Teil III

Komplexitätstheorie

Übersicht

Übersicht

Die Klasse P

Ein Problem A ist in der Klasse P, wenn

- es eine DTM M gibt, die A entscheidet,
- die Berechnung vom M bei Eingabe w hält nach $p(|w|)$ Schritten, für ein Polynom $p()$.

Die Klasse P

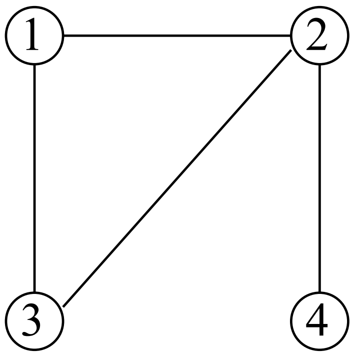
Ein Problem A ist in der Klasse P, wenn

- es eine DTM M gibt, die A entscheidet,
- die Berechnung vom M bei Eingabe w hält nach $p(|w|)$ Schritten, für ein Polynom $p()$.

Seit den Arbeiten von *Jack Edmonds* (1965) wird P mit der Klasse der effizient lösbaren Probleme identifiziert.

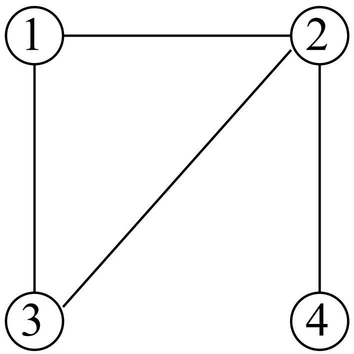
Codierung von Graphen

Ein Graph $G = (V, E)$ wird codiert als Adjazenzmatrix:



Codierung von Graphen

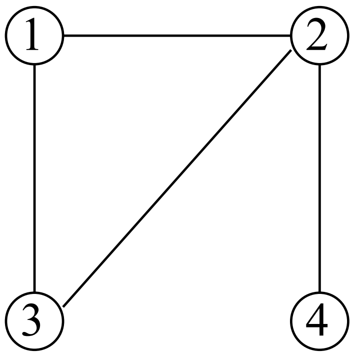
Ein Graph $G = (V, E)$ wird codiert als Adjazenzmatrix:



$$\begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

Codierung von Graphen

Ein Graph $G = (V, E)$ wird codiert als Adjazenzmatrix:



$$\begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

Repräsentation als String: $0110\#1011\#1100\#0100$

Probleme in P

Problem Minimum Path

Instanz:	Graph $G = (V, E)$, Knoten s, t, $k \in \mathbb{N}$
Frage:	Gibt es Weg von s nach t der Länge $\leq k$?

Probleme in P

Problem MINIMUM PATH

Instanz:	Graph $G = (V, E)$, Knoten s, t, $k \in \mathbb{N}$
Frage:	Gibt es Weg von s nach t der Länge $\leq k$?

Problem MAXIMUM MATCHING

Instanz:	Graph $G = (V, E)$, $k \in \mathbb{N}$
Frage:	Gibt es Matching M mit $|M| \geq k$?

Probleme in P

Problem Minimum Path

Instanz:	Graph $G = (V, E)$, Knoten s, t, $k \in \mathbb{N}$
Frage:	Gibt es Weg von s nach t der Länge $\leq k$?

Problem Maximum Matching

Instanz:	Graph $G = (V, E)$, $k \in \mathbb{N}$
Frage:	Gibt es Matching M mit $\|M\| \geq k$?

Matching: $M \subseteq E$ mit $e_1 \cap e_2 = \emptyset$ für alle $e_1, e_2 \in M$

Die Klasse NP

Ein Problem A ist in NP, wenn es

- eine Relation R_A in P und
- ein Polynom $p()$ gibt, so dass

$$x \in A \iff \exists z : |z| \leq p(|x|) \;\&\; (x, z) \in R_A$$

Die Klasse NP

Ein Problem A ist in NP, wenn es

- eine Relation R_A in P und
- ein Polynom $p()$ gibt, so dass

$$x \in A \iff \exists z : \ |z| \leq p(|x|) \ \& \ (x, z) \in R_A$$

Ein z mit $(x, z) \in R_A$ ist **Zertifikat** für $x \in A$.

P versus NP

Offenbar ist $\mathrm{P} \subseteq \mathrm{NP}$.

P versus NP

Offenbar ist P $\subseteq$ NP.

Andererseits: Probleme in NP in exponentieller Zeit lösbar:

P versus NP

Offenbar ist P $\subseteq$ NP.

