Vyčíslitelnost 1

Základní funkce

$$O(x) = 0$$
$$S(x) = x + 1$$
$$I_n^j(x_1 \dots x_n) = x_j$$
$$S_n^m(f, g_{[1,m]}) = h \text{ s.t. } h(x_{[1,n]}) \simeq f(g_1(x_{[1,n]}) \dots g_m(x_{[1,n]}))$$
$$R_n(f,g) = h \text{ s.t. } \begin{cases} h(0, x_{[2,n]}) = f(x_{[2,n]}) \\ h(i, x_{[2,n]}) = g(i, h(i, x_{[2,n]}), x_{[2,n]}) \end{cases}$$
$$M_n(f) = h \text{ s.t.}$$
$$h(x_{[1,n]}) \downarrow = z \leftrightarrow \begin{cases} f(x_{[1,n]}, z) \downarrow = 0 \\ \forall j < z : f(x_{[1,n]}) \downarrow \neq 0 \end{cases}$$

- ČRF– lze ji odvodit pomocí základních funkcí.
- ORF– ČRFa zároveň totální (všude definovaná).
- PRF– lze ji odvodit bez použití minimalizace.

O: Zneužití značení v taháku: občas ČRFtřída (píši $f \in CRF$), občas zastupuje slova *částečně rekurzivní funkce* (píši) f CRF n. f je CRF. Mělo by být jasné z kontextu.

T: $PRF \subset ORF \subset CRF$.

P:

- $CRF \& \neg ORF$ je prázdná funkce f: $g(x,y) = y+1, f = M_1(g)$.
- $ORF \& \neg PRF$ je Ackermannova funkce. Dá se naprogramovat, totální též, tedy je ORF. Pokud však definujeme úrovně výpočtu pro každé k, tak se dokážeme pomocí k for cyklů (PRF) dostat jen do hloubky k a nikdy to tedy nepokryjeme celé.

T: $TM \simeq CRF$, co se výpočetní síly týče.

P:

T:Kleene $\forall k \geq 1$:

1. $\exists CRF \Psi_k(e, x_{[1,k]})$ univerzální pro k proměnných.
2. Lze efektivně získat z funkce její e a z e funkci.
3. $\exists PRF_1 U \& \exists PRF_{k+2} T_k$ s.t. $\Psi_k(e, x_{[1,k]}) \simeq U(\mu_y(T_k(e, x_{[1,k]}, y)))$
4. $\exists PRF_{m+1} s_m$ prostá a rostoucí s.t. $\Psi_{m+n}(e, y_{[1,m]}, x[1,n]) \simeq \Psi_m\left(s_m(e, y_{[1,m]}), x_{[1,n]}\right)$
5. Univerzální funkce je standardní.

T: Univerzální PRFnení sama PRF, univerzální ORFnení sama ORF. Univerzální PRFje v ORF.

P: První dvě části diagonalizací.

Rekurzivní spočetnost

- $\chi \equiv$ pravdivostní funkce výroku nebo charakteristická funkce mny.
- PRP/ORP (predikáty) $\equiv$ jeho χ je PRF/ORF.
- RSP predikát $\equiv$ obor konvergence ČRF.
- M mna je rekurzivní $\equiv \chi \in ORF$.
- M mna je rekurzivně spočetná (RSM) $\equiv M = dom(f), f \in CRF$.
- $W_x = \{m | \varphi_x(m) \downarrow\}$.
- $K = \{x | x \in W_x\}$.
- $K_0 = \{(y,x) | y \in W_x\}$.

T:Post M rekurzivní $\leftrightarrow M$ i $\overline{M}$ jsou RSM. P je $ORP \leftrightarrow P$ a $\neg P$ jsou RSP.

P: Tam: Když je $\chi \in ORF$, můžeme rozhodovat o přítomnosti i nepřítomnosti efektivně. Zpátky: Prostě pustíme oba výpočty souběžně, jeden se zastaví, neboť jsou obě RSM. Pro výroky se to získá z věty o selektoru (níže).

T:Vlastnosti Ψ

1. $\Psi_k(e, x_{[1,k]}) \downarrow, \Psi_k(x_{[1,k]}) \downarrow$ jsou RSP, ale ne ORP/PRP.
2. $\neg\left(\Psi_k(e, x_{[1,k]}) \downarrow\right), \neg\left(\Psi_k(x_{[1,k]}) \downarrow\right)$ nejsou RSP.
3. Ψ_k nelze rozšířit do ORF.

