1-AIN-625 Úvod do matematickej logiky pre programátorov
1-INF-450 Logika pre informatikov

Zimný semester 2012/13

10. prednáška

Ján Komara

Obsah 10. prednášky

Zopakovanie

Cieľ predmetu

- Vybudovať matematické základy deklaratívnych programovacích jazykov.

Stručná osnova predmetu

- Primitívne rekurzívne funkcie
  - Aritmetizácia dátových štruktúr (Gödelizácia).
  - Regulárne rekurzívne definície s mierou.
- Obecne rekurzívne funkcie
  - Regulárne rekurzívne definície do dobre založených relácií:
    - Ackermannova funkcia (1928),
    - univerzálna funkcia pre primitívne rekurzívne funkcie.
- Čiastočne rekurzívne funkcie
  - Kleeneho prvá veta o rekurzii (veta o pevnom bode).
  - Kleeneho veta o normálnej forme.
  - Churchova téza a algoritmicky nerozhodnuteľné problémy.

Zopakovanie

Dobre založené relácie

Vravíme, že relácia $\vec{x} \prec \vec{y}$ na N^n je dobre založená (tiež noetheriánska), ak každá klesajúca postupnosť

$$\vec{x}_1 \succ \vec{x}_2 \succ \vec{x}_3 \succ \vec{x}_4 \succ \cdots$$

je konečná. Tu $\vec{x} \succ \vec{y} \leftrightarrow \vec{y} \prec \vec{x}$.
Úplné dobre založené usporiadanie sa nazýva dobré usporiadanie.

Príklady

- Relácia $\vec{x} \prec \vec{y}$ indukovaná mierou $\mu[\vec{x}]$ do štandardného usporiadania prirodzených čísel:

$$\vec{x} \prec \vec{y} \leftrightarrow \mu[\vec{x}] < \mu[\vec{y}].$$

- Lexikografické usporiadanie dvojíc prirodzených čísel:

$$(a, b) <_{\mathrm{lex}} (c, d) \leftrightarrow a < c \vee a = c \wedge b < d.$$

Zopakovanie

Regulárna rekurzia do dobre založenej relácie $\prec$

Sú to definície v tvare

$$f(\vec{x}) = \tau[f;\vec{x}], \tag{1}$$

pre ktoré sú splnené podmienky regularity.
Podmienky regularity majú tvar:

$$\Gamma^{\tau}_{f(\vec{\rho})}[f;\vec{x}] \to \vec{\rho}[f;\vec{x}] \prec \vec{x}$$

pre každú rekurzívnu aplikáciu $f(\vec{\rho})$ funkcie f, ktorá je strážená podmienkou $\Gamma^{\tau}_{f(\vec{\rho})}$ v terme τ.
Splnenie podmienok pre funkciu definovanou pridruženou rovnosťou

$$f(\vec{x}) = \tau\left[[f]^{\prec}_{\vec{x}};\vec{x}\right].$$

Táto funkcia je potom jediným riešením funkcionálnej rovnice (1).

Zopakovanie

Primitívne rekurzívne funkcie (charakterizácia)

Trieda primitívne rekurzívnych funkcií je najmenšia trieda funkcií, ktorá obsahuje funkciu nasledovníka $\mathrm{S}(x) = x + 1$, funkciu predchodcu $x \dot{-} 1$ a je uzavretá na explicitné definície a regulárne rekurzívne definície s mierou.

Obecne rekurzívne funkcie (definícia)

Trieda obecne rekurzívnych funkcií je najmenšia trieda funkcií, ktorá obsahuje funkciu nasledovníka $\mathrm{S}(x) = x + 1$, funkciu predchodcu $x \dot{-} 1$ a je uzavretá na explicitné definície a regulárne rekurzívne definície do dobre založených relácií.

Obecne rekurzívne funkcie, ktoré nie sú primitívne rekurzívne

- Ackermannova funkcia (1928).
- Univerzálna funkcia pre primitívne rekurzívne funkcie.

