Technische Universität Braunschweig

Theoretische Informatik 2

Arne Schmidt

Kapitel 5 – Satz von Rice

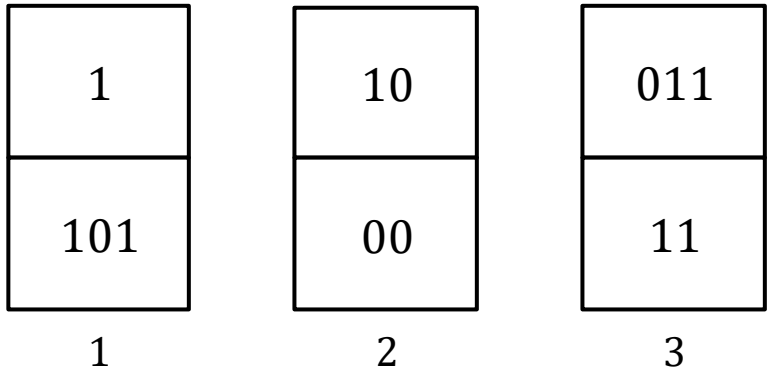

Welche Eigenschaften von Sprachen sind eigentlich unentscheidbar?
Fast alle!

Kapitel 5.1 – Das Postsche Korrespondenzproblem (PCP)

Das Postsche Korrespondenzproblem (PCP)

Lege Kopien der Kacheln so nebeneinander, das oben und unten derselbe Binärstring entsteht.

Geht das in diesem Beispiel?

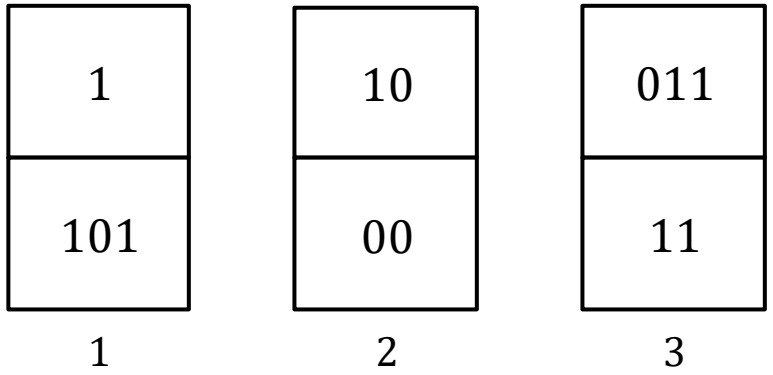


Das Postsche Korrespondenzproblem (PCP)

Lege Kopien der Kacheln so nebeneinander, das oben und unten derselbe Binärstring entsteht.

Geht das in diesem Beispiel?

Ja! Sequenz ist 1323

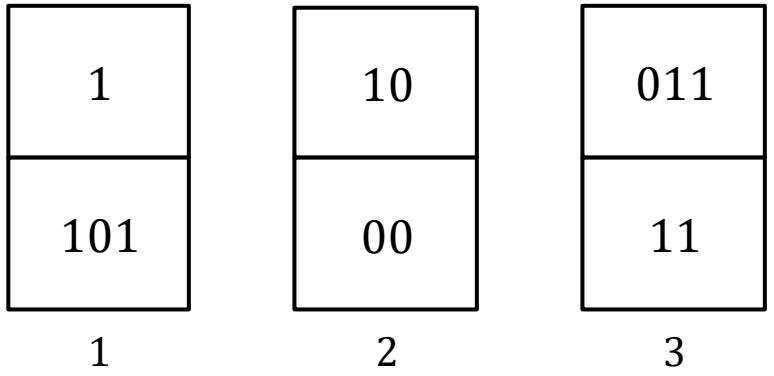


1	011	10	011	101110011
101	11	00	11	101110011
1	3	2	3	

Definition 5.1 – Das Postsche Korrespondenzproblem (PCP)

Lege Kopien der Kacheln so nebeneinander, das oben und unten derselbe Binärstring entsteht.

Geht das in diesem Beispiel?



<u>Postsches Korrespondenzproblem (PCP)</u>
Gegeben: Eine endliche Sequenz von Tupeln aus Wörtern $(x_1, y_1), \dots, (x_k, y_k)$.
Frage: Gibt es eine endliche, nicht-leere Sequenz von Indizes $i_1 \dots i_n$ mit

$$x_{i_1} x_{i_2} \dots x_{i_n} = y_{i_1} y_{i_2} \dots y_{i_n}?$$

Unentscheidbarkeit

Theorem 5.3
Das PCP ist unentscheidbar.

Wir betrachten zunächst eine modifizierte Variante.

