Gliederung

Erfüllbarkeitsproblem

SAT

Eingabe: aussagenlogische Formel F

Frage: Ist F **erfüllbar**, d.h. gibt es eine $\{0,1\}$-wertige Belegung der in F verwendeten Booleschen Variablen derart, dass F zu **wahr** (d.h. 1) ausgewertet wird?

Beispiele

$0, 1,$ $\quad x_1, x_2, \overline{x_3},$ $\quad (x_1 \wedge \overline{x_2}),$ $\quad (\overline{(x_1 \wedge \overline{x_2})} \vee x_2 \vee \overline{x_3})$

Theorem (Satz von Cook und Levin)

SAT ist NP-vollständig.

Beweis (Idee, Details später)

Teil 1: „SAT $\in$ NP“: rate erfüllende Belegung (Zertifikat) und verifiziere sie.

Teil 2: „SAT ist NP-schwer“: mit $L \in \mathrm{NP}$ beliebig,
transformiere NTM N mit $T(N) = L$ in Formel $\varphi(x)$ sodass $x \in L \Leftrightarrow \varphi(x) \in$ SAT.

CNF-SAT ist NP-vollständig

CNF-SAT

Eingabe: aussagenlogische Formel F in „konjunktiver Normalform"

Frage: Ist F **erfüllbar**, d.h. gibt es eine $\{0,1\}$-wertige Belegung der in F verwendeten Booleschen Variablen derart, dass F zu **wahr** (d.h. 1) ausgewertet wird?

Theorem

$\mathrm{SAT} \leq_m^p \mathrm{CNF\text{-}SAT}$ ($\rightsquigarrow$ $\mathrm{CNF\text{-}SAT}$ NP-vollständig)

Beweis (Skizze)

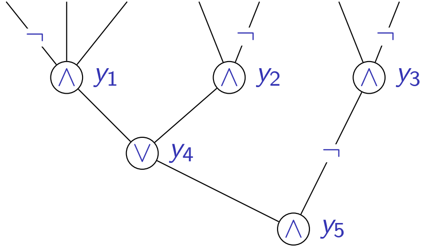
Reduktion: $\varphi \rightsquigarrow$ **erfüllbarkeits**-äquivalente Formel ψ:
(1) neue Variable y_i für jeden Knoten im "Formelbaum" mit "äquivalentem Wahrheitswert"
(2) neue Klausel für die Wurzel

ψ erfüllbar $\Leftrightarrow$ φ erfüllbar ✓

poly-time computable ✓ (ab jetzt implizit)

Beispiel

$((\overline{x_1} \land x_2 \land x_1) \lor (x_1 \land \overline{x_3})) \land \overline{(x_1 \land \overline{x_2})}$



3-SAT ist NP-vollständig

Theorem

CNF-SAT $\leq_m^p$ 3-SAT (also ist 3-SAT NP-vollständig).

Beweis (Skizze)

Reduktion: CNF-Formel $\varphi \rightsquigarrow$ **erfüllbarkeits**-äquivalente 3CNF-Formel ψ

Für jede Klausel $c_j = (\ell_1 \vee \ell_2 \vee \ldots \vee \ell_r) \in \varphi$,

- falls $r \leq 3$, dann füge c_j zu ψ hinzu;
- sonst füge c_j' hinzu mit

$$c_j' := (\ell_1 \vee \ell_2 \vee y_1) \wedge (\overline{y_1} \vee \ell_3 \vee y_2) \wedge (\overline{y_2} \vee \ell_4 \vee y_3) \ldots (\overline{y_{r-3}} \vee \ell_{r-1} \vee \ell_r)$$

wobei $y_1, \ldots, y_{r-3}$ neue Variablen sind.

$\rightsquigarrow$ Belegung β erfüllt $c_j \Leftrightarrow$ Erweiterung von β erfüllt c_j'

ψ erfüllbar $\Leftrightarrow$ φ erfüllbar ✓

Bemerkung: $|\psi| \leq 2|\varphi|$

Vertex Cover ist NP-vollständig

Theorem

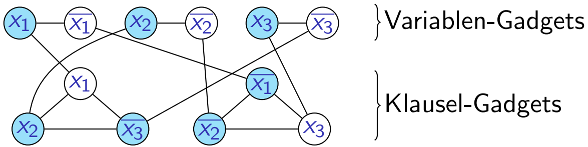
3-SAT $\leq_m^p$ Vertex Cover.

