

Theorie der Informatik

III.5. Postsches Korrespondenzproblem

Malte Helmert Christian Tschudin

Universität Basel

24. April 2013

Theorie der Informatik

24. April 2013 — III.5. Postsches Korrespondenzproblem

III.5.1 Postsches Korrespondenzproblem

III.5.2 (Un-)Entscheidbarkeit des PCP

Überblick: Berechenbarkeitstheorie

III. Berechenbarkeitstheorie

III.1. ~~Turing-Berechenbarkeit~~

III.2. ~~LOOP-, WHILE-, GOTO-Berechenbarkeit~~

III.3. ~~primitive Rekursion und μ -Rekursion~~

III.4. ~~Entscheidbarkeit, Reduktionen, Halteproblem~~

III.5. **Postsches Korrespondenzproblem** ← hier!

III.5.1 Postsches Korrespondenzproblem

Wie beweist man Unentscheidbarkeit?

- ▶ Aussage über berechnete Funktion einer TM/eines Algorithmus
 - am einfachsten mit **Satz von Rice**
- ▶ andere Fragestellungen
 - ▶ **direkt mit Definition Entscheidbarkeit**
 - meist recht kompliziert
 - ▶ **Reduktion von unentscheidbarem Problem**, z.B.
 - (allgemeines) Halteproblem (H)
 - Halteproblem auf leerem Band (H_0)

Mehr Auswahl für Reduktionsbeweise?

☹ Alle Halteprobleme sehr ähnlich

- Wollen mehr Auswahl für Reduktionsbeweise
- andersartiges unentscheidbares Problem?

Postsches Korrespondenzproblem
(benannt nach dem Mathematiker **Emil Leon Post**)

Postsches Korrespondenzproblem

Beispiel (Postsches Korrespondenzproblem)

Gegeben: „Dominosteine“ der Sorten

1:	<table><tr><td>1</td></tr><tr><td>101</td></tr></table>	1	101	2:	<table><tr><td>10</td></tr><tr><td>00</td></tr></table>	10	00	3:	<table><tr><td>011</td></tr><tr><td>11</td></tr></table>	011	11
1											
101											
10											
00											
011											
11											

(unendlich viele Steine jeder Sorte)

Lösung: Folge von Steinen, so dass obere und untere Zeile gleich

<table><tr><td>1</td></tr><tr><td>101</td></tr></table>	1	101	<table><tr><td>011</td></tr><tr><td>11</td></tr></table>	011	11	<table><tr><td>10</td></tr><tr><td>00</td></tr></table>	10	00	<table><tr><td>011</td></tr><tr><td>11</td></tr></table>	011	11
1											
101											
011											
11											
10											
00											
011											
11											
1	3	2	3								

Postsches Korrespondenzproblem: Definition

Definition (Postsches Korrespondenzproblem PCP)

Gegeben: Endliche **Folge von Wortpaaren**
 $(x_1, y_1), (x_2, y_2), \dots, (x_k, y_k)$, wobei $x_i, y_i \in \Sigma^+$
 (für ein beliebiges Alphabet Σ)

Gefragt: Gibt es eine Folge von Indizes
 $i_1, i_2, \dots, i_n \in \{1, \dots, k\}$, $n \geq 1$,
 mit $x_{i_1} x_{i_2} \dots x_{i_n} = y_{i_1} y_{i_2} \dots y_{i_n}$?

Eine **Lösung** des Korrespondenzproblems ist solch eine Folge
 $i_1, \dots, i_n$.

Gegeben-Gefragt-Notation vs. Definition als Menge

Bisher: Problem immer als Menge definiert

Jetzt: Definition in **gegeben-gefragt-Notation**

Definition (neues Problem P)

Gegeben: Instanz $\mathcal{I}$

Gefragt: Hat $\mathcal{I}$ eine bestimmte Eigenschaft?

entspricht der Definition

Definition (neues Problem P)

Das Problem P ist die Sprache

$P = \{w \mid w \text{ kodiert eine Instanz } \mathcal{I} \text{ mit der gefragten Eigenschaft}\}.$

PCP Definition als Menge

PCP lässt sich also alternativ folgendermassen definieren:

Definition (Postsches Korrespondenzproblem PCP)

Das Postsche Korrespondenzproblem PCP ist die Menge

$PCP = \{w \mid w \text{ kodiert eine Folge von Wortpaaren}$

$(x_1, y_1), (x_2, y_2), \dots, (x_k, y_k), \text{ für die es eine}$
 Folge von Indizes $i_1, i_2, \dots, i_n \in \{1, \dots, k\}$ gibt,
 so dass $x_{i_1}x_{i_2} \dots x_{i_n} = y_{i_1}y_{i_2} \dots y_{i_n}\}.$

III.5.2 (Un-)Entscheidbarkeit des PCP

Postsches Korrespondenzproblem

PCP kann doch nicht so schwer sein!

