

Berechenbarkeit

Vorlesung 9: Unentscheidbarkeit

19. Juni 2025

Termine — Modul Berechenbarkeit

ÜBUNGEN	PRÜFUNG	VORLESUNG
17.6. Übung 5 A-Woche	18.6. _____	19.6. Unentscheidbarkeit (Übungsblatt 6)
24.6. Übung 6 B-Woche	25.6. _____	26.6. Spez. Probleme
1.7. Übung 6 A-Woche	2.7. _____	3.7. Klasse P
8.7. Abschlussübung beide Wochen	9.7. _____	10.7. NP-Vollständigkeit
15.7. _____	16.7. Prüfung ab 13:30 Uhr in AudiMax & Hs. 9	17.7. _____

Unentscheidbarkeit

Definition (§8.2 Entscheidbarkeit; *decidability*)

Problem $L \subseteq \Sigma^*$ **entscheidbar** (*decidable*) falls χ_L berechenbar

$$\chi_L: \Sigma^* \rightarrow \{0,1\} \quad \text{mit} \quad \chi_L(w) = \begin{cases} 1 & \text{falls } w \in L \\ 0 & \text{sonst} \end{cases} \quad \text{für alle } w \in \Sigma^*$$

L **unentscheidbar** (*undecidable*) falls χ_L nicht berechenbar

Unentscheidbarkeit

Kodierung TM

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

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

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

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

Unentscheidbarkeit

Kodierung TM

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

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

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

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

- Kodierung TM

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

Unentscheidbarkeit

Beispiel

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

mit Übergängen Δ

$$(q_0, a) \rightarrow (q_a, \square, \triangleright) \quad (q_0, b) \rightarrow (q_b, \square, \triangleright) \quad (q_0, \square) \rightarrow (q_+, \square, \diamond)$$

$$(q_a, a) \rightarrow (q_a, a, \triangleright) \quad (q_a, b) \rightarrow (q_a, b, \triangleright) \quad (q_a, \square) \rightarrow (q'_a, \square, \triangleleft)$$

$$(q_b, a) \rightarrow (q_b, a, \triangleright) \quad (q_b, b) \rightarrow (q_b, b, \triangleright) \quad (q_b, \square) \rightarrow (q'_b, \square, \triangleleft)$$

$$(q'_a, a) \rightarrow (q, \square, \triangleleft) \quad (q'_b, b) \rightarrow (q, \square, \triangleleft)$$

$$(q, a) \rightarrow (q, a, \triangleleft) \quad (q, b) \rightarrow (q, b, \triangleleft) \quad (q, \square) \rightarrow (q_0, \square, \triangleright)$$

Unentscheidbarkeit

Beispiel

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

mit Übergängen Δ

$$(0, 0) \rightarrow (3, 2, \triangleright) \quad (0, 1) \rightarrow (4, 2, \triangleright) \quad (0, 2) \rightarrow (1, 2, \diamond)$$

$$(3, 0) \rightarrow (3, 0, \triangleright) \quad (3, 1) \rightarrow (3, 1, \triangleright) \quad (3, 2) \rightarrow (5, 2, \triangleleft)$$

$$(4, 0) \rightarrow (4, 0, \triangleright) \quad (4, 1) \rightarrow (4, 1, \triangleright) \quad (4, 2) \rightarrow (6, 2, \triangleleft)$$

$$(5, 0) \rightarrow (7, 2, \triangleleft) \quad (6, 1) \rightarrow (7, 2, \triangleleft)$$

$$(7, 0) \rightarrow (7, 0, \triangleleft) \quad (7, 1) \rightarrow (7, 1, \triangleleft) \quad (7, 2) \rightarrow (0, 2, \triangleright)$$

Unentscheidbarkeit

Beispiel

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

mit Übergängen Δ

$$(0, 0) \rightarrow (3, 2, \triangleright) \quad (0, 1) \rightarrow (4, 2, \triangleright) \quad (0, 2) \rightarrow (1, 2, \diamond)$$

$$(3, 0) \rightarrow (3, 0, \triangleright) \quad (3, 1) \rightarrow (3, 1, \triangleright) \quad (3, 2) \rightarrow (5, 2, \triangleleft)$$

$$(4, 0) \rightarrow (4, 0, \triangleright) \quad (4, 1) \rightarrow (4, 1, \triangleright) \quad (4, 2) \rightarrow (6, 2, \triangleleft)$$