Zopakovanie

Základné konštrukcie pri tvorbe deklaratívnych programov

- Premenné, konštanty a funkčné aplikácie.
- Podmienkové výrazy:

$$
\begin{array}{l}
\textbf{case} \\
\quad \varphi_1[\vec{x};\vec{y}_1] \Rightarrow \rho_1[\vec{x},\vec{y}_1] \\
\quad \vdots \\
\quad \varphi_m[\vec{x};\vec{y}_m] \Rightarrow \rho_m[\vec{x};\vec{y}_m] \\
\textbf{end}
\end{array}
\qquad
\begin{array}{l}
\textbf{case} \\
\quad \chi_1[\vec{x}] = 1 \wedge \vec{\omega}_1[\vec{x}] = \vec{y}_1 \Rightarrow \rho_1[\vec{x},\vec{y}_1] \\
\quad \vdots \\
\quad \chi_m[\vec{x}] = 1 \wedge \vec{\omega}_m[\vec{x}] = \vec{y}_m \Rightarrow \rho_m[\vec{x},\vec{y}_m] \\
\textbf{end}.
\end{array}
$$

$\chi_i[\vec{x}]$ je charakt. term pre porovnávanie so vzorom $\varphi_i[\vec{x};\vec{y}_i]$:

$$\chi_i[\vec{x}] = 1 \vee \chi_i[\vec{x}] = 0 \qquad \exists \vec{y}_i \varphi_i[\vec{x};\vec{y}_i] \leftrightarrow \chi_i[\vec{x}] = 1.$$

Sémantika:

$$\mathsf{D}\Big(\chi_1[\vec{x}], \rho_1[\vec{x},\vec{\omega}_1[\vec{x}]], \ldots, \mathsf{D}\big(\chi_m[\vec{x}], \rho_m[\vec{x},\vec{\omega}_m[\vec{x}]], 0\big) \ldots\Big).$$

Zopakovanie

Základné konštrukcie pri tvorbe deklaratívnych programov

- Premenné, konštanty a funkčné aplikácie.
- Podmienkové výrazy:

case
$\varphi_1[\vec{x};\vec{y}_1] \Rightarrow \rho_1[\vec{x},\vec{y}_1]$
$\vdots$
$\varphi_m[\vec{x};\vec{y}_m] \Rightarrow \rho_m[\vec{x};\vec{y}_m]$
end

case
$\chi_1[\vec{x}] = 1 \land \vec{\omega}_1[\vec{x}] = \vec{y}_1 \Rightarrow \rho_1[\vec{x},\vec{y}_1]$
$\vdots$
$\chi_m[\vec{x}] = 1 \land \vec{\omega}_m[\vec{x}] = \vec{y}_m \Rightarrow \rho_m[\vec{x},\vec{y}_m]$
end.

Podmienka úplnosti a jednoznačnosti:

$$\bigvee_{i=1}^{m} \exists \vec{y}_i \varphi_i[\vec{x};\vec{y}_1] \land \bigwedge_{i,j=1}^{m} \forall \vec{y}_i \forall \vec{y}_j \big(\varphi_i[\vec{x};\vec{y}_i] \land \varphi_j[\vec{x};\vec{y}_j] \to \rho_i[\vec{x},\vec{y}_i] = \rho_j[\vec{x},\vec{y}_j]\big).$$

Matematická notácia:

$$\mathcal{D}^{\vec{\omega}_1,\ldots,\vec{\omega}_m}_{\chi_1,\ldots,\chi_m}\big(\varphi_1[\vec{x};\vec{y}_1], \rho_1[\vec{x},\vec{y}_1], \ldots, \varphi_m[\vec{x};\vec{y}_m], \rho_m[\vec{x},\vec{y}_m]\big).$$

Čiastočné funkcie

Čiastočné funkcie

n-árna čiastočná funkcia f je jednoznačná relácia z N^n do N:

$$(\vec{x}, y) \in f \wedge (\vec{x}, z) \in f \rightarrow y = z.$$

Definičný obor čiastočnej funkcie f:

$$\mathrm{dom}\, f = \{\vec{x} \in \mathrm{N}^n \mid \exists y\, (\vec{x}, y) \in f\}.$$

Čiastočná funkcia f je totálna, ak $\mathrm{dom}\, f = \mathrm{N}^n$, t.j.

$$\forall \vec{x} \exists y (\vec{x}, y) \in f.$$

Pre každé $n \geq 1$, symbolom $\emptyset^{(n)}$ označujeme n-árnu čiastočnú funkciu, ktorá nie je nikde definovaná.

