

# Das Postsche Korrespondenzproblem

Prof. Dr. David Sabel

LFE Theoretische Informatik



## Motivation / Überblick

- Vorgeschlagen von Emil Post im Jahr 1946
- Es ist ein einfaches aber unentscheidbares Problem
- Es wird häufig verwendet, um es auf andere Probleme zu reduzieren und deren Unentscheidbarkeit zu zeigen
- Es hat nichts mit Turingmaschinen und deren Akzeptanzverhalten zu tun (im Gegensatz zu den verschiedenen Varianten vom Halteproblem)

## Definition (Postsches Korrespondenzproblem)

Gegeben sei ein Alphabet  $\Sigma$  und eine

Folge von Wortpaaren  $K = ((x_1, y_1), \dots, (x_k, y_k))$  mit  $x_i, y_i \in \Sigma^+$ .

Das **Postsche Korrespondenzproblem (PCP)** ist die Frage, ob es für die gegebene Folge  $K$  eine Folge von Indizes  $i_1, \dots, i_m$  mit  $i_j \in \{1, \dots, k\}$  gibt, sodass

$$x_{i_1} \cdots x_{i_m} = y_{i_1} \cdots y_{i_m}$$

gilt.

# PCP ist wie ein Domino-Spiel

---

Spielsteinarten:  $\left( \begin{bmatrix} x_1 \\ y_1 \end{bmatrix}, \dots, \begin{bmatrix} x_k \\ y_k \end{bmatrix} \right)$

Gesucht: Aneinanderreihung der Spielsteine, sodass oben wie unten dasselbe Wort abgelesen werden kann. Dabei dürfen beliebig (aber endlich) viele Spielsteine verwendet werden.

Beispiel:

Sei  $K = \left( \begin{bmatrix} a \\ aba \end{bmatrix}, \begin{bmatrix} baa \\ aa \end{bmatrix}, \begin{bmatrix} ab \\ bb \end{bmatrix} \right)$

# PCP ist wie ein Domino-Spiel

Spielsteinarten:  $\left( \begin{bmatrix} x_1 \\ y_1 \end{bmatrix}, \dots, \begin{bmatrix} x_k \\ y_k \end{bmatrix} \right)$

Gesucht: Aneinanderreihung der Spielsteine, sodass oben wie unten dasselbe Wort abgelesen werden kann. Dabei dürfen beliebig (aber endlich) viele Spielsteine verwendet werden.

Beispiel:

Sei  $K = \left( \begin{bmatrix} a \\ aba \end{bmatrix}, \begin{bmatrix} baa \\ aa \end{bmatrix}, \begin{bmatrix} ab \\ bb \end{bmatrix} \right)$

$I = (1, 2, 3, 2)$  ist eine Lösung, da

$$\begin{bmatrix} a \\ aba \end{bmatrix} \begin{bmatrix} baa \\ aa \end{bmatrix} \begin{bmatrix} ab \\ bb \end{bmatrix} \begin{bmatrix} baa \\ aa \end{bmatrix} = abaaabbaa$$
$$= abaaabbaa$$

$$\text{Instanz } K = \left( \begin{bmatrix} ab \\ bba \end{bmatrix}, \begin{bmatrix} ba \\ baa \end{bmatrix}, \begin{bmatrix} ba \\ aba \end{bmatrix}, \begin{bmatrix} bba \\ b \end{bmatrix} \right)$$

$$\text{Instanz } K = \left( \begin{bmatrix} ab \\ bba \end{bmatrix}, \begin{bmatrix} ba \\ baa \end{bmatrix}, \begin{bmatrix} ba \\ aba \end{bmatrix}, \begin{bmatrix} bba \\ b \end{bmatrix} \right)$$

Die kürzeste Lösung benötigt 66 Paare:

(2, 1, 3, 1, 1, 2, 4, 2, 1, 3, 1, 3, 1, 1, 3, 1, 1, 2, 4, 1, 1, 2, 4, 3, 1, 4, 4, 3, 1, 1, 1, 2, 4, 2, 4, 4, 4, 3, 1, 3, 1, 4, 2, 4, 1, 1, 2, 4, 1, 4, 4, 3, 1, 4, 4, 3, 4, 4, 3, 4, 2, 4, 1, 4, 4, 3).

# Unentscheidbarkeit von PCP

---

Beweis in 2 Schritten:

①  $\text{MPCP} \leq \text{PCP}$

MPCP ist das **Modifizierte Postsche Korrespondenzproblem**:

Nur Lösungen zulässig, die mit dem ersten Spielstein  $\begin{bmatrix} x_1 \\ y_1 \end{bmatrix}$  beginnen

②  $H \leq \text{MPCP}$

Damit folgt aus der Unentscheidbarkeit von  $H$  die Unentscheidbarkeit von MPCP und damit die Unentscheidbarkeit von PCP.