Beweis (Skizze)

Formel $\varphi \rightsquigarrow (G, k = \#\text{Var} + 2\#\text{Klauseln})$

1. Variablen-Gadget: Variable $x_i \rightsquigarrow$ 2 benachbarte Knoten mit Beschriftungen x_i und $\overline{x_i}$
2. Klausel-Gadget: Klausel $(\ell_{i_1} \vee \ell_{i_2} \vee \ell_{i_3}) \rightsquigarrow$ Dreieck mit Beschriftungen $\ell_{i_1}, \ell_{i_2}, \ell_{i_3}$
3. Verbinde Knoten mit gleicher Beschriftung

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



„$\Rightarrow$“: aus Variablen-Gadget, wähle entsprechend der Belegung

$\rightsquigarrow$ alle anderen Kanten mit 2 Knoten aus jedem Klausel-Gadget überdeckt

„$\Leftarrow$“:

(a) $= 1$ Knoten von jedem Variablen-Gadget in jeder VC-Lösung

(b) $= 2$ Knoten von jedem Klausel-Gadget in jeder VC-Lösung.

$\rightsquigarrow$ jedes Klausel-Gadget benachbart zu einem Knoten in VC-Lösung

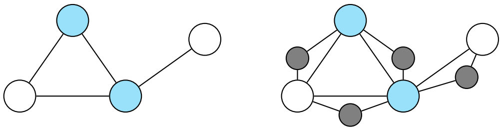
$\rightsquigarrow$ entsprechende Belegung erfüllt die Formel!

DOMINATING SET ist NP-vollständig

Theorem

VERTEX COVER $\leq_m^p$ DOMINATING SET.

Beispiel



Beweis (Skizze)

$(G, k) \leadsto (G', k)$

1. setze initial $G' = G$
2. für jede Kante $e = \{u, v\}$ in G:

   erzeuge einen neuen (grauen) Knoten in G' und verbinde ihn mit u und v

Korrektheit: „$\Rightarrow$“: VC-Lösung in G ist auch DS-Lösung in G'

„$\Leftarrow$“: Sei $X \subseteq V(G')$ eine DS-Lösung für G' mit $|X| \leq k$

(a) neuer (grauer) Knoten $\in$ DS-Lösung $\leadsto$ mit weißem Nachbarn tauschen

$\leadsto$ Lösung ohne graue Knoten

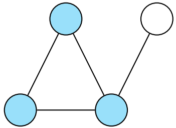
(b) graue Knoten dominiert $\leadsto$ jede Kante in G hat Endpunkt in X

$\leadsto$ X ist vertex cover in G

Clique ist NP-vollständig

Clique
Eingabe: ungerichteter Graph G und Zahl $k \in \mathbb{N}$
Frage: Hat G einen vollständigen Teilgraph G' mit $\geq k$ Knoten?

Beispiel



$k = 3$

Theorem

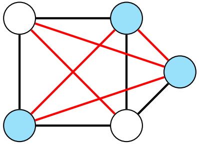
Independent Set $\leq_m^p$ Clique.

Beweis (Skizze)

$(G = (V, E), k) \rightsquigarrow (\overline{G} = (V, \binom{V}{2} \setminus E), k)$

Korrektheit:
Jede unabhängige Knotenmenge in G
bildet eine Clique in $\overline{G}$ und umgekehrt, also:
$(G, k) \in$ Independent Set $\Leftrightarrow (\overline{G}, k) \in$ Clique

Beispiel



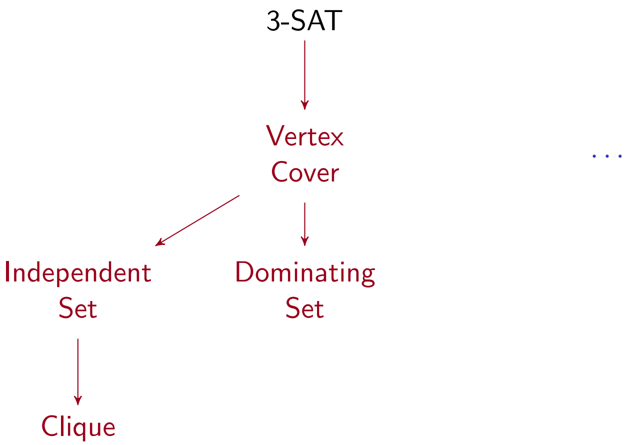
$k = 3$

Independent Set
Clique

Wenn ein Dominostein fiele...

