Unentscheidbarkeit

Kodierung TM

$$M = (\{0,1,2,\ldots,n\},\{0,1\},\{0,1,2,\ldots,k\},\Delta,2,0,1,2)$$

- Kodierung Übergang $(q,\gamma) \to (q',\gamma',d) \in \Delta$

$$\text{code}((q,\gamma) \to (q',\gamma',d)) = 1^q 0 1^\gamma 0 1^{q'} 0 1^{\gamma'} 0 1^{\text{bin}'(d)} 0$$

$$\text{bin}'(d) = \begin{cases} 1 & \text{falls } d = \triangleleft \\ 2 & \text{falls } d = \diamond \\ 3 & \text{sonst} \end{cases}$$

- Kodierung TM

$$\text{code}(M) = \prod_{\delta \in \Delta} \text{code}(\delta)$$

Unentscheidbarkeit

Beispiel

$$M = (\{q_0, q, q_a, q'_a, q_b, q'_b, q_+, q_-\},\{a,b\},\{a,b,\square\},\Delta,\square,q_0,q_+,q_-)$$

mit Übergängen Δ

$$(q_0,a) \to (q_a,\square,\triangleright) \quad (q_0,b) \to (q_b,\square,\triangleright) \quad (q_0,\square) \to (q_+,\square,\diamond)$$
$$(q_a,a) \to (q_a,a,\triangleright) \quad (q_a,b) \to (q_a,b,\triangleright) \quad (q_a,\square) \to (q'_a,\square,\triangleleft)$$
$$(q_b,a) \to (q_b,a,\triangleright) \quad (q_b,b) \to (q_b,b,\triangleright) \quad (q_b,\square) \to (q'_b,\square,\triangleleft)$$
$$(q'_a,a) \to (q,\square,\triangleleft) \quad (q'_b,b) \to (q,\square,\triangleleft)$$
$$(q,a) \to (q,a,\triangleleft) \quad (q,b) \to (q,b,\triangleleft) \quad (q,\square) \to (q_0,\square,\triangleright)$$

Unentscheidbarkeit

Beispiel

$$M = (\{0,1,2,3,4,5,6,7\},\{0,1\},\{0,1,2\},\Delta,2,0,1,2)$$

mit Übergängen Δ

$$(0,0) \to (3,2,\triangleright) \quad (0,1) \to (4,2,\triangleright) \quad (0,2) \to (1,2,\diamond)$$
$$(3,0) \to (3,0,\triangleright) \quad (3,1) \to (3,1,\triangleright) \quad (3,2) \to (5,2,\triangleleft)$$
$$(4,0) \to (4,0,\triangleright) \quad (4,1) \to (4,1,\triangleright) \quad (4,2) \to (6,2,\triangleleft)$$
$$(5,0) \to (7,2,\triangleleft) \quad (6,1) \to (7,2,\triangleleft)$$
$$(7,0) \to (7,0,\triangleleft) \quad (7,1) \to (7,1,\triangleleft) \quad (7,2) \to (0,2,\triangleright)$$

$$\text{code}(M) = \underbrace{0 0 1^3 0 1^2 0 1^3 0}_{(0,0)\to(3,2,\triangleright)} \underbrace{0 1^1 0 1^4 0 1^2 0 1^3 0}_{(0,1)\to(4,2,\triangleright)} \cdots$$

Unentscheidbarkeit

Konvention

- Zustände nummeriert ab 0
- Initialzustand 0, akzeptierender Zustand 1, ablehnender Zustand 2
- Arbeitssymbole nummeriert ab 0; Eingabesymbole $\mathfrak{B} = \{0,1\}$
- Blanksymbol 2
- Betrachten bereinigte TM
  (jeder Zustand & jedes Symbol an mind. 1 Übergang beteiligt)
- Ausnahme Zustände & Symbole $\{0,1,2\}$ immer vorhanden
- Sequenz $\# = 00000$ kommt in keiner gültigen Kodierung vor

Unentscheidbarkeit

§9.1 Definition (Dekodierung; *decoding*)

Sei $\widehat{M}$ beliebige bereinigte det. TM über $\mathfrak{B}$ und
$\text{decode}\colon \mathfrak{B}^* \to \{M \mid M \text{ bereinigte det. TM über } \mathfrak{B}\}$ mit

$$\text{decode}(w) = \begin{cases} M & \text{falls } \text{code}(M) = w \\ \widehat{M} & \text{sonst} \end{cases} \qquad \text{für alle } w \in \mathfrak{B}^*$$

