Gliederung

1. Einführung
2. Berechenbarkeitsbegriff
3. LOOP-, WHILE-, und GOTO-Berechenbarkeit
4. Primitive und partielle Rekursion
5. Grenzen der LOOP-Berechenbarkeit
6. (Un-)Entscheidbarkeit, Halteproblem
7. Aufzählbarkeit & (Semi-)Entscheidbarkeit
8. Reduzierbarkeit
9. Satz von Rice
10. Das Postsche Korrespondenzproblem
11. Komplexität – Einführung
12. NP-Vollständigkeit
13. coNP
14. PSPACE

Co-Nichtdeterministische Turing-Maschinen

Definition (Co-Nichtdeterministische Turing-Maschine)

- $\delta \subseteq (Z \setminus E) \times \Gamma \times Z \times \Gamma \times \{L, R, N\}$
- "Folgekonfiguration"-Relation $\vdash_M^1$ von M spannt Berechnungsbaum auf
- coNTM akzeptiert $\Leftrightarrow$ alle Berechnungspfade erreichen akzeptierende Konfiguration

time_{coN} und $\mathrm{coNTIME}\,(f(n))$ analog zu time_N und $\mathrm{NTIME}\,(f(n))$

Definition (coNP)

$\mathrm{coNP} := \bigcup_{k\geq 1} \mathrm{coNTIME}\,(n^k)$. "**co-nicht**deterministisch, in Polynomzeit"

Theorem (Alternative Definition für coNP („Guess and Check"))

Eine Sprache $L \subseteq \Sigma^*$ ist in coNP, gdw. ein Polynom $p : \mathbb{N} \to \mathbb{N}$ und eine polynomiell zeitbeschränkte **D**TM M (d.h. $\mathrm{time}_M(n) \in O(n^c)$) existieren, sodass für jedes $x \in \Sigma^*$ gilt

$$x \in L \Leftrightarrow \forall_{u \in \Sigma^{p(|x|)}} \langle x, u\rangle \in T(M)$$

beziehungsweise $$x \notin L \Leftrightarrow \exists_{u \in \Sigma^{p(|x|)}} \langle x, u\rangle \notin T(M).$$

Beachte: zentraler Unterschied zu NP: „$\forall$" statt „$\exists$"

Die Komplexitätsklasse coNP I

Erinnerung: Sei $L \subseteq \Sigma^*$, dann ist $\bar{L} := \Sigma^* \setminus L$ das Komplement von L.

Theorem

$\text{coNP} = \{L \subseteq \Sigma^* \mid \bar{L} \in \text{NP}\}$.

Beweis

Sei $L \subseteq \Sigma^*$. "Guess and Check" $\rightsquigarrow$ $\bar{L} \in \text{NP}$ genau dann wenn es eine polynomiell zeitbeschränkte DTM M gibt mit

$$x \in \bar{L} \Leftrightarrow \exists_{u \in \Sigma^{p(|x|)}} \langle x, u \rangle \in T(M).$$

Eine solche DTM M gibt es genau dann, wenn es auch eine polynomiell zeitbeschränkte DTM M' gibt, die genau dann ablehnt, wenn M akzeptiert. Also gilt

$$\begin{aligned} x \in L \Leftrightarrow x \notin \bar{L} &\Leftrightarrow \neg \left(\exists_{u \in \Sigma^{p(|x|)}} \langle x, u \rangle \in T(M) \right) \\ &\Leftrightarrow \forall_{u \in \Sigma^{p(|x|)}} \langle x, u \rangle \notin T(M) \\ &\Leftrightarrow \forall_{u \in \Sigma^{p(|x|)}} \langle x, u \rangle \in T(M') \end{aligned}$$

Die Komplexitätsklasse coNP II

Erinnerung: Sei $L \subseteq \Sigma^*$, dann ist $\bar{L} := \Sigma^* \setminus L$ das Komplement von L.

Theorem

$\mathrm{coNP} = \{L \subseteq \Sigma^* \mid \bar{L} \in \mathrm{NP}\}$.

Bemerkungen:

- coNP ist nicht das Komplement von NP (z.B. $H \notin \mathrm{NP}$ und $H \notin \mathrm{coNP}$)
- $\mathrm{P} \subseteq \mathrm{NP} \cap \mathrm{coNP}$ (da $L \in \mathrm{P} \Leftrightarrow \bar{L} \in \mathrm{P}$)
- coNP-Vollständigkeit analog zu NP-Vollständigkeit:
  $A \subseteq \Sigma^*$ ist coNP-vollständig $\Leftrightarrow \forall_{L \in \mathrm{coNP}}\ L \leq_m^p A$ und $A \in \mathrm{coNP}$
- $\overline{\mathrm{SAT}} := \{\varphi \mid \varphi$ ist unerfüllbar$\} \in \mathrm{coNP}$ (sogar coNP-vollständig)
- $(\mathrm{P} = \mathrm{NP}) \Rightarrow (\mathrm{NP} = \mathrm{coNP} = \mathrm{P})$
  für alle $L \in \mathrm{coNP}$ gilt: $\bar{L} \in \mathrm{NP} \Rightarrow \bar{L} \in \mathrm{P} \Rightarrow L \in \mathrm{P}$ und somit $L \in \mathrm{NP}$
- **Offen:** $(\mathrm{NP} = \mathrm{coNP}) \Rightarrow (\mathrm{P} = \mathrm{NP})$?

Ein coNP-vollständiges Problem

TAUT

Eingabe: aussagenlogische Formel F

Frage: Ist F eine **Tautologie**, d.h. wird F für **alle** $\{0,1\}$-wertigen Belegungen der in F verwendeten Booleschen Variablen zu wahr (d.h. 1) ausgewertet?

Theorem

TAUT ist coNP-vollständig.

Beweis

1. $\mathrm{TAUT} \in \mathsf{coNP}$ via "Guess and Check" (nicht-erfüllende Belegung zertifiziert $F \notin \mathrm{TAUT}$)
2. TAUT ist coNP-schwer (d.h. $\forall_{L \in \mathsf{coNP}}\ L \leq_m^p \mathrm{TAUT}$):

Da $\bar{L} \in \mathsf{NP}$, gilt $\bar{L} \leq_m^p \mathrm{SAT}$ vermöge einer Polynomzeitreduktion $f\colon x \mapsto F_x$. Also

$$x \in L \Leftrightarrow x \notin \bar{L} \Leftrightarrow F_x \notin \mathrm{SAT} \Leftrightarrow \neg F_x \in \mathrm{TAUT}.$$

Also ist $g\colon x \mapsto \neg F_x$ eine Polynomzeitreduktion von L auf TAUT.