ZÁKLADY MATEMATICKEJ TEÓRIE PROGRAMOV

Časť 2.2: Správnosť programov – Hoareova metóda

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

Logický systém

Jazyk – dobre vytvorené formuly α, β.

Sémantika – platnosť (pravdivosť) formúl: $\models \alpha$;
formula α platí v danej triede modelov.

Dokazovací systém – dokazateľnosť formúl: $\vdash \alpha$;
formula α sa dá dokázať (odvodiť) z **axióm** a **inferenčných pravidiel** systému

$$\frac{\alpha_1 \cdots \alpha_n}{\beta}.$$

Vlastnosti systému –

zdravý systém – dokazateľné sú len pravdivé formuly

$$\vdash \alpha \quad \Rightarrow \quad \models \alpha,$$

úplný systém – každá pravdivá formula je dokazateľná

$$\models \alpha \quad \Rightarrow \vdash \alpha.$$

Hoareova metóda – logický systém pre dokazovanie čiastočnej správnosti programov založený na jazyku **induktívnych formúl**

$$\{p\}\, P\, \{q\}.$$

Induktívna (invariantná) formula

Význam induktívnej formuly

$$\models \quad \{p\}\, P\, \{q\}$$

závisí od významu podmienok p, q a významu programu P:

formula je pravdivá $\Leftrightarrow$ ak vstupné hodnoty programu P spĺňajú podmienku p a po zastavení programu (príkazu) P výstupné hodnoty P vyhovujú podmienke q.

- $\{x = 0\}\, x := x + 1\, \{x = 1\}$ – je pravdivá formula,
- $\{x = 0\}\, x := x + 1\, \{x = 2\}$ – nie je pravdivá formula,
- $\{x = 0\}\, x := x + 1\, \{x > 0\}$ – je pravdivá formula, ale ...

najslabšia vstupná podmienka – $wp(P, q)$
k programu P a výstupnej podmienke q:

$\forall p$ ak platí $\{wp(P,q)\}\, P\, \{q\},\ \{p\}\, P\, \{q\}$ potom $p \Longrightarrow wp(P,q)$

najsilnejšia výstupná podmienka – $sp(P, p)$
k programu P a vstupnej podmienke p

$\forall q$ ak platí $\{p\}\, P\, \{sp(P,p)\},\ \{p\}\, P\, \{q\}$ potom $sp(P,p) \Longrightarrow q$

Najslabšia vstupná podmienka $wp(P, q)$

$$\forall p \text{ ak platí } \{p\}\, P\, \{q\} \text{ potom } p \Longrightarrow wp(P, q)$$

- $wp(x := s, q) = q[x/s]$
- $wp(S_1; S_2, q) = wp(S_1, wp(S_2, q))$
- $wp(\textbf{if } b \textbf{ then } S_1 \textbf{ else } S_2 \textbf{ fi}, q) = \text{if } b \text{ then } wp(S_1, q) \text{ else } wp(S_2, q) \text{ fi}$
- $wp(\textbf{while } b \textbf{ do } S \textbf{ od}, q)$ – nevieme vyjadriť v jazyku 1. rádu

Najsilnejšia výstupná podmienka $sp(P, p)$

$$\forall q \text{ ak platí } \{p\}\, P\, \{q\} \text{ potom } sp(P, p) \Longrightarrow q$$

- $sp(x := s, p) = \exists y\, \{p[x/y] \;\&\; x = s[x/y]\}$
- $sp(S_1; S_2, p) = sp(S_2, sp(S_1, p))$
- $sp(\textbf{if } b \textbf{ then } S_1 \textbf{ else } S_2 \textbf{ fi}, p) = sp(S_1, p\&b) \wedge sp(S_2, p\&\neg b)$
- $sp(\textbf{while } b \textbf{ do } S \textbf{ od}, p)$ – nevieme vyjadriť

Inferenčný systém $\mathcal{H}$

Axiómatická schéma priradenia

$$\{p(\overline{x}, g(\overline{x}, \overline{y}))\}\, \overline{y} := g(\overline{x}, \overline{y})\, \{p(\overline{x}, \overline{y})\}$$

$$\{q[x/s]\}\, x := s\, \{q\}$$

Kompozičné pravidlo

$$\frac{\{p\}\, S_1\, \{q\} \qquad \{q\}\, S_2\, \{r\}}{\{p\}\, S_1; S_2\, \{r\}}$$

