Formale Sprachen und Komplexitätstheorie

WS 2019/20

Robert Elsässer

Klasse NP

Definition

NP ist die Klasse der Sprachen, die polynomiell verifizierbar sind.

Satz

P ist eine Teilmenge von NP.

Millenium-Problem

Ist $P = NP$? (Clay Mathematics Institute)

Polynomielle Reduktion

Definition

Sei Σ ein Alphabet. Eine Funktion $f\colon \Sigma^* \to \Sigma^*$ heißt polynomiell berechenbar, wenn es eine DTM M mit polynomieller Laufzeit gibt, die f berechnet.

Definition

Seien A, B zwei Sprachen. A heißt auf B polynomiell reduzierbar, wenn es eine polynomiell berechenbare Funktion f gibt mit:

$$w \text{ in } A \Leftrightarrow f(w) \text{ in B}$$

Die Funktion f wird polynomielle Reduktion genannt und man schreibt

$$A \leq_P B$$

Polynomielle Reduktion – Eigenschaften

Satz

Seien A, B zwei Sprachen. Gilt $A \leq_P B$ und B ist in P, so ist auch A in P.

Lemma

Die Relation $\leq_P$ ist transitiv.

NP-Vollständigkeit

Definition

Eine Sprache L heißt NP-vollständig, wenn sie die folgenden Bedingungen erfüllt:

- L ist in NP
- Für jede Sprache L' aus NP gilt: $L' \leq_P L$

Satz

Ist L NP-vollständig und in P, so gilt $P = NP$.

Satz

Ist L in NP und gilt $L' \leq_P L$ für eine Sprache L', die NP-vollständig ist, so ist auch L NP-vollständig.

NP-Vollständigkeit

Satz von Cook-Levin

SAT ist NP-vollständig.

Satz von Cook-Levin

$3SAT$ ist NP-vollständig.

3. Komplexität

Definition

$Clique \coloneqq \{(G, k)\ G$ ist ein ungerichteter Graph mit einer $k-$Clique$\}$

