Das Postsche Korrespondenzproblem I

Definition

Für ein endliches Alphabet Σ ist das Postsche Korrespondenzproblem die Menge

$$\mathrm{PCP} := \{((x_1, y_1), (x_2, y_2), \dots, (x_k, y_k)) \in (\Sigma^* \times \Sigma^*)^k \mid \exists_{n \geq 1} \exists_{i_1, i_2, \dots, i_n \in \{1,2,\dots,k\}} : x_{i_1} \cdot x_{i_2} \cdot \ldots \cdot x_{i_n} = y_{i_1} \cdot y_{i_2} \cdot \ldots \cdot y_{i_n}\}$$

Beispiel 1

$$\left(\binom{x_1}{y_1} = \binom{1}{101}, \binom{x_2}{y_2} = \binom{10}{00}, \binom{x_3}{y_3} = \binom{011}{11}\right) \in \mathrm{PCP}$$

Wähle $i_1 = 1, i_2 = 3, i_3 = 2, i_4 = 3$.

$$x_1 \cdot x_3 \cdot x_2 \cdot x_3 = 1 \cdot 011 \cdot 10 \cdot 011 = 101110011$$

$$y_1 \cdot y_3 \cdot y_2 \cdot y_3 = 101 \cdot 11 \cdot 00 \cdot 11 = 101110011$$

Beispiel 2

$$\left(\binom{1}{10}, \binom{10}{1}, \binom{01}{0}, \binom{0}{001}\right) \notin \mathrm{PCP}$$

„Suffixfreiheit“: jedes x_i endet mit einem anderen Zeichen als y_i

Das Postsche Korrespondenzproblem II

Hinweise:

1. PCP oft in Unentscheidbarkeitsbeweisen (Reduktionen) benutzt
2. PCP semi-entscheidbar für beliebiges Σ (vermöge Brute-Force-Algorithmus).
3. „unäres PCP“ ($|\Sigma| = 1$) entscheidbar:

   Beweisidee: Es kommt nur darauf an, dass

   $$\sum_{j \leq n} |x_{i_j}| = \sum_{j \leq n} |y_{i_j}| \quad \text{also} \quad \sum_{j \leq n} (|x_{i_j}| - |y_{i_j}|) = 0.$$

   $\rightsquigarrow$ unäres PCP äquivalent zur Frage:

   "lassen sich k gegebene ganze Zahlen $(|x_i| - |y_i|) \in \mathbb{Z}$ nichttrivial linear zu 0 kombinieren?"

   $\rightsquigarrow$ genau dann unmöglich wenn alle Zahlen positiv oder alle negativ
4. PCP entscheidbar für $k = 2$ Eingabepaare, aber unentscheidbar für $k \geq 4$ Eingabepaare.
5. PCP entscheidbar falls nur nach einer Lösung mit Länge $\leq n$ gesucht
6. Für beliebiges Σ lässt sich PCP auf PCP mit $\Sigma' = \{0, 1\}$ zurückführen

Das Modifizierte PCP

Folgende Variante MPCP (M wie „Modified") sehr nützlich

$$\text{MPCP} := \left\{ \left(\binom{x_1}{y_1}, \binom{x_2}{y_2}, \ldots, \binom{x_k}{y_k} \right) \in \text{PCP} \mid \exists_{n \geq 1} \exists_{i_2,\ldots,i_n \in \{1,2,\ldots,k\}} : x_1 \cdot x_{i_2} \cdot \cdots \cdot x_{i_n} = y_1 \cdot y_{i_2} \cdot \cdots \cdot y_{i_n} \right\}$$

Lemma

MPCP $\leq$ PCP.

Reduktion f

$$\binom{x_j}{y_j} \mapsto \binom{x_j^{\text{re}}}{y_j^{\text{li}}}$$

Sowie neue Paare

$$\binom{\#x_1^{\text{re}}}{y_1^{\text{li}}} \binom{\$}{\#\$}$$

Verwende neue Symbole $\$, \# \notin \Sigma$

Definiere für $a \in \Sigma$, $w \in \Sigma^*$:

$$(aw)^{\text{li}} = \#aw^{\text{li}} \qquad (aw)^{\text{re}} = a\#w^{\text{re}} \qquad \varepsilon^{\text{li}} = \varepsilon^{\text{re}} = \varepsilon$$

Noch zu zeigen: f ist Reduktion, also $P \in \text{MPCP} \Leftrightarrow f(P) \in \text{PCP}$.

"$\Rightarrow$": $(1, i_2, \ldots, i_n)$ Lösung für $P \Rightarrow (k+1, i_2, \ldots, i_n, k+2)$ Lösung für $f(P)$

"$\Leftarrow$": $(k+1, i_2, \ldots, i_n, k+2)$ Lösung für $f(P)$

oBdA. $i_m \neq k+2$, sonst $(k+1, i_2, \ldots, i_m)$ auch Lösung $\rightsquigarrow (1, i_2, \ldots, i_n)$ Lösung für P.

H_0 reduzierbar auf MPCP

Beweis (Skizze)

Reduktion f erhält des Codewortes von $M = (Z, \Sigma, \Gamma, \delta, z_0, \square, \{z_e\})$ und erzeugt MPCP-Instanz.

oBdA: Eingabemaschine M hält $\Leftrightarrow$ M hält in akzeptierendem Zustand

Zeigen $M \in H_0 \Leftrightarrow f(\langle M \rangle) \in MPCP$

"$\Rightarrow$": M hält auf leerem Band

$\leadsto$ es gibt Konfigurationenfolge

$$\square z_0 \square \vdash_M^* \alpha z_e \beta \text{ mit } \alpha, \beta \in \Gamma^*.$$

Simulation durch MPCP wie im Beispiel,

am Ende β entfernt durch Löschregel,

Abschluss durch Abschlussregel

"$\Leftarrow$": haben MPCP Lösung für $f(\langle M \rangle)$

$\leadsto$ Lösung beginnt mit initialer Konfiguraion

Überführungsregeln erzwingen valide Übergänge

$\# \leadsto$ Lösung hört mit Abschluss auf

$\leadsto$ z_e wird erreicht

$\binom{\#}{\#\square z_0 \square \#}$ - **initiale Konfiguration**

$\binom{a}{a}$ für alle $a \in \Gamma$ – **Kopierregeln**

$\binom{\#}{\#}, \binom{\#}{\#\square}, \binom{\#}{\square\#}$ – **Randregeln**

$\binom{z_e a}{z_e}$ für alle $a \in \Gamma$ – **Löschregeln**

$\binom{z_e\#\#}{\#}$ – **Abschlussregel**

Überführungsregeln: $\forall_{z_i, z_j \in Z}$ & $\forall_{a,b,c \in \Gamma}$

$\binom{z_i a}{z_j b}$ falls $\delta(z_i, a) = (z_j, b, N)$

$\binom{z_i a}{b z_j}$ falls $\delta(z_i, a) = (z_j, b, R)$

$\binom{a z_i b}{z_j a c}$ falls $\delta(z_i, b) = (z_j, c, L)$

Unentscheidbarkeit von PCP

Korollar

- $H_0 \leq$ MPCP.
- PCP (und MPCP) sind unentscheidbar.
- H_0 ist semi-entscheidbar (und damit H und K)
- es gibt "universelle Turing-Maschine"