

# 1-AIN-470 Špecifikácia a verifikácia programov

Letný semester 2022/23

12. prednáška

Ján Komara

# Obsah 12. prednášky

Čiastočne rekurzívne funkcie

Výpočtový model pre čiastočne rekurzívne funkcie

Aritmetizácia výpočtového modelu

# Čiastočne rekurzívne funkcie

## Čiastočné funkcie

$n$ -árna čiastočná funkcia  $f$  je jednoznačná relácia z  $\mathbb{N}^n$  do  $\mathbb{N}$ :

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

Čiastočné funkcie sú usporiadané množinovou reláciou  $f \subseteq g$ .

## Silná rovnosť (Kleene)

$\tau \simeq \rho$  platí, ak jedna z nasledujúcich podmienok je splnená:

- ▶ Výrazy  $\tau, \rho$  sú definované a ich hodnoty sú rovnaké.
- ▶ Výrazy  $\tau, \rho$  nie sú definované.

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

Označenie:

- ▶  $\tau \downarrow$ , ak výraz  $\tau$  je definovaný (má hodnotu, konverguje).
- ▶  $\tau \uparrow$ , ak výraz  $\tau$  nie je definovaný (nemá hodnotu, diverguje).

# Čiastočne rekurzívne funkcie

## Kleeneho prvá veta o rekurzii

*Funkcionálna rovnica v neznámej  $f$ :*

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

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

$$f_0 = \emptyset^{(n)}$$

$$f_{i+1}(x_1, \dots, x_n) \simeq \tau[f_i; x_1, \dots, x_n].$$

## Poznámka

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

# Čiastočne rekurzívne funkcie

## Rekurzívne definície čiastočných funkcií

Sú to definície čiastočných funkcií v tvare

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

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

## Poznámka

Regulárne rekurzívne definície do dobre založených relácií

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

sú špeciálnym prípadom rekurzívnych definícií čiastočných funkcií.

# Čiastočne rekurzívne funkcie

## Výpočtový model

- ▶ Výpočet prebieha na monadických numeráloch:  $\underline{x} \equiv \overbrace{S \dots S}^{x\text{-krát}}(0)$ .
- ▶ Jeden krok výpočtu:  $\rho \triangleright_1 \sigma$ . Vyberáme najľavejší redex:

$$\begin{array}{ll} D(\underline{0}, \rho_2, \rho_3) \triangleright_1 \rho_3 & D(\underline{x+1}, \rho_2, \rho_3) \triangleright_1 \rho_2 \\ g_i(\underline{y_1}, \dots, \underline{y_{m_i}}) \triangleright_1 \underline{g_i(y_1, \dots, y_{m_i})} & \text{pre } i = 1, \dots, k \\ f(\underline{x_1}, \dots, \underline{x_n}) \triangleright_1 \tau[f; \underline{x_1}, \dots, \underline{x_n}]. & \end{array}$$

- ▶ Viac krokov výpočtu:  $\rho \triangleright \sigma$ .

## Veta (Ekvivalentnosť výpočtovej a definičnej sémantiky)

Platí

$$f(\underline{x_1}, \dots, \underline{x_n}) \triangleright \underline{y} \leftrightarrow f(x_1, \dots, x_n) \simeq y.$$

# Čiastočne rekurzívne funkcie

## Definícia triedy čiastočne rekurzívnych funkcií

- ▶ Základné funkcie:
  - ▶ funkcia nasledovníka  $S(x) = x + 1$ ,
  - ▶ funkcia predchodcu  $P(x) = x \div 1$ .
- ▶ Explicitné definície čiastočných funkcií:

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

- ▶ Rekurzívne definície čiastočných funkcií:

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

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

# Čiastočne rekurzívne funkcie

## Rekurzívne odvodenia

### Sčítanie

$$x + y \simeq \text{if } x \neq 0 \text{ then } S(P(x) + y) \text{ else } y.$$

### Odčítanie

$$x \dot{-} y \simeq \text{if } x \neq 0 \text{ then if } y \neq 0 \text{ then } P(x) \dot{-} P(y) \text{ else } x \text{ else } 0.$$

### Násobenie

$$x \cdot y \simeq \text{if } x \neq 0 \text{ then } P(x) \cdot y + y \text{ else } 0.$$

