ZÁKLADY MATEMATICKEJ TEÓRIE PROGRAMOV

Časť 3.2: Sémantika programov – Algebraická štruktúra sémantických oborov

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

Algebraická štruktúra sémantických oborov

Sémantická doména – algebraická štruktúra

- množina, čiastočne usporiadaná reláciou *aproximácie* $\sqsubseteq$
- nekonečný objekt – ako limita jeho konečných aproximácií
- existuje najmenšia aproximácia ľubovoľného objektu – $\perp$ (určuje len "príslušnosť" k doméne)
- vyjadriteľnosť objektov pomocou spočitateľnej bázy danej domény

Charakterizácia výpočtov – totálne funkcie nad doménami

- matematický aparát – popis ľubovoľnej funkcie definovanej výpočtom programu
- nekonečný výpočet programu – výsledok funkcie vyjadrujúcej význam programu je nedefinovaný prvok $\perp$ (žiadna informácia)
- ak aspoň jeden argument funkcie je definovaný (iné nemusia byť nedefinované – $\perp$), výsledok môže byť definovaný
- viac informácii o argumente (lepšia aproximácia) nemôže zmenšiť "úroveň" aproximácie výsledku

Štruktúra sémantických oborov – rôzne prístupy

- úplné čiastočné usporiadanie – cpo,
- úplné sväzy (D. Scott – beztypové jazyky),
- metrické priestory (moderný prístup).

Úplné čiastočné usporiadanie (cpo)

Čiastočne usporiadaná množina – množina C, čiastočne usporiadaná usporiadaním $\sqsubseteq$, t.j. reláciou

- reflexívnou – $x \sqsubseteq x$
- antisymetrickou – ak $x \sqsubseteq y$ a $y \sqsubseteq x$ potom $x = y$
- tranzitívnou – ak $x \sqsubseteq y$ a $y \sqsubseteq z$ potom $x \sqsubseteq z$

Najmenšia horná a najväčšia dolná hranica – množiny $X \subseteq C$

- $z = \sqcup X \in C$ je najmenšou hornou hranicou X ak
  - $x \sqsubseteq z$ pre všetky $x \in X$
  - $\forall y \in C$ také, že $x \sqsubseteq y$ pre všetky $x \in X$ platí $z \sqsubseteq y$
- $y = \sqcap X \in C$ je najväčšou dolnou hranicou X ak
  - $y \sqsubseteq x$ pre všetky $x \in X$
  - $\forall z \in C$ také, že $z \sqsubseteq x$ pre všetky $x \in X$ platí $z \sqsubseteq y$

Reťazec – postupnosť $\{x_i\}_0^\infty = x_1, x_2, \ldots, x_n, \ldots$ taká, že pre všetky i platí $x_i \sqsubseteq x_{i+1}$ (resp. $x_i \sqsupseteq x_{i+1}$)

Úplné čiastočné usporiadanie – cpo $(C, \sqsubseteq)$
čiastočné usporiadanie $(C, \sqsubseteq)$ s vlastnosťou

- existuje najmenší element vzhľadom na $\sqsubseteq$, t.j. prvok $\bot$ (dolník) taký, že $\forall x \in X \;\; \bot \sqsubseteq x$
- každý reťazec $\{x_i\}_0^\infty$ má najmenšiu hornú hranicu $\sqcup_0^\infty x_i$ v C.

Konštrukcia cpo

Diskrétne cpo – $(C \cup \{\bot_C\}, \sqsubseteq)$

dolník – $\bot_C \notin C$

usporiadanie – $x_1 \sqsubseteq x_2$ práve vtedy, keď $x_1 = \bot_C \ \vee x_1 = x_2$

Lema: $(C \cup \{\bot_C\}, \sqsubseteq)$ je cpo.

Dôkaz: len triviálne re»azce (obsahujú najviac dva rôzne prvky)

Priamy súčin cpo $(C_1, \sqsubseteq_1)$ **a** $(C_2, \sqsubseteq_2)$ – $(C_1 \times C_2, \sqsubseteq)$

dolník – $\bot_{C_1 \times C_2} = \langle \bot_{C_1}, \bot_{C_2} \rangle$

usporiadanie – $\langle x_1, y_1 \rangle \sqsubseteq \langle x_2, y_2 \rangle \Leftrightarrow x_1 \sqsubseteq_1 x_2 \wedge y_1 \sqsubseteq_2 y_2$

Lema: Ak $(C_1, \sqsubseteq_1)$ a $(C_2, \sqsubseteq_2)$ sú cpo potom aj $(C_1 \times C_2, \sqsubseteq)$ je cpo.

