# Semantyka i Weryfikacja programów

Praca domowa 1.

Hubert Michalski hm438596

6 lutego 2024

## 1 Zadanie

Podaj semantykę naturalną (semantykę operacyjną dużych kroków) dla języka o następującej gramatyce:

**Num** $\ni n ::= 0 \mid 1 \mid -1 \mid 2 \mid -2 \mid \ldots$
**Var** $\ni x ::= x \mid y \mid \ldots$
**Expr** $\ni e ::= n \mid x \mid e_1 + e_2 \mid e_1 * e_2 \mid e_1 - e_2$
**Instr** $\ni I ::= x := e \mid I_1; I_2 \mid$ **skip** $\mid$ **if** $e = 0$ **then** $I_1$ **else** $I_2 \mid$ **step** $x$ **by** $e$ **check** $\mid$ **for var** $x := e_1$ **to** $e_2$ **do** $I$ **end**

## 2 Rozwiązanie

Zdefiniujmy początkowo konfiguracje robocze oraz końcowe rozwiązania:

- $\Gamma = Inst \times State \times Limit$ (konf. robocze)
- $T = State \cup State \times \{B, C\} \times Var$ (konf. końcowe)

gdzie:

- $State : Var \to \mathbb{Z}$ – "podstawowa" definicja stanu
- $Limit : Var \to \mathbb{Z}$ – definicja dla wartości granicznych, tzn. jeśli $Limit(x) = y$ to $y$ jest wartością graniczną dla zmiennej $x$ w ciele najbardziej wewnętrznej pętli
- $\{B, C\} \times Var$ – flaga, którą będziemy propagować wyżej do zatrzymania ($B = break$) lub kontynuowania ($C = continue$) pętli, oraz zmienna której dotyczy ta flaga

"Kształt" relacji strzałka:

- $I, s, l \to s'$
- $I, s, l \to s', f, x$ gdzie $f \in \{B, C\}$, $x \in Var$

Teraz możemy opisać sementykę:

- Rozpatrzmy na początku semantykę związaną z operacją:

  **step** $x$ **by** $e$ **check**

  W przypadku, gdy nowa wartość zmiennej $x$ jest równa wartości granicznej tej zmiennej, to zwracamy jedynie stan ze zmodyfikowaną zmienną:

  $$\frac{}{\langle \textbf{step } x \textbf{ by } e \textbf{ check}, s, l\rangle \to \langle s[x \mapsto n]\rangle} n := \mathcal{E}[\![x + e]\!]s,\ n = l(x)$$

  Jeśli jednak nowa wartość zmiennej $x \neq l(x)$, to musimy przekazać adekwatną flagę oraz nazwę zmiennej której dotyczy ta flaga:

  $$\frac{}{\langle \textbf{step } x \textbf{ by } e \textbf{ check}, s, l\rangle \to \langle s[x \mapsto n], C, x\rangle} n := \mathcal{E}[\![x + e]\!]s,\ n < l(x)$$

  $$\frac{}{\langle \textbf{step } x \textbf{ by } e \textbf{ check}, s, l\rangle \to \langle s[x \mapsto n], B, x\rangle} n := \mathcal{E}[\![x + e]\!]s,\ n > l(x)$$

- Teraz rozpatrzmy semantykę dla operacji:

$$\textbf{for var } x := e_1 \textbf{ to } e_2 \textbf{ do } I \textbf{ end}$$

Jest to miejsce w którym będą realizowane wszystkie funkcjonalności związane z operacją **step**. Spójrzmy najpierw na podstawową sytuację, gdy ciało pętli nie zwraca flagi, wtedy wykonujemy **jedną** iterację pętli zgodnie z opisem instrukcji:

$$\frac{\langle I, s[x \mapsto n_1], l[x \mapsto n_2]\rangle \to \langle s'\rangle}{\langle \textbf{for var } x := e_1 \textbf{ to } e_2 \textbf{ do } I \textbf{ end}, s, l\rangle \to \langle s'\rangle} n_1 := \mathcal{E}[\![e_1]\!]s,\ n_2 := \mathcal{E}[\![e_2]\!]s$$

Następnie możemy zająć się definiowaniem zachowania dla sytuacji, gdy ciało pętli zwróci flagę *break* oraz flaga ta będzie dotyczyła zmiennej $x$. W tym wypadku jedynie zwracamy stan w którym flaga ta została podniesiona:

$$\frac{\langle I, s[x \mapsto n_1], l[x \mapsto n_2]\rangle \to \langle s', B, x\rangle}{\langle \textbf{for var } x := e_1 \textbf{ to } e_2 \textbf{ do } I \textbf{ end}, s, l\rangle \to \langle s'\rangle} n_1 := \mathcal{E}[\![e_1]\!]s,\ n_2 := \mathcal{E}[\![e_2]\!]s$$

