ZÁKLADY MATEMATICKEJ TEÓRIE PROGRAMOV

Časť 3.3: Sémantika programov – Sémantika iteratívnych programov

Igor Prívara
Inštitút informatiky a štatistiky

FMFI UK Bratislava, Katedra informatiky

Základy teórie programovania

Programové schémy – abstrakcia programov

- základné pojmy, vlastnosti programových schém
- rozhodnuteľnosť vlastností programových schém
- porovnávanie tried programových schém

Správnosť programov – vzhľadom na špecifikácie

- Floydova metóda a Hoareova metóda
- indukčné techniky použité pri dokazovaní správnosti
- (systematická) konštrukcia správnych programov
- dokazovanie správnosti rekurzívnych programov

Sémantika programov – formálny význam programov

- princípy operačnej, denotačnej a axiomatickej sémantiky
- algebraická štruktúra sémantických domén
- **formálna definícia denotačného a operačného významu imperatívnych** a rekurzívnych **programov**
- **porovnanie denotačného a operačného významu programov**

Typy a sémantika – využitie typov pri definícii sémantiky

Sémantika imperatívnych programov

Syntax – jednoduchý imperatívny jazyk

- syntaktické obory – výrazy (celočíselné, booleovské), príkazy
- syntaktické konštruktory – zložené (štruktúrované) príkazy

Sémantika – "metajazyk" pre popis sémantiky

- sémantické obory (celé čísla, pravdivostné hodnoty, stavy pamäte)
- semantické funkcie - sémantické konštruktory

Operačná sémantika – vyjadrená postupnou zmenou stavu

- príkaz cyklu umožňuje nekonečné výpočty
- úlohu nedefinovaného stavu (reprezentujúceho nekonečný výpočet) bude hrať špeciálny stav – "dolník" $\perp \notin \Sigma$
- vstupno/výstupná charakterizácia operačnej sémantiky

Denotačná sémantika – vyjadrená funkciou nad stavmi

- sémantika príkazu cyklu – čiastočne definovaná funkcia (keď sa výpočet neskončí, hodnota nie je definovaná)
- rozšírenie čiastočných funkcií $\Sigma \mapsto \Sigma$ na totálne $(\Sigma \cup \perp) \mapsto (\Sigma \cup \perp)$
- výsledkom výpočtu, začínajúceho nedefinovaným stavom nemôže byť "dobre definovaný" stav
- sémantiku cyklu $\mathcal{M}[\![$ **while** b **do** S **od** $]\!]\sigma$ popíšeme ako limitu postupnosti funkcií – aproximujúcich k "otočení" cyklu

Syntax jazyka

Symboly – $Ivar, Icon, Bcon$

celočíselné premenné – $Ivar =_{nt} \{x, y, z, \ldots\}$

celočíselné konštanty – $Icon =_{nt} \{m, n, \ldots\}$

booleovské konštanty – $Bcon = \{$ **true** , **false** $\}$

Syntaktické obory – $Iexp, Bexp, Stat$

celočíselné výrazy – $Iexp =_{nt} \{s, s_i, \ldots\}$

$$s ::= x \mid m \mid s_1 + s_2 \mid \cdots \mid \textbf{if } b \textbf{ then } s_1 \textbf{ else } s_2 \textbf{ fi}$$

booleovské výrazy – $Bexp =_{nt} \{b, b_i, \ldots\}$

$$b ::= \textbf{ true } \mid \textbf{ false } \mid s_1 \textbf{ eq } s_2 \mid \cdots \mid \textbf{ not } b \mid b_1 \textbf{ and } b_2 \mid \cdots$$

príkazy – $Stat =_{nt} \{S, S_i, \ldots\}$

$$S ::= x := s \mid S_1; S_2 \mid \textbf{if } b \textbf{ then } S_1 \textbf{ else } S_2 \textbf{ fi} \mid \textbf{while } b \textbf{ do } S \textbf{ od}$$

program – príkaz

Syntaktická identita – $\equiv$ $(\equiv_{Iexp}, \equiv_{Bexp}, \equiv_{Stat})$

dve konštrukcie sú syntakticky identické ak pozostávajú z rovnakých postupností symbolov

