \langle \text{skip} \cdot cs, \bar{\sigma} \cdot \text{POP} \cdot \bar{\sigma}' \cdot st, \sigma \rangle \rightarrow_1 \langle cs, \bar{\sigma}' \cdot st, \sigma \rangle$$

$$\text{SKIPRET}_{\text{PSS}}: P \vdash \langle \text{skip} \cdot cs, \bar{\sigma} \cdot y \leftarrow \text{POP} \cdot \bar{\sigma}' \cdot st, \sigma \rangle \rightarrow_1 \langle cs, \bar{\sigma}'[y \mapsto \bar{\sigma}(\text{result})] \cdot st, \sigma \rangle$$

Die Assignment-Regel muss nun zwischen lokalen und globalen Zuweisungen unterscheiden.

$$\text{ASSLOCAL}_{\text{PSS}}: \frac{\bar{\sigma}(x) = n}{P \vdash \langle x := a \cdot cs, \bar{\sigma} \cdot st, \sigma \rangle \rightarrow_1 \langle cs, \bar{\sigma}[x \mapsto \mathcal{A}[[a]] \sigma[\bar{\sigma}]] \cdot st, \sigma \rangle}$$

$$\text{ASSGLOBAL}_{\text{PSS}}: \frac{\bar{\sigma}(x) = \perp}{P \vdash \langle x := a \cdot cs, \bar{\sigma} \cdot st, \sigma \rangle \rightarrow_1 \langle cs, \bar{\sigma} \cdot st, \sigma[x \mapsto \mathcal{A}[[a]] \sigma[\bar{\sigma}]] \rangle}$$

Die restlichen Regeln müssen nicht nennenswert geändert werden.

$$\text{IFTT}_{\text{PSS}}: \frac{\mathcal{B} \llbracket b \rrbracket \sigma[\bar{\sigma}] = \mathbf{tt}}{P \vdash \langle \text{if } (b) \text{ then } c_0 \text{ else } c_1 \cdot cs, \bar{\sigma} \cdot st, \sigma \rangle \rightarrow_1 \langle c_0 \cdot cs, \bar{\sigma} \cdot st, \sigma \rangle}$$

$$\text{IFFF}_{\text{PSS}}: \frac{\mathcal{B} \llbracket b \rrbracket \sigma[\bar{\sigma}] = \mathbf{ff}}{P \vdash \langle \text{if } (b) \text{ then } c_0 \text{ else } c_1 \cdot cs, \bar{\sigma} \cdot st, \sigma \rangle \rightarrow_1 \langle c_1 \cdot cs, \bar{\sigma} \cdot st, \sigma \rangle}$$

$\text{WHILE}_{\text{PSS}}:$

$$P \vdash \langle \text{while } (b) \text{ do } c \cdot cs, st, \sigma \rangle \rightarrow_1 \langle \text{if } (b) \text{ then } c; \text{ while } (b) \text{ do } c \text{ else skip} \cdot cs, st, \sigma \rangle$$

**Übung:** Was sollte der Startzustand dieser Semantik sein, was sind die blockierten Zustände?

### 3. Call by reference (Ü)

Die in der Vorlesung vorgestellte Big-Step-Semantik für Prozeduren mit einem Parameter wertet den übergebenen Parameter beim Aufruf aus und übergibt nur den Wert an die aufgerufene Prozedur. Insbesondere bleibt der Wert einer Variablen, die als Parameter übergeben wird, im aufrufenden Kontext unverändert. Diese Parameterübergabeart heißt *call by value*. Daneben gibt es auch noch *call by reference*, bei der Änderungen am Parameterwert in der aufgerufenen Prozedur auch nach dem Ende des Aufrufs in der aufrufenden Prozedur sichtbar sind. Passen Sie in dieser Aufgabe die Big-Step-Semantik von  $\text{While}_{\text{PROCP}}$  entsprechend an:

- Passen Sie die Syntax-Definition von  $\text{While}_{\text{PROCP}}$  an, so dass nur noch Variablen als Parameter verwendet können.
- Ändern Sie die Big-Step-Semantik so, dass Parameter immer als call by reference übergeben werden.
- Ändern Sie die Regeln erneut so, dass auch die Rückgabewertvariable mit call by reference übergeben wird.
- Finden Sie ein Programm, bei dem sich das Verhalten in beiden Varianten von call by reference und call by value unterscheidet. Belegen Sie dies durch die Ableitungsbäume.

**Lösung:**

- Die Syntax muss die erlaubten Ausdrücke für Parameter in Prozeduraufrufe auf Variablen einschränken. Die Anweisungssyntax lautet:

$$\text{Com } c ::= \dots \mid y \leftarrow \text{call } p(x)$$

- Es muss nur die Big-Step-Semantikregel angepasst werden:

$$\frac{(p, x, c) \in P \quad P, E_0, E_0[x \mapsto E(z), \text{result} \mapsto s(\text{next})] \vdash \langle c, s[\text{next} \mapsto s(\text{next}) + 1] \rangle \Downarrow s'}{P, E_0, E \vdash \langle y \leftarrow \text{call } p(z), s \rangle \Downarrow s'[E(y) \mapsto s'(s(\text{next}))], \text{next} \mapsto s(\text{next})]}$$

- 

$$\frac{(p, x, c) \in P \quad P, E_0, E_0[x \mapsto E(z), \text{result} \mapsto E(y)] \vdash \langle c, s \rangle \Downarrow s'}{P, E_0, E \vdash \langle y \leftarrow \text{call } p(z), s \rangle \Downarrow s'}$$

Auch wenn diese Regel jetzt ohne `next` auskommt, braucht man dies trotzdem noch für die Blockregel  $\text{BLOCK}_{\text{BS}}^{\text{P1}}$ .

