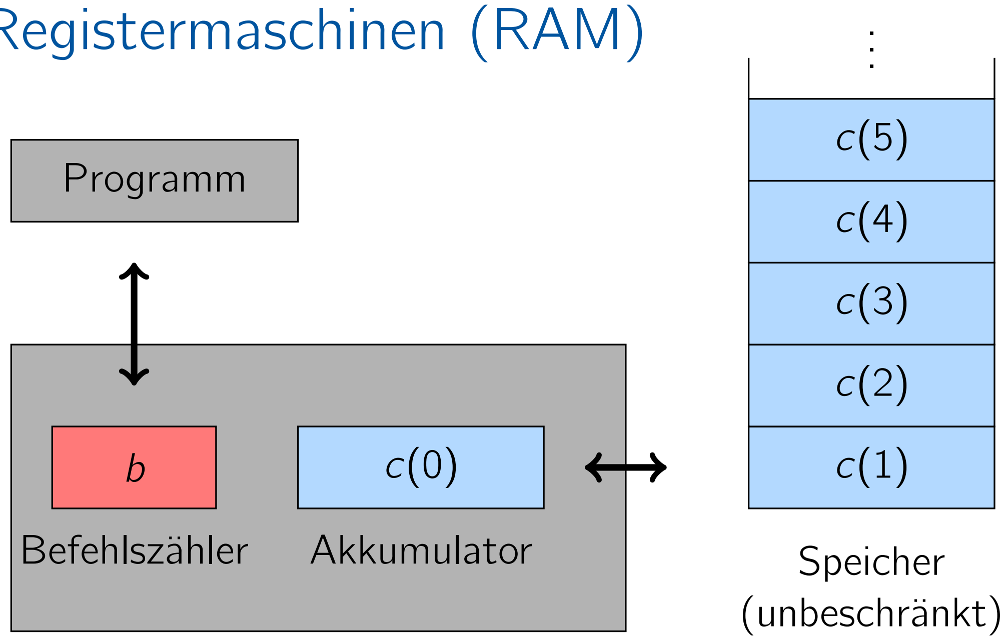
Teil II
Berechenbarkeit

Vorlesung 5
Unentscheidbare Probleme: Diagonalisierung

Wdh.: Registermaschinen (RAM)



Befehlssatz:

LOAD, STORE, ADD, SUB, MULT, DIV
INDLOAD, INDSTORE, INDADD, INDSUB, INDMULT, INDDIV
CLOAD, CADD, CSUB, CMULT, CDIV
GOTO, IF c(0)?x THEN GOTO j (wobei ? aus {=,<,<=,>,>=} ist),
END

Wdh.: RAM vs. TM

Satz (RAM → TM)

Für jede im logarithmischen Kostenmaß $t(n)$-zeitbeschränkte RAM R gibt es ein Polynom q und zu diesem eine $O\big(q(n+t(n))\big)$-TM M, die R simuliert.

Satz (TM → RAM)

Jede $t(n)$-zeitbeschränkte TM kann durch eine RAM simuliert werden, die zeitbeschränkt ist durch

- $O(t(n)+n)$ *im uniformen Kostenmaß und*
- $O((t(n)+n)\cdot\log(t(n)+n))$ *im logarithmischen Kostenmaß.*

Wdh.: Hintereinanderausführung von Polynomen

Beobachtung

Die Klasse der Polynome ist unter Hintereinanderausführung abgeschlossen.

(Wenn $p(x)$ und $q(x)$ Polynome sind, dann ist $p(q(x))$ ein Polynom.

Des Weiteren gilt für Polynome p, q:
Wenn $t(n) \in O(p(n))$ und $t'(n) \in O(q(n))$ dann $t(t'(n)) \in O(p(q(n)))$.

Wdh.: Die Church-Turing-These

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

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 Klassen der TM-berechenbaren (partiellen) Funktionen und TM-entscheidbaren Sprachen stimmen mit den Klassen der “intuitiv berechenbaren” (partiellen) Funktionen bzw. “intuitiv entscheidbaren” Sprachen überein.

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 Klassen der TM-berechenbaren (partiellen) Funktionen und TM-entscheidbaren Sprachen stimmen mit den Klassen der “intuitiv berechenbaren” (partiellen) Funktionen bzw. “intuitiv entscheidbaren” Sprachen überein.

Wir werden deshalb nicht mehr von TM-berechenbaren (partiellen) Funktionen oder TM-entscheidbaren Sprachen sprechen, sondern allgemein von berechenbaren (partiellen) Funktionen bzw. entscheidbaren Sprachen.

Gibt es unentscheidbare Probleme?

Terminologie: unentscheidbar bedeutet einfach “nicht entscheidbar”

Gibt es unentscheidbare Probleme?

Terminologie: unentscheidbar bedeutet einfach “nicht entscheidbar”

Ja, es gibt unentscheidbare Probleme

Gibt es unentscheidbare Probleme?

Terminologie: unentscheidbar bedeutet einfach “nicht entscheidbar”

Ja, es gibt unentscheidbare Probleme,

denn die Mächtigkeit der Menge aller Sprachen ist größer

als die Mächtigkeit der Menge aller TMen.

Exkurs: abzählbare und überabzählbare Mengen

Definition (Abzählbare Menge)

Eine Menge M heißt abzählbar, wenn sie leer ist oder wenn es eine surjektive Funktion $c\colon \mathbb{N} \to M$ gibt.

Exkurs: abzählbare und überabzählbare Mengen

Definition (Abzählbare Menge)

Eine Menge M heißt abzählbar, wenn sie leer ist oder wenn es eine surjektive Funktion $c\colon \mathbb{N} \to M$ gibt.

- Jede endliche Menge M ist abzählbar.

