Metoda redukce

Přednáška č. 5

Osnova

- m-redukce
- m-úplné množiny
- důkazy redukcí
- jiné typy redukce
- redukce v teorii jazyků

Princip redukce

Riceova věta poskytuje silný nástroj k důkazu nerekurzívnosti množiny. Důvodem je to, že ve větě je obsažena **obecná metoda.**

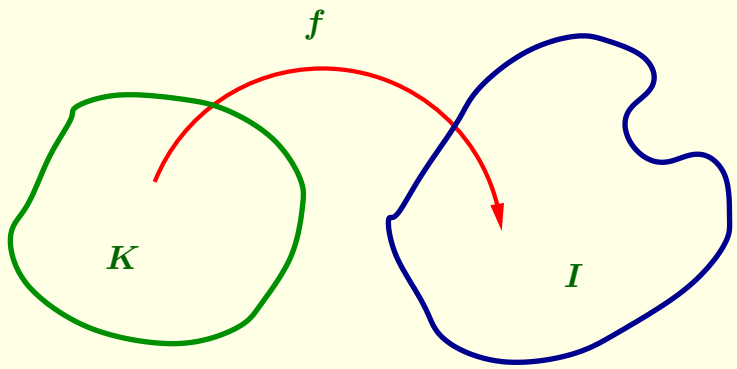
Jádro důkazu: spor s nerekurzívností problému zastavení.

Sporu je dosaženo tak, že v důkazu je definována totálně vyčíslitelná funkce f taková, že

$$i \in K \text{ právě když } f(i) \in I$$

Funkce f tak **efektivně převádí** problém příslušnosti pro K na problém příslušnosti pro I. Pokud bychom uměli rozhodovat problém I, pak bychom uměli rozhodovat i problém K. Říkáme, že K se **redukuje** na I.

Princip redukce



Redukce

Definice 1 Nechť $A, B \subseteq \mathbb{N}$.

1. Říkáme, že A se **m-redukuje** na B (píšeme $A \leq_m B$) právě když existuje totálně vyčíslitelná funkce $f : \mathbb{N} \to \mathbb{N}$ taková, že $A = f^{-1}(B)$.

2. Říkáme, že A a B jsou **m-ekvivalentní** (píšeme $A \equiv_m B$) právě když $A \leq_m B$ a $B \leq_m A$.

Index m u označení relace znamená, že funkce f nemusí být prostá (může být **many-to-one**).

Redukce

$\leq_m$ lze ekvivalentně charakterizovat takto:

- $\forall x : x \in A \Leftrightarrow f(x) \in B$

  $[x \in A \Leftrightarrow x \in f^{-1}(B) = \{x \mid f(x) \in B\} \Leftrightarrow f(x) \in B]$

- $f(A) \subseteq B \wedge f(\overline{A}) \subseteq \overline{B}$

  [Je-li $x \in A$, pak $f(x) \in f(A)$ a tedy $f(x) \in B$. Je-li $x \notin A$, pak $f(x) \in f(\overline{A})$ a tedy $f(x) \notin B$.

  Jestliže $y \in f(A)$, pak $y = f(x)$ pro $x \in A$ a tedy $y \in B$. Je-li $y \in f(\overline{A})$, pak $y = f(x)$ pro $x \notin A$ a tedy $y = f(x) \notin B$]

- $\chi_A = \chi_B \circ f$

  $[\chi_A = \chi_B \circ f \Leftrightarrow \forall x : \chi_A(x) = \chi_B(f(x)) \Leftrightarrow$
  $(\forall x : x \in A \Leftrightarrow f(x) \in B)]$

Redukce

Lema 2 Relace $\leq_m$ je reflexívní a tranzitívní, t.j. je **kvaziuspořádání**.

Je-li $A \leq_m B$ říkáme také, že B je **těžší** než A.

Důkaz:

1. $A = \{x \mid x \in A\} = f^{-1}(A)$, kde $f = \mathit{Identita}$

2. Nechť $A = f^{-1}(B)$ a $B = g^{-1}(C)$. Pak $x \in A \Leftrightarrow f(x) \in B \Leftrightarrow g(f(x)) \in C$, t.j. $x \in A \Leftrightarrow (g \circ f)(x) \in C$, t.j. $A \leq_m C$.

∎

Důkazy redukcí

Věta 3 Nechť $A \leq_m B$.

1. Je-li B rekurzívní, pak i A je rekurzívní.

2. Je-li B rekurzívně spočetná, pak i A je rekurzívně spočetná.

3. $\overline{A} \leq_m \overline{B}$.