$$(5, 0) \rightarrow (7, 2, \triangleleft) \quad (6, 1) \rightarrow (7, 2, \triangleleft)$$

$$(7, 0) \rightarrow (7, 0, \triangleleft) \quad (7, 1) \rightarrow (7, 1, \triangleleft) \quad (7, 2) \rightarrow (0, 2, \triangleright)$$

$$\text{code}(\mathcal{M}) = \underbrace{001^3 01^2 01^3 0}_{(0,0) \rightarrow (3,2,\triangleright)} \underbrace{01^1 01^4 01^2 01^3 0}_{(0,1) \rightarrow (4,2,\triangleright)} \dots$$

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

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 \hat{M} beliebige bereinigte det. TM über \mathfrak{B} und
 $\text{decode}: \mathfrak{B}^* \rightarrow \{M \mid M \text{ bereinigte det. TM über } \mathfrak{B}\}$ mit

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

Unentscheidbarkeit

§9.1 Definition (Dekodierung; *decoding*)

Sei \hat{M} beliebige bereinigte det. TM über \mathfrak{B} und
 $\text{decode}: \mathfrak{B}^* \rightarrow \{M \mid M \text{ bereinigte det. TM über } \mathfrak{B}\}$ mit

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

Notizen

- Invertierung Binärdarstellung
- Liefert Standard-TM für ungültige Binärdarstellungen

§9.2 Definition (Halteproblem; *halting problem*)

Halteproblem ist Sprache ($\# = 00000$)

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

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

Unentscheidbarkeit

§9.2 Definition (Halteproblem; *halting problem*)

Halteproblem ist Sprache ($\# = 00000$)

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

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

Charakteristische Funktion $\chi_H: \mathcal{B}^* \rightarrow \mathcal{B}$

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

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 $\chi_{\underline{H}}: \mathfrak{B}^* \rightarrow \mathfrak{B}$

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

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

§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

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

Unentscheidbarkeit

§9.5 Theorem

Spezielles Halteproblem H unentscheidbar

Unentscheidbarkeit

§9.5 Theorem

Spezielles Halteproblem \underline{H} unentscheidbar

Beweis (1/2)

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

Unentscheidbarkeit

§9.5 Theorem

Spezielles Halteproblem \underline{H} unentscheidbar

Beweis (1/2)

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

P	(berechne $\chi_{\underline{H}}$ von Eingabe)
IF ($x_1 \neq 0$) { ... <i>Endlosschleife</i> ... }	(falls $\text{decode}(x_1)$ auf x_1 hält)
ELSE { $x_1 = 1$ }	(liefern 1 falls $\text{decode}(x_1)$ auf x_1 nicht hält)

Unentscheidbarkeit

§9.5 Theorem

Spezielles Halteproblem \underline{H} unentscheidbar

Beweis (1/2)

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

P	(berechne $\chi_{\underline{H}}$ von Eingabe)
IF ($x_1 \neq 0$) { ... <i>Endlosschleife</i> ... }	(falls $\text{decode}(x_1)$ auf x_1 hält)
ELSE { $x_1 = 1$ }	(liefern 1 falls $\text{decode}(x_1)$ auf x_1 nicht hält)

Programm P' berechnet

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

Unentscheidbarkeit

Beweis (2/2)

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

$M' = \text{decode}(w')$ hält auf w'

$$\iff \rho_{\underline{H}}(w') = 1 \quad (\text{da } M' \rho_{\underline{H}} \text{ berechnet})$$

$$\iff \chi_{\underline{H}}(w') = 0 \quad (\text{Def. } \rho_{\underline{H}})$$

$$\iff w' \notin \underline{H} \quad (\text{Def. } \chi_{\underline{H}})$$

$$\iff \text{decode}(w') \text{ hält auf } w' \text{ nicht} \quad (\text{Def. } \underline{H})$$

Unentscheidbarkeit

Beweis (2/2)

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

$M' = \text{decode}(w')$ hält auf w'

$$\iff \rho_{\underline{H}}(w') = 1 \quad (\text{da } M' \rho_{\underline{H}} \text{ berechnet})$$

$$\iff \chi_{\underline{H}}(w') = 0 \quad (\text{Def. } \rho_{\underline{H}})$$

$$\iff w' \notin \underline{H} \quad (\text{Def. } \chi_{\underline{H}})$$

$$\iff \text{decode}(w') \text{ hält auf } w' \text{ nicht} \quad (\text{Def. } \underline{H})$$

