Tafelwerk Berechenbarkeitstheorie

Vorlesungen BT 25.1.16 und 28.1.16

Zusammenfassung des Tafelwerks zur Vorlesung Berechenbarkeitstheorie. Achtung: Diese kann Fehler und Irrtümer enthalten!

Wie formalisiere ich einen Computer?

- Berechnungsmodelle: DEA, NEA, Kellerautomat, TM, NTM, MehrbandTM

Welche Probleme kann ein Berechnungsmodell lösen?

- Wir betrachten nur Entscheidungsprobleme, d.h. Probleme mit Antwort ja/nein

Etwa: Gegeben Graph G durch Code $\langle G \rangle \in \Sigma^*$, wobei Σ endliches Alphabet.
Betrachte $L = \{\langle G \rangle \mid G \text{ hat Hamiltonkreis } \}$

Nun äquivalent:

Löse Entscheidungsproblem (gilt Eigenschaft $\mathbb{E}$ für Objekt O)
$\Leftrightarrow$ löse Wortproblem für L (gilt $w \in L = \{\langle O \rangle \mid O \text{ hat Eigenschaft } \mathbb{E}\}$?)

§1 Reguläre Sprachen / Welche Probleme kann ein DEA lösen?

(äq. Welche Sprachen kann ein DEA erkennen?)

$$
\begin{aligned}
REG &= \{L \mid \text{ex. DEA } M \text{ mit } L(M) = L\} \\
&= \{L \mid \text{ex. NEA } N \text{ mit } L(N) = L\} \\
&= \{L \mid \text{ex. RA } R \text{ mit } L(R) = L\} && \text{Satz von Kleene} \\
&= \{L \mid \equiv_L \text{ hat endl. Index}\} && \text{Myhill Nerode}
\end{aligned}
$$

$[\forall u, v \in \Sigma^* : u \equiv_L v \Leftrightarrow \forall z \in \Sigma^* \ (uz \in L \Leftrightarrow vz \in L)]$

Jede endl. Sprache ist regulär.

Minimierung von DEAs (min # von Zuständen)

Finde äq. Zustände mittels Table-Filling Algorithmus.

Abschlusseigenschaften reg. Sprachen

abg. unter: Konkatenation, Kleene Stern, Vereinigung, Schnitt, Komplement

Nachweis von Nicht-Regularität:

- Zeige $\equiv_L$ hat unendl. Index

- **Pumping Lemma**

  $\exists k \in \mathbb{N}$ s.d. $\forall w \in L$ mit $|w| \geq k$ $\exists$ Zerlegung $w = xyz$ mit:

  (i) $|xy| \leq k$

  (ii) $\forall i \geq 0 : xy^i z \in L$

  (iii) $|y| > 0$

  $L \in$ REG $\Rightarrow L$ ist pumpbar
  (Umkehrung L nicht pumpbar $\Rightarrow L$ nicht regulär)

$\{a^n b^n\}$ ist nicht regulär. Was nun?

§2 Kontextfreie Sprachen / Welche Probleme kann ein Kellerautomat lösen?

$$\begin{aligned} CFL &= \{L \mid \text{ ex. kontextfreie Grammatik } G \text{ mit } L(G) = L\} \\ &= \{L \mid \text{ ex. kontextfreie Grammatik } G \text{ in CNF mit } L(G) = L\} \\ &= \{L \mid \text{ ex. Kellerautomat } K \text{ mit } L(K) = L\} \end{aligned}$$

kf. Grammatik G : Startsymbol S , Variablen $X, Y, ...$, Terminalsymbole $0, 1, ...$

$$\begin{aligned} \text{Regeln:} \quad & S \to XYX \mid X0 \\ & X \to \varepsilon \mid 00 \\ & Y \to YY \mid 1 \mid S \end{aligned}$$

z.B. $00100 \in L(G)$, $\varepsilon \notin L(G)$
Bemerkung: $REG \subsetneq CFL$.

