

1.9 Das Postsche Korrespondenz-Problem

Definition.

Das nachfolgend beschriebene Problem heißt *Postsches Korrespondenz-Problem* (PCP).

gegeben: Eine endliche Folgen $(x_1, y_1), \dots, (x_k, y_k)$ von Wortpaaren mit $x_i, y_i \in A^+$ (A endliche Alphabet)
 gefragt: Gibt es eine Folge von Indizes $i_1, \dots, i_n \in \{1, \dots, k\}$, $n \geq 1$, mit $x_{i_1}, \dots, x_{i_n} = y_{i_1}, \dots, y_{i_n}$?

Beispiel.

Das Postsche Korrespondenz-Problem

$$K = ((1, 101), (10, 00), (011, 11)),$$

also

$$\begin{array}{lll} x_1 = 1 & x_2 = 10 & x_3 = 011 \\ y_1 = 101 & y_2 = 00 & y_3 = 11 \end{array}$$

besitzt die Lösung $(1, 3, 2, 3)$, denn es gilt:

$$x_1 x_3 x_2 x_3 = 101110011 = y_1 y_3 y_2 y_3$$

PCP ist schwer.

z.B.: $K = ((001, 0), (01, 011), (01, 101), (10, 001))$

besitzt eine Lösung, aber die kürzeste besteht aus 66 Indizes!

PCP ist semi-entscheidbar:

Probiere alle möglichen Indexfolgen mit zunehmender Länge durch.

Satz.

Das Postsche Korrespondenz-Problem ist nicht entscheidbar.

Beweis.

Betrachte modifiziertes PCP:

MPCP

gegeben: wie bei PCP
 gefragt: gibt es eine Lösung $i_1, \dots, i_n$ mit $i_1 = 1$

Lemma

$\text{MPCP} \leq \text{PCP}$

Beweis.

Sei $\#$ ein neues Symbol.

Für $w = a_1 \dots a_m \in A^+$ sei

$$\bar{w} = \#a_1\#a_2\#\dots\#a_m\#$$

$$\begin{aligned}\dot{w} &= \#a_1\#a_2\#\dots\#a_m \\ \acute{w} &= a_1\#a_2\#\dots\#a_m\#\end{aligned}$$

Sei $K = ((x_1, y_1), \dots, (x_k, y_k))$ die Eingabe von MPCP.
 $\rightarrow f(K) = ((\bar{x}_1, \dot{y}_1), (x'_1, \dot{y}_1), (x'_2, \dot{y}_2), \dots, (x'_k, \dot{y}_k), (\$, \#\$))$
 f ist berechenbar.
 f vermittelt eine Reduktion von MPCP auf PCP.

Behauptung.

K besitzt eine Lösung mit $i_1 = 1$
 $\Leftrightarrow f(K)$ besitzt irgend eine Lösung.

Beweis.

- ($\rightarrow$) Besitzt K eine Lösung $(i_1, \dots, i_n)$ mit $i_1 = 1$,
dann ist $(1, i_2 + 1, \dots, i_n + 1, k + 2)$ eine Lösung für $f(K)$.
($\leftarrow$) Besitzt $f(K)$ eine Lösung $(i_1, \dots, i_n)$,
so muß gelten:
 $i_1 = 1, i_n = k + 2$ mit $i_j \in \{2, \dots, k + 1\}$ für $2 \leq j \leq n + 1$
 $\Rightarrow (1, i_2 - 1, \dots, i_{n-1} - 1)$ ist Lösung für K .

Zur Unentscheidbarkeit von MPCP:

Lemma

$H \leq MPCP$

Beweis.

Sei $M = (Q, \Sigma, \Gamma, \delta, z_0, \square, F)$ eine kodierte TM

$w \in \Sigma^+$ die Eingabe.

Suche eine allgemeine Vorschrift, die (M, w) eine Folge $(x_1, y_1), \dots, (x_n, y_n)$ zuordnet mit

M angesetzt auf w stoppt $\Leftrightarrow (x_1, y_1), \dots, (x_n, y_n)$ besitzt eine Lösung mit $i_1 = 1$

Konstruktion von MPCP über dem Alphabet $\Gamma \cup Q \cup \{\#\}$.

erstes Wortpaar: $(\#, \#q_0w\#)$

weitere Paare:

1. Kopieregeln:

$$(a, a) \text{ für alle } a \in \Gamma \cup \{\#\}$$

2. Überführungsregeln:

$$\begin{aligned}(qa, q'c) & \text{ falls } \delta(q, a) = (q', c, N) \\ (qa, cq') & \text{ falls } \delta(q, a) = (q', c, R)\end{aligned}$$

$$\begin{aligned}
(qa, q'bc) & \text{ falls } \delta(q, a) = (q', c, L) \text{ für alle } b \in \Gamma \\
(\#qa, \#q'\square c) & \text{ falls } \delta(q, a) = (q', c, L) \\
(q\#, q'c\#) & \text{ falls } \delta(q, \square) = (q', c, N) \\
(q\#, cq'\#) & \text{ falls } \delta(q, \square) = (q', c, R) \\
(bq\#, q'b\#) & \text{ falls } \delta(q, \square) = (q', c, L) \text{ für alle } b \in \Gamma
\end{aligned}$$

3. Löschregeln:

$$(aq_e, q_e) \text{ und } (q_e a, q_e) \text{ für alle } a \in \Gamma, q_e \in F$$

4. Abschlußregeln:

$$(q_e \# \# \#, \#) \text{ für alle } q_e \in F$$

- ($\rightarrow$) Falls M bei w stoppt gibt es eine Folge von Konfigurationen $(k_0, k_1, \dots, k_t)$ mit $k_0 = q_0 w$, k_t ist Endkonfiguration also $k_t = uq_e v$ mit $u, v \in A^*$, $q_e \in F$) und $k_i \vdash k_{i+1}$
 $\Leftrightarrow$ Die obige Eingabe für das MPCP besitzt ein Lösungswort

$$\#k_0\#k_1\ldots\#k_t\#k'_t\#k''_t\ldots\#q_e\#\#$$

($k'_t, k''_t, \dots$ entstehen aus $k_t = uq_e v$ durch Löschung von Nachbarsymbolen aus q_e)

- ($\leftarrow$) Besitzt der obige MPCP eine Lösung mit $i_1 = 1$, dann läßt sich eine stoppende Rechnung von M bei w ablesen. ■

Folgerung

PCP bleibt unentscheidbar, falls für das Alphabet A gilt: $A = \{0, 1\}$. ("01-PCP")

Beweis.

Es reicht zu zeigen: $\text{PCP} \leq 01\text{-PCP}$.

Sei A das Alphabet von PCP.

Betrachte: $f: A \rightarrow \{0, 1\}^*$ mit $f(a_r) = \hat{a}_r = 01^r$.

Setze die Abbildung f auf A^* fort.

Es gilt:

$$(x_1, y_1), \dots, (x_n, y_n) \text{ besitzt Lösung} \Leftrightarrow (\hat{x}_1, \hat{y}_1), \dots, (\hat{x}_n, \hat{y}_n) \text{ besitzt Lösung.} \quad \blacksquare$$

Bemerkung

Sei PCP_k die Variante des PCPs, deren Eingabe aus genau k Wortpaaren besteht.

Es gilt:

PCP_k ist unentscheidbar für $k \geq 9$.

PCP_k ist entscheidbar für $k \leq 2$.