ZÁKLADY MATEMATICKEJ TEÓRIE PROGRAMOV

Časť 1.1: Programové schémy

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

Témy štúdia programových schém

Abstrakcia programu – "odfiltrovanie" nepodstatných informácií

- štúdium vlastností riadiacich štruktúr –nezávisle od funkcií a predikátov použitých v programe
- ak nejaká vlastnosť platí pre schému S, platí pre každý program P, ktorý je "inštanciou" schémy S

Triedy schém – štandardné, štruktúrované, rekurzívne

- triedy schém sa odlišujú charakterom riadiacich štruktúr
- abstrakcia niektorých základných tried programov
- porovnávanie tried – "sily" riadiacich štruktúr

Rôzne stupne abstrakcie – stanovenie elementárnych objektov

- elementárne objekty – premenné, príkazy
- napr. rôzne pohľady na abstrakciu priradenia – monolitný stav, modifikácia položiek stavu

Syntax – symboly, termy, predikáty

Individuálne premenné – $X = \{x, y, z, \cdots\}$

- vstupné premenné – X_x – $\overline{x} = \{x_1, \cdots, x_k\}$
- výstupné premenné – X_z – $\overline{z} = \{z_1, \cdots, z_m\}$
- pracovné premenné – X_y – $\overline{y} = \{y_1, \cdots, y_n\}$

Funkčné symboly – $F = \cup_{i=0}^{\infty} F^i$

- pre $f \in F^n$ platí $arity(f) = n$
- $F^n = \{f, g, h, \cdots\}$ – n–árne funkčné symboly
- $F^0 = \{a, b, \cdots\}$ – konštanty

Predikátové symboly – $B = \cup_{i=0}^{\infty} B^i$

- pre $p \in B^n$ platí $arity(p) = n$
- $B^n = \{p, q, \cdots\}$ – n–árne predikátové symboly
- $B^0 = \{0, 1\}$ – logické konštanty: true, false

Špeciálne symboly – $[,], (,), :=, :$

Termy – $T = \{t, t_i, \ldots\}$

1. $F^0 \subseteq T$, $X \subseteq T$
2. ak $t_1, \cdots, t_n \in T$ potom $f(t_1, \cdots, t_n) \in T$

Predikáty – $P = \{q\}$

1. $B^0 \subseteq P$
2. ak $t_1, \cdots, t_n \in T$ potom $p(t_1, \cdots, t_n) \in P$

Syntax – príkazy, schémy

Príkazy – $C = \{st, st_i, \cdots\}$

- počiatočný – **begin** $[\overline{y}] := [t_1(\overline{x}), \cdots, t_n(\overline{x})]$
- koncový – **end** $[\overline{z}] := [t_1(\overline{x}, \overline{y}), \cdots, t_n(\overline{x}, \overline{y})]$
- priraďovací – $[\overline{y}] := [t_1(\overline{x}, \overline{y}), \cdots, t_n(\overline{x}, \overline{y})]$
- príkaz skoku – **goto** i
- podmienkový – **if** $p(\overline{x}, \overline{y})$ **then** st ,
  kde st je priradenie alebo príkaz skoku
- príkaz s návestím – $i : st$
  (st – priradenie, podmienka, skok)

Štandardná programová schéma – konečná postupnosť príkazov

$$S = \{st_0, st_1, \cdots, st_n, st_{n+1}\}$$

- st_0 je počiatočný príkaz
- st_{n+1} je koncový príkaz
- st_i $(1 \leq i \leq n)$ je podmienkový, priraďovací alebo skokový príkaz s návestím i
- skok mieri na návestie z intervalu $< 1, n >$ alebo na návestie **end**