– Oder doch?

1101	0110	1
1	11	110

Formal: $K = ((1101, 1), (0110, 11), (1, 110))$
 → Kürzeste Lösung hat Länge 252!

10	0	100
0	001	1

Formal: $K = ((10, 0), (0, 001), (100, 1))$
 → Unlösbar

PCP: Semi-Entscheidbarkeit

Satz (Semi-Entscheidbarkeit von PCP)

PCP *ist semi-entscheidbar*.

Beweis.

Semi-Entscheidungsverfahren für Eingabe w :

- ▶ Falls w eine Wortpaarfolge $(x_1, y_1), \dots, (x_k, y_k)$ kodiert:
Teste systematisch immer längere Indexfolgen $i_1, i_2, \dots, i_n$, ob sie eine Lösung darstellen. Falls ja, stoppe mit Antwort „Ja“.
- ▶ Falls w keine Wortpaarfolge kodiert: Gehe in Endlosschleife.

Falls $w \in \text{PCP}$, terminiert das Verfahren mit „Ja“. Ansonsten stoppt das Verfahren nicht. $\square$

PCP: Unentscheidbarkeit

Satz (Unentscheidbarkeit von PCP)

PCP *ist unentscheidbar*.

Beweis mit Zwischenschritt über anderes Problem:

modifiziertes PCP (MPCP)

- ① Reduziere MPCP auf PCP ($\text{MPCP} \leq \text{PCP}$)
- ② Reduziere Halteproblem auf MPCP ($H \leq \text{MPCP}$)

→ Machen wir uns an die Arbeit. . .

MPCP: Definition

Definition (Modifiziertes Postsches Korrespondenzproblem MPCP)

Gegeben: Folge von Wortpaaren wie beim PCP

Gefragt: Gibt es eine Lösung $i_1, i_2, \dots, i_n \in \{1, \dots, k\}$ mit $i_1 = 1$?

Reduzierbarkeit von MPCP auf PCP(1)

Lemma

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

Beweis.

Sei $\#, \$ \notin \Sigma$. Für Wort $w = a_1 a_2 \dots a_m \in \Sigma^+$ sei

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

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

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

Für Eingabe $K = ((x_1, y_1), \dots, (x_k, y_k))$ definiere
 $f(K) = ((\bar{x}_1, \dot{y}_1), (\acute{x}_1, \grave{y}_1), (\acute{x}_2, \grave{y}_2), \dots, (\acute{x}_k, \grave{y}_k), (\$, \#\$))$

...

Reduzierbarkeit von MPCP auf PCP(2)

Beweis (Fortsetzung).

$$f(K) = ((\bar{x}_1, \bar{y}_1), (\bar{x}_1, \bar{y}_1), (\bar{x}_2, \bar{y}_2), \dots, (\bar{x}_k, \bar{y}_k), (\$, \#\$))$$

Abbildung f ist **berechenbar**, kann leicht geeignet zu einer **totalen** Funktion erweitert werden und es gilt
 K besitzt Lösung mit $i_1 = 1$ gdw $f(K)$ besitzt eine Lösung:

Angenommen $1, i_2, i_3, \dots, i_n$ ist Lösung von K , dann ist
 $1, i_2 + 1, \dots, i_n + 1, k + 2$ Lösung für $f(K)$.

Falls $i_1, \dots, i_n$ Lösung von $f(K)$ ist, muss (wg. der Bauart der Wortpaare) gelten, dass es ein $m \leq n$ gibt, so dass
 $i_1 = 1, i_m = k + 2$ und $i_j \in \{2, \dots, k + 1\}$ für $j \in \{2, \dots, m - 1\}$.
 Dann ist $1, i_2 - 1, \dots, i_{m-1} - 1$ Lösung für K .

Damit ist f eine Reduktion von MPCP auf PCP. $\square$

PCP: Unentscheidbarkeit – Wo sind wir?

Satz (Unentscheidbarkeit von PCP)

PCP ist **unentscheidbar**.

Beweis mit Zwischenschritt über anderes Problem:
modifiziertes PCP (MPCP)

- ① Reduziere MPCP auf PCP ($\text{MPCP} \leq \text{PCP}$) ✓
- ② Reduziere Halteproblem auf MPCP ($H \leq \text{MPCP}$)

Reduzierbarkeit von H auf MPCP(1)

Lemma

$H \leq \text{MPCP}$.

Beweis.

Ziel: Bilde Turingmaschine $M = (Z, \Sigma, \Gamma, \delta, z_0, \square, E)$ und Wort
 $w \in \Sigma^*$ auf MPCP-Instanz $K = ((x_1, y_1), \dots, (x_k, y_k))$ ab, so dass

M angesetzt auf w stoppt gdw. $K \in \text{MPCP}$.

