Berechenbarkeit und Komplexität
7. Vorlesung

Prof. Dr. Dietrich Kuske

FG Automaten und Logik, TU Ilmenau

Sommersemester 2023

Um die Grenzen dessen auszuloten, was berechnet werden kann, werden wir in diesem Kapitel Entscheidungsprobleme kennenlernen, die nicht von einem Algorithmus gelöst werden können, d.h., die „(algorithmisch) unentscheidbar“ sind.

Formal ist hierbei ein Entscheidungsproblem eine Sprache (die Menge aller „Probleminstanzen“, auf die die Antwort „ja“ sein muß).

Beispiel: das Wortproblem

Sei G eine Grammatik und das Problem sei $L(G)$.

Automaten und Formale Sprachen (Folie 2.24): $L(G)$ entscheidbar für G vom Typ 1.

später: es gibt Grammatik G, deren Wortproblem unentscheidbar ist.

Beispiel: das allgemeine Wortproblem

Das allgemeine Wortproblem ist die Menge

$$\{(G, w) \mid w \in L(G),\ G \text{ Grammatik}\},$$

wobei die Paare (G, w) geeignet als Zeichenketten kodiert werden müssen.

später: das allgemeine Wortproblem ist unentscheidbar.

Beispiel: das Schnittproblem

Das Schnittproblem für kontextfreie Grammatiken ist die Menge

$$\Big\{(G_1, G_2) \;\Big|\; \begin{array}{l} G_1, G_2 \text{ kontextfreie Grammatiken,} \\ L(G_1) \cap L(G_2) = \varnothing \end{array}\Big\}.$$

später: das Schnittproblem ist unentscheidbar.

Beispiel: allgemeines Halteproblem

Das Halteproblem ist die Menge aller Paare (M, x), wobei M eine TM ist und $x \in \{0, 1\}^*$, so daß M bei Eingabe von x hält.

später: das allgemeine Halteproblem ist unentscheidbar
(und aus seiner Unentscheidbarkeit folgen die anderen).

Entscheidbarkeit

Definition

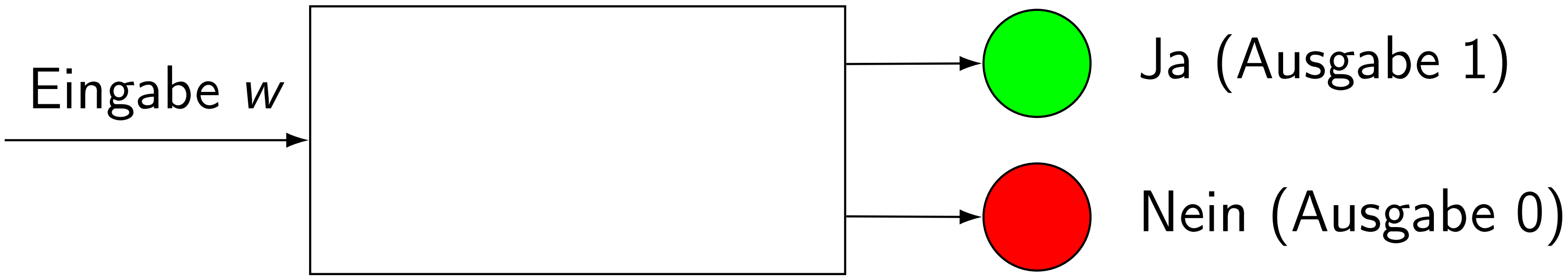
Eine Sprache $L \subseteq \Sigma^*$ heißt entscheidbar, falls die charakteristische Funktion von L, d.h. die Funktion $\chi_L \colon \Sigma^* \to \{0, 1\}$ mit

$$\chi_L(w) = \begin{cases} 1 & \text{falls } w \in L \\ 0 & \text{falls } w \notin L \end{cases}$$

berechenbar ist.

Eine Sprache, die nicht entscheidbar ist, heißt unentscheidbar.

Darstellung der Entscheidbarkeit an einem Maschinenmodell:



Bei jeder Eingabe rechnet die Maschine endliche Zeit und gibt dann entweder „Ja“ oder „Nein“ aus.

Halteproblem

Unser Ziel ist es nun zu beweisen, daß das Halteproblem unentscheidbar ist.