Exkurs: abzählbare und überabzählbare Mengen

Definition (Abzählbare Menge)

Eine Menge M heißt abzählbar, wenn sie leer ist oder wenn es eine surjektive Funktion $c\colon \mathbb{N} \to M$ gibt.

- Jede endliche Menge M ist abzählbar.

- Im Fall einer abzählbar unendlichen Menge M gibt es immer auch eine bijektive Abbildung $c\colon \mathbb{N} \to M$, denn Wiederholungen können bei der Abzählung offensichtlich ausgelassen werden.

Exkurs: abzählbare und überabzählbare Mengen

Definition (Abzählbare Menge)

Eine Menge M heißt abzählbar, wenn sie leer ist oder wenn es eine surjektive Funktion $c\colon \mathbb{N} \to M$ gibt.

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

Exkurs: abzählbare und überabzählbare Mengen

Definition (Abzählbare Menge)

Eine Menge M heißt abzählbar, wenn sie leer ist oder wenn es eine surjektive Funktion $c\colon \mathbb{N} \to M$ gibt.

- Jede endliche Menge M ist abzählbar.
- Im Fall einer abzählbar unendlichen Menge M gibt es immer auch eine bijektive Abbildung $c\colon \mathbb{N} \to M$, 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 $\mathbb{Z}$:

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

Exkursion: abzählbare und überabzählbare Mengen

Beispiele für abzählbar unendliche Mengen

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

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

$$0, -1, 1, -2, 2, -3, 3, -4, 4, \ldots,$$

- die Menge der rationalen Zahlen $\mathbb{Q}$

Exkursion: abzählbare und überabzählbare Mengen

Beispiele für abzählbar unendliche Mengen

- die Menge der ganzen Zahlen $\mathbb{Z}$:
$$c(i) = \begin{cases} i/2 & \text{falls } i \text{ gerade} \\ -(i+1)/2 & \text{falls } i \text{ ungerade} \end{cases}$$
$$0, -1, 1, -2, 2, -3, 3, -4, 4, \dots,$$
- die Menge der rationalen Zahlen $\mathbb{Q}$
$$0, \frac{1}{1}, \frac{2}{1}, \frac{1}{2}, \frac{3}{1}, \dots, \frac{i}{1}, \frac{i-1}{2}, \frac{i-2}{3}, \dots \frac{1}{i}, \dots$$

Abzählbarkeit der rationalen Zahlen

	1	2	3	4	5	6	$\cdots$
1	1/1	2/1	3/1	4/1	5/1	6/1	
2	1/2	2/2	3/2	4/2	5/2	6/2	
3	1/3	2/3	3/3	4/3	5/3	6/3	$\cdots$
4	1/4	2/4	3/4	4/4	5/4	6/4	
5	1/5	2/5	3/5	4/5	5/5	6/5	
6	1/6	2/6	3/6	4/6	5/6	6/6	
$\vdots$				$\vdots$			$\ddots$

Abzählbarkeit der rationalen Zahlen

	1	2	3	4	5	6	$\cdots$
1	1/1	2/1	3/1	4/1	5/1	6/1	
2	1/2	2/2	3/2	4/2	5/2	6/2	
3	1/3	2/3	3/3	4/3	5/3	6/3	$\cdots$
4	1/4	2/4	3/4	4/4	5/4	6/4	
5	1/5	2/5	3/5	4/5	5/5	6/5	
6	1/6	2/6	3/6	4/6	5/6	6/6	
$\vdots$				$\vdots$			$\ddots$

Abzählbarkeit der rationalen Zahlen

	1	2	3	4	5	6	$\cdots$
1	1/1	2/1	3/1	4/1	5/1	6/1	
2	1/2	2/2	3/2	4/2	5/2	6/2	
3	1/3	2/3	3/3	4/3	5/3	6/3	$\cdots$
4	1/4	2/4	3/4	4/4	5/4	6/4	
5	1/5	2/5	3/5	4/5	5/5	6/5	
6	1/6	2/6	3/6	4/6	5/6	6/6	
$\vdots$				$\vdots$			$\ddots$

Abzählbarkeit der rationalen Zahlen

	1	2	3	4	5	6	$\cdots$
1	1/1	2/1	3/1	4/1	5/1	6/1	
2	1/2	2/2	3/2	4/2	5/2	6/2	
3	1/3	2/3	3/3	4/3	5/3	6/3	$\cdots$
4	1/4	2/4	3/4	4/4	5/4	6/4	
5	1/5	2/5	3/5	4/5	5/5	6/5	
6	1/6	2/6	3/6	4/6	5/6	6/6	
$\vdots$				$\vdots$			$\ddots$

Abzählbarkeit der rationalen Zahlen

	1	2	3	4	5	6	$\cdots$
1	1/1	2/1	3/1	4/1	5/1	6/1	
2	1/2	2/2	3/2	4/2	5/2	6/2	
3	1/3	2/3	3/3	4/3	5/3	6/3	$\cdots$
4	1/4	2/4	3/4	4/4	5/4	6/4	
5	1/5	2/5	3/5	4/5	5/5	6/5	
6	1/6	2/6	3/6	4/6	5/6	6/6	
$\vdots$				$\vdots$			$\ddots$

Abzählbarkeit der rationalen Zahlen

	1	2	3	4	5	6	$\cdots$
1	1/1	2/1	3/1	4/1	5/1	6/1	
2	1/2	2/2	3/2	4/2	5/2	6/2	
3	1/3	2/3	3/3	4/3	5/3	6/3	$\cdots$
4	1/4	2/4	3/4	4/4	5/4	6/4	
5	1/5	2/5	3/5	4/5	5/5	6/5	
6	1/6	2/6	3/6	4/6	5/6	6/6	
$\vdots$				$\vdots$			$\ddots$

