Grundzüge der Theoretischen Informatik

Kapitel 21 und 22

Markus Bläser

Universität des Saarlandes

12.1.2022

Berühmte letzte Worte

Der Akku hat noch 18% . . .

Kapitel 22: P und NP

P und NP

NP
nichtdeterministische Polynomzeit

Definition (22.1)

$$P := \bigcup_{i \in \mathbb{N}} \mathrm{DTime}(O(n^i))$$

$$NP := \bigcup_{i \in \mathbb{N}} \mathrm{NTime}(O(n^i))$$

- P und NP sind robuste Klassen,
  d.h. unabhängig von konkreten Maschinenmodell.

$$NP = \bigcup_{i \in \mathbb{N}} \mathrm{NTime}(O(n^i)) \subseteq \bigcup_{i \in \mathbb{N}} \mathrm{DTime}(2^{O(n^i)}) =: EXP,$$

Probleme in P

$$s\text{-t-CONN} = \{(G, s, t) \mid \text{G ist ein gerichteter Graph}$$
$$\text{der einen Pfad von } s \text{ nach } t \text{ hat}\}.$$

Theorem (22.2)

s-t-CONN $\in$ P.

Stärker gilt: s-t-CONN $\in$ NL := NSpace$(\log n)$

NP und Zertifikate

$V(M) \neq L(M)$

x $[x, c]$

Definition (22.3)

Eine polynomialzeit-beschränkte DTM M heißt *Polynomialzeit-Verifizierer* für $L \subseteq \{0,1\}^*$, falls es ein Polynom p gibt mit:

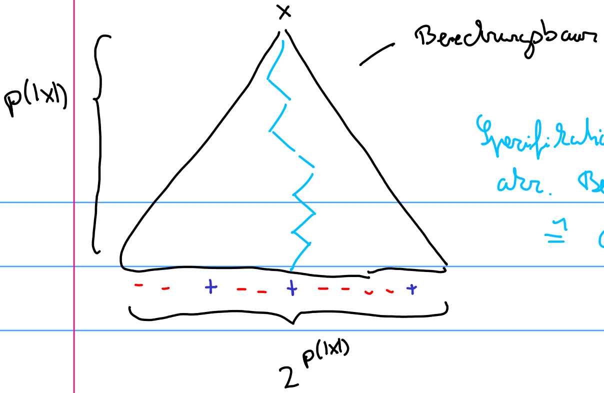
1. Für alle $x \in L$ gibt es ein $c \in \{0,1\}^*$ mit $|c| \leq p(|x|)$, so dass M das Paar $[x, c]$ akzeptiert.
2. Für alle $x \notin L$ und alle $c \in \{0,1\}^*$ liest M auf Eingabe $[x, c]$ höchstens $p(|x|)$ Bits von c und verwirft $[x, c]$ immer.

Die von M verifizierte Sprache L bezeichnen wir mit $V(M)$.

Theorem (22.4)

$L \in \mathrm{NP}$ *genau dann wenn es einen Polynomialzeit-Verifizierer für* L *gibt.*

"$\Rightarrow$"



Spezifikation eines akz. Berechnungspfades $\hat{=}$ c

Probleme in NP

- Eine *Clique* eines Graphs $G = (V, E)$ ist eine Teilmenge $C \subseteq V$, so dass $\{u, v\} \in E$ für alle $u, v \in C$ mit $u \neq v$.
  C heißt k-*Clique*, falls zusätzlich $|C| = k$.

  $$\mathrm{Clique} = \{(G, k) \mid G \text{ ist ein ungerichteter Graph mit einer } k\text{-Clique}\}.$$

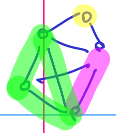
- Ein *Vertex-Cover* von $G = (V, E)$ ist eine Teilmenge $C \subseteq V$, so dass $e \cap C \neq \emptyset$ für alle $e \in E$. $e = \{u, v\}$

  $$\mathrm{VC} = \{(G, k) \mid G \text{ ist ein ungerichteter Graph, der einen Vertex-Cover der Größe } \leq k \text{ hat}\}.$$

- Subset-Sum ist das folgende Problem:

  $$\mathrm{Subset\text{-}Sum} = \{(x_1, \ldots, x_n, b) \mid x_1, \ldots, x_n, b \in \mathbb{N} \text{ und es gibt ein } I \subseteq \{1, \ldots, n\} \text{ mit } \sum_{i \in I} x_i = b.\}$$