Halteproblem (informell)

- **Eingabe:** Turing-Maschine M und deren Eingabe x.
- **Frage:** Hält M auf x?

Dazu werden wir jedoch zunächst genauer definieren, wie eine Turing-Maschine kodiert werden kann, um als Eingabe einer berechenbaren Funktion verwendet zu werden.

Ziel: Kodierung von Turing-Maschinen über dem Alphabet $\Sigma = \{0, 1\}$.

Annahme: alle Elemente von Γ (Bandalphabet) bzw. Z (Zustandsmenge) sind durchnummeriert und Endzustände (E) haben großen Index:

$$\begin{aligned}
\Gamma &= \{a_0, a_1, \ldots, a_k\}, \quad \square = a_0 \\
Z &= \{z_0, z_1, \ldots, z_n\} \\
E &= \{z_m, z_{m+1}, \ldots, z_n\}
\end{aligned}$$

Um die berechnete Funktion zu bestimmen, reichen die Kenntnis von δ und E (bzw. m).

Kodierung:

1. Für $i, j, i', j' \in \mathbb{N}$ und $y \in \{L, N, R\}$ sei

$$\begin{aligned} w_{i,j,i',j',y} &= 0\,0\,1^{i+1}\,0\,1^{j+1}\,0\,1^{i'+1}\,0\,1^{j'+1}\,0\,code(y) \\ &\in 0(01^+)^4 0\,\{1, 11, 111\} =: L_{Tr}\,. \end{aligned}$$

Dabei ist $code(y) = \begin{cases} 1 & \text{falls } y = L \\ 11 & \text{falls } y = N \\ 111 & \text{falls } y = R \end{cases}$

2. Kodierung der TM: Konkatenation aller Wörter $w_{i,j,i',j',y}$ für $z_i \in Z$, $a_j \in \Gamma$ und $(z_{i'}, a_{j'}, y) = \delta(z_i, a_j)$ in beliebiger Reihenfolge, gefolgt von 01^{m+1} (um die Endzustände zu kodieren).

Bemerkungen:

1. Jede TM hat mehrere Kodes oder „Namen“ (da die Wörter $w_{i,j,i',j',y}$ in beliebiger Reihenfolge aufgezählt werden).
2. Jeder Kode einer TM gehört zur Sprache

$$L_{TM} = (L_{Tr})^* \, 01^+ \, .$$

3. Nicht jedes Wort dieser Sprache entsteht wie oben beschrieben aus einer Turingmaschine.

Dekodierung:
Fixiere zunächst eine Turing-Maschine $\widehat{M}$.
Sei $w \in L_{TM}$. Mit M_w bezeichnen wir die Turing-Maschine, die die Kodierung w hat. Falls w nicht die Kodierung einer Turing-Maschine ist, so setzen wir $M_w = \widehat{M}$.
Weiterhin ist $\varphi_w\colon \{0,1\}^* \dashrightarrow \{0,1\}^*$ die von M_w berechnete partielle Funktion.

Bemerkung:
Viele der Festlegungen bei dieser Kodierung sind absolut willkürlich.
Wichtig ist hier nur, daß es eine mögliche Kodierung gibt (von der wir später benötigen werden, daß sie Eigenschaften wie im Lemma auf Folie 7.25 hat).

Damit können wir nun zwei verschiedene Varianten des Halteproblems definieren.

Definition

Das allgemeine Halteproblem ist die Sprache

$$H = \left\{ w\#x \;\middle|\; w \in L_{TM}, x \in \{0,1\}^*, M_w \text{ angesetzt auf } x \text{ hält} \right\}.$$

Das spezielle Halteproblem ist die Sprache

$$K = \{ w \in L_{TM} \mid M_w \text{ angesetzt auf } w \text{ hält} \}.$$

Man beachte die Selbstbezüglichkeit! Hier wird eine Turing-Maschine auf ihre eigene Kodierung angesetzt.

Satz

Das spezielle Halteproblem $K = \left\{ w \in L_{TM} \;\middle|\; M_w \text{ angesetzt auf } w \text{ hält} \right\}$ ist unentscheidbar.