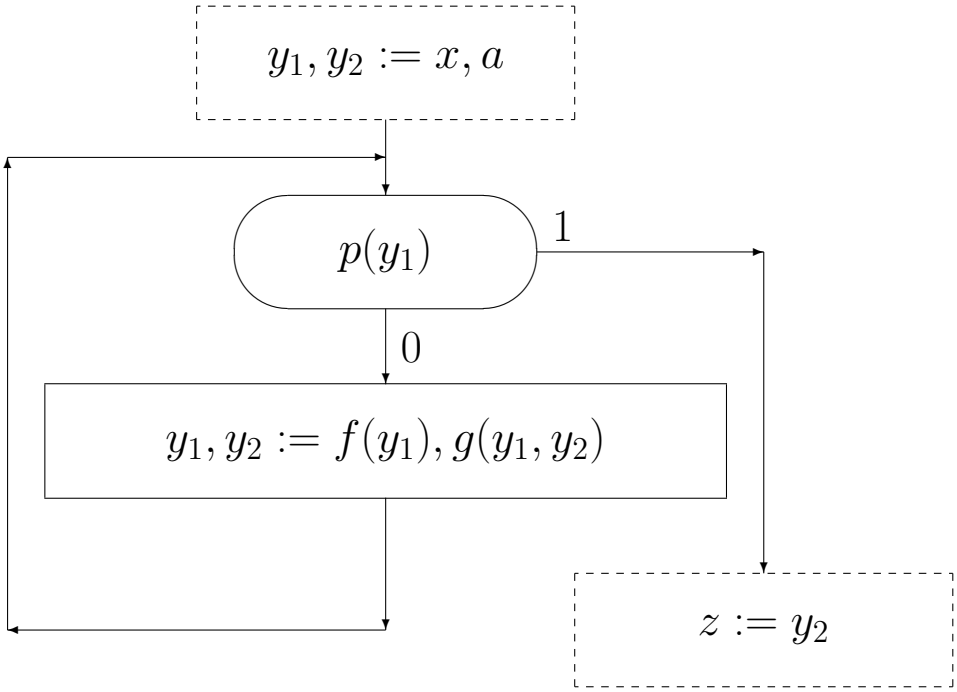
Poznámka – v niektorých prípadoch budeme uvažovať aj schémy bez koncového príkazu

Grafická reprezentácia schémy

S: **begin** $[y_1, y_2] := [x, a]$

1: **if** $p(y_1)$ **then goto end**
2: $[y_1, y_2] := [f(y_1), g(y_1, y_2)]$
3: **goto** 1

end $[z] := [y_2]$



Interpretácia schémy

Interpretácia programovej schémy S - dvojica $\mathcal{I} = (D, i)$

- D – obor interpretácie
- i – interpretačný morfizmus
  - $\forall a \in F^0 \qquad i(a) \in D$
  - $\forall f \in F^n \qquad i(f) \in D^n \mapsto D$
  - $\forall c \in B^0 \qquad i(c) \in \{0, 1\}$
  - $\forall p \in B^n \qquad i(p) \in D^n \mapsto \{0, 1\}$

Program – interpretovaná schéma, dvojica $P = (S, \mathcal{I})$

S: **begin** $[y_1, y_2] := [x, a]$
1: **if** $p(y_1)$ **then goto end**
2: $[y_1, y_2] := [f(y_1), g(y_1, y_2)]$
3: **goto** 1
end $[z] := [y_2]$

$\mathcal{I}$	N
a	1
p	$y_1 = 0$
f	$y_1 - 1$
g	$y_1 * y_2$

Príklad:

S: **begin** $[y_1, y_2] := [x, a]$

1: **if** $p(y_1)$ **then goto end**
2: $[y_1, y_2] := [f(y_1), g(y_1, y_2)]$
3: **goto** 1

end $[z] := [y_2]$

$\mathcal{I}_1$	N
a	1
p	$y_1 = 0$
f	$y_1 - 1$
g	$y_1 * y_2$

P_1: **begin** $[y_1, y_2] := [x, 1]$

1: **if** $y_1 = 0$ **then goto end**
2: $[y_1, y_2] := [y_1 - 1, y_1 * y_2)]$
3: **goto** 1

end $[z] := [y_2]$

Príklad:

S: **begin** $[y_1, y_2] := [x, a]$

1: **if** $p(y_1)$ **then goto end**
2: $[y_1, y_2] := [f(y_1), g(y_1, y_2)]$
3: **goto** 1

end $[z] := [y_2]$

$\mathcal{I}_2$	N
a	0
p	$y_1 = 0$
f	$y_1 - 1$
g	$y_1 + y_2$

P_2: **begin** $[y_1, y_2] := [x, 0]$

1: **if** $y_1 = 0$ **then goto end**
2: $[y_1, y_2] := [y_1 - 1, y_1 + y_2)]$
3: **goto** 1

end $[z] := [y_2]$

Príklad:

