Satz von Cook: SAT ist NP-vollständig

Beweis: SAT $\in$ NP

Rate $\quad a = (a_1, \ldots, a_n) \in \{0,1\}^n$

Akzeptiere, wenn alle Klauseln erfüllt, poly. Zeit.

$L \in$ NP. $\quad$ ZZ.: $L \leq_p$ SAT

Für L RV-NTM $\quad M = (Q, \Sigma, q_0, \Gamma, \delta, F)$

die L in poly. Zeit entscheidet

- $w \in L$: $\exists\, K_0, \ldots, K_t$
  K_0 Startkonfig. zu w
  $K_i \vdash K_{i+1} \quad 0 \leq i \leq t-1$
  K_t akzeptierend, $\quad t \leq p(|w|)$
- $w \notin L$: Konfigurationsfolge existiert nicht

Idee: Berechnung von M ausgedrückt durch

Boolesche Formeln in konjunktiver Normalform

M akzeptiert $\Longleftrightarrow$ Formel erfüllbar

Berechnung: Genau $p(|w|) + 1$ Konfigurationen

$K_0(w), \ldots, K_{p(|w|)}(w)$

Rel. Bandpos.: $-p(|w|), \ldots, -1, 0, 1, \ldots, p(|w|)$

Konfigurationen: Variablen

(1) Aktueller Zustand $Q(i,k)$

$Q(i,k) = 1$, wenn M zum Zeitpunkt i im Zustand k

$0 \leq i \leq p(|w|), \quad 0 \leq k \leq |Q| - 1$

(2) Kopfposition $H(i,j)$

$H(i,j) = 1$, wenn M zum Zeitpunkt i an Position j

$0 \leq i \leq p(|w|), \quad -p(|w|) \leq j \leq p(|w|)$

(3) Bandinschrift $S(i,j,k)$

$S(i,j,k) = 1$, wenn zum Zeitpunkt i an Position j der Buchstabe k steht

$0 \leq i \leq p(|w|), \quad -p(|w|) \leq j \leq p(|w|)$

$1 \leq k \leq |\Gamma|, \quad \Gamma = \{a_1, \ldots, a_{|\Gamma|}\}$

Anz. Variablen

$$(p(|w|)+1)|Q| + (p(|w|)+1)(2p(|w|)+1) + (p(|w|)+1)(2p(|w|)+1)|\Gamma|$$

Konfigurationen: Klauselmenge

(1) $\forall i$: Genau ein $Q(i,k) = 1$

(2) $\forall i$: Genau ein $H(i,j) = 1$

(3) $\forall i\ \forall j$: Genau ein $S(i,j,k) = 1$

Klauselmenge nur dann erfüllbar, wenn Variablen Konfiguration beschreiben

$y_1, \ldots, y_m$

$$(y_1 \vee \ldots \vee y_m) \wedge (\bigwedge_{i \neq j} (\overline{y_i} \vee \overline{y_j}))$$

$O(m^2)$ Klauseln

(1) $(p(|w|)+1) \cdot O(|Q|^2) = O(p(|w|))$
(2) $(p(|w|)+1) \cdot O(p(|w|)^2) = O(p(|w|)^3)$
(3) $(p(|w|)+1)(2p(|w|)+1) \cdot O(|\Gamma|^2)$
$= O(p(|w|)^2)$

(4) $i = 0$ Anfangskonfiguration
nach Ratephase, da diese nicht vom
TM-Programm abhängt

$Q(0,k) = 1$ q_k Anfangszustand n. Ratephase
$H(0,1) = 1$ $S(0,0,t) = 1$ a_t Trennsymbol

Für $j < 0$
$$\frac{S(0,j,k_0) \vee S(0,j,k_1) \vee S(0,j,k_2) \qquad a_{k_0} = 0 \quad a_{k_1} = 1 \quad a_{k_2} = B}{S(0,j,k_2) \vee S(0,j-1,k_2)}$$
$-p(|w|) + 1 \leq j \leq -1$

Für $j \geq 1$
$S(0,j,k_0) = \overline{w_j}$ $S(0,j,k_1) = w_j$ $1 \leq j \leq |w|$
$S(0,j,k_2)$ $j > |w|$
$3 + p(|w|) + p(|w|) - 1 + |w| + p(|w|) - |w|$
$= O(p(|w|))$

(5) Letzte Konfiguration akzeptierend
$Q(p(|w|), k^*)$ k^* Index akzep. Zustand
1

(6) $K_i \vdash K_{i+1}$

(b) Nichtgelesene Speicherzellen dürfen nicht verändert werden

$\overline{S(i,j,k)} \vee H(i,j) \vee S(i+1,j,k)$

$0 \leq i < p(|w|) \quad -p(|w|) \leq j \leq p(|w|)$

$1 \leq k \leq |\Gamma|$

(b) Gelesene Speicherzelle muß korrekt verändert werden

Sei $b(k,l)$ Index mit $\delta(q_k, a_l) = (\;.\;, a_{b(k,l)},\;.)$

$\overline{H(i,j)} \vee \overline{Q(i,k)} \vee \overline{S(i,j,l)} \vee S(i+1,j,b(k,l))$

$0 \leq i < p(|w|) \quad -p(|w|) \leq j \leq p(|w|),$

$0 \leq k \leq |Q|-1 \quad 1 \leq l \leq |\Gamma|$

(c) Zustand muß korrekt verändert werden

$c(k,l)$ Index mit $\delta(q_k, a_l) = (q_{c(k,l)},\;.\;,\;.)$

$\overline{H(i,j)} \vee \overline{Q(i,k)} \vee \overline{S(i,j,l)} \vee Q(i+1,c(k,l))$

$0 \leq i < p(|w|), -p(|w|) \leq j \leq p(|w|)$

$0 \leq k \leq |Q|-1, 1 \leq l \leq |\Gamma|$

$O(p(|w|)^2)$

(d) Kopfpos. muß korrekt verändert werden

$d(k,l)$ Wert mit $\delta(q_k, a_l) = (\ .\ ,\ \ .\ , d(k,l))$

$R = +1 \quad N = 0 \quad L = -1$

$$\overline{H(i,j)} \vee \overline{Q(i,k)} \vee \overline{S(i,j,l)} \vee H(i{+}1, j{+}d(k,l))$$

$\forall\ 0 \leq i \leq p(|w|), \quad -p(|w|) \leq j \leq p(|w|)$

$0 \leq k \leq |Q| - 1, \quad 1 \leq l \leq |\Gamma|$

$O(p(|w|)^2)$ Variablen

$O(p(|w|)^3)$ Klauseln