Unentscheidbare Probleme: Diagonalisierung

Prof. Dr. Berthold Vöcking
Lehrstuhl Informatik 1
Algorithmen und Komplexität
RWTH Aachen

Oktober 2011

Wdh: Die Church-Turing-These

Kein jemals bisher vorgeschlagenes „vernünftiges“ Rechnermodell hat eine größere Mächtigkeit als die TM.

Diese Einsicht hat Church zur Formulierung der folgenden These veranlasst.

Church-Turing-These

Die Klasse der TM-berechenbaren Funktionen stimmt mit der Klasse der “intuitiv berechenbaren” Funktionen überein.

Wir werden deshalb nicht mehr von *TM-berechenbaren* Funktionen sprechen, sondern allgemein von *berechenbaren* Funktionen.

Gleichbedeutend verwenden wir den Begriff *rekursive* Funktion bzw. *rekursive* oder auch *entscheidbare* Sprache.

Gibt es nicht-rekursive Probleme?

Ja, es gibt nicht-rekursive Probleme,

denn die Mächtigkeit der Menge aller Sprachen ist größer

als die Mächtigkeit der Menge aller TMen.

Exkursion: abzählbare und überabzählbare Mengen

Def: abzählbare Menge

Eine Menge M heißt *abzählbar*, wenn es eine surjektive Funktion $c : \mathbb{N} \to M$ gibt.

Jede endliche Menge M ist offensichtlich abzählbar.

Im Fall einer abzählbar unendlichen Menge M gibt es immer auch eine bijektive Abbildung $c : \mathbb{N} \to M$, denn Wiederholungen können bei der Abzählung offensichtlich ausgelassen werden. Die Elemente einer abzählbaren Menge können also *nummeriert* werden.

Abzählbar unendliche Mengen haben somit dieselbe Mächtigkeit wie die Menge der natürlichen Zahlen $\mathbb{N}$.

Exkursion: abzählbare und überabzählbare Mengen

Beispiele für abzählbar unendliche Mengen:

- die Menge der ganzen Zahlen $\mathbb{Z}$:

$$c(i) = \begin{cases} i/2 & \text{falls } i \text{ gerade} \\ -(i+1)/2 & \text{falls } i \text{ ungerade} \end{cases}$$

- die Menge der rationalen Zahlen $\mathbb{Q}$
- Σ^*, die Menge der Wörter über einem endlichen Alphabet Σ

Beispiel: $\{0,1\}^*$ in kanonischer Reihenfolge

$$\epsilon, 0, 1, 00, 01, 10, 11, 000, 001, 010, 011, 100, 101, \ldots$$

Exkursion: abzählbare und überabzählbare Mengen

Beispiele für abzählbar unendliche Mengen:

- die Menge der Gödelnummern, da Gödelnummern Wörter über dem Alphabet $\{0, 1\}$ sind, und somit auch
- die Menge der TMen, weil jede TM durch eine eindeutige Gödelnummer beschrieben wird.

Das *i-te Wort* gemäß der kanonischen Reihenfolge bezeichnen wir im Folgenden mit w_i und die *i-te TM* mit M_i.

Exkursion: abzählbare und überabzählbare Mengen

Nun betrachte die *Potenzmenge* $\mathcal{P}(\mathbb{N})$, also die Menge aller Teilmengen von $\mathbb{N}$.

Satz:

Die Menge $\mathcal{P}(\mathbb{N})$ ist überabzählbar.

Beweis: (Diagonalisierung)

- Zum Zweck des Widerspruchs nehmen wir an, dass $\mathcal{P}(\mathbb{N})$ abzählbar ist.
- Mit S_i bezeichnen wir die i-te Menge aus $\mathcal{P}(\mathbb{N})$.
- Wir definieren eine zwei-dimensionale unendliche Matrix $(A_{i,j})_{i\in\mathbb{N},j\in\mathbb{N}}$ mit

$$A_{i,j} = \begin{cases} 1 & \text{falls } j \in S_i \\ 0 & \text{sonst} \end{cases}$$

Exkursion: abzählbare und überabzählbare Mengen

Illustration: die Matrix A könnte etwa folgendermaßen aussehen

	0	1	2	3	4	5	6	
S_0	**0**	1	1	0	1	0	1	$\cdots$
S_1	1	**1**	1	0	1	0	1	$\cdots$
S_2	0	0	**1**	0	1	0	1	$\cdots$
S_3	0	1	1	**0**	0	0	1	$\cdots$
S_4	0	1	0	0	**1**	0	1	$\cdots$
S_5	0	1	1	0	1	**0**	0	$\cdots$
S_6	1	1	1	0	1	0	**1**	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$		

Wir definieren die Menge

$$S_{diag} = \{i \in \mathbb{N} \mid A_{i,i} = 1\}.$$

Das Komplement dieser Menge ist

$$\bar{S}_{diag} = \mathbb{N} \setminus S_{diag} = \{i \in \mathbb{N} \mid A_{i,i} = 0\}.$$

Exkursion: abzählbare und überabzählbare Mengen

- Beachte: Auch $\bar{S}_{diag}$ ist eine Teilmenge von $\mathbb{N}$ und kommt somit in der Aufzählung $S_1, S_2, \ldots$ von $\mathcal{P}(\mathbb{N})$ vor.
- Es gibt also ein $k \in \mathbb{N}$, so dass $\bar{S}_{diag} = S_k$.
- Jetzt gibt es zwei Fälle, die jeweils zum Widerspruch führen.
  - **Fall 1:**

$$A_{k,k} = 1 \overset{Def.\bar{S}_{diag}}{\Rightarrow} k \notin \bar{S}_{diag} \Rightarrow k \notin S_k \overset{Def.A}{\Rightarrow} A_{k,k} = 0$$

Widerspruch!