Quelle: pixabay.com/en/mikado-domino-stones-pay-steinchen-1013878/

Netzwerk polynomieller Reduktionen I



Hitting Set und Set Cover

Eingabe:

(1) Grundmenge („Universum“) $U := \{x_1, x_2, \ldots, x_n\}$,
(2) eine Teilmengenfamilie $\mathcal{F} := \{S_1, S_2, \ldots, S_m\}$ mit $S_i \subseteq U$ für $1 \leq i \leq n$ und
(3) ein $k \in \mathbb{N}$

Hitting Set

Frage: Existiert eine Teilmenge $X \subseteq U$ mit $|X| \leq k$ und $X \cap S_i \neq \emptyset$ für jedes S_i?

Set Cover

Frage: Existiert ein $\mathcal{Z} \subseteq \mathcal{F}$ mit $|\mathcal{Z}| \leq k$ und $\bigcup_{S \in \mathcal{Z}} S = U$?

Beispiel

(1) $U = \{1, 2, 3, 4, 5, 6\}$,
(2) $S_1 = \{1, 3\}$, $S_2 = \{3, 4\}$, $S_3 = \{1, 5\}$, $S_4 = \{2, 4, 6\}$, $S_5 = \{1, 3, 5\}$
(3) $k = 2$

$\rightsquigarrow X = \{1, 4\}$, $\mathcal{Z} = \{S_4, S_5\}$.

Hitting Set ist NP-vollständig

Theorem

Vertex Cover $\leq_m^p$ Hitting Set.

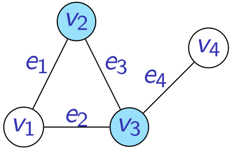
Beweis (Skizze)

$(G = (V, E), k) \rightsquigarrow (U = V, \mathcal{F} = E, k)$

Korrektheit: klar

In der Tat ist Vertex Cover auch bekannt als „2-Hitting Set“.

Beispiel



$k = 2$

$U = \{v_1, v_2, v_3, v_4\}$
$\mathcal{F} = \{\{v_1, v_2\}, \{v_1, v_3\}, \{v_2, v_3\}, \{v_3, v_4\}\}$

Set Cover ist NP-vollständig

Theorem

Hitting Set $\leq_m^p$ Set Cover.

Beweis (Skizze)

$(U, \mathcal{F}, k) \leadsto (U_{SC} = \mathcal{F}, \mathcal{F}_{SC} = \{F_x \mid x \in U\}, k)$
mit $F_x := \{S_i \in \mathcal{F} \mid x \in S_i\}$

Korrektheit:

$X \subseteq U$ ist ein Hitting Set für $\mathcal{F}$

$\Leftrightarrow \forall_{S_i \in \mathcal{F}} \exists_{x \in X}\ x \in S_i$

$\Leftrightarrow \bigcup_{x \in X} F_x = \mathcal{F}$

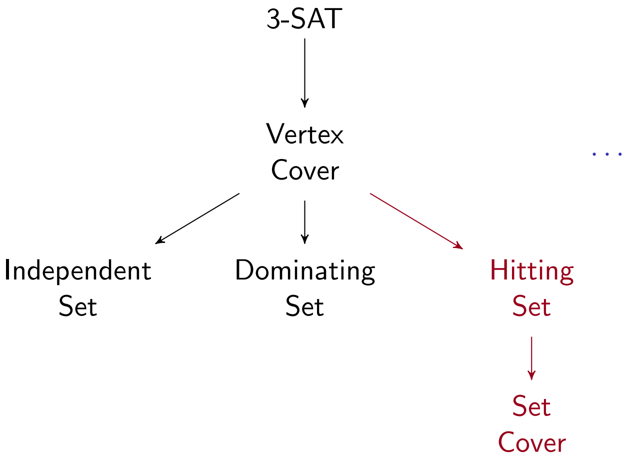
$\Leftrightarrow \mathcal{Z} := \{F_x \mid x \in X\}$ ist ein Set Cover für $\mathcal{F} = U_{SC}$