### Umocňovanie

$$x^y \simeq \text{if } y \neq 0 \text{ then } x \cdot x^{P(y)} \text{ else } 1.$$



# Výpočtový model pre čiastočne rekurzívne funkcie

## Rekurzívne termy a funkčné symboly (príklad)

Primitívne rekurzívna definícia

$$\begin{aligned}0 + y &= y \\ S(x) + y &= S(x + y).\end{aligned}$$

Regulárna rekurzívna definícia

$$x + y = \text{if } x \neq 0 \text{ then } S(P(x) + y) \text{ else } y.$$

Rekurzívna definícia so silnou rovnosťou

$$x_1 + x_2 \simeq D(x_1, S(P(x_1) + x_2), x_2).$$

Rekurzívny funkčný symbol

$$\lambda_2.D(x_1, S f_2(P(x_1), x_2), x_2).$$

# Výpočtový model pre čiastočne rekurzívne funkcie

## Rekurzívne termy a funkčné symboly

Induktívna definícia triedy rekurzívnych termov a triedy rekurzívnych funkčných symbolov:

- ▶ Premenné  $x_1, x_2, \dots, x_n, \dots$  a konštanta 0 sú rekurzívne termy.
- ▶ Ak  $\tau_1, \tau_2, \tau_3$  sú rekurzívne termy, potom aplikácia diskriminačnej funkcie  $D(\tau_1, \tau_2, \tau_3)$  je rekurzívny term.
- ▶ Ak  $\tau$  je rekurzívny term, potom aplikácie funkcie nasledovníka  $S(\tau)$  a funkcie predchodcu  $P(\tau)$  sú rekurzívne termy.
- ▶ Ak  $\tau_1, \dots, \tau_n$  sú rekurzívne termy, potom aplikácia  $n$ -árnej funkčnej premennej  $f_n(\tau_1, \dots, \tau_n)$  je rekurzívny term.
- ▶ Ak  $\rho_1, \dots, \rho_n$  sú rekurzívne termy a  $\tau$  je rekurzívny term v premenných  $x_1, \dots, x_n$  a funkčnej premennej  $f_n$ , potom aplikácia  $(\lambda_n.\tau)(\rho_1, \dots, \rho_n)$  je rekurzívny term.

$S$ ,  $P$  a  $\lambda_n.\tau$  sa nazývajú rekurzívne funkčné symboly.

## Výpočtový model pre čiastočne rekurzívne funkcie

### Interpretácia rekurzívnych termov a funkčných symbolov

Interpretáciu (denotáciu) definovaných rekurzívnych funkčných symbolov  $\lambda_n.\tau$  definujeme indukciou na štruktúru rekurzívnych termov  $\tau$ :

*Nech  $\tau[f_n; x_1, \dots, x_n]$  je rekurzívny term v premenných  $x_1, \dots, x_n$  a funkčnej premennej  $f_n$ . Predpokladajme ďalej, že rekurzívne funkčné symboly vyskytujúce sa vo výraze  $\tau$  sú interpretované podľa indukčného predpokladu. Potom rekurzívny funkčný symbol  $\lambda_n.\tau$  interpretujeme ako čiastočnú funkciu  $f$  definovanú vzťahom*

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

Interpretáciu rekurzívneho funkčného symbolu  $\lambda_n.\tau$  označujeme tým istým menom  $\lambda_n.\tau$ .

# Výpočtový model pre čiastočne rekurzívne funkcie

## Veta

*Čiastočná funkcia je rekurzívna práve vtedy, keď je interpretáciou nejakého rekurzívneho funkčného symbolu.*

## Dôkaz.

- ▶ Indukciou na dĺžku rekurzívneho odvodu dokážeme, že každá čiastočne rekurzívna funkcia je interpretáciou nejakého rekurzívneho funkčného symbolu.
- ▶ Indukciou na štruktúru rekurzívneho termu  $\tau$  dokážeme, že interpretácia rekurzívneho funkčného symbolu  $\lambda_n.\tau$  je čiastočne rekurzívna funkcia.