Dôkaz: stačí položiť $\sqcup_0^\infty \langle x_i, y_i \rangle = \langle \sqcup_0^\infty x_i, \sqcup_0^\infty y_i \rangle$.

Funkcie z cpo $(C_1, \sqsubseteq_1)$ **do** $(C_2, \sqsubseteq_2)$ – $(C_1 \mapsto C_2, \sqsubseteq)$

dolník – $\bot_f = \lambda x.\ \bot_{C_2}$, t.j. $\forall x \in C_1 \ \ \bot_f(x) = \bot_{C_2}$

usporiadanie – $f \sqsubseteq g$ práve vtedy, keď $\forall x \in C_1$ platí $f(x) \sqsubseteq_2 g(x)$

Lema: Ak $(C_1, \sqsubseteq_1)$ a $(C_2, \sqsubseteq_2)$ sú cpo potom aj $(C_1 \mapsto C_2, \sqsubseteq)$ je cpo.

Dôkaz: K re»azcu $\{f_i\}_0^\infty$ definujeme $f = \sqcup_0^\infty f_i$ predpisom $f(x) = \sqcup_0^\infty f_i(x)$. Potom

- pretože pre každé i a x platí $f_i(x) \sqsubseteq_2 \sqcup_0^\infty f_i(x)$, platí aj $f_i \sqsubseteq f$.
- nech $f_i \sqsubseteq g$ pre všetky i; pre každé $x \in C$ a i platí $f_i(x) \sqsubseteq_{C_2} \sqcup_0^\infty f_i(x) \sqsubseteq_{C_2} g(x)$ a teda $f \sqsubseteq g$.

Konštrukcia cpo

Monotónne funkcie z cpo $(C_1, \sqsubseteq_1)$ **do** $(C_2, \sqsubseteq_2)$ – $(C_1 \mapsto_m C_2, \sqsubseteq)$

monotónna funkcia – $f \in C_1 \mapsto_m C_2$ ak pre všetky $x, y \in C_1$ platí $x \sqsubseteq_1 y \Rightarrow f(x) \sqsubseteq_2 f(y)$

dolník, usporiadanie – ako v cpo $(C_1 \mapsto C_2, \sqsubseteq)$

Lema: Ak $(C_1, \sqsubseteq_1)$, $(C_2, \sqsubseteq_2)$ sú cpo potom aj $(C_1 \mapsto_m C_2, \sqsubseteq)$ je cpo.

Dôkaz: $\bot_f$ je zrejme monotónna funkcia; ukážeme, že $\sqcup$ reťazca monotónnych funkcií je monotónna funkcia. Ak pre $x_1, x_2 \in C_1$ platí $x_1 \sqsubseteq_1 x_2$, potom $f_i(x_1) \sqsubseteq_2 f_i(x_2)$ pre všetky i. Odtiaľ $\sqcup_0^\infty f_i(x_1) \sqsubseteq_2 \sqcup_0^\infty f_i(x_2)$ a teda $f(x_1) \sqsubseteq_2 f(x_2)$.

Striktné funkcie z cpo $(C_1, \sqsubseteq_1)$ **do** $(C_2, \sqsubseteq_2)$ – $(C_1 \mapsto_s C_2, \sqsubseteq)$

striktná funkcia – $f \in C_1 \mapsto_s C_2$ ak $f(\bot_{C_1}) = \bot_{C_2}$

dolník, usporiadanie – ako v cpo $(C_1 \mapsto C_2, \sqsubseteq)$

Lema: Ak $(C_1, \sqsubseteq_1)$, $(C_2, \sqsubseteq_2)$ sú cpo potom aj $(C_1 \mapsto_s C_2, \sqsubseteq)$ je cpo.

Dôkaz: $\bot_f$ je zrejme striktná funkcia. Pre každý reťazec $\{f_i\}_0^\infty$ striktných funkcií je aj $f = \sqcup_0^\infty f_i$ striktná funkcia ($\forall i : \ f_i(\bot_{C_1}) = \bot_{C_2}$ a teda aj $f(\bot_{C_1}) = \bot_{C_2}$).

Lema: Ak C_1 je diskrétne cpo, potom $C_1 \mapsto_s C_2 \ \subseteq \ C_1 \mapsto_m C_2$.

Dôkaz: nech $x_1 \sqsubseteq_1 x_2$, potom buď $x_1 = \bot_{C_1}$ a teda $f(x_1) = f(\bot_{C_1}) = \bot_{C_2} \sqsubseteq_2 f(x_2)$, alebo $x_1 = x_2$ a teda aj $f(x_1) = f(x_2)$.