05.05.2023

Definition 3.14 (Postsches Korrespondenzproblem, Emil Post, 1946). Für ein Alphabet Σ sei eine Instanz des Postschen Korrespondenzproblems über Σ eine endliche Teilmenge $I \subseteq (\Sigma^+)^2$. Eine Lösung für eine solche Instanz ist eine endliche Folge $(u_1, v_1), \ldots, (u_n, v_n)$ von Paaren in I mit $n \geq 1$, so dass

$$u_1 \ldots u_n = v_1 \ldots v_n$$

Gibt es eine Lösung für eine Instanz des Postschen Korrespondenzproblems, so heißt diese Instanz lösbar.

Das Postsche Korrespondenzproblem über einem Alphabet Σ, kurz PKP_Σ ist die Menge aller lösbaren Instanzen des Postschen Korrespondenzproblems über Σ.

Für ein Alphabet Σ sei eine Instanz des modifizierten Postschen Korrespondenzproblems über Σ ein Paar (p, I), wobei $I \subseteq (\Sigma^+)^2$ eine endliche Teilmenge und $p \in I$ ein Paar von Wörtern ist. Eine Lösung für eine solche Instanz ist eine endliche Folge $(u_1, v_1), \ldots, (u_n, v_n)$ von Paaren in I, so dass

$$p = (u_1, v_1) \qquad \text{und} \qquad u_1 \dots u_n = v_1 \dots v_n.$$

Gibt es eine Lösung für eine Instanz des modifizierten Postschen Korrespondenzproblems so heißt diese Instanz lösbar. Das modifizierte Postsche Korrespondenzproblem über einem Alphabet Σ, kurz $MPCP_\Sigma$ ist die Menge aller lösbaren Instanzen des modifizierten Postschen Korrespondenzproblems über Σ.

Plan: Für Alphabet mit $|\Sigma| \geq 2$:

$$H_{init} \overset{(3)}{\leq_m} MPCP_T \overset{(2)}{\leq_m} PCP_T \overset{(1)}{\leq_m} PCP_\Sigma$$

Lemma 3.15. Für Alphabete Σ und T mit $|\Sigma| \geq 2$ gilt $PCP_T \leq_m PCP_\Sigma$

Beweis. Wir suchen eine effektive Transformation, die jede Instanz I des Postschen Korrespondenzproblems über T in eine Instanz I' des Postschen Korrespondenzproblems über Σ transformiert, so dass I genau dann lösbar ist, wenn I' lösbar ist.

Seien $a_1, a_2 \in \Sigma$ verschieden und seien $b_1, \dots, b_{|\Gamma|}$ die Elemente von Γ.
Es bezeichne $\varphi : \Gamma^* \to \Sigma^*$ den eindeutigen Homomorphismus von Sprachen mit $\varphi(b_i) = a_1^i a_2$ für alle $i \in [|\Gamma|]$. Gegeben eine solche Instanz I wie oben sei $I' := \{ (\varphi(u), \varphi(v)) : (u,v) \in I \}$.

Die Funktion, die geeignete Codes von Instanzen I auf geeignete Codes von Instanzen I' abbildet ist berechenbar.

Ist $(u_1, v_1), \dots, (u_n, v_n)$ eine Lösung von I, so gilt

$$\varphi(u_1) \dots \varphi(u_n) = \varphi(u_1 \dots u_n) = \varphi(v_1, \dots, v_n) = \varphi(v_1) \dots \varphi(v_n)$$

und somit ist $(\varphi(u_1), \varphi(v_1)), \dots, (\varphi(u_n), \varphi(v_n))$ eine Lösung von I'. Die Instanz I' ist also lösbar wenn I lösbar ist.

Ist $(u_1', v_1'), \dots, (u_n', v_n')$ eine Lösung von I', so gibt es eine Folge $(u_1, v_1), \dots, (u_n, v_n)$ von Paaren in I mit $\varphi(u_i) = u_i'$ und $\varphi(v_i) = v_i'$ für alle $i \in [n]$, also mit

$$\varphi(u_1 \dots u_n) = u_1' \dots u_n' = v_1' \dots v_n' = \varphi(v_1 \dots v_n)$$