Abzählbarkeit der rationalen Zahlen

	1	2	3	4	5	6	$\cdots$
1	1/1	2/1	3/1	4/1	5/1	6/1	
2	1/2	2/2	3/2	4/2	5/2	6/2	
3	1/3	2/3	3/3	4/3	5/3	6/3	$\cdots$
4	1/4	2/4	3/4	4/4	5/4	6/4	
5	1/5	2/5	3/5	4/5	5/5	6/5	
6	1/6	2/6	3/6	4/6	5/6	6/6	
$\vdots$				$\vdots$			$\ddots$

Exkursion: abzählbare und überabzählbare Mengen

Beispiele für abzählbar unendliche Mengen

- die Menge der ganzen Zahlen $\mathbb{Z}$:
$$c(i) \;=\; \begin{cases} i/2 & \text{falls } i \text{ gerade} \\ -(i+1)/2 & \text{falls } i \text{ ungerade} \end{cases}$$
$$0, -1, 1, -2, 2, -3, 3, -4, 4, \dots,$$
- die Menge der rationalen Zahlen $\mathbb{Q}$
$$0, \frac{1}{1}, \frac{2}{1}, \frac{1}{2}, \frac{3}{1}, \dots, \frac{i}{1}, \frac{i-1}{2}, \frac{i-2}{3}, \dots \frac{1}{i}, \dots$$
- Σ^*, die Menge der Wörter über einem endlichen Alphabet Σ
  - Zum Beispiel: $\{0,1\}^*$ in kanonischer Reihenfolge:
$$\epsilon, 0, 1, 00, 01, 10, 11, 000, 001, 010, 011, 100, 101, \dots$$

Exkursion: abzählbare und überabzählbare Mengen

Beispiele für abzählbar unendliche Mengen

- die Menge der ganzen Zahlen $\mathbb{Z}$:
$$c(i) \;=\; \begin{cases} i/2 & \text{falls } i \text{ gerade} \\ -(i+1)/2 & \text{falls } i \text{ ungerade} \end{cases}$$
$$0, -1, 1, -2, 2, -3, 3, -4, 4, \dots,$$
- die Menge der rationalen Zahlen $\mathbb{Q}$
$$0, \frac{1}{1}, \frac{2}{1}, \frac{1}{2}, \frac{3}{1}, \dots, \frac{i}{1}, \frac{i-1}{2}, \frac{i-2}{3}, \dots \frac{1}{i}, \dots$$
- Σ^*, die Menge der Wörter über einem endlichen Alphabet Σ
  - Zum Beispiel: $\{0,1\}^*$ in kanonischer Reihenfolge:
$$\epsilon, 0, 1, 00, 01, 10, 11, 000, 001, 010, 011, 100, 101, \dots$$
  - Zum Beispiel:  in kanonischer Reihenfolge:

Exkursion: abzählbare und überabzählbare Mengen

Beispiele für abzählbar unendliche Mengen

- die Menge der Gödelnummern, da Gödelnummern Wörter über dem Alphabet $\{0, 1\}$ sind

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.

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.

Die i-te Gödelnummer in der kanonischen Reihenfolge von $\{0, 1\}^*$ bezeichnen wir mit w_i, die i-te Turingmaschine mit M_i. Es gilt also $w_i = \langle M_i \rangle$.

Exkursion: abzählbare und überabzählbare Mengen

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

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.

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.

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.
- Sei $S_0, S_1, S_2, S_3, \ldots$ eine Aufzählung von $\mathcal{P}(\mathbb{N})$.

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.
- Sei $S_0, S_1, S_2, S_3, \ldots$ eine Aufzählung von $\mathcal{P}(\mathbb{N})$.
- Wir definieren eine zweidimensionale 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

Die Matrix A könnte etwa folgendermaßen aussehen

$$
\begin{array}{c|ccccccc c}
 & 0 & 1 & 2 & 3 & 4 & 5 & 6 & \\
\hline
S_0 & \mathbf{0} & 1 & 1 & 0 & 1 & 0 & 1 & \cdots \\
S_1 & 1 & \mathbf{1} & 1 & 0 & 1 & 0 & 1 & \cdots \\
S_2 & 0 & 0 & \mathbf{1} & 0 & 1 & 0 & 1 & \cdots \\
S_3 & 0 & 1 & 1 & \mathbf{0} & 0 & 0 & 1 & \cdots \\
S_4 & 0 & 1 & 0 & 0 & \mathbf{1} & 0 & 1 & \cdots \\
S_5 & 0 & 1 & 1 & 0 & 1 & \mathbf{0} & 0 & \cdots \\
S_6 & 1 & 1 & 1 & 0 & 1 & 0 & \mathbf{0} & \cdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & &
\end{array}
$$

Exkursion: abzählbare und überabzählbare Mengen

Die Matrix A könnte etwa folgendermaßen aussehen

$$
\{1, 2, 4, 6, \ldots\} = \quad
\begin{array}{c|ccccccc c}
 & 0 & 1 & 2 & 3 & 4 & 5 & 6 & \\
\hline
S_0 & \mathbf{0} & 1 & 1 & 0 & 1 & 0 & 1 & \cdots \\
S_1 & 1 & \mathbf{1} & 1 & 0 & 1 & 0 & 1 & \cdots \\
S_2 & 0 & 0 & \mathbf{1} & 0 & 1 & 0 & 1 & \cdots \\
S_3 & 0 & 1 & 1 & \mathbf{0} & 0 & 0 & 1 & \cdots \\
S_4 & 0 & 1 & 0 & 0 & \mathbf{1} & 0 & 1 & \cdots \\
S_5 & 0 & 1 & 1 & 0 & 1 & \mathbf{0} & 0 & \cdots \\
S_6 & 1 & 1 & 1 & 0 & 1 & 0 & \mathbf{0} & \cdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & &
\end{array}
$$