Definition

$3SAT \coloneqq \{\varphi \mid \varphi$ ist eine erfüllbare 3−KNF Formel$\}$

NP-Vollständigkeit

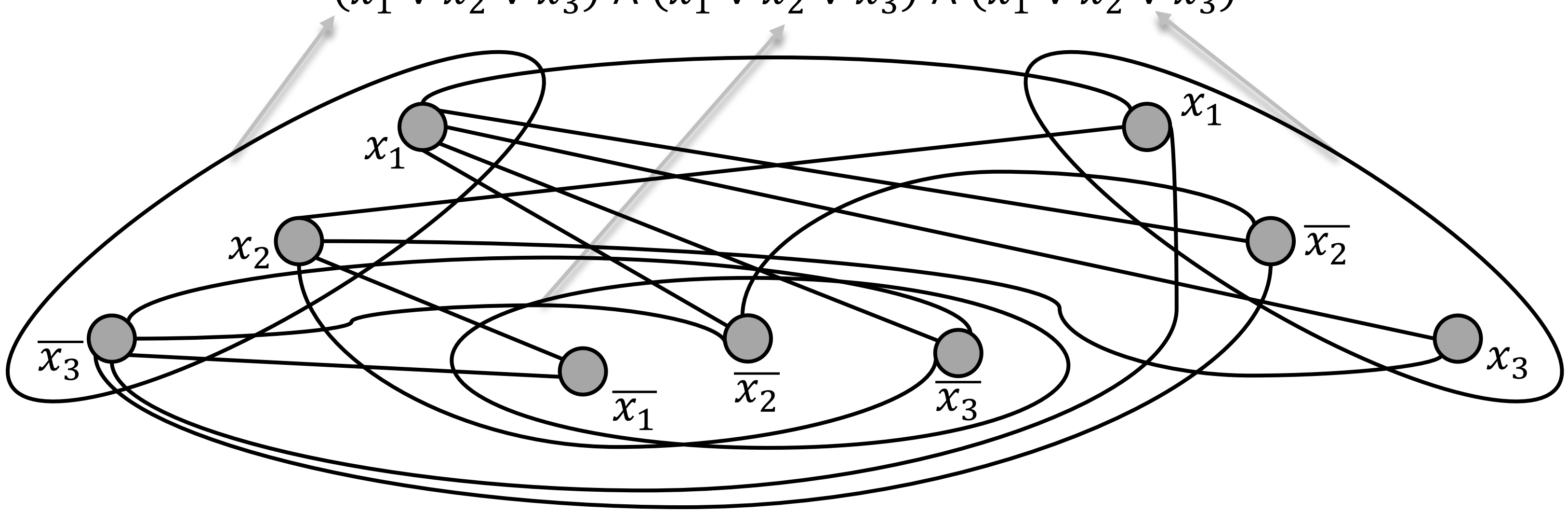
Satz

$Clique$ ist NP-vollständig.

Satz

$3SAT$ ist auf $Clique$ polynomiell reduzierbar.

$$(x_1 \vee x_2 \vee \overline{x_3}) \wedge (\overline{x_1} \vee \overline{x_2} \vee \overline{x_3}) \wedge (x_1 \vee \overline{x_2} \vee x_3)$$



NP-Vollständigkeit

Satz

$SubsetSum$ ist NP-vollständig.

$$SubsetSum \coloneqq \left\{ \begin{matrix} (S,t) \mid S = \{s_1, \dots, s_n\}, \text{wobei } s_1, \dots, s_n, t \text{ natürliche Zahlen} \\ \text{und es gibt eine Teilmenge } T \text{ aus } \{1, \dots, n\} \text{ mit } \sum_i s_i = t \end{matrix} \right\}$$

3. Komplexität

$$\varphi = (x_1 \vee x_2 \vee \overline{x_3}) \wedge (\overline{x_1} \vee x_2 \vee x_3)$$

	x_1	x_2	x_3	c_1	c_2
y_1	1	0	0	1	0
z_1	1	0	0	0	1
y_2	0	1	0	1	1
z_2	0	1	0	0	0
y_3	0	0	1	0	1
z_3	0	0	1	1	0
g_1	0	0	0	1	0
h_1	0	0	0	1	0
g_2	0	0	0	0	1
h_2	0	0	0	0	1
t	1	1	1	3	3

3. Komplexität

$$\varphi = (x_1 \vee x_2 \vee \overline{x_3}) \wedge (\overline{x_1} \vee x_2 \vee x_3)$$

	$\boldsymbol{x_1}$	$\boldsymbol{x_2}$	$\boldsymbol{x_3}$	$\boldsymbol{c_1}$	$\boldsymbol{c_2}$
y_1	1	0	0	1	0
z_1	1	0	0	0	1
y_2	0	1	0	1	1
z_2	0	1	0	0	0
y_3	0	0	1	0	1
z_3	0	0	1	1	0
g_1	0	0	0	1	0
h_1	0	0	0	1	0
g_2	0	0	0	0	1
h_2	0	0	0	0	1
t	1	1	1	3	3

$x_1 = 0$
$x_2 = 1$
$x_3 = 1$

Graphen und Knotenüberdeckung

Satz

Knotenüberdeckung ist NP-vollständig.

