Kapitola 1

Státnice - Rekurzivní a rekurzivně spočetné množiny

1.1 Rekurzivně spočetné množiny

Definice (Rekurzivní a rekurzivně spočetná množina)

Charakteristická funkce množiny M označuje charakteristickou funkci predikátu náležení do množiny, tj. funkci $c_M(x)$, kde $c_M(x) =\downarrow 1$ pro $x \in M$ a $c_M(x) \downarrow= 0$ pro $x \notin M$.

Analogicky se definuje částečná charakteristická funkce množiny – $c_M(x) =\downarrow 1$ pro $x \in M$ a $c_M(x) \uparrow$ pro $x \notin M$.

Množina M je rekurzivní, je-li její charakteristická funkce obecně rekurzivní (každá char. fce je totální, takže ČRF by bylo totéž). Množina M je rekurzivně spočetná, jestliže je definičním oborem nějaké ČRF (neboli jestliže je její částečná char. funkce částečně rekurzivní).

Množina je rekurzivní, jestliže existuje program, který se na libovolném vstupu zastaví a rozhodne, zda do ní vstup patří. Množina je rekurzivně spočetná, jestliže existuje program, který se zastaví právě na jejích prvcích. Je-li množina rekurzivní, je i rekurzivně spočetná, opačně to neplatí.

Definice (dom, rng)

V následujícím dom značí definiční obor, rng obor hodnot.

Definice (x-tá rekurzivně spočetná množina)

$$W_x \ (x\text{-tá rekurzivně spočetná množina}) = dom(\varphi_x) = \{y : \varphi_x(y)\downarrow\}$$

Definice (K)

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

Množina K vlastně odpovídá halting problému. Platí o ní následující tvrzení.

Věta (Rekurzivní spočetnost K)

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.

1.2 1-převeditelnost, m-převeditelnost

Definice (1-převeditelnost, m-převeditelnost, 1-úplnost, m-úplnost)

- 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.

Věta (1-úplnost K)

K je 1-úplná. Tedy halting problem je vzhledem k 1 a m-převoditelnosti nejtěžší mezi rekurzivně spočetnými problémy.

Důkaz

Mějme libovolnou rekurzivně spočetnou množinu W_x.

Mějme ČRF $\alpha(y,x,w)$, popisující x-tou rekurzivně spočetnou množinu. Tedy $\alpha(y,x,w)\downarrow \Leftrightarrow y \in W_x \Leftrightarrow \Psi_1(x,y)\downarrow \Leftrightarrow \varphi_x(y)\downarrow$. w je tady fiktivní proměnná, funkce α na její hodnotě nezáleží. Z s-m-n věty dostáváme: $\alpha(y,x,w) \simeq \Psi_3(a,y,x,w) \simeq \Psi_1(s_2(a,y,x),w) \simeq \varphi_{s_2(a,y,x)}(w)$. Označme $h(y,x) = s_2(a,y,x)$ (s_2 je PRF, tím spíše ORF). $y \in W_x \Leftrightarrow \alpha(y,x,w)\downarrow \Leftrightarrow \varphi_{h(y,x)}(w)\downarrow \Leftrightarrow \varphi_{h(y,x)}(h(y,x))\downarrow \Leftrightarrow h(y,x) \in K$ 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 (K_0 je 1-úplná)

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

Důkaz

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

Lemma (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 $x \in A$. Dostáváme $c_A(x) = c_B(f(x))$.
4. Stejně.

Důsledek

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 (Rekurzivní permutace)

Permutace na $\mathbb{N}$, která je ORF, se nazývá rekurzivní permutace.

Definice (Rekurzivní isomorfismus)

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

Definice (1-ekvivalence a m-ekvivalence)

- $A \equiv_1 B$, jestliže $A \leq_1 B \wedge B \leq_1 A$.
- $A \equiv_m B$, jestliže $A \leq_m B \wedge B \leq_m A$.

Věta (Myhillova)

$$A \equiv B \Leftrightarrow A \equiv_1 B$$

Důkaz

Jedná se o vlastně o obdobu Cantor-Bernsteinovy věty.

$\Rightarrow$ Triviální.