...

Reduzierbarkeit von H auf MPCP(2)

Beweis (Fortsetzung).

Idee:

- Wortfolge beschreibt Konfigurationsfolge der TM

- „x-Zeile“ folgt „y-Zeile“ $x : \boxed{\# \ k_0 \ \# \ k_1 \ \# \ k_2 \ \#}$

$$y : \boxed{\# \ k_0 \ \# \ k_1 \ \# \ k_2 \ \# \ k_3 \ \#}$$

- Konfigurationen werden grösstenteils kopiert, nur Region um den Kopf wird verändert.
- Nach Erreichen einer Zielkonfiguration: Angleichen der Zeilen durch Löschen der Konfiguration.

...

Reduzierbarkeit von H auf MPCP(3)

Beweis (Fortsetzung).

Alphabet von K ist $\Gamma \cup Z \cup \{\#\}$.

1. Wortpaar: $(\#, \# \sqcap z_0 w \#)$

Weitere Wortpaare:

① Kopierregeln: (a, a) für alle $a \in \Gamma \cup \{\#\}$

② Überführungsregeln:

$(za, z'c)$ falls $\delta(z, a) = (z', c, N)$

(za, cz') falls $\delta(z, a) = (z', c, R)$

$(bza, z'bc)$ falls $\delta(z, a) = (z', c, L)$ für alle $b \in \Gamma$

$(\#za, \#z' \sqcap c)$ falls $\delta(z, a) = (z', c, L)$

...

Reduzierbarkeit von H auf MPCP(4)

Beweis (Fortsetzung).

$(z\#, z'c\#)$ falls $\delta(z, \sqcap) = (z', c, N)$

$(z\#, cz'\#)$ falls $\delta(z, \sqcap) = (z', c, R)$

$(bz\#, z'bc\#)$ falls $\delta(z, \sqcap) = (z', c, L)$ für alle $b \in \Gamma$

③ Löschregeln: (az_e, z_e) und $(z_e a, z_e)$ für alle $a \in \Gamma$ und $z_e \in E$

④ Abschlussregeln: $(z_e \# \#, \#)$ für alle $z_e \in E$

...

Reduzierbarkeit von H auf MPCP(5)

Beweis (Fortsetzung).

„ $\Rightarrow$ “ Falls M auf w stoppt, existiert eine Folge von Konfigurationen $k_0, \dots, k_t$ mit

- ▶ $k_0 = \sqcap z_0 w$ ist Startkonfiguration
- ▶ k_t ist Endkonfiguration ($k_t = uz_e v$ mit $u, v \in \Gamma^*$ und $z_e \in E$)
- ▶ $k_i \vdash k_{i+1}$ für $i = 0, 1, \dots, t-1$

K besitzt dann Lösung mit Lösungswort

$\#k_0\#k_1\#\dots\#k_t\#k'_t\#k''_t\#\dots\#z_e\#\#$

Bis k_t : „x-Zeile“ folgt „y-Zeile“

Ab k'_t : Löschen der Nachbarsymbole von z_e .

...

Reduzierbarkeit von H auf MPCP(6)

Beweis (Fortsetzung).

„ $\Leftarrow$ “ Falls K eine Lösung hat, hat diese die Form

$\#k_0\#k_1\#\dots\#k_n\#\#$,

wobei $k_0 = \sqcap z_0 w$. und es gibt ein $l \leq n$, so dass ein Endzustand z_e zum ersten Mal in k_l vorkommt.

Alle k_i für $i \leq l$ sind Konfigurationen von M und es gilt, dass

$k_i \vdash k_{i+1}$ für $i \in \{0, \dots, l-1\}$.

$k_0, \dots, k_l$ ist damit die Konfigurationsfolge von M auf Eingabe w , die zeigt, dass die TM in einem Endzustand stoppt. $\square$

PCP: Unentscheidbarkeit – Fertig!

Satz (Unentscheidbarkeit von PCP)

PCP *ist unentscheidbar*.

Beweis mit Zwischenschritt über anderes Problem:

modifiziertes PCP (MPCP)

- ① Reduziere MPCP auf PCP ($\text{MPCP} \leq \text{PCP}$) ✓
- ② Reduziere Halteproblem auf MPCP ($H \leq \text{MPCP}$) ✓

Beweis.

Wegen $H \leq \text{MPCP}$ und $\text{MPCP} \leq \text{PCP}$ gilt $H \leq \text{PCP}$. Da H unentscheidbar ist, muss also auch PCP unentscheidbar sein. $\square$

PCP mit $\Sigma = \{0, 1\}$

Satz

Das Postsche Korrespondenzproblem ist bereits unentscheidbar, wenn man sich auf das Alphabet $\{0, 1\}$ beschränkt.

Beweis durch Reduktion von allgemeinem PCP $\rightarrow$ Übungen.