Sémantické obory

Sémantické obory – diskrétne cpo

Diskrétne cpo celých čísiel – $V_\perp = V \cup \{\perp_V\}$

- množina celých čísiel – $V =_{nt} \{\alpha, \alpha_i, \ldots\}$
- aritmetické funkcie na celých číslach, napr. $\_ +_V \_ : V \times V \mapsto V$
- monotónne rozšírenie funkcií nad V na $V_\perp$

Diskrétne cpo pravdivostných hodnôt – $W_\perp = W \cup \{\perp_W\}$

- pravdivostné hodnoty – $W = \{tt, ff\}$
- relácie (podmnožiny $V \times V$), napr. $\_ =_W \_ : V \times V \mapsto W$
- booleovské funkcie, napr. $\neg_W \_ : W \mapsto W$; $\_ \wedge_W \_ : W \times W \mapsto W$
- monotónne rozšírenie relácií a funkcií nad W na $W_\perp$

Diskrétne cpo stavov – $\Sigma_\perp = \Sigma \cup \{\perp_\Sigma\}$

- množina stavov $\Sigma =_{df} Ivar \mapsto V_\perp =_{nt} \{\sigma, \ldots\}$
- stav σ – charakterizácia stavu pamäti
- $\sigma(x)$ – okamžitá hodnota premennej x v stave σ

Základné sémantické funkcie

Sémantický podmienkový výraz

$$if\_then\_else\_fi : W_\perp \times C \times C \mapsto C$$

- cpo $W_\perp = W \cup \{\perp_W\}$
- ľubovoľné cpo C
- pre ľubovoľné $c_1, c_2 \in C$ a $\beta \in W_\perp$

$$if\ \beta\ then\ c_1\ else\ c_2\ fi = \begin{cases} c_1 & \text{ak } \beta = tt \\ c_2 & \text{ak } \beta = ff \\ \perp_C & \text{ak } \beta = \perp_W \end{cases}$$

Variant stavu

$$\sigma\{x/\alpha\} : \Sigma_\perp \times Ivar \times V_\perp \mapsto \Sigma_\perp$$

- vlastnosti variantu stavu - pre ľubovoľné $\sigma \in \Sigma_\perp$, $\alpha \in V_\perp$,
  - $\perp_\Sigma\{x/\alpha\} = \perp_\Sigma$
  - $\sigma\{x/\alpha\}(y) = \alpha \quad$ ak $x \equiv y$
  - $\sigma\{x/\alpha\}(y) = \sigma(y) \quad$ ak $x \not\equiv y$
- prefixový zápis - $variant(\sigma, x, \alpha)$

Lema: Pre všetky $\sigma, \alpha_1, \alpha_2$ a $x \not\equiv y$ platí:

- $\sigma\{x/\sigma(x)\} = \sigma$
- $\sigma\{x/\alpha_1\}\{x/\alpha_2\} = \sigma\{x/\alpha_2\}$
- $\sigma\{x/\alpha_1\}\{y/\alpha_2\} = \sigma\{y/\alpha_2\}\{x/\alpha_1\}$

Dôkaz: priamo z vlastností variantu pre všetky $z \in Ivar$

Sémantika výrazov

Význam celočíselných výrazov – $\mathcal{V} : Iexp \mapsto (\Sigma_\perp \mapsto V_\perp)$

- $\mathcal{V}[\![s]\!] \perp_\Sigma =_{df} \perp_V$
- $\mathcal{V}[\![x]\!]\sigma =_{df} \sigma(x)$
- $\mathcal{V}[\![m]\!]\sigma =_{df} \alpha_m$
- $\mathcal{V}[\![s_1 + s_2]\!]\sigma =_{df} \mathcal{V}[\![s_1]\!]\sigma \ +_V \ \mathcal{V}[\![s_2]\!]\sigma$
- ...
- $\mathcal{V}[\![$ **if** b **then** s_1 **else** s_2 **fi** $]\!]\sigma =_{df}$
  $if\ \mathcal{W}[\![b]\!]\sigma\ then\ \mathcal{V}[\![s_1]\!]\sigma\ else\ \mathcal{V}[\![s_2]\!]\sigma\ fi$