# Výpočtový model pre čiastočne rekurzívne funkcie

## Monadické numerály

Výpočet prebieha na monadických numeráloch:

$$0 \quad S(0) \quad SS(0) \quad SSS(0) \quad SSSS(0) \quad \dots$$

Označenie:

- ▶ Ak  $x$  je prirodzené číslo, potom  $\underline{x}$  je monadický numerál, ktorý denotuje číslo  $x$ :

$$\underline{x} \equiv \overbrace{S \dots S}^{x\text{-krát}}(0).$$

- ▶ Ak  $x_1, \dots, x_n$  sú prirodzené čísla, potom

$$\underline{x_1, \dots, x_n} \equiv \underline{x_1}, \dots, \underline{x_n} \equiv \overbrace{S \dots S}^{x_1\text{-krát}}(0), \dots, \overbrace{S \dots S}^{x_n\text{-krát}}(0).$$

## Výpočtový model pre čiastočne rekurzívne funkcie

### Jeden krok výpočtu

Ak uzavretý rekurzívny term  $\tau$  nie je numerál, tak musí obsahovať aspoň jeden podvýraz (*redex*) v tvare

$$D(\underline{x}, \sigma_2, \sigma_3) \quad P(\underline{x}) \quad (\lambda_n.\sigma)(\vec{x}).$$

Jeden výpočtový krok spočíva v nájdení najľavejšieho redexu a jeho nahradením kontrakciou podľa nasledujúcich pravidiel

$$\begin{aligned} D(\underline{0}, \sigma_2, \sigma_3) &\triangleright_1 \sigma_3 \\ D(\underline{x + 1}, \sigma_2, \sigma_3) &\triangleright_1 \sigma_2 \\ P(\underline{x}) &\triangleright_1 \underline{x \div 1} \\ (\lambda_n.\sigma[f_n; \vec{x}])(\vec{x}) &\triangleright_1 \sigma[\lambda_n.\sigma; \vec{x}]. \end{aligned}$$

Tak dostaneme nový uzavretý rekurzívny term  $\rho$  a píšeme

$$\tau \triangleright_1 \rho.$$

# Výpočtový model pre čiastočne rekurzívne funkcie

## Viac krokov výpočtu

Označenie:

- ▶  $\tau_1 \triangleright_k \tau_2$ , ak výraz  $\tau_1$  sa redukuje do výrazu  $\tau_2$  po  $k$  krokoch. To znamená, že existujú uzavreté rekurzívne termy  $\rho_0, \rho_1, \dots, \rho_k$  také, že

$$\tau_1 \equiv \rho_0 \triangleright_1 \rho_1 \triangleright_1 \dots \triangleright_1 \rho_k \equiv \tau_2.$$

Umožníme tiež prípad  $k = 0$ . Vtedy  $\tau_1 \triangleright_0 \tau_2 \leftrightarrow \tau_1 \equiv \tau_2$ .

- ▶  $\tau_1 \triangleright \tau_2$ , ak  $\tau_1 \triangleright_k \tau_2$  pre nejaké  $k$ .
- ▶ Ak  $\tau \triangleright \underline{x}$ , tak vravíme, že výpočet skončil s výsledkom  $x$ .

## Veta (Ekvivalentnosť definičnej a výpočtovej sémantiky)

Pre každý rekurzívny funkčný symbol  $f$  platí:

$$f(\vec{x}) \simeq y \leftrightarrow f(\vec{x}) \triangleright \underline{y}.$$

# Aritmetizácia výpočtového modelu

## Aritmetizácia rekurzívnych termov a funkčných symbolov

Pomocou párových konštruktorov z rôznymi rozlišovacími položkami:

$x_i = \langle 0, i \rangle$  (premenné)

$0 = \langle 1, 0 \rangle$  (konštanta 0)

$D(t_1, t_2, t_3) = \langle 2, t_1, t_2, t_3 \rangle$  (podmienkový výraz)

$\langle t, ts \rangle = \langle 3, t, ts \rangle$  (kontrakcia argumentov)

$e(ts) = \langle 4, e, ts \rangle$  (aplikácia funkcie)

$S = \langle 5, 0 \rangle$  (funkcia nasledovníka)

$P = \langle 6, 0 \rangle$  (funkcia predchodcu)

$f_n = \langle 7, n \rangle$  (funkčná premenná)

$\lambda_n. t = \langle 8, n, t \rangle$  (definovaná funkcia)



# Aritmetizácia výpočtového modelu

## Kontrakcia argumentov

- ▶ Notačná konvencia pre kontrakčnú funkciu:

$$\langle t_1, t_2, ts \rangle \equiv \langle t_1, \langle t_2, ts \rangle \rangle.$$

- ▶ Kontrakciou  $n$ -tice argumentov  $(t_1, \dots, t_n) \in \mathbb{N}^n$  rozumieme číslo

$$\langle t_1, t_2, \dots, t_n \rangle \in \mathbb{N}.$$

- ▶ Projekčná funkcia  $[ts]_i^n$  operuje na kontrakciach argumentov

$$[\langle t_1, t_2, \dots, t_n \rangle]_i^n = t_i \quad \text{pre } 1 \leq i \leq n.$$

Je to primitívne rekurzívna funkcia.