Notizen

- Invertierung Binärdarstellung
- Liefert Standard-TM für ungültige Binärdarstellungen

Unentscheidbarkeit

§9.2 Definition (Halteproblem; *halting problem*)

Halteproblem ist Sprache $(\# = 00000)$

$$H = \{c\#w \mid c \in \mathfrak{B}^* \setminus \mathfrak{B}^*\{\#\}\mathfrak{B}^*, \text{ TM } \text{decode}(c) \text{ hält auf } w \in \mathfrak{B}^*\}$$

d.h. hält geg. bereinigte det. TM $\text{decode}(c)$ auf Eingabe $w \in \mathfrak{B}^*$?
(erreicht $\text{decode}(c)$ mit Eingabe w Endzustand)

Charakteristische Funktion $\chi_H\colon \mathfrak{B}^* \to \mathfrak{B}$

$$\chi_H(v) = \begin{cases} 1 & \text{falls } v = c\#w \text{ mit } c \in \mathfrak{B}^* \setminus \mathfrak{B}^*\{\#\}\mathfrak{B}^*, w \in \mathfrak{B}^* \text{ und} \\ & \quad \text{decode}(c) \text{ auf } w \text{ hält} \\ 0 & \text{sonst} \end{cases}$$

Unentscheidbarkeit

§9.3 Definition (spez. Halteproblem; *special halting problem*)

Spezielle Halteproblem ist Sprache

$$\underline{H} = \{w \in \mathfrak{B}^* \mid \text{TM } \text{decode}(w) \text{ hält auf Eingabe } w\}$$

d.h. hält geg. TM $\text{decode}(w)$ auf (potentiell) eigener Kodierung w?

Charakteristische Funktion $\chi_{\underline{H}}\colon \mathfrak{B}^* \to \mathfrak{B}$

$$\chi_{\underline{H}}(w) = \begin{cases} 1 & \text{falls TM } \text{decode}(w) \text{ auf } w \text{ hält} \\ 0 & \text{sonst} \end{cases}$$

Unentscheidbarkeit

§9.4 Theorem (universelle TM; *universal Turing machine*)

Det. TM U die bei Eingabe $u\#w$ det. TM $\text{decode}(u)$ auf w simuliert

Notizen

- **Universelle Turingmaschine** U
- U hält auf $u\#w$ gdw. $\text{decode}(u)$ auf w hält
- U produziert auf $u\#w$ gleiche Ausgabe wie $\text{decode}(u)$ auf w

$$T(U) = \{(u\#w, v) \mid (w, v) \in T(\text{decode}(u))\}$$

Unentscheidbarkeit

§9.5 Theorem

Spezielles Halteproblem $\underline{H}$ unentscheidbar

Beweis (1/2)

Sei spezielles Halteproblem $\underline{H}$ entscheidbar. Dann existiert det. TM M für charakteristische Funktion $\chi_{\underline{H}}$. Sei P äquivalentes While-Programm. Betrachte Programm P'

P (berechne $\chi_{\underline{H}}$ von Eingabe)
IF$(x_1 \neq 0)\,\{\ldots \textit{Endlosschleife} \ldots\}$ (falls decode(x_1) auf x_1 hält)
ELSE $\{x_1 = 1\}$ (liefere 1 falls decode(x_1) auf x_1 nicht hält)

Programm P' berechnet

$$\rho_{\overline{\underline{H}}}(w) = \begin{cases} 1 & \text{falls } \chi_{\underline{H}}(w) = 0 \\ \text{undef} & \text{sonst} \end{cases}$$

Unentscheidbarkeit

Beweis (2/2)

Sei M' äquivalente det. TM zu P'. Betrachte Eingabe $w' = \text{code}(M')$

$$\begin{aligned} & M' = \text{decode}(w') \text{ hält auf } w' \\ \iff & \rho_{\overline{\underline{H}}}(w') = 1 && \text{(da } M' \ \rho_{\overline{\underline{H}}} \text{ berechnet)} \\ \iff & \chi_{\underline{H}}(w') = 0 && \text{(Def. } \rho_{\overline{\underline{H}}}) \\ \iff & w' \notin \underline{H} && \text{(Def. } \chi_{\underline{H}}) \\ \iff & \text{decode}(w') \text{ hält auf } w' \text{ nicht} && \text{(Def. } \underline{H}) \end{aligned}$$

Widerspruch ↯ □

Unentscheidbarkeit

- Beweis nutzt Diagonalisierung
- Illustration Halteverhalten

$M \setminus w$	$f(0)$	$f(1)$	$f(2)$	$f(3)$	$\cdots$	$w' = \text{code}(M')$
decode$(f(0))$	✗	✗	✓	✓	$\cdots$	✓
decode$(f(1))$	✗	✓	✓	✗	$\cdots$	✓
decode$(f(2))$	✗	✗	✓	✗	$\cdots$	✗
decode$(f(3))$	✓	✓	✗	✓	$\cdots$	✓
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
$M' = \text{decode}(w')$	✓	✗	✗	✗	$\cdots$	?