Význam booleovských výrazov – $\mathcal{W} : Bexp \mapsto (\Sigma_\perp \mapsto W_\perp)$

- $\mathcal{W}[\![b]\!] \perp_\Sigma =_{df} \perp_W$
- $\mathcal{W}[\![$ **true** $]\!]\sigma =_{df} tt$
- $\mathcal{W}[\![$ **false** $]\!]\sigma =_{df} ff$
- $\mathcal{W}[\![s_1$ **eq** $s_2]\!]\sigma =_{df} \mathcal{V}[\![s_1]\!]\sigma =_W \mathcal{V}[\![s_2]\!]\sigma$
- ...
- $\mathcal{W}[\![$ **not** $b]\!]\sigma =_{df} \neg_W \mathcal{W}[\![b]\!]\sigma$
- $\mathcal{W}[\![b_1$ **and** $b_2]\!]\sigma =_{df} \mathcal{W}[\![b_1]\!]\sigma \ \wedge_W \ \mathcal{W}[\![b_2]\!]\sigma$
- ...

Príklady – nech $\sigma(x) = 3, \sigma(y) = 4$

- $\mathcal{V}[\![$ **if** x **eq** y **then** $x + z$ **else** $y + 1$ **fi** $]\!]\sigma = 5$
- $\mathcal{W}[\![$ **true and not** $(x$ **eq** $y)]\!]\sigma = tt$

Operačná v/v sémantika

$$\mathcal{O}_v : Stat \mapsto (\Sigma_\perp \mapsto_s \Sigma_\perp)$$

- $\mathcal{O}[\![x := s]\!]\sigma =_{df} \sigma\{x/\mathcal{V}[\![s]\!]\sigma\}$
- $\mathcal{O}[\![S_1; S_2]\!]\sigma =_{df} \mathcal{O}[\![S_2]\!](\mathcal{O}[\![S_1]\!]\sigma)$
- $\mathcal{O}[\![\textbf{if } b \textbf{ then } S_1 \textbf{ else } S_2 \textbf{ fi}]\!]\sigma =_{df}$
  $if\ \mathcal{W}[\![b]\!]\sigma\ then\ \mathcal{O}[\![S_1]\!]\sigma\ else\ \mathcal{O}[\![S_2]\!]\sigma\ fi$
- $\mathcal{O}[\![\textbf{while } b \textbf{ do } S \textbf{ od}]\!]\sigma =_{df}$
  - $\sigma' \in \Sigma$, ak existuje $n \geq 0$ a $\sigma_0, \ldots, \sigma_n$ také že $\sigma = \sigma_0$, $\sigma' = \sigma_n$ a $\sigma_i = \mathcal{O}[\![S]\!]\sigma_{i-1}$ (pre $i = 1, 2, \ldots, n$), $\mathcal{W}[\![b]\!]\sigma_i = tt$ (pre $i = 0, 1, \ldots, n-1$) a $\mathcal{W}[\![b]\!]\sigma_n = ff$
  - $\perp_\Sigma$, inak

Lema: $\forall S \in Stat \quad \mathcal{O}[\![S]\!]\perp_\Sigma = \perp_\Sigma$

Dôkaz: indukciou vzhľadom na štruktúru S:
$S \equiv x := s$: $\mathcal{O}[\![S]\!]\perp_\Sigma = \perp_\Sigma \{x/\mathcal{V}[\![s]\!]\perp_\Sigma\} = \perp_\Sigma$
$S \equiv \textbf{if } b \textbf{ then } S_1 \textbf{ else } S_2 \textbf{ fi}$:
$\mathcal{O}[\![S]\!]\perp_\Sigma = if\ \mathcal{W}[\![b]\!]\perp_\Sigma\ then \cdots fi = if\ \perp_W\ then \cdots fi = \perp_\Sigma$

Lema (OS): Nech $S^0 =$ **skip** a $S^i = S^{i-1}; S$.
Potom $\mathcal{O}[\![\textbf{while } b \textbf{ do } S \textbf{ od}]\!]\sigma =$

- $\sigma' \in \Sigma$, ak $\exists n :\ n \geq 0$ také, že $\sigma' = \mathcal{O}[\![S^n]\!]\sigma$, $\mathcal{W}[\![b]\!](\mathcal{O}[\![S^m]\!]\sigma) = tt$ pre $m = 0, 1, \cdots, n-1$ a $\mathcal{W}[\![b]\!](\mathcal{O}[\![S^n]\!]\sigma) = ff$
- $\perp_\Sigma$ v opačnom prípade

Dôkaz: priamo z definície $\mathcal{O}$.

