ZÁKLADY MATEMATICKEJ TEÓRIE PROGRAMOV

Časť 2.3: Indukcia pri dokazovaní správnosti 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

Floydova metóda

redukcia dôkazu čiastočnej správnosti programu na dokazovanie predikátových formúl:

- program rozdelíme **deliacimi bodmi** na konečné cesty (počiatočný, koncový, resp. vnútorné body),
- pre každý vnútorný deliaci bod sformulujeme **invariant** $I_A(\overline{x}, \overline{y})$ – podmienku, ktorá platí pri každom prechode deliacim bodom; počiatočnému deliacemu bodu zodpovedá vstupná podmienka, koncovému výstupná podmienka,
- ku každej konečnej ceste AB odvodíme a dokážeme **verifikačnú podmienku**: ak pri prechode deliacim bodom A je splnená podmienka I_A potom po prechode cestou AB bude v deliacom bode B splnená podmienka I_B

  $$\forall \overline{x}, \overline{y} \;\; I_A(\overline{x}, \overline{y}) \;\&\; R_{AB}(\overline{x}, \overline{y}) \Rightarrow I_B(\overline{x}, r_{AB}(\overline{x}, \overline{y})).$$

  Sémantické vlastnosti cesty:

  – $R_{AB}(\overline{x}, \overline{y})$ – podmienka pre prechod cesty AB,

  – $r_{AB}(\overline{x}, \overline{y})$ – modifikácia pracovných premenných pri prechode AB.

Veta: Ak pre všetky cesty v programe P (definované deliacimi bodmi) platia zodpovedajúce verifikačné podmienky, potom je program P čiastočne správny.

Dôkaz: tvrdenie vyplýva z tranzitivity implikácie (indukcia vzhľadom na výpočet).

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.

Výpočtová indukcia

- indukcia vzhľadom na (vybrané) stavy výpočtu, uvažujme výpočtovú postupnosť $s^* = s_0 s_1 \cdots s_n \cdots$
- $next(P, s)$ – množina stavov generovaných programom P zo stavu s
  $S = next(P, s_0)$ – stavy, dosiahnuteľné z daného vstupného stavu s_0

Princíp výpočtovej indukcie: ϕ – totálny predikát na S

$$\{\phi(s_0) \ \wedge \ (\forall s \in S)[\phi(s) \Rightarrow (\forall s' \in next(P, s))\phi(s')]\} \implies (\forall s \in S)\phi(s)$$

Indukcia vzhľadom na konečné cesty – Floydova metóda

Štrukturálna (noetherovská) indukcia

- indukcia na čiastočne usporiadanej množine (S,$\succ$)
- $\succ$ – dobre založené čiastočné usporiadanie

Princíp štrukturálnej indukcie: ϕ – totálny predikát na S

$$(\forall a \in S) \ \{[(\forall b \in S)(a \succ b \ \Rightarrow \ \phi(b))] \ \Rightarrow \ \phi(a)\} \implies (\forall c \in S)\phi(c)$$

Indukcia vzhľadom na štruktúru programu – Hoareova metóda

- usporiadanie $\succ$ je definované reláciou “byť podtermom"