Modifiziertes Postsches Korrespondenzproblem (MPCP)
Gegeben: Eine endliche Sequenz von Tupeln aus Wörtern $(x_1, y_1), \dots, (x_k, y_k)$.
Frage: Gibt es eine endliche, nicht-leere Sequenz von Indizes $i_1 \dots i_n$ mit

$$x_{i_1} x_{i_2} \dots x_{i_n} = y_{i_1} y_{i_2} \dots y_{i_n} \text{ und } i_1 = 1?$$

Lemma 5.4
MPCP $\leq$ PCP.

Beweisskizze

Lemma 5.4
MPCP $\leq$ PCP.

Für $w = a_1 a_2 \dots a_m \in \Sigma^*$ betrachte

$$\overline{w} = \#a_1\#a_2\# \dots \#a_m\#$$
$$w` = \#a_1\#a_2\# \dots \#a_m$$
$$w´ = a_1\#a_2\# \dots \#a_m\#$$

Für eine gegebene MPCP Instanz $K = (x_1, y_1), \dots, (x_k, y_k)$ konstruiere die Instanz

$$f(K) = (\overline{x_1}, y_1`), (x_1´, y_1`), (x_2´, y_2`), \dots, (x_k´, y_k`), (\$, \#\$)$$

"=>"

Hat K eine Lösung $i_1 = 1, i_2, \dots i_n$, dann hat $f(K)$ die Lösung $1, i_2 + 1, i_3 + 1, \dots, i_n + 1, k + 2$.

Beweisskizze

Lemma 5.4
MPCP $\leq$ PCP.

Für $w = a_1 a_2 \dots a_m \in \Sigma^*$ betrachte

$$\overline{w} = \#a_1\#a_2\# \dots \#a_m\#$$
$$w` = \#a_1\#a_2\# \dots \#a_m$$
$$w´ = a_1\#a_2\# \dots \#a_m\#$$

Für eine gegebene MPCP Instanz $K = (x_1, y_1), \dots, (x_k, y_k)$ konstruiere die Instanz

$$f(K) = (\overline{x_1}, y_1`), (x_1´, y_1`), (x_2´, y_2`), \dots, (x_k´, y_k`), (\$, \#\$)$$

"<="

Betrachte eine Lösung von $f(K)$ minimaler Länge $i_1 \dots i_n \in \{1, \dots, k+2\}^*$.
Dann ist nach Konstruktion $i_1 = 1$ und $i_n = k + 2$.
1 und k+2 tauchen nur einmal auf! (Warum?)
Damit ist $1, i_2 - 1, \dots, i_{n-1} - 1$ eine Lösung für K.

Unentscheidbarkeit

Theorem 5.3
Das PCP ist unentscheidbar.

Wir betrachten zunächst eine modifizierte Variante.

Modifiziertes Postsches Korrespondenzproblem (MPCP)
Gegeben: Eine endliche Sequenz von Tupeln aus Wörtern $(x_1, y_1), \dots, (x_k, y_k)$.
Frage: Gibt es eine endliche, nicht-leere Sequenz von Indizes $i_1 \dots i_n$ mit

$$x_{i_1} x_{i_2} \dots x_{i_n} = y_{i_1} y_{i_2} \dots y_{i_n} \text{ und } i_1 = 1?$$

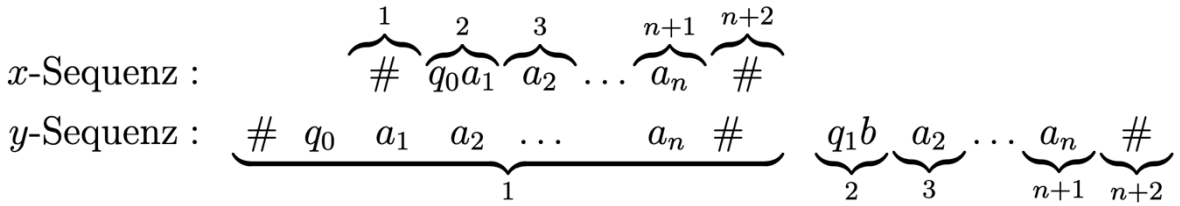
Lemma 5.4
MPCP $\leq$ PCP.

Lemma 5.5
ACCEPT $\leq$ MPCP.

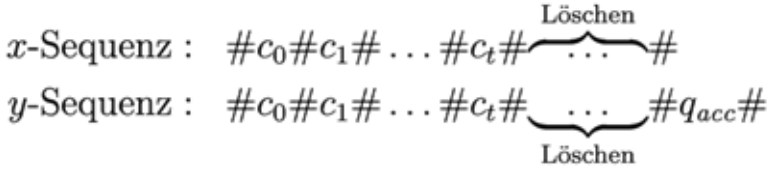
Beweisidee

Lemma 5.5
ACCEPT $\leq$ MPCP.

