1.8 Das Halte–Problem und die Reduzierbarkeit

- Kennenlernen unentscheidbarer Probleme.
  Besonders berühmt: Das Halteproplem für TM .
  Dazu Kodierung der TM $M = (Q, \Sigma, \Gamma, \delta, q_0, \square, F)$ als Wort über {0,1}

1. Kodierung von M als Wort über {0,1,# }:

   Sei $Q = \{q_0, \ldots, q_n\}$
   $\Gamma = \{a_0, \ldots a_k\}$

   Schreibe $\delta(q_i, a_j) = (q_{i'}, a_{j'}, y)$
   als

   $$w_{i,j,i',j',y} = \#\#bin(i)\#bin(j)\#bin(i')\#bin(j')\#bin(m) \quad \text{mit } m = \begin{cases} 0 & y = L \\ 1 & y = R \\ 2 & y = N \end{cases}$$

   Kodierung von M durch Konkatenation aller Worte $w_{i,j,i',j',y}$, die zu δ gehören.

2. Kodierung von M durch ein Wort über { 0,1}:
   Kodierung mit Hilfe von

   $0 \mapsto 00$

   $1 \mapsto 01$

   $\# \mapsto 11$

   $w_{i,j,i',j',y}$ durch ein Wort über {0,1}

Sei M_0 eine fixierte TM

$$w \in \{0,1\}^* \mapsto M_w = \begin{cases} M & \text{falls } w \text{ Codewort von } M \text{ ist} \\ 0 & \text{sonst} \end{cases}$$

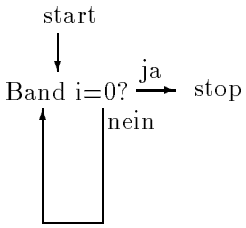
Definiton
Die folgende Sprache

$$K = \{w \in \{0,1\}^* \mid M_w \text{ angesetzt auf } w \text{ hält}\}$$

heißt *spezielles Halte–Problem.*

Satz.
Das spezielle Halte–Problem ist nicht entscheidbar.

Beweis.
Annahme: K ist entscheidbar.
$\Leftrightarrow \chi_K$ ist berechenbar mittles TM M.
Betrachte: TM M'



M' stoppt, falls M 0 ausgibt.
Gibt M 1 aus, geht M' in eine Endlos–Schleife.

Sei $w' \in \{0,1\}$ mit $M_{w'} = M$

Es gilt:
M' angesetzt auf w' hält.
$\Leftrightarrow$ M angesetzt auf w' gibt 0 aus.
$\Leftrightarrow \chi_K(w') = 0$ (Def. von M)
$\Leftrightarrow w' \in K$
$\Leftrightarrow M_{w'} = M'$ hält angesetzt auf w' nicht. (Widerspruch) ■

Das Reduktionskonzept ermöglicht eine "leichte" Übertragung dieses Resultats auf weitere Probleme:

Definition.
Seien $A, B \subseteq \Sigma^*$
A heißt *auf B reduzierbar* $(A \leq B)$, falls es eine totale und berechenbare Funktion $f : \Sigma^* \to \Sigma^*$ gibt mit

$$x \in A \Leftrightarrow f(x) \in B$$

für alle $x \in \Sigma^*$.

Lemma
(i) Gilt $A \leq B$ und ist B entscheidbar, so ist auch A entscheidbar.
(ii) Gilt $A \leq B$ und ist B semientscheidbar, so ist auch A semientscheidbar.

Beweis.
(i) Sei $A \leq B$ mittels f

Sei χ_B berechenbar
$\Leftrightarrow \chi_B \circ f$ ist berechenbar
Es gilt:

$$\chi_A(x) = \left\{ \begin{array}{ll} 1 & x \in A \\ 0 & x \notin A \end{array} \right\} = \left\{ \begin{array}{ll} 1 & f(x) \in B \\ 0 & f(x) \notin B \end{array} \right\} = \chi_B(f(x))$$

$\Leftrightarrow \chi_A$ ist berechenbar und A ist entscheidbar

(ii) ersetze in (i) χ durch χ' und 0 durch undefiniert. ■

Korollar
$A \leq B$ und A ist nicht entscheidbar.
$\Rightarrow$ B ist nicht entscheidbar.