- Beispiel:

$$\begin{aligned} P &\equiv [(p, x, x := 1; \text{result} := 2; y := 3)] \\ V &\equiv [x, y] \\ c &\equiv x := 4; y \leftarrow \text{call } p(x) \end{aligned}$$

Bei call-by-value hat  $x$  am Ende den Wert 4, bei call-by-reference den Wert 1.

Die Ableitungsbäume:

$$\begin{array}{c}
 \frac{}{P, E_0, E_0 \vdash \langle x := 4, s_0 \rangle \Downarrow s_1} \\
 \frac{}{P, E_0, E_1 \vdash \langle x := 1, s_2 \rangle \Downarrow s_3} \quad \frac{}{P, E_0, E_1 \vdash \langle \text{result} := 2, s_3 \rangle \Downarrow s_4} \quad \frac{}{P, E_0, E_1 \vdash \langle y := 3, s_4 \rangle \Downarrow s_5} \\
 \frac{}{P, E_0, E_1 \vdash \langle \text{result} := 2; y := 3, s_3 \rangle \Downarrow s_5} \\
 \frac{}{P, E_0, E_1 \vdash \langle c_p, s_2 \rangle \Downarrow s_5} \\
 \frac{}{P, E_0, E_0 \vdash \langle y \leftarrow \text{call } p(x), s_1 \rangle \Downarrow s_6} \\
 \hline
 P, E_0, E_0 \vdash \langle c, s_0 \rangle \Downarrow s_6
 \end{array}$$

call by value:

Umgebung:	Belegung:	x	y	result		
$E_0 = [x \mapsto 0, y \mapsto 1]$		0	1			
$E_1 = E_1[x \mapsto s_1(\text{next}), \text{result} \mapsto s_1(\text{next}) + 1]$		2	1	3		
Zustand:	Werte:	next	0	1	2	3
$s_0 = [E_0(x) \mapsto?, E_0(y) \mapsto?, \text{next} \mapsto  V ]$		2	?	?		
$s_1 = s_0[E_0(x) \mapsto 4]$		2	4	?		
$s_2 = s_1[s_0(\text{next}) \mapsto \mathcal{A}[[x]](s_1 \circ E_0), \text{next} \mapsto s_0(\text{next}) + 2]$		4	4	?	4	?
$s_3 = s_2[E_1(x) \mapsto 1]$		4	4	?	1	?
$s_4 = s_3[E_1(\text{result}) \mapsto 2]$		4	4	?	1	2
$s_5 = s_4[E_1(y) \mapsto 3]$		4	4	3	1	2
$s_6 = s_5[E_0(y) \mapsto s_5(s_1(\text{next}) + 1), \text{next} \mapsto s_1(\text{next})]$		2	4	2	1	2

call by reference für Parameter

Umgebung:	Belegung:	x	y	result	
$E_0 = [x \mapsto 0, y \mapsto 1]$		0	1		
$E_1 = E_1[x \mapsto E_0(x), \text{result} \mapsto s_1(\text{next})]$		0	1	2	
Zustand:	Werte:	next	0	1	2
$s_0 = [E_0(x) \mapsto?, E_0(y) \mapsto?, \text{next} \mapsto  V ]$		2	?	?	
$s_1 = s_0[E_0(x) \mapsto 4]$		2	4	?	
$s_2 = s_1[\text{next} \mapsto s_0(\text{next}) + 1]$		3	4	?	?
$s_3 = s_2[E_1(x) \mapsto 1]$		3	1	?	?
$s_4 = s_3[E_1(\text{result}) \mapsto 2]$		3	1	?	2
$s_5 = s_4[E_1(y) \mapsto 3]$		3	1	3	2
$s_6 = s_5[E_0(y) \mapsto s_5(s_1(\text{next})), \text{next} \mapsto s_1(\text{next})]$		2	1	2	2

call by reference für Parameter und Rückgabe

Umgebung:	Belegung:	x	y	result
$E_0 = [x \mapsto 0, y \mapsto 1]$		0	1	
$E_1 = E_1[x \mapsto E_0(x), \text{result} \mapsto E_0(y)]$		0	1	1
Zustand:	Werte:	next	0	1
$s_0 = [E_0(x) \mapsto?, E_0(y) \mapsto?, \text{next} \mapsto  V ]$		2	?	?
$s_2 = s_1 = s_0[E_0(x) \mapsto 4]$		2	4	?
$s_3 = s_2[E_1(x) \mapsto 1]$		2	1	?
$s_4 = s_3[E_1(\text{result}) \mapsto 2]$		2	1	2
$s_6 = s_5 = s_4[E_1(y) \mapsto 3]$		2	1	3