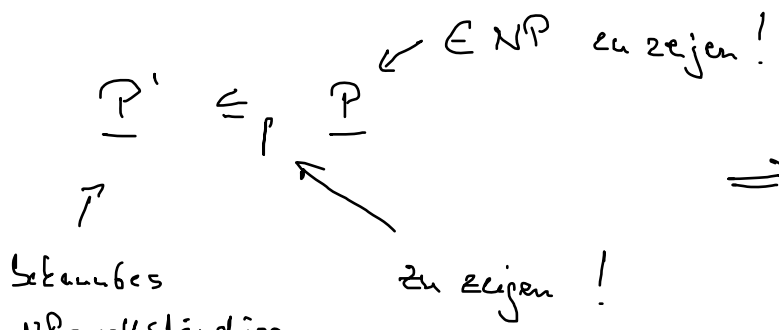
4.3 Weitere NP-vollständige Probleme

Im Folgenden stellen wir eine kleine Auswahl NP-vollständiger Probleme vor. Das generelle Argumentationsschema, um nachzuweisen, dass ein Entscheidungsproblem P in NPC (= Klasse der NP-vollständigen Probleme) liegt ist wie folgt:



$\Rightarrow$ P NP vollständig:

P ist in NP und P ist NP-hart, denn für jedes $P'' \in NP$ gilt $P'' \leq_p P'$ und wg Transitivität von $\leq_p$ also $P'' \leq_p P$.

Laut Wikipedia mehr als 3000 NP-vollständige Probleme bekannt.

Buchempfehlung:

M. Garey u. D. Johnson: Computers and Intractability, 1979.

Appendix enthält Liste von ca 300 Problemen

3 CNF-SAT

Gegeben: Eine aussagenlogische Formel F in konjunktiver Normalform, d.d. jedes Konjunktionsglied ("Klausel") aus höchstens 3 Literalen besteht.

Gefragt: Ist F erfüllbar?

Satz: 3 CNF-SAT ist NP-vollständig.

Beweis: 3 CNF-SAT ist in NP, weil Spezialfall von SAT

Es bleibt zu zeigen: $SAT \leq_p$ 3 CNF-SAT

Erste Idee: Wandle F in CNF um.

Aber: * Umwandlung i.a. zu exponentiell langen Formeln führt (vs. zeige polynomielle Reduktion

* .. und resultiert i.a. nicht in 3CNF-Form

Klausel

$F = (\ell_{11} \vee \ell_{12} \vee \ell_{13}) \wedge \dots$

$\wedge (\ell_{m1} \vee \ell_{m2} \vee \ell_{m3})$

Literale

$\ell_{ij} \in \{x_i : 1 \leq i \leq n\} \cup \{\neg x_i : 1 \leq i \leq n\}$

$V(F) = \{x_1, \dots, x_n\}$

d.h.: in F besteht jede Klausel aus genau 3 Literalen bestehend.

2 CNF-SAT in P

3 CNF-SAT:

$F = \bigvee_{i=1}^{m} \bigwedge_{k=1}^{n_i} \ell_{ik}$

$\in P$

Hierzu ist es nicht nötig, einer SAT-Instanz F eine äquivalente 3CNF-SAT-Instanz F' zuzuordnen.

Es reicht, dass F und F' erfüllbarkeitsäquivalent sind, d.h. dass gilt:

$$F \text{ erfüllbar} \iff F' \text{ erfüllbar}.$$

Gehe wie folgt vor:

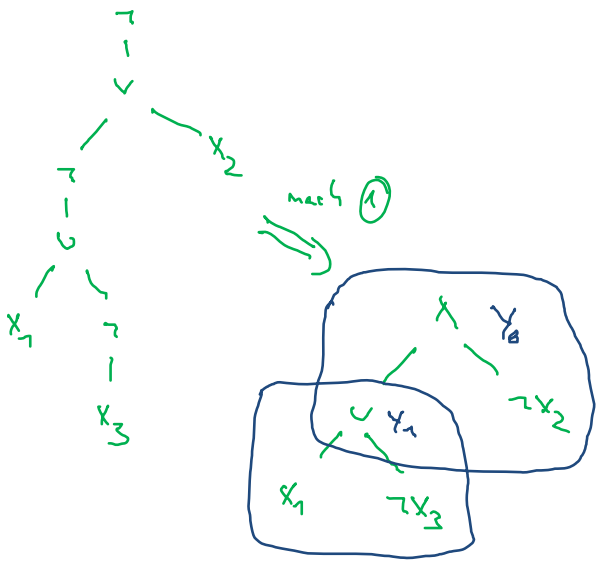
(1) Überführe F in NNF (Negationszeichen kommt nur unmittelbar vor Satzvariablen vor; de Morgan'sche Regeln). Umwandlung in $O(|F|)$ $\Rightarrow$ F^1

