Entscheidungsprobleme

- übliche Formulierung

  gegeben: Eingabe x aus einer Grundmenge U

  Frage: Hat x eine bestimmte Eigenschaft P?

- Beispiel:

  gegeben: $n \in \mathbb{N}$

  Frage: Ist n eine Primzahl?

- Formalisierung:
  Grundmenge ist die Menge aller Wörter über einem Alphabet Σ.
  Menge aller Eingaben mit Antwort "JA" ist Sprache $L \subseteq \Sigma^*$

- Beispiel: $L_{prim} = \{\text{bin}(p) \mid p \text{ ist Primzahl}\}$

Definition Entscheidbarkeit

Definition: Die charakteristische Funktion einer Menge $A \subseteq \Sigma^*$ ist die (totale) Funktion

$$\chi_A : \Sigma^* \to \{0,1\} \text{ vermöge } \chi_A(w) = \begin{cases} 1 & \text{falls } w \in A, \\ 0 & \text{falls } w \notin A, \end{cases}$$

Definition: Eine Menge $A \subseteq \Sigma^*$ heißt (Turing-)entscheidbar, falls ihre charakteristische Funktion (Turing-)berechenbar ist.

Definition Semi-Entscheidbarkeit

Definition: Die “halbe” charakteristische Funktion einer Menge $A \subseteq \Sigma^*$ ist die (partielle) Funktion

$$\chi'_A : \Sigma^* \to \{0,1\} \text{ vermöge } \chi'_A(w) = \begin{cases} 1 & \text{falls } w \in A, \\ \text{nicht definiert} & \text{falls } w \notin A, \end{cases}$$

Definition: Eine Menge $A \subseteq \Sigma^*$ heißt semi-entscheidbar, falls ihre “halbe” charakteristische Funktion berechenbar ist.

(Semi-)Entscheidbarkeit und Turingmaschinen

Satz: Eine Menge $A \subseteq \Sigma^*$ ist genau dann entscheidbar, wenn es eine Turingmaschine M mit der Menge der Endzustände $\{ja, nein\}$ gibt, die für jedes Wort $w \in \Sigma^*$ einen Endzustand erreicht und genau dann den Endzustand ja erreicht, wenn $w \in A$ gilt.

Sprechweise: M entscheidet A.

Satz: Eine Menge $A \subseteq \Sigma^*$ ist genau dann semi-entscheidbar, wenn es eine Turingmaschine M gibt, die
für jedes Wort $w \in \Sigma^*$ genau dann einen Endzustand erreicht, wenn $w \in A$ gilt.

Sprechweise: M akzeptiert A.

Beziehung zwischen Entscheidbarkeit und Semi-Entscheidbarkeit

Satz. Eine Menge $A \subseteq \Sigma^*$ ist entscheidbar genau dann, wenn sowohl die Menge A als auch ihr Komplement $\overline{A} = \Sigma^* \setminus A$ semi-entscheidbar sind.

Beweis.

- Aus Entscheidbarkeit von A folgt sofort Semi-Entscheidbarkeit von A und $\overline{A}$.
- Sind A und $\overline{A}$ jeweils semi-entscheidbar,
  - so lasse man für eine Eingabe w gleichzeitig Algorithmen M_A und $M_{\overline{A}}$ zur Berechnung von χ'_A und $\chi'_{\overline{A}}$ laufen, bis einer stoppt.
    Wegen der Semi-Entscheidbarkeit von A und $\overline{A}$ muss einer der Algorithmen stoppen!
  - Stoppt M_A: Ausgabe 1; stoppt $M_{\overline{A}}$: Ausgabe 0.

Rekursiv aufzählbare Mengen

Definition. Eine Menge $A \subseteq \Sigma^*$ heißt rekursiv aufzählbar, falls $A = \emptyset$ oder falls es eine totale und berechenbare Funktion $f : \mathbb{N} \to \Sigma^*$ gibt, so dass

$$A = \{f(0), f(1), f(2), \ldots\}$$

gilt. Sprechweise: f zählt A auf.
Man beachte: $f(i) = f(j)$ für $i \neq j$ ist zulässig.