M' hält auf $w \iff$ decode(w) auf w nicht hält

Problem-Reduktionen

Komposition oder Verkettung (§3.4)

- **Komposition** $f\colon \Sigma_1^* \dashrightarrow \Sigma_2^*$ und $g\colon \Sigma_2^* \dashrightarrow \Sigma_3^*$ ist $(f\,;g)\colon \Sigma_1^* \dashrightarrow \Sigma_3^*$

$$(f\,;g)(w) = g(f(w)) = \begin{cases} \text{undef} & \text{falls } f(w) = \text{undef} \\ g(f(w)) & \text{sonst} \end{cases}$$

§9.6 Theorem

$(f\,;g)$ berechenbar falls $f\colon \Sigma_1^* \dashrightarrow \Sigma_2^*$ und $g\colon \Sigma_2^* \dashrightarrow \Sigma_3^*$ berechenbar

Beweis

Verkettung det. TM für f und g (Sequenz While-Programme) □

Problem-Reduktionen

§9.7 Theorem

Sei $f : \Sigma^* \to \Gamma^*$ total und berechenbar und $K \subseteq \Gamma^*$.
Falls K entscheidbar, dann $f^{-1}(K)$ entscheidbar

Beweis

Da K entscheidbar, ist $\chi_K : \Gamma^* \to \{0,1\}$ berechenbar. Gemäß Theorem §9.6 ist $(f \,;\, \chi_K) : \Sigma^* \to \{0,1\}$ berechenbar.

$$(f \,;\, \chi_K)(w) = \chi_K(f(w)) = \begin{cases} 1 & \text{falls } f(w) \in K \\ 0 & \text{sonst} \end{cases}$$
$$= \begin{cases} 1 & \text{falls } w \in f^{-1}(K) \\ 0 & \text{sonst} \end{cases} = \chi_{f^{-1}(K)}(w)$$

Also $f^{-1}(K)$ entscheidbar □

Problem-Reduktionen

Notizen

- Kontraposition von Theorem §9.7 ebenso interessant:

  Sei $f : \Sigma^* \to \Gamma^*$ total & berechenbar und $K \subseteq \Gamma^*$.
  Falls $f^{-1}(K)$ unentscheidbar, dann K unentscheidbar
- Betrachte berechenbare totale Funktion f
  - Sprache K entscheidbar → Urbild $f^{-1}(K)$ entscheidbar
  - Urbild $f^{-1}(K)$ unentscheidbar → Sprache K unentscheidbar

Problem-Reduktionen

§9.8 Definition (Reduktion; *reduction*)

Problem $L \subseteq \Sigma^*$ **reduzierbar** auf $K \subseteq \Gamma^*$, geschrieben $L \preceq K$, falls (totale) berechenbare Funktion $f : \Sigma^* \to \Gamma^*$ existiert mit $L = f^{-1}(K)$

Notizen

- $L = f^{-1}(K)$ entspricht Aussage

  $w \in L$ gdw. $f(w) \in K$ für alle $w \in \Sigma^*$
- f übersetzt Instanz Problem L in Instanz Problem K
  (Bestimmung "$w \in L$" per Bestimmung "$f(w) \in K$")
- $L \preceq K$ bedeutet "L höchstens so schwer wie K"
  (aktuell 2 Schwierigkeiten: entscheidbar & unentscheidbar)
- Berechenbarkeit & Totalität von f essentiell

Problem-Reduktionen

§9.9 Theorem

Seien $L \subseteq \Sigma^*$ und $K \subseteq \Gamma^*$ mit $L \preceq K$

- Falls K entscheidbar, dann L entscheidbar
  (entscheidbar falls leichter als entscheidbares Problem)
- Falls L unentscheidbar, dann K unentscheidbar
  (unentscheidbar falls schwerer als unentscheidbares Problem)

Problem-Reduktionen

§9.10 Theorem

Allgemeines Halteproblem H unentscheidbar

Beweis

Reduktion spezielles Halteproblem $\underline{H}$ auf H

$\underline{H} = \{w \mid \text{decode}(w) \text{ hält auf } w\} \quad H = \{c\#w \mid \text{decode}(c) \text{ hält auf } w\}$