Exkursion: abzählbare und überabzählbare Mengen

Die Matrix A könnte etwa folgendermaßen aussehen

$$
\begin{array}{r|ccccccc}
 & 0 & 1 & 2 & 3 & 4 & 5 & 6 \\
\hline
\{1,2,4,6,\dots\} = \quad S_0 & \mathbf{0} & 1 & 1 & 0 & 1 & 0 & 1 & \cdots \\
\{0,1,2,4,6,\dots\} = \quad S_1 & 1 & \mathbf{1} & 1 & 0 & 1 & 0 & 1 & \cdots \\
S_2 & 0 & 0 & \mathbf{1} & 0 & 1 & 0 & 1 & \cdots \\
S_3 & 0 & 1 & 1 & \mathbf{0} & 0 & 0 & 1 & \cdots \\
S_4 & 0 & 1 & 0 & 0 & \mathbf{1} & 0 & 1 & \cdots \\
S_5 & 0 & 1 & 1 & 0 & 1 & \mathbf{0} & 0 & \cdots \\
S_6 & 1 & 1 & 1 & 0 & 1 & 0 & \mathbf{0} & \cdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots &
\end{array}
$$

Exkursion: abzählbare und überabzählbare Mengen

Die Matrix A könnte etwa folgendermaßen aussehen

$$
\begin{array}{c|ccccccc}
 & 0 & 1 & 2 & 3 & 4 & 5 & 6 \\
\hline
S_0 & \mathbf{0} & 1 & 1 & 0 & 1 & 0 & 1 & \cdots \\
S_1 & 1 & \mathbf{1} & 1 & 0 & 1 & 0 & 1 & \cdots \\
S_2 & 0 & 0 & \mathbf{1} & 0 & 1 & 0 & 1 & \cdots \\
S_3 & 0 & 1 & 1 & \mathbf{0} & 0 & 0 & 1 & \cdots \\
S_4 & 0 & 1 & 0 & 0 & \mathbf{1} & 0 & 1 & \cdots \\
S_5 & 0 & 1 & 1 & 0 & 1 & \mathbf{0} & 0 & \cdots \\
S_6 & 1 & 1 & 1 & 0 & 1 & 0 & \mathbf{0} & \cdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots &
\end{array}
$$

Wir definieren die Menge

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

Exkursion: abzählbare und überabzählbare Mengen

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	**0**	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$		

$$S_{\text{diag}} = \{1, 2, 4, \ldots\}$$

Wir definieren die Menge

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

Exkursion: abzählbare und überabzählbare Mengen

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	**0**	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$		

$$S_{\text{diag}} = \{1, 2, 4, \ldots\}$$

Wir definieren die Menge

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

Das Komplement dieser Menge ist

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

Exkursion: abzählbare und überabzählbare Mengen

- Beachte: Auch $\overline{S}_{\text{diag}}$ ist eine Teilmenge von $\mathbb{N}$ und kommt somit in der Aufzählung $S_1, S_2, \ldots$ von $\mathcal{P}(\mathbb{N})$ vor.

Exkursion: abzählbare und überabzählbare Mengen

- Beachte: Auch $\overline{S}_{\text{diag}}$ 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 $\overline{S}_{\text{diag}} = S_k$.

Exkursion: abzählbare und überabzählbare Mengen

- Beachte: Auch $\overline{S}_{\text{diag}}$ 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 $\overline{S}_{\text{diag}} = S_k$.
- Jetzt gibt es zwei Fälle, die jeweils zum Widerspruch führen.

Exkursion: abzählbare und überabzählbare Mengen

- Beachte: Auch $\overline{S}_{\text{diag}}$ 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 $\overline{S}_{\text{diag}} = S_k$.
- Jetzt gibt es zwei Fälle, die jeweils zum Widerspruch führen.
    - Fall 1:

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

Widerspruch!

Exkursion: abzählbare und überabzählbare Mengen

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

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

Widerspruch!

  - Fall 2:

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

Widerspruch!

Exkursion: abzählbare und überabzählbare Mengen

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

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

Widerspruch!

  - Fall 2:

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

Widerspruch!

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

Kardinalitäts-Battle

Welches Ansammlung hat größere Kardinalität?

Kardinalitäts-Battle

1. $\{1, \dots, n\}$ $\mathbb{N}$

Kardinalitäts-Battle

1. $\{1, \dots, n\}$ $<$ $\mathbb{N}$

Kardinalitäts-Battle

1. $\{1, \dots, n\}$ $<$ $\mathbb{N}$

endlich abzählbar unendlich

Kardinalitäts-Battle

1.	$\{1, \ldots, n\}$	$<$	$\mathbb{N}$
	endlich		abzählbar unendlich
2.	$\{☺\}^*$		$\mathcal{P}(\mathbb{N})$

Kardinalitäts-Battle

1.	$\{1, \ldots, n\}$	$<$	$\mathbb{N}$
	endlich		abzählbar unendlich
2.	$\{☺\}^*$	$<$	$\mathcal{P}(\mathbb{N})$

Kardinalitäts-Battle

1. $\{1, \ldots, n\}$ $<$ $\mathbb{N}$
   endlich — abzählbar unendlich
2. $\{\text{☺}\}^*$ $<$ $\mathcal{P}(\mathbb{N})$
   abzählbar unendlich — überabzählbar

Kardinalitäts-Battle

1. $\{1, \ldots, n\}$ $<$ $\mathbb{N}$
   endlich — abzählbar unendlich
2. $\{\text{☺}\}^*$ $<$ $\mathcal{P}(\mathbb{N})$
   abzählbar unendlich — überabzählbar
3. $\mathbb{R}$ $\mathcal{P}(\mathbb{N})$