Definition

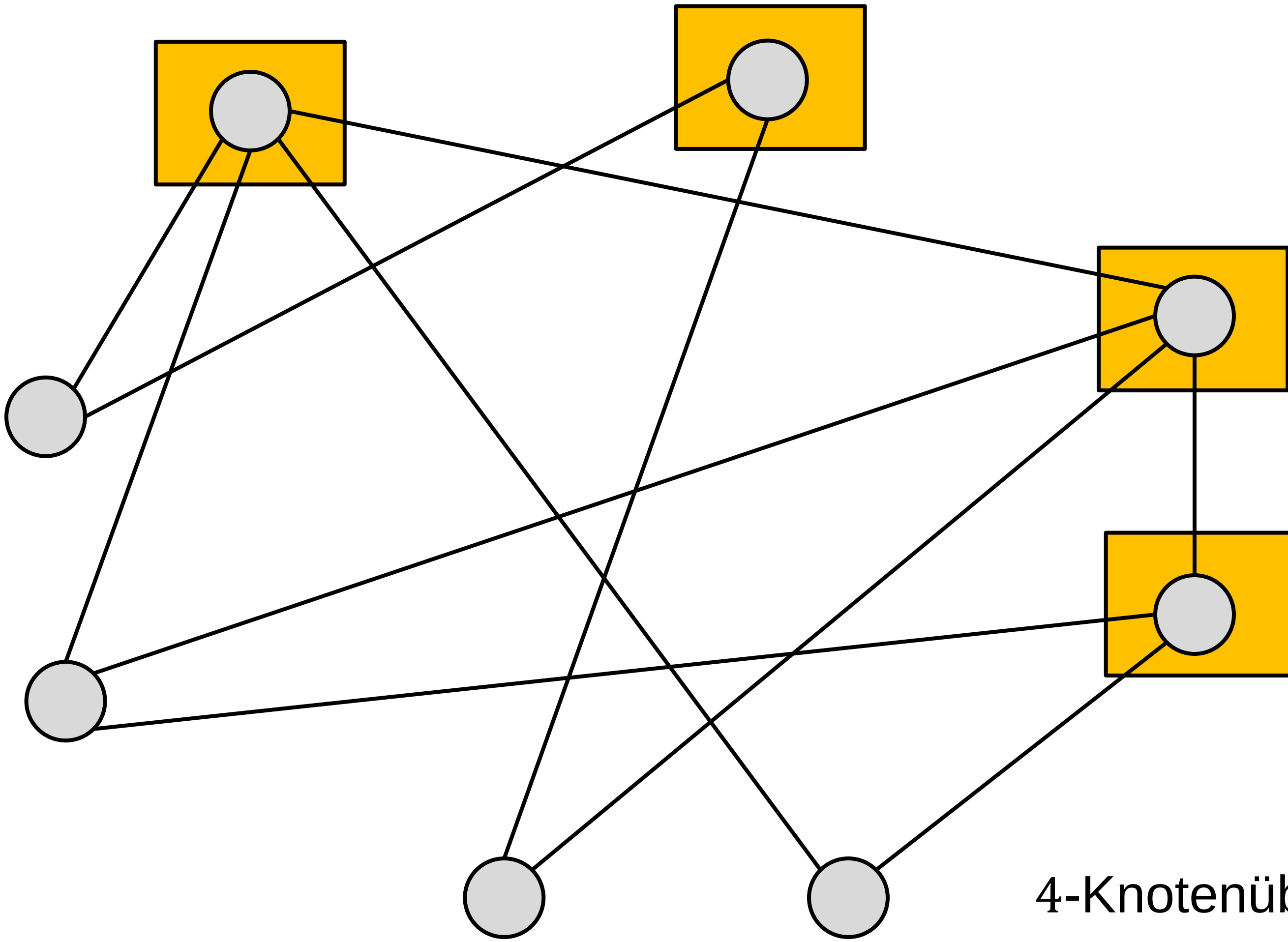
$G = (V, E)$ ist ein ungerichteter Graph.

Eine Teilmenge U von V heißt Knotenüberdeckung, wenn für alle Kanten $\{u, v\}$ aus E gilt $|\{u, v\} \cap U| \neq 0$.

U heißt k-Knotenüberdeckung, wenn U Knotenüberdeckung und $|U| = k$.

$$\text{Knotenüberdeckung} \coloneqq \{(G, k) \mid G \text{ besitzt eine } k\text{−Knotenüberdeckung}\}$$