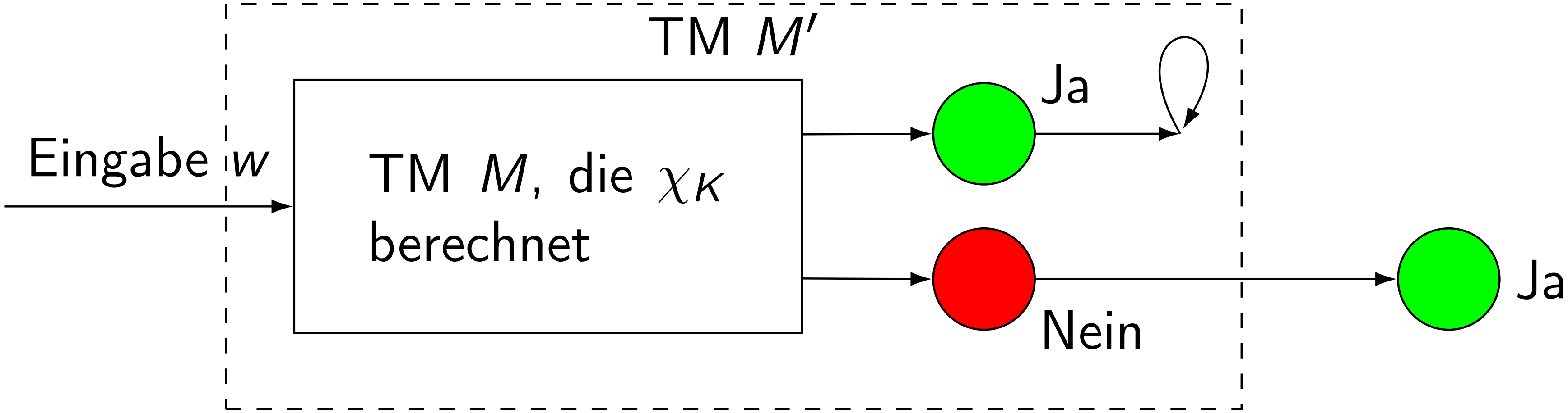
Beweis:

Angenommen K ist entscheidbar, d.h. die charakteristische Funktion $\chi_K : \{0,1\}^* \to \{0,1\}$ wird durch eine Turing-Maschine M berechnet.

Dann existiert eine TM M', die sich wie folgt verhält:

`input` $w \in \{0,1\}^*$
Simuliere M auf Eingabe w (d.h. berechne $\chi_K(w)$)
`if` $\chi_K(w) = 0$
 then gib 1 aus
 `else` gehe in Endlosschleife über
`endif`

Veranschaulichung der Turing-Maschine M':



Sei w' ein Kode der TM M', d.h. $w' \in L_{TM}$ und $M' = M_{w'}$.
Dann erhalten wir den folgenden Widerspruch:

$$\begin{array}{rcl} M' \text{ hält bei Eingabe } w' & \iff & M \text{ gibt } 0 \text{ bei Eingabe } w' \text{ aus} \\ & \iff & \chi_K(w') = 0 \\ & \iff & w' \notin K \\ & \iff & M' = M_{w'} \text{ hält bei Eingabe } w' \text{ nicht} \end{array}$$

$\square$

Es handelt sich hierbei wieder um einen Diagonalisierungsbeweis:

Sei $L_{TM} = \{w_0, w_1, w_2, \ldots\}$

Wir tragen in eine Tabelle folgendes ein: „Wie verhält sich M_{w_i} auf w_j?“

Es gibt zwei Möglichkeiten: H (M_{w_i} hält) oder HN (M_{w_i} hält nicht).

	w_0	w_1	w_2	w_3	w_4	$\cdots$
M_{w_0}	H	HN	H	H	HN	$\cdots$
M_{w_1}	H	HN	HN	H	H	$\cdots$
M_{w_2}	HN	HN	H	HN	HN	$\cdots$
M_{w_3}	H	H	H	H	H	$\cdots$
M_{w_4}	HN	HN	H	HN	H	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	

	w_0	w_1	w_2	w_3	w_4	$\cdots$
M_{w_0}	H HN	HN	H	H	HN	$\cdots$
M_{w_1}	H	HN H	HN	H	H	$\cdots$
M_{w_2}	HN	HN	H HN	HN	HN	$\cdots$
M_{w_3}	H	H	H	H HN	H	$\cdots$
M_{w_4}	HN	HN	H	HN	H HN	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	

	w_0	w_1	w_2	w_3	w_4	$\cdots$	w'
M_{w_0}	H HN	HN	H	H	HN	$\cdots$	H
M_{w_1}	H	HN H	HN	H	H	$\cdots$	HN
M_{w_2}	HN	HN	H HN	HN	HN	$\cdots$	H
M_{w_3}	H	H	H	H HN	H	$\cdots$	HN
M_{w_4}	HN	HN	H	HN	H HN	$\cdots$	HN
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$		$\vdots$
$M_{w'}$	HN	H	HN	HN	HN	$\cdots$	H HN