G hat Chomsky-Normalform (CNF)

Alle Regeln sind von der Form: $A \to BC$, $A \to a$, $S \to \varepsilon$
Für G in CNF kann man Wortproblem (gilt $w \in L(G)$?) mittels des CYK-Algorithmus lösen.

Abschlusseigenschaften kontextfreier Sprachen

- abg. unter: Vereinigung , Konkatenation, Kleene Stern
- nicht abg. unter: Schnitt, Komplement

Grenzen kf. Sprachen / Nachweis nicht kontextfrei

kontextfreies Pumping Lemma

$\exists k \in \mathbb{N}$ s.d. $\forall w \in L$ mit $|w| \geq k$ $\exists$ Zerlegung $w = uvxyz$ mit:

(i) $|vxy| \leq k$

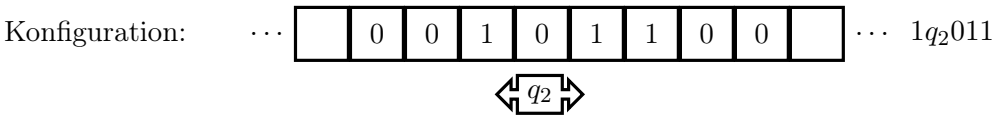
(ii) $\forall i \geq 0 : uv^i xy^i z \in L$

(iii) $|vy| > 0$

$L \in \text{CFL} \Rightarrow L$ ist kf-pumpfbar (L nicht pumpbar $\Rightarrow L \notin$ CFL)
$\{a^n b^n c^n \mid n \geq 0\}$ ist nicht kontextfrei. Was nun?

§3 Berechenbarkeitstheorie / Welche Probleme kann eine TM lösen?

TM - besteht aus Zustandsmenge Q, Eingabealphabet Σ, Arbeitsalphabet Γ (mit $\Sigma \subseteq \Gamma$), Übergangsfunktion $\delta : Q \times \Gamma \to Q \times \Gamma \times \{L, R\}$ und q_0 Startzustand, q_A akzeptierender Zustand, q_V verwerfender Zustand mit $q_0, q_V, q_A \in Q$ und $q_A \neq q_V$



TM akz. Wort $w \in \Sigma^*$ gdw. es ex. Folge von nicht-verwerfenden (d.h. q_V kommt nicht vor) Konfigurationen $C_1, ..., C_n$ mit

(1.) $C_1 = q_0 w$ (Startkonfiguration)

(2.) $\forall i : 1, ..., n-1 : C_i$ geht über nach C_{i+1}

(3.) C_n akzeptierend (d.h. Zustand q_A kommt vor)

Möglichkeiten einer TM bei Eingabe $w \in \Sigma^*$

∘ akzeptieren ∘ verwerfen ∘ zykeln (weder akzeptieren noch verwerfen)

Was heißt jetzt "TM löst Wortproblem"?

Zwei Möglichkeiten: $L(M) = \{w \in \Sigma^* \mid M(w) \text{ stoppt akzeptierend } \}$

"entscheidbar"
$\mathbb{E} = \{L \mid$ ex. TM M mit $L(M) = L$ und M stoppt auf allen Eingaben $\}$ (d.h. M ist Entscheider)

"erkennbar"
$\mathbb{A} = \{L \mid$ ex. TM M mit $L(M) = L\}$

"aufzählbar"
$\mathbb{A} = \{L \mid$ ex. Aufzähler für $L\}$

$\mathbb{E} \subseteq \mathbb{A}$

Andere Berechnungsmodelle:

NTM, Mehrband TM, Halbband-TM; alle äquivalent zur "herkömmlichen" TM.