## Definition (Modifiziertes Postsches Korrespondenzproblem)

Gegeben sei ein Alphabet  $\Sigma$  und eine Folge von Wortpaaren

$K = ((x_1, y_1), \dots, (x_k, y_k))$  mit  $x_i, y_i \in \Sigma^+$ .

Das Modifizierte Postsche Korrespondenzproblem (MPCP) ist die Frage, ob es für die gegebene Folge  $K$  eine Folge von Indizes  $i_1 = 1, i_2, \dots, i_m$  mit  $i_j \in \{1, \dots, k\}$  gibt, sodass  $x_{i_1} \cdots x_{i_m} = y_{i_1} \cdots y_{i_m}$  gilt.

# MPCP $\leq$ PCP

---

## Lemma

MPCP  $\leq$  PCP

Beweis: Gesucht: Berechenbares  $f$  mit:  $K$  MPCP-lösbar g.d.w.  $f(K)$  PCP-lösbar.

## Lemma

### MPCP $\leq$ PCP

Beweis: Gesucht: Berechenbares  $f$  mit:  $K$  MPCP-lösbar g.d.w.  $f(K)$  PCP-lösbar.

Für  $w = a_1 \cdots a_n \in \Sigma^+$  sei:

$$\bar{w} = \#a_1\#a_2\#\cdots\#a_n\# \quad \acute{w} = a_1\#a_2\#\cdots\#a_n\# \quad \grave{w} = \#a_1\#a_2\#\cdots\#a_n$$

## Lemma

### MPCP $\leq$ PCP

Beweis: Gesucht: Berechenbares  $f$  mit:  $K$  MPCP-lösbar g.d.w.  $f(K)$  PCP-lösbar.

Für  $w = a_1 \cdots a_n \in \Sigma^+$  sei:

$$\bar{w} = \#a_1\#a_2\#\cdots\#a_n\# \quad \acute{w} = a_1\#a_2\#\cdots\#a_n\# \quad \grave{w} = \#a_1\#a_2\#\cdots\#a_n$$

$$\text{Sei } f\left(\begin{bmatrix} x_1 \\ y_1 \end{bmatrix}, \dots, \begin{bmatrix} x_k \\ y_k \end{bmatrix}\right) = \left( \underbrace{\begin{bmatrix} \bar{x}_1 \\ \grave{y}_1 \end{bmatrix}}_{(x'_1, y'_1)}, \underbrace{\begin{bmatrix} \acute{x}_1 \\ \grave{y}_1 \end{bmatrix}}_{(x'_2, y'_2)}, \dots, \underbrace{\begin{bmatrix} \acute{x}_k \\ \grave{y}_k \end{bmatrix}}_{(x'_{k+1}, y'_{k+1})}, \underbrace{\begin{bmatrix} \$ \\ \#\$ \end{bmatrix}}_{(x'_{k+2}, y'_{k+2})} \right)$$

## Lemma

### MPCP $\leq$ PCP

Beweis: Gesucht: Berechenbares  $f$  mit:  $K$  MPCP-lösbar g.d.w.  $f(K)$  PCP-lösbar.

Für  $w = a_1 \cdots a_n \in \Sigma^+$  sei:

$$\bar{w} = \#a_1\#a_2\#\cdots\#a_n\# \quad \acute{w} = a_1\#a_2\#\cdots\#a_n\# \quad \grave{w} = \#a_1\#a_2\#\cdots\#a_n$$

$$\text{Sei } f\left(\begin{bmatrix} x_1 \\ y_1 \end{bmatrix}, \dots, \begin{bmatrix} x_k \\ y_k \end{bmatrix}\right) = \left( \underbrace{\begin{bmatrix} \bar{x}_1 \\ \grave{y}_1 \end{bmatrix}}_{(x'_1, y'_1)}, \underbrace{\begin{bmatrix} \acute{x}_1 \\ \grave{y}_1 \end{bmatrix}}_{(x'_2, y'_2)}, \dots, \underbrace{\begin{bmatrix} \acute{x}_k \\ \grave{y}_k \end{bmatrix}}_{(x'_{k+1}, y'_{k+1})}, \underbrace{\begin{bmatrix} \$ \\ \#\$ \end{bmatrix}}_{(x'_{k+2}, y'_{k+2})} \right)$$

- $1, i_2, \dots, i_m$  Lösung für  $K \Rightarrow 1, i_2+1, \dots, i_m+1, \dots, k+2$  Lösung für  $f(K)$ .