Denotačná sémantika

$$\mathcal{M} : Stat \mapsto (\Sigma_\perp \mapsto_s \Sigma_\perp)$$

- $\mathcal{M}[\![x := s]\!] =_{df} \lambda\sigma.\ \sigma\{x/\mathcal{V}[\![s]\!]\sigma\}$
- $\mathcal{M}[\![S_1; S_2]\!] =_{df} \lambda\sigma.\ \mathcal{M}[\![S_2]\!](\mathcal{M}[\![S_1]\!]\sigma)$
- $\mathcal{M}[\![\textbf{if } b \textbf{ then } S_1 \textbf{ else } S_2 \textbf{ fi}]\!] =_{df}$
  $\lambda\sigma.\ if\ \mathcal{W}[\![b]\!]\sigma\ then\ \mathcal{M}[\![S_1]\!]\sigma\ else\ \mathcal{M}[\![S_2]\!]\sigma\ fi$
- $\mathcal{M}[\![\textbf{while } b \textbf{ do } S \textbf{ od}]\!] =_{df} \sqcup_0^\infty \phi_i$, kde
  - $\phi_0 = \lambda\sigma.\ \perp_\Sigma$
  - $\phi_{i+1} = \lambda\sigma.\ if\ \mathcal{W}[\![b]\!]\sigma\ then\ \phi_i(\mathcal{M}[\![S]\!]\sigma)\ else\ \sigma\ fi$, pre $i \geq 0$

Lema: $\forall S \in Stat \quad \mathcal{M}[\![S]\!] \in \Sigma_\perp \mapsto_s \Sigma_\perp$

Dôkaz: indukciou vzhľadom na i dokážeme, že $\{\phi_i\}_0^\infty$ je reťazcom striktných funkcií. Prípad $\phi_0 \sqsubseteq \phi_1$ vyplýva priamo z definície ϕ_0. Pri dôkaze $\phi_{i+1} \sqsubseteq \phi_{i+2}$ treba uvažovať pre ľubovoľné σ' tri prípady $\beta = \mathcal{W}[\![b]\!]\sigma'$:

- $\beta = \perp_W$: zrejme $\phi_{i+1}(\sigma') = \perp_\Sigma = \phi_{i+2}(\sigma')$
- $\beta = tt$: z indukčnej hypotézy $\phi_i(\mathcal{M}[\![S]\!]\sigma') \sqsubseteq \phi_{i+1}(\mathcal{M}[\![S]\!]\sigma')$
- $\beta = ff$: zrejme $\phi_{i+1}(\sigma') = \sigma' = \phi_{i+2}(\sigma')$

Lema (MS): Pre všetky $\sigma, \sigma' \in \Sigma$ a $i \geq 0$ platí $\sigma' = \phi_i(\sigma)$ práve vtedy, keď $\exists j : 0 \leq j < i$ také, že (pre $k = 0, 1, \cdots, j-1$)

- $\sigma' = \mathcal{M}[\![S^j]\!]\sigma$
- $\mathcal{W}[\![b]\!](\mathcal{M}[\![S^k]\!]\sigma) = tt$ a $\mathcal{W}[\![b]\!](\mathcal{M}[\![S^j]\!]\sigma) = ff$

Dôkaz: indukciou vzhľadom na i (intuícia!).