TM M mit Ausgabe:

TM wie bisher + "Ausgabeband" (nur beschreibbar)
M beschreibt Funktion: $f_M(x) = y$, mit $M(\langle x \rangle)$ stoppt akzeptierend und auf dem Ausgabeband steht $\langle y \rangle$ (partielle Fkt.)
d.h. f_M ist nur definiert, falls $M(\langle x \rangle)$ akzeptiert

Berechenbare Fkt.:

partielle Funktion f s.d. TM M existiert $f_M \equiv f$

TM als Aufzähler:

2-Band TM mit Arbeitsband + Ausgabeband
Aufzähler für eine Sprache L ist 2-Band TM M (wie oben), die auf das Ausgabeband $w_1\#w_2\#w_3\#...$ schreibt, wobei $L = \bigcup_i w_i$

Grenzen entscheidbarer / erkennbarer Sprachen

Betrachtungen zur Unendlichkeit

$\mathbb{A} = \{L(M) \subseteq \Sigma^* \mid M \text{ ist TM } \}$ abzählbar unendlich
$\mathcal{L} = \{L \subseteq \Sigma^*\}$ überabzählbar unendlich ($\mathcal{L}$ ist größer als $\mathbb{A}$)
$\Rightarrow \mathbb{A} \subsetneq \mathcal{L}$, d.h. ex. nicht-erkennbare Sprache

$A_{TM} = \{\langle M, w\rangle \mid M(w) \text{ akzeptiert } \} \notin \mathbb{E}$ (Beweisidee: Diagonalisierer)
$A_{TM} \in \mathbb{A}$, $A_{TM} \notin \mathbb{A}^{co} \Rightarrow \overline{A_{TM}} = \{\langle M, w\rangle \mid M(w) \text{ akzeptiert nicht } \} \notin \mathbb{A}$
Gleiche Methode: HALT $= \{\langle M, w\rangle \mid M(w) \text{ hält } \} \notin \mathbb{E}$

Abschlusseigenschaften

$\mathbb{E} = \mathbb{E}^{co}$, $\mathbb{A}$ nicht abgeschlossen unter Komplement, $\mathbb{A} \cap \mathbb{A}^{co} = \mathbb{E}$ (Aufgabe ans Publikum: Welche andere Abschlusseigenschaften gelten?)

Fortsetzung: Berechenbarkeitstheorie / Welche Probleme kann eine TM lösen? (Zweite Zusammenfassungsvorlesung)

Erinnerung:

$$\begin{aligned}\mathbb{E} &= \{L \mid \text{ex. TM } M \text{ mit } L(M) = L, M \text{ stoppt auf jeder Eingabe}\}\\ \mathbb{A} &= \{L \mid \text{ex. TM } M \text{ mit } L(M) = L\}\\ &= \{L \mid \text{ex. Aufzähler für } L\}\\ \mathbb{A}^{co} &= \{L \mid \overline{L} \in \mathbb{A}\}\\ \mathbb{E} &= \mathbb{A} \cap \mathbb{A}^{co}\end{aligned}$$

Many-one Reduktion

$L_1 \subseteq \Sigma^*$, $L_2 \subseteq (\Sigma')^*$ $f : \Sigma^* \to (\Sigma')^*$ heißt many-one Reduktion von L_1 auf L_2 gdw.

(1.) f ist berechenbar und total

(2.) $\forall w \in \Sigma^* w \in L_1$ gdw. $f(w) \in L_2$ schreibe dann $L_1 \leq_m L_2$

$L_1 \leq_m L_2$

(i) $L_2 \in \mathbb{E} \Rightarrow L_1 \in \mathbb{E}$

(ii) $L_2 \in \mathbb{A} \Rightarrow L_1 \in \mathbb{A}$

(iii) $L_2 \in \mathbb{A}^{co} \Rightarrow L_1 \in \mathbb{A}^{co}$

Bsp.: HALT $\leq_m A_{TM}$ $EQ_{TM} = \{\langle M_1, M_2\rangle \mid L(M_1) = L(M_2)\} \notin \mathbb{A} \cup \mathbb{A}^{co}$

Satz von Rice (Korollar)

Sei $L \subsetneq \{L \in \mathbb{A}\}$ mit $\mathcal{L} \neq \emptyset$, dann ist $\{\langle M\rangle \mid L(M) \in L\} \notin \mathbb{E}$
(Aussage über Sprachen, die aus Codes von TM bestehen!)