Satz. Eine Menge ist genau dann rekursiv aufzählbar, wenn sie semi-entscheidbar ist.

Folgerung

Sei $A \subseteq \Sigma^*$ eine Menge. Dann sind folgende Aussagen äquivalent.

(i) A ist rekursiv aufzählbar.

(ii) A ist semi-entscheidbar.

(iii) χ'_A ist berechenbar.

(iv) A ist Definitionsbereich einer berechenbaren Funktion.

(v) A ist Wertebereich einer berechenbaren Funktion.

Nicht-entscheidbare Probleme

1. Probleme mit Turingmaschinen als Eingaben (Halteproblem)
   - Turingmaschinen werden durch Wörter codiert.
   - Anwendung der Diagonalisierung
2. Reduktion als Beweistechnik für Nicht-Entscheidbarkeit
3. Weitere nicht-entscheidbare Probleme

Codierung von Turing-Maschinen

Gegeben: TM $M = (Z, \{0,1\}, \Gamma, \delta, z_0, \Box, E)$
Ziel: Codierung von M durch ein Wort $w \in \{0,1\}^*$

$Z = \{z_0, z_1, \ldots, z_k\}$, $\Gamma = \{a_0, a_1, \ldots, a_n\}$ wobei $a_0 = 0, a_1 = 1, a_2 = \Box$,
$E = \{z_{i_1}, \ldots, z_{i_\ell}\}$.

Codierung von Z, Γ, E durch Wort $u \in \{0,1,\#\}^*$:
$u = \#\#\mathrm{bin}(k)\#\#\mathrm{bin}(n)\#\#\mathrm{bin}(i_1)\#\mathrm{bin}(i_2)\# \cdots \mathrm{bin}(i_\ell)$

Jeder δ-Regel der Form $\delta(z_i, a_j) = (z_{i'}, a_{j'}, y)$ entspricht das Wort

$$w_{i,j} = \#\#\mathrm{bin}(i)\#\mathrm{bin}(j)\#\mathrm{bin}(i')\#\mathrm{bin}(j')\#\mathrm{bin}(y),$$

$$\text{wobei } \mathrm{bin}(L) = 00, \mathrm{bin}(R) = 01, \mathrm{bin}(N) = 10$$

Codierung von δ durch Wort v, das durch Konkatenation der Wörter $w_{i,j}$ entsteht.
Codierung von M durch $uv \in \{0,1,\#\}^*$.

Codierung von Turing-Maschinen – Fortsetzung

Jedes Wort über $\{0, 1, \#\}^*$ kann durch ein Wort über $\{0, 1\}$ codiert werden, indem man folgende Codierung vornimmt:

$$0 \mapsto 00, \qquad 1 \mapsto 01, \qquad \# \mapsto 11.$$

Nicht jedes Wort in $\{0, 1\}^*$ ist die Codierung einer Turingmaschine. Sei aber M_0 irgendeine beliebige feste Turingmaschine, dann können wir *für jedes* $w \in \{0, 1\}^*$ festlegen, dass M_w eine bestimmte Turingmaschine bezeichnet, nämlich

$$M(w) = M_w = \begin{cases} M & \text{falls } w \text{ Codewort von } M \text{ ist,} \\ M_0 & \text{sonst.} \end{cases}$$

Spezielles Halteproblem für Turingmaschinen

Definition. Das spezielle Halteproblem für Turingmaschinen ist die Menge

$$K = \{w \in \{0,1\}^* \mid M_w \text{ angesetzt auf } w \text{ hält}\}.$$

Satz.

$$\boxed{\text{Das spezielle Halteproblem für Turingmaschinen } (K) \text{ ist nicht entscheidbar.}}$$

Unentscheidbarkeit des speziellen Halteproblems – Beweis I

Angenommen, K wäre entscheidbar. Dann wäre χ_K berechenbar mittels einer Turingmaschine M. Diese Maschine M könnte nun leicht zu einer Turingmaschine M' umgebaut werden, die durch folgende Abbildung definiert ist.

$$
\begin{tikzcd}
\text{start} \arrow[r] & M \arrow[r] & \text{„Band} = 0\,\text{?“} \arrow[r, "ja"] \arrow[loop below, "nein"] & \text{stop}
\end{tikzcd}
$$

Das heißt, M' stoppt genau dann, wenn M den Wert 0 ausgeben würde. Falls M den Wert 1 ausgibt, gerät M' in eine Endlosschleife.

