Vyčíslitelnost

přednášející: Doc. RNDr. Antonín Kučera, CSc.

VERZE 1.0

Do formátu TEX převedl Ladislav Strojil

Připomínky, dotazy, opravy na emailu: Ladislav@Strojil.cz

Nejnovější verze k nalezení vždy na http://ladislav.strojil.cz/vycislitelnost.php

Obsah

1 Základní definice

1.1 Výpočetní model

Definice 1 (Turingův stroj).

Deterministický Turingův stroj (DTS) M s k-páskami, kde k je konstanta, je pětice

$$M = (Q, \Sigma, \delta, q_0, F) \tag{1}$$

$Q =$ *konečná množina stavů řídící jednotky*
$\Sigma =$ *konečná pásková abeceda*
$\delta : Q \times \Sigma^k \mapsto Q \times \Sigma^k \times \{L, N, R\}^k$ *je přechodová funkce (částečná)*
$q_0 \in Q =$ *počáteční stav*
$F \subseteq Q =$ *množina přijímajících stavů*

Věta 1 (Kleenova o normální formě). *Pro každé $k \geq 1$ existují*

- *ČRF Ψ_k $k+1$ proměnných*
- *PRP T_k $k+2$ proměnných*
- *PRF U jedné proměnné*
- *PRF s_k $k+1$ proměnných*

takové, že

1) *Ψ_k je univerzální funkcí pro třídu všech ČRF k proměnných.*

   $\Psi_k(e, x_1, \ldots, x_k)$ vyčísluje e-tou ČRF k proměnných.

   Navíc z odvození ČRF lze efektivně získat e a naopak z e lze efektivně získat odvození příslušné ČRF.

2) $\Psi_k(e, x_1, \ldots, x_k) \simeq U(\mu_y T_k(e, x_1, \ldots, x_k, y))$

3) *s_k jsou prosté funkce rostoucí ve všech proměnných.*

   $\lambda x_1, \ldots, x_k\ s_k(e, x_1, \ldots, x_k)$

4) $\Psi_{m+n}(e, z_1, \ldots, z_m, x_1, \ldots, x_n) \simeq \Psi_n(s_m(e, z_1, \ldots, z_m), x_1, \ldots, x_n)$

   $T_{m+n}(e, \vec{z}, \vec{x}) \equiv T_n(s_m(e, \vec{z}), \vec{x})$

5) $T_k(e, x_1, \ldots, x_k, y)$ & $T_k(e, x_1, \ldots, x_k, z) \Rightarrow y = z$

Důkaz. Oklikou přes Turingovy stroje (univerzální stroj).

Univerzální TS Y blok1 Y blok2 Δ blok3 $\times O_1 \times O_2 \ldots$ Y. Čísla kódujeme unárně (x jako $x+1$ čar).

Základní idea: bez dat Y M Y blok2 Δ blok3 $\times O_1 \times O_2 \ldots$ Y (očekáváme data).

Y $|| \ldots |\lambda|| \ldots |\lambda \ldots \lambda|| \ldots |M$

Konstrukce $s_m(e, x_1, \ldots, x_m)$. Chceme PRF. Zkontrolujeme, zda e po rozkódování obsahuje M, jestliže ne, je výsledkem nulová funkce. Jestliže ano, nejlevější výskyt M nahradíme $|| \ldots |\lambda|| \ldots |\lambda \ldots \lambda|| \ldots |M$. $\square$

Věta 2. *Predikát $\Psi_k(e, x_1, \ldots, x_k)\downarrow$ je rekurzivně spočetný, není rekurzivní, jeho negace není rekurzivně spočetná. Dále Ψ_k nelze rozšířit do ORF.*

Dokonce pokud α je ČRF, která je rozšířením Ψ_k, potom lze efektivně nalézt vstup $\vec{z}$ takový, že $\alpha(\vec{z})\uparrow$.

Důkaz. Z definice je zřejmé, že $\Psi_k(\ldots)\downarrow$ je rekurzivně spočetný predikát.

Stačí ukázat, že $\neg\Psi_k(\ldots)\downarrow$ není rekurzivně spočetný. Z toho přímo plyne, že $\Psi_k(\ldots)\downarrow$ není rekurzivní.

Bez újmy na obecnosti uvažujme $k = 1$. Použijeme Cantorovu diagonální metodu.

Kdyby $\Psi_1(\ldots)\downarrow$ byl rekurzivní, potom by $\neg\Psi_1(x, x)\downarrow$ byl také rekurzivní, tím spíše rekurzivně spočetný. Tedy pro nějakou ČRF φ by platilo $\neg\Psi_1(x, x)\downarrow \Leftrightarrow \varphi(x)\downarrow$. Vezmeme-li index funkce φ (označme jej x_0), dostáváme $\Psi_1(x, x)\downarrow \Leftrightarrow \Psi_1(x_0, x)\downarrow$, po dosazení $x = x_0$ dostáváme $\neg\Psi_1(x_0, x_0)\downarrow \Leftrightarrow \Psi_1(x_0, x_0)\downarrow$. Spor.

Pro důkaz zbytku tvrzení předpokládejme, že $h(e, x)$ je ORF rozšířením $\Psi_1(e, x)$. Potom $1 \dot{-} h(x, x)$ je ORF g. Nechť g má index x_0, tj. $g(x) \simeq \Psi_1(x_0, x)$. Protože g je ORF, pro všechna x platí $\Psi_1(x_0, x)\downarrow$, tím spíše $\Psi_1(x_0, x_0)\downarrow$. Tedy dostáváme $h(x_0, x_0) = \Psi_1(x_0, x_0)$. Což ovšem vede ke sporu: $1 \dot{-} \Psi_1(x_0, x_0) \simeq h(x_0, x_0) \simeq \Psi_1(x_0, x_0)$.

Dodatek: Ke každé ČRF $\varphi(e, x)$, která je rozšířením univerzální ČRF, lze efektivně najít x_0 takové, že $\varphi(x_0, x_0)\uparrow$. Důkaz je totožný. □

Myšlenka obsažená v předchozím důkazu je založená na Cantorově diagonální metodě. Spor na diagonále si vynutí divergenci, neboť rovnost funkcí je jenom podmíněná, tedy v případě divergence je vše v pořádku.

Univerzální funkce pro danou třídu funkcí buď nemůže patřit do této třídy, nebo nemůže být totální.

2 Rekurzivně spočetné množiny

Definice 2. *W_x (x-tá rekurzivně spočetná množina) $= dom(\varphi_x) = \{y : \varphi_x(y)\downarrow\}$*

Definice 3 (K). *$K = \{x : x \in W_x\} = \{x : \varphi_x(x)\downarrow\} = \{x : \Psi_1(x, x)\downarrow\}$*

Množina K souvisí s tzv. *halting problémem*, neboli problémem zastavení Turingova stroje. Platí o ní následující tvrzení.

Věta 3. *Množina K je rekurzivně spočetná, není rekurzivní, $\overline{K}$ není rekurzivně spočetná.*

Důkaz. K není rekurzivní, neboť $\overline{K}$ není rekurzivně spočetná. $\overline{K}$ není rekurzivně spočetná, neboť kdyby byla, měla by index x_0. Jednoduchou diagonalizací dostáváme $x_0 \in \overline{K} \Leftrightarrow x_0 \in W_{x_0} \Leftrightarrow x_0 \in K$. Spor. □

2.1 1-převeditelnost, m-převeditelnost

Definice 4. *Množina A je 1-převedilná na B (značíme $A \leq_1 B$), jestliže existuje prostá ORF f taková, že $x \in A \Leftrightarrow f(x) \in B$.*

Množina A je m-převedilná na B (značíme $A \leq_m B$), jestliže existuje ORF f (ne nutně prostá) taková, že $x \in A \Leftrightarrow f(x) \in B$.

Množina M je 1-úplná, jestliže M je rekurzivně spočetná a každá rekurzivně spočetná množina je na ni 1-převedilná.

Množina M je m-úplná, jestliže M je rekurzivně spočetná a každá rekurzivně spočetná množina je na ni m-převedilná.

Následující věta ukazuje, že *halting problem* je vzhledem k 1 a m-převoditelnosti nejtěžší mezi rekurzivně spočetnými problémy.

Věta 4. *K je 1-úplná.*

Důkaz. Mějme libovolnou rekurzivně spočetnou množinu W_x.

Mějme ČRF $\alpha(y,x,w)$, popisující x-tou rekurzivně spočetnou množinu. Tedy

$$\alpha(y,x,w)\downarrow \Leftrightarrow y \in W_x \Leftrightarrow \Psi_1(x,y)\downarrow \Leftrightarrow \varphi_x(y)\downarrow . \tag{2}$$

Provádíme obvyklý trik s fiktivní proměnnou, funkce α na hodnotě w nezáleží. Z s-m-n věty dostáváme:

$$\alpha(y,x,w) \simeq \Psi_3(a,y,x,w) \simeq \Psi_1(s_2(a,y,x),w) \simeq \varphi_{s_2(a,y,x)}(w). \tag{3}$$

Označme $h(y,x) = s_2(a,y,x)$ (s_2 je PRF, tím spíše ORF).

$$y \in W_x \Leftrightarrow \alpha(y,x,w)\downarrow \Leftrightarrow \varphi_{h(y,x)}(w)\downarrow \Leftrightarrow \varphi_{h(y,x)}(h(y,x))\downarrow \Leftrightarrow h(y,x) \in K \tag{4}$$

Zde jsme mohli za w dosadit $h(y,x)$, neboť hodnota α na w nezáleží! Tedy $W_x \leq_1 K$ pomocí funkce $\lambda y\, h(y,x)$. □

Lemma 1. *$K_0 = \{\langle y,x\rangle : y \in W_x\}$ je 1-úplná.*

Důkaz. Zřejmé. $K \leq_1 K_0$ a K je 1-úplná. □

Lemma 2 (Poznámky k 1-převeditelnosti).

1) *Relace $\leq_1$ a $\leq_m$ jsou tranzitivní, reflexivní.*

2) *$A \leq_1 B \Rightarrow A \leq_m B$*

3) *B rekurzivní, $A \leq_m B \Rightarrow A$ rekurzivní.*

4) *B rekurzivně spočetná, $A \leq_m B \Rightarrow A$ rekurzivně spočetná.*

Důkaz.

1) Zřejmé.

2) Zřejmé.

3) Složením funkce dokazující $\leq_m$ s procedurou, která rozhoduje o $x \in B$ dostaneme proceduru rozhodující o A. Dostáváme $c_A(x) = c_B(f(x))$.

4) Stejně.

□

Důsledek 1. *K a $\overline{K}$ jsou m-nesrovnatelné.*

Důkaz. Plyne z faktu, že K je rekurzivně spočetná, $\overline{K}$ není a z bodu 4 předchozího lemma. □

Definice 5 (Rekurzivní permutace). *Permutace na $\mathbb{N}$, která je ORF, se nazývá rekurzivní permutace.*

Definice 6 (Rekurzivní isomorfismus). *Množiny A a B jsou rekurzivně isomorfní, jestliže existuje rekurzivní permutace p taková, že $p(A) = B$. Značíme $A \equiv B$.*

Definice 7.

$A \equiv_1 B$, *jestliže* $A \leq_1 B$ & $B \leq_1 A$.

$A \equiv_m B$, *jestliže* $A \leq_m B$ & $B \leq_m A$.

Věta 5 (Myhill). $A \equiv B \Leftrightarrow A \equiv_1 B$

Důkaz. Jedná se o efektivní verzi Cantor-Bernsteinovy věty.