Kardinalitäts-Battle

1.	$\{1, \ldots, n\}$	$<$	$\mathbb{N}$
	endlich		abzählbar unendlich
2.	$\{☺\}^*$	$<$	$\mathcal{P}(\mathbb{N})$
	abzählbar unendlich		überabzählbar
3.	$\mathbb{R}$	$=$	$\mathcal{P}(\mathbb{N})$

Kardinalitäts-Battle

1.	$\{1, \ldots, n\}$	$<$	$\mathbb{N}$
	endlich		abzählbar unendlich
2.	$\{☺\}^*$	$<$	$\mathcal{P}(\mathbb{N})$
	abzählbar unendlich		überabzählbar
3.	$\mathbb{R}$	$=$	$\mathcal{P}(\mathbb{N})$
	überabzählbar		überabzählbar

Kardinalitäts-Battle

1.	$\{1, \dots, n\}$ endlich	$<$	$\mathbb{N}$ abzählbar unendlich
2.	$\{☺\}^*$ abzählbar unendlich	$<$	$\mathcal{P}(\mathbb{N})$ überabzählbar
3.	$\mathbb{R}$ überabzählbar	$=$	$\mathcal{P}(\mathbb{N})$ überabzählbar
4.	Graphen mit $\exists n V(G) = \{1, \dots, n\}$		$\{0, 1\}^*$

Kardinalitäts-Battle

1.	$\{1, \dots, n\}$ endlich	$<$	$\mathbb{N}$ abzählbar unendlich
2.	$\{☺\}^*$ abzählbar unendlich	$<$	$\mathcal{P}(\mathbb{N})$ überabzählbar
3.	$\mathbb{R}$ überabzählbar	$=$	$\mathcal{P}(\mathbb{N})$ überabzählbar
4.	Graphen mit $\exists n V(G) = \{1, \dots, n\}$	$=$	$\{0, 1\}^*$

Kardinalitäts-Battle

1.	$\{1,\dots,n\}$	$<$	$\mathbb{N}$
	endlich		abzählbar unendlich
2.	$\{☺\}^*$	$<$	$\mathcal{P}(\mathbb{N})$
	abzählbar unendlich		überabzählbar
3.	$\mathbb{R}$	$=$	$\mathcal{P}(\mathbb{N})$
	überabzählbar		überabzählbar
4.	Graphen mit $\exists n V(G) = \{1,\dots,n\}$	$=$	$\{0,1\}^*$
	abzählbar unendlich		abzählbar unendlich

Kardinalitäts-Battle

1.	$\{1,\dots,n\}$	$<$	$\mathbb{N}$
	endlich		abzählbar unendlich
2.	$\{☺\}^*$	$<$	$\mathcal{P}(\mathbb{N})$
	abzählbar unendlich		überabzählbar
3.	$\mathbb{R}$	$=$	$\mathcal{P}(\mathbb{N})$
	überabzählbar		überabzählbar
4.	Graphen mit $\exists n V(G) = \{1,\dots,n\}$	$=$	$\{0,1\}^*$
	abzählbar unendlich		abzählbar unendlich
5.	$\mathbb{N}^*$		$\{\mathbb{R}\}$

Kardinalitäts-Battle

1.	$\{1, \ldots, n\}$ endlich	$<$	$\mathbb{N}$ abzählbar unendlich
2.	$\{\smiley\}^*$ abzählbar unendlich	$<$	$\mathcal{P}(\mathbb{N})$ überabzählbar
3.	$\mathbb{R}$ überabzählbar	$=$	$\mathcal{P}(\mathbb{N})$ überabzählbar
4.	Graphen mit $\exists n V(G) = \{1, \ldots, n\}$ abzählbar unendlich	$=$	$\{0, 1\}^*$ abzählbar unendlich
5.	$\mathbb{N}^*$	$>$	$\{\mathbb{R}\}$

Kardinalitäts-Battle

1.	$\{1, \ldots, n\}$ endlich	$<$	$\mathbb{N}$ abzählbar unendlich
2.	$\{\smiley\}^*$ abzählbar unendlich	$<$	$\mathcal{P}(\mathbb{N})$ überabzählbar
3.	$\mathbb{R}$ überabzählbar	$=$	$\mathcal{P}(\mathbb{N})$ überabzählbar
4.	Graphen mit $\exists n V(G) = \{1, \ldots, n\}$ abzählbar unendlich	$=$	$\{0, 1\}^*$ abzählbar unendlich
5.	$\mathbb{N}^*$ abzählbar unendlich	$>$	$\{\mathbb{R}\}$ einelementig

Kardinalitäts-Battle

1.	$\{1,\dots,n\}$	$<$	$\mathbb{N}$
	endlich		abzählbar unendlich
2.	$\{☺\}^*$	$<$	$\mathcal{P}(\mathbb{N})$
	abzählbar unendlich		überabzählbar
3.	$\mathbb{R}$	$=$	$\mathcal{P}(\mathbb{N})$
	überabzählbar		überabzählbar
4.	Graphen mit $\exists n V(G) = \{1,\dots,n\}$	$=$	$\{0,1\}^*$
	abzählbar unendlich		abzählbar unendlich
5.	$\mathbb{N}^*$	$>$	$\{\mathbb{R}\}$
	abzählbar unendlich		einelementig
6.	Graphen mit $V(G) = \mathbb{N}$		$\mathbb{N}$

Kardinalitäts-Battle

1.	$\{1,\dots,n\}$	$<$	$\mathbb{N}$
	endlich		abzählbar unendlich
2.	$\{☺\}^*$	$<$	$\mathcal{P}(\mathbb{N})$
	abzählbar unendlich		überabzählbar
3.	$\mathbb{R}$	$=$	$\mathcal{P}(\mathbb{N})$
	überabzählbar		überabzählbar
4.	Graphen mit $\exists n V(G) = \{1,\dots,n\}$	$=$	$\{0,1\}^*$
	abzählbar unendlich		abzählbar unendlich
5.	$\mathbb{N}^*$	$>$	$\{\mathbb{R}\}$
	abzählbar unendlich		einelementig
6.	Graphen mit $V(G) = \mathbb{N}$	$>$	$\mathbb{N}$