Unentscheidbarkeit des speziellen Halteproblems – Beweis II

Sei w' ein Codewort der Maschine M'. Nun gilt

M' angesetzt auf w' hält

$\Leftrightarrow$ M angesetzt auf w' gibt 0 aus	(wegen Definition von M'),
$\Leftrightarrow$ $\chi_K(w') = 0$	(da M die Menge K entscheidet),
$\Leftrightarrow$ $w' \notin K$	(wegen Definition von χ_K),
$\Leftrightarrow$ $M_{w'}$ angesetzt auf w' hält nicht	(wegen Definition von K),
$\Leftrightarrow$ M' angesetzt auf w' hält nicht	(da w' Code von M' ist).

Dieser Widerspruch beweist, dass die Eingangsannahme falsch war, also ist K nicht entscheidbar.

Reduzierbarkeit von Sprachen

Definition.

Eine Sprache $A \subseteq \Sigma^*$ heißt reduzierbar auf die Sprache $B \subseteq \Gamma^*$, Notation $A \leq B$, wenn es eine totale und berechenbare Funktion $f : \Sigma^* \to \Gamma^*$ gibt, so dass

$$\text{für alle } w \in \Sigma^*\text{: } w \in A \text{ genau dann, wenn } f(w) \in B.$$

In diesem Fall nennt man f eine Reduktion von A auf B.

Die Relation $\leq$ ist transitiv und reflexiv, aber nicht antisymmetrisch.

Reductionen und (Semi-)Entscheidbarkeit

Satz. Es seien A und B Sprachen mit $A \leq B$.
Ist B entscheidbar, so ist auch A entscheidbar.
Ist B semi-entscheidbar, so ist auch A semi-entscheidbar.
Ist A nicht entscheidbar, so ist auch B nicht entscheidbar.

Beweis. Sei $f : \Sigma^* \to \Gamma^*$ eine Reduktion von A auf B.
Es gilt: $\chi_A(w) = \chi_B(f(w))$ sowie $\chi'_A(w) = \chi'_B(f(w))$;
aus der Berechenbarkeit von χ_B bzw. χ'_B sowie der Berechenbarkeit von f folgt die Berechenbarkeit von χ_A bzw. χ'_A.

Reduktion als Beweistechnik

Ist die Entscheidbarkeit von B bekannt, so genügt für den Beweis der Entscheidbarkeit von A die Angabe einer Reduktion von A auf B.

Ist die Unentscheidbarkeit von A bekannt, so genügt für den Beweis der Unentscheidbarkeit von B die Angabe einer Reduktion von A auf B.

Das Halteproblem für Turingmaschinen

Definition. Das (allgemeine) Halteproblem für Turingmaschinen ist die Menge

$$H = \{w\#x \mid M_w \text{ angesetzt auf } x \text{ hält}\}.$$

> **Satz.** Das Halteproblem für Turingmaschinen (H) ist nicht entscheidbar.

Beweis: durch Reduktion des speziellen Halteproblems K auf H

$$\text{für alle } w \in \{0,1\}^*\text{: } w \in K \text{ genau dann, wenn } w\#w \in H$$

Funktion $f : \{0,1\}^* \to \{0,1,\#\}^*$ mit $f(w) = w\#w$ ist berechenbar.

Da K nicht entscheidbar ist, ist auch H nicht entscheidbar.