$\Leftarrow$ Z předpokladů máme dvě prosté ORF f, g 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 kroku n bude platit $\{0, \ldots, n\} \subseteq dom(h), \{0, \ldots, n\} \subseteq rng(h)$.

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) $g(0) \neq 0$: 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 kroku k je z první volný prvek. Všechna čísla menší než 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 "cik-cak" další volný (podobně jako pro 0, maximálně z prvků je blokovaných, tj. maximálně po z iteracích tohoto postupu dojdu k volnému prvku).

Důsledek

$K \equiv K_0$.

Důkaz

Zřejmé, neboť $K \equiv_1 K_0$ (obě množiny jsou 1-úplné).

1.3 Rekurzivně spočetné predikáty

Lemma (ORF $\rightarrow$ RSP)

Je-li Q obecně rekurzivní predikát, potom $\exists y : Q$ je rekurzivně spočetný predikát.

Důkaz

$\mu_y Q$ je ČRF, její definiční obor je $\{\exists y : Q\}$.

Věta (Univerzální RSP)

Predikát $\exists y T_k(e, x_1, \ldots, x_k, y)$ je univerzálním RSP pro třídu RSP k proměnných, tj. lze definovat index (Gödelovo číslo) rekurzivně spočetného predikátu.

Důkaz

Z věty o normální formě – numerace ČRF nám dává numeraci predikátů.

Věta (Log. spojky a rek. spočetnost)

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 ($(w)_{2,1}$ znamená to, že w kóduje usp. dvojici a vybíráme z ní první prvek; to je PRF): $\exists s_1 T_k(a,\vec{x},w_1) \wedge \exists s_2 T_k(b,\vec{x},w_2) \Leftrightarrow \exists w(T_k(a,\vec{x},(w)_{2,1}) \wedge T_k(b,\vec{x},(w)_{2,2}))$. Uvedený predikát je rekurzivně spočetný, tedy má nějaký index, tj. ekvivalence pokračuje: $\exists w T_{k+2}(e,a,b,\vec{x},w) \Leftrightarrow \exists w T_k(s_2(e,a,b),\vec{x},w)$

Poznámka

Konjunkce a disjunkce tedy rek. spočetnost zachovávají, o negaci (tj. doplňku) to ale už samozřejmě neplatí.

Věta (Kvantifikace a rek. spočetnost)

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: $(\forall y)_{y\leq t}\ \exists s : T_k(e,x_1,\ldots,x_{k-1},y,s) \Leftrightarrow \exists$ kód $(t+1)$-tice w : $(\forall y)_{y\leq t}\ T_k(e,x_1,\ldots,x_{k-1},y,(w)_{t+1,y})$.

y můžeme zkoušet primitivní rekurzí, w minimalizací, dostáváme tedy rekurzivně spočetný predikát, který má nějaký index b, dále můžeme použít S-m-n větu. $\exists s : T_{k+1}(b,e,x_1,\ldots,x_{k-1},t,s) \Leftrightarrow \exists s : T_k(s_1(b,e),x_1,\ldots,x_{k-1},t,s)$.

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 (a použijeme opět S-m-n větu). Dostáváme predikát $k-1$ proměnných, proto je ve větě požadavek na minimální velikost $k \geq 2$.

$$\exists y : \exists s : T_k(e,x_1,\ldots,x_{k-1},y,s) \Leftrightarrow \exists w : T_k(e,x_1,\ldots,x_{k-1},(w)_{2,1},(w)_{2,2})$$

$$\Leftrightarrow \exists s : T_k(b,e,x_1,\ldots,x_{k-1},s) \Leftrightarrow \exists s : T_{k-1}(s_1(b,e),x_1,\ldots,x_{k-1},s)$$

Poznámka

Neomezená obecná kvantifikace $(\forall)$ rekurzivní spočetnost nezachovává.

Věta (O selektoru)

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

$$\varphi(x_1,\ldots,x_k)\downarrow \Leftrightarrow \exists y : Q(x_1,\ldots,x_k,y)$$

$$\varphi(x_1,\ldots,x_k)\downarrow \Rightarrow Q(x_1,\ldots,x_k,\varphi(x_1,\ldots,x_k))$$

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.