P:

1. Zřejmá.
2. $\Psi_1(x,x) \uparrow$ je $RSP \rightarrow \exists g \in CRF$ co to počítá, tedy má kód x_0, diagonalizační spor.
3. Varianta důkazu, že neexistuje univerzální PRF.

T:O selektoru $\forall RSP_{k+1} Q \exists CRF_k \varphi$ s.t.

$$\Phi(x_{[1,n]}) \downarrow \leftrightarrow \exists y : Q\left(x_{[1,n]}, y\right)$$
$$\Phi(x_{[1,n]}) \downarrow \rightarrow Q\left(x_{[1,n]}, \varphi(x_{[1,n]})\right)$$

P: Pro $Q \in RSP \exists T$ Turingův stroj takový, že T se zastaví a přijme vstup $\leftrightarrow Q(x_{[1,n]}, y)$.

- $\varphi \in CRF \leftrightarrow$ má rek. spočetný graf.
- $\forall RSM$ je oborem hodnot nějaké ČRF.
- $\forall f \in CRF : \text{Rng}(f) \in RSM$.

Převoditelnost

- $A \leq_m B \equiv \exists f, f \in ORF$ s.t. $x \in A \leftrightarrow f(x) \in B$.
- $A \leq_1 B \equiv f$ navíc prostá.
- M 1-úplná $\equiv M \in RSM$ a $\forall B \in RSM : B \leq_1 M$.
- M m-úplná $\equiv M \in RSM$ a $\forall B \in RSM : B \leq_m M$.

T:Vlastnosti K $K \in RSM$, K není rekurzivní, K je 1-úplná.

P: První dvě vlastnosti zřejmé, pro třetí vezměme W_x a $\alpha(y,x,w)$, která ji popisuje (w volná). Použijeme s-m-n větu, získejme $h(y,x) = s_2(e,y,x)$. Pak $\forall y \in W_x$:

$$\alpha(x,y,w) \downarrow \leftrightarrow \varphi_{h(y,x)}(w) \downarrow \leftrightarrow \varphi_{h(y,x)}(h(y,x)) \downarrow \leftrightarrow h(y,x) \in K.$$

T:Vlastnosti K_0 K_0 je 1-úplná.

P: Převodem K na K_0.

Generování RSM

D: f úseková $\equiv \text{Dom}(f) = [0,n]$.

O: PRF, ORF jsou úsekové vždy.

T:Generátory PRM Rekurzivní množiny jsou právě Rng rostoucích úsekových ČRF.

P:

- „$\rightarrow$“: očísluj prvky rek. množiny, $f(0) = \mu_x(x \in M)$, $f(k+1) = \mu_y(y > f(k), y \in M)$.
- „$\leftarrow$“: Pokud f není totální, tak ji konečným cyklem umíme vyčíslit, $\text{Rng}(f)$ je rekurzivní. Pokud f totální je, tak musíme pro y najít x s.t. $f(x) = y$ bez minimalizace. Jenže víme, že díky úsekovosti a růstu platí, že $\exists x : x \leq f(x)$. Tak prostě najdeme horní mez pomocí y a pak minimalizujeme.

T: Rekurzivně spočetné množiny jsou právě obory hodnot prostých úsekových ČRF.

P: Vyrob z φ množinu $B = \{(x,s) | \varphi(x)$ vydá $x \in M$ přesně po s krocích $\}$. Ta je rekurzivní, takže má generátor rostoucí úsekovou f. Zadefinujeme $g(j) = (f(j))_{2,1}$ (první složka). Funkce g je úseková a prostá, neboť ke každému x existuje nejvýše jedno s.

T: Každá nekonečná RSM obsahuje nekonečnou rostoucí podmnožinu.

Imunní a simple množiny

D: M imunní $\equiv |M| \geq \omega \& W_x \subseteq M \rightarrow |W_x| < \omega$.

D: X simple $\equiv X \in RSM \& \overline{X}$ imunní.

O:Neefektivní konstrukce imunní množiny Procházej prvky W_x pro každé x a přidávej elementy do $\overline{M}$.

O:Efektivní konstrukce simple množiny Definujme predikát Q:

$$Q(x,y) \leftrightarrow y \in W_x \& y > 2x.$$

Tvrdíme, že $A = \text{Rng}(\varphi)$ je simple:

- Obor hodnot ČRFje RSM.
- $\varphi(x) > 2x$, pokud $\varphi(x) \downarrow \rightarrow$ z množiny $[0, 2x]$ jsme do A dali nejvýš x čísel $\rightarrow \overline{A}$ je nekonečná.
- z konstrukce plyne: nepřidali jsme žádnou nekonečnou RSM do $\overline{A}$.