Die konstruierte Turing-Maschine M' und ein w' mit $M' = M_{w'}$ sind ebenfalls in die Tabelle eingetragen.

Aufgrund der Konstruktion von M': die Felder in der Diagonalen bedingen die Felder in der Zeile von M'.

Problem: nichts paßt in der Zeile $M_{w'}$ und die Spalte w'!

$\leadsto$ es kann keine Turing-Maschine geben, die das spezielle Halteproblem löst.

Reduktionen

Wir haben die Unentscheidbarkeit eines Problems, des speziellen Halteproblems, nachgewiesen.

Daraus sollen weitere Unentscheidbarkeitsresultate gewonnen werden.

Dies erfolgt mit Argumentationen folgender Art:

1. Wenn man Problem B lösen könnte, dann könnte man auch A lösen (Reduktionsschritt). Das Problem B ist also „schwieriger“ bzw. „allgemeiner“ ist als A ($A \leq B$).
2. Wir wissen jedoch bereits, daß A unentscheidbar ist.
3. Also muß das schwierigere Problem B auch unentscheidbar sein.

Definition

Seien $A \subseteq \Sigma^*$, $B \subseteq \Gamma^*$. Eine Reduktion von A auf B ist eine totale und berechenbare Funktion $f\colon \Sigma^* \to \Gamma^*$, so daß für alle $w \in \Sigma^*$ gilt:

$$w \in A \iff f(w) \in B.$$

A heißt auf B reduzierbar (in Zeichen $A \leq B$), falls es eine Reduktion von A auf B gibt.

Bemerkung „Reduktion“ kommt von lat. *reductio* = Zurückführung

„f ist Reduktion von A auf B“ heißt also „Die Frage, ob ein Wort w zu A gehört, kann zurückgeführt werden auf die Frage, ob $f(w)$ zu B gehört.“

Lemma

Seien $A, B \subseteq \Sigma^*$, $A \leq B$ und sei B entscheidbar. Dann ist auch A entscheidbar.

Beweis: Wegen $A \leq B$ existiert eine Reduktion von A auf B, d.h. eine berechenbare totale Funktion $f : \Sigma^* \to \Sigma^*$ mit

$$w \in A \iff f(w) \in B$$

für alle $w \in \Sigma^*$.
Es folgt $\chi_A(w) = \chi_B\big(f(w)\big)$ für alle $w \in \Sigma^*$. Also ist $\chi_A = \chi_B \circ f = \mathrm{subst}(\chi_B; f)$ und damit berechenbar, d.h. A ist entscheidbar. □

Kochrezept um die Unentscheidbarkeit eines Problems B zu zeigen

- Finde ein geeignetes Problem A, von dem bekannt ist, daß es unentscheidbar ist.

  (Bisher kennen wir nur das spezielle Halteproblem K, wir werden allerdings bald weitere geeignete Probleme kennenlernen.)
- Finde eine geeignete Funktion f, die A auf B reduziert.
- Dann folgt, daß B unentscheidbar ist.

Satz

Das allgemeine Halteproblem

$$H = \left\{ w\#x \;\middle|\; w \in L_{TM}, x \in \{0,1\}^*, M_w \text{ angesetzt auf } x \text{ hält} \right\}$$

ist unentscheidbar.

Beweis: Sei die totale berechenbare Funktion f definiert durch $f(w) = w\#w$ für $w \in \{0,1\}^*$.

Dann gilt für alle $w \in \{0,1\}^*$:

$$w \in K \iff w\#w \in H \iff f(w) \in H\,.$$

Also ist die Funktion f eine Reduktion von K auf H, d.h. es gilt $K \leq H$.

