11. Übung

26.06.13

P und NP

Modulklausur:

- 2 Termine: vor mündl. Prüfung: 2 schriftl. Versuche
- Anmeldung: QISPOS, bis 3 Tage vor Prüfung
  Vorr: Bachelor Student, CoMa I+II Schein eingetr.
  TAN-Liste,
  andere Studenten: Anmeldung bei Prüfungsamt
- Inhalt: VL, aller Stoff (Anwendungen, Beweise, kein Java code, Pseudocode)
- Zeit: 150 Minuten
- Material: Stifte, kein Papier, Taschenrechner, Buch ....

P und NP

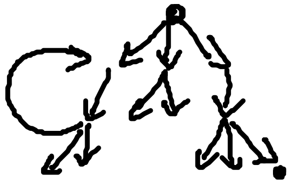
Entscheidungsproblemen: Problemklassen stellen Ja / Nein Fragen
Bsp: $\exists$ Clique mit $\geq k$ Elementen in Graph G?

Klasse P: Problem P' ist in P: es ex. determ. TM die jede Instanz von P' in polynom. Zeit bezgl. Eingabegröße entscheidet.

Bsp: Ist kürz. s-t Weg kürzer als l?
Eingabegrößen: Kanten, Knoten, s,t, Kantenlängen

Klasse NP: nichtdeterm. Turingmaschinen:
anstatt fester Übergangsfkt. δ gibt es Menge möglicher Übergänge als Relation
- NTM wählt einen möglichen Übergang aus

Akzeptanz: NTM ein Wort w akz. falls es eine Folge von Übergängen gibt, so dass die NTM in akzep. Zustand endet



• akzept. Zustand ⇒ NTM akzeptiert Wort w

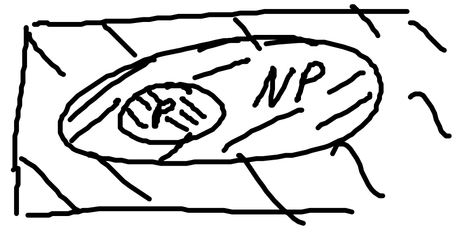
Laufzeit: Länge eines kürz. Pfades in akzept. Zustand

NP: (nichtdeterministisch polynomial) NICHT: nicht polynomial

Problem P' ist in NP: nichtdeterm. TM existiert, die jede Instanz von P' in Polynomialzeit entscheidet

Anschaulich: P: leichten Probleme

NP: leichten + schweren Probleme (aber entscheidbare)



äquivalente Def. für NP:

Problem $P' \in NP$: $\exists$ Zertifikat für Ja-Instanzen, das in Polynomialzeit prüfbar ist und die Ja-Antwort beweist. (Zertifikat hat Polyn. Länge)

Bsp: • kürzester s-t Weg $\leq l$? Zertifikat: • s-t Weg mit Länge $\leq k$
• oder leeres Zertifikat

• Clique mit $\geq k$ Elementen? Zert: Clique mit k Elementen

⇒ Probleme in NP: leicht Lösung zu verifizieren, finden vermutlich nicht

weitere Unterscheidungen:

$P' \in NP$	$P' \in NP\text{-}C$ (NP vollständig)	P' ist NP schwer
• NTM entsch. P' in Polynomialzeit • Clique, SAT • kürzeste Wege	- $P' \in NP$ - P' ist NP schwer • Clique, SAT → alle Probleme in NP über polyn. Reduktion auf Problem in NP-C lösbar	• P' ist min. so schwer wie jedes andere Probl. in NP • Probl. aus NP per polyn. Red. über P' lösbar – Clique, SAT – Halteproblem

Wichtigkeit von $P \neq NP$?:
- nahezu alle Optimierungsprobleme sind NP-vollständig
  $\Rightarrow \exists$ polyn. Algo.?
- Kryptographische Fragen
- scheinbar verifizieren leichter als lösen

<u>Reduktionen:</u> Ziel: zeig dass Problem NP vollst. ist

· zeige dass P' andere Probleme aus NP-C löst

$$\begin{tikzcd} \text{SAT} \arrow[r, "\text{polyn. Reduk.}"] & P' \arrow[d, "\text{löse}"] \\ \text{Lsg. von SAT} & \text{Lsg} \arrow[l, "\text{polyn. Red.}"] \end{tikzcd}$$

2. Typen:
- Ähnliche Probleme / Spezialfälle
- Gadgets (Konstrukte)

<u>Ähnliche Probleme:</u>

SAT $\Rightarrow$ 3SAT,

· Reduktion: Klauseln verlängern/verkürzen

$x_1 \vee x_2 \Rightarrow x_1 \vee x_2 \vee \bar{y}$
$\qquad\qquad\quad x_1 \vee x_2 \vee y$

$x_1 \vee x_2 \vee x_3 \vee x_4$

$\Rightarrow x_1 \vee x_2 \vee y$

$\quad \bar{y} \vee x_3 \vee x_4$

3SAT: Gegeben Var. x_i, $1 \leq i \leq n$
Clauseln C_i, $1 \leq i \leq m$
jede Clausel besitzt exakt 3 Literale

Frage: $\exists$ eine Belegung, s.d. in jeder Clausel min. 1 Literal erfüllt ist?