Kardinalitäts-Battle

1.	$\{1, \dots, n\}$ endlich	$<$	$\mathbb{N}$ abzählbar unendlich
2.	$\{☺\}^*$ abzählbar unendlich	$<$	$\mathcal{P}(\mathbb{N})$ überabzählbar
3.	$\mathbb{R}$ überabzählbar	$=$	$\mathcal{P}(\mathbb{N})$ überabzählbar
4.	Graphen mit $\exists n V(G) = \{1, \dots, n\}$ abzählbar unendlich	$=$	$\{0, 1\}^*$ abzählbar unendlich
5.	$\mathbb{N}^*$ abzählbar unendlich	$>$	$\{\mathbb{R}\}$ einelementig
6.	Graphen mit $V(G) = \mathbb{N}$ überabzählbar	$>$	$\mathbb{N}$ abzählbar unendlich

Kardinalitäts-Battle

1.	$\{1, \dots, n\}$ endlich	$<$	$\mathbb{N}$ abzählbar unendlich
2.	$\{☺\}^*$ abzählbar unendlich	$<$	$\mathcal{P}(\mathbb{N})$ überabzählbar
3.	$\mathbb{R}$ überabzählbar	$=$	$\mathcal{P}(\mathbb{N})$ überabzählbar
4.	Graphen mit $\exists n V(G) = \{1, \dots, n\}$ abzählbar unendlich	$=$	$\{0, 1\}^*$ abzählbar unendlich
5.	$\mathbb{N}^*$ abzählbar unendlich	$>$	$\{\mathbb{R}\}$ einelementig
6.	Graphen mit $V(G) = \mathbb{N}$ überabzählbar	$>$	$\mathbb{N}$ abzählbar unendlich

7.	endliche Graphen		$\mathbb{N}$

Kardinalitäts-Battle

1.	$\{1, \dots, n\}$	$<$	$\mathbb{N}$
	endlich		abzählbar unendlich
2.	$\{☺\}^*$	$<$	$\mathcal{P}(\mathbb{N})$
	abzählbar unendlich		überabzählbar
3.	$\mathbb{R}$	$=$	$\mathcal{P}(\mathbb{N})$
	überabzählbar		überabzählbar
4.	Graphen mit $\exists n V(G) = \{1, \dots, n\}$	$=$	$\{0, 1\}^*$
	abzählbar unendlich		abzählbar unendlich
5.	$\mathbb{N}^*$	$>$	$\{\mathbb{R}\}$
	abzählbar unendlich		einelementig
6.	Graphen mit $V(G) = \mathbb{N}$	$>$	$\mathbb{N}$
	überabzählbar		abzählbar unendlich
7.	endliche Graphen	???	$\mathbb{N}$

Kardinalitäts-Battle

1.	$\{1, \dots, n\}$	$<$	$\mathbb{N}$
	endlich		abzählbar unendlich
2.	$\{☺\}^*$	$<$	$\mathcal{P}(\mathbb{N})$
	abzählbar unendlich		überabzählbar
3.	$\mathbb{R}$	$=$	$\mathcal{P}(\mathbb{N})$
	überabzählbar		überabzählbar
4.	Graphen mit $\exists n V(G) = \{1, \dots, n\}$	$=$	$\{0, 1\}^*$
	abzählbar unendlich		abzählbar unendlich
5.	$\mathbb{N}^*$	$>$	$\{\mathbb{R}\}$
	abzählbar unendlich		einelementig
6.	Graphen mit $V(G) = \mathbb{N}$	$>$	$\mathbb{N}$
	überabzählbar		abzählbar unendlich
7.	endliche Graphen	???	$\mathbb{N}$
	keine Menge		abzählbar unendlich

Kardinalitäts-Battle

1.	$\{1, \ldots, n\}$ endlich	$<$	$\mathbb{N}$ abzählbar unendlich
2.	$\{☺\}^*$ abzählbar unendlich	$<$	$\mathcal{P}(\mathbb{N})$ überabzählbar
3.	$\mathbb{R}$ überabzählbar	$=$	$\mathcal{P}(\mathbb{N})$ überabzählbar
4.	Graphen mit $\exists n V(G) = \{1, \ldots, n\}$ abzählbar unendlich	$=$	$\{0, 1\}^*$ abzählbar unendlich
5.	$\mathbb{N}^*$ abzählbar unendlich	$>$	$\{\mathbb{R}\}$ einelementig
6.	Graphen mit $V(G) = \mathbb{N}$ überabzählbar	$>$	$\mathbb{N}$ abzählbar unendlich
7.	endliche Graphen keine Menge	???	$\mathbb{N}$ abzählbar unendlich
8.	Gödelnummern		$\mathcal{P}(\{0, 1\}^*)$

Kardinalitäts-Battle

1.	$\{1, \ldots, n\}$ endlich	$<$	$\mathbb{N}$ abzählbar unendlich
2.	$\{☺\}^*$ abzählbar unendlich	$<$	$\mathcal{P}(\mathbb{N})$ überabzählbar
3.	$\mathbb{R}$ überabzählbar	$=$	$\mathcal{P}(\mathbb{N})$ überabzählbar
4.	Graphen mit $\exists n V(G) = \{1, \ldots, n\}$ abzählbar unendlich	$=$	$\{0, 1\}^*$ abzählbar unendlich
5.	$\mathbb{N}^*$ abzählbar unendlich	$>$	$\{\mathbb{R}\}$ einelementig
6.	Graphen mit $V(G) = \mathbb{N}$ überabzählbar	$>$	$\mathbb{N}$ abzählbar unendlich
7.	endliche Graphen keine Menge	???	$\mathbb{N}$ abzählbar unendlich
8.	Gödelnummern	$<$	$\mathcal{P}(\{0, 1\}^*)$