Widerspruch \nexists



Unentscheidbarkeit

- Beweis nutzt Diagonalisierung
- Illustration Halteverhalten

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

\mathcal{M}' hält auf $w \iff \text{decode}(w)$ auf w nicht hält

Problem-Reduktionen

Komposition oder Verkettung (§3.4)

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

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

Problem-Reduktionen

Komposition oder Verkettung (§3.4)

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

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

§9.6 Theorem

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

Problem-Reduktionen

Komposition oder Verkettung (§3.4)

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

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

§9.6 Theorem

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

Beweis

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



Problem-Reduktionen

§9.7 Theorem

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

Problem-Reduktionen

§9.7 Theorem

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

Beweis

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

Problem-Reduktionen

§9.7 Theorem

Sei $f: \Sigma^* \rightarrow \Gamma^*$ total und berechenbar und $K \subseteq \Gamma^*$.

Falls K entscheidbar, dann $f^{-1}(K)$ entscheidbar

Beweis

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

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

Problem-Reduktionen

§9.7 Theorem

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

Beweis

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

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

Also $f^{-1}(K)$ entscheidbar



Problem-Reduktionen

Notizen

- Kontraposition von Theorem §9.7 ebenso interessant:

Sei $f: \Sigma^* \rightarrow \Gamma^*$ total & berechenbar und $K \subseteq \Gamma^*$.

Falls $f^{-1}(K)$ unentscheidbar, dann K unentscheidbar

Problem-Reduktionen

Notizen

- Kontraposition von Theorem §9.7 ebenso interessant:

Sei $f: \Sigma^* \rightarrow \Gamma^*$ total & berechenbar und $K \subseteq \Gamma^*$.

Falls $f^{-1}(K)$ unentscheidbar, dann K unentscheidbar

- Betrachte berechenbare totale Funktion f
 - Sprache K entscheidbar \rightarrow Urbild $f^{-1}(K)$ entscheidbar
 - Urbild $f^{-1}(K)$ unentscheidbar \rightarrow 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 $f: \Sigma^* \rightarrow \Gamma^*$ existiert mit $L = f^{-1}(K)$

Problem-Reduktionen

§9.8 Definition (Reduktion; *reduction*)

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

Notizen

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

$$w \in L \quad \text{gdw.} \quad f(w) \in K \quad \text{für alle } w \in \Sigma^*$$

- f übersetzt Instanz Problem L in Instanz Problem K
(Bestimmung " $w \in L$ " per Bestimmung " $f(w) \in K$ ")

Problem-Reduktionen

§9.8 Definition (Reduktion; *reduction*)

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

Notizen

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

$$w \in L \quad \text{gdw.} \quad f(w) \in K \quad \text{für alle } w \in \Sigma^*$$

- 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

§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)

§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

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 $f: \mathfrak{B}^* \rightarrow \mathfrak{B}^*$, die Elemente von \underline{H} in Elemente von H übersetzt.

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 $f: \mathfrak{B}^* \rightarrow \mathfrak{B}^*$, 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 $c = \text{code}(\hat{M})$ sonst (klar berechenbar).

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 $f: \mathfrak{B}^* \rightarrow \mathfrak{B}^*$, 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 $c = \text{code}(\hat{M})$ 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) \square

Problem-Reduktionen

§9.11 Theorem

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

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 .

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

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 $c \in \mathcal{B}^* \setminus \mathcal{B}^*\{\#\}\mathcal{B}^*$ und $w \in \mathcal{B}^*$, 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 $f(v) \notin H_\varepsilon$).

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 $c \in \mathcal{B}^* \setminus \mathcal{B}^*\{\#\}\mathcal{B}^*$ und $w \in \mathcal{B}^*$, 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 $c \in \mathcal{B}^* \setminus \mathcal{B}^*\{\#\}\mathcal{B}^*$ und $w \in \mathcal{B}^*$

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

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 \mathcal{B}^* , die berechenbar ist und entweder $\perp \in \mathcal{F}$ oder $\perp \notin \mathcal{F}$.

Problem-Reduktionen

Beweis (1/3)

Sei $\perp = \emptyset \in \mathcal{R}$ überall undefinierte partielle Funktion auf \mathcal{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.