Andererseits: Probleme in NP in exponentieller Zeit lösbar:

Ist R_A in Zeit $q(|x|, |z|)$ entscheidbar,

P versus NP

Offenbar ist P $\subseteq$ NP.

Andererseits: Probleme in NP in exponentieller Zeit lösbar:

Ist R_A in Zeit $q(|x|, |z|)$ entscheidbar,

und gilt $|z| \leq p(|x|)$ für Zertifikate z für $x \in A$:

P versus NP

Offenbar ist P $\subseteq$ NP.

Andererseits: Probleme in NP in exponentieller Zeit lösbar:

Ist R_A in Zeit $q(|x|, |z|)$ entscheidbar,

und gilt $|z| \leq p(|x|)$ für Zertifikate z für $x \in A$:

entscheide A durch Testen aller möglichen Zertifikate

P versus NP

Offenbar ist P $\subseteq$ NP.

Andererseits: Probleme in NP in exponentieller Zeit lösbar:

Ist R_A in Zeit $q(|x|, |z|)$ entscheidbar,

und gilt $|z| \le p(|x|)$ für Zertifikate z für $x \in A$:

entscheide A durch Testen aller möglichen Zertifikate

Zeit: $q(|x|, p(|x|))$

P versus NP

Offenbar ist P $\subseteq$ NP.

Andererseits: Probleme in NP in exponentieller Zeit lösbar:

Ist R_A in Zeit $q(|x|, |z|)$ entscheidbar,

und gilt $|z| \leq p(|x|)$ für Zertifikate z für $x \in A$:

entscheide A durch Testen aller möglichen Zertifikate

Zeit: $2^{p(|x|)} \cdot q(|x|, p(|x|))$

P versus NP

Offenbar ist $\mathrm{P} \subseteq \mathrm{NP}$.

Andererseits: Probleme in NP in exponentieller Zeit lösbar:

Ist R_A in Zeit $q(|x|, |z|)$ entscheidbar,

und gilt $|z| \leq p(|x|)$ für Zertifikate z für $x \in A$:

entscheide A durch Testen aller möglichen Zertifikate

Zeit: $2^{p(|x|)} \cdot q(|x|, p(|x|))$

Ist $\mathrm{P} = \mathrm{NP}$?

P versus NP

Offenbar ist P $\subseteq$ NP.

Andererseits: Probleme in NP in exponentieller Zeit lösbar:

Ist R_A in Zeit $q(|x|, |z|)$ entscheidbar,

und gilt $|z| \leq p(|x|)$ für Zertifikate z für $x \in A$:

entscheide A durch Testen aller möglichen Zertifikate

Zeit: $2^{p(|x|)} \cdot q(|x|, p(|x|))$

Ist P $=$ NP ?

- Das zentrale offene Problem der theoretischen Informatik!

P versus NP

Offenbar ist P $\subseteq$ NP.

Andererseits: Probleme in NP in exponentieller Zeit lösbar:

Ist R_A in Zeit $q(|x|, |z|)$ entscheidbar,

und gilt $|z| \leq p(|x|)$ für Zertifikate z für $x \in A$:

entscheide A durch Testen aller möglichen Zertifikate

Zeit: $\quad 2^{p(|x|)} \cdot q(|x|, p(|x|))$

Ist P $=$ NP ?

- Das zentrale offene Problem der theoretischen Informatik!
- Die Clay Foundation gibt einen Preis von \$ 1.000.000 für die Lösung (Millenium Prize).

Probleme in NP

Problem INDEPENDENT SET

Instanz:	Graph $G = (V, E)$, $k \in \mathbb{N}$
Frage:	Gibt es unabhängige Menge I mit $\|I\| \geq k$?

Probleme in NP

Problem INDEPENDENT SET

Instanz: Graph $G = (V, E)$, $k \in \mathbb{N}$
Frage: Gibt es unabhängige Menge I mit $|I| \geq k$?

unabhängige Menge: $I \subseteq V$ mit $\{x, y\} \notin E$ für alle $x, y \in I$

Probleme in NP

Problem INDEPENDENT SET

Instanz:	Graph $G = (V, E)$, $k \in \mathbb{N}$
Frage:	Gibt es unabhängige Menge I mit $\|I\| \geq k$?

unabhängige Menge: $I \subseteq V$ mit $\{x, y\} \notin E$ für alle $x, y \in I$

Problem VERTEX COVER

Instanz:	Graph $G = (V, E)$, $k \in \mathbb{N}$
Frage:	Gibt es vertex cover U mit $\|U\| \leq k$?