Důkaz:

1. Existuje totálně vyčíslitelná funkce f tak, že $x \in A \Leftrightarrow f(x) \in B$. Je-li B rekurzívní, pak χ_B je totálně vyčíslitelná funkce. Tedy $x \in A \Leftrightarrow f(x) \in B \Leftrightarrow \chi_B(f(x)) = 1 \Leftrightarrow (\chi_B \circ f)(x) = 1$. Proto $A = (\chi_B \circ f)^{-1}\{1\}$, kde $\chi_B \circ f$ je totálně vyčíslitelná.

Důkazy redukcí

2. Je-li B rekurzívně spočetná, pak $B = \mathrm{dom}(g)$ pro nějakou vyčíslitelnou funkci g. Protože $g \circ f$ je vyčíslitelná funkce a $A = f^{-1}(B) = f^{-1}(\mathrm{dom}(g)) = \mathrm{dom}(g \circ f)$, je množina A rekurzívně spočetná.

3. $x \in A \Leftrightarrow f(x) \in B$, tedy $x \notin A \Leftrightarrow f(x) \notin B$.

∎

Důkazy redukcí

Důsledek 4 Nechť $A \leq_m B$.

1. Jestliže A není rekurzívní, pak B není rekurzívní.

2. Jestliže A není rekurzívně spočetná, pak B není rekurzívně spočetná.

O důkazu založeném na větě 3 či na důsledku 4 říkáme, že je proveden **metodou redukce (redukcí)**.

Důkaz redukcí vyžaduje vhodnou množinu. Velice často je touto množinou problém zastavení K resp. problém nezastavení $\overline{K}$. To je dáno tím, že problém zastavení má mezi nerekurzívními rekurzívně spočetnými množinami výsadní postavení.

Úplné problémy

Věta 5 Je-li množina $A \subseteq \mathbb{N}$ rekurzívně spočetná, pak $A \leq_m K$.

Důkaz: Definujme funkci $\theta : \mathbb{N}^2 \to \mathbb{N}$ následovně

$$\theta(x, y) = \begin{cases} 1 & \text{je-li } x \in A \\ \perp & \text{je-li } x \notin A \end{cases}$$

Funkce θ je vyčíslitelná. Podle translačního lemmatu existuje totálně vyčíslitelná funkce $f : \mathbb{N} \to \mathbb{N}$ taková, že $\theta(x, y) = \varphi_{f(x)}(y)$. Protože $\varphi_{f(x)}(f(x))$ je definováno právě když $x \in A$, platí $x \in A \Leftrightarrow f(x) \in K$.

∎

Těžké a úplné problémy

Předchozí výsledek znamená, že problém příslušnosti pro K je alespoň tak **těžký** jako jakýkoliv jiný rekurzívně spočetný problém.

Řečeno jinak: pokud by existoval algoritmus pro rozhodování problému zastavení K, pak by existoval i algoritmus pro rozhodování libovolného jiného r.e. problému.

Protože K je rekurzívně spočetná množina, říkáme, že K je **nejtěžší** mezi r.e. množinami.

Definice 6 Nechť $\mathbb{C}$ je třída podmnožin množiny $\mathbb{N}$ a $A \subseteq \mathbb{N}$. Řekneme, že množina A je **$\mathbb{C}$-těžká**, právě když pro každou množinu $B \in \mathbb{C}$ platí $B \leq_m A$. Je-li navíc $A \in \mathbb{C}$, pak A se nazývá **$\mathbb{C}$-úplná** (úplná v třídě $\mathbb{C}$).

Věta 7 Množina K je úplná v třídě všech rekurzívně spočetných množin.

Problém nezastavení

Problém nezastavení $\overline{K}$ není rekurzívně spočetná množina. Jeho použití při důkazech dává věta:

Věta 8 Jestliže $\overline{K} \leq_m A$, pak A není rekurzívně spočetná.

Důkaz: Tvrzení je zřejmé, neboť $\overline{K} = f^{-1}(A)$ a tedy pokud by A byla r.e., musela by být i množina $\overline{K}$ r.e. ∎

Některé ukázky redukcí

Příklad 9 **Problém verifikace je nerozhodnutelný**.

Množina $A = \{i \mid \varphi_i = g\}$, kde g je pevná totálně vyčíslitelná funkce, není rekurzívní.

Nejprve ukážeme, že množina $B = \{i \mid \varphi_i = identita\}$ není rekurzívní.