Beweis.
Kontraposition von (i) ■

Definition.
Die Sprache

$$H = \{w\#x \mid M_w \text{ angesetzt auf } x \text{ hält}\}$$

heißt (allgemeines) *Halte–Problem.*

Satz.
Das Halte–Problem ist nicht entscheidbar.

Beweis.
Es reicht zu zeigen: $K \leq H$
wähle $f(w) = w\#w$
$\Rightarrow w \in K \Leftrightarrow f(w) \in H$ ■

Definiton
Die Sprache

$$H_0 = \{w \mid M_w \text{ angesetzt auf leeren Band hält}\}$$

heißt *Halte–Problem auf leeren Band.*

Satz.
Das Halte–Problem auf dem leeren Band H_0 ist nicht entscheidbar.

Beweis.
Es reicht zu zeigen: $H \leq H_0$.
Ordne $w\#x$ folgende TM zu:

gestartet mit leeren Band schreibt M x auf das Band, arbeitet dann wie M_w (angesetzt auf x).
Die Arbeitsweise von M gestartet mit nicht leeren Band ist unerheblich.

$f : w\#x \to$ Code von M.
f ist berechenbar Man kann f zu einer totalen und berechenbaren Funktion erweitern.

Es gilt:

$$\begin{aligned} w\#x \in H &\Leftrightarrow M_w \text{angestzt auf } x \text{ hält} \\ &\Leftrightarrow M \text{ angesetzt auf leerem Band hält} \\ &\Leftrightarrow f(w\#x) \in H_0 \end{aligned}$$

Satz von Rice.
Sei $\mathcal{R}$ die Klasse aller TM–berechenbaren Funktionen
Sei $\mathcal{S} \subset \mathcal{R}$, $\mathcal{S} \neq \emptyset$,
Dann ist die Sprache

$$C(\mathcal{S}) := \{w \mid \textit{die von } M_w \textit{ berechnetet Funktion liegt in } \mathcal{S}\}$$

unentscheidbar.

Beweis.
Sei $\Omega \in \mathcal{R}$ eine überall undefinierte Funktion.

1. Fall: $\Omega \in \mathcal{S}$
Wegen $\mathcal{S} \neq \mathcal{R}$ gibt es eine Funktion $q \in \mathcal{R} - \mathcal{S}$.
Sei Q eine TM , die q berechnet.
ordne $w \in \{0,1\}$ die TM M zu mit:

Angesetzt auf die Eingabe y ignoriert M diese zunächst und verhält sich wie M_w angesetzt auf das leere Band.
Falls diese Rechnung zu Ende kommt, so verhält sich M danach wie Q angesetzt auf y.

Für die von M berechnete Funktion g gilt:

$$g = \begin{cases} \Omega & \text{falls } M_w \text{ auf dem leeren Band nicht stoppt} \\ q & \text{sonst} \end{cases}$$

Betrachte: $f : w \mapsto$ Code von M
f ist total und berechenbar.

Es gilt:

$w \in H_0$ $\Rightarrow M_w$ stoppt angesetzt auf dem leeren Band.
$\Rightarrow M$ berechnet q.
$\Rightarrow$ die von $M_{f(w)}$ berechnete Funktion liegt nicht in $\mathcal{S}$.
$\Rightarrow f(w) \notin C(\mathcal{S})$

$w \notin H_0$ $\Rightarrow M_w$ stoppt angesetzt auf dem leeren Band nicht.
$\Rightarrow M$ berechnet Ω.
$\Rightarrow$ die von $M_{f(w)}$ berechnete Funktion liegt in $\mathcal{S}$.
$\Rightarrow f(w) \in C(\mathcal{S})$

d.h.: f vermittelt eine Reduktion :

$$\overline{H_0} \leq C(\mathcal{S})$$

wegen H_0 unentscheidbar
$\Rightarrow \overline{H_0}$ unentscheidbar
$\Rightarrow C(\mathcal{S})$ unentscheidbar

2. Fall:
Man zeigt analog $H_0 \leq C(\mathcal{S})$ ■

Anwendung:
Betrachte: $\mathcal{S} = \{f \in \mathcal{R} \mid f \text{ ist konstant}\}$
$\Rightarrow_{Satz von Rice} C(\mathcal{S}) = \{w \mid M_w \text{ berechnet eine konstante Funktion}\}$ ist nicht entscheidbar.

