

Theorem 5. $NP \subseteq EXP$

Beweis. Sei $L \in NP$ und sei T eine NTM, die L in Zeit $TIME_T(w) \leq |w|^k$, $k \in \mathbb{N}$ akzeptiert.

Also: $w \in L \iff$ es gibt einen Pfad im Berechnungsbaum zu w ,
der nach höchstens $|w|^k$ Schritten akzeptiert.

Deterministischer Algorithmus: Tiefensuche im Berechnungsbaum bis zur Tiefe $|w|^k$.

Anmerkung: Der Berechnungsbaum ist potenziell beliebig tief; da die Zeit aber durch $|w|^k$ begrenzt wird, genügt es, nur bis zu dieser Tiefe zu suchen.
Zeit für Tiefensuche: Linear in der Größe des Baums.

Da die Übergangstafel der NTM T endlich ist, gibt es eine Konstante d , sodass $S \rightarrow S'$ für maximal d viele S' . Diese Konstante lässt sich durch $|\Sigma|^b \cdot 3^b \cdot |Q|$ nach oben abschätzen, wobei b Anzahl der Bänder von T .

Der Baum hat also höchstens Verzweigungsgrad d , also ist die Größe $\leq 2 \cdot d^{|w|^k} \leq 2^{(\log d) \cdot |w|^k + 1} \leq O(2^{|w|^{k+1}})$.

Also $L \in EXP$. □

Bemerkung 1. Genauso zeigt man: $NE \subseteq 2 \cdot E$.

Dieses Theorem lässt sich auch leicht in folgendem Sinne verallgemeinern:
nichtdeterministische Zeit $t \subseteq$ deterministische Zeit 2^t

Padding

Technik zum Übertragen von Resultaten "nach oben".

Theorem 6. Falls $P = NP$, dann auch $E = NE$.

Beweis. Sei $\# \notin \Sigma$.

Für $w \in \Sigma^*$ sei $pad(w) := w \overbrace{\#\#\dots\#}^{2^{|w|}-|w|}$, also $|pad(w)| = 2^{|w|}$.

Für $L \subseteq \Sigma^*$ definiere entsprechend $pad(L) := \{pad(w) \mid w \in L\}$.

Sei $L \in NE$, sei T eine NTM, die L akzeptiert mit $TIME_T(w) \leq O(2^{k \cdot |w|})$.

Maschine T' verhält sich bei Input $pad(w)$ genau wie T bei w . Dabei muss die Maschine zunächst natürlich überprüfen, dass das gegeben Wort auch von der gewünschten, "gepaddingten" Form ist.

T' akzeptiert $pad(L)$ in Zeit $TIME_{T'}(pad(w)) = TIME_T(w) \leq O(2^{k \cdot |w|}) = O(pad(w)^k)$, und damit $pad(L) \in NP$, also wegen Annahme $pad(L) \in P$.

Sei T'' eine DTM, die $pad(L)$ akzeptiert in der Zeit $O(|pad(w)|^{k'})$.

Konstruiere T^* wie folgt:

- Lese Input w .
- Ergänze w zu $pad(w)$. (Zeit $O(2^{|w|})$)
- Setze T'' auf $pad(w)$ an. (Zeit $O(2^{k' \cdot |w|}) = O(|pad(w)|^{k'})$)

Insgesamt also Zeit $O(2^{(k'+1) \cdot |w|})$, und damit $L \in E$. □

3 Die Klassen P und NP

3.0 Übersicht

- Probleme in NP , P
- NP -vollständige Probleme
- Struktur von NP
- Relativierung

3.1 Probleme in NP und P

- Klassisches Problem in NP : SAT.

Gegeben: Aussagenlogische Formel F in KNF

Frage: Ist F erfüllbar?

- KNF: $\bigwedge_j C_j$, wobei $C_j = \bigvee_i a_{ij}$, a_{ij} Literale
 - Die C_j nennt man Klauseln
 - Erfüllbar: Gibt es eine Belegung $\alpha : Var \rightarrow \{0, 1\}$, derart, dass der Wert $\alpha(F) = 1$
- Spezialfall k-SAT: Jede Klausel enthält höchstens k Literale
Dabei gilt: 2-SAT $\in P$, 3-SAT $\in NP$.
 - Spezialfall Horn-SAT: Jede Klausel enthält höchstens ein positives Literal
Dabei gilt: Horn-SAT $\in P$.

Graphenprobleme:

- k-Färbbarkeit

Gegeben: $G = (V, E)$, $E \subseteq V^2$

Frage: Gibt es eine Färbung $c : V \rightarrow \{1, \dots, k\}$ mit $\{u, v\} \in E \Rightarrow c(u) \neq c(v)$

- Spezialfall: 2-Färbbarkeit $\in P$.
- Vertex Cover (Knotenüberdeckungsproblem) $\in NP$

Gegeben: Graph $G = (V, E)$ und $k \in \mathbb{N}$.

Frage: Gibt es ein V.C. $U \subseteq V$ mit $|U| \leq k$, d.h. $\forall e \in E : e \cap U \neq \emptyset$

- Matching $\in P$ (Edmonds, 1964)

Gegeben: Graph $G = (V, E)$ und $k \in \mathbb{N}$.

Frage: Gibt es Matching $M \subseteq E$ mit $|M| \geq k$, d.h. $\forall e \neq e' \in M : e \cap e' = \emptyset$.

- Anmerkung: Ein perfektes Matching ist ein Matching der Größe $\frac{n}{2}$.
- Anmerkung 2: Die genaue Komplexität dieses Problems ist bis heute (2006) unbekannt.

Proposition 1. $L \in NP$ gdw. es eine $R_L(\cdot, \cdot) \in P$ und $k \in \mathbb{N}$ gibt, mit

$$\forall x : x \in L \iff \exists w : |w| \leq |x|^k \wedge R_L(x, w)$$

Beweis. " $\Leftarrow$ ": NTM rät w mit $|w| \leq |x|^k$ bei Input x , überprüfe, dass $(x, w) \in R_L$.

" $\Rightarrow$ ": Sei T eine NTM, die L akzeptiert mit $TIME_T(x) \leq |x|^k$.

$x \in L$ gdw. es gibt $S_0, \dots, S_{|x|^k}$ von globalen Zuständen von T , sodass $S_1 = S_0(x)$, $S_{|x|^k}$ akzeptierend und $\forall i : S_i \rightarrow_T S_{i+1}$.

Die Folge $S_1, \dots, S_{|x|^k}$ ist Zeuge für $x \in L$. Da jedes $|S_i| \leq O(|x|^k)$, d.h. $|S_1, \dots, S_{|x|^k}| \leq |x|^{2k}$. $\square$

Beispiel 1. *co-PRIM*

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

Frage: Ist n zusammengesetzt?

$\exists k, l : \underbrace{k > 1 \wedge l > 1 \wedge k \cdot l = n}_{\in P}, \text{ also } co\text{-PRIM} \in NP$