Nechť $f(i)$ je index programu

$$\underline{\textbf{begin}}\ x_2 := \Phi(i, x_1)\ \underline{\textbf{end}}$$

Zřejmě

$$\varphi_{f(i)}(x) = \begin{cases} x & \text{je-li } \varphi_i(x) \text{ je definováno} \\ \perp & \text{jinak} \end{cases}$$

Tedy $\varphi_{f(i)} = identita$ právě když $\varphi_i(x)$ je definováno pro všechna x a to je právě když φ_i je totální.

Některé ukázky redukcí

Funkce f je totálně vyčíslitelná, $A_1 = \{i \mid \varphi_i$ je totální$\}$ není rekurzívní a $A_1 \leq_m B$. Tedy B není rekurzívní.

Nyní ukážeme, že $B \leq_m A$. Nechť $g : \mathbb{N} \to \mathbb{N}$ je libovolná vyčíslitelná funkce, t.j. $g = \varphi_e$ pro nějaké e. Buď $h(i)$ index programu

$$\begin{array}{l} \underline{\textbf{begin}}\ x_2 := \Phi(i, x_1); \\ \quad \underline{\textbf{while}}\ x_2 \neq x_1\ \underline{\textbf{do}}\ x_1 := x_1; \\ \quad x_1 := \Phi(e, x_1) \\ \underline{\textbf{end}} \end{array}$$

Zřejmě

$$\varphi_{h(i)} = g \text{ právě když } \varphi_i = identita$$

Poznamenejme, že jsme současně dokázali i to, že množina A není rekurzívně spočetná, neboť A_1 není rekurzívně spočetná.

Některé ukázky redukcí

Příklad 10 **Problém ekvivalence je nerozhodnutelný.** Množina $A_{12} = \{(i, j) \mid \varphi_i = \varphi_j\}$ není rekurzívní.

Ukážeme, že $B \leq_m A_{12}$. Nechť e je index identity. Položme $f(i) =< i, e >$. Funkce f je totálně vyčíslitelná a $\varphi_i = identita$ právě když $\varphi_i = \varphi_e$, což je právě když $f(i) \in A_{12}$.

Stupně nerozhodnutelnosti

- Relace m-ekvivalence $\equiv_m$ je ekvivalencí.
- Třídy m-ekvivalence nazýváme **m-stupně nerozhodnutelnosti**.
- Kvaziuspořádání $\leq_m$ indukuje částečné uspořádání na třídách m-ekvivalence vzhledem k $\equiv_m$.
- Doposud jsme získali tyto znalosti o struktuře uspořádání na třídách m-ekvivalence:
  1. Množina K má maximální stupeň nerozhodnutelnosti mezi rekurzívně spočetnými množinami.
  2. Množiny $\emptyset$ a $\mathbb{N}$ jsou **nesrovnatelné**, i když jsou obě rekurzívní.
  3. Množiny K a $\overline{K}$ jsou nesrovnatelné.

Stupně nerozhodnutelnosti

- Každý m-stupeň obsahující rekurzívní množinu, je tvořen jen rekurzívními množinami (**rekurzívní stupeň**). Každý m-stupeň obsahující r.e. množinu, je tvořen jen r.e. množinami (**r.e. stupeň**).
- Uspořádání na m-stupních tvoří horní polosvaz: každé dva stupně mají jednu nejmenší horní závoru.

  Důkaz: Nechť $d(X)$ je m-stupeň obsahující množinu X. Nechť jsou dány množiny A a B. Položme

  $$A \text{ join } B = \{y \mid (y = 2x \wedge x \in A) \vee (y = 2x + 1 \wedge x \in B)\}$$

  Pak $d(A \text{ join } B)$ je nejmenší horní závora pro $d(A)$ a $d(B)$. ∎
- Každá nejmenší horní závora dvou r.e. stupňů je r.e.

Stupně nerozhodnutelnosti

- Neporovnatelné množiny generují neporovnatelné stupně.
- **Existují neporovnatelné nerekurzívní r.e. m-stupně ?**

  ANO
- Tvoří m-stupně svaz ? (Existují i největší dolní závory ?)

  NE

Jiné typy redukce

Základem pro **klasifikaci** nerekurzívních množin byla **redukce.**

Dodatečné požadavky na redukční funkci: prostá, bijekce, "jednoduše vyčíslitelná" ap.

Definice 11 Nechť $A, B \subseteq \mathbb{N}$.

1. Říkáme, že A se **1-redukuje** na B (píšeme $A \leq_1 B$) právě když existuje totálně vyčíslitelná funkce $f : \mathbb{N} \to \mathbb{N}$ taková, že f je **prostá** a $A = f^{-1}(B)$.
2. Říkáme, že A a B jsou **1-ekvivalentní** (píšeme $A \equiv_1 B$) právě když $A \leq_1 B$ a $B \leq_1 A$.
3. Říkáme, že A a B jsou **izomorfní** (píšeme $A \approx B$) právě když existuje totálně vyčíslitelná **bijekce** $f : \mathbb{N} \to \mathbb{N}$ taková, že $A = f^{-1}(B)$.