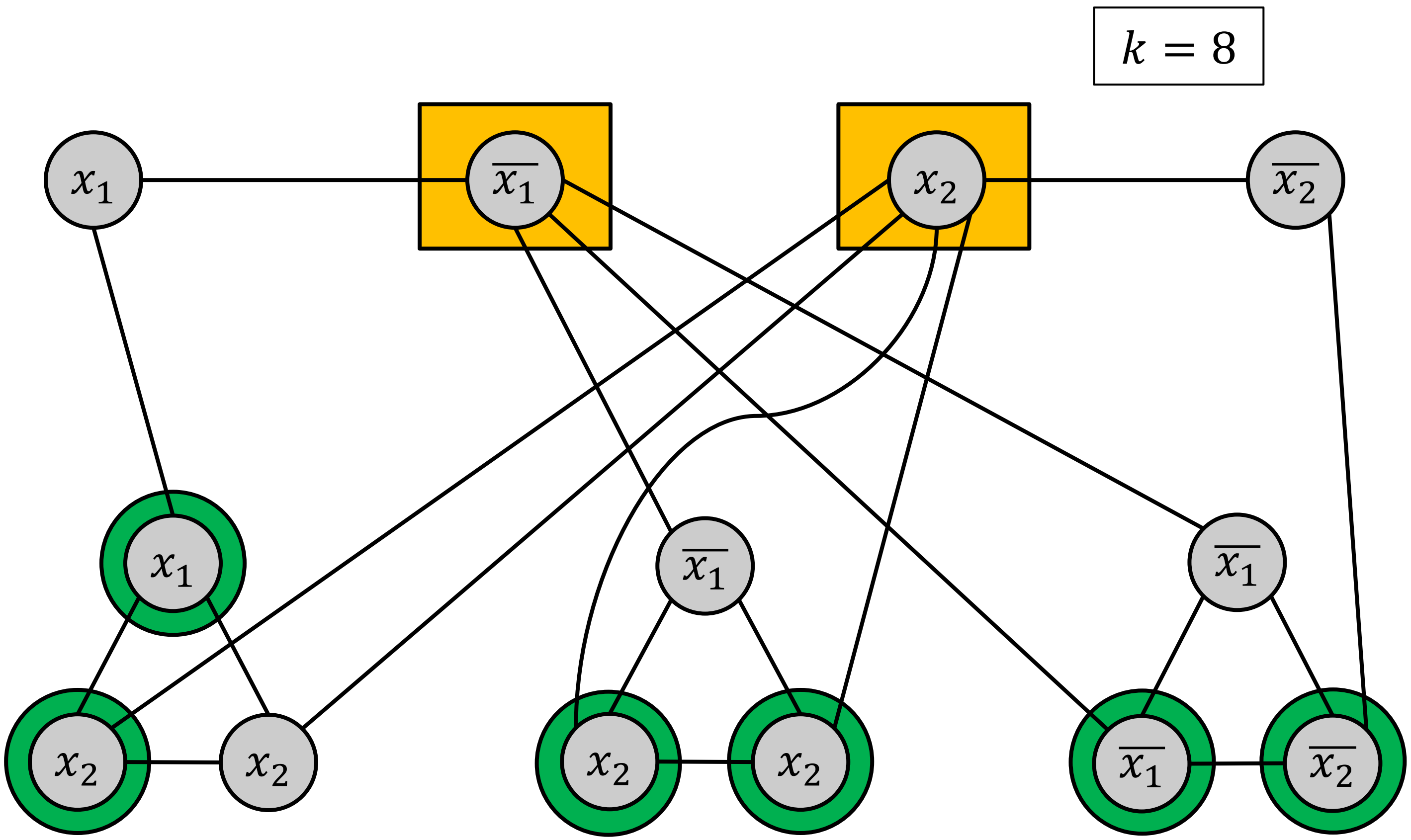
Knotenüberdeckung



4-Knotenüberdeckung

Reduktion $3SAT$ auf Knotenüberdeckung

$$\varphi = (x_1 \vee x_2 \vee x_2) \wedge (\overline{x_1} \vee x_2 \vee x_2) \wedge (\overline{x_1} \vee \overline{x_1} \vee \overline{x_2})$$



NP-Vollständigkeit

Satz

$SubsetSum$ ist polynomiell reduzierbar auf RS_{ent}.

Satz

RS_{ent} ist NP-vollständig.

Definition

$$RS_{ent} \coloneqq \left\{ \begin{array}{c} (G, W, g, w) \mid G = \{g_1, \dots, g_n\}, W = \{w_1, \dots, w_n\} \text{ und es gibt eine} \\ \text{Teilmenge } S \text{ aus } \{1, \dots, n\} \text{ mit } \sum_i g_i \leq g \text{ und } \sum_i w_i \geq w \end{array} \right\}$$