Sémantická interpretácia príkazov

Sémantické rovnice – "prepisovacie pravidlá"

- $\mathcal{M}[\![x := s]\!]\sigma =_{df} \sigma\{x/\mathcal{V}[\![s]\!]\sigma\}$
- $\mathcal{M}[\![\textbf{skip}]\!]\sigma =_{df} \sigma$
- $\mathcal{M}[\![S_1; S_2]\!]\sigma =_{df} \mathcal{M}[\![S_2]\!](\mathcal{M}[\![S_1]\!]\sigma)$
- $\mathcal{M}[\![\textbf{if } b \textbf{ then } S_1 \textbf{ else } S_2 \textbf{ fi}]\!]\sigma =_{df}$
  $if\ \mathcal{W}[\![b]\!]\sigma\ then\ \mathcal{M}[\![S_1]\!]\sigma\ else\ \mathcal{M}[\![S_2]\!]\sigma\ fi$
- $\mathcal{M}[\![\textbf{while } b \textbf{ do } S \textbf{ od}]\!]\sigma =_{df}$
  $\mathcal{M}[\![\textbf{if } b \textbf{ then } S; \textbf{while } b \textbf{ do } S \textbf{ od else skip fi}]\!]\sigma$

Príklady:

1. $\mathcal{M}[\![x := 0;\ y := x + 1]\!]\sigma = \mathcal{M}[\![y := x + 1]\!](\mathcal{M}[\![x := 0]\!]\sigma) =$
   $\mathcal{M}[\![y := x + 1]\!]\sigma\{x/\mathcal{V}[\![0]\!]\sigma\} = \mathcal{M}[\![y := x + 1]\!]\sigma\{x/0\} =$
   $\sigma\{x/0\}\{y/\mathcal{V}[\![x + 1]\!]\sigma\{x/0\}\} =$
   $\sigma\{x/0\}\{y/(\mathcal{V}[\![x]\!]\sigma\{x/0\} + \mathcal{V}[\![1]\!]\sigma\{x/0\})\} =$
   $\sigma\{x/0\}\{y/(\sigma\{x/0\}(x) + 1)\} = \sigma\{x/0\}\{y/(0 + 1)\} =$
   $\sigma\{x/0\}\{y/1\}$

2. Cvičenie: pre $z \not\equiv x,\ z \not\equiv y,\ x \not\equiv y$ dokázať:
   $\mathcal{M}[\![z := x;\ x := y;\ y := z]\!]\sigma\{x/2\}\{y/3\} = \sigma\{x/3\}\{y/2\}\{z/2\}$

Príklady:

1. $\mathcal{M}[\![\textbf{while true do } S \textbf{ od}]\!] = \sqcup_0^\infty \phi_i$
   - $\phi_0 = \lambda\sigma.\ \perp_\Sigma$
   - $\phi_{i+1} = \lambda\sigma.\ if\ \mathcal{W}[\![\textbf{true}]\!]\sigma\ then\ \phi_i(\mathcal{M}[\![S]\!]\sigma)\ else\ \sigma\ fi = \lambda\sigma.\ \perp_\Sigma$

2. $\mathcal{M}[\![\textbf{while false do } S \textbf{ od}]\!] = \sqcup_0^\infty \phi_i$
   - $\phi_0 = \lambda\sigma.\ \perp_\Sigma$
   - $\phi_{i+1} = \lambda\sigma.\ if\ \mathcal{W}[\![\textbf{false}]\!]\sigma\ then\ \phi_i(\mathcal{M}[\![S]\!]\sigma)\ else\ \sigma\ fi = \lambda\sigma.\ \sigma$

3. $\mathcal{M}[\![\textbf{while } x > 0 \textbf{ do } x := x - 1 \textbf{ od}]\!]\sigma\{x/2\} = \sigma\{x/0\}$ pre $\sigma \in \Sigma$:

   $$\phi_i = \lambda\sigma.\ if\ \mathcal{W}[\![x > 0]\!]\sigma\ then\ \phi_{i-1}(\mathcal{M}[\![x := x - 1]\!]\sigma)\ else\ \sigma\ fi$$

   - $\phi_0(\sigma\{x/2\}) = \perp_\Sigma$
   - $\phi_1(\sigma\{x/2\}) = \phi_0(\sigma\{x/1\}) = \perp_\Sigma$
   - $\phi_2(\sigma\{x/2\}) = \phi_1(\sigma\{x/1\}) = \phi_0(\sigma\{x/0\}) = \perp_\Sigma$
   - $\phi_3(\sigma\{x/2\}) = \phi_2(\sigma\{x/1\}) = \phi_1(\sigma\{x/0\}) = \sigma\{x/0\}$
   - $\phi_i(\sigma\{x/2\}) = \sigma\{x/0\}$ pre $i > 3$.