(2) Es sei $\mathrm{Sub}^{\wedge\vee}(F^1) \subseteq \mathrm{Sub}(F^1)$ die Menge der Teilformeln von F^1 der Gestalt $F_1 \wedge F_2$ oder $F_1 \vee F_2$; davon gibt es höchstens $O(|F^1|)$ viele. Für jedes $G \in \mathrm{Sub}^{\wedge\vee}(F^1)$ sei y_G eine neue Variable. Ist $G \in \mathrm{Sub}(F^1)$ ein Literal, so bezeichne y_G einfach G.

Definiere

$$F^2 = y_{F_1} \wedge \bigwedge_{\substack{G \in \mathrm{Sub}^{\wedge\vee}(F^1) \\ G = G_1 \circ G_2,\ \circ \in \{\wedge,\vee\}}} (y_G \leftrightarrow y_{G_1} \circ y_{G_2})$$

Beispiel: $F = \neg(\neg(x_1 \vee \neg x_3) \vee x_2)$



$$F^2 = y_0 \wedge (y_0 \leftrightarrow y_1 \wedge \neg x_2) \wedge (y_1 \leftrightarrow x_1 \vee \neg x_3)$$

Offenbar sind F^1 und F^2 erfüllbarkeitsäquivalent:

ist $\alpha^1 : V(F^1) \to \{0,1\}$ eine Belegung mit $\alpha \models F^1$

so ist $\alpha^2 : V(F^1) \cup \{Y_G : G \in Sub^{AV}(F^1)\} \to \{0,1\}$

mit $\alpha^2|_{V(F^1)} = \alpha^1$ und $\alpha^2(Y_G) = 1 \iff \alpha^1 \models G$

mit $\alpha^2 \models F^2$, Umkehrung trivial.

(3) In F^2 wandle jede Formel der Gestalt $Y_G \leftrightarrow Y_{G_1} \circ_G Y_{G_2}$ in CNF um mit Verwendung der folgenden Regeln:

$$a \leftrightarrow b \vee c \quad \equiv \quad (a \vee \neg b) \wedge (a \vee \neg c) \wedge (\neg a \vee b \vee c)$$

$$a \leftrightarrow b \wedge c \quad \equiv \quad (\neg a \vee b) \wedge (\neg a \vee c) \wedge (a \vee \neg b \vee \neg c)$$

$\neg(b \wedge c)$

Diese Umformung nur 1-mal pro Teilformel in $Sub^{AV}(F^1)$

$\Rightarrow$ $G(|F^2|)$

Insgesamt erhalten wir also

$$SAT \leq_p 3CNF\text{-}SAT$$

$\square$

$\Downarrow$ nach (3)

$F^3 = Y_0 \wedge (\neg Y_0 \vee Y_2)$

$\wedge (\neg Y_0 \vee \neg X_2)$

$\wedge (Y_0 \vee \neg Y_1 \vee X_2)$

$\wedge (Y_1 \vee \neg X_1)$

$\wedge (Y_1 \vee X_3)$

$\wedge (\neg Y_1 \vee X_1 \vee \neg X_3)$

3CNF

SETCOVER:

Gegeben: Eine endliche Menge M, ein Mengensystem

$$\mathcal{T} = \{T_1, \dots, T_t\} \subseteq 2^M$$

und eine natürliche Zahl $u \leq t$.

Gefragt: Gibt es $\{i_1, \dots, i_u\} \subseteq \{1, \dots, t\}$ mit

$$T_{i_1} \cup \dots \cup T_{i_u} = M \; ?$$

Satz: SETCOVER ist NP-vollständig.

Beweis: SETCOVER ist in NP, da "raten" von $i_1, \dots, i_u$ und prüfen, ob $M = T_{i_1} \cup \dots \cup T_{i_u}$ gilt. ($\mathcal{O}(u \cdot |M|^2)$)

Wir wollen zeigen: 3KNF-SAT $\leq_p$ SETCOVER

Sei dazu $F = K_1 \wedge \dots \wedge K_m$ eine 3KNF-Formel mit m Klauseln und Variablen $V(F) = \{x_1, \dots, x_n\}$.

P NP-äquivalent, falls P NP-leicht und NP-schwer ist.

Ziele: Entscheidungsprobleme

Praktisch wichtiger: Suchprobleme

Suchprobleme: "Gegeben / Gesucht"

Suchprobleme lasse sich auf Entscheidungsprobleme reduzieren ("Turing"-Reduktion).