Alternatívne pravidlo

$$\frac{\{p\&b\}\, S_1\, \{q\} \qquad \{p\&\neg b\}\, S_2\, \{q\}}{\{p\}\ \textbf{if}\ b\ \textbf{then}\ S_1\ \textbf{else}\ S_2\ \textbf{fi}\ \{q\}}$$

Iteratívne pravidlo

$$\frac{\{p\&b\}\, S\, \{p\}}{\{p\}\ \textbf{while}\ b\ \textbf{do}\ S\ \textbf{od}\ \{p\&\neg b\}}$$

Pravidlo následku

$$\frac{p \Rightarrow p_1 \qquad q_1 \Rightarrow q \qquad \{p_1\}\, S\, \{q_1\}}{\{p\}\, S\, \{q\}}$$

Veta: Nech P je štruktúrovaný program, p vstupná a q výstupná podmienka. Ak $\mathcal{H} \vdash \{p\}\, P\, \{q\}$ potom program P je čiastočne správny vzhľadom na p, q.

Dôkaz Hoareovou metódou – časť 1

Program Q – počítajúci $\lfloor\sqrt{x}\rfloor$

Q: **begin** $\{x \geq 0\}$
$[y_1, y_2, y_3] := [0, 1, 1];$
while $y_2 \leq x$ **do** $[y_1, y_2, y_3] := [y_1 + 1, y_2 + y_3 + 2, y_3 + 2]$ **od**;
$[z] := [y_1]$
end $\{z^2 \leq x < (z+1)^2\}$

Induktívna formula – čiastočná správnosť

$$\{x \geq 0\} \;\; \lfloor\sqrt{x}\rfloor \;\; \{z^2 \leq x < (z+1)^2\}$$

Invariant – $R(x, y_1, y_2, y_3)$

$$R(x, y_1, y_2, y_3) : \; (y_1^2 \leq x) \;\&\; (y_2 = (y_1 + 1)^2) \;\&\; (y_3 = 2y_1 + 1)$$

Postačujúce podmienky správnosti –

- $x \geq 0 \;\Rightarrow\; R(x, 0, 1, 1)$
- $R(x, y_1, y_2, y_3) \;\&\; y_2 \leq x \;\Rightarrow\; R(x, y_1 + 1, y_2 + y_3 + 2, y_3 + 2)$
- $R(x, y_1, y_2, y_3) \;\&\; y_2 > x \;\Rightarrow\; y_1^2 \leq x < (y_1 + 1)^2$

Dôkaz Hoareovou metódou – časť 2

1. $x \geq 0 \;\Rightarrow\; R(x,0,1,1)$
2. $\{R(x,0,1,1)\}\,[y_1,y_2,y_3] := [0,1,1]\,\{R(x,y_1,y_2,y_3)\}$ (AP)
3. $\{x \geq 0\}\,[y_1,y_2,y_3] := [0,1,1]\,\{R(x,y_1,y_2,y_3)\}$ (PN – 1,2)
4. $R(x,y_1,y_2,y_3)\ \&\ y_2 \leq x \quad\Rightarrow\quad R(x,y_1+1,y_2+y_3+2,y_3+2)$
5. $\{R(x,y_1+1,y_2+y_3+2,y_3+2)\}$
   $[y_1,y_2,y_3] := [y_1+1,y_2+y_3+2,y_3+2]$
   $\{R(x,y_1,y_2,y_3)\}$ (AP)
6. $\{R(x,y_1,y_2,y_3)\ \&\ y_2 \leq x\}$
   $[y_1,y_2,y_3] := [y_1+1,y_2+y_3+2,y_3+2]$
   $\{R(x,y_1,y_2,y_3)\}$ (PN – 4,5)
7. $\{R(x,y_1,y_2,y_3)\}$
   while $y_2 \leq x$ **do** $[y_1,y_2,y_3] := [y_1+1,y_2+y_3+2,y_3+2]$ **od**
   $\{R(x,y_1,y_2,y_3)\ \&\ y_2 > x\}$ (PI – 6)
8. $\{x \geq 0\}$
   $[y_1,y_2,y_3] := [0,1,1];$
   while $y_2 \leq x$ **do** $[y_1,y_2,y_3] := [y_1+1,y_2+y_3+2,y_3+2]$ **od**
   $\{R(x,y_1,y_2,y_3)\ \&\ y_2 > x\}$ (PK – 3,7)
9. $R(x,y_1,y_2,y_3)\ \&\ y_2 > x \quad\Rightarrow\quad y_1^2 \leq x < (y_1+1)^2$
10. $\{y_1^2 \leq x < (y_1+1)^2\}\,[z] := [y_1]\,\{z^2 \leq x < (z+1)^2\}$ (AP)
11. $\{R(x,y_1,y_2,y_3)\ \&\ y_2 > x\}\,[z] := [y_1]\,\{z^2 \leq x < (z+1)^2\}$ (PN–9,10)
12. $\{x \geq 0\}$
    $[y_1,y_2,y_3] := [0,1,1];$
    while $y_2 \leq x$ **do** $[y_1,y_2,y_3] := [y_1+1,y_2+y_3+2,y_3+2]$ **od** ;
    $[z] := [y_1]$
    $\{z^2 \leq x < (z+1)^2\}$ (PK – 8,12)

