

Satz von Rice

Angenommen wir betrachten irgendeine interessante, "nicht-triviale" Eigenschaft / Bedingung an Turing-berechenbare Funktionen (z.B. f sei konstant, polynomiell berechenbar, nur an endlich vielen Stellen nicht definiert, etc.).

Gibt es ein Verfahren, das für eine beliebige TM M entscheidet, ob die von M berechnete Funktion diese Eigenschaft hat oder nicht?

Der Satz von Rice besagt: Nein! Das Problem ist unentscheidbar.

Triviale Eigenschaft: die von M berechnete Funktion ist berechenbar.

Satz (Rice): Es sei $\mathcal{R}$ die Klasse aller Turing-berechenbaren Funktionen. Ferner sei $\underline{S} \neq \emptyset, \neq \mathcal{R}$ eine beliebige Teilmenge von $\mathcal{R}$. Dann ist die Sprache

$$\mathcal{L}(\underline{S}) := \{ w \in \{0,1\}^* : \text{die von } \Pi_w \text{ berechnete Funktion liegt in } \underline{S} \}$$

unentscheidbar.

Erinnerung: Jedem Wort w über $\{0,1\}^*$ läßt sich bei einer gegebenen Codierung von TM über dem Alphabet $\{0,1\}$ eine TM Π_w zuordnen:

$$\Pi_w := \begin{cases} \Pi, & \text{falls } w \text{ codiert} \\ \Pi^*, & \text{sonst} \end{cases}$$

wobei Π^* beliebige, fest gewählte TM ist.

Fasse obige Fragestellung als ein Entscheidungsproblem in einer geeigneten Sprache auf.

Beachte: Π_w berechnet also dieselbe Funktion wie Π , sofern w Π codiert. Andernfalls berechnet Π_w irgendeine andere Funktion.

Beweis: Es sei $\Omega \in \mathcal{R}$ die überall undefinierte Funktion.

Ω ist trivialerweise berechenbar.

Dann gilt es zwei Fälle $\Omega \in \underline{S}$ oder $\Omega \notin \underline{S}$. Wir beschränken uns auf den Fall $\Omega \in \underline{S}$ ($\Omega \notin \underline{S} \rightarrow$ Übungsaufgabe).

Wir wollen zeigen:

$$(*) \quad H_0 \leq \mathcal{C}(\underline{S})$$

Da H_0 (Halteproblem auf leeren Band) unentscheidbar ist, ist auch $\bar{H}_0$ (komplementäres Problem) unentscheidbar. Also folgt mit (*), dass auch $\mathcal{C}(\underline{S})$ unentscheidbar ist.

Zu zeigen: Es gibt eine totale und berechenbare Funktion

$$f: \{0,1\}^* \rightarrow \{0,1\}^*$$

d.h. für jedes $w \in \{0,1\}^*$ gilt:

$$w \notin H_0 \iff f(w) \in \mathcal{C}(\underline{S})$$

Idee: Konstruiere f als Funktion, die (implizit) jeder Π M eine Π $\hat{M}$ zuordnet, sodass gilt:

Π stoppt $\iff$ die von $\hat{M}$ berechnete Funktion liegt nicht in $\underline{S}$

Nach Voraussetzung ist $\underline{R} \setminus \underline{S} \neq \emptyset$. Wähle $g^* \in \underline{R} \setminus \underline{S}$ beliebig. Weil g^* berechenbar ist, gibt es eine TM Π^* , die g berechnet.

← Wir haben nun zwei "Indikator"-Funktionen, eine in $\underline{S}$ und eine in $\underline{R} \setminus \underline{S}$.

Zu einem beliebigen $w \in \{0,1\}^*$ betrachte dann die folgende TM Π_w^* :

Π_w^* , angesetzt auf $y \in \{0,1\}^*$, verhält sich zunächst wie Π_w angesetzt auf das leere Band. Falls Π_w anhält, verhält sich Π_w^* danach wie Π^* angesetzt auf y .

← Implementiere das z.B. als 2-Band TM

Welche Funktion berechnet Π_w^* ? Falls Π_w auf leerem Band stoppt, so berechnet Π_w^* gerade die Funktion g^* , ← $\notin \underline{S}$ andernfalls berechnet Π_w^* offenbar Ω . ← $\in \underline{S}$

f sei nun jene Funktion, die jedem $w \in \{0,1\}^*$ die Codierung von Π_w^* über dem Alphabet $\{0,1\}$ zuordnet. f ist offenbar total und f ist berechenbar. ← Warum?

Dann gilt:

$\omega \in H_0 \Rightarrow \Pi_\omega$, aufgesetzt auf's leere Band, stoppt

$\Rightarrow \Pi_\omega^*$ berechnet f^* ($\notin \underline{S}$)

$\Rightarrow$ die von $\Pi_{f(\omega)}$ berechnete Funktion ist nicht in $\underline{S}$

$\Rightarrow f(\omega) \notin \mathcal{C}(\underline{S})$

Beachte: $f(\omega)$ ist
Codewort von Π_ω^* , d.h.
 $\Pi_\omega^* = \Pi_{f(\omega)}$

Umgekehrt:

$\omega \notin H_0 \Rightarrow \Pi_\omega$, aufgesetzt auf's leere Band, stoppt nicht

$\Rightarrow \Pi_\omega^*$ berechnet $f \in \underline{S}$

$\Rightarrow$ die von $\Pi_{f(\omega)}$ berechnete Funktion ist in $\underline{S}$