Vlastnosti 1-redukce

Věta 12 Nechť $A, B \subseteq \mathbb{N}$.

1. $\leq_1$ je reflexivní a tranzitivní relace, t.j. je kvaziuspořádání.
2. Jestliže $A \leq_1 B$, pak $\overline{A} \leq_1 \overline{B}$.
3. Jestliže $A \leq_1 B$ a B je rekurzívní, pak A je rekurzívní.
4. Jestliže $A \leq_1 B$ a B je r.e., pak A je r.e.

Vztah mezi redukcemi

Věta 13 Nechť $A, B \subseteq \mathbb{N}$.

1. Jestliže $A \leq_1 B$, pak $A \leq_m B$.
2. Jestliže $A \equiv_1 B$, pak $A \equiv_m B$.
3. Jestliže $A \approx B$, pak $A \equiv_1 B$.

Obrácená tvrzení obecně neplatí.

1-stupně nerozhodnutelnosti

Relace 1-ekvivalence $\equiv_1$ je ekvivalencí. Třídy 1-ekvivalence nazýváme **1-stupně nerozhodnutelnosti**.

Kvaziuspořádání $\leq_1$ indukuje opět kvaziuspořádání na třídách 1-ekvivalence vzhledem k $\equiv_1$.

1-ekvivalence představuje ostře jemnější nástroj pro rozlišení "obtížnosti" problémů.

m-úplnost a 1-úplnost

Ve třídě rekurzívně spočetných množin jsou pojmy m-úplnosti a 1-úplnosti ekvivalentní.

Věta 14 Nechť $A \subseteq \mathbb{N}$ je rekurzívně spočetná množina. Pak následující tvrzení jsou ekvivalentní:

1. A je m-úplná v třídě r.e. množin.
2. A je 1-úplná v třídě r.e. množin.
3. $K \leq_m A$
4. $K \leq_1 A$
5. $K \equiv_m A$

m-úplnost a 1-úplnost

Důkaz: Důkaz je veden posloupností těchto implikací:

A je m-úplná v r.e. $\Rightarrow$ $K \leq_m A$ (K je r.e.)
$\Rightarrow$ $K \equiv_m A$ (K je úplná)
$\Rightarrow$ $K \approx A$
$\Rightarrow$ $K \leq_1 A$
$\Rightarrow$ A je 1-úplná (K je 1-úplná)
$\Rightarrow$ A je m-úplná v r.e.

∎

Semi-Thueovy systémy

Definice 15 **Semi-Thueův systém** $\mathcal{T}$ nad konečnou abecedou Σ je určen konečnou množinou $\mathcal{P}$ přepisovacích pravidel tvaru $\alpha \to \beta$, kde $\alpha \in \Sigma^+$ a $\beta \in \Sigma^*$.

Řekneme, že $y \in \Sigma^*$ je **přímo odvoditelné** z $x \in \Sigma^*$ (píšeme $x \Rightarrow_{\mathcal{T}} y$), právě když existují $u, v \in \Sigma^*$ tak, že $x = u\alpha v, y = u\beta v$ a $\alpha \to \beta \in \mathcal{P}$.

Nechť $\Rightarrow^*_{\mathcal{T}}$ je reflexivní a tranzitivní uzávěr relace $\Rightarrow_{\mathcal{T}}$.

Semi-Thueovy systémy

Příklad 16 $\mathcal{T} = (\{a, b\}, \{ab \to bbb, bb \to \epsilon\})$. Máme:

1. $abbab \Rightarrow^*_{\mathcal{T}} bbbbbbb$

   $abbab \Rightarrow_{\mathcal{T}}$ **bbb**bab $\Rightarrow_{\mathcal{T}} bbbb$**bbb**

2. $babb \Rightarrow^*_{\mathcal{T}} b$

   $babb \Rightarrow_{\mathcal{T}} bbbbb \Rightarrow_{\mathcal{T}} bbb \Rightarrow_{\mathcal{T}} b$

3. $abbabbb \not\Rightarrow^*_{\mathcal{T}} bbbb$

   slovo obsahuje **sudý** počet b, právě když obsahuje sudý počet b po aplikaci libovolného pravidla

   $abbabbb$ obsahuje lichý počet b; $bbbb$ obsahuje sudý počet b

Slovní problém pro semi-Thueovy systémy

Věta 17 Množina $\{(\mathcal{T}, x, y) \mid x \Rightarrow^*_{\mathcal{T}} y\}$ není rekurzívní.