Čiastočné funkcie

Usporiadanie čiastočných funkcií

Trieda n-árnych čiastočných funkcií je usporiadaná reláciou inklúzie:

$$f \subseteq g \leftrightarrow \forall \vec{x} \forall y \big((\vec{x}, y) \in f \to (\vec{x}, y) \in g \big).$$

Základné pojmy:

- f je rozšírením g, ak $g \subseteq f$.
- f je zúžením g, ak $f \subseteq g$.
- Rozšírenie f, ktoré je totálne, nazveme zúplnením čiastočnej funkcie f.

Niektoré základné vzťahy:

- $\emptyset^{(n)} \subseteq f$ pre každú čiastočnú n-árnu funkciu f.
- Ak $f \subseteq g$ a f je totálna, potom $f = g$.

Čiastočné funkcie

Reťazec

Nekonečná postupnosť n-árnych čiastočných funkcií

$$f_0, f_1, f_2, \ldots, f_i, f_{i+1}, \ldots$$

je reťazec, ak platí

$$f_0 \subseteq f_1 \subseteq f_2 \subseteq \cdots \subseteq f_i \subseteq f_{i+1} \subseteq \cdots .$$

Množinové zjednotenie $\bigcup_{i=0}^{\infty} f_i$:

$$(\vec{x}, y) \in \bigcup_{i=0}^{\infty} f_i \leftrightarrow \exists i\, (\vec{x}, y) \in f_i,$$

je jeho limita. Je to opäť n-árna čiastočná funkcia.

Čiastočné funkcie

Čiastočná denotácia termov

Tvrdenie $\tau \simeq y$, ktoré čítame takto

hodnota výrazu τ existuje a je rovná číslu y,

je definované induktívne na štruktúru termu τ:

$$x \simeq y \equiv x = y$$

$$f(\rho_1, \ldots, \rho_n) \simeq y \equiv \exists z_1 \cdots \exists z_n \Big(\bigwedge_{i=1}^{n} \rho_i \simeq z_i \wedge (z_1, \ldots, z_n, y) \in f \Big)$$

$$\begin{aligned} \mathrm{D}(\rho_1, \rho_2, \rho_3) \simeq y \equiv \ & \exists z_1 \big(\rho_1 \simeq z_1 \wedge (z_1 \neq 0 \wedge \rho_2 \simeq z \vee \\ & z_1 = 0 \wedge \rho_3 \simeq z) \big). \end{aligned}$$

Ak hodnota termu existuje, potom je určená jednoznačne:

$$\tau \simeq y \wedge \tau \simeq z \to y = z.$$

Ak τ obsahuje len funkcie, potom $\tau \simeq y \leftrightarrow \tau = y$.

Čiastočné funkcie

Silná rovnosť (Kleene)

Označenie:

$\tau\downarrow \equiv \exists y\, \tau \simeq y$ (τ je definovaný, má hodnotu, konverguje)
$\tau\uparrow \equiv \neg\exists y\, \tau \simeq y$ (τ nie je definovaný, nemá hodnotu, diverguje).

Silná rovnosť $\tau \simeq \rho$ je definovaná predpisom

$$\tau \simeq \rho \equiv \exists y \exists z (\tau \simeq y \wedge \rho \simeq z \wedge y = z) \vee \tau\uparrow \wedge \rho\uparrow.$$

Platí

$$\tau \simeq \rho \leftrightarrow \forall y (\tau \simeq y \leftrightarrow \rho \simeq y)$$
$$\tau \simeq \tau \qquad\qquad \tau \simeq \rho \to \rho \simeq \tau$$
$$\tau \simeq \rho \wedge \rho \simeq \sigma \to \tau \simeq \sigma.$$

Ak termy τ, ρ obsahujú len funkcie, potom $\tau \simeq \rho \leftrightarrow \tau = \rho$.