Benötigen berechenbare Funktion $f : \mathfrak{B}^* \to \mathfrak{B}^*$, die Elemente von $\underline{H}$ in Elemente von H übersetzt. Sei $f(w) = c\#w$ für alle $w \in \mathfrak{B}^*$ mit $c = w$ falls $w \in \mathfrak{B}^* \setminus \mathfrak{B}^*\{\#\}\mathfrak{B}^*$ und $c = \text{code}(\widehat{M})$ sonst (klar berechenbar). Für alle $w \in \mathfrak{B}^*$ gelten $\text{decode}(c) = \text{decode}(w)$ und

$$w \in \underline{H} \iff \text{decode}(w) \text{ hält auf } w \iff c\#w = f(w) \in H$$

Damit $\underline{H} = f^{-1}(H)$, $\underline{H} \preceq H$ und H unentscheidbar (Theorem §9.9) □

Problem-Reduktionen

§9.11 Theorem

Leerband-Halteproblem $\{c \mid \text{decode}(c) \text{ hält auf } \varepsilon\}$ unentscheidbar

Beweis

Wir reduzieren allgemeines Halteproblem H auf H_ε.

$H = \{c\#w \mid \text{decode}(c) \text{ hält auf } w\} \quad H_\varepsilon = \{c \mid \text{decode}(c) \text{ hält auf } \varepsilon\}$

Sei $f(c\#w) = \text{code}(M'_{c,w})$ für alle $c \in \mathfrak{B}^* \setminus \mathfrak{B}^*\{\#\}\mathfrak{B}^*$ und $w \in \mathfrak{B}^*$, wobei $M'_{c,w}$ det. TM die w auf Band schreibt, zurückläuft und $\text{decode}(c)$ simuliert. Sonst sei $f(v) = \text{code}(M_\perp)$ mit $M_\perp$ det. TM die nie hält (es gilt $v \notin H$ und $f(v) \notin H_\varepsilon$). Für alle $c \in \mathfrak{B}^* \setminus \mathfrak{B}^*\{\#\}\mathfrak{B}^*$ und $w \in \mathfrak{B}^*$

$$c\#w \in H \iff \text{decode}(c) \text{ hält auf } w \iff \text{code}(M'_{c,w}) \in H_\varepsilon$$

Damit $H = f^{-1}(H_\varepsilon)$, $H \preceq H_\varepsilon$ und H_ε unentscheidbar (Thm. §9.9) □

Problem-Reduktionen

§9.12 Theorem (Satz von Rice)

Sei $\mathcal{R}$ Klasse aller berechenbaren partiellen Funktionen und $\mathcal{F} \subseteq \mathcal{R}$ mit $\emptyset \subsetneq \mathcal{F} \subsetneq \mathcal{R}$. Dann $\mathcal{C}(\mathcal{F})$ unentscheidbar

$$\mathcal{C}(\mathcal{F}) = \{w \in \mathfrak{B}^* \mid T(\text{decode}(w)) \in \mathcal{F}\}$$

(Kodierungen aller det. TM, die Funktionen in $\mathcal{F}$ berechnen)

Henry Gordon Rice (* 1920; † 2003)

- Amer. Logiker & Mathematiker
- Bewies berühmten Satz in Dissertation
- Arbeitete zuletzt bei Computer Science Cooperation

Problem-Reduktionen

Beweis (1/3)

Sei $\perp = \emptyset \in \mathcal{R}$ überall undefinierte partielle Funktion auf $\mathfrak{B}^*$, die berechenbar ist und entweder $\perp \in \mathcal{F}$ oder $\perp \notin \mathcal{F}$.

Sei $\perp \in \mathcal{F}$. Da $\mathcal{F} \subsetneq \mathcal{R}$ existiert berechenbare partielle Funktion $g \in \mathcal{R} \setminus \mathcal{F}$. Sei M det. TM die g berechnet.