Es gibt verschiedene Klassen der "Unlösbarkeit":
Betrachte: Das Äquivalenzproblem für TM :

$$\ddot{A} = \{u\#w \mid M_w \text{ berechnet dieselbe Funktion wie } M_u\}$$

Es gilt:
$H \leq \ddot{A}$ aber nicht $\ddot{A} \leq H$

Man kann unendlich lange Folgen von Problemen $A_1, A_2, \ldots$ konstruieren mit

$$A_i \leq A_{i+1} \text{ aber nicht } A_{i+1} \leq A_i$$

1.9 Das Postsche Korrespondenz–Problem

Definition.
Das nachfolgend beschriebene Problem heißt *Postsches Korrespondenz–Problem (PCP).*

gegeben:	Eine endliche Folgen $(x_1, y_1), \ldots, (x_k, y_k)$ von Wortpaaren mit $x_i, y_i \in A^+$ (A endliche Alphabet)
gefragt:	Gibt es eine Folge von Indizes $i_1, \ldots, i_n \in \{1, \ldots, k\},\ n \geq 1$, mit $x_{i_1}, \ldots, x_{i_n} = y_{i_1}, \ldots, y_{i_n}$?

Beispiel.
Das Postsche Korrespondenz–Problem

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

also

$$\begin{array}{lll} x_1 = 1 & x_2 = 10 & x_3 = 011 \\ y_1 = 101 & y_2 = 00 & y_3 = 11 \end{array}$$

besitzt die Lösung (1,3,2,3), denn es gilt:

$$x_1 x_3 x_2 x_3 = 101110011 = y_1 y_3 y_2 y_3$$

PCP ist schwer.
z.B.: $K = ((001, 0), (01, 011), (01, 101), (10, 001))$
besitzt eine Lösung, aber die kürzeste besteht aus 66 Indizes!

PCP ist semi–entscheidbar:
Probiere alle möglichen Indexfolgen mit zunehmender Länge durch.

Satz.
Das Postsche Korrespondenz–Problem ist nicht entscheidbar.

Beweis.

Betrachte modifiziertes PCP:
MPCP

gegeben:	wie bei PCP
gefragt:	gibt es eine Lösung $i_1, \ldots, i_n$ mit $i_1 = 1$

Lemma
MPCP $\leq$ PCP

Beweis.
Sei # ein neues Symbol.
Für $w = a_1 \ldots a_m \in A^+$ sei

$$\bar{w} \quad = \quad \#a_1\#a_2\#\ldots\#a_m\#$$

$$\grave{w} = \#a_1\#a_2\#\ldots\#a_m$$
$$\acute{w} = a_1\#a_2\#\ldots\#a_m\#$$

Sei $K = ((x_1, y_1), \ldots, (x_k, y_k))$ die Eingabe von MPCP.
$\rightarrow f(K) = ((\bar{x_1}, \grave{y_1}), (\acute{x_1}, \grave{y_1}), (\acute{x_2}, \grave{y_2}), \ldots, (\acute{x_k}, \grave{y_k}), (\$, \#\$))$
f ist berechenbar.
f vermittelt eine Reduktion von MPCP auf PCP.

Behauptung.
K besitzt eine Lösung mit $i_1 = 1$
$\Leftrightarrow f(K)$ besitzt irgend eine Lösung.

Beweis.
($\rightarrow$) Besitzt K eine Lösung $(i_1, \ldots, i_n)$ mit $i_1 = 1$,
dann ist $(1, i_2 + 1, \ldots, i_n + 1, k + 2)$ eine Lösung für $f(K)$.
($\leftarrow$) Besitzt $f(K)$ eine Lösung $(i_1, \ldots, i_n)$,
so muß gelten:
$i_1 = 1, i_n = k + 2$ mit $i_j \in \{2, \ldots, k + 1\}$ für $2 \leq j \leq n + 1$
$\Rightarrow (1, i_2 - 1, \ldots, i_{n-1} - 1)$ ist Lösung für K.

