ZÁKLADY MATEMATICKEJ TEÓRIE PROGRAMOV

Časť 2.5 (3.5): Dokazovanie vlastností rekurzívnych 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

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
- **dokazovanie vlastností rekurzívnych programov**

Typy a sémantika – využitie typov pri definícii sémantiky

Indukcia pre rekurzívne programy

Rekurzívny program – $\phi(\overline{x}) \Leftarrow \tau[\phi](\overline{x})$, kde τ je spojitý funkcionál z $[D^n \to D] \to [D^n \to D]$

Spojitý funkcionál τ má najmenší pevný bod $f_\tau = \sqcup_0^\infty \tau^i[\Omega]$, kde $\tau^0[\Omega] = \Omega$ a $\tau^{i+1}[\Omega] = \tau[\tau^i[\Omega]]$

Úplná výpočtová indukcia - prístupný predikát θ – z predpokladu, že pre všetky $i \geq 0$ platí $\theta(\tau^i[\Omega])$ vyplýva $\theta(\sqcup_0^\infty \tau^i[\Omega])$

$$\forall i \ \{[\forall j \ (j < i \Rightarrow \theta(\tau^j[\Omega]))] \Rightarrow \theta(\tau^i[\Omega])\} \ \Rightarrow \ \theta(f_\tau)$$

Fixpointová indukcia - prípustný predikát θ

$$\theta(\Omega) \ \wedge \ \forall f \ \{\theta(f) \ \Rightarrow \ \theta(\tau[f])\} \ \Rightarrow \ \theta(f_\tau)$$

nech $g \in [D^n \to D]$ a $\theta(\phi) : \ \phi \sqsubseteq g$, potom

$$\tau[g] \sqsubseteq g \ \Rightarrow \ f_\tau \sqsubseteq g$$

Štrukturálna indukcia - čiastočne usporiadaná množina $(D, \succ)$

- $\succ$ je dobre založené čiastočné usporiadanie
- θ totálny predikát na D

$$(\forall a \in D) \ \{[(\forall b \in D)(a \succ b \ \Rightarrow \ \theta(b))] \ \Rightarrow \ \theta(a)\} \ \Rightarrow \ (\forall c \in D)\theta(c)$$

Dôkaz úplnou výpočtovou indukciou

Prípustné predikáty - $\wedge\ \alpha_i[\phi] \sqsubseteq \beta_i[\phi]$

α_i, β_i – spojité funkcionály

Programy -

$\phi_1(x) \Leftarrow$ **if** $p(x)$ **then** y **else** $h(\phi_1(k(x), y))$ **fi**

$\phi_2(x) \Leftarrow$ **if** $p(x)$ **then** y **else** $\phi_2(k(x), h(y))$ **fi**

Vlastnosť - $\forall x \forall y\ [f_{\tau_1}(x, y) \equiv f_{\tau_2}(x, y)]$

Dôkaz - prípustný predikát $\theta(\phi_1, \phi_2) :\quad \forall x \forall y\ [\phi_1(x, y) \equiv \phi_2(x, y)]$

krok 1 - $\theta(\tau_1^0[\Omega], \tau_2^0[\Omega]) :\quad \forall x \forall y\ [\tau_1^0[\Omega](x, y) \equiv \tau_2^0[\Omega](x, y)]$

priamo z definície $\tau_1^0[\Omega] = \Omega = \tau_2^0[\Omega]$

krok 2 - $\theta(\tau_1^1[\Omega], \tau_2^1[\Omega]) :\quad \forall x \forall y\ [\tau_1^1[\Omega](x, y) \equiv \tau_2^1[\Omega](x, y)]$

$\tau_1^1[\Omega](x, y) \equiv$

if $p(x)$ then y else $h(\tau_1^0[\Omega](k(x), y))$ fi $\equiv$

if $p(x)$ then y else $\perp$ fi $\equiv$

if $p(x)$ then y else $\tau_2^0[\Omega](k(x), h(y))$ fi $\equiv$

$\tau_2^1[\Omega](x, y) \equiv$

krok 3 - dokážeme $\forall x \forall y\ [\tau_1^i[\Omega](x, y) \equiv \tau_2^i[\Omega](x, y)]$ pre $i \geq 2$

indukčné predpoklady - $\forall x \forall y\ [\tau_1^{i-2}[\Omega](x, y) \equiv \tau_2^{i-2}[\Omega](x, y)]$

$\forall x \forall y\ [\tau_1^{i-1}[\Omega](x, y) \equiv \tau_2^{i-1}[\Omega](x, y)]$

Dôkaz úplnou výpočtovou indukciou (2)

Programy -

$\phi_1(x) \Leftarrow$ **if** $p(x)$ **then** y **else** $h(\phi_1(k(x), y))$ **fi**

$\phi_2(x) \Leftarrow$ **if** $p(x)$ **then** y **else** $\phi_2(k(x), h(y))$ **fi**

krok 3 - dokážeme $\forall x \forall y\ [\tau_1^i[\Omega](x, y) \equiv \tau_2^i[\Omega](x, y)]$ pre $i \geq 2$

indukčné predpoklady - $\forall x \forall y\ [\tau_1^{i-2}[\Omega](x, y) \equiv \tau_2^{i-2}[\Omega](x, y)]$