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 $\overline{H_\epsilon}$ auf leerem Band.
Sei $f: \mathfrak{B}^* \rightarrow \mathfrak{B}^*$ 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

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 $f: \mathfrak{B}^* \rightarrow \mathfrak{B}^*$ 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 $w \in \overline{H_\epsilon}$ gdw. $f(w) \in \mathcal{C}(\mathcal{F})$

- Sei $w \notin \overline{H_\epsilon}$. Dann $T(M_w) = g$ und $T(M_w) \notin \mathcal{F}$.

Problem-Reduktionen

Beweis (2/3)

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

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

Problem-Reduktionen

Beweis (2/3)

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

- Sei $w \notin \overline{H_\epsilon}$. 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 $w \in \overline{H_\epsilon}$. Dann $T(M_w) = \perp$ und $T(M_w) \in \mathcal{F}$.

Problem-Reduktionen

Beweis (2/3)

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

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

Problem-Reduktionen

Beweis (2/3)

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

- Sei $w \notin \overline{H_\epsilon}$. 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 $w \in \overline{H_\epsilon}$. Dann $T(M_w) = \perp$ 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, $\overline{H_\epsilon} \preceq \mathcal{C}(\mathcal{F})$ und $\mathcal{C}(\mathcal{F})$ unentscheidbar da $\overline{H_\epsilon}$ unentscheidbar (wäre $\overline{H_\epsilon}$ entscheidbar, so wäre H_ϵ entscheidbar per Theorem §8.6; dies widerspricht Theorem §9.11)

Problem-Reduktionen

Beweis (3/3)

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

Problem-Reduktionen

Beweis (3/3)

Sei $\perp \notin \mathcal{F}$. 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 $w \in H_\epsilon$ gdw. $f(w) \in \mathcal{C}(\mathcal{F})$

- Sei $w \in H_\epsilon$. Dann $T(M_w) = g$ und $T(M_w) \in \mathcal{F}$.

Problem-Reduktionen

Beweis (3/3)

Sei $\perp \notin \mathcal{F}$. 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 $w \in H_\epsilon$ gdw. $f(w) \in \mathcal{C}(\mathcal{F})$

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

Problem-Reduktionen

Beweis (3/3)

Sei $\perp \notin \mathcal{F}$. 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 $w \in H_\epsilon$ gdw. $f(w) \in \mathcal{C}(\mathcal{F})$

- Sei $w \in H_\epsilon$. 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 $w \notin H_\epsilon$. Dann $T(M_w) = \perp$ und $T(M_w) \notin \mathcal{F}$.

Problem-Reduktionen

Beweis (3/3)

Sei $\perp \notin \mathcal{F}$. 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 $w \in H_\epsilon$ gdw. $f(w) \in \mathcal{C}(\mathcal{F})$

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

Problem-Reduktionen

Beweis (3/3)

Sei $\perp \notin \mathcal{F}$. 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 $w \in H_\epsilon$ gdw. $f(w) \in \mathcal{C}(\mathcal{F})$

- Sei $w \in H_\epsilon$. 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 $w \notin H_\epsilon$. Dann $T(M_w) = \perp$ 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, $H_\epsilon \preceq \mathcal{C}(\mathcal{F})$ 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

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

§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?)

§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?)

§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 ?)

§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 $\{w \mid \exists u: T(\text{decode}(w))(\{0,1\}^*) = \{u\}\}$
(Berechnet $\text{decode}(w)$ konstante partielle Funktion?)

§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?)
- Singular 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 $\{w \mid \exists u: T(\text{decode}(w))(\{0,1\}^*) = \{u\}\}$
(Berechnet $\text{decode}(w)$ konstante partielle Funktion?)
- Nicht verkürzend $\{w \mid \forall v \forall u \in T(\text{decode}(w))(\{v\}): |u| \geq |v|\}$
(Ist Ausgabe immer mind. so lang wie Eingabe?)

Problem-Reduktionen

Notizen

- Problem $L = \{w \mid T(\text{decode}(w)) = f\}$ für nicht berechenbares f ist entscheidbar denn $L = \emptyset$
(keine det. TM berechnet nicht berechenbare Funktion)
- Fall wäre $\mathcal{F} = \{f\}$, aber $\mathcal{F} \not\subseteq \mathcal{R}$

Zusammenfassung

- Unentscheidbarkeit spezielles Halteproblem
- Problem-Reduktion
- Satz von Rice

Sechste Übungsserie bereits im Moodle