$\overline{A}$ je tedy imunní.

Věty o rekurzi

T:První $f \in CRF_1 \rightarrow \exists a$ s.t. $\forall x$:

$$\varphi_{f(a)}(x) \downarrow = \varphi_a(x).$$

P: Hledané a bude tvaru $a = s_1(z,z)$. Protože $s_1 \in PRF$, tak $\varphi_{f(s_1(z,x))}(x)$ je funkcí jen $z, x \rightarrow \exists e$ s.t. :

$$\varphi_{f(s_1(z,z))}(x) \simeq \Psi_2(e,z,x) \simeq \Psi_1(s_1(e,z),x) \simeq \varphi_{s_1(e,z)}(x).$$

Dosaď za $z = e$, $a = s_1(e,e)$.

T:Druhá $f \in CRF_1 \rightarrow \exists$rostoucí$g \in PRF_1$ s.t. $\forall x$:

$$\varphi_{f(g(j))}(x) \simeq \varphi_{g(j)}(x).$$

P: $g(j) = s_2(z,z,j)$, vol $z = e$, podobně jako první věta.

T:Třetí, pro více proměnných $f \in CRF_{n+1} \to \exists a \forall x_{[1,n]}$:

$$\varphi_a(x_{[1,n]}) \simeq f(a, x_{[1,n]}).$$

P:

- Jedna proměnná:

$$f(y,x) \simeq \Psi_2(e,y,x) \simeq \Psi_1(s_1(e,y),x) \simeq \varphi_{s_1(e,y)}(x).$$

  Vol $g(y) = s_1(e,y)$, použij první větu.
- Více proměnných:

$$f(y, x_{[1,n]}) \simeq \Psi_{n+1}(e,y,x_{[1,n]}) \simeq \Psi_n(s_1(e,y), x_{[1,n]})$$
$$\Psi_n(s_1(e,y), x_{[1,n]}) \simeq \varphi_{s_1(e,y)}(x_{[1,n]}).$$

  $s_1(e,y)$ má pevný bod a, vol $y = a$.

T:Čtvrtá $f \in CRF_{n+1} \to \exists g \in PRF_n$ s.t. $\forall x, y_{[1,n]}$:

$$\varphi_{f(g(y_{[1,n]}),y_{[1,n]})}(x) \simeq \varphi_{g(y_{[1,n]})}(x).$$

P: Vol $g(y_{[1,n]}) = s_{n+1}(z,z,y_{[1,n]})$, zopakuj postup stejný, jako výše.

T:Rice A buď netriviální třída $CRF_1 \to B = \{x | \varphi_x \in A\}$ není rekurzivní.

P: Sporem, existuje nutně $b \in B$, $c \notin B$, zadefinuj $f(x) = b$ pokud $x \notin B$, c jinak. $f(x)$ je $ORF \to \exists e$ s.t. $\varphi_{f(e)}(x) \simeq \varphi_e(x)$, a tedy $e \in B$ a $e \notin B$.

R: Nelze efektivně rozhodnout ekvivalence programů.

Produktivní a kreativní množiny

D: B je produktivní $\equiv \exists \Phi \in CRF$ s.t. $\forall x : W_x \subseteq B \to \Phi(x) \downarrow \& \Phi(x) \in B \; W_x$.

D: Funkci Φ, která dokazuje produktivitu pro B, také říkáme produktivní.

D: A kreativní $\equiv A \; RSM \& \overline{A}$ je produktivní.

O: K je kreativní. Φ by byla identita.

O: f prostá a ORF, pak $\{x | f(x) \notin W_x\}$ produktivní

O: Každá produktivní množina obsahuje nekonečnou RSM.

T:O produktivní ORF $\forall B$ produktivní $\exists$ produktivní $f \in ORF$.

P: B je produktivní, Φ přiřazená produktivní funkce. Výsledkem (jako obvykle) bude nějaká funkce $f \equiv \varphi_{g(x)}$ pro vhodné g.

Nejprve pomocná funkce $\alpha(x,y,z)$: $\alpha(x,y,z) \downarrow \leftrightarrow \Phi(x) \downarrow \& z \in W_y$. Použijeme $s-m-n$ větu, dostaneme:

$$\alpha(x,y,z) \simeq \Psi_3(e,x,y,z) \simeq \Psi_1(s_2(e,z,y),z).$$

Zadefinuj PRF$\beta(x,y) \equiv s_2(e,x,y)$. Pak platí:

$$\Psi_1(\beta(x,y),z) \downarrow \leftrightarrow \Phi(x) \downarrow \& z \in W_y.$$

Co je $W_{\beta(x,y)}$? Pokud $\Phi(x) \uparrow$, tak $\emptyset$, jinak W_y.