Da K nach dem Satz auf Folie 7.14 unentscheidbar ist, muß auch H unentscheidbar sein. □

Das Halteproblem mit leerer Eingabe

Ziel: Unentscheidbarkeit des Halteproblems mit leerer Eingabe

$$H_0 = \{w \in L_{TM} \mid M_w \text{ hält angesetzt auf ein leeres Band}\}$$

Idee: Gegeben ist ein $w \in L_{TM}$, also eine Turingmaschine M_w.

- es gibt Turingmaschine M'_w, die
  - zunächst w vor die Eingabe schreibt
  - und sich dann wie die Turingmaschine M_w verhält.
- Sei w' ein Kode der Maschine M'_w, d.h. $M'_w = M_{w'}$.
- dann gilt: $w \in K$ gdw. M_w hält bei Eingabe w
  gdw. M'_w hält bei leerer Eingabe
  gdw. $w' \in H_0$

Die Abbildung $f\colon L_{TM} \to L_{TM}\colon w \mapsto w'$ scheint also Reduktion von K auf H_0 zu sein. Hierzu muß sie aber berechenbar sein!

Rechnen mit Kodierungen

etwas allgemeiner:
Sei M eine Turing-Maschine und $x \in \{0,1\}^*$. Dann existiert eine Turing-Maschine M', die zunächst x vor die Eingabe schreibt und dann M simuliert.

Frage: Können wir aus einem Kode w für M und dem Wort x einen Kode w' für M' berechnen?

Lemma

Es gibt eine berechenbare Funktion $f : \{0,1,\#\}^* \to L_{TM}$, so daß für alle $w \in L_{TM}$ und $x, y \in \{0,1\}^*$ gilt:

$$\varphi_{f(w\#x)}(y) = \varphi_w(xy)$$

Insbes. hält die TM $M_{f(w\#x)}$ bei Eingabe y genau dann, wenn die TM M_w bei Eingabe von xy anhält.

Beweis:

Hinweis: Uns interessieren nur die Eingaben $w\#x \in L_{TM}\#\{0,1\}^*$ mit $x = a_n a_{n-1} \cdots a_1$, bei anderen Argumenten kann f beliebige Ergebnisse produzieren.

Die gewünschte Maschine $M_{f(w\#x)}$ erhält man durch

- zusätzliche Zustände $p_0, \ldots, p_{n+1}$,
- zusätzliche Regeln $\delta(p_0, a) = (p_1, a, L)$ und $\delta(p_i, a) = (p_{i+1}, a_i, L)$ f.a. $a \in \Gamma$ und $0 < i \leq n$
- zusätzliche Regeln $\delta(p_{n+1}, a) = (z_0, a, R)$ f.a. $a \in \Gamma$
- und die Forderung, daß p_0 der neue Startzustand ist.

Eine Kodierung dieser Maschine erhält man, indem

- alle Zustände in w um $n + 2$ erhöht und
- Kodierungen der neuen Regeln dem Wort w vorangestellt werden. □

Satz

Das Halteproblem auf leerem Band

$$H_0 = \{w \in L_{TM} \mid M_w \text{ hält angesetzt auf ein leeres Band}\}$$

ist unentscheidbar.

Beweis: Betrachte die berechenbare totale Funktion f aus dem Lemma auf Folie 7.25.
Wir zeigen, daß f Reduktion von H auf H_0 ist:

$$\begin{aligned}
u \in H \quad &\Longleftrightarrow \quad u = w\#x \text{ mit } w \in L_{TM}, x \in \{0,1\}^* \text{ und} \\
& \quad M_w \text{ hält bei Eingabe } x \\
&\Longleftrightarrow \quad u \in L_{TM}\#\{0,1\}^* \text{ und } M_{f(u)} \text{ hält bei Eingabe } \varepsilon \\
&\Longleftrightarrow \quad f(u) \in H_0
\end{aligned}$$

$\square$

Zusammenfassung 7. Vorlesung

in dieser Vorlesung neu

- Entscheidung von Problemen mittels Turingmaschinen
- K, H und H_0 können nicht von Turingmaschinen entschieden werden
  Beweistechniken: Diagonalisierung, Reduktionen, Rechnen mit Kodierungen

kommende Vorlesung

- keine Eigenschaft des Verhaltens von M_w kann von einer Turingmaschine entschieden werden
- aber viele können „zur Hälfte" entschieden werden (was zum natürlichen Begriff der „Semientscheidbarkeit" führt).