Orakel-TM:

* Orakel-Band
* z_q, z_a
* Anfrage in $G(\dots)$

$P \leq_T P' \Leftrightarrow$ es gibt eine OTM die P in polynomieller Zeit berechnet und dabei ein Orakel für das Problem P' benutzt (ggf. polynomiell oft)

$\leq_p \Rightarrow \leq_T \Rightarrow \leq$

P ist NP-leicht, falls $P \leq_T P'$ mit $P' \in NP$

P ist NP-schwer, falls es ein $P' \in NPC$ $P' \leq_T P$.

Betrachte zu F die folgende SET COVER-Instanz:

$$M_F := \{1, \dots, m, m+1, \dots, m+n\}$$

$$T_i := \{ j \in [1,m] : x_i \text{ kommt in } K_j \text{ negiert vor} \} \cup \{m+i\}$$

$$T_i' := \{ j \in [1,m] : x_i \text{ kommt in } K_j \text{ negiert vor} \} \cup \{m+i\}$$

$$\mathcal{T}_F := \{ T_i : 1 \le i \le n \} \cup \{ T_i' : 1 \le i \le n \}$$

$$n_F := n$$

Zu zeigen: F ist erfüllbar $\Leftrightarrow$

$$\exists\, \mathcal{T} \subseteq \mathcal{T}_F \text{ mit } |\mathcal{T}| = n_F \text{ und } \bigcup \mathcal{T} = M_F.$$

„$\Rightarrow$" Es sei $\alpha : V(F) \to \{0,1\}$ eine Belegung mit $\alpha \models F$, d.h. $\alpha \models K_j$ für alle $1 \le j \le m$. Definiere $T_i^\alpha := T_i$ falls $\alpha(x_i) = 1$ und $T_i^\alpha = T_i'$, sonst. $\mathcal{T} := \{T_i^\alpha : 1 \le i \le n\}$. $|\mathcal{T}| = n = n_F$.

„$\Leftarrow$" Umgekehrt.

z.z. $\bigcup \mathcal{T} = M_F$. „$\subseteq$" gilt trivialerweise. „$\supseteq$" für $m' \ge m+1, \in m+n$. Dann gilt $m' = m+i$ für geeignetes i. $\mathcal{T}$ enthält T_i oder T_i'. Also $m' \in \bigcup \mathcal{T}$. Für jedes $j \in \{1, \dots, m\}$ gilt $\alpha \models K_j$ auch $\alpha \models K_i$ für eine Variable x_i, die in K_j negiert vorkommt. Oder $\alpha \models \neg x_i$ für eine Variable x_i, die in K_j negiert vorkommt. Also $j \in T_i$ oder $j \in T_i'$ $\Rightarrow j \in T_i^\alpha \Rightarrow j \in \bigcup \mathcal{T}$

„⇐" Sei nun $\mathcal{T} \subseteq \mathcal{T}_F$ mit $|\mathcal{T}| = n$ und $\bigcup \mathcal{T} = \eta_F$.

Für jedes $1 \leq i \leq n$ gibt es dann ein $X_i \in \mathcal{T}$ mit $x_i \in X_i$.

Weil $\mathcal{T}$ nur n-viele Teilmengen enthält, muss X_i entweder T_i oder T_i' sein. Definiere nun eine Belegung $\alpha : V(F) \to \{0,1\}$:

$$\alpha(x_i) := \begin{cases} 1 & \text{falls } X_i = T_i \\ 0 & \text{falls } X_i = T_i' \end{cases}$$

Für jedes $1 \leq j \leq n$ gilt dann: $\alpha \vDash K_j$, denn:

Wegen $j \in \Pi \subseteq \bigcup \mathcal{T}$ gibt es ein $X \in \mathcal{T}$ mit $j \in X$.

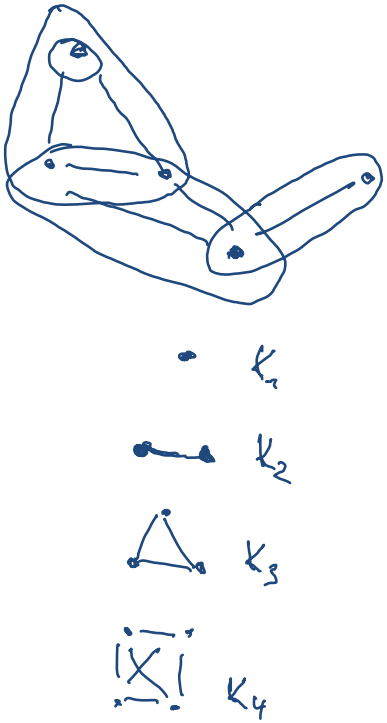
Ist $X = T_i$, so gilt: x_i kommt in K_j unnegiert vor und $\alpha(x_i) = 1$, also $\alpha \vDash K_j$.