W przeciwnym przypadku, gdy flaga ta nie dotyczy zmiennej z tej pętli – propagujemy ją wyżej:

$$\frac{\langle I, s[x \mapsto n_1], l[x \mapsto n_2]\rangle \to \langle s', B, y\rangle}{\langle \textbf{for var } x := e_1 \textbf{ to } e_2 \textbf{ do } I \textbf{ end}, s, l\rangle \to \langle s', B, y\rangle} n_1 := \mathcal{E}[\![e_1]\!]s,\ n_2 := \mathcal{E}[\![e_2]\!]s$$

Musimy także zapisać analogiczne reguły dla flagi *continue*. Zatem jeśli flaga dotyczy zmiennej z danej pętli, to zostanie wykonana kolejna iteracja. W przeciwnym wypadku propagujemy flagę wyżej do pętli której ona dotyczy – takiej pętli może oczywiście nie być, ale mamy dowolność co do zachowania w tej sytuacji. Jasne jest, że uwaga ta tyczy się obu flag.

$$\frac{\langle I, s[x \mapsto n_1], l[x \mapsto n_2]\rangle \to \langle s', C, x\rangle \quad \langle \textbf{for var } x := x \textbf{ to } n_2 \textbf{ do } I \textbf{ end}, s', l\rangle \to \langle z\rangle}{\langle \textbf{for var } x := e_1 \textbf{ to } e_2 \textbf{ do } I \textbf{ end}, s, l\rangle \to \langle z\rangle} n_1 := \mathcal{E}[\![e_1]\!]s,\ n_2 := \mathcal{E}[\![e_2]\!]s$$

$$\frac{\langle I, s[x \mapsto n_1], l[x \mapsto n_2]\rangle \to \langle s', C, y\rangle}{\langle \textbf{for var } x := e_1 \textbf{ to } e_2 \textbf{ do } I \textbf{ end}, s, l\rangle \to \langle s', C, y\rangle} n_1 := \mathcal{E}[\![e_1]\!]s,\ n_2 := \mathcal{E}[\![e_2]\!]s$$

Gdzie $\langle z\rangle$ w tym przypadku może być zarówno $\langle s''\rangle$ jak i $\langle s'', f, y\rangle$ ($y \neq x$).

- Następnie weźmy semantykę dla operacji:

$$I_1; I_2$$

Poza łączeniem kolejnych instrukcji ma ona także za zadanie przerywanie obliczeń w momencie napotkania na flagę, zatem jej semantyka jest kluczowa dla prawidłowego zachowania reszty operacji:

$$\frac{\langle I_1, s, l\rangle \to \langle s'\rangle \quad \langle I_2, s', l\rangle \to \langle z\rangle}{\langle I_1; I_2, s, l\rangle \to \langle z\rangle}$$

gdzie $\langle z\rangle$ jest zdefiniowane jak poprzednio tzn. rozbija się na sytuację z flagą i bez. Gdy $I_1$ zwróci flagę to:

$$\frac{\langle I_1, s, l\rangle \to \langle s', f, x\rangle}{\langle I_1; I_2, s, l\rangle \to \langle s', f, x\rangle}$$

- Pozostały teraz jedynie w miarę "podstawowe" reguły. Kolejną operacją niech będzie:

$$\textbf{if } e = 0 \textbf{ then } I_1 \textbf{ else } I_2$$

Definiując semantykę tej operacji, warto jednak pamiętać, że ona także musi propagować zwracane flagi:

$$\frac{\langle I_1, s, l\rangle \to \langle z\rangle}{\langle \textbf{if } e = 0 \textbf{ then } I_1 \textbf{ else } I_2, s, l\rangle \to \langle z\rangle} n := \mathcal{E}[\![e]\!]s,\ n = 0$$

gdzie $\langle z\rangle$ jest zdefiniowane tak samo jak wyżej. Zupełnie analogiczna reguła będzie dla przypadku $n \neq 0$:

$$\frac{\langle I_2, s, l\rangle \to \langle z\rangle}{\langle \textbf{if } e = 0 \textbf{ then } I_1 \textbf{ else } I_2, s, l\rangle \to \langle z\rangle} n := \mathcal{E}[\![e]\!]s,\ n \neq 0$$

- Semantykę dla operacji:

$$x := e$$

definiujemy standardowo:

$$\frac{}{\langle x := e, s, l\rangle \to \langle s[x \mapsto n]\rangle} n := \mathcal{E}[\![e]\!]s$$

- Na koniec definiujemy operację:

$$\frac{}{\langle \textbf{skip}, s, l\rangle \to \langle s\rangle}$$