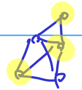
Clique



Wenn C eine Clique ist dann ist auch $C' \subseteq C$ eine Clique

n^k

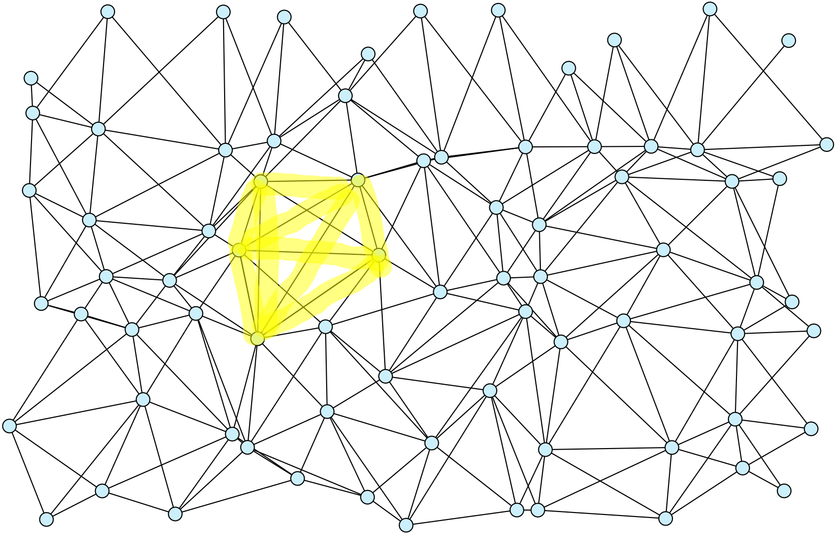
Vertex - Cover



$2^k \cdot poly(n)$

Hat dieser Graph eine 5-Clique?

$\binom{n}{k}$



Probleme in NP (2)

2^n $2^{n/2}$

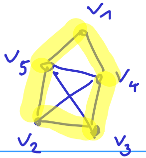
- Sei $G = (V, E)$ ein Graph und $V = \{v_1, \ldots, v_n\}$.
  G hat einen *Hamiltonschen Kreis* falls es eine Permutation π gibt, so dass $\{v_{\pi(i)}, v_{\pi(i+1)}\} \in E$ für alle $1 \le i < n$ und $\{v_{\pi(n)}, v_{\pi(1)}\} \in E$.

$$\mathrm{HC} = \{G \mid G \text{ hat einen Hamiltonschen Kreis}\}.$$

- Sei $G = (V, \binom{V}{2}, w)$ ein vollständiger kantengewichteten Graph, wobei $w : \binom{V}{2} \to \mathbb{N}$.
  Das Gewicht eines Hamiltonschen Kreises ist
  $$\sum_{i=1}^{n-1} w(\{v_{\pi(i)}, v_{\pi(i+1)}\}) + w(\{v_{\pi(n)}, v_{\pi(1)}\}).$$

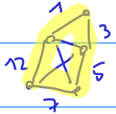
$$\mathrm{TSP} = \{(G, b) \mid G \text{ ist ein vollständiger kantengewichteter Graph mit einem Hamiltonschen Kreis mit Gewicht} \le b\}.$$

H C.



$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 2 & 5 \end{pmatrix}$$

TSP



$1 + 3 + 5 + 7 + 12 = 28$

Probleme in NP (3)

- Seien $x_1, \ldots, x_n$ Boolesche Variablen.
- Ein *Literal* ist eine Variable x_i oder ihre Negation $\bar{x}_i$.
- Eine *Klausel* ist eine Disjunktion von Literalen $\ell_1 \vee \cdots \vee \ell_k$. k ist die Länge der Klausel. $x_1 \vee x_7 \vee \overline{x_{13}}$
- Eine *Formel in konjunktiver Normalform (CNF)* ist eine Konjunktion von Klauseln $c_1 \wedge \cdots \wedge c_m$.
- Eine *Belegung* weist jeder Variablem eine Wert aus $\{0, 1\}$ zu.
- Eine Belegung a erfüllt eine Formel F, falls F unter a zu 1 auswertet.
- Eine Formel ϕ heißt erfüllbar, falls es eine erfüllende Belegung für ϕ gibt.

