Übung 12: Komplexitätstheorie

Theoretische Informatik Sommersemester 2013

Markus Kaiser

July 15, 2013

Definition (*TIME*)

Wir bezeichnen die minimale Anzahl der Schritte, bis eine DTM M mit Eingabe w hält als $time_M(w) \in \mathbb{N} \cup \{\infty\}$.

Sei $f : \mathbb{N} \to \mathbb{N}$ total. Dann ist

$$TIME(f(n)) := \{A \subseteq \Sigma^* \mid \exists DTM\ M.A = L(M) \wedge \forall w \in \Sigma^*.time_M(w) \leq f(|w|)\}$$

die Klasse der in Zeit $f(n)$ von einer DTM entscheidbaren Sprachen.

- $TIME(\mathcal{O}(n))$ enthält alle "linearen Probleme".
- Also alle Probleme, für die ein Linearzeitalgorithmus existiert.

Definition (*NTIME*)

Wir bezeichnen die minimale Anzahl der Schritte, bis eine NTM M mit Eingabe w hält als $ntime_M(w) \in \mathbb{N}$.

$$ntime_M(w) := \begin{cases} \text{minimale Schrittanzahl} & \text{falls } w \in L(M) \\ 0 & \text{falls } w \notin L(M) \end{cases}$$

Dann ist

$$NTIME(f(n)) := \{A \subseteq \Sigma^* \mid \exists NTM\ M. A = L(M) \wedge \forall w \in \Sigma^*. ntime_M(w) \leq f(|w|)\}$$

die Klasse der in Zeit $f(n)$ von einer NTM entscheidbaren Sprachen.

P und NP

Definition

P ist die Menge aller von einer DTM in polynomieller Zeit entscheidbaren Sprachen.

$$P := \bigcup_{p \text{ Polynom}} TIME(p(n)) = \bigcup_{k \in \mathbb{N}} TIME(\mathcal{O}(n^k))$$

Definition

NP ist die Menge aller von einer NTM in polynomieller Zeit entscheidbaren Sprachen.

$$NP := \bigcup_{p \text{ Polynom}} NTIME(p(n)) = \bigcup_{k \in \mathbb{N}} NTIME(\mathcal{O}(n^k))$$

Verifikator

Definition (Verifikator)

Sei M eine DTM mit $L(M) \subseteq \{w\#c \mid w \in \Sigma^*, c \in \Delta^*\}$.

- Falls $w\#c \in L(M)$, dann heißt c Zertifikat für w.
- M ist ein polynomiell beschränkter Verifikator für

$$\{w \in \Sigma^* \mid \exists c \in \Delta^*. w\#c \in L(M)\}$$

falls $time_M(w\#c) \leq p(|w|)$ für ein Polynom p.

- NTM rät Lösung (Zertifikat), DTM probiert sie aus.
- Verifizieren (wahrscheinlich) einfacher als Lösung finden.

Satz

$A \in NP$ gdw es einen pol. beschränkten Verifikator für A gibt.

Definition (Polynomielle Reduzierbarkeit)

Eine Menge $A \subseteq \Sigma^*$ ist polynomiell reduzierbar auf eine Menge $B \subseteq \Gamma^*$ gdw es eine totale und von einer DTM in polynomieller Zeit berechenbare Funktion $f : \Sigma^* \to \Gamma^*$ gibt mit

$$\forall w \in \Sigma^*.w \in A \iff f(w) \in B$$

Wir schreiben dann $A \leq_P B$.

- Die Relation $\leq_P$ ist transitiv.
- P und NP sind nach unten abgeschlossen:

$$A \leq_P B \in P/NP \implies A \in P/NP$$

NP-Vollständigkeit

Definition (NP-Schwere)

Eine Sprache L heißt NP-schwer (NP-hart) wenn sich alle Sprachen in NP auf L reduzieren lassen.

$$\forall A \in NP.A \leq_P L$$

Definition (NP-Vollständigkeit)

Eine Sprache L heißt NP-vollständig wenn L NP-schwer ist und $L \in NP$.

Fragen:

- Gibt es überhaupt NP-vollständige Sprachen?
- Gibt es eine NP-vollständige Sprache in P?

Definition (Aussagenlogik)

Syntax der Aussagenlogik.

$$\text{Formeln} \quad F \to \neg F \mid (F \wedge F) \mid (F \vee F) \mid X$$
$$\text{Variablen} \quad X \to x \mid y \mid z \mid \ldots$$

Definition (SAT)

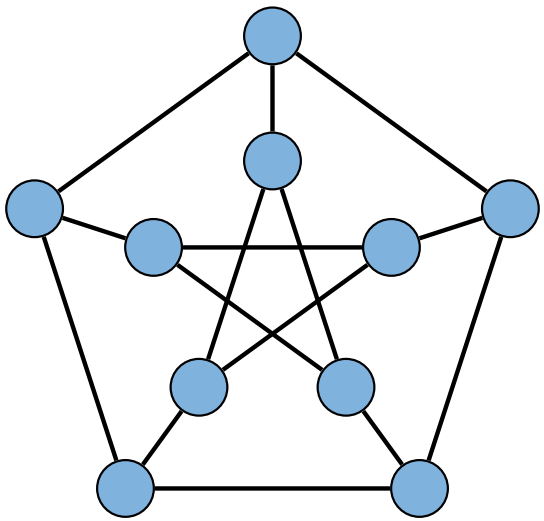
Gegeben eine aussagenlogische Formel F.
Ist F erfüllbar, also gibt es eine Belegung der Variablen in F, sodass F gilt?

Satz (Cook 1971)

SAT *ist NP-vollständig.*

Definition (3COL)

Gegeben ein Graph $G = (V, E)$.
Gibt es eine Färbung der Knoten V mit 3 Farben, so dass keine zwei benachbarten Knoten die gleiche Farbe haben?

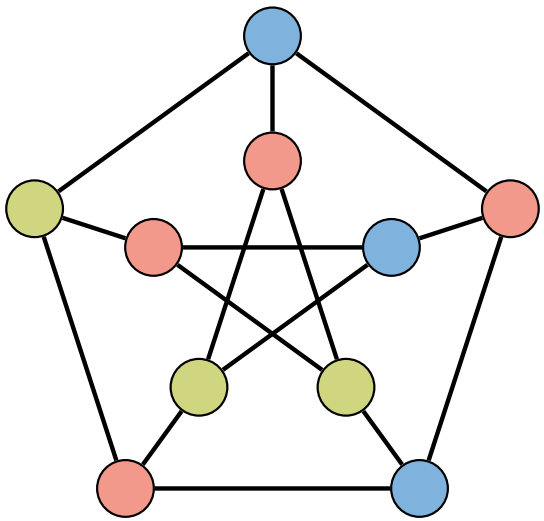


Satz

Es ist **3COL** $\leq_P$ **SAT** *und* **SAT** $\leq_P$ **3SAT** $\leq_P$ **3COL**.

Definition (3COL)

Gegeben ein Graph $G = (V, E)$.
Gibt es eine Färbung der Knoten V mit 3 Farben, so dass keine zwei benachbarten Knoten die gleiche Farbe haben?



Satz

Es ist **3COL** $\leq_P$ **SAT** *und* **SAT** $\leq_P$ **3SAT** $\leq_P$ **3COL**.