## Lemma

### MPCP $\leq$ PCP

Beweis: Gesucht: Berechenbares  $f$  mit:  $K$  MPCP-lösbar g.d.w.  $f(K)$  PCP-lösbar.

Für  $w = a_1 \cdots a_n \in \Sigma^+$  sei:

$$\bar{w} = \#a_1\#a_2\#\cdots\#a_n\# \quad \acute{w} = a_1\#a_2\#\cdots\#a_n\# \quad \grave{w} = \#a_1\#a_2\#\cdots\#a_n$$

$$\text{Sei } f\left(\begin{bmatrix} x_1 \\ y_1 \end{bmatrix}, \dots, \begin{bmatrix} x_k \\ y_k \end{bmatrix}\right) = \left( \underbrace{\begin{bmatrix} \bar{x}_1 \\ \grave{y}_1 \end{bmatrix}}_{(x'_1, y'_1)}, \underbrace{\begin{bmatrix} \acute{x}_1 \\ \grave{y}_1 \end{bmatrix}}_{(x'_2, y'_2)}, \dots, \underbrace{\begin{bmatrix} \acute{x}_k \\ \grave{y}_k \end{bmatrix}}_{(x'_{k+1}, y'_{k+1})}, \underbrace{\begin{bmatrix} \$ \\ \#\$ \end{bmatrix}}_{(x'_{k+2}, y'_{k+2})} \right)$$

- $1, i_2, \dots, i_m$  Lösung für  $K \Rightarrow 1, i_2+1, \dots, i_m+1, \dots, k+2$  Lösung für  $f(K)$ .
- $i_1, \dots, i_m$  Lösung für  $f(K) \Rightarrow i_1, i_2 - 1, \dots, i_{m-1} - 1$  Lösung für  $K$

Für Lösungen muss gelten:  $i_1 = 1$ ,  $\begin{bmatrix} x_{i_m} \\ y_{i_m} \end{bmatrix} = \begin{bmatrix} \$ \\ \#\$ \end{bmatrix}$  und  $\begin{bmatrix} x_{i_j} \\ y_{i_j} \end{bmatrix} = \begin{bmatrix} \acute{x}_{j(r)} \\ \grave{y}_{j(r)} \end{bmatrix}$  für  $2 \leq i_j \leq i_{m-1}$

## Lemma

$H \leq \text{MPCP}$ .

Beweis:

- $m\#w$  mit Turingmaschinenbeschreibung  $m$  und Eingabe  $w$
- Erstelle MPCP-Instanz  $K = f(m\#w)$ , so dass TM  $M_m$  auf Eingabe  $w$  genau dann anhält, wenn  $K$  lösbar.
- Sei  $M_m = (Z, \Sigma, \Gamma, \delta, z_0, \square, E)$ .
- Alphabet für das MPCP:  $\Gamma \cup Z \cup \{\#\}$ .
- Idee: Lösung des MPCP simuliert Transitionsfolge der TM.
- Erstes Wortpaar (mit dem jede Lösung anfangen muss):  $\begin{bmatrix} x_1 \\ y_1 \end{bmatrix} = \begin{bmatrix} \# \\ \#z_0w\# \end{bmatrix}$
- Weitere Paare lassen sich in Gruppen von Regeln aufteilen
- Kopierregeln, Transitionsregeln, Löseregeln, Abschlussregeln

## $H \leq$ MPCP: Kopierregeln

---

- $\begin{bmatrix} a \\ a \end{bmatrix}$  für alle  $a \in \Gamma \cup \{\#\}$



## $H \leq \text{MPCP}$ : Transitionsregeln

- $\begin{bmatrix} za \\ z'c \end{bmatrix}$  falls  $\delta(z, a) = (z', c, N)$
- $\begin{bmatrix} za \\ cz' \end{bmatrix}$  falls  $\delta(z, a) = (z', c, R)$
- $\begin{bmatrix} bza \\ z'bc \end{bmatrix}$  falls  $\delta(z, a) = (z', c, L)$  für alle  $b \in \Gamma$
- $\begin{bmatrix} \#za \\ \#z'\square c \end{bmatrix}$  falls  $\delta(z, a) = (z', c, L)$
- $\begin{bmatrix} z\# \\ z'c\# \end{bmatrix}$  falls  $\delta(z, \square) = (z', c, N)$
- $\begin{bmatrix} z\# \\ cz'\# \end{bmatrix}$  falls  $\delta(z, \square) = (z', c, R)$
- $\begin{bmatrix} bz\# \\ z'bc\# \end{bmatrix}$  falls  $\delta(z, \square) = (z', c, L)$  für alle  $b \in \Gamma$