S: **begin** $[y_1, y_2] := [x, a]$

1: **if** $p(y_1)$ **then goto end**
2: $[y_1, y_2] := [f(y_1), g(y_1, y_2)]$
3: **goto** 1

end $[z] := [y_2]$

$\mathcal{I}_3$	Σ^*
a	nil
p	$isnil(y_1)$
f	$tail(y_1)$
g	$head(y_1).y_2$

P_3: **begin** $[y_1, y_2] := [x, nil]$

1: **if** $isnil(y_1)$ **then goto end**
2: $[y_1, y_2] := [tail(y_1), head(y_1).y_2)]$
3: **goto** 1

end $[z] := [y_2]$

Abstrakcia – riadiaca štruktúra programu

S: **begin** $[y_1, y_2] := [x, a]$

1: **if** $p(y_1)$ **then goto end**
2: $[y_1, y_2] := [f(y_1), g(y_1, y_2)]$
3: **goto** 1

end $[z] := [y_2]$

$\mathcal{I}_1$	N
a	1
p	$y_1 = 0$
f	$y_1 - 1$
g	$y_1 * y_2$

$\mathcal{I}_2$	N
a	0
p	$y_1 = 0$
f	$y_1 - 1$
g	$y_1 + y_2$

$\mathcal{I}_3$	Σ^*
a	nil
p	$isnil(y_1)$
f	$tail(y_1)$
g	$head(y_1).y_2$

- $P_1 = (S, \mathcal{I}_1)$ – počíta faktoriál x
- $P_2 = (S, \mathcal{I}_2)$ – počíta sumu $1 + 2 + \cdots + x$
- $P_3 = (S, \mathcal{I}_3)$ – obracia reťazec x

Výpočet interpretovanej schémy S

Program – interpretovaná schéma $P = (S, \mathcal{I})$

Výpočet programu P so vstupom v – $(S, \mathcal{I}, v)$

- v je ohodnotenie vstupných premenných – $v : X_x^k \mapsto D^k$
- prirodzená operačná sémantika – (simultánne priradenie)
- ohodnotenie výstupných premenných, dôsledok ukončenia výpočtu – $X_z^m \mapsto D^m$

Výsledok výpočtu – $val(S, \mathcal{I}, v)$

- $\overline{d}$ – ohodnotenie výstupných premenných $\overline{z}$, ak sa výpočet skončí
- nedefinovaný, ak sa výpočet neskončí

Stav výpočtu – $[y_1, \cdots, y_n]$

- hodnoty pracovných premenných

Konfigurácia – $[y_1, \cdots, y_n]_k$

- k – návestie vykonaného príkazu

História výpočtu – výpočtová postupnosť

- stavov
- konfigurácií
- príkazov

Vlastnosti programových schém

Zastavenie –

Program $P = (S, \mathcal{I})$ sa zastaví, ak pre každé ohodnotenie v vstupných premenných $\overline{x}$ je hodnota $val(S, \mathcal{I}, v)$ definovaná.

Schéma S sa zastaví, ak pre každú interpretáciu $\mathcal{I}$ sa zastaví program $(S, \mathcal{I})$.

Divergencia –

Program $P = (S, \mathcal{I})$ diverguje, ak pre každé ohodnotenie v vstupných premenných $\overline{x}$ je hodnota $val(S, \mathcal{I}, v)$ nie je definovaná.

Schéma S diverguje, ak pre každú interpretáciu $\mathcal{I}$ program $(S, \mathcal{I})$ diverguje.

Kompatibilita –

Schémy S_1, S_2 sú kompatibilné, ak majú rovnaké vektory vstupných a výstupných premenných.
Programy $(S_1, \mathcal{I}_1), (S_2, \mathcal{I}_2)$ sú kompatibilné, ak sú kompatibilné schémy S_1, S_2 a obory interpretácií $\mathcal{I}_1, \mathcal{I}_2$ sú rovnaké.

Ekvivalencia – označenie $\equiv$

Kompatibilné programy $(S_1, \mathcal{I}_1), (S_2, \mathcal{I}_2)$ sú ekvivalentné, ak pre rovnaké ohodnotenia vstupných premenných v sú výsledné hodnoty $val(S_1, \mathcal{I}_1, v), val(S_2, \mathcal{I}_2, v)$ buď obe nedefinované alebo obe rovnaké.

Kompatibilné schémy S_1, S_2 sú ekvivalentné, ak pre všetky intepretácie $\mathcal{I}$ sú programy $(S_1, \mathcal{I}), (S_2, \mathcal{I})$ ekvivalentné.