HS/SC Dualität

$\mathcal{F} \setminus U$	1	2	3	4
$\{1,2\}$	■	■		
$\{1,4\}$	■			■
$\{2,3,4\}$		■	■	■

$\mathcal{F}_{SC} \setminus \mathcal{F}$	$\{1,2\}$	$\{1,4\}$	$\{2,3,4\}$
$F_1 1$	■	■	
$F_2 2$	■		■
$F_3 3$			■
$F_4 4$		■	■

Netzwerk polynomieller Reduktionen II



Subset Sum

Ein Problem u.a. aus dem Bereich „Scheduling“ (Ablaufsteuerung).

Subset Sum

Eingabe: Multi-Menge $U := \{u_1, u_2, \ldots, u_n\}$ von natürlichen Zahlen und eine Zahl $B \in \mathbb{N}$

Frage: Existiert eine Teilmenge $X \subseteq U$, die sich zu B summiert, d.h. $\sum_{u \in X} u = B$?

Beispiel

$U = \{4, 4, 11, 16, 21\}$ und $B = 29$.

$\rightsquigarrow X = \{4, 4, 21\}$.

SUBSET SUM ist NP-vollständig

Theorem

3-SAT $\leq_m^p$ SUBSET SUM.

Beweis (Skizze)

Konstruktion: Variablen $x_1, \dots, x_n$, Klauseln $c_1, \dots, c_m$

1. Für jedes x_i bilde zwei Dezimalzahlen $y_i, z_i \in \{0,1\}^{n+m}$ mit:
   Vordere n Ziffern: i-te Stelle von y_i und z_i ist 1, alle anderen sind 0.
   Hintere m Ziffern: j-te Stelle von y_i ist 1 falls $x_i \in c_j$, und sonst 0.
   j-te Stelle von z_i ist 1 falls $\overline{x_i} \in c_j$, und sonst 0.
2. Für jede Klausel c_j, bilde zwei **dezimale** „Füllzahlen“ g_j, h_j
3. Setze Dezimalzahl $B := \underbrace{1\dots1}_{n}\underbrace{3\dots3}_{m}$.

Korrektheit „$\Rightarrow$“: Sei β eine erfüllende Belegung.
$\rightsquigarrow$ Lösung $= \{y_i \mid \beta(x_i) = 1\} \cup \{z_i \mid \beta(x_i) = 0\}$ + geeignete g_i & h_i
„$\Leftarrow$“: Sei X eine Menge von Zahlen mit $\sum_{u \in X} u = B$.
erste n Ziffern $\rightsquigarrow y_i \in X \Leftrightarrow z_i \notin X$
Die Belegung β mit $\beta(x_i) = 1$ falls $y_i \in X$, und $\beta(x_i) = 0$ sonst, ist erfüllend.

Beispiel

$c_1 : x_1 \vee x_2 \vee \overline{x_3}$

$c_2 : \overline{x_1} \vee x_2 \vee x_3$

$c_3 : \overline{x_1} \vee \overline{x_2} \vee \overline{x_3}$

	x_1	x_2	x_3	c_1	c_2	c_3
y_1:	1	0	0	1	0	0
z_1:	1	0	0	0	1	1
y_2:	0	1	0	1	1	0
z_2:	0	1	0	0	0	1
y_3:	0	0	1	0	1	0
z_3:	0	0	1	1	0	1
g_1:	0	0	0	1	0	0
h_1:	0	0	0	1	0	0
g_2:	0	0	0	0	1	0
h_2:	0	0	0	0	1	0
g_3:	0	0	0	0	0	1
h_3:	0	0	0	0	0	1
B:	1	1	1	3	3	3

Netzwerk polynomieller Reduktionen III