Rekursionstheorem

Wir können annehmen, dass jede TM M das Programm "get your own code" als Unterprogramm aufrufen kann.

Abschluss von §3

Bew.: PKP, MPKP $\notin \mathbb{E}$
Exkurs: $Th(\mathbb{N},+) \in \mathbb{E}$, $Th(\mathbb{N},+,\cdot) \notin \mathbb{E}$, $Pr(Th(\mathbb{N},+,\cdot)) \subsetneq Th(\mathbb{N},+,\cdot)$
$\Rightarrow$ Nicht jede wahre Aussage ist beweisbar (1ste Gödelsche Unvollständigkeitssatz)

§4 Komplexitätstheorie / Wie schnell kann TM ein Problem lösen?

P

Sei $f : \mathbb{N} \to \mathbb{N}$, dann $\text{TIME}(f(n)) = \{L \mid$ ex. TM M mit $t_M = \mathcal{O}(f(n))\}$
"Sprachen, die ungefähr so schnell entscheidbar sind, wie f wächst."

$$\begin{aligned} P :&= \bigcup_{k=1}^{\infty} \text{TIME}(n^k) \\ &= \{L \mid \text{ex. TM } M \text{ mit } L(M) = L \text{ und } t_M(n) = \mathcal{O}(n^k) \text{ für ein } k \geq 1\} \\ &= \{L \mid \text{ex. TM } M \text{ mit } L(M) = L \text{ und } t_M(n) = \mathcal{O}(f(n)) \text{ für ein Polynom } f\} \end{aligned}$$

"In polynomieller Zeit lösbar" $\Rightarrow$ effizient lösbar

NP

$NP = \{L \mid$ ex. TM V mit $t_V(n) = \mathcal{O}(n^k)$ für ein $k \geq 1$ und $L = \{w \mid \exists z \in \Sigma^*, |z| \leq |w|^*$ und $\langle w, z\rangle \in L(V)\}\}$

$$\begin{aligned} \text{NTIME}(f(n)) &= \{L \mid \exists \text{ NTM } N \text{ mit } t_N(n) = \mathcal{O}(f(n))\} \\ NP :&= \bigcup_{k=1}^{\infty} \text{NTIME}(n^k) \\ &= \{L \mid \text{ex. NTM } N \text{ mit } L(N) = L \text{ und } t_N(n) = \mathcal{O}(f(n)) \\ &\qquad \text{für ein Polynom } f\} \end{aligned}$$

$$\subseteq \text{EXPTIME} = \bigcup_{k=1}^{\infty} \text{TIME}(2^{(n^k)})$$

NP = nicht-determistisch in polynomieller Zeit berechenbar
Bsp.: $SAT \in NP$ Bem.: $CFL \subseteq P$, da CYK in polynomieller Zeit läuft (ohne Beweis).

Grenze zwischen P und NP?

Offenes Problem gilt $P = NP$?

Polyzeitreduktion

$L_1 \subseteq \Sigma^*, L_2 \subseteq (\Sigma')^*, f$ heißt polyzeit Reduktion von L_1 auf L_2, wenn

(1.) f ist berechenbar und total

(2.) $\forall w \in \Sigma^* : w \in L_1 \Leftrightarrow f(w) \in L_2$

(3.) f wird durch TM M berechnet mit $t_M(n) = \mathcal{O}(n^k)$ für ein $k \geq 1$

Schreibe dann $L_1 \leq_p L_2$.
Bem.: $L_1 \leq_p L_2, L_2 \in P \Rightarrow L_1 \in P$