Důkaz

Dáno $\vec{x}$, hledáme nejmenší dvojici (y,s) takovou, že za s kroků ověříme, že $Q(\vec{x},y)$ (tj. program pro Q konverguje za s kroků). Pak vydáme y.

Obecně: univerzální vyjádření RSP $\exists s : T_{k+1}(e,\vec{x},y,s)$, hledáme nejmenší w (kód dvojice) takové, že $\varphi(\vec{x}) \simeq (\mu_w T_{k+1}(e,\vec{x},(w)_{2,1},(w)_{2,2}))_{2,1}$. Funkce φ vrací první složku z první dvojice, kterou najde (v uspořádání daném naším kódováním dvojic).

Věta (Vztah ČRF a RS grafů)

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

1.4 Generování rekurzivně spočetných množin

Lemma (Rek. spočetná množina je obor hodnot ČRF)

Každá rekurzivně spočetná množina je oborem hodnot nějaké ČRF.

Důkaz

Pro každou množinu W_x vytvoříme množinu dvojic $R = \{\langle y, y\rangle : y \in W_x\}$. 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 (ČRF odpovídá Rek. spočetným množinám)

Každý obor hodnot ČRF je rekurzivně spočetná množina.

Důkaz

Máme ČRF g a její obor hodnot. Zkonstruujeme pseudoinverzní funkci h k ČRF g, tj. funkci takovou, že $dom(h) = rng(g)$ a to tak, že vyrobíme RS predikát $Q(x, y) \Leftrightarrow g(x) \simeq y$ a to má ČRF selektor, který hledáme – h.

Definice (Úseková funkce)

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

Věta (Rek. množiny a úsekové ČRF)

Rekurzivní množiny jsou právě obory hodnot rostoucích úsekových ČRF.

Důkaz

$\Rightarrow$: Definujeme ČRF f, která bude rostoucí a úseková.

- Začneme $f(0) \simeq \mu_x(x \in M)$.
- Dále $f(n+1) \simeq \mu_y(y > f(n) \wedge y \in M)$

$\Leftarrow$: Máme f rostoucí úsekovou ČRF.

1. V případě, že je f má konečné dom (tohle ale nejsme schopni efektivně rozpoznat!), víme jak, známe $D = dom(f)$ a tedy $rng(f)$ je rekurzivní.
2. V případě, že je f je všude definovaná (totální): $y \in M = rng(f) \Leftrightarrow \exists x : (f(x) = y)) \Leftrightarrow \exists x \leq y : (f(x) = y)$ Poslední ekvivalence platí, protože f je rostoucí a úseková. Tedy $y \in M \Leftrightarrow y \in \{f(0), \ldots, f(y)\}$.

Věta (O generování)

Mějme nekonečnou množinu M. Potom:

- Množina M je rekurzivní, právě když M lze generovat rostoucí ORF.
- Množina M je rekurzivně spočetná, právě když M lze generovat prostou ORF.

Důkaz

Důsledek předchozí, resp. následující věty.

Věta (Rek. spočetné množiny a prosté úsekové ČRF)

Rekurzivně spočetné množiny jsou právě obory hodnot prostých úsekových ČRF.

Důkaz

"$\Leftarrow$": Víme, obor hodnot ČRF je rekurzivně spočetná množina (z věty o tom, že ČRF odpovídají RSM).

"$\Rightarrow$": Mějme ČRF φ ($M = rng(\varphi)$ pro nějaké φ, z lemmatu o tom, že RSM je obor hodnot ČRF).

Důkaz provedeme pomocí rekurzivní množiny $B = \{\langle x, s\rangle : \varphi(x)\downarrow \text{ přesně za } s \text{ kroků }\}$. Je vidět, že každé x bude pouze v jednom z párů $\langle x, s\rangle$.

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 $rng(\varphi)$).

Důsledek

Každá nekonečná rekurzivně spočetná množina obsahuje nekonečnou rekurzivní podmnožinu.

Důkaz

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

$$g(0) = f(0)$$

$$g(n+1) = f(\mu_j(f(j) > g(n)))$$

Obor hodnot g je nekonečná rekurzivní množina a je podmnožinou M.