Kardinalitäts-Battle

1.	$\{1, \ldots, n\}$ endlich	$<$	$\mathbb{N}$ abzählbar unendlich
2.	$\{\text{☺}\}^*$ abzählbar unendlich	$<$	$\mathcal{P}(\mathbb{N})$ überabzählbar
3.	$\mathbb{R}$ überabzählbar	$=$	$\mathcal{P}(\mathbb{N})$ überabzählbar
4.	Graphen mit $\exists n V(G) = \{1, \ldots, n\}$ abzählbar unendlich	$=$	$\{0, 1\}^*$ abzählbar unendlich
5.	$\mathbb{N}^*$ abzählbar unendlich	$>$	$\{\mathbb{R}\}$ einelementig
6.	Graphen mit $V(G) = \mathbb{N}$ überabzählbar	$>$	$\mathbb{N}$ abzählbar unendlich
7.	endliche Graphen keine Menge	???	$\mathbb{N}$ abzählbar unendlich
8.	Gödelnummern abzählbar unendlich	$<$	$\mathcal{P}(\{0, 1\}^*)$ überabzählbar

Kardinalitäts-Battle

1.	$\{1, \ldots, n\}$ endlich	$<$	$\mathbb{N}$ abzählbar unendlich
2.	$\{\text{☺}\}^*$ abzählbar unendlich	$<$	$\mathcal{P}(\mathbb{N})$ überabzählbar
3.	$\mathbb{R}$ überabzählbar	$=$	$\mathcal{P}(\mathbb{N})$ überabzählbar
4.	Graphen mit $\exists n V(G) = \{1, \ldots, n\}$ abzählbar unendlich	$=$	$\{0, 1\}^*$ abzählbar unendlich
5.	$\mathbb{N}^*$ abzählbar unendlich	$>$	$\{\mathbb{R}\}$ einelementig
6.	Graphen mit $V(G) = \mathbb{N}$ überabzählbar	$>$	$\mathbb{N}$ abzählbar unendlich
7.	endliche Graphen keine Menge	???	$\mathbb{N}$ abzählbar unendlich
8.	Gödelnummern abzählbar unendlich	$<$	$\mathcal{P}(\{0, 1\}^*)$ überabzählbar

Zwischenfrage für übermotivierte Zuhörende: Gibt es eine Mächtigkeit zwischen $|\mathbb{N}|$ und $|\mathbb{R}|$?

Wie viele verschiedene Entscheidungsprobleme gibt es?

Wie viele verschiedene Entscheidungsprobleme gibt es?

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

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

Wie viele verschiedene Entscheidungsprobleme gibt es?

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

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

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

Wie viele verschiedene Entscheidungsprobleme gibt es?

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

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

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

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

Wie viele verschiedene Entscheidungsprobleme gibt es?

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

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

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

$\mathcal{L}$ 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 $\mathbb{N}$.

Wie viele verschiedene Entscheidungsprobleme gibt es?

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

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

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

$\mathcal{L}$ 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 $\mathcal{P}(\mathbb{N})$.

Wie viele verschiedene Entscheidungsprobleme gibt es?

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

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

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

$\mathcal{L}$ 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

Zusammengefasst:

- Es gibt überabzählbar viele Sprachen.

Existenz unentscheidbarer Probleme

Zusammengefasst:

- Es gibt überabzählbar viele Sprachen.
- Aber es gibt nur abzählbar viele TMen.

Existenz unentscheidbarer Probleme

Zusammengefasst:

- Es gibt überabzählbar viele Sprachen.
- Aber es gibt nur abzählbar viele TMen.

Schlussfolgerung

Es gibt unentscheidbare Sprachen.

Existenz unentscheidbarer Probleme

Zusammengefasst:

- Es gibt überabzählbar viele Sprachen.
- Aber es gibt nur abzählbar viele TMen.

Schlussfolgerung

Es gibt unentscheidbare Sprachen.

- Die reine Existenz unentscheidbarer Probleme ist noch nicht dramatisch, denn es könnte sich ja um uninteressante, nicht praxis-relevante Probleme handeln.

Existenz unentscheidbarer Probleme

Zusammengefasst:

- Es gibt überabzählbar viele Sprachen.
- Aber es gibt nur abzählbar viele TMen.

Schlussfolgerung

Es gibt unentscheidbare 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.

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

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*.

$$\begin{aligned} D &= \{\, w \in \{0,1\}^* \mid w = w_i \text{ und } M_i \text{ akzeptiert } w \text{ nicht}\} \\ &= \{\langle M\rangle \mid M \text{ akteptiert } \langle M\rangle \text{ nicht}\}. \end{aligned}$$

Anders gesagt, die i-te Gödelnummer w_i ist genau dann in D, wenn die i-te TM, also M_i, dieses Wort nicht akzeptiert.

Unentscheidbarkeit der Diagonalsprache

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

$$\begin{aligned} D &= \{\, w \in \{0,1\}^* \mid w = w_i \text{ und } M_i \text{ akzeptiert } w \text{ nicht}\} \\ &= \{\langle M\rangle \mid M \text{ akteptiert } \langle M\rangle \text{ nicht}\}. \end{aligned}$$

Anders gesagt, die i-te Gödelnummer w_i ist genau dann in D, wenn die i-te TM, also M_i, dieses Wort nicht akzeptiert.