$\forall x \forall y\ [\tau_1^{i-1}[\Omega](x, y) \equiv \tau_2^{i-1}[\Omega](x, y)]$

$\tau_1^i[\Omega](x, y) \equiv$

definícia $\tau_1^i[\Omega]$

if $p(x)$ then y else $h(\tau_1^{i-1}[\Omega](k(x), y))$ fi $\equiv$

IP pre $i - 1$

if $p(x)$ then y else $h(\tau_2^{i-1}[\Omega](k(x), y))$ fi $\equiv$

definícia $\tau_2^{i-1}[\Omega]$

if $p(x)$ then y else $h($if $p(k(x))$ then y else $\tau_2^{i-2}[\Omega](k(k(x)), h(y))$ fi$)$ fi $\equiv$

IP pre $i - 2$

if $p(x)$ then y else $h($if $p(k(x))$ then y else $\tau_1^{i-2}[\Omega](k(k(x)), h(y))$ fi$)$ fi $\equiv$

prenos h za if

if $p(x)$ then y else if $p(k(x))$ then $h(y)$ else $h(\tau_1^{i-2}[\Omega](k(k(x)), h(y)))$ fi fi $\equiv$

definícia $\tau_1^{i-1}[\Omega]$

if $p(x)$ then y else $\tau_1^{i-2}[\Omega](k(x), h(y))$ fi $\equiv$

IP pre $i - 1$

if $p(x)$ then y else $\tau_2^{i-2}[\Omega](k(x), h(y))$ fi $\equiv$

definícia $\tau_2^i[\Omega]$

$\tau_2^i[\Omega](x, y)$

Dôkaz fixpointovou indukciou

Program - $\phi(x) \Leftarrow$ if $x > 100$ then $x - 10$ else $\phi(\phi(x + 11))$ fi

pevný bod - $f_\tau(x) \equiv$ if $x > 100$ then $x - 10$ else $f_\tau(f_\tau(x + 11))$ fi

Vlastnosť - pre všetky celé čísla x platí $f_\tau(x) \sqsubseteq g(x)$, kde
$g(x)$: if $x > 100$ then $x - 10$ else 91 fi

Dôkaz - podľa fixpointovej indukcie stačí dokázať $\tau[g] \sqsubseteq g$

if $x > 100$ then $x - 10$ else
if [if $x + 11 > 100$ then $x + 11 - 10$ else 91 fi] > 100
then [if $x + 11 > 100$ then $x + 11 - 10$ else 91 fi] $- 10$
else 91 fi $\sqsubseteq$
$\sqsubseteq$ if $x > 100$ then $x - 10$ else 91 fi

prípad $x > 100$ -
$\tau[g](x) = x - 10 = g(x)$

prípad $89 < x \leq 100$ -
$x + 11 > 100$ a $x + 1 \leq 100$, potom $\tau[g](x) = 91 = g(x)$

prípad $x \leq 89$ -
$x + 11 \leq 100$, potom $\tau[g](x) = 91 = g(x)$

Dôkaz štrukturálnou indukciou

Program - $\phi(x) \Leftarrow$ if $x > 100$ then $x - 10$ else $\phi(\phi(x + 11))$ fi

pevný bod - $f_\tau(x) \equiv$ if $x > 100$ then $x - 10$ else $f_\tau(f_\tau(x + 11))$ fi

Vlastnosť - pre všetky celé čísla x platí $f_\tau(x) \equiv g(x)$, kde
$g(x)$: if $x > 100$ then $x - 10$ else 91 fi

Dôkaz - usporiadanie $x \prec y$ práve vtedy, keď $y < x \leq 101$
evidentne $101 \prec 100 \prec 99 \prec \ldots$ ale $102 \not\prec 101$

indukčný krok - pre ľubovoľné x, ak $f_\tau(y) \equiv g(y)$ pre všetky $y \prec x$,
potom platí aj $f_\tau(x) \equiv g(x)$

prípad $x > 100$ -
priamo z definícií oboch funkcií vyplýva $f_\tau(x) \equiv x - 10 \equiv g(x)$

prípad $100 \geq x \geq 90$ -
z definície priamo vyplýva $f_\tau(x) \equiv f_\tau(f_\tau(x + 11)) \equiv f_\tau(x + 1)$
keďže $x + 1 \prec x$, z IP vyplýva $f_\tau(x) \equiv f_\tau(x + 1) \equiv g(x + 1)$
keďže $x + 1 \leq 101$, z definície $g(x + 1) \equiv g(x) \equiv 91$,
odtiaľ $f_\tau(x) \equiv 91 \equiv g(x)$

prípad $x < 90$ -
z definície vyplýva $f_\tau(x) \equiv f_\tau(f_\tau(x + 11))$
keďže $x + 11 \prec x$, z IP $f_\tau(x) \equiv f_\tau(f_\tau(x + 11)) \equiv f_\tau(g(x + 11))$
keďže $x + 11 \leq 100$, z definície $g(x + 11) \equiv 91$
keďže $91 \prec x$, z IP $f_\tau(x) \equiv f_\tau(91) \equiv g(91)$
záverom $f_\tau(x) \equiv f_\tau(91) \equiv g(91) \equiv 91 \equiv g(x)$