$\Rightarrow f(\omega) \in \mathcal{C}(\underline{S})$

Insgesamt also:

$\omega \in \overline{H_0} \Leftrightarrow f(\omega) \in \mathcal{C}(\underline{S})$

Nachbemerkung:

Das Halteproblem ist nicht das schwierigste entscheidbare Problem. z.B. gilt für das Äquivalenz-Problem:

$$E_q := \{ u \# v : \Pi_u \text{ berechnet dieselbe Funktion wie } \Pi_v \}$$

$$H \leq E_q, \text{ aber } E_q \not\leq H.$$

3.7 Das Postsche Korrespondenzproblem

IM
MAC

S
ASS

II
I

SP
TS

ACHT
H

AS
P

FO
OII

IN
INF

Können Sie diese Spielstreife so nebeneinander legen, dass in der oberen und unteren Zeile das gleiche Wort steht?

Eine Lösung:

IN	FO	II	IM	ACHT	SP	AS	S
INF	OII	I	MAC	H	TS	P	ASS

PCP (Postisches Korrespondenzproblem)

Gegeben: Eine endliche Folge von Wortpaaren

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

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

Gefragt: Gilt es eine Folge von Indizes

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

derart, dass:

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

Ist dies der Fall, so heißt $i_1, \dots, i_n$ eine Lösung.
von $(x_1, y_1), \dots, (x_k, y_k)$.

Beachte: Die Indizes $i_1, \dots, i_k$
können mehrfach aus $\{1, \dots, k\}$
gewählt werden

Die Länge n einer Lösung
 $i_1, \dots, i_n$ ist nicht beschränkt.

Beispiel:

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

Eine Lösung hiervon ist dann: $(1, 2, 2, 3, 4, 4, 1, 1)$

denn:

$$\begin{array}{cccccccc} 1 & 2 & 2 & 3 & 4 & 4 & 1 & 1 \\ \boxed{0} & \boxed{011} & \boxed{011} & \boxed{11} & \boxed{000} & \boxed{0} & & \\ = & \boxed{00} & \boxed{11} & \boxed{011} & \boxed{11} & \boxed{00} & \boxed{00} & \\ & 1 & 2 & 2 & 3 & 4 & 4 & 1 & 1 \end{array}$$

PCP ist offenbar semi-entscheidbar: Siehe einfach
immer längste Indexfolgen $i_1, \dots, i_n$ daraufhin ab,
ob sie eine Lösung einer gegebenen PCP-Instanz
sind.

PCP ist aber nicht entscheidbar!

Wir beweisen dies in zwei Schritten.

Wir betrachten dazu eine modifizierte Variante des PCP, MPCP, und zeigen dann $\text{MPCP} \leq \text{PCP}$ und $H \leq \text{MPCP}$.

Da H unentscheidbar und $\leq$ transitiv ist, folgt dann, dass auch PCP unentscheidbar ist.

Beachte: Wegen der Semi-Entscheidbarkeit von PCP

folgt aus $H \leq \text{PCP}$, dass H semi-entscheidbar ist. Also ist H rekursiv aufzählbar.

MPCP:

Gegeben: Eine endliche Folge von Paaren von nicht-leeren Wörtern über einer Alphabet Σ .

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

PCP mit fest
gewähltem „Anfangs-
stein“

Lemma: $\Pi PCP \leq PCP$

Beweis: Wir geben eine berechenbare Funktion f an, die jeder ΠPCP -Instanz eine PCP -Instanz zuordnet und zwar d.d. gilt:

K hat eine Lösung mit $i_1 = 1$
 $\Leftrightarrow f(K)$ hat irgendeine Lösung.

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

Für $w = a_1 \dots a_m \in \Sigma^*$ ($a_i \in \Sigma$) definiere:

$\hat{w} := a_1 \# a_2 \# \dots \# a_m \#$ $\leftarrow \#$ hinten: $\backslash$

$\check{w} := \# a_1 \# a_2 \# \dots \# a_m$ $\leftarrow \#$ vorne: $/$

Dann setze:

$f(K) := \left((\# \hat{x}_1, \check{y}_1), (\hat{x}_1, \check{y}_1), \dots, (\hat{x}_k, \check{y}_k), (\$, \# \$) \right)$

$\leftarrow$ Zwei Varianten des (x_1, y_1) -Steins
 $\leftarrow$ "Endausgleichs"-Stein
 $\leftarrow k+2$ viele Steine

Offenbar ist f berechenbar. Es bleibt zu

zeigen:

$$K \in \text{NPCP} \iff f(K) \in \text{PCP}$$

" $\Rightarrow$ " Sei $(i_1, i_2, \dots, i_n)$ eine Lösung für K ,

$$\text{d.h. } x_{i_1} x_{i_2} \dots x_{i_n} = y_{i_1} y_{i_2} \dots y_{i_n}$$

$$= a_1 \dots a_m \quad \text{für geeignete } a_i \in \Sigma$$

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

denn:

$$\begin{aligned} \# \tilde{x}_1 \tilde{x}_{i_2} \dots \tilde{x}_{i_n} \$ &= \# a_1 \# a_2 \# \dots a_m \# \$ \\ &= \tilde{y}_1 \tilde{y}_{i_2} \dots \tilde{y}_{i_n} \# \$ \end{aligned}$$

← Umindizierung der
Friste in $f(K)$: fange
bei 0 zu zählen an!