Universelle Turingmaschinen

Satz. Es gibt eine Turingmaschine U mit dem Eingabealphabet $\{0, 1, \#\}$, die für jede Eingabe $u\#v$ mit $u, v \in \{0, 1\}^*$ die Ausgabe $f_{M_u}(v)$ liefert bzw. nicht stoppt, falls M_u angesetzt auf v nicht stoppt.

Bemerkungen

1. Eine solche universelle Turingmaschine kann effektiv konstruiert werden.
2. Universelle Turingmaschinen kann man als das Modell eines universellen Computers ansehen, der zu einem Programm und einer Eingabe des Programmes die Ausgabe des Programmes berechnet.

Semi-Entscheidbarkeit des Halteproblems

Satz. Das Halteproblem für Turingmaschinen (H) ist semi-entscheidbar.

Beweis. H wird durch eine universelle Turingmaschine U akzeptiert.

Folgerungen.

1. Das spezielle Halteproblem K ist semi-entscheidbar.
2. Das Komplement von K, $\overline{K} = \{0,1\}^* \setminus K$, ist nicht semi-entscheidbar.

Das 10. Hilbertsche [3] Problem

Definition. Das 10. Hilbertsche Problem ist definiert durch:

Gegeben:	$n \in \mathbb{N}$, ein Polynom $p(x_1, \ldots, x_n)$ in n Unbekannten,
Frage:	Besitzt p ganzzahlige Nullstellen?

Satz. Das 10. Hilbertsche Problem ist nicht entscheidbar.

Satz. Das 10. Hilbertsche Problem ist semi-entscheidbar.

[3] David Hilbert, deutscher Mathematiker, 1862-1943

Das Postsche [4] Korrespondenzproblem

Definition. Das Postsche Korrespondenzproblem (PKP) ist definiert durch:

Gegeben: Alphabet A, $k \in \mathbb{N}$ sowie die Folge von Wortpaaren (x_1, y_1), (x_2, y_2), $\ldots$, (x_k, y_k) mit $x_i, y_i \in A^+$ für $1 \leq i \leq k$.

Frage: Gibt es eine Folge von Indizes $i_1, i_2, \ldots, i_n$ mit $i_j \in \{1, 2, \ldots, k\}$ für $1 \leq j \leq n,\ n \in \mathbb{N},$ so dass $x_{i_1} x_{i_2} \ldots x_{i_n} = y_{i_1} y_{i_2} \ldots y_{i_n}$ gilt ?

Satz. Das Postsche Korrespondenzproblem ist nicht entscheidbar.

Satz. Das Postsche Korrespondenzproblem ist semi-entscheidbar.

[4] Emil Post, amerikanischer Mathematiker, 1897-1954

Beispiel für Postsches Korrespondenzproblem

Das Korrespondenzproblem

$$A = \{0, 1\}, \qquad k = 3, \qquad K = ((1, 101), (10, 00), (011, 11)),$$

also

$$\begin{array}{lll} x_1 = 1 & x_2 = 10 & x_3 = 011 \\ y_1 = 101 & y_2 = 00 & y_3 = 11 \end{array}$$

besitzt die Lösung $(1, 3, 2, 3)$, denn es gilt

$$x_1 x_3 x_2 x_3 = 101110011 = 101110011 = y_1 y_3 y_2 y_3.$$

Weiteres Beispiel für Postsches Korrespondenzproblem

Gegeben ist folgende Belegung des PKP:

$$\begin{array}{llll} x_1 = 001 & x_2 = 01 & x_3 = 01 & x_4 = 10 \\ y_1 = 0 & y_2 = 011 & y_3 = 101 & y_4 = 001. \end{array}$$

Dieses Problem besitzt eine Lösung, aber die kürzeste Lösung besteht aus 66 Indizes, nämlich

$$2,4,3,4,4,2,1,2,4,3,4,3,4,4,3,4,4,2,1,4,4,2,1,3,4,1,1,3,4,4,4,2,1,$$
$$2,1,1,1,3,4,3,4,1,1,1,4,4,2,1,4,1,1,3,4,1,1,3,1,1,3,1,2,1,4,1,1,3$$