$\Rightarrow$ Triviální.

$\Leftarrow$ Z předpokladů máme dvě prosté ORF převádějící vzájemně A na B a opačně. Chceme sestrojit rekurzivní permutaci h takovou, že $h(A) = B$.

Plán: v krocích budeme generovat graf h tak, že v kroce n bude platit

$$\{0, \ldots, n\} \subseteq dom(h), \qquad \{0, \ldots, n\} \subseteq rng(h).$$

Z toho plyne, že h bude definovaná na celém $\mathbb{N}$ a bude na. Současně zajistíme, že h bude prostá.

Navíc budeme chtít, aby platilo $y \in A \Leftrightarrow h(y) \in B$, tedy aby h převáděla A na B.

Začneme v bodě 0 a položíme $h(0) = f(0)$. Rozlišíme následující případy:

1) $f(0) = 0$: vše je v pořádku, $h(0) = f(0) = 0$ a $0 \in A \Leftrightarrow 0 \in B$, pokračujeme dalším prvkem.

2) $f(0) \neq 0$: rozlišíme dva podpřípady

   a) $g(0) \neq 0$: vše v pořádku, definujeme $h(g(0)) = 0$.
   Tedy $0 \in dom(h) \cap rng(h)$.

   b) $g(0) = 0$: nemůžeme použít $h(g(0)) = 0$, protože v bodě 0 je již h definována. Najdeme tedy volný bod. Definujme $h(g(f(0))) = 0$. Určitě $g(f(0)) \neq 0$, protože g je prostá a $f(0) \neq 0$. Tímto jsme opět dostali bod 0 do definičního oboru h i oboru hodnot. Zároveň funkci h definujeme podle f a g, tedy převádí vzájemně A na B.

Indukční krok: nechť v kroce k je z první volný prvek. Všechna čísla menší jak z máme v $dom(h) \cap rng(h)$. Podíváme se, zda je $f(z)$ volný. Jestliže ano, položíme $h(z) = f(z)$. Jestliže $f(z)$ není volný, hledám zig-zag další volný. Maximálně z prvků je blokovaných. □

Důsledek 2. $K \equiv K_0$

Důkaz. Zřejmé, neboť $K \equiv_1 K_0$. □

Množin, které jsou ekvivalentní množině K, je však mnohem více. Ještě jich mnoho uvidíme v dalším textu. Ukažme si však nyní alespoň jednu takovou. Uvažme množinu $A = \{x : W_x \neq \emptyset\}$, tedy množinu programů, které konvergují alespoň na jednom vstupu.

A je rekurzivně spočetná, $A = \{x : \exists y, s \ (y \text{ patří do } W_x \text{ za } s \text{ kroků})\}$.

Ukážeme, že $A \equiv K$. Protože K je 1-úplná, zřejmě platí $A \leq_1 K$.

Pro opačný směr chceme prostou ORF h takovou, že

$$x \in W_x \Leftrightarrow x \in K \Leftrightarrow h(x) \in A \Leftrightarrow W_{h(x)} \neq \emptyset \tag{5}$$

Idea. Vytvoříme program, který čeká, zda x padne do K, jestliže ano, dá $\varphi_{h(x)}$ všude definované. Jinak nedělá nic.

$$\begin{aligned} \alpha(x,w){\downarrow} \quad &\Leftrightarrow \quad \varphi_x(x){\downarrow} && (6)\\ \alpha(x,w) \quad &\simeq \quad \varphi_{h(x)}(w) && (7) \end{aligned}$$

Tedy $x \in K$ znamená $W_{h(x)} = \mathbb{N}$. Naopak $x \notin K$ znamená $W_{h(x)} = \emptyset$.

Lemma 3. *Q je ORF, potom $\exists y Q$ je rekurzivně spočetný predikát.*

Důkaz. $\mu_y Q$ je ČRF, její definiční obor je $\exists y\, Q$. □

Věta 6. *Predikát $\exists y T_k(e, x_1, \ldots, x_k, y)$ je univerzálním RSP pro třídu RSP k proměnných.*

Důkaz. Z věty o normální formě. □

Důsledek 3. *Lze definovat index (Gödelovo číslo) rekurzivně spočetného predikátu.*

Věta 7. *Konjukce a disjunkce zachovávají rekurzivní spočetnost. Tedy průnik a sjednocení rekurzivně spočetných množin je rekurzivně spočetná množina. Stejně pro predikáty.*

Důkaz. Pro průnik spustíme oba programy současně a čekáme, až se oba zastaví. Pro sjednocení čekáme, až se zastaví alespoň jeden.

Formálně pro průnik.

$$\exists s_1 T_1(x,z,s_1) \;\&\; \exists s_2 T_1(y,z,s_2) \Leftrightarrow \exists w (T_1(x,z,(w)_{2,1}) \;\&\; T_1(y,z,(w)_{2,2})) \quad (8)$$

Uvedený predikát je rekurzivně spočetný, tedy má nějaký index.

$$\exists s T_3(e,x,y,z,s) \Leftrightarrow \exists s T_1(s_2(e,x,y),z,s)$$

□

Věta 8. *Omezená kvantifikace $(\forall y)_{y \leq t}$ a existenční kvantifikace (pro $k \geq 2$) zachovávají rekurzivní spočetnost.*

Důkaz. Neformálně: omezený kvantifikátor lze zkontrolovat for cyklem.

Formálně:

$$\begin{aligned} (\forall y)_{y \leq t}\; \exists s\; T_k(e, x_1, \ldots, x_{k-1}, y, s) \Leftrightarrow && (9)\\ \Leftrightarrow \exists \text{ kód } (k{+}1)\text{-tice } w\; (\forall y)_{y \leq t}\; T_k(e, x_1, \ldots, x_{k-1}, y, (w)_{t+1,y}) && (10) \end{aligned}$$

Část s omezeným kvantifikátorem je PRP, včetně existenčního kvantifikátoru je to rekurzivně spočetný predikát, tedy má nějaký index b.

$$\exists s\; T_{k+1}(b, e, x_1, \ldots, x_{k-1}, t, s) \Leftrightarrow \exists s\; T_k(s_1(b,e), x_1, \ldots, x_{k-1}, t, s). \quad (11)$$

Pro existenční kvantifikátor je situace ještě jednodušší. Kvantifikaci přes dvě proměnné převedeme na kvantifikaci přes jednu, kterou budeme považovat za kód dvojice a v predikátu potom vydělíme jednotlivé složky. Dostáváme predikát $k-1$ proměnných, proto požadavek na minimální velikost k!

$$\begin{aligned} \exists y \exists s\; T_k(e, x_1, \ldots, x_{k-1}, y, s) &\Leftrightarrow \exists w\; T_k(e, x_1, \ldots, x_{k-1}, (w)_{2,1}, (w)_{2,2}) && (12)\\ \Leftrightarrow \exists s\; T_k(d, e, x_1, \ldots, x_{k-1}, s) &\Leftrightarrow \exists s\; T_{k-1}(s_1(d,e), x_1, \ldots, x_{k-1}, s) && (13) \end{aligned}$$

□

Věta 9. *Nechť Q je RSP $k+1$ proměnných. Potom existuje ČRF φ k proměnných taková, že*

$$\varphi(x_1,\ldots,x_k)\downarrow \quad\Leftrightarrow\quad \exists y\ Q(x_1,\ldots,x_k,y) \tag{14}$$

$$\varphi(x_1,\ldots,x_k)\downarrow \quad\Rightarrow\quad Q(x_1,\ldots,x_k,\varphi(x_1,\ldots,x_k)) \tag{15}$$

Důkaz. Věta říká, že pro každý rekurzivně spočetný predikát existuje ČRF taková, že konverguje právě, když existuje y splňující predikát. Tato funkce navíc přímo vrací jedno takové y, pro které predikát platí. Tato φ je selektor na grafu Q.

Pro $k = 1$. Dáno x, hledáme nejmenší dvojici (y, s) takovou, že za s kroků ověříme, že $Q(x, y)$ (tj. program pro Q konverguje za s kroků). Pak vydáme y.

Obecně: univerzální vyjádření RSP $\exists s\, T_2(e, x, y, s)$, hledáme nejmenší w (kód dvojice) tak, že

$$\varphi(x) \simeq (\mu_w T_2(e, x, (w)_{2,1}, (w)_{2,2}))_{2,1}. \tag{16}$$

Funkce φ tedy vrací první složku z první dvojice, kterou najde (v uspořádání daném naším kódováním dvojic). □

Věta 10. *Funkce je ČRF $\Leftrightarrow$ má rekurzivně spočetný graf.*

Důkaz. Je-li φ ČRF, je její graf rekurzivně spočetný: $\langle x_1,\ldots,x_k,y\rangle \in$ Graf $\Leftrightarrow \exists s$ za s kroků program konverguje.

Opačně, je-li graf funkce φ rekurzivně spočetný, je selektor na něm ČRF, ale selektor na grafu funkce je přímo ona funkce. □

Věta 11 (Postova).
Množina M je rekurzivní právě, když M i $\overline{M}$ jsou rekurzivně spočetné.
Predikát Q je ORP právě, když Q i $\neg Q$ jsou RSP.

Důkaz. "$\Rightarrow$": Triviální.

"$\Leftarrow$": Intuitivně: $M = dom(P_1)$, $\overline{M} = dom(P_2)$. Pustíme oba programy současně a čekáme, který se zastaví. Zastaví se právě jeden.

Formálně: $(x \in M\ \&\ y = 1) \vee (x \in \overline{M}\ \&\ y = 0)$ je rekurzivně spočetný predikát, selektor na něm je ORF, která je charakteristickou funkcí pro M. □

Lemma 4. *Každá rekurzivně spočetná množina je oborem hodnot nějaké ČRF.*

Důkaz. Vytvoříme množinu dvojic $R = \{\langle z, y\rangle : z \in W_x\ \&\ y = z\}$. Množina R je rekurzivně spočetná, tedy má ČRF selektor φ, platí $dom(\varphi) = rng(\varphi) = W_x$.

Myšlenka toho důkazu je, že body, kde φ_x konverguje, vyneseme na diagonálu a vytvoříme selektor. Jeho definiční obor bude zároveň jeho oborem hodnot. □

Věta 12. *Každý obor hodnot ČRF je rekurzivně spočetná množina.*

Důkaz. Zkontruujeme pseudoinverzní funkci h k ČRF φ. □

2.2 Generování rekurzivně spočetných množin

Definice 8. *Funkce f je úseková, jestliže jejím definičním oborem je počáteční úsek $\mathbb{N}$ (nebo celé $\mathbb{N}$).*

Věta 13. *Rekurzivní množiny jsou právě obory hodnot rostoucích úsekových ČRF.*

Důkaz. Definujeme ČRF f, která bude rostoucí a úseková.

Začneme $f(0) \simeq \mu_x(x \in M)$.

Dále $f(n+1) \simeq \mu_y(y > f(n) \,\&\, y \in M)$

Opačně. Máme f rostoucí úsekovou ČRF. V případě, že je f konečná (tohle ale nejsme schopni efektivně rozpoznat!), víme jak, známe $D = dom(f)$ a tedy $rng(f)$ je rekurzivní.

