Übersicht

Polynomielle Reduktion

Seien $A, B \subseteq \Sigma^*$.

Eine polynomielle Reduktion von A auf B ist eine Funktion $f : \Sigma^* \to \Sigma^*$ die in polynomieller Zeit berechenbar ist, mit der Eigenschaft:

$$w \in A \iff f(w) \in B \quad \text{für alle } w \in \Sigma^*$$

Notation: $A \leq_P B$ falls es eine polynomielle Reduktion von A auf B gibt.

Eigenschaft:

- Ist B in P und $A \leq_P B$, dann ist auch A in P.
- Ist B in NP und $A \leq_P B$, dann ist auch A in NP.

Beispiel

Theorem

INDEPENDENT SET $\leq_P$ VERTEX COVER

Beweis: $I \subseteq V$ ist unabhängig gdw. $V \setminus I$ ein Vertex Cover ist.

Also hat G eine unabhängige Menge der Größe k
gdw. G eine Vertex Cover der Größe $|V| - k$ hat.

$\rightsquigarrow$ $(G, k) \mapsto (G, |V| - k)$ ist polynomielle Reduktion
von INDEPENDENT SET auf VERTEX COVER.

NP-vollständige Probleme

A ist NP-schwer, falls $B \leq_P A$ für alle B in NP ist.

A ist NP-vollständig, falls A in NP und NP-schwer ist.

Theorem

Ist A NP-vollständig, und ist A in P, dann ist $P = NP$.

Aussagenlogik: Syntax

Aussagenlogische Formeln über einer Menge X von Variablen sind induktiv definiert:

- jede Variable $x \in X$ ist eine Formel
- ist F eine Formel, dann auch $\neg F$
- sind F und G Formeln, dann auch $(F \wedge G)$
- sind F und G Formeln, dann auch $(F \vee G)$

Aussagenlogik: Semantik

Für eine Bewertung $\alpha : X \to \{0, 1\}$ der Variablen X wird induktiv der Wert $\alpha(F)$ einer Formel F definiert:

- $\alpha(x)$ ist durch α gegeben
- $\alpha(\neg F) = 1 - \alpha(F)$
- $\alpha(F \wedge G) = \min(\alpha(F), \alpha(G))$
- $\alpha(F \vee G) = \max(\alpha(F), \alpha(G))$

Definition: α erfüllt F, wenn $\alpha(F) = 1$ ist.

Man schreibt dafür auch $\alpha \models F$

F ist Tautologie, wenn $\alpha \models F$ für alle α gilt.

F ist erfüllbar, wenn es eine Bewertung α gibt mit $\alpha \models F$.

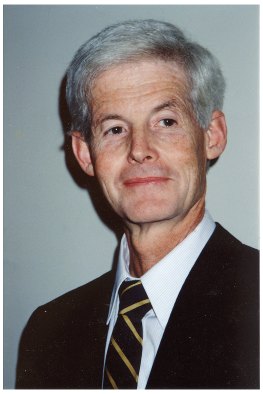
Das Erfüllbarkeitsproblem

Problem SAT

Instanz:	aussagenlogische Formel F
Frage:	Ist F erfüllbar ?

Theorem

SAT ist NP-vollstängig.



Stephen A. Cook hat den Begriff der NP-Vollständigkeit entdeckt, und SAT als erstes NP-vollständiges Problem nachgewiesen.

NP-Vollständigkeit von SAT

SAT ist in NP: F erfüllbar gdw $\exists \alpha : \alpha \models F$
$\alpha \models F$ kann in Zeit $O(|F|)$ geprüft werden.

SAT ist NP-schwer: Sei A in NP, wir werden zeigen $A \leq_P$ SAT.

Sei M eine NTM, die A entscheidet, und $p()$ Polynom mit:
für $|w| = n$ hält jede Berechnung von M nach $p(n)$ Schritten.