NP-vollständigkeit

L ist NP-vollständig, wenn gilt

1. $L \in NP$
2. $\forall L' \in NP$ gilt $L' \leq_p L$

NPC $= \{L \mid L$ ist NP-vollst. $\} \subseteq NP$

Satz

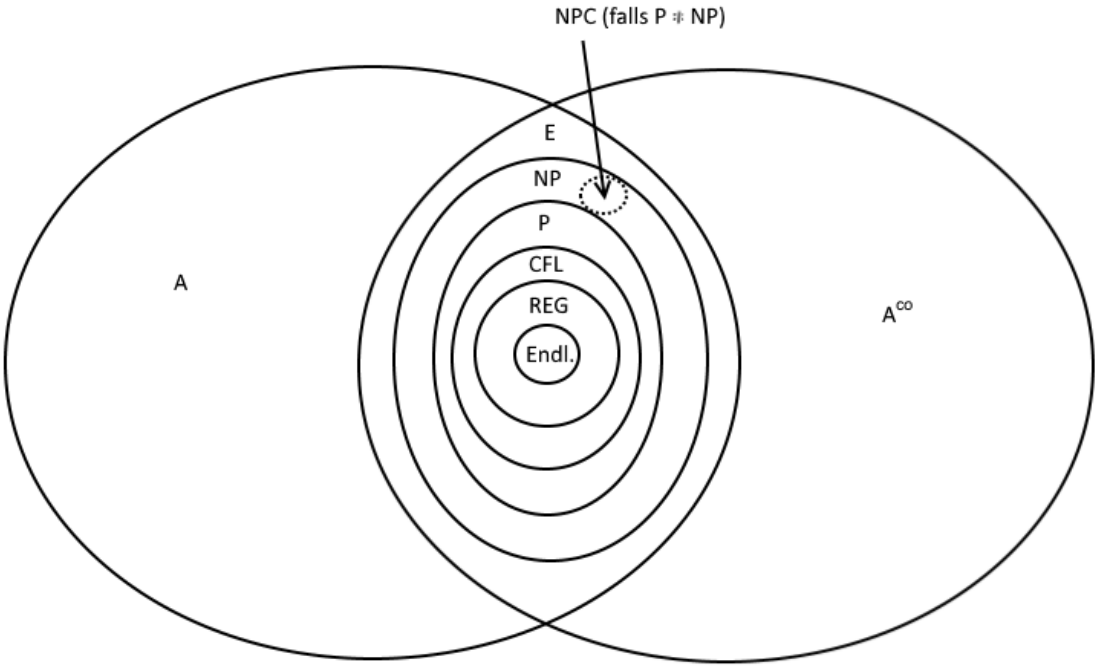
Wenn $P \neq NP$, dann ist $NPC \cap P = \emptyset$

Satz (Cook-Levin)

SAT ist NP-vollständig

Lemma

$A \in NPC, B \in NP, A \leq_p B \Rightarrow B \in NPC$ ($\rightsquigarrow 3SAT$ NP-vollständig)



Auf einen Blick

Sprache	REG	CFL	P	NP	$\mathbb{E}$	$\mathbb{A}$	$\mathbb{A}^{co}$
endl. z.B. $\{a^n \mid n < 13\}$	✓	✓	✓	✓	✓	✓	✓
$\{0^n \mid n \text{ gerade}\}$	✓	✓	✓	✓	✓	✓	✓
$\{0^n 1^n \mid n \geq 0\}$	×	✓	✓	✓	✓	✓	✓
$\{0^n 1^n 2^n \mid n \geq 0\}$	×	×	✓	✓	✓	✓	✓
SAT	×	×	?	✓	✓	✓	✓
$Pr(Th(\mathbb{N}, +, \cdot))$	×	×	×	×	✓	✓	✓
A_{TM}	×	×	×	×	×	✓	×
HALT	×	×	×	×	×	✓	×
$\overline{A_{TM}}$	×	×	×	×	×	×	✓
EQ_{TM}	×	×	×	×	×	×	×

Es gilt: $REG \subset CFL \subset P \subset NP \subset \mathbb{E} \subset \mathbb{A}$.