V případě, že je f totální

$$y \in M = rng(f) \Leftrightarrow \exists x(f(x) = y)) \Leftrightarrow \exists x \leq y(f(x) = y) \tag{17}$$

Poslední ekvivalence platí, protože f je rostoucí a úseková. Tedy

$$y \in M \Leftrightarrow y \in \{f(0), \ldots, f(y)\}. \tag{18}$$

□

Věta 14. *Množina M je nekonečná a rekurzivní právě, když je oborem hodnot rostoucí ORF. Tedy M lze generovat prostou ORF.*

Důkaz. Důsledek následující věty. □

Věta 15. *Rekurzivně spočetné množiny jsou právě obory hodnot prostých úsekových ČRF.*

Důkaz. "$\Leftarrow$": Víme, obor hodnot ČRF je rekurzivně spočetná množina.

"$\Rightarrow$": Mějme ČRF φ.

Důkaz provedeme pomocí rekurzivní množiny

$$B = \{\langle x, s\rangle : \varphi(x)\downarrow \text{ přesně za } s \text{ kroků}\}. \tag{19}$$

Množinu B lze, protože je rekurzivní, generovat pomocí rostoucí úsekové ČRF h. Funkce h generuje dvojice, definujeme tedy $g(x) \simeq (h(x))_{2,1}$. Zřejmě g je prostá, úseková a ČRF (a generuje $dom(\varphi)$). □

Důsledek 4. *Každá nekonečná rekurzivně spočetná množina obsahuje nekonečnou rekurzivní podmnožinu.*

Důkaz. Mějme f, která prostě generuje M. Vyber rostoucí podposloupnost. Ta je rekurzivní.

$$g(0) = f(0) \tag{20}$$

$$g(n+1) = f(\mu_j(f(j) > g(n))) \tag{21}$$

Obor hodnot g je nekonečné rekurzivní množina a je podmnožinou M. □

Definice 9 (Imunní množina). *Množina M je imunní, jestliže M je nekonečná a neobsahuje nekonečnou rekurzivně spočetnou podmnožinu.*

Definice 10 (Simple množina). *Množina A je simple, jestliže A je rekurzivně spočetná a $\overline{A}$ je imunní.*

Lemma 5. *Existuje imunní množina.*

Důkaz. Nejprve neefektivní konstrukce. Budeme požadovat, aby M byla nekonečná a od každé nekonečné rekurzivně spočetné se lišila alespoň v jednom bodě. Naše strategie bude dát do M mnoho prvků a potom, kdykoliv je W_x nekonečná, vzít nějaký prvek z W_x, který je ještě volný, a ten dát do $\overline{M}$.

Krok s. Nějaký volný prvek dáme do M. Vezmu W_s, zeptám se, zda je W_s nekonečná (neefektivní krok!), pokud ano, vezmu nějaký volný prvek z W_s a dám jej do $\overline{M}$. V kroce s je blokováno nejvýše $2s+2$ prvků, tedy vždy můžeme volit.

Nyní si ukážeme efektivní konstrukci.

Problém je rozhodnout, zda W_x je nekonečná. Nebudeme se tedy ptát, zda je nekonečná, ale odstraníme všechny "hodně velké" množiny. V kroce s odstraníme množinu W_s, jestliže W_s obsahuje prvek větší jak $2s$.

$$Q(x,y) \Leftrightarrow y \in W_x \ \& \ y > 2x \tag{22}$$

Q je rekurzivně spočetná relace, její selektor φ je ČRF. Nechť $A = rng(\varphi)$, potom $\overline{A}$ je hledaná množina.

Ověření, že $\overline{A}$ splňuje požadované vlastnosti. Pro $j \geq x$ platí $\varphi(j) > 2x$ (pokud konverguje). Tedy příspěvky do $W_x, W_{x+1}, \ldots$ jsou všechny větší než $2x$. Do množiny $0, \ldots, 2x$ mohou tedy přispět jenom množiny $W_0, \ldots, W_{x-1}$. Máme tedy $2x+1$ čísel, šanci má jenom x, tedy nejméně $x+1$ z nich zůstane mimo A, tj. padnou do $\overline{A}$. Tedy $\overline{A}$ je nekonečná.

Ověřme druhou podmínku. Je-li W_x nekonečná, potom nemůže být podmnožinou $\overline{A}$. Dokonce platí $W_x \subseteq \overline{A} \Rightarrow W_x \subseteq \{0, \ldots, 2x\}$. □

Výše uvedená konstrukce dokonce dává konstrukci *simple* množiny množiny..

Definice 11.

$$\begin{aligned} Tot &= \{x : W_x = \mathbb{N}\} && (23)\\ Inf &= \{x : W_x \ \textit{nekonečná}\} && (24)\\ Fin &= \{x : W_x \ \textit{konečná}\} && (25) \end{aligned}$$

Věta 16. *Tot* $\equiv$ *Inf*

Důkaz. Stačí dokázat Tot $\leq_1$ Inf a Inf $\leq_1$ Tot.

Definujme $\alpha(x,w)\downarrow \Leftrightarrow \forall j = 0, \ldots, w \ \varphi_x(j)\downarrow$

Z s-m-n věty dostaneme $\alpha(x,w) \simeq \varphi_{h(x)}(w)$.

Jestliže $x \in Tot$, potom $W_{h(x)} = \mathbb{N}$. Naopak pro $x \notin Tot$ je $W_{h(x)}$ konečná.

Naopak, definujme $\beta(x,w)\downarrow \Leftrightarrow W_x$ obsahuje alespoň w prvků.

Z s-m-n věty dostaneme $\beta(x,w) \simeq \varphi_{g(x)}(w)$.

Jestliže $w \in Inf$, potom $g(x) \in Tot$. Naopak pro $w \notin Inf$ je $g(x) \notin Tot$. □

Definice 12 (Hyperimunní množina). *Množina B je hyperimunní, jestliže je nekonečná a neexistuje ORF f taková, že majorizuje množinu B.*

Definice 13. *Říkáme, že ORF f majorizuje nekonečnou množinu B, jestliže $B = \{x_0, x_1, x_2, \ldots\}$ je rostoucí seznam prvků B a platí $f(n) \geq x_n$.*

Definice 14 (Hypersimple množina). *Množina A je hypersimple, jestliže A je simple a $\overline{A}$ je hyperimunní.*

Lemma 6. *Hyperimunní množina je imunní.*

Důkaz. Sporem. Nechť hyperimunní A není imunní. Potom mám nekonečnou rekurzivně spočetnou množinu W_z, kterou A obsahuje.

Definujeme $D_{f(i)} = i$-tý bod W_z. Dostali jsme nekonečnou posloupnost konečných (jednobodových) množin, které všechny protínají A. Spor. □

Věta 17. *Množina A je hyperimunní $\Leftrightarrow$ A je nekonečná a neexistuje ORF f taková, že*

$$\forall n(D_{f(n)} \cap A \neq \emptyset) \;\&\; \forall i, j\; (i \neq j \;\Rightarrow D_{f(i)} \cap D_{f(j)} = \emptyset). \tag{26}$$

Zde D_x označuje x-tou konečnou množinu. Požadujeme tedy, aby neexistovala ORF vybírající prostým způsobem konečné množiny tak, aby všechny vybrané měly neprázdný průnik s A.

Důkaz. "$\Rightarrow$": Dokážeme, že negace pravé strany implikuje negaci levé strany. Tedy A je konečná nebo existuje ORF taková, že

$$\forall n(D_{f(n)} \cap A \neq \emptyset) \;\&\; \forall i, j\; (i \neq j \;\Rightarrow D_{f(i)} \cap D_{f(j)} = \emptyset). \tag{27}$$

Je-li A konečná, nemůže být hyperimunní. Existuje-li taková f, zvolme $g(n) = max(\bigcup_{j=0}^{n} D_{f(j)})$. Potom $g(n)$ majorizuje A. Zřejmé.

Opačnou implikaci budeme opět dokazovat jako převrácenou implikaci negací. Nechť A není hyperimunní, tedy máme g, která ji majorizuje. Položme

$$\begin{aligned} h(0) &= g(0) && (28)\\ h(n+1) &= g(h(n)+1) \qquad (\text{platí } g(h(n)+1) \geq x_{h(n)+1}) && (29) \end{aligned}$$

Zvolíme f následovně

$$\begin{aligned} D_{f(0)} &= \{0, \ldots, h(0)\} && (30)\\ D_{f(n+1)} &= \{h(n)+1, \ldots, h(n+1)\} && (31) \end{aligned}$$

Protože platí $g(h(n)+1) \geq x_{h(n)+1}$, což je $h(n)+2$ prvků, je každá $D_{f(n)}$ neprázdná. □

Věta 18 (Existence hypersimple množiny). *Existuje hypersimple množina.*

Důkaz. Pracný, pokud se provádí přímo diagonalizací. □

Věta 19 (Dekker). *Nechť množina A je rekurzivně spočetná, nerekurzivní, potom existuje B hypersimple.*

Důkaz. Množina A je zřejmě nekonečná. Existuje f prostá ORF generující A. Definujeme

$$B = \{x : \exists y(y > x \wedge f(y) < f(x))\} \tag{32}$$
$$\overline{B} = \{x : \forall y(y > x \Rightarrow f(y) > f(x))\} \tag{33}$$

Lze ukázat, že $\overline{B}$ je nekonečná (plyne to z faktu, že f generuje množinu A prostě).

Neexistuje ORF majorizující B. Kdyby ano, potom by A byla rekurzivní. Tj. g nechť je ORF majorizující $\overline{B}$.

$$x \in A \Leftrightarrow x \in rng(f) \Leftrightarrow x \in \{f(0), \ldots, f(g(x))\}. \tag{34}$$

Spor.

Ukažme ještě, že A a B jsou stejně složité ve smyslu vyčíslitelnosti, tedy že z jedné vypočítám druhou.

Mám-li B a potřebuji rozhodnout o $x \in A$, najdu prvních $x + 1$ prvků z $\overline{B}$, nechť poslední z nich je w.

$$x \in A \Leftrightarrow z \in \{f(0), \ldots, f(w)\} \tag{35}$$

Naopak, mám-li A a rozhoduji, zda $x \in B$.

$$x \in B \Leftrightarrow \exists y(y > x \wedge f(y) < f(x)) \tag{36}$$
$$x \in B \Leftrightarrow (\{0, \ldots, f(x)\} \setminus \{f(0), \ldots, f(x)\}) \cap A \neq \emptyset. \tag{37}$$

□

Věta 20 (Matijasevič). *Predikát P je rekurzině spočetný právě, když je diofantický, tj. existují 2 polynomy s přirozenými koeficienty p_1, p_2 takové, že*

$$P(y_1, \ldots, y_n) \Leftrightarrow \exists x_1, \ldots, x_k(p_1(\vec{y}, \vec{x}) = p_2(\vec{y}, \vec{x})) \tag{38}$$

3 Věty o rekurzi

Věta 21 (O rekurzi). *Jestliže f je ČRF jedné proměnné, potom existuje a takové, že $\varphi_{f(a)}(x) \simeq \varphi_a(x)$ pro všechna x.*

Důkaz.

$$\lambda z,x\ (\varphi_{f(s_1(z,z))}(x)) \simeq \Psi_2(e, z, x) \simeq \varphi_{s_1(e,z)}(x) \tag{39}$$

Dosadíme $z = e$ a dostáváme hledané $a = s_1(e, e)$. Platí totiž

$$\varphi_{f(s_1(e,e))}(x) \simeq \Psi_2(e, e, x) \simeq \varphi_{s_1(e,e)}(x). \tag{40}$$

□

Funkce f zobrazuje program na program. Bod a je pevný bodem zobrazení f. Jak vypadají programy a a $f(a)$? Který z nich počítá déle? Uvidíme, že program a počítá déle, než $f(a)$.