Konstruiere Formel $F_{M,w}$ so dass $F_{M,w}$ erfüllbar ist gdw.
eine Berechnung von M bei Eingabe w im Endzustand hält.
$F_{M,w}$ wird in Zeit $O(p(|w|)^2)$ aus w berechnet.

Konstruktion der Formel $F_{M,w}$

Sei $w = a_1 \ldots a_n$ und $t := p(n)$.

Berechnung von M hat $t+1$ Konfigurationen

$K_0\,,\; K_1\,,\; \ldots\;,\; K_t.$

Jede Konfiguration K_i hat $t+1$ Symbole

$a_{i,0}\,,\; a_{i,1}\,,\; \ldots\;,\; a_{i,t}.$

Für $i, j \leq t$, $q \in Q$ und $b \in \Gamma$ gibt es Variablen

- $x_{i,j,b}$ mit der Bedeutung $a_{i,j} = b$
- $x_{i,j,q}$ mit der Bedeutung $a_{i,j} = q$

Konstruktion der Formel $F_{M,w}$

Die Formel $F_{M,w}$ ist $S \wedge \bigwedge_{i=1}^{t} N_i \wedge E$, wobei

- S drückt aus, dass K_0 richtige Startkonfiguration ist,
- E drückt aus, dass K_t im Endzustand ist
- N_i drückt aus, dass $K_{i-1} \vdash_M K_i$,
  oder K_{i-1} ist Haltekonfiguration und $K_{i-1} = K_i$.

S ist $x_{0,0,q_0} \wedge x_{0,1,a_1} \wedge \ldots \wedge x_{0,n,a_n} \wedge x_{0,n+1,\Box} \wedge \ldots \wedge x_{0,t,\Box}$

E ist $\bigvee_{q \in F} E_q$ wobei $E_q = x_{t,0,q} \vee \ldots \vee x_{t,t,q}$

Konstruktion der Formel N_i

Die Formel N_i ist $\bigwedge_{j \le t} (A_{i,j} \vee B_{i,j})$, wobei

- $A_{i,j}$ drückt aus, wie $a_{i,j}$ von $a_{i-1,j-1} a_{i-1,j} a_{i-1,j+1}$ abhängt, wobei eines davon der Zustand in K_{i-1} ist.
- $B_{i,j}$ sagt: der Zustand in K_{i-1} ist so weit von $a_{i-1,j}$ entfernt, dass $a_{i,j} = a_i$.

B_i, j ist:

$$\bigvee_{a \in \Gamma} x_{i-1,j-1,a} \ \wedge \ \bigvee_{a \in \Gamma} x_{i-1,j+1,a} \ \wedge \ \bigvee_{a \in \Gamma} (x_{i-1,j,a} \wedge x_{i,j,a})$$

Konstruktion der Formel N_i

$A_{i,j}$ ist eine Disjunktion von Teilformeln, die jeweils $a_{i,j}$ für eine Kopfposition $j-1$, j oder $j+1$ in K_{i-1} und einen Übergang von M beschreiben.

Ist z.B. $(p, b, R) \in \delta(q, a)$, dann enthält $A_{i,j}$ die Teilformeln

$$x_{i-1,j-1,q} \wedge x_{i-1,j,a} \wedge x_{i,j-1,b} \wedge x_{i,j,p} \wedge \bigvee_{a \in \Gamma} (x_{i-1,j+1,a} \wedge x_{i,j+1,a})$$

$$\bigvee_{a \in \Gamma} (x_{i-1,j-1,a} \wedge x_{i,j-1,a}) \wedge x_{i-1,j,q} \wedge x_{i-1,j+1,a} \wedge x_{i,j,b} \wedge x_{i,j+1,p}$$

Ist $(p', b, L) \in \delta(q, a)$, dann enthält $A(i,j)$ auch die Teilformel

$$\bigvee_{a \in \Gamma} (x_{i-1,j,a} \wedge x_{i,j+1,a}) \wedge x_{i-1,j+1,q} \wedge x_{i-1,j+2,a} \wedge x_{i,j,p'} \wedge x_{i,j+2,b}$$