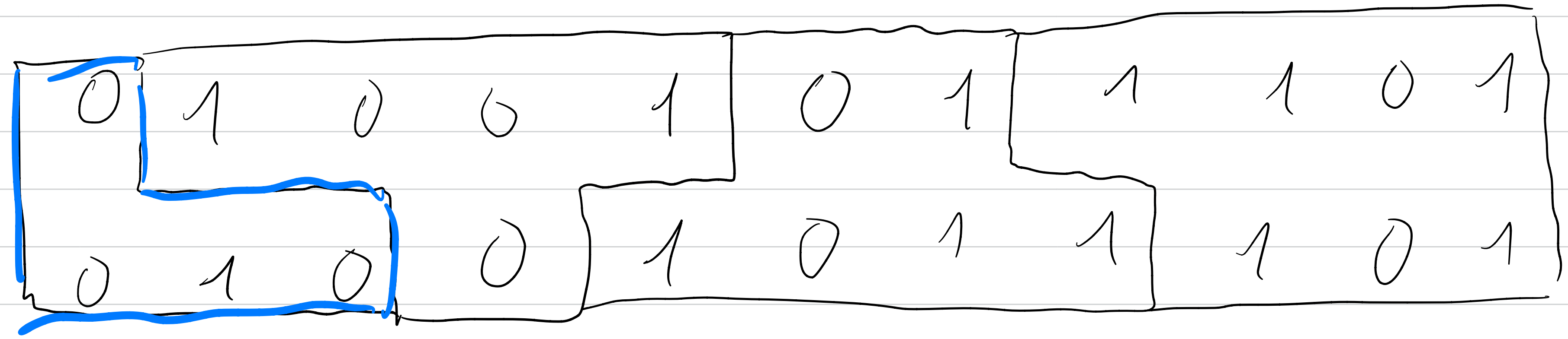
Da $\varphi|_{\Gamma}$ injektiv und $\varphi(\Gamma)$ präfixfrei ist, ist φ injektiv (siehe Übung), folglich gilt $u_1 \dots u_n = v_1 \dots v_n$ und somit ist $(u_1, v_1), \dots, (u_n, v_n)$ eine Lösung von I. Die Instanz I ist also lösbar wenn I' lösbar ist. □

Lemma 3.16. Für jedes Alphabet Σ mit $|\Sigma| \geq 2$ gilt $MPCP_{\Sigma} \leq_m PCP_{\Sigma}$.

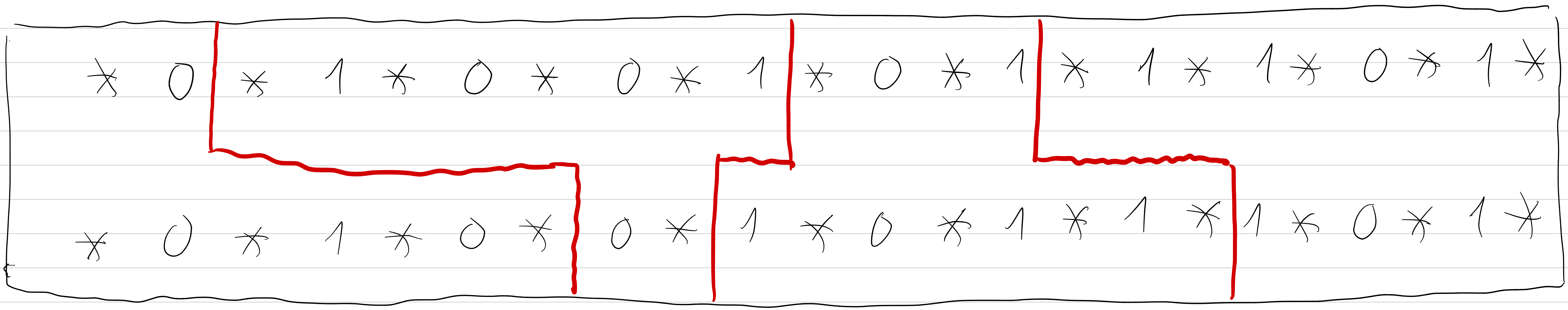
Beweis. Sei Σ ein Alphabet mit $|\Sigma| \geq 2$.
Nach Lemma 3.14 genügt es ein Alphabet Γ zu finden, so dass $MPCP_{\Sigma} \leq_m PCP_{\Gamma}$ gilt.

Wir suchen eine effektive Transformation, die jede Instanz (p, I) des modifizierten Postschen Korrespondenzproblems über Σ in eine Instanz I' des Postschen Korrespondenzproblems über einem geeigneten Alphabet Γ transformiert, so dass (p, I) genau dann lösbar ist, wenn I' lösbar ist.

Idee:



$* \notin \Sigma$



Betrachte die Homomorphismen von Sprachen $\sigma_\rightarrow, \sigma_\leftarrow : \Sigma^* \to (\Sigma \cup \{*\})^*$ mit $\sigma_\rightarrow(a) = a*$ und $\sigma_\leftarrow(a) = *a$ für alle $a \in \Sigma$.

Für jede Instanz $(p, I) = ((u_1, v_1), I)$ wie oben sei

$$I' := \{(\sigma_{\leftarrow}(u_1), *\sigma_{\rightarrow}(v_1))\} \cup \{(\sigma_{\leftarrow}(u), \sigma_{\rightarrow}(v)) : (u,v) \in I\}$$

$$\cup \{\sigma_{\leftarrow}(u)*, \sigma_{\rightarrow}(v)) : (u,v) \in I\}$$

Die Funktion die geeignete Codes von Instanzen (p, I) auf geeignete Codes der zugehörigen Instanzen I' abbildet ist berechenbar.