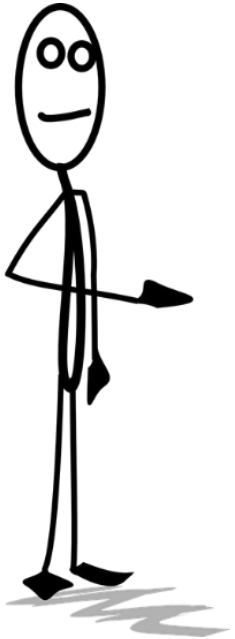
Codiere für die Eingabe $w\#x$ von ACCEPT die Konfigurationen $c_0 \to c_1 \to \ldots \to c_t$ von M_w.
MPCP soll dann eine Lösung der Form $\#c_0\#c_1\# \ldots \#c_t\#c_t'\# \ldots \#q_{acc}\#\#$ besitzen.
Dabei erhält y eine Konfiguration Vorsprung:



Ist c_t erreicht, muss dieser Vorsprung wieder behoben werden



Bemerkung 5.6



Für $k \in \mathbb{N}$ ist PCPk das PCP für Instanzen mit genau k Paaren.

Für $k = 1$ ist es trivial entscheidbar.
Für $k = 2$ ist es auch entscheidbar.

Für $k \in \{3,4\}$ ist es unbekannt.

Für $k \geq 5$ ist es unentscheidbar.

Kapitel 5.2 – Satz von Rice

Nicht-Triviale Eigenschaften

Definition 5.7
Sei Σ ein Alphabet. Wir bezeichnen mit $\mathrm{RE}(\Sigma)$ die Menge aller rekursiv-aufzählbaren (semi-entscheidbaren) Sprachen über Σ, also die Menge aller Sprachen $\mathcal{L}$, zu denen eine TM M mit $\mathcal{L}(M) = \mathcal{L}$ existiert.

Eine **Eigenschaft** P der Sprachen in $\mathrm{RE}(\Sigma)$ ist eine Funktion

$$P: \mathrm{RE}(\Sigma) \to \{0,1\} \mathrel{\widehat{=}} \mathbb{B} = \{\mathrm{false}, \mathrm{true}\}.$$

Wir sagen, dass eine Sprache $\mathcal{L} \in \mathrm{RE}(\Sigma)$ Eigenschaft P hat, falls $P(\mathcal{L}) = 1$ gilt.

Eine Eigenschaft heißt **trivial**, wenn P eine konstante Funktion ist. Andernfalls heißt die Eigenschaft **nicht-trivial**.

Bemerkungen

Für nicht-triviale Eigenschaften existieren also Sprachen $\mathcal{L}, \mathcal{L}'$ mit $P(\mathcal{L}) = 1$ und welche mit $P(\mathcal{L}) = 0$.

Wir können die Sprache über eine definierende TM beschreiben, damit ist P die Sprache

$$P = \{ w \in \{0,1\}^* \mid P(\mathcal{L}(M_w)) \}$$

Beachte: P beschreibt Eigenschaften von Sprachen; nicht von Turing-Maschinen!

Beispiele 5.8

Nicht-Triviale Eigenschaften

- $\mathcal{L} = \mathcal{L}(M_w)$ ist endlich.
- $\mathcal{L} = \mathcal{L}(M_w)$ ist regulär.
- $\mathcal{L} = \mathcal{L}(M_w)$ ist kontextfrei.
- $\mathcal{L} = \mathcal{L}(M_w)$ ist entscheidbar.
- $10110 \in \mathcal{L}$, d.h. M_w akzeptiert Eingabe 10110.
- $\mathcal{L} = \Sigma^*$, d.h. M_w ist universell.

Eigenschaften von TMs

- M_w hat 481 Kontrollzustände.
- Die Berechnung von M_w auf Eingabe 10110 hält nach höchstens 10 Schritten.
- M_w ist ein Entscheider.
- Es gibt eine kleinere TM mit derselben Sprache

Triviale Eigenschaften

- $\mathcal{L}$ ist Bild einer totalen berechenbaren Funktion.
- $\mathcal{L}$ ist nicht-semi-entscheidbar.

Satz von Rice

Theorem 5.9
Jede nicht-triviale Eigenschaft der semi-entscheidbaren Sprachen ist unentscheidbar.

Beweis: Tafel!

Achtung: Der Beweis sagt nicht aus, ob die Sprache nicht semi-entscheidbar oder nicht co-semi-entscheidbar ist.