Satz

Die Diagonalsprache D *ist unentscheidbar.*

Unentscheidbarkeit der Diagonalsprache – Intuition

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

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

Unentscheidbarkeit der Diagonalsprache – Intuition

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

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

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**	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$		

Vorlesung BuK im WS 22/23, M. Grohe **Seite 136** Version 26. Oktober 2022

Unentscheidbarkeit der Diagonalsprache – Intuition

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

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

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**	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$		

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

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

Unentscheidbarkeit der Diagonalsprache – Beweis

Satz

Die Diagonalsprache D ist unentscheidbar.

Beweis

- Wir führen einen Widerspruchsbeweis und nehmen an, D ist entscheidbar.

Unentscheidbarkeit der Diagonalsprache – Beweis

Satz

Die Diagonalsprache D ist unentscheidbar.

Beweis

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

Unentscheidbarkeit der Diagonalsprache – Beweis

Satz

Die Diagonalsprache D ist unentscheidbar.

Beweis

- Wir führen einen Widerspruchsbeweis und nehmen an, D ist entscheidbar.
- 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.

Unentscheidbarkeit der Diagonalsprache – Beweis

Satz

Die Diagonalsprache D ist unentscheidbar.

Beweis

- Wir führen einen Widerspruchsbeweis und nehmen an, D ist entscheidbar.
- 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:

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

Unentscheidbarkeit der Diagonalsprache – Beweis

Satz

Die Diagonalsprache D ist unentscheidbar.

Beweis

- Wir führen einen Widerspruchsbeweis und nehmen an, D ist entscheidbar.
- 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:

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

Unentscheidbarkeit der Diagonalsprache – Beweis

Satz

Die Diagonalsprache D ist unentscheidbar.

Beweis

- Wir führen einen Widerspruchsbeweis und nehmen an, D ist entscheidbar.
- 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!

Unentscheidbarkeit der Diagonalsprache – Beweis

Satz

Die Diagonalsprache D ist unentscheidbar.

Beweis

- Wir führen einen Widerspruchsbeweis und nehmen an, D ist entscheidbar.
- 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:

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

Unentscheidbarkeit der Diagonalsprache – Beweis

Satz

Die Diagonalsprache D ist unentscheidbar.

Beweis

- Wir führen einen Widerspruchsbeweis und nehmen an, D ist entscheidbar.
- 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:
    $$w_j \notin D \overset{M_j \text{ entsch. } D}{\Rightarrow} M_j \text{ akzeptiert } w_j \text{ nicht} \overset{\text{Def. von } D}{\Rightarrow} w_j \in D$$

Unentscheidbarkeit der Diagonalsprache – Beweis

Satz

Die Diagonalsprache D ist unentscheidbar.

Beweis

- Wir führen einen Widerspruchsbeweis und nehmen an, D ist entscheidbar.
- 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!

Unentscheidbarkeit der Diagonalsprache – Beweis

Satz

Die Diagonalsprache D ist unentscheidbar.

Beweis

- Wir führen einen Widerspruchsbeweis und nehmen an, D ist entscheidbar.
- 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!
- Somit is D unentscheidbar. □

Das Halteproblem für JAVA-Programme

Eingabe:	String `method` (Name der zu überprüfenden JAVA-Methode) Array `parameters` von Objekten (die Parameter, die an die Methode übergeben werden)
Ausgabe:	`true`, falls `method` wirklich eine Methode in einer verfügbaren Klasse bezeichnet, `parameters` die richtige Zahl von Parametern mit den richtigen Typen enthält und die Methode `method` bei Eingabe `parameters` (irgendwann) anhält, `false` sonst.

In JAVA:

```java
class Halt {
    ...

    static boolean halt(String method,
                        Object[] parameters) {
        ...
    }
    ...
}
```

Wir können annehmen, dass die Methode `halt` Zugriff auf den Quellcode von `method` hat.

Die Unentscheidbarkeit des Halteproblems

Satz

Es gibt kein JAVA-Programm, welches das Halteproblem löst.

Beweis des Satzes

Angenommen, es gibt ein Programm, welches das Halteproblem löst. Wir können annehmen, dass dies mittels einer Methode

`static boolean halt(String method,Object[] parameters)`

in einer Klasse `Halt` geschieht.

Beweis des Satzes

Angenommen, es gibt ein Programm, welches das Halteproblem löst. Wir können annehmen, dass dies mittels einer Methode

`static boolean halt(String method,Object[] parameters)`

in einer Klasse `Halt` geschieht.

Wir definieren eine neue Methode `diag` in einer Klasse `Diag`:

```
class Diag{
    static void diag(String method) {
        Object[] parameters = { method };
                // Eingaben bestehen nur aus
                // dem einen String ``method''.
        if ( Halt.halt(method,parameters) ) {
            while ( true ) {};
                // Wenn Methode method bei
                // Eingabe method hält,
                // dann laufe in Endlosschleife.
        }
    }
}
```

Was passiert beim Aufruf

`Diag.diag("foo")`

wenn `foo` der Name einer Methode ist, die einen String als Parameter erwartet?

Was passiert beim Aufruf

`Diag.diag("foo")`

wenn `foo` der Name einer Methode ist, die einen String als Parameter erwartet?

`Diag.diag("foo")` hält.
$\iff$ `Halt.halt("foo",{"foo"})` gibt `false` zurück.
$\iff$ `foo("foo")` hält nicht.

Was passiert beim Aufruf

```
Diag.diag("foo")
```

wenn `foo` der Name einer Methode ist, die einen String als Parameter erwartet?

`Diag.diag("foo")` hält.
$\iff$ `Halt.halt("foo",{"foo"})` gibt `false` zurück.
$\iff$ `foo("foo")` hält nicht.

Also beim Aufruf `Diag.diag("Diag.diag")`:

`Diag.diag("Diag.diag")` hält.
$\iff$ `Diag.diag("Diag.diag")` hält nicht.

Widerspruch!

Hilbert’s Hotel