Co dělá program e na datech (z, x)? Počítá $\varphi_{f(s_1(z,z))}$, tj. vezme z a spočítá neprve $s_1(z, z)$, potom $f(s_1(z, z))$, který ale nemusí konvergovat. Jestliže $f(s_1(z, z))\downarrow$, spustí se na vstup x.

Co dělá program a? Program a vznikne jako $s_1(e, e)$. Mějme na vstupu x. Program a vezme e a přidá ho k x a spustí program e na (e, x). Co udělá program

e na těchto datech? Spočítá $s_1(e,e)$ (tedy spočítá a), potom $f(s_1(e,e)) = f(a)$ a spustí program $f(a)$ na x.

Program a tedy neprve spočítá a, potom spočítá $f(a)$ (pokud konverguje) a ten simuluje na vstupu x. Program a je tedy složitější než $f(a)$ a počítá déle.

Věta 22 (O generování pevných bodů). *Pro každou $f \in$ ČRF existuje prostá rostoucí PRF g taková, že platí:*

$$\varphi_{f(g(j))}(x) \simeq \varphi_{g(j)}(x) \tag{41}$$

Tedy g rostoucím způsobem generuje nekonečně mnoho pevných bodů funkce f.

Důkaz. $\varphi_{f(s_2(z,z,j))}(x) \simeq \psi(e,z,j,x) \simeq \varphi_{s_2(e,z,j)}(x)$.
Zvolme $g(j) = s_2(e,e,j)$. □

Věta 23 (??). *Nechť h je ČRF $n+1$ proměnných. Potom existuje číslo a takové, že a je indexem funkce $\lambda_{x_1,\ldots,x_n} h(a,x_1,\ldots,x_n)$, tedy platí $\varphi_a(x_1,\ldots,x_n) \simeq h(a,x_1,\ldots,x_n)$*

Důkaz. $h(v,x_1,\ldots,x_n) \simeq \psi_{n+1}(b,v,x_1,\ldots,x_n) \simeq \varphi_{s_1(b,v)}(x_1,\ldots,x_n)$
Následně aplikujeme větu o rekurzi na $s_1(b,v)$ v proměnné v a dostáváme hledané a. □

Věta 24 (Věta o rekurzi v závislosti na parametrech). *Jestliže f je ČRF $n+1$ proměnných, potom existuje PRF g n proměnných taková, že*
$\varphi_{h(g(y_1,\ldots,y_n),y_1,\ldots,y_n)}(x) \simeq \varphi_{g(y_1,\ldots,y_n)}(x)$

Důkaz.

$$\varphi_{h(s_{n+1}(z,z,y_1,\ldots,y_n),y_1,\ldots,y_n)}(x) \simeq \psi_{n+2}(e,z,y_1,\ldots,y_n,x) \simeq \varphi_{s_{n+1}(e,z,y_1,\ldots,y_n)}(x)$$

Zvolme $g(y_1,\ldots,y_n) = s_{n+1}(e,e,y_1,\ldots,y_n)$. □

Věta 25 (Rice). *Jestliže $\mathcal{A}$ je třída ČRF (jedné proměnné), která je netriviální, potom $A_{\mathcal{A}} = \{x : \varphi_x \in \mathcal{A}\}$ je nerekurzivní.*

Důkaz. Sporem. Nechť A je rekurzivní. Potom lze vytvořit ORF f takovou, že všechny prvky z A zobrazí na nějaký prvek $b \notin A$ a všechny prvky mimo A zobrazí na nějaký prvek $a \in A$. Podle věty o rekurzi existuje pevný bod f u_0, tedy platí:

$$\varphi_{u_0} = \varphi_{f(u_0)} \tag{42}$$

Tedy

$$u_0 \in A \Rightarrow f(u_0) = b \notin A \tag{43}$$

$$u_0 \notin A \Rightarrow f(u_0) = a \in A \tag{44}$$

To je ovšem spor, protože u_0 a $f(u_0)$ jsou indexy stejné funkce, a tedy buď obě čísla v A leží nebo obě neleží.

Pozor, nejedná se o třídu programů, ale třídu funkcí. Tedy i pro jednoprvkovou $\mathcal{A}$ bude $A_{\mathcal{A}}$ nekonečná a nerekurzivní (každá funkce je vyčíslovaná nekonečně mnoha programy a rozhodnout o jejich ekvivalenci je nelze efektivně). Viz následující důsledek. □

Důsledek 5. *Nechť $\mathcal{A} = \{\varphi_e\}$, potom $A = \{x : \varphi_x = \varphi_e\}$ je nerekurzivní. Rozhodnout o rovnosti funkcí vyčíslovaných dvěma programy nelze algoritmicky.*

4 Produktivní a kreativní množiny

Definice 15 (Produktivní množina). *Množina B je* produktivní, *jestliže existuje ČRF φ taková, že $W_x \subseteq B \Rightarrow \varphi(x)\downarrow\ \&\ \varphi(x) \in B \setminus W_x$*

Definice 16 (Kreativní množina). *Množina A je* kreativní, *jestliže A je rekurzivně spočetná a $\overline{A}$ je produktivní.*

Věta 26 (O produktivní funkci). *Každá produktivní množina má produktivní funkci, která je ORF.*

Důkaz. Mějme nějakou ČRF f produktivní pro B.

$$W_{g(y)} = \begin{cases} W_y & \text{jestliže } f(g(y))\downarrow \\ \\ \emptyset & \text{jestliže } f(g(y))\uparrow \end{cases}$$

$f(g(y))$ nemůže divergovat, protože potom by $W_{g(y)}$ bylo rovno prázdné množině, která je ale triviálně podmnožinou B. Tedy by $f(g(y))$ muselo konvergovat a vracet prvek mimo B. Což by byl spor.

$f(g(y))$ tedy konverguje a $W_g(y) = W_y$, tedy pokud $W_y \subseteq B$, potom také $W_{g(y)} \subseteq B$ a tedy $f(g(y))$ musí konvergovat a vracet prvek mimo $W_{g(y)}$ (což je rovno W_y), tedy nový prvek $f(g(y)) \in B \setminus W_y$.

Konstrukci g provedeme pomocí věty o rekurzi. Mějme pomocnou ORF h takovou, že platí

$$W_{h(x,y)} = \begin{cases} W_y & \text{jestliže } f(x)\downarrow \\ \\ \emptyset & \text{jestliže } f(x)\uparrow \end{cases} \tag{45}$$

Takovou h získáme pomocí s-m-n věty následovně.

$$\alpha(x,y,w)\downarrow \Leftrightarrow f(x)\downarrow\ \&\ w \in W_y \tag{46}$$

Aplikací s-m-n věty dostaneme h. Nyní použijeme větu o rekurzi.

$$\exists \text{ PRF } g : W_{g(y)} = W_{h(g(y),y)} = \begin{cases} W_y & \text{jestliže } f(g(y))\downarrow \\ \\ \emptyset & \text{jestliže } f(g(y))\uparrow \end{cases} \tag{47}$$

□

Věta 27. *Každá produktivní množina obsahuje nekonečnou rekursivně spočetnou množinu.*

Důkaz. Neformálně. Mějme množinu A a její produktivní funkci f. Začneme s $W_{z_0} = \emptyset$ a aplikujeme f. Dostáváme první prvek $f(z_0) \in A$. $W_{z_1} = \{f(z_0)\}$ atd. □

Důsledek 6. *Produktivní množiny nejsou imunní, imunní nejsou produktivní.*

Věta 28 (O rekurzivní permutaci). *Každá produktivní množina má produktivní funkci, která je rekurzivní permutací, tj. je prostá a na.*

Důkaz. Mějme funkci f produktivní pro množinu A.

Dvě strategie, jedna pro *na* a jedna pro *prostá*.

na:

Snadno nalezneme nekonečnou rekurzivní množinu M takovou, že $x \in M \Rightarrow W_x = \mathbb{N}$ a tedy jistě $x \in M \Rightarrow W_x \nsubseteq A$.

Definujeme

$$g(x) = \begin{cases} f(x) & x \notin M \\ j & x \in M \ \&\ x \text{ je } j\text{-tým prvkem } M. \end{cases} \tag{48}$$

Takto definovaná g je jistě produktivní ($W_x \subseteq A \Rightarrow x \notin M$ a tedy platí $g(x) = f(x)$) a na (M je nekonečná).

prostá:

$$h(0) = f(0) \tag{49}$$

$$h(n+1) = \begin{cases} f(n+1) & f(n+1) \notin \{h(0), \ldots, h(n)\} \\ ? & f(n+1) \in \{h(0), \ldots, h(n)\} \end{cases} \tag{50}$$

V případě, že je $f(n+1)$ již blokovaná, přidáme k W_{n+1} prvek $f(n+1)$ a aplikujeme na index této množiny funkci f. V případě, že platilo $W_{n+1} \subseteq A$, dostáváme iterací tohoto postupu prostou posloupnost prvků, z nichž maximálně n je blokovaných. První neblokovaný zvolíme jako $h(n+1)$. V případě, že opakováním nedostaneme neblokovaný prvek, muselo platit $W_{n+1} \nsubseteq A$, tedy můžeme volit libovolně (ale prostě).

Spojením těchto dvou strategií dostáváme funkci, která je na a prostá. □

Věta 29 (O ekvivalenci pojmů). *A je kreativní $\Leftrightarrow$ A je 1-úplná $\Leftrightarrow$ A je m-úplná.*

Důkaz. Plyne přímo z následující věty. □

Věta 30 (O ekvivalenci pojmů II). *B je produktivní $\Leftrightarrow \overline{K} \leq_1 B \Leftrightarrow \bar{K} \leq_m B$*

Důkaz. $2 \Rightarrow 3$: triviální

$3 \Rightarrow 1$:

Lemma 7. *Jestliže množina C je produktivní a $C \leq_m B$, potom i B je produktivní. Produktivita se tedy zachovává směrem vzhůru při $\leq_m$.*

Důkaz. Neformálně: nechť $W_x \subseteq B$, hledáme nový bod mimo W_x. Vezmeme vzor W_x při f, kde h je funkce dokazující $\leq_m$.

Platí $h^{-1}(W_x) \subseteq C$, protože h musí převádět C na B. Tedy můžeme na index množiny $h^{-1}(W_x)$ aplikovat funkci f, která je produktivní pro C. Dostáváme bod mimo $h^{-1}(W_x)$ a tedy jeho obraz při h musí padnout mimo W_x.

Formálně: Existuje ORF g taková, že složení $h \circ f \circ g$ je hledaná produktivní funkce pro B. (Funkce g vrací index množiny $h^{-1}(W_x)$.) $W_{g(x)} = h^{-1}(W_x) = \{y : h(y) \in W_x\}$ (g ze s-m-n věty)

$$W_x \subseteq B \Rightarrow W_{g(x)} \subseteq C \Rightarrow f(g(x)) \in C \setminus W_{g(x)} \Rightarrow hfg(x) \in B \setminus W_x \tag{51}$$

□

Protože $\overline{K}$ je produktivní, je i B dle předchozího lemma produktivní.

$1 \Rightarrow 2$: (B produktivní $\Rightarrow \overline{K} \leq_1 B$) Cíl: prostá ORF g taková, že

$$W_{g(x)} = \begin{cases} \{f(g(x))\} & x \in K \\ \emptyset & x \notin K \end{cases} \tag{52}$$

Potom platí:

$$x \in \overline{K} \quad \Rightarrow \quad W_{g(x)} = \emptyset \subseteq B \Rightarrow fg(x) \in B \setminus W_{g(x)} \Rightarrow fg(x) \in B \tag{53}$$

$$x \in K \quad \Rightarrow \quad W_{g(x)} = \{f(g(x))\} \tag{54}$$

Situace $f(g(x)) \in B$ nemůže nastat, protože potom by

$$W_{g(x)} \subseteq B \Rightarrow f(g(x)) \in B \setminus W_{g(x)}, \tag{55}$$

ale protože platí $W_{g(x)} = \{f(g(x))\}$, muselo by platit $f(g(x)) \in B \setminus \{f(g(x))\}$, což nelze. Proto musí platit $f(g(x)) \in \overline{B}$.