Důkaz: Důkaz je veden redukcí z množiny

$\{(M, x, y) \mid$ Turingův stroj M pro vstup x skončí s výstupem $y\}$

kde $x, y \in \mathbb{N}$. Tato množina není rekurzívní.

K libovolnému TS M libovolné dvojici čísel $x, y \in \mathbb{N}$ sestrojíme semi-Thueův systém $\mathcal{T}$ nad abecedou Σ a dvojici slov $u, v \in \Sigma^*$ tak, že $M(x) = y$ právě když $u \Rightarrow^*_{\mathcal{T}} v$.

Slovo u bude: $\triangleright q_0 B \overline{x} \triangleleft$ (q_0 je počáteční stav TS M)
Slovo v bude: $\overline{y}$

Semi-Thueův systém $\mathcal{T}$ bude **simulovat** výpočet TS M.

Slovní problém pro semi-Thueovy systémy

Konstrukci ukážeme na příkladě. Čísla kódujeme unárně pomocí symbolů I.

Uvažujme TS

$$\begin{array}{llllll}(q_0 & B & q_1 & B & R)\\ (q_1 & I & q_1 & I & R)\\ (q_1 & B & q_2 & I & L)\\ (q_2 & I & q_2 & I & L)\\ (q_2 & B & q_H & B & N)\end{array}$$

Slovní problém pro semi-Thueovy systémy

Simulace začíná se slovem

$$\triangleright \;\; q_0 \;\; B \;\; \overline{x} \;\; \triangleleft$$

Poté $\mathcal{T}$ "provádí" přechody podle pravidel TS M. Pravidlu

$$(q_0 \;\; B \;\; q_1 \;\; B \;\; R)$$

odpovídá přepisovací pravidlo

$$q_0 \;\; B \;\; \rightarrow \;\; B \;\; q_1$$

Slovní problém pro semi-Thueovy systémy

Pravidlu

$$(q_2 \;\; I \;\; q_2 \;\; I \;\; L)$$

odpovídají dvě přepisovací pravidla

$$\begin{array}{llllll} I & q_2 & I & \rightarrow & q_2 & I \;\; I\\ B & q_2 & I & \rightarrow & q_2 & B \;\; I\end{array}$$

Rovněž potřebujeme přepisovací pravidla, která umožní přidávat prázdné symboly na oba konce slova (vytvářet potencionálně nekonečnou pásku).

$$\begin{array}{llll}\triangleright & \rightarrow & \triangleright & B\\ \triangleleft & \rightarrow & B & \triangleleft\end{array}$$

Slovní problém pro semi-Thueovy systémy

Po skončení simulace je nutné převést slovo na tvar, který odpovídá požadovanému výstupu TS M, t.j.

$$\begin{array}{c}\ldots \;\; B \;\; B \;\; I \;\; I \;\; \ldots \;\; I \;\; B \;\; \ldots\\ \triangle\\ q_H\end{array}$$

t.j. slovu

$$\ldots \;\; B \;\; q_H \;\; B \;\; I \;\; I \;\; \ldots \;\; I \;\; B \;\; \ldots$$

Slovní problém pro semi-Thueovy systémy

Požadovaný formát získáme pomocí těchto pravidel:

$$\begin{array}{llll} q_H & B & \to & A \\ A & I & \to & I \quad A \\ A & B & \to & C \\ C & B & \to & C \\ C & I & \to & C \end{array} \qquad \begin{array}{llll} C & \lhd & \to & D \\ I & D & \to & D \quad I \\ & D & \to & E \\ B & E & \to & E \\ \rhd & E & \to & \epsilon \end{array}$$

Smyslem pravidel je:

1. zaměnit q_H za A a posunout A za první blok tvořený symboly I
2. změnit stav na nový stav (C), který vymaže všechny symboly napravo od prvního bloku
3. přesunout nový symbol D doleva přes první blok
4. vymazat všechny symboly B a $\rhd$ nalevo od prvního bloku

Postovy systémy

Definice 18 **Postův systém** P nad konečnou abecedou Σ je konečná množina uspořádaných dvojic $\{(\alpha_i, \beta_i)\}, 1 \leq i \leq n$, kde $\alpha_i, \beta_i \in \Sigma^*$.