Čiastočné funkcie

Explicitné definície čiastočných funkcií

Sú to definície čiastočných funkcií v tvare

$$f(x_1, \ldots, x_n) \simeq \tau[x_1, \ldots, x_n].$$

Funkcionálna rovnica má jediné riešenie. Je to n-árna čiastočná funkcia f definovaná vzťahom

$$\forall x_1 \cdots \forall x_n \forall y \big(f(x_1, \ldots, x_n) \simeq y \leftrightarrow \tau[x_1, \ldots, x_n] \simeq y\big).$$

Explicitné definície (totálnych) funkcií

$$f(x_1, \ldots, x_n) = \tau[x_1, \ldots, x_n]$$

sú špeciálnym prípadom explicitných definícií čiastočných funkcií.

Kleeneho prvá veta o rekurzii

Veta

Funkcionálna rovnica v neznámej f:

$$f(x_1, \ldots, x_n) \simeq \tau[f; x_1, \ldots, x_n]$$

má najmenšie riešenie n-árnu čiastočnú funkciu $\bigcup_{i=0}^{\infty} f_i$, ktorá je limitou reťazca $f_0, f_1, f_2, \ldots$ definovaného predpisom

$$f_0 = \emptyset^{(n)}$$
$$f_{i+1}(x_1, \ldots, x_n) \simeq \tau[f_i; x_1, \ldots, x_n].$$

Poznámka

Toto je prvá časť Kleeneho prvej vety o rekurzii. V druhej časti sa tvrdí, že najmenšie riešenie je vypočítateľné.

Kleeneho prvá veta o rekurzii

Funkcionálna notácia

Symbolom $\tau[f]$ označme n-árnu čiastočnú funkciu definovanú predpisom:

$$\tau[f](x_1, \dots, x_n) \simeq \tau[f; x_1, \dots, x_n].$$

Kleeneho prvá veta o rekurzii charakterizuje pevné body funkcionálu $\lambda f.\tau[f]$.

Veta o pevnom bode

Funkcionálna rovnica v neznámej f:

$$f = \tau[f]$$

má najmenšie riešenie n-árnu čiastočnú funkciu $\bigcup_{i=0}^{\infty} f_i$, ktorá je limitou reťazca $f_0, f_1, f_2, \dots$ definovaného predpisom

$$f_0 = \emptyset^{(n)} \qquad\qquad f_{i+1} = \tau[f_i].$$

Kleeneho prvá veta o rekurzii

Lema (Monotónnosť)

Pre ľubovolné n-árne čiastočné funkcie f a g platí

$$f \subseteq g \to \tau[f] \subseteq \tau[g].$$

Dôkaz

Indukciou na štruktúru termu τ.

Dôsledok

Ak postupnosť n-árnych čiastočných funkcií

$$f_0, f_1, f_2, \ldots, f_i, \ldots$$

je reťazec, potom aj táto postupnosť n-árnych čiastočných funkcií

$$\tau[f_0], \tau[f_1], \tau[f_2], \ldots, \tau[f_i], \ldots$$

je reťazec.

Kleeneho prvá veta o rekurzii

Lema (Monotónnosť)

Pre ľubovolné n-árne čiastočné funkcie f a g platí

$$\forall\vec{x}\forall y\big(f(\vec{x}) \simeq y \to g(\vec{x}) \simeq y\big) \to \forall\vec{x}\forall y\big(\tau[f;\vec{x}] \simeq y \to \tau[g;\vec{x}] \simeq y\big).$$

Dôkaz

Indukciou na štruktúru termu τ.

Dôsledok

Ak postupnosť n-árnych čiastočných funkcií

$$f_0, f_1, f_2, \ldots, f_i, \ldots$$

je reťazec, potom aj táto postupnosť n-árnych čiastočných funkcií

$$\tau[f_0], \tau[f_1], \tau[f_2], \ldots, \tau[f_i], \ldots$$

je reťazec.