Tedy $h = f \circ g$ 1-převádí $\overline{K}$ do B.

Pro pořádek ukážeme konstrukci g. Pomocí s-m-n věty a věty o rekurzi.

$$W_{\alpha(x,y)} = \begin{cases} \{f(y)\} & x \in K \\ \emptyset & x \notin K \end{cases} \tag{56}$$

Potřebné α dostaneme pomocí s-m-n věty následovně.

$$\beta(x, y, w)\downarrow \Leftrightarrow \; y \in K \;\&\; w = f(y) \tag{57}$$

Nyní použijeme větu o rekurzi.

$$W_{g(x)} = W_{\alpha(x,g(x))} = \begin{cases} \{f(g(x))\} & x \in K \\ \emptyset & x \notin K \end{cases} \tag{58}$$

□

Definice 17 (Úplně produktivní množina). *Množinu A nazveme* úplně produktivní *množinou, když existuje ORF f taková, že*

$$f(x) \in A \setminus W_x \text{ nebo } f(x) \in W_x \setminus A \tag{59}$$

Lemma 8. *Úplná produktivita implikuje produktivitu.*

Důkaz. Zřejmé. Jestliže platí $W_x \subseteq A$, potom $W_x \setminus A = \emptyset$ a tedy musí nastat případ $f(x) \in A \setminus W_x$, což dokazuje produktivitu A. □

Věta 31 (O úplné produktivitě). *A je produktivní $\Leftrightarrow$ A je úplně produktivní.*

Důkaz. Produktivita se zachovává při $\leq_m$ a $\leq_1$. Stejně tak se zachovává úplná produktivita (důkaz je totožný).

$\overline{K}$ je úplně produktivní (a to dokonce při identické funkci - snadno se ověří, že $(x \in \overline{K} \setminus W_x) \vee (x \in W_x \setminus \overline{K})$. Zbytek je zřejmý. □

Důsledek 7. *Protože $\overline{K} \leq_m Tot = \{x : \varphi_x \text{ totální}\} = \{x : W_x = \mathbb{N}\}$, platí Tot je produktivní.*

5 Dvojice množin

Definice 18 (Rekurzivní neoddělitelnost). *Dvojice množin A, B ($A \cap B = \emptyset$) je rekurzivně neoddělitelná, jestliže neexistuje rekurzivní množina M taková, že*

$$A \subseteq M, M \cap B = \emptyset \text{ (tj. } B \subseteq \overline{M}) \tag{60}$$

Definice 19 (Efektivní neoddělitelnost). *Dvojice množin A, B ($A \cap B = \emptyset$) je efektivně neoddělitelná, jestliže existuje ČRF φ taková, že*

$$\left.\begin{array}{r} A \subseteq W_x \\ B \subseteq W_y \\ W_x \cap W_y = \emptyset \end{array}\right\} \Rightarrow \varphi(x,y)\downarrow \ \& \ \varphi(x,y) \notin W_x \cup W_y \tag{61}$$

Jinými slovy, z indexů aproximace A a B efektivně naleznu další bod, který leží mimo tuto aproximaci.

Lemma 9. *Efektivní neoddělitelnost je silnější než rekurzivní neoddělitelnost*

Důkaz. Sporem. Zvolme $W_x = M$ a $W_y = \overline{M}$, kde M je rekurzivní množina vyvracející rekurzivní neoddělitelnost. Funkce dokazující efektivní neoddělitelnost by musela nelézt bod mimo $M \cup \overline{M}$, což nelze. □

Lemma 10. *Existuje dvojice rekurzivně spočetných disjunktních množin A, B taková, že A, B jsou rekurzivně neoddělitelné, ale nejsou efektivně neoddělitelné.*

Důkaz. Těžký. □

Věta 32 (Existence efektivně neoddělitelné dvojice). *Existují disjunktní rekurzivně spočetné množiny A a B, které jsou efektivně neoddělitelné.*

Důkaz. Definujeme:

$$A = \{x : \varphi_x(x) \simeq 0\} \qquad B = \{x : \varphi_x(x) \simeq 1\} \tag{62}$$

A a B jsou zřejmě disjunktní a rekurzivně spočetné. Podle s-m-n věty existuje PRF α taková, že

$$\varphi_{\alpha(x,y)}(w) \simeq \begin{cases} 1 & w \text{ padne dříve do } W_x \text{ než do } W_y \\ 0 & w \text{ padne dříve do } W_y \text{ než do } W_x \\ \uparrow & w \notin W_x \cup W_y \end{cases} \tag{63}$$

Prostou diagonalizací nalezneme bod, na kterém musí $\varphi_{\alpha(x,y)}$ divergovat, protože jinak bychom došli ke sporu. Divergence α ale znamená, že daný bod leží mimo $W_x \cup W_y$.

Formálně. Co udělá $\varphi_{\alpha(x,y)}(\alpha(x,y))$? Kdyby $\alpha(x,y)$ padlo do W_x, potom zřejmě padne dříve do W_x než do W_y, $\varphi_{\alpha(x,y)}(\alpha(x,y))$ by zakonvergovalo a vrátilo 1 a tedy by muselo $\alpha(x,y)$ padnout do B. To nelze. Symetricky se ukáže, že $\alpha(x,y)$ nemůže padnout do W_y. Tedy padne mimo tyto dvě množiny. □

Definice 20 (1-úplnost dvojic). *Disjunktní dvojice rekurzivně spočetných množin A, B je 1-úplná, jestliže pro libovolnou disjunktní dvojici rekurzivně spočetných množin C, D existuje prostá ORF f taková, že*

$$x \in C \quad \Leftrightarrow \quad f(x) \in A \tag{64}$$
$$x \in D \quad \Leftrightarrow \quad f(x) \in B \tag{65}$$
$$x \notin C \cup D \quad \Leftrightarrow \quad f(x) \notin A \cup B \tag{66}$$

Značíme $(C, D) \leq_1 (A, B)$.

Věta 33 (Dvojná forma věty o rekurzi). *Pro libovolné ORF f, g existují m a n takové, že*

$$\varphi_m = \varphi_{f(m,n)} \qquad \varphi_n = \varphi_{g(m,n)} \tag{67}$$

Obecnější znění: pro libovolné ORF f, g obě $k+2$ proměnných existují PFR ω_1, ω_2 obě k proměnných takové, že

$$\varphi_{\omega_1(y_1,\ldots,y_k)} = \varphi_{f(\omega_1(y_1,\ldots,y_k),\omega_2(y_1,\ldots,y_k),y_1,\ldots,y_k)} \tag{68}$$
$$\varphi_{\omega_2(y_1,\ldots,y_k)} = \varphi_{g(\omega_1(y_1,\ldots,y_k),\omega_2(y_1,\ldots,y_k),y_1,\ldots,y_k)} \tag{69}$$

Důkaz. Mějme $\varphi_{f(x,y)}$, pomocí věty o rekurzi dostaneme funkci α takovou, že $\varphi_{f(\alpha(y),y)} = \varphi\alpha(y)$. Vezmeme $\varphi_{g(\alpha(y),y)}$, aplikujeme na g větu o rekurzi a dostáváme n takové, že $\varphi_n = \varphi_{g(\alpha(n),n)}$. Nyní stačí volit $m = \alpha(n)$.

Jinými slovy, nalezneme funkci α, která nám bude počítat pevné body v závilosti na druhé proměnné. Potom opětovnou aplikací věty o rekurzi získáme pevný bod této funkce. Jako m volíme hodnotu α v pevném bodě. □

Věta 34. 1*-úplné dvojice rekurzivně spočetných množin jsou právě efektivně neoddělitelné dvojice rekurzivně spočetných množin.*

Důkaz. 1-úplnost $\Rightarrow$ efektivní neoddělitelnost

Mějme (A, B) efektivně neoddělitelné (s funkcí f, která to dokazuje), (C, D) 1-úplná, tedy platí $(A, B) \leq_1 (C, D)$ (via h). Vezmeme vzory W_x a W_y při h, aplikujeme f a opět aplikujeme h.

efektivní neoddělitelnost $\Rightarrow$ 1-úplnost

Nechť (A, B) jsou efektivě neoddělitelné, tj. existuje ČRF f, která to dokazuje. Budeme hledat dvojici ORF funkcí ω_1, ω_2 takové, že

$$W_{\omega_1(x)} = \begin{cases} A \cup \{f(\omega_1(x), \omega_2(x))\} & x \in D \\ A & x \notin D \end{cases} \tag{70}$$

$$W_{\omega_2(x)} = \begin{cases} B \cup \{f(\omega_1(x), \omega_2(x))\} & x \in C \\ B & x \notin C \end{cases} \tag{71}$$

Snadno se nahlédne, že potom platí:

$$x \notin C \cup D \Rightarrow \left.\begin{matrix} W_{\omega_1(x)=A} \\ W_{\omega_2(x)=B} \end{matrix}\right\} \Rightarrow f(\omega_1(x), \omega_2(x)) \notin A \cup B \tag{72}$$

$$x \in C \Rightarrow x \notin D \Rightarrow \begin{matrix} W_{\omega_1(x)=A} \\ W_{\omega_2(x)=B\cup\{f(\omega_1(x),\omega_2(x))\}} \end{matrix} \tag{73}$$

Kdyby $f(\omega_1(x), \omega_2(x)) \notin A$, potom by $W_{\omega_1(x)}, W_{\omega_2(x)}$ byly korektní nadobaly množin A a B, tedy by funkce f na jejich indexech musela vracet nový bod, tj.

$$f(\omega_1(x), \omega_2(x)) \notin W_{\omega_1(x)} \cup W_{\omega_2(x)}, \tag{74}$$

ale to je spor, protože $f(\omega_1(x), \omega_2(x)) \in W_{\omega_2(x)}$. Tedy platí $f(\omega_1(x), \omega_2(x)) \in A$.

Analogicky se ukáže případ $x \in D$.