Izomorfizmus – označenie $\cong$ – história výpočtu

Kompatibilné programy $(S_1, \mathcal{I}_1), (S_2, \mathcal{I}_2)$ sú izomorfné, ak pre rovnaké ohodnotenia vstupných premenných v sú postupnosti stavov (histórie) oboch výpočtov $(S_1, \mathcal{I}_1, v), (S_2, \mathcal{I}_2, v)$ rovnaké.

Kompatibilné schémy S_1, S_2 sú izomorfné, ak pre každú interpretáciu $\mathcal{I}$ sú programy $(S_1, \mathcal{I}), (S_2, \mathcal{I})$ izomorfné.

Herbrandove interpretácie

Herbrandovo univerzum $\mathcal{H}$ – reťazce symbolov, zostrojené zo vstupných premenných a funkčných symbolov schémy S:

- ak $x_i \in X_x$ potom "x_i" $\in \mathcal{H}$
- ak $a \in F^0$ potom "a" $\in \mathcal{H}$
- ak $f \in F^n$; "t_1", $\cdots$, "t_n" $\in \mathcal{H}$ potom "$f(t_1, \cdots, t_n)$" $\in \mathcal{H}$

Príklad – $x \in X_x, a \in F^0, h \in F^1, g \in F^2$

$\mathcal{H} = \{$"a", "x", "$h(a)$", "$h(x)$", "$g(x,x)$", "$g(a,a)$",
"$g(a,x)$", "$g(x,a)$", "$h(h(a))$", "$h(h(x))$",
"$h(g(a,a))$", "$h(g(a,x))$", "$h(g(x,a))$",
"$h(g(x,x))$", "$g(h(a),a)$", "$g(a,h(a))$", $\ldots\}$

Herbrandova interpretácia schémy S – dvojica $\mathcal{I}_H = (\mathcal{H}, i_H)$

- $\mathcal{H}$ – Herbrandovo univerzum
- i_H – interpretačný morfizmus symbolov schémy S
  - $\forall x \in X_x \qquad i_H(x) =$ "x"
  - $\forall a \in F^0 \qquad i_H(a) =$ "a"
  - $\forall f \in F^n \qquad i_H(f) \in \mathcal{H}^n \mapsto \mathcal{H}$
    n–tici "t_1", $\cdots$, "t_n" priradí "$f(t_1, \cdots, t_n)$"

Vlastnosti Herbrandovej interpretácie

- interpretácia funkčných symbolov je "pevná", voľná je interpretácia predikátov
- Herbrandova interpretácia "zastupuje" triedu všetkých interpretácií, odlišujúcich sa interpretáciou predikátových symbolov
- umožňujú využiť indukciu vzhľadom na konštrukciu termu

Zladené interpretácie

Interpretácia $\mathcal{I}$ s ohodnotením v je zladená s Herbrandovou interpretáciou $\mathcal{I}_H$ s ohodnotením predikátov práve vtedy, keď pre každé $p \in B^n$

$$i_H(p)(\text{“}t_1\text{”}, \cdots, \text{“}t_n\text{”}) \iff i(p)(i^v(t_1), \cdots, i^v(t_n)).$$

Lema 1: (o existencii zladenej interpretácie)
Ku každej interpretácii $\mathcal{I}$ symbolov danej schémy S a každému ohodnoteniu vstupných premenných v existuje interpretácia $\mathcal{I}_H$, ktorá je s ňou zladená (a naopak).

Myšlienka dôkazu – existencia zladených interpretácií:

Nech $\forall \mathcal{I},\ \forall p \in B^n$: $\quad T = T^0_{p,\mathcal{I}} + T^1_{p,\mathcal{I}}$, kde

$$T^k_{p,\mathcal{I}} = \{(t_1, \cdots, t_n) : i(p)(i^v(t_1), \cdots, i^v(t_n)) = k\}.$$

Interpretáciu $\mathcal{I}_H$, zladenú s $\mathcal{I}$, definuje predpis:

$$i_H(p)(\text{“}t_1\text{”}, \cdots, \text{“}t_n\text{”}) = k,$$

ak $(t_1, \cdots, t_n) \in T^k_{p,\mathcal{I}}$.