Nyní aplikuj čtvrtou větu o rekurzi:

$$\exists g \in PRF : \Psi_1(\beta(g(y),y),z) \simeq \Psi_1(g(y),z).$$

$W_g(y)$ je tedy $W_{\beta(g(y),y)}$. Když $\Psi(g(y)) \downarrow$, tak je to rovno W_y. Sporem dokáži, že $\Psi(g(y))$ nemůže nikdy divergovat.

T:O produktivní ORFbijekci Každá produktivní množina B má i příslušnou produktivní funkci, která je v ORFa je bijekcí.

P: Z minulé věty máme ORFf pro příslušnou B. Tu nejdřív přepočítáme na surjektivní g, a nakonec i na injektivní h.

- V prvním kroku vytvoříme nekonečnou M s.t. $x \in M \to W_x = \omega$. Volíme programy, které se zastaví na každý vstup.
- V druhém kroku zadefinujeme $g(x)$ jako $g(x) = f(x) | x \notin M$ a nebo $g(x) = j$, pokud x je j-tý prvek M.
- V třetím kroku definujeme $h(x)$ jako $g(x)$, pokud neporušíme prostotu. Když ji porušíme, najdeme index y_1 množiny $W_{y_1} = W_x \cup \{g(x)\}$ a podíváme se na $g(y_1)$.
  1. Pokud $W_{y_1} \subseteq B$, tak $g(y_1) \in B \backslash W_{y_1}$. Kdyby i $g(y_1)$ se trefilo do předchozích $h(x)$, přidej předchozí $h(x)$ do W_{y_1}, vytvoř y_2 a opakuj, dokud se nedostaneš mimo předchozí hodnoty $h(x)$.
  2. Pokud $W_{y_1} \not\subseteq B$, tak zvol $h(x)$ libovolně z nových hodnot.

T:O ekvivalenci pojmů $\overline{K} \leq_1 B \leftrightarrow \overline{K} \leq_m B \leftrightarrow B$ je produktivní.

P:

- $1 \to 2$ jasné.
- $2 \to 3$: Ukážeme, že produktivita se zachovává vzhůru. Máme $C \leq_m B$, čili $x \in C \leftrightarrow h(x) \in B$. Je-li $W_x \subseteq B$, tak $h^{-1}(W_x) \subseteq C$. Sestrojíme tedy $\beta(x,y)$ tak, aby $\beta(x,y) \downarrow \leftrightarrow h(y) \in W_x$.
- $3 \to 1$: Hledáme prostou $h \in ORF$ s.t. $x \in \overline{K} \leftrightarrow h(x) \in B$. Zadefinuj $\beta(y,x,w) \downarrow \leftrightarrow w = f(y) \& x \in K$. Použij $s-m-n$ větu: $\alpha(y,x) = s_2(e,y,x) \to W_{\alpha(y,x)} = \{w | f(w) = f(y) \& x \in K\}$. Nyní použij čtvrtou větu o rekurzi: $\exists g(x)$ s.t. $\varphi_{g(x}(z) \simeq \varphi_{\alpha(g(x),x)}(z)$.

Neoddělitelné množiny

D: A, B jsou rekurzivně neoddělitelné $\equiv \neg\exists$ rekurzivní M s.t. $A \subseteq M \& B \subseteq \overline{M}$.

D: A, B jsou efektivně neoddělitelné $\exists CRF f$ s.t. :

$$(A \subseteq W_x \& B \subseteq W_y \& W_x \cap W_y = \emptyset) \to f(x,y) \downarrow \& f(x,y) \notin W_x \cup W_y.$$

O: Efektivně neoddělitelné množiny jsou rek. neoddělitelné.

P: Mám-li rekurzivní množinu M, pak snadno najdu funkce tak, aby $W_x = M$ a $W_y = \overline{M}$ a tedy f nemůže existovat.

T: Rek. neoddělitelné množiny nemusí být efektivně neoddělitelné.

T: Existují dvě efektivně neoddělitelné množiny, a to: $A = \{x | \varphi_x(x) \simeq 0\}, B = \{x | \varphi_x(x) \simeq 1\}$.

