Satz (Rice)

Es sei $\mathcal{R}$ die Klasse aller Turing-berechenbaren Fkt.
Sei $S \subseteq \mathcal{R}$ und $S \neq \emptyset$, $S \neq \mathcal{R}$. Dann ist die Sprache

$$C(S) = \{ w \in \{0,1\}^* \mid \text{die von } M_w \text{ berechnete Funktion liegt in } S \}$$

unentscheidbar.

Bew.: Sei $\Omega \in \mathcal{R}$ die überall undefinierte Funktion.
Es gibt 2 Fälle: Entweder $\Omega \in S$ oder $\Omega \notin S$.
Wir beschränken uns auf den Fall $\Omega \notin S$ ($\Omega \in S$ ist analog).
Wir wollen zeigen: $E \leq C(S)$.
Zu zeigen: Es ex. eine totale, berechenbare Fkt. $f : \{0,1\}^* \to \{0,1\}^*$
so dass

$$w \in E \quad \text{gdw} \quad f(w) \in C(S).$$

Nach Voraussetzung ist $S \neq \emptyset$. Wähle $g^* \in S$ beliebig.
Weil $g^*$ berechenbar ist, ex. eine TM $M^*$, die $g^*$ berechnet.

Zu einem bel. Wort $\underline{w \in \{0,1\}^*}$ konstruieren wir die folgende TM $M_w^*$:

> $M_w^*$, angesetzt auf ein $y \in \{0,1\}^*$, verhält sich wie $\underline{M_w}$ angesetzt auf das leere Band. Falls $M_w$ anhält, verhält sie sich hinterher wie $M^*$ angesetzt auf $y$. Ansonsten behaut sie in ihrer Totschleife.

Falls $M_w$ auf dem leeren Band stoppt, dann berechnet $M_w^*$ die Funktion $\underline{g^*}$. $(g^* \in S)$
Falls $M_w$ nicht auf dem leeren Band stoppt, dann berechnet $M_w^*$ die überall undefinierte Funktion $\Omega$. $(\Omega \notin S)$

$f$ sei jetzt die Fkt., die zu jedem Wort $w$ die Codierung von $M_w^*$ berechnet: $f(w) = \underline{\text{code}(M_w^*)}$.

$\underline{w \in E}$ $\Rightarrow$ $M_w$, angesetzt auf das leere Band, hält

$\Rightarrow$ $M_w^*$ berechnet $g^*$ $\quad (g^* \in S)$

$\Rightarrow$ die von $M_w^* = M_{f(w)}$ berechnete Fkt. liegt in $S$

$\Rightarrow$ $\underline{f(w) \in C(S)}$.

Umgekehrt

$\underline{w \notin E}$ $\Rightarrow$ $M_w$, angesetzt auf das leere Band, hält nicht

$\Rightarrow$ $M_w^*$ berechnet $\Omega$ $\quad (\Omega \notin S)$

$\Rightarrow$ die von $M_w^* = M_{f(w)}$ berechnete Fkt. liegt nicht in $S$

$\Rightarrow$ $\underline{f(w) \notin C(S)}$.

Da $f$ auch total und berechenbar ist, ist $f$ tatsächlich die geforderte Reduktion. $\square$

Bem: Da Sprachen durch ihre charakteristische Fkt. beschrieben werden können, gilt das Ergebnis für alle entscheidbaren Spracheigenschaften.

Bsp: Ist die von einer vorliegenden TM akzeptierten Sprache regulär?

## 2.7 Postsches Korrespondenz

| Typ | A | B | C | D |
|---|---|---|---|---|
| | L | ELT | OW | HAL |
| | L | T | LOWEL | HA |

Gegeben: Diverse Spielsteintypen

<u>Gefragt</u>: Gibt es eine <u>nicht-leere Sequenz</u> von Steinen, so dass oben und unten das gleiche steht?

<u>Wiederholungen</u> von Steintypen und Weglassungen sind erlaubt.

| | | | |
|---|---|---|---|
| HAL | L | OW | ELT |
| HA | L | LOWEL | T |

| | | |
|---|---|---|
| L | L | L |
| L | L | L |

PCP (Postsche Korrespondenzproblem)

Gegeben: Eine endliche Folge von Wortpaaren:

$$(x_1, y_1), \dots, (x_k, y_k)$$

über einem Alphabet $\Sigma$ mit $x_i, y_i \in \Sigma^+$.

Gefragt: Gibt es eine Folge von Indizes

$$i_1, i_2, \dots, i_n, \quad i_j \in \{1, \dots, k\}, \quad n \geq 1$$

so dass:

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

Ist das der Fall, heißt $i_1, \dots, i_n$ Lösung des PCPs

$(x_1, y_1), \dots, (x_k, y_k)$.

## MPCP

Gegeben: Eine endliche Folge von Wortpaaren über einem Alphabet $\Sigma$

Gefragt: Gibt es eine Lösung $i_1, i_2, \ldots, i_n$ mit $i_1 = 1$?