$x_1 \vee \bar{x}_2 \vee x_3$, $x_2 \vee x_3 \vee \bar{x}_4$

$\rightarrow$ Ja: $x_1 = true$
$\qquad\quad x_2 = true$

• unabhängige Mengen:

- Komplement $\bar{G}$:

$\bar{G} = (\bar{V}, \bar{E})$ mit $\bar{V} = V$
$\qquad\qquad\qquad \bar{E} = \{e \mid e \notin E\}$

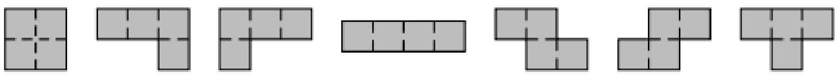
Gegeben: Graph $G(V,E)$, $k \in \mathbb{N}$

Frage: $\exists$ $U \subset V$ mit $|U| = k$
s.d. keine Kante zwischen Knoten aus U

⇒ Clique in G ist
unabh. Menge in $\overline{G}$

Konstruktionen / Gadgets:

Steine:
O J L I Z S T



Tetris-Clearance:

Gegeben: · gefülltes Feld mit Steinen
· Steinfolge

Frage: Kann ich das Tetrisfeld leeren.
Regel: Reihe verschwindet, sobald sie voll mit Steinen ist

Reduktion: 3Partition

Gegeben: A, $a_i \in \mathbb{N}$, $1 \leq i \leq n$

Frage: $\exists$ disj. Teilmengen $J_1, \dots, J_{n/3}$ mit

$$|J_i| = 3, \quad \bigcup_{i=1}^{n/3} J_i = A$$

$$\sum_{a \in J_i} a = \frac{\sum_{i=1}^{n} a_i}{n/3}$$

, gibt es 3er Mengen mit jeweils gleicher Summe?

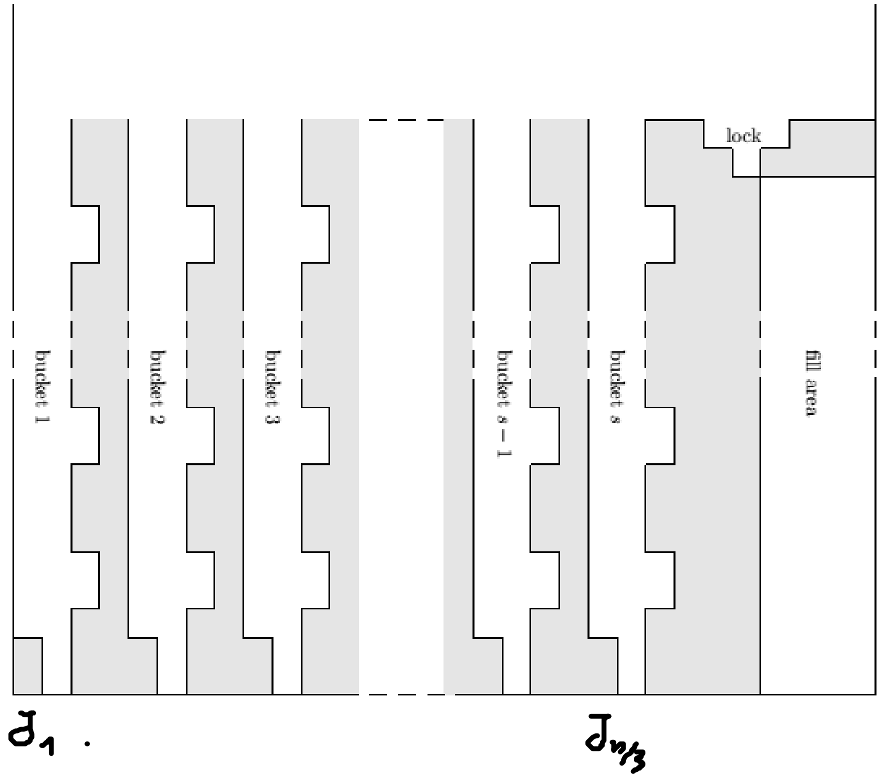
Bsp: 1, 2, 2, 2, 3, 3, 4, 6, 7

(7, 2, 1) (3, 3, 4) (6, 2, 2) $\Sigma = 10$

3Partition ist NP-vollst. ⇒ 3Part. auf Tetris Reduzieren

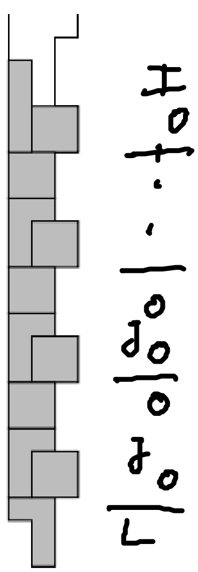
Instanz von Tetris:

Feld:



Ziel der Instanz: · buckets füllen, per Zahlen a_i mit gleicher Summe
· T stück löscht erste beiden Reihen
· Folge von I-Stücken löscht Rest

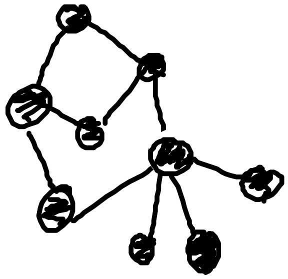
a_i als Steine: L, $\underbrace{OJO, OJO, \ldots, OJO}_{a_i\text{-mal}}$, OI



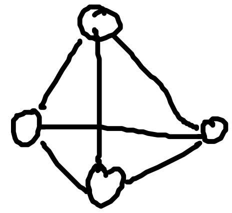
=> 3 Partition löscht Tetris Feld
rückwärts richtung schwerer

<u>weitere Reduktion:</u> 3 - Färbbarkeit:

Frage: kann man Knoten in Graph färben, so daß Knoten mit Kante dazw. versch. Farben besitzen, wenn es max. 3 Farben gibt?



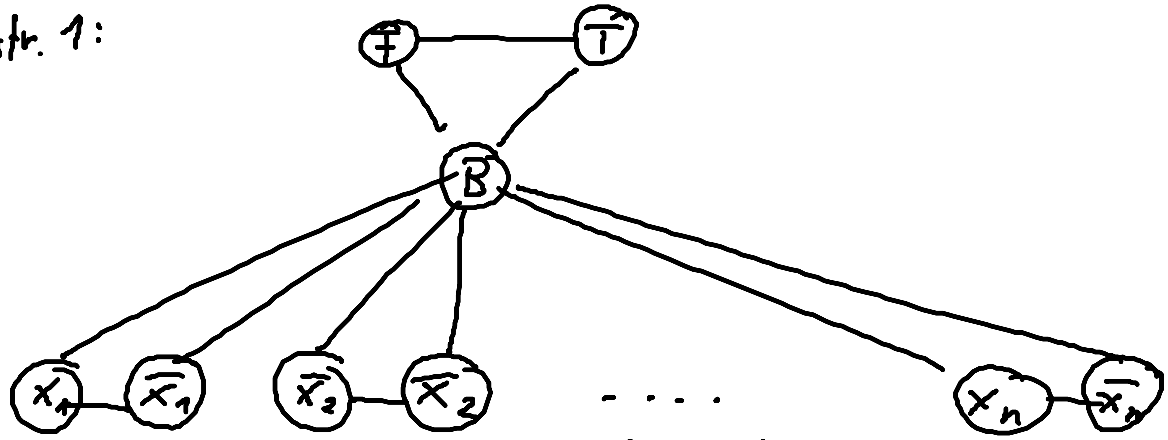
3 färbbar



nicht 3 färbbar

Reduktion: 3SAT → 3 Färbbarkeit

Konstr. 1:



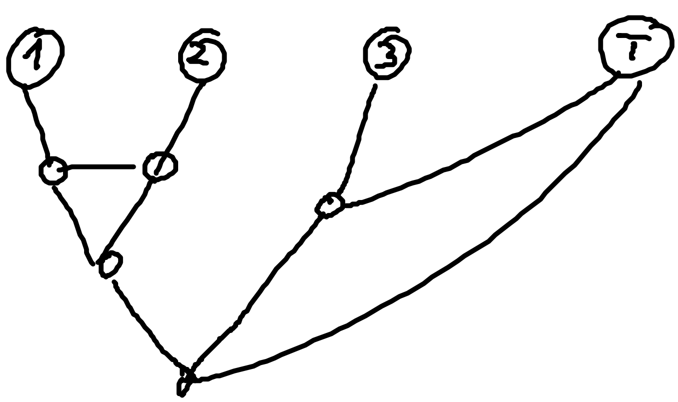
- Farbe von F heißt falsch
  T wahr

B = blank

$\Rightarrow$ x_i ist wahr/falsch gefärbt

x_i ist wahr gefärbt $\Rightarrow$ $\overline{x_i}$ falsch ist

<u>Konstrukt 2:</u> (Klausel Konstrukt)



- 1 und 2 und 3 falsch $\Rightarrow$ ∃ keine Färbung
- 1 oder 2 oder 3 wahr $\Rightarrow$ ∃ Färbung

<u>Beispiel:</u> $x_1 \vee x_2 \vee \overline{x_3}$, $\overline{x_2} \vee x_3 \vee \overline{x_4}$

als 3 Färbbarkeit