Wir reduzieren vom Komplement Halteproblem $\overline{H_\varepsilon}$ auf leerem Band. Sei $f : \mathfrak{B}^* \to \mathfrak{B}^*$ mit $f(w) = \text{code}(M_w)$ für alle $w \in \mathfrak{B}^*$ und M_w det. 2-Band-TM die bei Eingabe $v \in \mathfrak{B}^*$

1. $\text{decode}(w)$ auf leerem zweiten Band simuliert
2. Bei Akzeptanz danach TM M auf Eingabe v simuliert

$$T(M_w) = \begin{cases} \perp & \text{falls } \text{decode}(w) \text{ auf } \varepsilon \text{ nicht hält (d.h. } w \notin H_\varepsilon) \\ g & \text{sonst (d.h. } w \in H_\varepsilon) \end{cases}$$

Problem-Reduktionen

Beweis (2/3)

Funktion f berechenbar. Wir zeigen $w \in \overline{H_\varepsilon}$ gdw. $f(w) \in \mathcal{C}(\mathcal{F})$

- Sei $w \notin \overline{H_\varepsilon}$. Dann $T(M_w) = g$ und $T(M_w) \notin \mathcal{F}$.
  Also $\text{code}(M_w) \notin \mathcal{C}(\mathcal{F})$, womit $f(w) \notin \mathcal{C}(\mathcal{F})$.
- Sei $w \in \overline{H_\varepsilon}$. Dann $T(M_w) = \bot$ und $T(M_w) \in \mathcal{F}$.
  Also $\text{code}(M_w) \in \mathcal{C}(\mathcal{F})$, womit $f(w) \in \mathcal{C}(\mathcal{F})$.

Also gilt Hilfsaussage, $\overline{H_\varepsilon} \preceq \mathcal{C}(\mathcal{F})$ und $\mathcal{C}(\mathcal{F})$ unentscheidbar da $\overline{H_\varepsilon}$ unentscheidbar (wäre $\overline{H_\varepsilon}$ entscheidbar, so wäre H_ε entscheidbar per Theorem §8.6; dies widerspricht Theorem §9.11)

Problem-Reduktionen

Beweis (3/3)

Sei $\bot \notin \mathcal{F}$. Da $\emptyset \subsetneq \mathcal{F}$ existiert partielle Funktion $g \in \mathcal{F}$. Sei M det. TM die g berechnet.

Wir reduzieren vom Halteproblem H_ε auf leerem Band und verwenden gleiche Funktion f wie vorher. Wir zeigen $w \in H_\varepsilon$ gdw. $f(w) \in \mathcal{C}(\mathcal{F})$

- Sei $w \in H_\varepsilon$. Dann $T(M_w) = g$ und $T(M_w) \in \mathcal{F}$.
  Also $\text{code}(M_w) \in \mathcal{C}(\mathcal{F})$, womit $f(w) \in \mathcal{C}(\mathcal{F})$.
- Sei $w \notin H_\varepsilon$. Dann $T(M_w) = \bot$ und $T(M_w) \notin \mathcal{F}$.
  Also $\text{code}(M_w) \notin \mathcal{C}(\mathcal{F})$, womit $f(w) \notin \mathcal{C}(\mathcal{F})$.

Damit gilt Hilfsaussage, $H_\varepsilon \preceq \mathcal{C}(\mathcal{F})$ und $\mathcal{C}(\mathcal{F})$ unentscheidbar da H_ε unentscheidbar (nach Theorem §9.11) □

Problem-Reduktionen

Notizen

- $\mathcal{F}$ (nicht-triviale) Eigenschaft partieller Funktionen
  (z.B. total, surjektiv; nicht Eigenschaft der TM)
- Unentscheidbar, ob geg. TM Funktion mit Eigenschaft $\mathcal{F}$ berechnet
- Sehr mächtige Aussage
- Kein Programm kann Korrektheit (Äquivalenz) oder Termination (Reduktion von Akzeptanz) beliebiger Programme entscheiden

Problem-Reduktionen

§9.13 Theorem (Konsequenzen Satz von Rice)

Folgende Probleme unentscheidbar

- Universell akzeptierend $\{w \mid T(\text{decode}(w)) \text{ total}\}$
  (Berechnet $\text{decode}(w)$ Funktion?)
- Singulär akzeptierend $\{w \mid T(\text{decode}(w)) \neq \emptyset\}$
  (Liefert $\text{decode}(w)$ mind. 1 Ausgabe?)
- f-äquivalent $\{w \mid T(\text{decode}(w)) = f\}$ für berechenbares f
  (Berechnet $\text{decode}(w)$ genau partielle Funktion f?)
- Konstant $\{w \mid \exists u\colon T(\text{decode}(w))(\{0,1\}^*) = \{u\}\}$
  (Berechnet $\text{decode}(w)$ konstante partielle Funktion?)
- Nicht verkürzend $\{w \mid \forall v \forall u \in T(\text{decode}(w))(\{v\})\colon |u| \geq |v|\}$
  (Ist Ausgabe immer mind. so lang wie Eingabe?)