Řešením Postova systému je každá neprázdná posloupnost přirozených čísel $i_1, i_2, \ldots, i_m$ $(1 \leq i_j \leq n)$ taková, že

$$\alpha_{i_1}\alpha_{i_2}\ldots\alpha_{i_m} = \beta_{i_1}\beta_{i_2}\ldots\beta_{i_m}$$

Postovy systémy

Příklad 19 Buď $\Sigma = \{a, b\}$. Postův systém

$$S = \{(b, bbb), (babbb, ba), (ba, a)\}$$

má řešení $i_1 = 2, i_2 = 1, i_3 = 1, i_4 = 3$ (je tedy $m = 4$), protože

babbb	b	b	ba	=	ba	bbb	bbb	a
α_2	α_1	α_1	α_3		β_2	β_1	β_1	β_3

Příklad 20 Buď $\Sigma = \{a, b\}$. Postův systém

$$S = \{(ab, abb), (a, ba), (b, bb)\}$$

nemá řešení, protože ve všech dvojicích je vždy α_i ostře kratší než β_i.

Postův problém přiřazení

Věta 21 Postův problém přiřazení (PCP) je nerozhodnutelný.

Důkaz: Redukcí z problému slov pro semi-Thueovy systémy.

Buď $\mathcal{T} = (\Sigma, P)$ semi-Thueův systém. Nechť Σ' je následující rozšíření abecedy Σ:

- Pro každé $a \in \Sigma$ přidáme do Σ' **nový** symbol $\overline{a}$.
- Do Σ' přidáme nové symboly: $*, \overline{*}, [,]$.

Pro $w \in \Sigma^*$ označme $\overline{w} \in \Sigma'^*$ slovo, které vznikne z w náhradou symbolů jejich "opruhovanými" protějšky.

Postův problém přiřazení

Nechť $x \Rightarrow_{\mathcal{T}}^{*} y$ je slovní problém. Převedeme ho na PCP, který bude vhodně kódovat odvození

$$x = w_1 \Rightarrow w_2 \Rightarrow \cdots \Rightarrow w_n = y$$

Každé řešení PCP bude začínat takto:

$$\begin{array}{ll} [w_1 * & \text{levá strana rovnice} \\ [& \text{pravá strana rovnice} \end{array}$$

Dále musí řešení pokračovat takto:

$$\begin{array}{llll} [w_1 & * & \overline{w_2} & \overline{*} \\ [w_1 & * & & \end{array}$$

Postův problém přiřazení

Dále musí být

$$\begin{array}{llllll} [w_1 & * & \overline{w}_2 & \overline{*} & w_3 & * \\ [w_1 & * & \overline{w}_2 & \overline{*} & & \end{array}$$

a tak dále se střídají pruhované a nepruhované bloky až dostaneme

$$\begin{array}{llllllll} [w_1 & * & \overline{w}_2 & \overline{*} & \ldots & \overline{w}_{n-1} & \overline{*} & w_n \\ [w_1 & * & \overline{w}_2 & \overline{*} & \ldots & \overline{w}_{n-1} & & \end{array}$$

V posledním kroku pravá strana "dožene" levou

$$[w_1 \quad * \quad \overline{w}_2 \quad \overline{*} \quad \ldots \quad \overline{w}_n \quad]$$

Postův problém přiřazení

Pro daný semi-Thueův systém $\mathcal{T}$ a slova x, y je odpovídající Postův systém určen těmito dvojicemi slov:

(1) $(a, \overline{a})$ a $(\overline{a}, a)$ pro každé $a \in \Sigma \cup \{*\}$

(2) $([w_1 *, [)$, kde $w_1 = x$

(3) $([, \overline{*} w_n])$, kde $w_n = y$

(4) $(\beta, \overline{\alpha})$ a $(\overline{\beta}, \alpha)$ pro každé $\alpha \to \beta \in T$

Je zřejmé, že (2) musí být použita jako první, pokud má být dosaženo shody. Podobně (3) musí být použita jako poslední.

Postův problém přiřazení

Předpokládejme nyní, že jsme získali

$$\begin{array}{llllllll} [w_1 & * & \ldots & \overline{*} & w_k & * & \overline{w}_{k+1} & \overline{*} \\ [w_1 & * & \ldots & \overline{*} & w_k & * & & \end{array}$$

pro $k+1 < n$. Předpokládejme, že $w_{k+1} \Rightarrow w_{k+2}$ podle pravidla $\alpha \to \beta$ pro $w_{k+1} = u\alpha v, w_{k+2} = u\beta v$. Tuto derivaci v Postově systému napodobíme takto: opakovaným použitím (1) máme

$$\begin{array}{llllllll} [w_1 & * & \ldots & \overline{*} & w_k & * & \overline{w}_{k+1} & \overline{*} & u \\ [w_1 & * & \ldots & \overline{*} & w_k & * & \overline{u} & & \end{array}$$

dále pomocí (4) máme

$$\begin{array}{llllllll} [w_1 & * & \ldots & \overline{*} & w_k & * & \overline{w}_{k+1} & \overline{*} & u\beta \\ [w_1 & * & \ldots & \overline{*} & w_k & * & \overline{u\alpha} & & \end{array}$$