Probleme in NP

Problem INDEPENDENT SET

Instanz:	Graph $G = (V, E)$, $k \in \mathbb{N}$
Frage:	Gibt es unabhängige Menge I mit $\lvert I \rvert \geq k$?

unabhängige Menge: $I \subseteq V$ mit $\{x, y\} \notin E$ für alle $x, y \in I$

Problem VERTEX COVER

Instanz:	Graph $G = (V, E)$, $k \in \mathbb{N}$
Frage:	Gibt es vertex cover U mit $\lvert U \rvert \leq k$?

Vertex cover: $U \subseteq V$ mit $e \cap U \neq \emptyset$ für alle $e \in E$

Alternative Definition von NP

Definition durch nichtdeterministische Turing-Maschinen (NTM):

Alternative Definition von NP

Definition durch nichtdeterministische Turing-Maschinen (NTM):

Ein Problem A ist in der Klasse NP, wenn

- es eine NTM M gibt, die A entscheidet,

Alternative Definition von NP

Definition durch nichtdeterministische Turing-Maschinen (NTM):

Ein Problem A ist in der Klasse NP, wenn

- es eine NTM M gibt, die A entscheidet,
- jede Berechnung bei Eingabe w hält nach $p(|w|)$ Schritten, für ein Polynom $p()$.

Polynomielle Reduktion

Seien $A, B \subseteq \Sigma^*$.

Eine polynomielle Reduktion von A auf B ist eine Funktion $f : \Sigma^* \longrightarrow \Sigma^*$ die in polynomieller Zeit berechenbar ist, mit der Eigenschaft:

$$w \in A \;\Leftrightarrow\; f(w) \in B \qquad \text{für alle } w \in \Sigma^*$$

Polynomielle Reduktion

Seien $A, B \subseteq \Sigma^*$.

Eine polynomielle Reduktion von A auf B ist eine Funktion $f : \Sigma^* \longrightarrow \Sigma^*$ die in polynomieller Zeit berechenbar ist, mit der Eigenschaft:

$$w \in A \;\Leftrightarrow\; f(w) \in B \qquad \text{für alle } w \in \Sigma^*$$

Notation: $A \leq_P B$ falls es eine polynomielle Reduktion von A auf B gibt.

Polynomielle Reduktion

Seien $A, B \subseteq \Sigma^*$.

Eine polynomielle Reduktion von A auf B ist eine Funktion $f : \Sigma^* \longrightarrow \Sigma^*$ die in polynomieller Zeit berechenbar ist, mit der Eigenschaft:

$$w \in A \;\Leftrightarrow\; f(w) \in B \qquad \text{für alle } w \in \Sigma^*$$

Notation: $A \leq_P B$ falls es eine polynomielle Reduktion von A auf B gibt.

Eigenschaft:

Polynomielle Reduktion

Seien $A, B \subseteq \Sigma^*$.

Eine polynomielle Reduktion von A auf B ist eine Funktion $f : \Sigma^* \to \Sigma^*$ die in polynomieller Zeit berechenbar ist, mit der Eigenschaft:

$$w \in A \Leftrightarrow f(w) \in B \quad \text{für alle } w \in \Sigma^*$$

Notation: $A \leq_P B$ falls es eine polynomielle Reduktion von A auf B gibt.

Eigenschaft:

- Ist B in P und $A \leq_P B$, dann ist auch A in P.

Polynomielle Reduktion

Seien $A, B \subseteq \Sigma^*$.

Eine polynomielle Reduktion von A auf B ist eine Funktion $f : \Sigma^* \longrightarrow \Sigma^*$ die in polynomieller Zeit berechenbar ist, mit der Eigenschaft:

$$w \in A \;\Leftrightarrow\; f(w) \in B \qquad \text{für alle } w \in \Sigma^*$$

Notation: $A \leq_P B$ falls es eine polynomielle Reduktion von A auf B gibt.

Eigenschaft:

- Ist B in P und $A \leq_P B$, dann ist auch A in P.
- Ist B in NP und $A \leq_P B$, dann ist auch A in NP.

NP-vollständige Probleme

A ist NP-schwer, falls $B \leq_P A$ für alle B in NP ist.

NP-vollständige Probleme

A ist NP-schwer, falls $B \leq_P A$ für alle B in NP ist.

A ist NP-vollständig, falls A in NP und NP-schwer ist.

NP-vollständige Probleme

A ist NP-schwer, falls $B \leq_P A$ für alle B in NP ist.

A ist NP-vollständig, falls A in NP und NP-schwer ist.

Theorem

Ist A NP-vollständig, dann ist A in P genau dann, wenn $P = NP$.