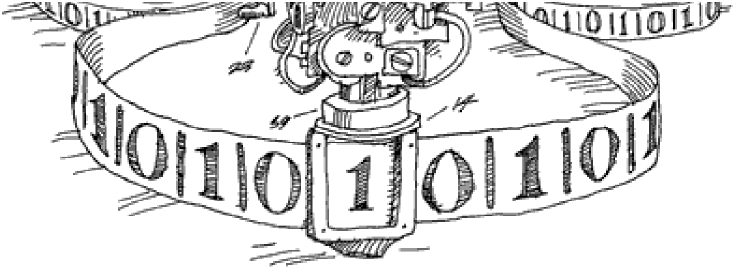
Karlsruher Institut für Technologie

Tutorium Theoretische Grundlagen der Informatik

Simon Bischof

Institut für Kryptographie und Sicherheit



KIT – Universität des Landes Baden-Württemberg und
nationales Forschungszentrum in der Helmholtz-Gemeinschaft

www.kit.edu

Ergänzung zur Gödelnummer

- für TM M bezeichnet $\langle M \rangle$ die Gödelnummer von M
- für $w \in \{0, 1\}^*$ ist M_w die TM mit Gödelnummer w

Ergänzung zur Gödelnummer

- für TM M bezeichnet $\langle M \rangle$ die Gödelnummer von M
- für $w \in \{0, 1\}^*$ ist M_w die TM mit Gödelnummer w
- für nicht korrekte Gödelnummer w ist $L(M_w) = \emptyset$

(Semi-)Entscheidbarkeit

Sei $L \subset \Sigma^*$ eine Sprache.

- $L \in R$ (L ist entscheidbar) $:\Leftrightarrow$ es existiert eine TM M, die L entscheidet (d.h. M hält immer)

(Semi-)Entscheidbarkeit

Sei $L \subset \Sigma^*$ eine Sprache.

- $L \in R$ (L ist entscheidbar) $:\Leftrightarrow$ es existiert eine TM M, die L entscheidet (d.h. M hält immer)
- $L \in RE$ (L ist semientscheidbar) $:\Leftrightarrow$ es existiert eine TM M, die L akzeptiert (d.h. für $w \notin L$ muss M nicht notwendigerweise halten)
- $L \in co-RE :\Leftrightarrow \bar{L} := \Sigma^* \setminus L \in RE$
- $R = RE \cap co-RE$

Nicht entscheidbare Sprachen / Probleme

- Diagonalsprache $L_D := \{w \in \Sigma^* | M_w \text{ akzeptiert } w \text{ nicht}\}$
- Wortproblem $A_{TM} := \{\langle M \rangle w \in \Sigma^* | M \text{ akzeptiert } w\}$
- Halteproblem $HALT := \{\langle M \rangle w \in \Sigma^* | M \text{ hält bei Eingabe } w\}$
- $MIN_{TM} := \{\langle M \rangle | M \text{ ist minimale TM}\}$.

Berechenbarkeit, Many-One-Reduzierbarkeit

- $f : \Sigma^* \rightarrow \Sigma^*$ heißt berechenbar, wenn eine TM M exisiert, die bei Eingabe w mit $f(w)$ auf dem Band hält.
- $A \leq_m B$ (A Many-One-reduzierbar auf B), wenn eine berechenbare Funktion $f : \Sigma^* \rightarrow \Sigma^*$ existiert mit $w \in A \Leftrightarrow f(w) \in B$

Sei $A \leq_m B$. Dann:

- B entscheidbar $\Rightarrow$ A entscheidbar.
- A nicht entscheidbar $\Rightarrow$ B nicht entscheidbar

Postsches Korrespondenzproblem

Gegeben: eine endliche Menge von ”Puzzlestücken”

$$S = \left\{ \binom{t_1}{b_1}, \ldots, \binom{t_n}{b_n} \right\}$$

mit $t_1, \ldots, t_n, b_1, \ldots, b_n \in \Sigma^*$.
Frage: Existieren $i_1, \ldots, i_k$ mit $b_{i_1} \ldots b_{i_k} = t_{i_1} \ldots t_{i_k}$?

Quines

- Sei P_w die TM, die w ausgibt und hält.
- Es gibt eine berechenbare Funktion $q : \Sigma^* \longrightarrow \Sigma^*$ mit $q(w) = \langle P_w \rangle$

Quines

- Sei P_w die TM, die w ausgibt und hält.
- Es gibt eine berechenbare Funktion $q : \Sigma^* \to \Sigma^*$ mit $q(w) = \langle P_w \rangle$
- Es existiert eine TM, die ihre eigene Gödelnummer ausgibt

Das Rekursionstheorem

- 1. Form: Die TM T berechne die Funktion $t : \Sigma^* \times \Sigma^* \to \Sigma^*$. Dann existiert eine TM R, die die Funktion $r : \Sigma^* \to \Sigma^*$ mit $r(w) = t(\langle R \rangle, w)$ berechnet.

Das Rekursionstheorem

- 1. Form: Die TM T berechne die Funktion $t : \Sigma^* \times \Sigma^* \to \Sigma^*$. Dann existiert eine TM R, die die Funktion $r : \Sigma^* \to \Sigma^*$ mit $r(w) = t(\langle R \rangle, w)$ berechnet.
- 2. Form: Es sei $t : \Sigma^* \to \Sigma^*$ berechenbar. Dann existiert eine TM F, so dass $M_{t(\langle F \rangle)}$ die gleiche Funktion berechnet wie F.