Kleeneho prvá veta o rekurzii

Lema (Spojitosť)

Pre ľubovolný reťazec n-árnych čiastočných funkcií

$$f_0, f_1, f_2, \ldots, f_i, \ldots$$

platí vzťah

$$\tau[\bigcup_{i=0}^{\infty} f_i] = \bigcup_{i=0}^{\infty} \tau[f_i].$$

Kleeneho prvá veta o rekurzii

Lema (Spojitosť)

Pre ľubovolný reťazec n-árnych čiastočných funkcií

$$f_0, f_1, f_2, \ldots, f_i, \ldots$$

platí vzťah

$$\forall \vec{x} \forall y \big(\tau[\bigcup_{i=0}^{\infty} f_i; \vec{x}] \simeq y \leftrightarrow \exists i \, \tau[f_i; \vec{x}] \simeq y \big).$$

Dôkaz

Implikácia ($\leftarrow$) je priamočiary dôsledok monotónosti. Opačná implikácia sa dokazuje indukciou na štruktúru termu τ.

Kleeneho prvá veta o rekurzii

Dôkaz vety o pevnom bode

- Postupnosť $f_0, f_1, f_2, \ldots$ je reťazec, t.j.

$$\forall i\, f_i \subseteq f_{i+1}.$$

- Limita reťazca $\bigcup_{i=0}^{\infty} f_i$ je riešenie funkcionálnej rovnice, t.j.

$$\bigcup_{i=0}^{\infty} f_i = \tau[\bigcup_{i=0}^{\infty} f_i].$$

- Limita reťazca $\bigcup_{i=0}^{\infty} f_i$ je najmenšie riešenie. Ak g je riešenie funkcionálnej rovnice, potom

$$\bigcup_{i=0}^{\infty} f_i \subseteq g.$$

  Tu stačí dokázať

$$\forall i\, f_i \subseteq g.$$

Kleeneho prvá veta o rekurzii

Dôkaz vety o pevnom bode

- Postupnosť $f_0, f_1, f_2, \dots$ je reťazec, t.j.

$$\forall i \forall \vec{x} \forall y \big(f_i(\vec{x}) \simeq y \to f_{i+1}(\vec{x}) \simeq y \big).$$

- Limita reťazca $\bigcup_{i=0}^{\infty} f_i$ je riešenie funkcionálnej rovnice, t.j.

$$\forall \vec{x} \, (\bigcup_{i=0}^{\infty} f_i)(\vec{x}) \simeq \tau[\bigcup_{i=0}^{\infty} f_i; \vec{x}].$$

- Limita reťazca $\bigcup_{i=0}^{\infty} f_i$ je najmenšie riešenie. Ak g je riešenie funkcionálnej rovnice, potom

$$\forall \vec{x} \forall y \big((\bigcup_{i=0}^{\infty} f_i)(\vec{x}) \simeq y \to g(\vec{x}) \simeq y \big).$$

  Tu stačí dokázať

$$\forall i \forall \vec{x} \forall y \big(f_i(\vec{x}) \simeq y \to g(\vec{x}) \simeq y \big).$$

Kleeneho prvá veta o rekurzii

Rekurzívne definície čiastočných funkcií

Sú to definície čiastočných funkcií v tvare

$$f(x_1, \ldots, x_n) \simeq \tau[f; x_1, \ldots, x_n].$$

Čiastočnou funkciou, ktorá je definovaná uvedeným vzťahom, rozumieme najmenšie riešenie tejto funkcionálnej rovnice v triede n-árnych čiastočných funkcií. Existencia takého riešenia plynie z Kleeneho prvej vety o rekurzii.

Nasledujúcu vetu dokážeme až na budúcej prednáške.

Veta

Regulárne rekurzívne definície do dobre založených relácií

$$f(x_1, \ldots, x_n) = \tau[f; x_1, \ldots, x_n]$$

sú špeciálnym prípadom rekurzívnych definícií čiastočných funkcií.

Čiastočne rekurzívne funkcie

Definícia triedy čiastočne rekurzívnych funkcií

- Základné funkcie:
  - funkcia nasledovníka $\mathrm{S}(x) = x + 1$,
  - funkcia predchodcu $x \dot{-} 1$.
- Explicitné definície čiastočných funkcií:

$$f(x_1, \ldots, x_n) \simeq \tau[x_1, \ldots, x_n].$$

- Rekurzívne definície čiastočných funkcií:

$$f(x_1, \ldots, x_n) \simeq \tau[f; x_1, \ldots, x_n].$$

Funkcia je rekurzívna, ak je to totálna čiastočne rekurzívna funkcia.
Predikát je rekurzívny, ak taká je jeho charakteristická funkcia.