Postův problém přiřazení

a opět pomocí (1) dostaneme

$$\begin{array}{l}[w_1 \ * \ \ldots \ \overline{*} \ w_k \ * \ \overline{w}_{k+1} \ \overline{*} \ u\beta v \\ [w_1 \ * \ \ldots \ \overline{*} \ w_k \ * \ \overline{u\alpha v}\end{array}$$

To dáva

$$\begin{array}{l}[w_1 \ * \ \ldots \ \overline{*} \ w_k \ * \ \overline{w}_{k+1} \ \overline{*} \ w_{k+2} \\ [w_1 \ * \ \ldots \ \overline{*} \ w_k \ * \ \overline{w}_{k+1}\end{array}$$

Postův problém přiřazení

Všimněme si, že w_n v pravidle (3) nemá pruhy. Je tedy použitelné jen pro n liché. Použitím pravidla (1) však můžeme dvojici

$$\begin{array}{l}[w_1 \ * \ \ldots \ \overline{*} \ w_k \ * \ \overline{w}_{k+1} \ \overline{*} \\ [w_1 \ * \ \ldots \ \overline{*} \ w_k \ *\end{array}$$

změnit na

$$\begin{array}{l}[w_1 \ * \ \ldots \ \overline{*} \ w_k \ * \ \overline{w}_{k+1} \ \overline{*} \ w_{k+1} \ * \\ [w_1 \ * \ \ldots \ \overline{*} \ w_k \ * \ \overline{w}_{k+1} \ \overline{*}\end{array}$$

a obrátit tak pruhování u posledního bloku.

Indukcí dostáváme

$x \Rightarrow_{\mathcal{T}}^{*} y$ **právě když vytvořený Postův systém má řešení**

Příklad

$\mathcal{T} = (\{a, b, \}, \{ba \to ab, aab \to \epsilon\})$.

$aba \Rightarrow^{*} \epsilon$?

$aba \Rightarrow aab \Rightarrow \epsilon$

PCP:

$\Sigma' = \{a, b, \overline{a}, \overline{b}, *, \overline{*}, [,]\}$

$$\begin{array}{rcl} S & = & \{ \ (a, \overline{a}), (b, \overline{b}), (\overline{a}, a), (\overline{b}, b), (*, \overline{*}), (\overline{*}, *) \\ & & \ ([aba*, [), (], \overline{*}\epsilon]), \\ & & \ (ab, \overline{b}\overline{a}), (\overline{a}\overline{b}, ba), (\epsilon, aab), (\epsilon, \overline{aab}) \\ & & \} \end{array}$$

Příklad

$$\begin{array}{l}[aba \ * \\ [\end{array}$$

$$\begin{array}{l}[aba \ * \ \overline{a} \\ [a\end{array}$$

$$\begin{array}{l}[aba \ * \ \overline{aa}\overline{b} \\ [aba\end{array}$$

$$\begin{array}{l}[aba \ * \ \overline{aa}\overline{b} \ \overline{*} \\ [aba \ *\end{array}$$

$$\begin{array}{l}[aba \ * \ \overline{aa}\overline{b} \ \overline{*} \ \epsilon \\ [aba \ * \ \overline{aa}\overline{b}\end{array}$$

$$\begin{array}{l}[aba \ * \ \overline{aa}\overline{b} \ \overline{*} \ \epsilon] \\ [aba \ * \ \overline{aa}\overline{b} \ \overline{*} \ \epsilon]\end{array}$$

Bezkontextové jazyky

Věta 22 Problém jednoznačnosti bezkontextové gramatiky je nerozhodnutelný.