Ist $X = T_i'$, so kommt x_i in K_j negiert vor und $\alpha(x_i) = 0$, also $\alpha(\neg x_i) = 1$, also $\alpha \vDash K_j$.

CLIQUE:

Gegeben: Ein ungerichteter Graph $G = (V, E)$ und eine natürliche Zahl $k \in \mathbb{N}$

Gefragt: Besitzt G eine Clique der Größe $\geq k$.



Definition: Eine Teilmenge $V' \subseteq V$ heißt eine Clique von G, falls für alle $u, v \in V'$ mit $u \neq v$ gilt $\{u, v\} \in E$.

Satz: CLIQUE ist NP-vollständig.

Beweis: Wir zeigen 3SAT $\leq_p$ CLIQUE

Betrachte eine 3SAT-Instanz F

$$F = (l_{11} \vee l_{12} \vee l_{13}) \wedge \dots \wedge (l_{m1} \vee l_{m2} \vee l_{m3})$$

mit $l_{ij} \in \{x_1, \dots, x_n\} \cup \{\neg x_1, \dots, \neg x_n\}$.

Betrachte dazu $G_F = \langle V_F, E_F \rangle$:

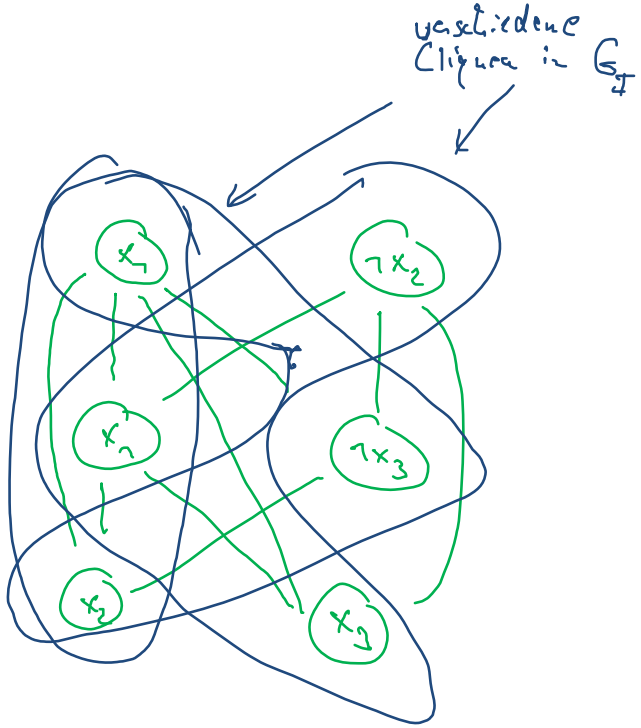
$$V_F := \{ (1,1), (1,2), (1,3), \dots, (m,1), (m,2), (m,3) \}$$

$$E_F := \{ \{(i,j), (p,q)\} : \underbrace{i \neq p}_{\text{unterschiedl. Klauseln}} \text{ und } \underbrace{c_{ij} \not\equiv \neg c_{pq}}_{c_{ij} \text{ und } c_{pq} \text{ sind miteinander konsistent}} \}$$

$$k_F := m$$

Beispiel:

$$F = (x_1 \vee \neg x_2) \wedge (x_1 \vee \neg x_3) \wedge (x_2 \vee x_3)$$



Dann gilt:

Es gibt eine Belegung $\alpha : V(F) \to \{0,1\}$ mit $\alpha \models F$

$\Leftrightarrow$ $\exists \alpha : V(F) \to \{0,1\}$ mit $\alpha \models \ell_{i,1} \vee \ell_{i,2} \vee \ell_{i,3}$

für jedes $1 \le i \le m$

$\Leftrightarrow$ $\exists \alpha : V(F) \to \{0,1\}$ und $\ell_{1,j_1}, \dots, \ell_{m,j_m}$ mit

$\alpha \models \ell_{i,j_i}$ für jedes $1 \le i \le m$

$\Leftarrow$ $\exists\, \ell_{1,j_1}, \dots, \ell_{m,j_m}$ mit $\ell_{i,j_i} \neq \neg \ell_{i',j_{i'}}$. für alle

$1 \le i \neq i' \le m$

$\Leftrightarrow$ $\exists\, (1,j_1), \dots, (m,j_m) \in V_F$ mit

$\{ (i,j_i), (i',j_{i'}) \} \in E_F$ für $1 \le i \neq i' \le m$

$\Leftarrow$ G_F hat eine Clique der Größe $k_F = m$.