   Takže $(\sqcup_0^\infty \phi_i)(\sigma\{x/2\}) = \sqcup_0^\infty \phi_i(\sigma\{x/2\}) = \sqcup_0^\infty \sigma\{x/0\} = \sigma\{x/0\}$

Veta: $\forall S \in Stat \;\; \mathcal{O}[\![S]\!] = \mathcal{M}[\![S]\!]$

Dôkaz: indukciou vzhľadom na štruktúru S. Ak S nie je príkaz cyklu, výsledok vyplýva priamo z definície.

Nech teda $S \equiv$ **while** b **do** S_1 **od**.

Prípad $\mathcal{O}[\![S]\!]\sigma = \sigma' \;\Rightarrow\; \mathcal{M}[\![S]\!]\sigma = \sigma'$:

- $\sigma' \in \Sigma$: Podľa lemy (OS) $\exists n \geq 0 : \;\; \sigma' = \mathcal{O}[\![S_1^n]\!]\sigma$, (pre $m = 0, 1, \ldots, n-1$) $\mathcal{W}[\![b]\!](\mathcal{O}[\![S_1^m]\!]\sigma) = tt$ a $\mathcal{W}[\![b]\!](\mathcal{O}[\![S_1^n]\!]\sigma) = ff$. Keďže na základe ind. hypotézy platí $\mathcal{O}[\![S_1]\!] = \mathcal{M}[\![S_1]\!]$, $\exists n \geq 0 :$ $\sigma' = \mathcal{M}[\![S_1^n]\!]\sigma$, $\mathcal{W}[\![b]\!](\mathcal{M}[\![S_1^m]\!]\sigma) = tt$ (pre $m = 0, 1, \ldots, n-1$) a $\mathcal{W}[\![b]\!](\mathcal{M}[\![S_1^n]\!]\sigma) = ff$. Uvažujme reťazec funkcií

  - $\phi_0 = \bot_\Sigma$
  - $\phi_{i+1} = \lambda\sigma.\; if \;\; \mathcal{W}[\![b]\!]\sigma \;\; then \;\; \phi_i(\mathcal{M}[\![S_1]\!]\sigma) \;\; else \;\; \sigma \;\; fi \quad$ pre $i > 0$.

  Keďže z lemy (MS) vyplýva $\sigma' = \phi_i(\sigma)$ pre $i \geq n+1$, dostaneme: $\sigma' = \sqcup_0^\infty \phi_i(\sigma) = (\sqcup_0^\infty \phi_i)\sigma = \mathcal{M}[\![S]\!]\sigma$.

- $\sigma' = \bot_\Sigma$: Potom musí platiť $\forall k : \;\; \phi_k(\sigma) = \bot_\Sigma$ a teda aj $\mathcal{M}[\![S]\!]\sigma = \bot_\Sigma$. Predpokladajme opak, t.j. že $\phi_k(\sigma) = \sigma' \in \Sigma$. Potom podľa lemy (MS), indukčnej hypotézy a lemy (OS) $\exists n \geq 0 : \;\; \sigma'' = \mathcal{O}[\![S_1^n]\!]\sigma$, (pre $m = 0, 1, \ldots, n-1$) $\mathcal{W}[\![b]\!](\mathcal{O}[\![S_1^m]\!]\sigma) = tt$ a $\mathcal{W}[\![b]\!](\mathcal{O}[\![S_1^n]\!]\sigma) = ff$. Takže $\mathcal{O}[\![S]\!]\sigma = \sigma' \in \Sigma$, čo je v spore s predpokladom.

Prípad $\mathcal{M}[\![S]\!]\sigma = \sigma' \;\Rightarrow\; \mathcal{O}[\![S]\!]\sigma = \sigma'$:

Predpokladajme, že $\mathcal{O}[\![S]\!]\sigma = \sigma'' \neq \sigma'$. Na základe predchádzajúcej úvahy aj $\mathcal{M}[\![S]\!]\sigma = \sigma''$, čo je v spore s predpokladom.