Gibt es eine Lösung $(u_1, v_1), \dots, (u_n, v_n)$ von (p, I), dann ist

$$\sigma_{\leftarrow}(u_1) \dots \sigma_{\leftarrow}(u_n)* = \sigma_{\leftarrow}(u_1 \dots u_n)*$$

$$= \sigma_{\leftarrow}(v_1 \dots v_n)*$$

$$= *\sigma_{\rightarrow}(v_1 \dots v_n)$$

$$= *\sigma_{\rightarrow}(v_1) \dots \sigma_{\rightarrow}(v_n)$$

und folglich ist

$(\sigma_{\leftarrow}(u_1), * \sigma_{\rightarrow}(v_1)), (\sigma_{\leftarrow}(u_2), \sigma_{\rightarrow}(v_2)), \ldots, (\sigma_{\leftarrow}(u_{n-1}), \sigma_{\rightarrow}(v_{n-1})),$

$(\sigma_{\leftarrow}(u_n) *, \sigma_{\rightarrow}(v_n))$

eine Lösung von I'.

Es bleibt zu zeigen, dass (p, I) lösbar ist, wenn I' lösbar ist.
Sei $\tau : (\Sigma \cup \{*\})^* \to \Sigma^*$ der Homomorphismus von Sprachen mit $\tau|_\Sigma = id_\Sigma$ und $\tau(*) = \lambda$.
Für $(u', v') \in I'$ gilt $(\tau(u'), \tau(v')) \in I$.
Sei $(u_1', v_1'), \ldots, (u_n', v_n')$ eine Lösung von I' und $(u_i, v_i) = (\tau(u_i'), \tau(v_i'))$ für $i \in [n]$.
Es gilt

$$\tau(u_1') \ldots \tau(u_n') = \tau(u_1' \ldots u_n') = \tau(v_1' \ldots v_n') = \tau(v_1') \ldots \tau(v_n')$$

und somit ist $(u_1, v_1), \ldots, (u_n, v_n)$ eine Lösung von I als Instanz des Postschen Korrespondenzproblems über Σ. Es genügt also zu zeigen, dass $(u_1, v_1) = p$ gilt.
Sei $p' := (\sigma_{\leftarrow}(u_1), * \sigma_{\rightarrow}(v_1))$. Für $(u', v') \in I' \setminus \{p'\}$ gilt $u'(1) \neq v'(1)$,
da $(u_1', v_1'), \ldots, (u_n', v_n')$ eine Lösung von I' ist gilt also $(u_1', v_1') = p'$ und damit

$(u_1, v_1) = (T(u_1'), T(v_1')) = p.$ $\square$

Lemma 3.17 Für jedes Alphabet Σ mit $|\Sigma| \geq 2$ gilt $H_{\text{ein}} \leq_m MPCP_{\{\square, 0, 1, *, \#, +\}}$

Beweisskizze. Wir suchen eine effektive Transformation, die jede natürliche Zahl e auf eine Instanz (p_e, I_e) des modifizierten Postschen Korrespondenzproblems über $\{\square, 0, 1, *, \#, +\}$ abbildet, so dass $M_e(\lambda)\downarrow$ genau dann gilt, wenn (p_e, I_e) lösbar ist.
Sei $e \in \mathbb{N}_0$. Sei Q die Zustandsmenge und Δ die Übergangsrelation von M_e.
Es gelte also $M_e = (Q, \Sigma, \Gamma, \Delta, 1, F)$ für $\Sigma = \{0,1\}$, $\Gamma = \{\square, 0, 1\}$, $s = 0$, $F = \{0\}$.

Für eine Instanz (p, I) des modifizierten Postschen Korrespondenzproblems über einem Alphabet bezeichnen wir eine Folge $p = (u_1, v_1), \dots, (u_n, v_n)$ für die $u_1 \dots u_n \sqsubseteq v_1 \dots v_n$ oder $v_1 \dots v_n \sqsubseteq u_1 \dots u_n$ gilt als partielle Lösung von (p, I)
Wir wollen (p_e, I_e) so wählen, dass partielle Lösungen von (p_e, I_e) partiellen Rechnungen von M_e entsprechen. Dabei codieren wir eine Konfiguration $(q, w, p) \in Q \times (\Gamma^*) \times \mathbb{N}_0$ von M_e durch das Wort

$\mathrm{code}(q, w, p) := \# w(1) \ldots w(p-1) * \mathrm{bin}(q) * w(p) \ldots w(|w|) \#.$

Im Wesentlichen wollen wir erreichen, dass es genau dann für ein Wort w eine partielle Lösung $(u_1, v_1), \ldots, (u_n, v_n)$ von (P_e, I_e) mit $w = v_1 \ldots v_n$ gibt, wenn w Präfix der Konkatenation $\mathrm{code}(C_1) \ldots \mathrm{code}(C_n)$ der Codes der Konfigurationen einer partiellen Rechnung $C_1, \ldots, C_n$ von M_e bei Eingabe λ ist.

Eine solche partielle Lösung soll genau dann zu einer Lösung von (P_e, I_e) vervollständigt werden können, wenn die durch w beschriebene partielle Rechnung mit einer Stoppkonfiguration endet, also eine Rechnung ist.

Dann ist (P_e, I_e) genau dann lösbar, wenn die Rechnung von M_e zur Eingabe λ endlich ist.

Für $q \in Q$ sei $\hat{q} := * \mathrm{bin}(q) *$