Čiastočne rekurzívne funkcie

Veta

Trieda rekurzívnych funkcií je obecne rekurzívne uzavretá.

Dôsledok

- *Každá obecne rekurzívna funkcia je rekurzívna.*
- *Každý obecne rekurzívny predikát je rekurzívny.*
- *Trieda rekurzívnych funkcií je primitívne rekurzívne uzavretá.*
- *Rekurzívne predikáty sú uzavreté na explicitné definície predikátov s ohraničenými formulami.*
- *Rekurzívne funkcie sú uzavreté na definície funkcií ohraničenou minimalizáciou.*
- *Rekurzívne funkcie sú uzavreté na definície funkcií regulárnou minimalizáciou.*

Čiastočne rekurzívne funkcie

Neohraničená minimalizácia

Sú to definície čiastočných funkcií v tvare

$$f(x_1, \ldots, x_n) \simeq \text{najmenšie číslo } y \text{ také, že platí } \varphi[x_1, \ldots, x_n, y],$$

kde φ je ohraničená formula. Skrátený zápis:

$$f(x_1, \ldots, x_n) \simeq \mu y \big[\varphi[x_1, \ldots, x_n, y]\big].$$

Regulárna minimalizácia:

$$f(\vec{x}) = \mu y \big[\varphi[\vec{x}, y]\big] \qquad\qquad \text{ak } \forall \vec{x} \exists y \varphi[\vec{x}, y],$$

je špeciálny prípad neohraničenej minimalizácie.

Veta

Trieda čiastočných rekurzívnych funkcií je uzavretá na definície čiastočných funkcií neohraničenou minimalizáciou.

Čiastočne rekurzívne funkcie

Neohraničená minimalizácia

Sú to definície čiastočných funkcií v tvare

$$f(x_1, \dots, x_n) \simeq y \leftrightarrow \varphi[x_1, \dots, x_n, y] \wedge \forall z < y \, \neg\varphi[x_1, \dots, x_n, z],$$

kde φ je ohraničená formula. Skrátený zápis:

$$f(x_1, \dots, x_n) \simeq \mu y \left[\varphi[x_1, \dots, x_n, y]\right].$$

Regulárna minimalizácia:

$$f(\vec{x}) = \mu y \left[\varphi[\vec{x}, y]\right] \qquad\qquad \text{ak } \forall \vec{x} \exists y \varphi[\vec{x}, y],$$

je špeciálny prípad neohraničenej minimalizácie.

Veta

Trieda čiastočných rekurzívnych funkcií je uzavretá na definície čiastočných funkcií neohraničenou minimalizáciou.

Čiastočne rekurzívne funkcie

Dôkaz.

V odvodení f použijeme túto čiastočne rekurzívnu funkciu:

$$g(y,\vec{x}) \simeq \begin{cases} y & \text{ak platí } \varphi[\vec{x},y], \\ g(y+1,\vec{x}) & \text{ak neplatí } \varphi[\vec{x},y]. \end{cases}$$

Rekurzívnosť čiastočnej funkcie f plynie z tohoto vyjadrenia

$$\begin{aligned} P(\vec{x},y) &\leftrightarrow \varphi[\vec{x},y] \\ g(y,\vec{x}) &\simeq \textbf{if } P(\vec{x},y) \textbf{ then } y \textbf{ else } g(y+1,\vec{x}) \\ f(\vec{x}) &\simeq g(0,\vec{x}). \end{aligned}$$

Korektnosť implementácie plynie z tejto vlastnosti čiastočne rekurzívnej funkcie g:

$$g(y,\vec{x}) \simeq z \leftrightarrow y \leq z \land \varphi[\vec{x},z] \land \forall z_1\big(y \leq z_1 < z \rightarrow \neg\varphi[\vec{x},z_1]\big).$$

Záver

8. a 9. cvičenie

- Výsledky s komentárom nájdete na webe.

10. cvičenie

- Začína hneď po prednáške v miestnosti F1-248.
- Semestrálny test.

11. prednáška

- Aritmetizácia výpočtového modelu pre čiastočne rekurzívne funkcie.