# $H \leq \text{MPCP}$ : Löseregeln und Abschlussregeln

---

## Löseregeln:

- $\begin{bmatrix} az_e \\ z_e \end{bmatrix}$  für alle  $a \in \Gamma, z_e \in E$
- $\begin{bmatrix} z_e a \\ z_e \end{bmatrix}$  für alle  $a \in \Gamma, z_e \in E$

## Abschlussregeln:

- $\begin{bmatrix} z_e \#\# \\ \# \end{bmatrix}$  für alle  $z_e \in E$

## $H \leq$ MPCP: Korrespondenz

---

Wenn  $TM$  akzeptierenden Lauf hat, dann gibt es Folge

$$K_0 \vdash K_1 \vdash \dots \vdash K_n,$$

wobei  $K_0 = z_0w$  und  $K_n = uz_ev$  für ein  $z_e \in E$ .

Dann hat das MPCP eine Lösung, die oben und unten das Wort

$$\#K_0\#K_1\#\dots\#K_n\#K_{n+1}\#\dots\#K_m\#\#$$

erzeugt, wobei  $K_m = z_e$  und jedes  $K_i$  mit  $n+1 \leq i \leq m$  jeweils aus  $K_{i-1}$  entsteht durch Löschen eines der benachbarten Zeichen von  $z_e$  in  $u'z_ev'$  entsteht.

## $H \leq \text{MPCP}$ : Korrespondenz (2)

---

Obere Folge hinkt der unteren um eine Konfiguration hinterher

oben:  $\#K_1\#K_2\#\cdots\#K_i\#$

unten:  $\#K_1\#K_2\#\cdots\#K_i\#K_{i+1}\#$

Verlängerung, um die nächste:

- Kopierregel anwenden bis in die Nähe des Zustands
- Dann Überführungsregel anwenden
- Kopierregel anwenden zum Vervollständigen

Ab  $K_n$ :

- Löschregeln anwenden, um die Symbole auf dem Band zu löschen.
- Wenn in unterer Folge  $z_e\#$  steht, dann Abschlussregel anwenden.

# Beispiel

$$z_0abc \vdash dz_1bc \vdash dez_2c \vdash defz_3\Box \vdash defz_e\Box$$

Lösende Spielsteinfolge:

$$\begin{bmatrix} \# \\ \#z_0abc\# \end{bmatrix} \begin{bmatrix} z_0a \\ dz_1 \end{bmatrix} \begin{bmatrix} b \\ b \end{bmatrix} \begin{bmatrix} c \\ c \end{bmatrix} \begin{bmatrix} \# \\ \# \end{bmatrix} \begin{bmatrix} d \\ d \end{bmatrix} \begin{bmatrix} z_1b \\ ez_2 \end{bmatrix} \begin{bmatrix} c \\ c \end{bmatrix} \begin{bmatrix} \# \\ \# \end{bmatrix} \begin{bmatrix} d \\ d \end{bmatrix} \begin{bmatrix} e \\ e \end{bmatrix} \begin{bmatrix} z_2c \\ fz_3 \end{bmatrix} \begin{bmatrix} \# \\ \# \end{bmatrix} \begin{bmatrix} d \\ d \end{bmatrix} \begin{bmatrix} e \\ e \end{bmatrix} \begin{bmatrix} f \\ f \end{bmatrix} \begin{bmatrix} z_3\# \\ z_e\Box\# \end{bmatrix}$$

$$\begin{bmatrix} \# \\ \# \end{bmatrix} \begin{bmatrix} d \\ d \end{bmatrix} \begin{bmatrix} e \\ e \end{bmatrix} \begin{bmatrix} f \\ f \end{bmatrix} \begin{bmatrix} z_e\Box \\ z_e \end{bmatrix} \begin{bmatrix} \# \\ \# \end{bmatrix} \begin{bmatrix} d \\ d \end{bmatrix} \begin{bmatrix} e \\ e \end{bmatrix} \begin{bmatrix} fz_e \\ z_e \end{bmatrix} \begin{bmatrix} \# \\ \# \end{bmatrix} \begin{bmatrix} d \\ d \end{bmatrix} \begin{bmatrix} ez_e \\ z_e \end{bmatrix} \begin{bmatrix} \# \\ \# \end{bmatrix} \begin{bmatrix} dz_e \\ z_e \end{bmatrix} \begin{bmatrix} \# \\ \# \end{bmatrix} \begin{bmatrix} z_e\#\# \\ \# \end{bmatrix}$$

## Umgekehrte Richtung

---

Jede Lösung für das MPCP erzeugt eine akzeptierende Konfigurationsfolge.