Zbývá ukázat konstrukci funkcí ω_1 a ω_2. Ty dostaneme pomocí dvojné formy věty o rekurzi.

$$W_{\alpha(y_1,y_2,x)} = \begin{cases} A \cup \{f(y_1,y_2)\} & x \in D \\ A & x \notin D \end{cases} \tag{75}$$

$$W_{\beta(y_1,y_2,x)} = \begin{cases} B \cup \{f(y_1,y_2)\} & x \in C \\ B & x \notin C \end{cases} \tag{76}$$

□

6 Gödelovy věty

Věta 35 (Gödelova věta o neúplnosti - 1. část). *V rozumných teoriích je množina dokazatelných a vyvratitelných formulí efektivně neoddělitelná dvojice.*

Definice 21 (Základní aritmetická síla). *Jazyk prvního řádu:*
$\overline{0}$ *- numerál pro nulu*
$\overline{1}$ *- numerál pro jedničku (aby neexistoval jednoprvkový model)*
$+, \times$ *- funkční symboly*
konečně mnoho axiomů

Definice 22 (Axiomatizovatelnost). *Teorie T je axiomatizovatelná, jestliže množina dokazatelných formulí v T je rekurzivně spočetná.*

Věta 36 (Gödelova věta). *Jestliže teorie T 1. řádu má základní aritmetickou sílu a je bezesporná, pak*

1) *množina formulí dokazatelných v T není rekurzivní*

2) *je-li T navíc axiomatizovatelná, pak*

   a) *existuje uzavřená formule F taková, že F je nerozhodnutelná v T (tj. $T \nvdash F$, $T \nvdash \neg F$)*

   b) *v T nelze dokázat vlastní bezespornost (za nepatrně silnějších předpokladů o teorii T).*

7 Reprezentovatelnost ČRF v teoriích ZAS

Definice 23 (Reprezentovatelnost). *ČRF f je reprezentovatelná v teorii T, která má základní aritmetickou sílu, jestliže existuje formule F taková, že*

$$f(x_1, \ldots, x_n) \simeq y \ \Rightarrow \vdash_T F(\overline{x_1}, \ldots, \overline{x_n}, \overline{y}) \tag{77}$$

$$\vdash_T F(\alpha_1, \ldots, \alpha_n, \beta) \ \& \ \vdash_T F(\alpha_1, \ldots, \alpha_n, \gamma) \ \Rightarrow \beta = \gamma \tag{78}$$

Věta 37 (O reprezentovatelnosti). *Každá ČRF je reprezentovatelná v libovolné teorii ZAS, dokonce existuje pro každou ČRF formule, která ji reprezentuje ve všech teoriích ZAS současně, je to dokonce Σ_1-formule.*

Důkaz. Pomocí Matijasevičovy věty. □

Důsledek 8. *Jsou-li A a B disjunktní rekurzivně spočetné množiny, potom existuje Σ_1-formule G taková, že*

$$x \in A \quad \Rightarrow \quad \vdash_T G(\overline{x}) \tag{79}$$

$$x \in B \quad \Rightarrow \quad \vdash_T \neg G(\overline{x}) \tag{80}$$

Důkaz. Návod:

$$\varphi(x) \simeq \begin{cases} 1 & x \in A \\ 0 & x \in B \\ \uparrow & x \notin A \cup B \end{cases} \tag{81}$$

□

Důkaz. Nyní dokážeme Gödelovu větu. Vezmeme A, B rekurzivně spočetné, efektivně neoddělitelné. Mějme formuli G, která je popisuje ve smyslu předchozího lemmatu.

$$A_1 \;=\; \{x : \vdash_T G(\overline{x})\} \quad (A \subseteq A_1) \tag{82}$$

$$B_1 \;=\; \{x : \vdash_T \neg G(\overline{x})\} \quad (B \subseteq B_1) \tag{83}$$

Z bezespornosti plyne, že $A_1 \cap B_1 = \emptyset$, navíc ani jedna nemůže být rekurzívní, protože by separovala A, B a tedy vztah dokazatelnosti v T není rekurzivní.

Přidáme-li navíc předpoklad axiomatizovatelnosti T, jsou A_1, B_1 rekurzivně spočetné a tedy z předpokladu efektivní neoddělitelnosti A, B dostáváme, že lze efektivně nalézt bod $k \notin A_1 \cup B_1$. Číslo k je kódem formule, která není dokazatelná v T a od které není v T dokazatelná ani její negace.

Části $2b$, která patří spíše do matematické logiky, se zde nezabýváme. □

8 Numerace

Definice 24 (Numerace). *Mějme spočetnou třídu funkcí $\mathcal{F}$. Numerací rozumíme indexaci funkcí z $\mathcal{F}$, tj. $\{\varphi_i\}_i$.*

Definice 25 (Vlastnosti numerací).

- *Numerace je* vyčíslitelná, *jestliže existuje ČRF α taková, že platí*

  $\alpha(i,x) \simeq \varphi_i(x)$.

- *Numerace je* přípustná, *jestliže existuje ORF h taková, že*

  $\varphi_{h(i,j)} = \varphi_i \circ \varphi_j$

- *Numerace je* hlavní, *jestliže libovolná jiná numerace ČRF je na ni 1-převedilná, tj. existuje prostá ORF g: $\varkappa_i = \varphi_{g(i)}$.*

Lemma 11. *Lze ukázat, že je-li $\{\varphi_i\}_i$ vyčíslitelná, pak je následující ekvivatelní:*

1) je přípustná;

2) je hlavní;

3) platí pro ni s-m-n věta;

4) je rekurzivně isomorfní nějaké standardní numeraci ČRF vzniklé efektivním očíslováním programů.

Věta 38. *Nechť $\mathcal{F}$ je třída ČRF. Potom*

1) $\exists f \in \mathcal{F}\ \exists g \supseteq f \quad g \notin \mathcal{F}$

2) $\mathcal{F} \neq \emptyset$ a neobsahuje žádnou ORF

3) $f \in \mathcal{F}$, ale pro každé p $f \restriction p \notin \mathcal{F}$

Každá z těchto podmínek implikuje $\overline{K} \leq_1 G(\mathcal{F}) = \{x : \varphi_x \in \mathcal{F}\}$. Speciálně to znamená, že $G(\mathcal{F})$ není rekursivně spočetná.

Důkaz.

1) Máme $f \in \mathcal{F}$, máme g ČRF, $g \supseteq f, g \notin \mathcal{F}$. Chceme nalézt ORF h takovou, že

$$z \notin K \Rightarrow \varphi_{h(z)} = f \tag{84}$$
$$z \in K \Rightarrow \varphi_{h(z)} = g \tag{85}$$

Pomocí s-m-n věty:

$$\varphi_{h(z)}(x) \simeq y \Leftrightarrow (f(x) \simeq y) \vee (z \in K \ \&\ g(x) \simeq y) \tag{86}$$

Funkce h převádí $\overline{K}$ na $G(\mathcal{F})$.

Poznámka: $\varphi_{h(z)}$ je definovaná tak, že pro $z \notin K$ musí platit $f(x) \simeq y$, pro $z \in K$ bude rozšířena o body $g(x)$. Jedná se o korektní definici, protože z předpokladů je g rozšířením f, tedy nemůže dojít ke kolizi.

2) Mějme nějakou f z $\mathcal{F}$, která z předpokladu není ORF (pouze ČRF). Definujeme rekurzivně spočetnou relaci

$$P(z, x, y) \Leftrightarrow (f(x) \simeq y) \vee (z \in K \ \&\ y = 0) \tag{87}$$

Vezmeme selektor, tedy prostou ORF h.

$$z \notin K \quad \Rightarrow \quad \varphi_{h(z)} = f \tag{88}$$
$$z \in K \quad \Rightarrow \quad \varphi_{h(z)} \text{totální} \tag{89}$$

Opět platí, že h převádí $\overline{K}$ na $G(\mathcal{F})$.

Poznámka: zde vystupuje v roli g z předchozího bodu nulová funkce. Ta ale není rozšířením funkce f, tedy musíme postupovat opatrněji, nelze přímo definovat funkci $h(x)$ jako v předchozím bodě.

Místo toho použijeme graf relace (může obsahovat kolize, tedy dvě různá y pro jedno x (a to při $z \in K$)), na grafu vezmeme selektor, který existuje podle věty 9. V případě, že $z \in K$, bude tento selektor totální (protože nulová funkce je totální, ale nebude obecně roven nulové funkci). Totální funkce určitě padne mimo $\mathcal{F}$, protože $\mathcal{F}$ neobsahuje žádnou ORF. V případě $z \notin K$ bude selektor roven funkci f, tedy padne do $\mathcal{F}$.

3) Mějme $f \in \mathcal{F}$, s-m-n věta (prostá) ORF h.

$$\varphi_{h(z)}(x) \simeq y \Leftrightarrow f(x) \simeq y \ \& \ z \notin K_x \tag{90}$$

Poznámka: v případě, že $z \notin K$, je $\varphi_{h(z)} = f$ a tedy padne do $\mathcal{F}$. V případě, že $z \in K$, je $\varphi_{h(z)} = f \restriction p$ pro nějaké p a tedy $\varphi_{h(z)}$ nepadne do $\mathcal{F}$. Tedy $h(z)$ převádí $\overline{K}$ na $G(\mathcal{F})$.

□

Důsledek 9. *Tedy pokud platí, že $G(\mathcal{F})$ je rekurzivně spočetná, potom musí $\mathcal{F}$ s každou f obsahovat i všechna její rozšíření (plyne z podmínky 1) a pro každou f musí obsahovat nějaký její počáteční úsek (podmínka 3).*

9 Relativní vyčíslitelnost

Definice 26 (B-ČRF). *φ je B-ČRF, jestliže existuje B-odvození. A je B-rekurzivní, jestliže c_A je B-ORF. A je B-rekurzivně spočetná, jestliže A je definiční obor α, kde α je nějaká B-ČRF.*

Definice 27 (String). *String (řetízek) je konečná posloupnost nul a jedniček. Označení*

$$\sigma * \tau \quad \textit{konkatenace} \tag{91}$$
$$\sigma \subseteq \tau \quad \sigma \textit{ je prefixem } \tau \tag{92}$$
$$\sigma \subseteq B \quad \sigma \textit{ je prefixem } c_B \tag{93}$$

Definice 28 (Funkcionální vlastnost). *Rekurzivně spočetná množina Φ má* funkcionální vlastnost*, jestliže*

$$\langle \sigma, x, y \rangle \in \Phi \ \wedge \ \langle \overline{\sigma}, x, \overline{y} \rangle \in \Phi \ \wedge \ \sigma \subseteq \overline{\sigma} \Rightarrow y = \overline{y} \tag{94}$$

Definice 29 (Částečně rekurzivní funkcionál). *Částečně rekurzivní funkcionál Φ je rekurzivně spočetná množina s funkcionální vlastností. Částečně rekurzivní funkcionál určuje zobrazení (parciální):*

$$\Phi(\sigma)(x) \simeq y \quad \Leftrightarrow \quad \langle \sigma, x, y \rangle \in \Phi \tag{95}$$
$$\Phi(\tau)(x) \simeq y \quad \Leftrightarrow \quad \textit{pro nějaké } \sigma \subseteq \tau \ \Phi(\sigma)(x) \simeq y \tag{96}$$
$$\Phi(B)(x) \simeq y \quad \Leftrightarrow \quad \textit{pro nějaké } \sigma \subseteq B \ \Phi(\sigma)(x) \simeq y \tag{97}$$

Lemma 12 (Regularizační funkce). *Existuje PRF ϱ taková, že pro libovolné z platí, že $W_{\varrho(z)}$ má funkcionální vlastnost a navíc platí, že je-li W_z již regulární, potom $W_z = W_{\varrho(z)}$.*

Důkaz. Idea. Efektivně generujeme W_z a každý prvek kontrolujeme, zda není v kolizi s nějakým již přidaným do $W_{\varrho(z)}$. □

Definice 30 (Numerace částečně rekurzivních funkcionálů).
$\Phi_i(B)(x) \simeq y \ \Leftrightarrow \ \exists \sigma \ \left(\langle \sigma, x, y \rangle \in W_{\varrho(i)} \wedge \sigma \subseteq B\right)$

Definice 31 (B-rekurzivita). *A je B-rekurzivní (značíme $A \leq_T B$), jestliže pro nějaké i platí $A = \Phi_i(B)$, tj. $\forall x \ c_A(x) = \Phi_i(B)(x)$*

A je B-rekursivně spočetná, jestliže $A = dom(\Phi_i(B))$.