$$\mathrm{SAT} = \{\phi \mid \phi \text{ ist eine erfüllbare Formel in CNF}\}$$

"Die Mutter aller NP-vollständigen Problemen"

Probleme in NP (4)

- Eine Formel in CNF ist in ℓ-CNF, falls alle Klauseln Länge $\leq \ell$ haben.

$$\ell\mathrm{SAT} = \{\phi \mid \phi \text{ is a satisfiable formula in } \ell\text{-CNF}\}.$$

Theorem (22.5)

Clique, VC, Subset-Sum, HC, TSP, SAT, ℓSAT $\in$ NP.

H ist vollständig für RE

$\forall L \in RE: \; L \leq H$

echte Inklusion

?

Beweis 22.5.

1) Wir konstruieren einen Polynomialzeit-Verifizierer für Clique:

Eingabe (G, k), Beweis ist eine Knoten C der Größe k

Verifizierer testet, ob alle Knoten in C miteinander verbunden. Falls ja akzeptiert er, sonst verwirft er.

Falls $(G, k) \in$ Clique, dann kann man als C eine k-Clique angeben und der Verifizierer wird akzeptieren

Falls $(G, k) \notin$ Clique, dann hat G keine k-Clique und egal welches C der Verifizierer erhält, er wird nie akzeptieren.

Der Verifizierer kann in Polynomialzeit implementiert werden, da $\binom{|C|}{2} \leq n^2$

Formal ist der Beweis $\in \{0,1\}^*$

Um die Details der Kodierung kümmern wir uns nicht.

3) Subset-Sum

Eingabe: $(x_1, \dots, x_n, b) \in \mathbb{N}^{n+1}$

Beweis: $I \subseteq \{1, \dots, n\}$

überprüfen, $\sum_{i \in I} x_i \overset{?}{=} b$

4) HC

Eingabe: $G = (V, E)$, $V = \{v_1, \dots, v_n\}$

Beweis: $\pi \in S_n$

überprüfen: ist $\{v_{\pi(i)}, v_{\pi(i+1)}\} \in E$

$i = 1, \dots, n-1$

$\{v_{\pi(n)}, v_{\pi(1)}\} \in E$?

6) SAT

Eingabe: ϕ in CNF (in Var $x_1, \dots, x_n$)

Beweis: eine $\{0,1\}$-Belegung der Var.

überprüfen, erfüllt die Belegung die

Formel.

Kapitel 23: Reduktion und Vollständigkeit

Polynomialzeit-Reduktionen

DTM

Definition (23.1)

Seien $L, L' \subseteq \Sigma^*$.

1. $f : \Sigma^* \to \Sigma^*$ ist eine *many-one-Polynomialzeit-Reduktion* von L auf L', falls f Polynomialzeit-berechenbar ist und

$$\text{für alle } x \in \Sigma^* \text{ gilt:} \quad x \in L \iff f(x) \in L'.$$

2. L ist *(many-one-)Polynomialzeit-reduzierbar* auf L' falls es so eine Reduktion f gibt. Wir schreiben: $L \leq_P L'$.

Polynomialzeit-Reduktionen (2)

Lemma (23.2)

Falls $\mathrm{L} \leq_{\mathrm{P}} \mathrm{L}'$ *und* $\mathrm{L}' \in \mathsf{P}$, *dann ist* $\mathrm{L} \in \mathsf{P}$.

Lemma (23.3)

$\leq_{\mathrm{P}}$ *ist transitiv.*

Beweis 23.2

Sei F eine Polyzeit-Red von L nach L' Laufzeit $p(n)$

Sei M' eine Polyzeit-DTM für L' Laufzeit $q(n)$

DTM M für L wie folgt

Eingabe $x \in \Sigma^*$

1) Rechne $F(x)$ aus $p(n)$, $n = |x|$

2) Simuliere M' auf $F(x)$. Falls M' akz. so akz. Sonst verwerfe $q(|F(x)|) \leq q(p(n))$

Polynom!

$L(M) = L$. Wenn $x \in L \Rightarrow F(x) \in L' \Rightarrow M'$ akz. ($\surd$)

$x \notin L \Rightarrow F(x) \notin L' \Rightarrow M'$ verw. $\square$