# Aritmetizácia výpočtového modelu

## Aritmetizácia rekurzívnych termov a funkčných symbolov

Číslo  $\ulcorner \tau \urcorner$  resp.  $\ulcorner f \urcorner$  je kódom termu  $\tau$  resp. funkčného symbolu  $f$ :

$$\ulcorner x_i \urcorner = x_i$$

$$\ulcorner 0 \urcorner = 0$$

$$\ulcorner D(\tau_1, \tau_2, \tau_3) \urcorner = \mathbf{D}(\ulcorner \tau_1 \urcorner, \ulcorner \tau_2 \urcorner, \ulcorner \tau_3 \urcorner)$$

$$\ulcorner f(\tau_1, \dots, \tau_n) \urcorner = \ulcorner f \urcorner(\langle \ulcorner \tau_1 \urcorner, \dots, \ulcorner \tau_n \urcorner \rangle)$$

$$\ulcorner S \urcorner = S$$

$$\ulcorner P \urcorner = P$$

$$\ulcorner f_n \urcorner = f_n$$

$$\ulcorner \lambda_n \cdot \tau \urcorner = \lambda_n \cdot \ulcorner \tau \urcorner.$$

# Aritmetizácia výpočtového modelu

## Príklad

Regulárna rekurzívna definícia

$$x + y = \text{if } x \neq 0 \text{ then } S(P(x) + y) \text{ else } y.$$

Rekurzívna definícia so silnou rovnosťou

$$x_1 + x_2 \simeq D(x_1, S(P(x_1) + x_2), x_2).$$

Rekurzívny funkčný symbol

$$\lambda_2.D(x_1, S f_2(P(x_1), x_2), x_2)$$

a jeho aritmetizácia

$$\lambda_2.D\left(x_1, S\left(f_2(\langle P(x_1), x_2 \rangle)\right), x_2\right).$$

# Aritmetizácia výpočtového modelu

## Monadické numerály, časť prvá

Unárna operácia  $\ulcorner \underline{x} \urcorner$  vytvorí kód numerálu  $\underline{x} \equiv \overbrace{S \dots S}^{x\text{-krát}}(0)$ :

$$\ulcorner \underline{x} \urcorner = \ulcorner \overbrace{S \dots S}^{x\text{-krát}}(0) \urcorner.$$

Primitívna rekurzívnosť funkcie  $\ulcorner \underline{x} \urcorner$  plynie z tohoto vyjadrenia

$$\ulcorner \underline{0} \urcorner = \mathbf{0} \qquad \ulcorner \underline{x+1} \urcorner = S(\ulcorner \underline{x} \urcorner).$$

Jej inverzia je funkcia  $Dc(t)$ , ktorá dekóduje kód numerálu:

$$Dc(\ulcorner \underline{x} \urcorner) = x.$$

Primitívna rekurzívnosť funkcie  $Dc(t)$  plynie z tohoto vyjadrenia

$$Dc(\mathbf{0}) = 0 \qquad Dc(S(t)) = Dc(t) + 1.$$

# Aritmetizácia výpočtového modelu

## Monadické numerály, časť druhá

Predikát  $Nm(t)$  platí, ak číslo  $t$  je kódom nejakého numerálu:

$$Nm(t) \leftrightarrow \exists x t = \ulcorner \underline{x} \urcorner.$$

Jej charakteristická funkcia  $Nm_*(t)$  je primitívne rekurzívna:

$$Nm_*(0) = 1$$

$$Nm_* S(t) = 1 \leftarrow Nm(t) = 1$$

$$Nm_* S(t) = 0 \leftarrow Nm(t) \neq 1$$

$$Nm_*(t) = 0 \leftarrow \neg(t = 0 \vee \exists t_1 t = S(t_1)).$$

Predikátová forma uvedenej definície

$$Nm(0)$$

$$Nm S(t) \leftarrow Nm(t).$$

# Aritmetizácia výpočtového modelu

## Substitúcia

Ternárna funkcia  $t[e; rs]$  je aritmetizácia operácie substitúcie  $\tau[\lambda_n.\sigma; \underline{x}]$  nad rekurzívnymi termami:

$$\ulcorner \tau \urcorner [\ulcorner \lambda_n.\sigma \urcorner; \langle \ulcorner \underline{x}_1 \urcorner, \dots, \ulcorner \underline{x}_n \urcorner \rangle] = \ulcorner \tau[\lambda_n.\sigma; \underline{x}_1, \dots, \underline{x}_n] \urcorner.$$

Primitívna rekurzívnosť funkcie  $t[e; rs]$  plynie z tohoto vyjadrenia

$$x_i[e; rs] = [rs]_i^{Ar(e)}$$

$$0[e; rs] = 0$$

$$D(t_1, t_2, t_3)[e; rs] = D(t_1[e; rs], t_2[e; rs], t_3[e; rs])$$

$$\langle t, ts \rangle[e; rs] = \langle t[e; rs], ts[e; rs] \rangle$$

$$f_n(ts)[e; rs] = e(ts[e; rs])$$

$$f(ts)[e; rs] = f(ts[e; rs]) \leftarrow \neg \exists n f = f_n.$$

Tu  $Ar(e)$  je primitívne rekurzívna funkcia taká, že  $Ar(\ulcorner f \urcorner) = n$  pre  $n$ -árny definovaný rekurzívny funkčný symbol  $f$ .

# Aritmetizácia výpočtového modelu

## Pomocné operácie

Špecifikácia:

$$Pn(\ulcorner \underline{x} \urcorner) = \ulcorner \underline{x} \dot{-} 1 \urcorner$$
$$Dn(\ulcorner \underline{x} \urcorner, t_2, t_3) = D(x, t_2, t_3).$$

Primitívna rekurzívnosť oboch funkcií plynie z tohoto vyjadrenia

$$Pn(\mathbf{0}) = \mathbf{0} \qquad Dn(\mathbf{0}, t_2, t_3) = t_3$$
$$Pn S(t) = t \qquad Dn(S(t_1), t_2, t_3) = t_2.$$

Pomocný primitívny rekurzívny predikát

$$Nms(n, ts) \leftrightarrow \forall i (1 \leq i \leq n \rightarrow Nm([ts]_i^n)).$$

# Aritmetizácia výpočtového modelu

## Jeden krok výpočtu

Špecifikácia redukčnej funkcie  $Rd(t)$ :

$$\text{ak } \tau \triangleright_1 \rho, \text{ potom } Rd(\ulcorner \tau \urcorner) = \ulcorner \rho \urcorner \qquad Rd(\ulcorner \underline{x} \urcorner) = \ulcorner \underline{x} \urcorner.$$

Primitívna rekurzívnosť funkcie plynie z tohoto vyjadrenia

$$Rd(0) = 0$$

$$Rd \mathbf{D}(t_1, t_2, t_3) = Dn(t_1, t_2, t_3) \leftarrow Nm(t_1)$$

$$Rd \mathbf{D}(t_1, t_2, t_3) = \mathbf{D}(Rd(t_1), t_2, t_3) \leftarrow \neg Nm(t_1)$$

$$Rd \langle t, ts \rangle = \langle t, Rd(ts) \rangle \leftarrow Nm(t)$$

$$Rd \langle t, ts \rangle = \langle Rd(t), ts \rangle \leftarrow \neg Nm(t)$$

$$Rd \mathbf{S}(t) = \mathbf{S}(Rd(t))$$

$$Rd \mathbf{P}(t) = Pn(t) \leftarrow Nm(t)$$

$$Rd \mathbf{P}(t) = \mathbf{P}(Rd(t)) \leftarrow \neg Nm(t)$$

$$Rd (\lambda_n. t)(ts) = t[\lambda_n. t; ts] \leftarrow Nms(n, ts)$$

$$Rd (\lambda_n. t)(ts) = (\lambda_n. t)(Rd(ts)) \leftarrow \neg Nms(n, ts).$$