Důkaz: Nechť $P = \{(\alpha_i, \beta_i)\}\ 1 \leq i \leq n$ je Postův systém nad abecedou Σ. Nechť $\Sigma' = \Sigma \cup \{\overline{1}, \overline{2}, \ldots, \overline{n}\}$. Uvažujme bezkontextovou gramatiku nad Σ' danou těmito pravidly:

$$\begin{array}{lcl} S & \rightarrow & S_1 \mid S_2 \\ S_1 & \rightarrow & \alpha_1 S_1 \overline{1} \mid \alpha_2 S_1 \overline{2} \mid \cdots \mid \alpha_n S_1 \overline{n} \mid \alpha_1 \overline{1} \mid \cdots \mid \alpha_n \overline{n} \\ S_2 & \rightarrow & \beta_1 S_2 \overline{1} \mid \beta_2 S_2 \overline{2} \mid \cdots \mid \beta_n S_2 \overline{n} \mid \beta_1 \overline{1} \mid \cdots \mid \beta_n \overline{n} \end{array}$$

Tato gramatika není jednoznačná právě když P má řešení. ∎

Bezkontextové jazyky

Věta 23 Nechť G_1 a G_2 jsou bezkontextové gramatiky. Pak tyto problémy nejsou rozhodnutelné:

1. $L(G) = \emptyset$
2. $L(G_1) \cap L(G_2) = \emptyset$
3. $L(G_1) = L(G_2)$
4. $L(G_1) \subset L(G_2)$

Problém zániku matic

Definice 24 Řekneme, že neprázdná konečná množina $\{M_i\}$ matic typu $(3, 3)$ nad oborem celých čísel **zaniká** pro $< j_1, j_2 >$, $1 \leq j_1$, $j_2 \leq 3$, existuje-li konečný součin

$$M = M_{i_1} M_{i_2} \ldots M_{i_k}$$

takový, že jeho prvek v j_1-tém řádku a j_2-tém sloupci je 0.

Věta 25 Problém zániku matic je nerozhodnutelný, t.j. množina

$$\{(\{M_i\}, j_1, j_2) \mid \{M_i\} \text{ zaniká pro } < j_1, j_2 >\}$$

není rekurzívní.

Problém zániku matic

Důkaz: Redukcí z PCP.

Idea konstrukce:
ke každé dvojici (u, v) slov nad Σ sestrojíme matici $M(u, v)$ tak, že

1. Prvek ve 3. řádku a 2. sloupci matice $M(u, v)$ je 0 právě když $u = v$.
2. Pro všechna slova u_1, u_2, v_1, v_2 je

$$M(u_1, v_1).M(u_2, v_2) = M(u_1 u_2, v_1 v_2)$$

K danému Postovu systému $S = \{(\alpha_i, \beta_i)\}$ nad Σ pak sestrojíme množinu matic $\{M_i\}$, kde $M_i = M(\alpha_i, \beta_i)$. Z vlastností 1. a 2. bude pak vyplývat požadované.

Problém zániku matic

Konstrukce matic $M(u,v)$:

Definujme

$k(x) = i$ právě když x je i-té slovo v lexikografickém uspořádání,
$m(x) = n^{|x|}$ kde $|x|$ je délka slova x a n je počet písmen v Σ

Je zřejmé, že

$$\begin{aligned} k(xy) &= k(x)m(y) + k(y) \\ m(xy) &= m(x)m(y) \end{aligned}$$

Položme pro každou dvojici (u,v) slov nad Σ

$$M(u,v) = \begin{bmatrix} m(u) & m(v) - m(u) & 0 \\ 0 & m(v) & 0 \\ k(u) & k(v) - k(u) & 1 \end{bmatrix}$$

Problém zániku matic

Matice $M(u,v)$ mají požadované vlastnosti:

1. Prvek ve 3. řádku a 2. sloupci matice $M(u,v) = 0$ právě když $u = v$ neboť $k(v) - k(u) = 0$ právě když $u = v$

2. Pro všechna slova $u_1, u_2, v_1, v_2 \in \Sigma^*$ je $M(u_1,v_1).M(u_2,v_2) = M(u_1u_2, v_1v_2)$ neboť

$$\begin{aligned} &M(u_1,v_1).M(u_2,v_2) = \\ &= \begin{bmatrix} m(u_1) & m(v_1) - m(u_1) & 0 \\ 0 & m(v_1) & 0 \\ k(u_1) & k(v_1) - k(u_1) & 1 \end{bmatrix} . \begin{bmatrix} m(u_2) & m(v_2) - m(u_2) & 0 \\ 0 & m(v_2) & 0 \\ k(u_2) & k(v_2) - k(u_2) & 1 \end{bmatrix} \end{aligned}$$

Problém zániku matic

$$= \begin{bmatrix} m(u_1)m(u_2) & m(v_1)m(v_2) - m(u_1)m(u_2) & 0 \\ 0 & m(v_1)m(v_2) & 0 \\ k(u_1)m(u_2) + k(u_2) & k(v_1)m(v_2) + k(v_2) - k(u_1)m(u_2) - k(u_2) & 1 \end{bmatrix}$$

$$= M(u_1u_2, v_1v_2)$$

∎