Program $\{x \geq 0\}\ \lfloor\sqrt{x}\rfloor\ \{z^2 \leq x < (z+1)^2\}$

Q1: **begin** $\{x \geq 0\}$

$[y_1] := [0];$
while $(y_1+1)^2 \leq x$ **do** $[y_1] := [y_1+1]$ **od** ;
$[z] := [y_1]$

end $\{z^2 \leq x < (z+1)^2\}$

Invariant: $(y_1^2 \leq x)$

Q2: **begin** $\{x \geq 0\}$

$[y_1, y_2] := [0, 1];$
while $y_2 \leq x$ **do** $[y_1, y_2] := [y_1+1, y_2+2y_1+3]$ **od** ;
$[z] := [y_1]$

end $\{z^2 \leq x < (z+1)^2\}$

Invariant: $(y_1^2 \leq x)\ \&\ (y_2 = (y_1+1)^2)$

Q3: **begin** $\{x \geq 0\}$

$[y_1, y_2, y_3] := [0, 1, 1];$
while $y_2 \leq x$ **do** $[y_1, y_2, y_3] := [y_1+1, y_2+y_3+2, y_3+2]$ **od**;
$[z] := [y_1]$

end $\{z^2 \leq x < (z+1)^2\}$

Invariant: $(y_1^2 \leq x)\ \&\ (y_2 = (y_1+1)^2)\ \&\ (y_3 = 2y_1+1)$

Dôkaz správnosti schémy – dekompozícia

Programová schéma S – podmienky $p(\overline{x}),\ q(\overline{x}, z)$

S: **begin**

$[y_1, y_2] := [x_1, x_2]$
while $r(y_1, y_2)$ **do**
if $s(y_1, y_2)$ **then** $[y_1] := [f(y_1, y_2)]$ **else** $[y_2] := [g(y_1, y_2)]$ **fi**
od
$[z] := [y_1]$

end

Dokazovaná induktívna formula – $\{p(\overline{x})\}\ S\ \{q(\overline{x}, z)\}$

Symbolický invariant – $R(x_1, x_2, y_1, y_2)$

Dekompozícia dôkazu – $\{p(\overline{x})\}\ S_1; S_2; S_3\ \{q(\overline{x}, z)\}$

- $\{p(\overline{x})\}\ S_1\ \{R(\overline{x}, \overline{y})\}$ S_1 – elementárny príkaz

  $\{R(\overline{x}, x_1, x_2)\}\ [y_1, y_2] := [x_1, x_2]\ \{R(\overline{x}, y_1, y_2)\}$
  $p(\overline{x})\ \Rightarrow\ R(\overline{x}, x_1, x_2)$
  $\{p(\overline{x})\}\ [y_1, y_2] := [x_1, x_2]\ \{R(\overline{x}, \overline{y})\}$

- $\{R(\overline{x}, \overline{y})\}\ S_2\ \{R(\overline{x}, \overline{y})\}$ S_2 – zložený príkaz

- $\{R(\overline{x}, \overline{y})\}\ S_3\ \{q(\overline{x}, z)\}$ S_3 – elementárny príkaz