Definice 32 (Značení).
$\Phi_{i,s}(\sigma)(x)$ *je výsledek za s kroků.*
$\Phi_{i,s}(\sigma)(x)\downarrow \Leftrightarrow \exists \tau, y\, \big(\langle \tau, x, y\rangle \in W_{\varrho(i),s} \wedge length(\tau) \leq s \wedge \tau \subseteq \sigma\big)$
$\Phi_{i,s}(\sigma)(x) \simeq y \;\Leftrightarrow\; \exists \tau\, \big(\langle \tau, x, y\rangle \in W_{\varrho(i),s} \wedge length(\tau) \leq s \wedge \tau \subseteq \sigma\big)$

Definice 33 (Numerace B-r.s.).
$W_z^B = dom(\Phi_z(B))$
$W_{z,s}^B = dom(\Phi_{z,s}(B))$

Věta 39. *$\Phi_z(B)(x_1,\ldots,x_n)$ je univerzální funkce pro třídu všech B-ČRF k proměnných a platí s-m-n věta. To znamená, že existují PRF $\overline{s_m}$ takové, že pro libovolnou B platí:*

$$\Phi_{\overline{s_m}(z,x_1,\ldots,x_m)}(B)(y_1,\ldots,y_n) \simeq \Phi_z(B)(x_1,\ldots,x_m,y_1,\ldots,y_n). \tag{98}$$

Důkaz. Důkaz pro jednoduchost jenom pro $m = n = 1$. Vypočítáme pomocnou rekurzivně spočetnou množinu

$$W = \{\langle \sigma, y, t\rangle : \langle \sigma, \langle x, y\rangle, t\rangle \in W_{\varrho(z)}\} \tag{99}$$

Tedy máme ČRF α

$$\alpha(z,x,w)\downarrow \Leftrightarrow\; w = \langle \sigma, y, t\rangle \wedge \langle \sigma, \langle x, y\rangle, t\rangle \in W_{\varrho(z)} \tag{100}$$

Zbývá ukázat:

$$\Phi_{\overline{s}_1(z,x)}(B)(y) \simeq \Phi_z(B)(x,y) \tag{101}$$

Nechť

$$\alpha(z,x,w) \simeq \varphi_{s_2(a,z,x)}(w) \tag{102}$$

Protože $W_{\varrho(z)}$ je regulární, je regulární i $W_{s_2(a,z,w)}$.

$$\overline{s}_1(z,x) = s_2(a,z,x) \tag{103}$$
$$W_{\varrho(s_2(a,z,x))} = W_{s_2(a,z,x)} \tag{104}$$

□

Jelikož s-m-n věta platí absolutně (stejnoměrně), dostáváme okamžitě platnost věty o rekurzi.

Věta 40 (O rekurzi II). *Nechť f je ČRF dvou proměnných, potom existuje PRF p taková, že $\forall B \forall x\, \Phi_{f(p(y),y)}(B)(x) \simeq \Phi_{p(y)}(B,x)$.*

10 Operace skoku

Definice 34 (Relativizovaný halting problem).

$$A' = \{x : \Phi_x(A)(x)\downarrow\} = \{x : x \in W_x^A\} \tag{105}$$

Dále induktivně definujeme

$$A^0 = A \tag{106}$$
$$A^{n+1} = (A^n)' \tag{107}$$

Věta 41. *1) A' je A-rekursivně spočetná*

2) $A' \not\leq_T A$ *(A' není A-rekurzivní)*

3) B *je* A*-rekursivně spočetná* $\Leftrightarrow$ $B \leq_1 A'$

4) A *je* B*-rekrusivně spočetná a* $B \leq_T C \Rightarrow A$ *je* C*-rekurzivně spočetná*

5) $A \leq_T B \Leftrightarrow A' \leq_1 B'$

6) $A \equiv_T B \Leftrightarrow A' \equiv_1 B'$

Důkaz. 1) z definice $A' = \{x : \Phi_x(A)(x) \downarrow\}$

2) Cantorova diagonální metoda

3) $\Leftarrow$ zřejmé

$\Rightarrow$ stejně jako u K

$$\Phi_a(A)(x, w) \downarrow \Leftrightarrow x \in B \ldots \qquad \text{(použití fiktivní proměnné)} \tag{108}$$

4) A je definičním oborem nějaké B-ČRF f, B je rekurzivní v C (via g), tedy s pomocí f a g dostáváme, že A je definičním oborem nějaké C-ČRF.

$$A = dom(\Phi_z(B)),\ B \leq_T C \Rightarrow A = dom(\Phi_{\text{něco}}(C)) \tag{109}$$

5) Nechť $A \leq_T B$. Potom z faktu, že A' je A-rekurzivně spočetná, a $A \leq_T B$ dostáváme, že A' je B-rekurzivně spočetná (podle bodu 4 této věty). A protože B' je úplná pro B-rekurzivně spočetné, dostáváme okamžitě $A' \leq_1 B'$.

Opačný směr. Mějmě $A' \leq_1 B'$. Zřejmě platí, že A i $\overline{A}$ jsou A-rekurzivní, tím spíše jsou A-rekurzivně spočetné. Tedy jsou obě 1-převedilné na A'. Ale dle předpokladu $A' \leq_1 B'$ a tedy $A \leq_1 B'$ i $\overline{A} \leq_1 B'$ a tedy dle relativizované Postovy věty je A B-rekurzivní.

6) Plyne okamžitě z bodu 5.

□

Důsledek 10. *Operace skoku je korektně definována na T-stupních. Tedy platí*

$$A \equiv_T B \Rightarrow A' \equiv_1 B' \quad (\Rightarrow A' \equiv_T B') \tag{110}$$

Lze tedy definovat skok stupně a jako stupeň obsahující skok libovolného prvku stupně a.

Věta 42 (Stejnoměrnost). *Existuje* z_0 *takové, že* $A' = W^A_{z_0}$ *pro všechna* A.

Důkaz.

$$W_{z_0} = \{\langle \sigma, x, y\rangle : \langle \sigma, x, y\rangle \in W_{\varrho(x)}\} \tag{111}$$

Protože $W_{\varrho(x)}$ je regulární, je i W_{z_0} je regulární a tedy $W_{z_0} = W_{\varrho(z_0)}$.

$$\begin{aligned} x \in A' &\Leftrightarrow \Phi_x(A)(x)\downarrow \Leftrightarrow \exists \sigma \subseteq A\ (\Phi_x(\sigma)(x)\downarrow) \Leftrightarrow \\ &\Leftrightarrow \exists \sigma \subseteq A \exists y\ (\Phi_x(\sigma)(x) \simeq y) \Leftrightarrow \\ &\Leftrightarrow \exists \sigma \subseteq A \exists y\ (\langle \sigma, x, y\rangle \in W_{\varrho(x)}) \Leftrightarrow \\ &\Leftrightarrow x \in W^A_{z_0} \end{aligned}$$

Tato složitě vypadající konstrukce je přirozeným zobecněním definice množiny $K = \{x : x \in W_x\}$. Akorát nyní konstruujeme množinu trojic obsahujících aproximaci orákula σ, proměnné x a y. Navíc musíme aplikovat regularizační funkci ϱ. Jinak zapsáno

$$W_{z_0} = \{w : w \in W_{\varrho((w)_{3,2})}\}. \tag{112}$$

□

Lemma 13. $\emptyset' \equiv K$

Důkaz. 1) K je rekurzivně spočetná a tedy $K \leq_1 \emptyset'$

2) $\emptyset' = \{x : x \in W_x^{\emptyset}\} \Rightarrow \emptyset'$ je rekurzivně spočetná v $\emptyset$, ale $\emptyset$ je rekurzivní a tedy $\emptyset'$ je absolutně rekurzivně spočetná a tedy je $\leq_1 K$, protože K je 1-úplná.

□

11 Limitní vyčíslitelnost

Definice 35 (Limitní vyčíslitelnost). *Množina M je limitně vyčíslitelná, jestliže existuje ORF h taková, že $M(x) \simeq \lim_s h(x,s)$.*

Funkce f je limitně vyčíslitelná, jestliže existuje ORF h taková, že $f(x) \simeq \lim_s h(x,s)$.

Věta 43. *M je rekurzivní v $\emptyset'$ právě, když M je limitně vyčíslitelná.*

Důkaz.

"$\Rightarrow$" $M \leq_T \emptyset' \Rightarrow \exists z\ M(x) = \Phi_z(\emptyset')(x)$. Tedy existuje program z, který z $\emptyset'$ počítá M. K tomu používá nerekurzivní orákulum, které ale můžeme efektivně generovat. Definujeme

$$h(x,s) = \begin{cases} \Phi_{z,s}(\emptyset'_s)(x) & \text{jestliže } \Phi_{z,s}(\emptyset'_s)(x)\downarrow \\ \\ 0 & \text{jinak} \end{cases} \tag{113}$$

Ukážeme, že $M(x) = \lim_s h(x,s)$. Je-li pro dané x $M(x)$ definováno, znamená to, že $\Phi_z(\emptyset')(x)\downarrow$ a tedy existuje počáteční úsek $\sigma \subseteq \emptyset'$, pro který platí $\Phi_z(\sigma)(x)\downarrow$.

Z $\sigma \subseteq \emptyset'$ plyne, že existuje t_0 takové, že $\forall t > t_0\ \ \emptyset'_{t_0}\restriction lh(\sigma) = \emptyset'_t\restriction lh(\sigma)$, tedy od určitého kroku t_0 počáteční úsek aproximace $\emptyset'$ o délce řetízku σ již pravdivě aproximuje $\emptyset'$.

Dále existuje t_1 takové, že $\Phi_{z,t_1}(\sigma)(x)\downarrow$, tedy vlastní výpočet se σ jako aproximací orákula konverguje za t_1 kroků.

Položme $s_0 = \max(t_0, t_1)$. Od kroku s_0 už nemůže dojít ke změně, neboť aproximace (v tuto chvíli již pravdivá) se již nemění a výpočet již zakonvergoval.

"$\Leftarrow$" Nechť $M(x)$ je limitně vyčíslitelná. Chceme s pomocí $\emptyset'$ vyčíslovat M. While cyklem najdeme nejmenší s_0 takové, že $\forall s \geq s_0\ h(x,s) = h(x,s_0)$. Jedná se o otázku rekurzivní v $\emptyset'$. Tedy máme μ_{s_0}($\emptyset'$-rekurzivní otázka). To je $\emptyset'$-ČRF, navíc $M(x)$ je totální, tedy tato minimalizace je $\emptyset'$-ORF. Z toho plyne, že $M \leq_T \emptyset'$. □

V předchozí větě bylo podstatné, že M je totální. Nyní tvrzení pro parciální funkce.

Věta 44.

1) *Jestliže f je ORF, potom $\lim_s f(x,s)$ je $\emptyset'$-ČRF.*

2) *Jestliže F je $\emptyset'$-ČRF, pak existuje ORF f taková, že $F(x) \simeq lim_s f(x,s)$.*
Přesněji: $\Phi_z(\emptyset')(x) \simeq \lim_s h(z,x,s)$ pro nějakou ORF h.

Důkaz. 1) Provedeme stejnou minimalizaci s jako v důkazu předchozí věty. Tentokrát ale nemusí minimalizace konvergovat.