**Lemma** $MPCP \leq PCP$

Bew: Wir geben eine totale und berechenbare Funktion $f$ an, die jeder MPCP-Instanz $K$ eine PCP-Instanz zuordnet, so dass

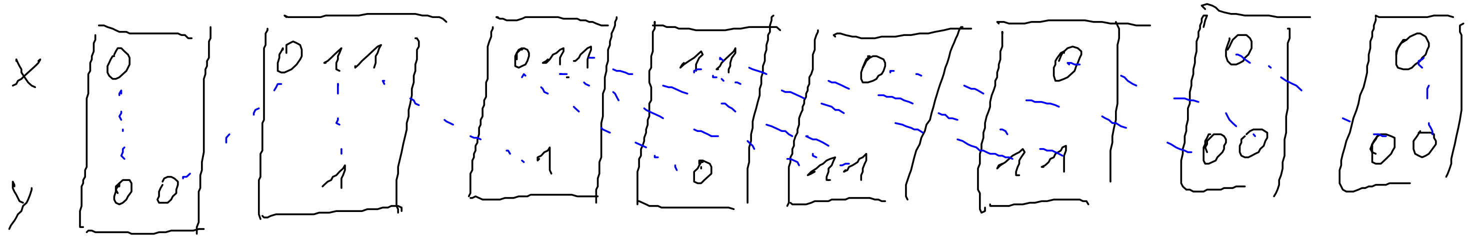
$K$ hat eine Lösung mit $i_1 = 1$

gdw $f(K)$ hat irgendeine Lösung.

Bsp:

$K = ((0, 00), (011, 1), (11, 0), (0, 11))$

Eine Lösung: $(1, 2, 2, 3, 4, 4, 1, 1)$




PCP ist offensichtlich semi-entscheidbar.

PCP ist aber unentscheidbar. Um das zu zeigen, wählen wir einen Umweg über das MPCP (Spezialisierung des PCPs). Wir zeigen dann, dass <u>MPCP $\leq$ PCP</u> und $H \leq$ MPCP, d.h. wg. <u>Transitivität</u> der Reduktionsbez. folgt dann $H \leq$ PCP, d.h. dass PCP muss unentscheidbar.

Für eine MPCP-Instanz $K = ((x_1, y_1), \dots, (x_k, y_k))$ über $\Sigma$ erweitern wir das Alphabet um zwei neue Zeichen # und $.

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

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

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

Dann setze

Index: $0 \quad 1 \quad 2 \quad k \quad k+1$

$$f(K) := (\underline{(\#\grave{x}_1, \acute{y}_1)}, (\grave{x}_1, \acute{y}_1), (\grave{x}_2, \acute{y}_2), \dots, (\grave{x}_k, \acute{y}_k), \underline{(\$, \#\$)})$$

k+2 Wortpaare

2 Varianten

neuer Abschluss

Offenbar ist f total und berechenbar. Zu zeigen:

$$K \in MPCP \ \underline{\text{gdw.}} \ f(K) \in PCP$$

$\Rightarrow$: Sei $(1, i_2, \dots, i_n)$ eine Lösung für das MPCP $K$.

D.h. $x_1 x_{i_2} \dots x_{i_n} = y_1 y_{i_2} \dots y_{i_n}$

$= a_1 a_2 \dots a_m$ für geeignete $a_i \in \Sigma$

Startwortpaar Abschlusswortpaar

Dann ist $(0, i_2, \dots, i_n, k+1)$ eine Lösung für das PCP $f(K)$, denn

$$\#\grave{x}_1 \grave{x}_{i_2} \dots \grave{x}_{i_n} \$ = \# a_1 \# a_2 \dots \# a_m \# \$$$

$$= \acute{y}_1 \acute{y}_{i_2} \dots \acute{y}_{i_n} \# \$$$

$\Leftarrow$: Sei $(i_1, \dots, i_n)$ für das PCP $f(K)$. OBdA ist diese Lösung nicht verkürzbar. Zu zeigen:

$(1, i_2, \dots, i_{n-1})$ ist eine Lösung des MPCP $K$.

Beobachtungen:

(a) Nur $(\#\bar{x}_1, \bar{y}_1)$ beginnt mit gleichen Zeichen $(\#)$

$\Rightarrow i_1 = 0$ ⟸ Anfangspaar

(b) Nur $(\$, \#\$)$ endet mit den gleichen Zeichen $(\$)$

$\Rightarrow i_n = k+1$ ⟸ Schlusspaar

(c) Nur $(\#\bar{x}_1, \bar{y}_1)$ ist das Tupel mit x-Wert,

das mit $\#$ beginnt.

$\Rightarrow i_j \neq 0$ für $j \geq 2$ (da sonst $\#\#$ hintereinander)

(d) $\$$ kommt nur in $(\$, \#\$)$ vor

$\Rightarrow i_j \neq k+1$ für $j < n$

D.h., da

$$\#\bar{x}_1 \bar{x}_{i_2} \ldots \bar{x}_{i_{n-1}} \$ = \bar{y}_1 \bar{y}_{i_2} \ldots \bar{y}_{i_{n-1}} \#\$$$

folgt bei Streichen von $\#$ von $\$$:

$$x_1 x_{i_2} \ldots x_{i_{n-1}} = y_1 y_{i_2} \ldots y_{i_{n-1}}$$

D.h. $(1, i_2, \ldots, i_{n-1})$ ist tatsächlich eine Lösung des MPCP. $\square$