Schließlich prüfe, dass  $f$  berechenbar ist.

Daher folgt:  $m\#w \in H \iff$  MPCP  $f(m\#w)$  lösbar

## Satz

Das Postsche Korrespondenzproblem (sowie das modifizierte Postsche Korrespondenzproblem) ist unentscheidbar.

Beweis: Da  $H$  unentscheidbar ist und  $H \leq \text{MPCP} \leq \text{PCP}$  gilt, folgt, dass MPCP als auch PCP unentscheidbar sind.

**Lemma (Unentscheidbarkeit des 01-PCP)**

Das Postsche Korrespondenzproblem über dem Alphabet  $\Sigma$  mit  $|\Sigma| = 2$  (01-PCP) ist unentscheidbar.

Beweis:

- Reduziere PCP auf 01-PCP
- Sei  $\Sigma = \{0, 1\}$ .
- Sei  $K = (x_1, y_1), \dots, (x_k, y_k)$  eine Instanz des PCP über dem Alphabet  $\{a_1, \dots, a_j\}$ .
- Sei  $f(\varepsilon) = \varepsilon$ ,  $f(a_i) = 10^i$ ,  $f(a_i w) = f(a_i) f(w)$  und  $f(K) = (f(x_1), f(y_1)), \dots, (f(x_k), f(y_k))$ .
- Dann ist  $f(K)$  eine Instanz des 01-PCPs und offensichtlich gilt:  $i_1, \dots, i_n$  ist eine Lösung für  $K$  g.d.w.  $i_1, \dots, i_n$  ist eine Lösung für  $f(K)$ .
- $f$  ist Turingberechenbar und daher folgt  $\text{PCP} \leq \text{01-PCP}$



## Lemma

Das PCP für unäre Alphabete ist entscheidbar.

Beweis:

- Alle Spielsteine von der Form  $\begin{bmatrix} a^n \\ a^m \end{bmatrix}$ .
- Wenn für alle  $(x_i, y_i)$ :  $|x_i| < |y_i|$ , dann gibt es keine Lösung.
- Wenn für alle  $(x_i, y_i)$ :  $|x_i| > |y_i|$ , dann gibt es keine Lösung.
- Wenn  $(x_i, y_i) = (a^n, a^{n+r})$  und  $(x_j, y_j) = (a^{m+s}, a^m)$  mit  $s, r \geq 0$ , dann ist das PCP immer lösbar:

Die Lösung ist  $\underbrace{i, \dots, i}_{s\text{-mal}}, \underbrace{j, \dots, j}_{r\text{-mal}}$ , denn:

oben  $a^{s \cdot n + r \cdot (m+s)}$  und unten  $a^{s \cdot (n+r) + r \cdot m}$ .

Daher oben wie unten  $(sn + rm + rs)$ -viele  $a$ 's

# Anzahl $k$ der Spielsteinarten beschränken

---

PCP mit  $k$ -vielen verschiedenen Spielsteinarten:

- $k = 1$  oder  $k = 2$ : als entscheidbar gezeigt, im Jahr 1982
- $k \geq 5$ : als unentscheidbar gezeigt im Jahr 2015  
(vorher war  $k \geq 7$  bekannt (1996))
- $k = 3, 4$ : unbekannt

PCP ist semi-entscheidbar:

- Probiere alle Folgen von  $i$ -Spielsteinen aus.
- Lasse  $i$  wachsen.

Findet Lösung, wenn eine existiert, in endlich vielen Schritten, aber terminiert nicht, wenn keine Lösung existiert.

Da  $H \leq \text{PCP}$  folgt auch, dass  $H$  semi-entscheidbar ist.

Daher: Es gibt Turingmaschine  $U$ , die die sich bei Eingabe  $w\#x$  so verhält wie  $M_w$  auf Eingabe  $x$ .

Die TM  $U$  nennt man eine **Universelle Turingmaschine**:

- verhält sich wie ein Interpreter für Turingmaschinen
- wird durch die Eingabe  $w$  **programmiert** und  $x$  ist dann die eigentliche Eingabe für das Programm.

- Entscheidbarkeit, Semi-Entscheidbarkeit
- Das Halteproblem ist unentscheidbar!
- Reduktion  $L_1 \leq L_2$  als Werkzeug zum Nachweis der Unentscheidbarkeit / Entscheidbarkeit
- PCP als „einfaches“ unentscheidbares Problem