Lema 2: (o výpočtoch pri zladených interpretáciách)
Nech S je schéma, $\mathcal{I}$ jej interpretácia, v ohodnotenie vstupov a $\mathcal{I}_H$ interpretácia zladená s $\mathcal{I}$ a v. Potom pre j–te konfigurácie $[d_1, \cdots, d_n]^j_s$ a $[\text{“}t_1\text{”}, \cdots, \text{“}t_n\text{”}]^j_{\overline{s}}$ výpočtov $(S, \mathcal{I}, v)$, $(S, \mathcal{I}_H, \text{“}\overline{x}\text{”})$ platí $s = \overline{s}$ a $i^v(t_i) = d_i$ pre všetky $i \in < 1, n >$.

Myšlienka dôkazu – o výpočtoch zladených interpretácií:

- indukcia vzhľadom na výpočet,
- v indukčnom kroku treba brať do úvahy všetky možné príkazy.

Zladené výpočty

S: **begin** $[y_1, y_2] := [x, a]$
1: **if** $p(y_1)$ **then goto end**
2: $[y_1, y_2] := [f(y_1), g(y_1, y_2)]$
3: **goto** 1
end $[z] := [y_2]$

P_1: **begin** $[y_1, y_2] := [x, 1]$
1: **if** $y_1 = 0$ **then goto end**
2: $[y_1, y_2] := [y_1 - 1, y_1 * y_2)]$
3: **goto** 1
end $[z] := [y_2]$

- výpočet programu $P_1 = (S, I_1)$ s ohodnotením vstupu $v = [x \leftarrow 2]$, charakterizovaný postupnosťou stavov (analogicky konfigurácií)
- symbolický výpočet so zladenou interpretáciou Herbrandovou $\mathcal{I}_H$ interpretáciou

$p(\text{“}x\text{”}) = false \qquad p(\text{“}f(x)\text{”}) = false \qquad p(\text{“}f(f(x))\text{”}) = true$

$[2, 1]$	$[\text{“}x\text{”}, \text{“}a\text{”}]$
$[1, 2]$	$[\text{“}f(x)\text{”}, \text{“}g(x, a)\text{”}]$
$[0, 2]$	$[\text{“}f(f(x))\text{”}, \text{“}g(f(x), g(x, a))\text{”}]$
$[2]$	$[\text{“}g(f(x), g(x, a))\text{”}]$

- interpetáciou stavov symbolického výpočtu dostaneme stavy výpočtu $P_1 = (S, I_1, [x \leftarrow 2])$
- výpočet (S, I_1, v) a "zladený" symbolický výpočet prechádzajú tou istou cestou v grafickej reprezentácii

Využitie Herbrandových interpretácií

1. **Schéma S diverguje práve vtedy, keď diverguje výpočet pre každú Herbrandovu interpretáciu schémy S.**
   - Dôkaz sporom – dôsledok uvedených liem
2. **Schéma S sa zastaví práve vtedy, keď sa zastaví výpočet pre každú Herbrandovu interpretáciu schémy S.**
   - Analógia s problémom divergencie.
3. **Dve kompatibilné schémy S_1, S_2 sú ekvivalentné vtedy a len vtedy, keď pre každú Herbrandovu interpretáciu $\mathcal{I}_H$ sa programy $(S_1, \mathcal{I}_H), (S_2, \mathcal{I}_H)$ buď oba zacyklia alebo sa oba zastavia, pričom platí**

$$val(S_1, \mathcal{I}_H, \text{“}\overline{x}\text{”}) = val(S_2, \mathcal{I}_H, \text{“}\overline{x}\text{”}).$$

   - Nech $S_1 \equiv S_2$ na triede voľných interpretácií, t.j.

$$\forall \mathcal{I}_H : val(S_1, \mathcal{I}_H, \text{“}\overline{x}\text{”}) = val(S_2, \mathcal{I}_H, \text{“}\overline{x}\text{”}).$$

   - $\forall \mathcal{I}, v\ \exists \mathcal{I}_H$ tak, že $(S_1, \mathcal{I}), (S_1, \mathcal{I}_H)$ alebo oba cyklia alebo

$$val(S_1, \mathcal{I}, v) = i^v(val(S_1, \mathcal{I}_H, \overline{x}));$$

     analogicky pre S_2 (dôsledok lemy 2).
   - Potom programy $(S_1, \mathcal{I}), (S_2, \mathcal{I})$ buď oba cyklia alebo sa oba zastavia s rovnakým výsledkom.
4. **Dve kompatibilné schémy S_1, S_2 sú izomorfné práve vtedy, keď pre každú Herbrandovu interpretáciu je výpočtová postupnosť stavov S_1 identická s výpočtovou postupnosťou stavov S_2.**
   - Analógia s ekvivalenciou