Das Postsche Korrespondenzproblem

Gegeben: Eine endliche Folge von Paaren (x_i, y_i), $1 \leq i \leq k$, wobei die x_i und y_i nichtleere Wörter über Σ sind.

Gesucht: Eine Folge von Indizes $i_1, \ldots, i_n$, $n \geq 1$, $i_j \in \{1, \ldots, k\}$, so dass $x_{i_1} \ldots x_{i_n} = y_{i_1} \ldots y_{i_n}$.

Eine Folge von Indizes mit dieser Eigenschaft nennen wir Lösung für das PCP. (PCP steht für *Post's Correspondence Problem)*

Meist als *Entscheidungsproblem*...

Beispiel

Das folgende PCP lässt sich leicht lösen:

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

Eine Lösung (und tatsächlich eine *kürzeste Lösung*) ist $(1, 3, 2, 3)$.

Jede Lösung muss mit dem Index 1 beginnen. (Warum?)
Das ergibt:

```
1
1 0 1
```

Nun muss Index 3 folgen, also:

```
1 0 1 1
1 0 1 1 1
```

Im nächsten Schritt haben wir zwei Möglichkeiten.
Machen Sie selbst den Beweis zu Ende, dass $(1, 3, 2, 3)$ die kürzeste Lösung bildet!

Noch ein Beispiel

$$R = (\underset{1}{(001, 0)}, \underset{2}{(01, 011)}, \underset{3}{(01, 101)}, \underset{4}{(10, 001)})$$

Wir sammeln möglichst viele Informationen über mögliche Lösungsfolgen, d.h. Indexfolgen, die Lösungen für R bilden:

- Index 1 und Index 4 müssen in jeder Lösung gleich oft vorkommen.
- Indizes 2 und 3 müssen zusammen genau so oft vorkommen wie Index 1.
- Der erste Index muss immer 1 oder 2 sein, der letzte muss 3 sein.
- **Alle Lösungen haben eine durch 3 teilbare Länge.**
- Als Lösung der Länge 3 wäre nur $(1, 4, 3)$ möglich – das ist aber keine Lösung!
- Lösungen der Länge 6 lassen sich auch relativ einfach ausschließen.

Tatsächlich ist dieses PCP lösbar! Aber:

Seine kürzeste Lösung hat die Länge 66.

PCP ist rekursiv aufzählbar

Satz: χ'_{PCP} ist berechenbar.

Als Beweis geben wir einen (Pseudocode-) Algorithmus an, der χ'_{PCP} berechnet.

```
ℓ := 1; found:=FALSE;
WHILE NOT found DO
  Prüfe alle Indexfolgen der Länge ℓ,
       ob sie das gegebene PCP lösen.
  IF Lösung gefunden THEN found:=TRUE ENDIF;
  ℓ := ℓ + 1
ENDWHILE;
OUTPUT 1
```

MPCP – das *modifizierte* PCP

Das modifizierte PCP (MPCP) ist definiert wie PCP,
einzige Ausnahme: Lösungen *müssen* mit $i_1 = 1$ beginnen!

Lemma: $H \leq MPCP$

Zum Beweis muss eine Eingabe $w\#x$ in eine Instanz $f(w\#x)$ von MPCP so umgerechnet werden, dass M_w auf Eingabe x genau dann nach endlicher Zeit hält, wenn $f(w\#x)$ als MPCP lösbar ist. Und natürlich muss diese Funktion f berechenbar sein.

Sei also $M = M_w$ als 7-Tupel $M = (Z, \Sigma, \Gamma, \delta, z_0, E, \Box)$ gegeben und $x \in \Sigma^*$. Startkonfiguration von M auf Input x ist damit z_0x.

Als erstes Paar unseres MPCP definieren wir $(\#, \#z_0x\#)$.

Die Reduktion von H auf MPCP (1)

Außer dem schon definierten Anfangspaar werden wir nun vier Serien von Paaren für das MPCP definieren, die jeweils einem speziellen Zweck dienen:

Kopierpaare: Für jedes $a \in \Gamma \cup \{\#\}$ das Paar (a, a).

Die Kopierpaare dienen dazu, Konfigurationsteile unverändert in die Folgekonfiguration übernehmen zu können.

Löschpaare: Für jedes $a \in \Gamma$ und $z \in E$ die Paare (za, z) und (az, z).

Die Löschpaare dienen dazu, am Ende der Berechnung die *vorausgeeilte* Konfigurationsdarstellung zu „beseitigen."

Schlusspaar: Für jedes $z \in E$ das Paar $(z\#\#, \#)$.

Hiermit soll das MPCP zum passenden Ende gebracht werden, falls die Turingmaschinensimulation terminiert.

Überführungspaare: Die Überführungspaare werden den Hauptteil einer Simulation von Turingmaschinen bilden. Dafür benötigen wir eine weitere Folie...

Die Reduktion von H auf MPCP (2)

Für die Überführungspaare müssen wir die drei Fälle unterscheiden, die den drei Möglichkeiten entsprechen, welche Bewegung der Schreib-/Lesekopf durchführt.

Wir beginnen mit dem einfachsten Fall: Der Kopf führt keine Bewegung durch, d.h. $\delta(z, a) = (z', c, N)$ für $a, c \in \Gamma$, $z, z' \in Z$.

In diesem Fall nehmen wir das Paar $(za, z'c)$ in das MPCP auf.

Nun betrachten wir den Fall, dass der Kopf eine Bewegung nach rechts durchführt, d.h. $\delta(z, a) = (z', c, R)$ für $a, c \in \Gamma$, $z, z' \in Z$.

In diesem Fall nehmen wir das Paar (za, cz') in das MPCP auf.

Am schwierigsten ist der Fall der Linksbewegung des Schreib-/Lesekopfes, d.h. $\delta(z, a) = (z', c, L)$ für $a, c \in \Gamma$, $z, z' \in Z$.

In diesem Fall nehmen wir die Paare $(bza, z'bc)$ für alle $b \in \Gamma$ auf.

Genau genommen müsste man noch einige Spezialfälle betrachten (z.B. was passiert, wenn der Kopf den rechten oder linken Rand unserer Konfigurationsbeschreibung erreicht), aber wir überlassen diese Details ebenso wie den formalen Korrektheitsbeweis den interessierten Teilnehmern als Übung.

Dass das konstruierte MPCP genau dann lösbar ist, wenn die Turingmaschine M_w auf x hält, erläutern wir an der Tafel.

PCP ist unentscheidbar

Zu guter Letzt wollen wir die Reduktion $H \leq MPCP$ benutzen, um auch die Unentscheidbarkeit von PCP zu beweisen.

Der Hauptpunkt hierfür ist die Reduktion von MPCP auf PCP:

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

Damit erhalten wir den folgenden Satz:

Satz: PCP und MPCP sind unentscheidbar.

Nun müssen wir also das Lemma beweisen.