  $\{q(\overline{x}, y_1)\}\ [z] := [y_1]\ \{q(\overline{x}, z)\}$
  $R(\overline{x}, \overline{y})\ \Rightarrow\ q(\overline{x}, y_1)$
  $\{R(\overline{x}, \overline{y})\}\ [z] := [y_1]\ \{q(\overline{x}, z)\}$

Dôkaz správnosti schémy – dekompozícia

S: **begin**

$[y_1, y_2] := [x_1, x_2]$
while $r(y_1, y_2)$ **do**
if $s(y_1, y_2)$ **then** $[y_1] := [f(y_1, y_2)]$ **else** $[y_2] := [g(y_1, y_2)]$ **fi**
od
$[z] := [y_1]$

end

Dekompozícia dôkazu – $\{R(\overline{x}, \overline{y})\}\, S_2\, \{R(\overline{x}, \overline{y})\}$

- $\{R(\overline{x}, \overline{y})\}$ **while** $r(\overline{y})$ **do** S_{21} **od** $\{R(\overline{x}, \overline{y}) \;\&\; \neg r(\overline{y})\}$

  $$R(\overline{x}, \overline{y}) \;\&\; \neg r(\overline{y}) \;\Rightarrow\; R(\overline{x}, y_1, y_2)$$

- $\{R(\overline{x}, \overline{y}) \;\&\; r(\overline{y})\}\, S_{21}\, \{R(\overline{x}, \overline{y})\}$
- $\{R(\overline{x}, \overline{y}) \;\&\; r(\overline{y})\}$ **if** $s(\overline{y})$ **then** S_{211} **else** S_{212} **fi** $\{R(\overline{x}, \overline{y})\}$
- $\{R(\overline{x}, \overline{y}) \;\&\; r(\overline{y}) \;\&\; s(\overline{y})\}\, S_{211}\, \{R(\overline{x}, \overline{y})\}$

  $$\{R(\overline{x}, f(y_1, y_2), y_2)\}\, [y_1] := [f(y_1, y_2)]\, \{R(\overline{x}, y_1, y_2)\}$$
  $$R(\overline{x}, \overline{y}) \;\&\; r(\overline{y}) \;\&\; s(\overline{y}) \;\Rightarrow\; R(\overline{x}, f(y_1, y_2), y_2)$$
  $$\{R(\overline{x}, \overline{y}) \;\&\; r(\overline{y}) \;\&\; s(\overline{y})\}\, [y_1] := [f(y_1, y_2)]\, \{R(\overline{x}, \overline{y})\}$$

- $\{R(\overline{x}, \overline{y}) \;\&\; r(\overline{y}) \;\&\; \neg s(\overline{y})\}\, S_{212}\, \{R(\overline{x}, \overline{y})\}$

  $$\{R(\overline{x}, y_1, g(y_1, y_2))\}\, [y_2] := [g(y_1, y_2)]\, \{R(\overline{x}, y_1, y_2)\}$$
  $$R(\overline{x}, \overline{y}) \;\&\; r(\overline{y}) \;\&\; s(\overline{y}) \;\Rightarrow\; R(\overline{x}, y_1, g(y_1, y_2))$$
  $$\{R(\overline{x}, \overline{y}) \;\&\; r(\overline{y}) \;\&\; s(\overline{y})\}\, [y_2] := [g(y_1, y_2)]\, \{R(\overline{x}, \overline{y})\}$$

Úplnosť Hoareovských kalkulov

$\mathcal{L}$ – špecifikačný jazyk;
$\mathcal{M}$ – trieda modelov definovaná sémantikou;
$\mathcal{H}$ – Hoareovský dokazovací systém.

- Neúplnosť logiky špecifikačného jazyka $\mathcal{L}$ (Peanova aritmetika);
  riešenie: relatívna úplnosť - všetky pravdivé formuly L sú axiómami $\mathcal{H}$.
- Neúplnosť vyvolaná nedostatočnou výrazovou silou $\mathcal{L}$;
  riešenie: definovateľnosť $wp(P, q)$.
- Neúplnosť vyvolaná programovacími konštrukciami
  (napr. kombinácia rekurzie, procedúry ako parametre, statického rozsahu premenných, globálnych premenných, interných procedúr);
  riešenie: vhodne definovať programovací jazyk.
- Neúplnosť vyplývajúca zo zvolených modelov sémantiky
  (inicializácia premenných s dynamickým rozsahom);
  riešenie: sémantika musí definovať adekvátnu triedu modelov.