Zur Unentscheidbarkeit von MPCP:

Lemma
$H \leq MPCP$

Beweis.
Sei $M = (Q, \Sigma, \Gamma, \delta, z_0, \Box, F)$ eine kodierte TM
$w \in \Sigma^+$ die Eingabe.
Suche eine allgemeine Vorschrift, die (M, w) eine Folge $(x_1, y_1), \ldots, (x_n, y_n)$ zuordnet mit
M angesetzt auf w stoppt $\Leftrightarrow (x_1, y_1), \ldots, (x_n, y_n)$ besitzt eine Lösung mit $i_1 = 1$

Konstruktion von MPCP über dem Alphabet $\Gamma \cup Q \cup \{\#\}$.
erstes Wortpaar: $(\#, \#q_0w\#)$
weitere Paare:

1. Kopieregeln:

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

2. Überführungsregeln:

   $$(qa, q'c) \quad \text{falls} \quad \delta(q, a) = (q', c, N)$$
   $$(qa, cq') \quad \text{falls} \quad \delta(q, a) = (q', c, R)$$

$$
\begin{array}{rll}
(qa, q'bc) & \text{falls} & \delta(q,a) = (q', c, L) \text{ fr alle } b \in \Gamma \\
(\#qa, \#q'\Box c) & \text{falls} & \delta(q,a) = (q', c, L) \\
(q\#, q'c\#) & \text{falls} & \delta(q, \Box) = (q', c, N) \\
(q\#, cq'\#) & \text{falls} & \delta(q, \Box) = (q', c, R) \\
(bq\#, q'b\#) & \text{falls} & \delta(q, \Box) = (q', c, L) \text{ für alle } b \in \Gamma
\end{array}
$$

3. Löschregeln:

   (aq_e, q_e) und $(q_e a, q_e)$ für alle $a \in \Gamma, q_e \in F$

4. Abschlußregeln:

   $(q_e\#\#, \#)$ für alle $q_e \in F$

($\rightarrow$) Falls M bei w stoppt gibt es eine Folge von Konfigurationen $(k_0, k_1, \ldots, k_t)$ mit $k_0 = q_0 w$, k_t ist Endkonfiguration also $k_t = uq_e v$ mit $u, v \in A^*, q_e \in F$) und $k_i \vdash k_{i+1}$
$\Leftrightarrow$ Die obige Eingabe für das MPCP besitzt ein Lösungswort

$$\#k_0\#k_1 \ldots \#k_t\#k_t'\#k_t'' \ldots \#q_e\#\#$$

($k_t', k_t'', \ldots$ entstehen aus $k_t = uq_e v$ durch Löschung von Nachbarsymbolen aus q_e)

($\leftarrow$) Besitzt der obige MPCP eine Lösung mit $i_1 = 1$, dann läßt sich eine stoppende Rechnung von M bei w ablesen. ■

Folgerung
PCP bleibt unentscheidbar, falls für das Alphabet A gilt: $A = \{0, 1\}$. ("01–PCP")

Beweis.
Es reicht zu zeigen: PCP $\leq$ 01–PCP.
Sei A das Alphabet von PCP.
Betrachte: $f : A \rightarrow \{0,1\}^*$ mit $f(a_r) = \hat{a_r} = 01^r$.
Setze die Abbildung f auf A^* fort.
Es gilt:
$(x_1, y_1), \ldots, (x_n.y_n)$ besitzt Lösung $\Leftrightarrow$ $(\hat{x_1}, \hat{y_1}), \ldots, (\hat{x_n}.\hat{y_n})$ besitzt Lösung. ■

Bemerkung
Sei PCP_k die Variante des PCPs, deren Eingabe aus genau k Wortpaaren besteht.

Es gilt:
PCP_k ist unentscheidbar für $k \geq 9$.
PCP_k ist entscheidbar für $k \leq 2$.