Satz von Rice mit nicht-monotonen Eigenschaften

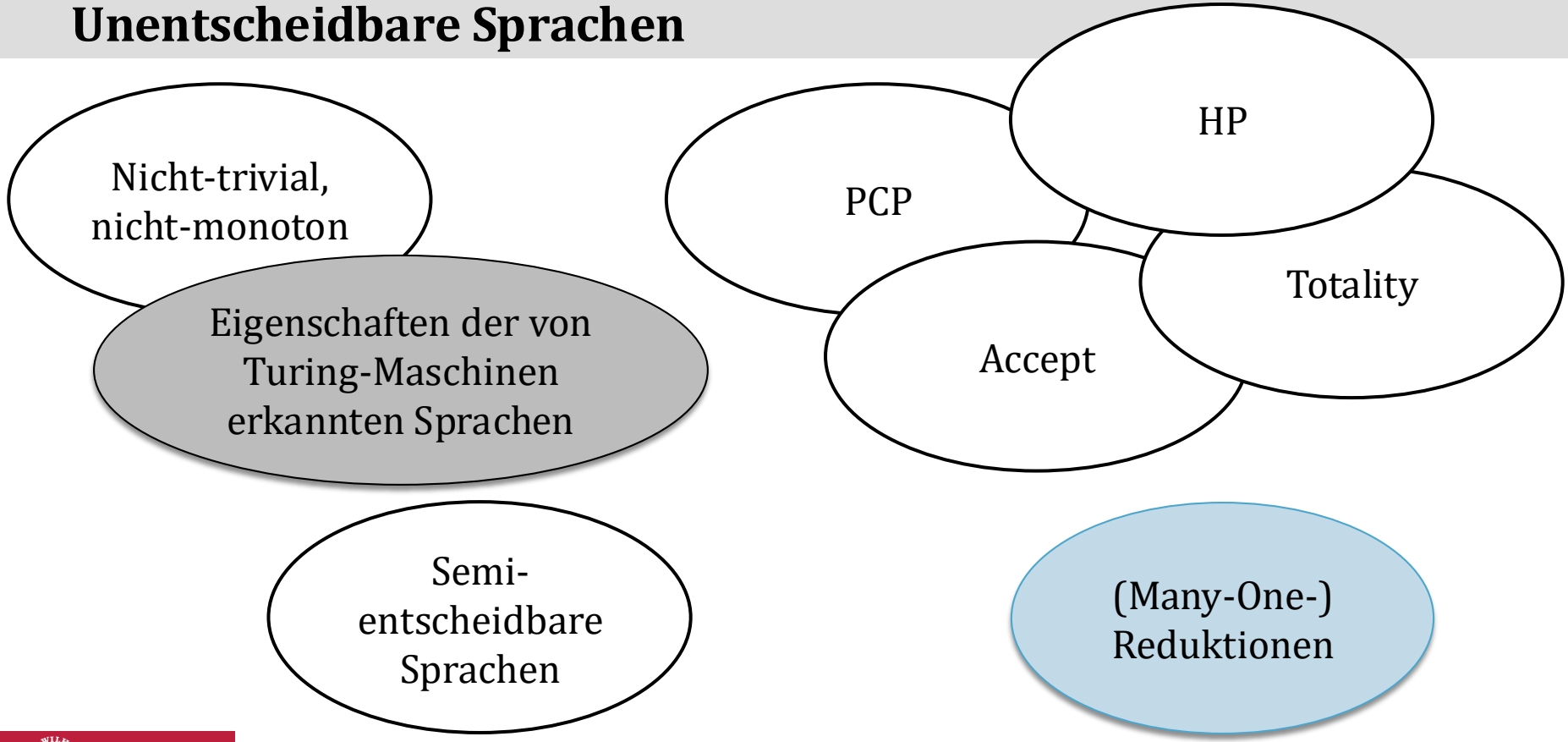
Eine Eigenschaft P heißt **monoton**, wenn für alle Sprachen $\mathcal{L}_1, \mathcal{L}_2 \in RE(\Sigma)$ gilt, dass

$$\mathcal{L}_1 \subseteq \mathcal{L}_2 \Rightarrow P(\mathcal{L}_1) \leq P(\mathcal{L}_2)$$

Andernfalls heißt die Eigenschaft **nicht-monoton**.

Theorem 5.10
Jede nicht-monotone Eigenschaft der semi-entscheidbaren Sprachen ist nicht semi-entscheidbar.

Unentscheidbare Sprachen



Nächstes Kapitel

Es gibt viele unentscheidbare Probleme.

Was können wir über **entscheidbare** Probleme aussagen?

Wie **effizient** können wir diese lösen?

Det. vs Nicht-Det.

Speicher vs. Laufzeit

1-Band vs. m-Band