3.3 NP-vollständige Probleme

(Zur Vorbereitung:) Aussagenlogik

Sei $V = \{v_1, v_2, v_3, \ldots\}$ eine abzählbare Menge von ***Aussagenvariablen***.

Induktive Definition der Menge $\mathcal{F}$ der ***Formeln***:

1. $v \in V \Longrightarrow v \in \mathcal{F}$.
2. $A, B \in \mathcal{F} \Longrightarrow \neg A, (A \wedge B), (A \vee B) \in \mathcal{F}$.

Eine ***Belegung*** ist eine Abbildung $\varphi : V \to \{0, 1\}$. Jede Belegung φ wird fortgesetzt auf $\mathcal{F}$ wie folgt:

$\varphi(\neg A) = 1 - \varphi(A)$;
$\varphi(A \wedge B) = \min(\varphi(A), \varphi(B))$;
$\varphi(A \vee B) = \max(\varphi(A), \varphi(B))$.

Eine Formel $A \in \mathcal{F}$ heißt ***erfüllbar***, wenn es eine Belegung φ gibt mit $\varphi(A) = 1$.

Erfüllbarkeitsproblem der Aussagenlogik (*SAT*):

Gegeben $A \in \mathcal{F}$; ist A erfüllbar?

Kodierung von *SAT* als Sprache

$v_i \in V \rightsquigarrow 1^i \quad \Longrightarrow \quad A \in \mathcal{F} \rightsquigarrow$ Wort über $\{1, \neg, \wedge, \vee, (,)\}$;
Sprache $SAT = \{\overline{A} \mid \overline{A}$ ist Kodierung eines erfüllbaren $A \in \mathcal{F}\}$.

Satz 3.3.1 SAT ist NP-vollständig.

Bemerkung

Bekannte deterministische Algorithmen für SAT haben Zeitkomplexität $2^{O(n)}$.

Variante von *SAT*

Eine Formel $A \in \mathcal{F}$ heißt in ***konjunktiver Normalform* (*kNF*)**, wenn $A \equiv B_1 \wedge \ldots \wedge B_n$ und $B_i \equiv B_{i1} \vee \ldots \vee B_{im_i}$ $(i = 1, \ldots, n)$ gilt $(n, m_i \geq 1)$, wobei $B_{ij} \equiv v$ oder $B_{ij} \equiv \neg v$ für ein $v \in V$ ist.
$SATNF = \{\overline{A} \mid \overline{A}$ ist Kodierung einer erfüllbaren Formel A in kNF$\}$.

Satz 3.3.2 $SATNF$ ist NP-vollständig.

Weitere NP-vollständige Probleme

1. **3-Erfüllbarkeitsproblem**
   Gegeben: $A \in \mathcal{F}$ in kNF $B_1 \wedge \ldots \wedge B_n$, wobei $B_i \equiv B_{i1} \vee \ldots \vee B_{im_i}$, $m_i \leq 3$ $(i = 1, \ldots, n)$ gilt.
   Ist A erfüllbar?
2. **Cliquen-Problem**
   Gegeben: Graph G und $k \in \mathbb{N}_0$.
   Enthält G eine k-Clique?
3. **Hamilton-Kreis-Problem**
   Gegeben: Graph G.
   Besitzt G einen Hamilton-Kreis?
4. **Rucksack-Problem**
   Gegeben: Folge $\alpha = (i_1, \ldots, i_n)$ ganzer Zahlen und $k \in \mathbb{Z}$.
   Gibt es eine Teilfolge $i_{j_1}, \ldots, i_{j_r}$ von α mit $\sum_{l=1}^{r} i_{j_l} = k$?
5. **Traveling-Salesman-Problem** (informell)
   Gegeben: n Städte, alle Entfernungen zwischen den Städten und eine Zahl k.
   Gibt es eine "Rundreise" (die alle Städte besucht), deren Gesamtlänge $\leq k$ ist?
6. **Prozessor-Zuteilungs-Problem**
   Gegeben: Menge $M = \{J_1, \ldots, J_n\}$ von Aufträgen, $t \in \mathbb{N}$ (Zeitschranke), $p \in \mathbb{N}$ (Anzahl der Prozessoren) und eine partielle Ordnung $<$ auf M.
   Gibt es eine Abbildung $f : M \to \{1, \ldots, t\}$ derart, dass höchstens p Aufträge auf die gleiche Zahl abgebildet werden und dass gilt: $J < J' \Rightarrow f(J) < f(J')$?

Das Cliquenproblem

Sei $G = (V, E)$ ein Graph. Eine ***k-Clique*** von G ist eine Teilmenge V' von V mit $|V'| = k$, so dass $(u, v) \in E$ für alle $u, v \in V'$, $u \neq v$ gilt.

Codierung als Sprache:
Knoten von $G \rightsquigarrow$ Zahlen 1,2,…, n, kodiert als $\overline{i} \equiv 1^i \quad (1 \leq i \leq n)$;
Kanten von $G \rightsquigarrow (\overline{i}, \overline{j}) \quad (\overline{i}, \overline{j}$ Kodierung der betreffenden Knoten);
$k \rightsquigarrow \overline{k} \equiv 1^k$.
$CLIQUE = \{\overline{k}(\overline{i}_1, \overline{j}_1) \ldots (\overline{i}_m, \overline{j}_m) \mid$
der durch $(\overline{i}_1, \overline{j}_1) \ldots (\overline{i}_m, \overline{j}_m)$ kodierte Graph besitzt eine k-Clique$\}$.

Satz 3.3.3 $CLIQUE$ ist NP-vollständig.