P: Mějme $A \subseteq W_x$, $B \subseteq W_y$. Vyrobíme $\varphi_{\alpha(x,y)}(w)$ divergující, když $w \notin A \cup B$. Úvahou plus použitím $s-m-n$ věty víme, že $\exists \varphi_{\alpha(x,y)}(w)$ taková, že vrátí 1, pokud w padne do W_x dříve než do W_y, 0 naopak a jinak diverguje. Diagonalizací vidíme, že $\varphi_{\alpha(x,y)}(\alpha(x,y))$ diverguje.

O: Efektivně neoddělitelné RSM A a B jsou kreativní.

T:Dvojná věta o rekurzi Pro ORFf, g existují m, n s.t. $\varphi_m \simeq \varphi_{f(m,n)} \& \varphi_n \simeq \varphi_{g(m,n)}$.

P: $\varphi_{f(x,y)} \to$ VR4 $\to \exists \alpha$ s.t. $\varphi_{f(\alpha(y),y)} \simeq \varphi_{\alpha(y)}$. $\varphi_{g(\alpha(y),y)} \to$ VR1 $\to \exists n$ s.t. $\varphi_{g(\alpha(n),n)} \simeq \varphi_m$. Vol $m = \alpha(n)$.

D:1-převoditelnost $(A,B),(C,D)$ disj. dvojice, pak $(A,B) \leq_1 (C,D) \equiv A \leq_1 C$ pomocí h a $B \leq_1 D$ pomocí té samé h.

T:Ekvivalence 1-úplnosti a efektivní neoddělitelnosti (A,B) je 1-úplná $\leftrightarrow (A,B)$ efekt. neodd.

P:

- „$\to$“: (A,B) 1-úplné, mohu zvolit (C,D) efektivně neoddělitelné, že $(C,D) \leq_1 (A,B)$. Převodem přes h tam a zpět získám funkci dokazující neodd. (A,B).
- „$\leftarrow$“: Máme (C,D) efekt. neodd., což dokazuje f, a nějaké (A,B). Zadefinuj $W_{\gamma_1(x)}$ a $W_{\gamma_2(x)}$ takto:

$$x \in D \to W_{\gamma_1(x)} = A \cup \{f(\gamma_1(x), \gamma_2(x))\} \& W_{\gamma_2(x)} = B,$$
$$x \in C \to W_{\gamma_2(x)} = B \cup \{f(\gamma_1(x), \gamma_2(x))\} \& W_{\gamma_1(x)} = A.$$

  Pokud $x \notin C \cup D$ pak $f(\gamma_1(x), \gamma_2(x)) \notin A \cup B$. Pokud $x \in C$, tak $f(\gamma_1(x), \gamma_2(x)) \in A$. Pro $x \in D$ podobně. Složení f s $\gamma_{\{1,2\}}$ tedy dokazuje 1-úplnost.

Gödelova věta

„V rozumných teoriích je množina dokazatelných a vyvratitelných formulí neoddělitelná.“

D: Teorie T je axiomatizovatelná $\equiv$ množina dokazatelných formulí v T je RSM.

T:Gödel Jestliže teorie T 1. řádu je ZAS a je bezesporná:

- Množina dokazatalných formulí není rekurzivní.
- je-li T axiomatizovatelná, tak $\exists$ formule f nerozhodnutelná v T a nelze v T rozhodnout vlastní bezespornost.

Reprezentovatelnost

D: $f \in CRF$ je reprezentovatelná $\equiv f(x_{[1,n]}) = y \leftrightarrow \vdash F(x_{[1,n]}, y)$ a také $\vdash F(x_{[1,n]}, q) \& \vdash F(x_{[1,n]}, j) \to q = j$.

D: P predikát je diofantický $\equiv \exists p_1, p_2$ polynomy s.t. $\forall x_{[1,n]}$:

$$\exists y_{[1,k]} P(x_{[1,n]}) \leftrightarrow p_1(x_{[1,n]}, y_{[1,k]}) = p_2(x_{[1,n]}, y_{[1,k]}).$$

T:Matjasevič P diofantický $\leftrightarrow P$ rek. spočetný.

P: Zpětná implikace je těžká a neříká se, dopředná naopak jednoduchá – zkoušíme všechny možnosti.

T: $\forall f \in CRF, f$ je reprezentovatelná, dokonce $\exists$ formule, která ji reprezentuje ve všech teoriích.

P: Podle Matjaseviče.

R: Jsou-li A, B disj. RSM, pak $\exists G$ formule v σ_1 s.t. ...

`Verze 0.02, chyby zaručeny.`