2) V tomto případě použijeme stejnou ideu, ale musíme dát pozor, aby $F(x)\downarrow$. Naším cílem bude stabilizace celého výpočtu. Definujeme

$$h_0(z,x,s) = \begin{cases} \langle \sigma, x, y\rangle & \text{jestliže } \langle \sigma, x, y\rangle \in W_{\varrho(z),s} \ \&\ \sigma \subseteq \emptyset'_s \\ \\ s+1 & \text{jinak} \end{cases} \tag{114}$$

Nelze pouze vydělit y a stabilizovat y (výsledek výpočtu), je třeba stabilizovat celý výpočet, protože se může stát, že se mění aproximace orákula.

$$h(z,x,s) = \begin{cases} (h_0(x,z,s))_{3,3} & \text{jestliže } h_0(z,x,s) = h_0(z,x,s+1) \\ \\ s & \text{jinak} \end{cases} \tag{115}$$

$\lim_s h(z,x,s)$ existuje právě, když existuje $\lim_s h_0(z,x,s)$.

$F(x)\downarrow \ \Rightarrow\ \Phi_z(\sigma)(x)\downarrow$ pro nějaké $\sigma \subseteq \emptyset'$.

Tedy $\lim_s h(z,x,s) = F(x)$.

Jestliže existuje $\lim_s h(z,x,s)$, potom existuje $\lim_s h_0(z,x,s)$ a tedy máme nějaké $\langle \sigma, x, y\rangle$ a s_0 takové, že $\forall s \geq s_0$ je $\langle \sigma, x, y\rangle$ stabilní. Z toho plyne $\Phi_{z,s}(\sigma)(x) \simeq y \ \&\ \sigma \subseteq \emptyset'_s$. Jinými slovy $\langle \sigma, x, y\rangle$ a s_0 je limitní výpočet a $\Phi_z(\emptyset')(x)\downarrow \ \& = y$.

□

Ukažme si případ, který demonstruje, proč je potřeba trvat na stabilizaci celého výpočtu a nejen výsledku. Snadno vytvoříme program z takový, že

$$\Phi_z(A)(x)\downarrow \ \Leftrightarrow\ \emptyset' \setminus A \neq \emptyset \quad (\text{a } \Phi_z(A)(x)\downarrow \ \Rightarrow \text{výsledek} = 0) \tag{116}$$

Program pracuje tak, že postupně generuje $\emptyset'$ a pro každý nový prvek w se ptá, zda $w \in A$. V okamžiku, kdy nějaký takový nalezne, zastaví se a vydá $\emptyset$.

Je zřejmé, že $\Phi_z(\emptyset')(\dots)\uparrow$, zatímco $\forall s\ \Phi_z(\emptyset'_s)(\dots)\downarrow$. Plyne to z toho, že žádná aproximace $\emptyset'$ nemůže zajistit, aby program nenalezl prvek, který do této aproximace nepatří. Tedy neexistuje limitní výpočet, ale prostou stabilizací výsledku (vždy $\emptyset$) bychom dostali, že limita existuje, což by bylo špatně.

Věta 45. *Pro každé n existuje ORF h taková, že*

$$\Phi_z(\emptyset^{n+1})(x) \simeq \lim_{s_0} \dots \lim_{s_n} h(z,x,s_0,\dots,s_n), \tag{117}$$

kde všechny limity $s_1,\dots,s_n$ existují, limita pro s_0 nemusí.

12 Aritmetická hierarchie

12.1 Definice a základní vlastnosti

Definice 36 (Σ_n, Π_n prefix). *Σ_n (resp. Π_n) prefix je skupina kvantifikátorů, která má n skupin stejných kvantifikátorů, sousední skupiny se střídají a začíná $\exists$ (resp. $\forall$).*

Definice 37. *Predikát patří do třídy Σ_n (resp. Π_n), jestliže lze vyjádřit ve tvaru Σ_n prefix na rekurzivní základ (resp. Π_n prefix).*

Lemma 14. *$\Sigma_0 = \Pi_0$ jsou právě rekurzivní predikáty.*

Důkaz. Zřejmé. □

Definice 38. *Prefikát je* aritmetický, *jestliže jej lze vyjádřit pomocí spojek predikátového počtu nad rekurzivními relacemi.*

Lemma 15. *Aritmetické predikáty jsou právě všechny predikáty ve třídách $\Sigma_n, \Pi_n, n \in \mathbb{N}$.*

Důkaz. $\Leftarrow$ Zřejmé.
$\Rightarrow$ Úprava logického výrazu do prenexního tvaru. □

Lemma 16 (Základní vlastnosti).

1) $A \in \Sigma_n \Leftrightarrow \overline{A} \in \Pi_n$

2) $\Sigma_n \cup \Pi_n \subseteq \Sigma_m \cap \Pi_m$ pro $m > n$.

3) $A \leq_m B$ a $B \in \Sigma_n$ (resp. Π_n), potom A je Σ_n (resp. Π_n).

Důkaz.

1) Zřejmé.

2) Kvantifikací přes fiktivní proměnnou přidáme potřebný kvantifikátor buď na konec nebo na začátek.

3) Transformace převodní funkcí nezmění aritmetickou složitost.

□

Věta 46 (O numeraci, univerzálním predikátu). *Pro každou třídu Σ_n (resp. Π_n) pro $n \geq 1$ existuje univerzální Σ_n (resp. Π_n) predikát.*

Důkaz. Nejprve případ Σ_n, kde n je liché. Máme predikát tvaru $\exists\forall\ldots\exists$(rek). Kvantifikátory kromě posledního odřízneme. Dostáváme Σ_1 predikát, tj. rekurzivně spočetný predikát. Pro něj existuje univerzální predikát $\exists T_n(e, x, \ldots)$. Nyní vrátíme kvantifikátory $\exists\forall\ldots\exists T_n(e, x, \ldots)$.

Případ pro Σ_n a n sudé. Po odříznutí dostáváme $\forall$(rek), negací $\exists T_n$, opětovnou negací $\forall\neg T_n$.

Pro případ Π_n analogicky (obráceně). □

Důsledek 11. *Pro $n \geq 1$ platí $\Sigma_n \setminus \Pi_n \neq \emptyset$.*

Důkaz. Máme univerzální Σ_n predikát $U(e,x) \in \Sigma_n$. Kdyby $U(e,e) \in \Pi_n$, potom by $\neg U(e,e) \in \Sigma_n$, vezmeme jeho index a a dosadíme $e = a$. Dostáváme spor $(U(a,a) \Leftrightarrow \neg U(a,a))$, $U(e,e)$ tedy musí být mimo Π_n. $\square$

Věta 47 (O hierarchii).

1) A je rekurzivně spočetná v $\emptyset^{(n)} \Leftrightarrow A \in \Sigma_{n+1}$

2) $\emptyset^{n+1}$ je Σ_{n+1}-úplná

3) $B \leq_T \emptyset^{(n)} \Leftrightarrow B \in \Sigma_{n+1} \cap \Pi_{n+1}$

Důkaz.

1) Pro $n = 0$ to víme. Indukcí pro všechna n. Nechť $A \in \Sigma_{n+1}$, tedy A je tvaru $\exists(\Pi_n)$. Negace toho Π_n je Σ_n a dle indukčního předpokladu je tedy rekurzivně spočetná v $\emptyset^{(n-1)}$. Z toho plyne $\leq_1 \emptyset^{(n)} \Rightarrow \leq_T \emptyset^{(n)} \Rightarrow$ původní predikát (před negací) je $\leq_T \emptyset^{(n)}$. Dostáváme $\exists$(rekurzivní v $\emptyset^{(n)}$), což je rekurzivně spočetné v $\emptyset^{(n)}$.

   Nyní nechť A je rekurzivně spočetná v $\emptyset^{(n)}$, tedy A je definiční obor nějaké g, která je $\emptyset^{(n)}$-ČRF. Dle věty o limitní vyčíslitelnosti je $g \simeq \lim_s f(x,s)$, kde f je $\emptyset^{(n-1)}$-ORF.

   $x \in A \Leftrightarrow g(x)\downarrow \Leftrightarrow \exists s_0 \forall s \geq s_0 \ (f(x,s) = f(x,s_0))$

   Výraz v závorkách je rekurzivní v $\emptyset^{(n-1)}$ a tedy podle bodu 3 této věty patří do $\Sigma_n \cap \Pi_n$. Dostáváme tedy $\exists\forall\Pi_n$, což je $\exists\Pi_n$, tedy Σ_{n+1}.

2) Plyne z bodu 1.

3) Plyne z bodu 1 pomocí Postovy věty.

Poznámka: v důkazu bodu 1 se odvoláváme na bod 3, který naopak dokazujeme z bodu 1. Nejde ale o nekorektní důkaz, protože v bodě 1 použijeme platnost bodu 3 pro $n-1$ a důkaz stavíme induktivně, tedy platnost pro $m < n$ už máme zaručenu. $\square$

Věta 48 (O úplnosti). *Pro $n \geq 1$ je $\emptyset^{(n)}$ Σ_n-úplná*

Důkaz. Nechť M je Σ_n, potom M je $\emptyset^{(n-1)}$-rekurzivně spočetná a dle vlastnosti operace skoku je $\leq_1 \emptyset^{(n)}$. $\square$

12.2 Σ_2 a Π_2 úplné množiny

Věta 49 (Tot je Π_2-úplná). *Tot$= \{x : \varphi_x$ je totální$\}$ je Π_2-úplná.*

Důkaz. Tot je zřejmě Π_2. Mějmě $B \in \Pi_2$, tedy

$$x \in B \Leftrightarrow \forall y \exists s \ Q(x,y,s). \tag{118}$$

Chceme nalézt ORF f takovou, že

$$x \in B \Leftrightarrow f(x) \in Tot \Leftrightarrow \varphi_{f(x)} \text{ je totální} \tag{119}$$

Zkonstruujeme funkci, která bude pro y vracet s (Σ_1 svědka).

$$\alpha(x,y) \simeq \mu_s Q(x,y,s) \simeq \Psi_2(a,x,y) \simeq \Psi_1(s_1(a,x),y) \simeq \varphi_{f(x)}(y) \tag{120}$$

Je zřejmé, že $x \in B \Leftrightarrow f(x) \in$ Tot. $\square$

Σ_2-úplné množiny: $\emptyset^{(2)}$, Fin
Π_2-úplné množiny: $\overline{\emptyset^{(2)}}$, Tot, Inf

Věta 50 (Relativizace). *A je* $\Sigma^B_{n+1} \Leftrightarrow A$ *je rekurzivně spočetná v* $B^{(n)}$
$A \leq_T B^{(n)} \Leftrightarrow A \in \Sigma^B_{n+1} \cap \Pi^B_{n+1}$

Lemma 17. *Fin* $= \{x | W_x$ *je končená*$\}$ *je* Σ_2 *úplná.*

Důkaz. Množina je konečná, jestliže má horní závoru, tedy prvek, pro který platí, že všechny větší jsou mimo tuto množinu.

$$x \in Fin \Leftrightarrow \exists y \; \forall y' > y \; \forall s \; \neg(y' \in W_{x,s}) \tag{121}$$

Mějme libovolnou $A \in \Sigma_2$. Platí

$$x \in A \Leftrightarrow \exists z \; \forall y \; Q(x, z, y). \tag{122}$$

Definujeme

$$\alpha(x, z){\downarrow} \Leftrightarrow \forall j \leq z \; \exists y \; (\neg Q(x, z, y)). \tag{123}$$

Podle s-m-n věty:

$$\alpha(x, z) \simeq \varphi_{f(x)}(z) \tag{124}$$

$$x \in A \Rightarrow \exists z \; \forall z' > z \; \varphi_{f(x)}(z'){\uparrow} \tag{125}$$

a tedy $W_{f(x)}$ je konečný počáteční úsek.

$$x \notin A \Rightarrow \forall z \varphi_{f(x)}(z){\downarrow} \Rightarrow W_{f(x)} = \mathbb{N} \tag{126}$$

□