  - **Fall 2:**

$$A_{k,k} = 0 \overset{Def.\bar{S}_{diag}}{\Rightarrow} k \in \bar{S}_{diag} \Rightarrow k \in S_k \overset{Def.A}{\Rightarrow} A_{k,k} = 1$$

Widerspruch!

- Folglich gibt es keine Aufzählung von $\mathcal{P}(\mathbb{N})$ $\square$

Wie viele verschiedene Entscheidungsprobleme gibt es?

Jedes Entscheidungsproblem mit binär kodierter Eingabe entspricht einer Sprache über dem Alphabet $\{0,1\}$ und umgekehrt.

Eine Sprache L über dem Alphabet $\{0,1\}$ ist eine Teilmenge von $\{0,1\}^*$.

Sei $\mathcal{L}$ die Menge aller Sprachen (bzw. Entscheidungsprobleme) über $\{0,1\}^*$.

$\mathcal{L}$ ist somit die Menge aller Teilmengen also die Potenzmenge über $\{0,1\}^*$, d.h $\mathcal{L} = \mathcal{P}(\{0,1\}^*)$.

Wir beobachten:

- $\{0,1\}^*$ hat dieselbe Mächtigkeit wie $\mathbb{N}$.
- $\mathcal{L} = \mathcal{P}(\{0,1\}^*)$ hat somit dieselbe Mächtigkeit wie $\mathcal{P}(\mathbb{N})$.

Die Menge der Entscheidungsprobleme $\mathcal{L}$ ist also überabzählbar.

Existenz unentscheidbarer Probleme

Es gibt überabzählbar viele Sprachen.

Aber es gibt nur abzählbar viele TMen.

Schlussfolgerung

Es gibt nicht-rekursive Sprachen.

Die reine Existenz unentscheidbarer Probleme ist noch nicht dramatisch, denn es könnte sich ja um uninteressante, nicht praxis-relevante Probleme handeln. Leider werden wir sehen, dass diese Hoffnung sich nicht bestätigt.

Das Halteproblem

Beim *Halteproblem* geht es darum, zu entscheiden, ob ein gegebenes Programm mit einer gegebenen Eingabe terminiert.

In der Notation der TMen ergibt sich die folgende formale Problemdefinition.

$$H = \{\langle M \rangle w \mid M \text{ hält auf } w\} \ .$$

Es wäre äußerst hilfreich, wenn Compiler das Halteproblem entscheiden könnten. Wir werden jedoch sehen, dass dieses elementare Problem nicht entscheidbar ist.

Unentscheidbarkeit der Diagonalsprache

Zum Beweis der Unentscheidbarkeit des Halteproblems machen wir einen Umweg über die sogenannte *Diagonalsprache*.

$$D = \{ w \in \{0,1\}^* \mid w = w_i \text{ und } M_i \text{ akzeptiert } w \text{ nicht} \} .$$

Anders gesagt, das i-te Wort bzgl. der kanonischen Reihenfolge, also w_i, ist genau dann in D, wenn die i-te TM, also M_i, dieses Wort nicht akzeptiert.

Satz:

Die Diagonalsprache D ist nicht rekursiv.

Unentscheidbarkeit der Diagonalsprache – Intuition

Warum trägt die Sprache den Namen *Diagonalsprache*? – Betrachte eine unendliche binäre Matrix A mit

$$A_{i,j} = \begin{cases} 1 & \text{falls } M_i \text{ akzeptiert } w_j \\ 0 & \text{sonst} \end{cases}$$

Beispiel:

	w_0	w_1	w_2	w_3	w_4	
M_0	**0**	1	1	0	1	$\cdots$
M_1	1	**0**	1	0	1	$\cdots$
M_2	0	0	**1**	0	1	$\cdots$
M_3	0	1	1	**1**	0	$\cdots$
M_4	0	1	0	0	**0**	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	

Die Diagonalsprache läßt sich auf der Diagonale der Matrix ablesen. Es ist

$$D = \{w_i \mid A_{i,i} = 0\} .$$

Unentscheidbarkeit der Diagonalsprache – Beweis

Beweis:

Wir führen einen Widerspruchsbeweis und nehmen an, D ist rekursiv. Dann gibt es eine TM M_j, die D entscheidet.

Wir starten die TM M_j mit der Eingabe w_j. Es ergeben sich zwei Fälle, die jeweils direkt zum Widerspruch führen.

- **Fall 1:**

$$w_j \in D \overset{M_j \text{ entsch. } D}{\Rightarrow} M_j \text{ akzeptiert } w_j \overset{\text{Def. von } D}{\Rightarrow} w_j \notin D$$

Widerspruch!

- **Fall 2:**

$$w_j \notin D \overset{M_j \text{ entsch. } D}{\Rightarrow} M_j \text{ akzeptiert } w_j \text{ nicht} \overset{\text{Def. von } D}{\Rightarrow} w_j \in D$$

Widerspruch!

□