Satz von Cook: SAT ist NP-vollständig

- SAT $\in$ NP

  Rate $z = (z_1, \ldots, z_n) \in \{0,1\}^n$

  Akzeptiere, wenn alle Klauseln erfüllt, poly. Zeit

- $L \in$ NP Z.Z.: $L \leq_p$ SAT

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

  die L in poly. Zeit entscheidet

  $w \in L : \exists K_0, \ldots, K_t$ K_0 Startkonfig. zu w

  K_{i+1} Nachfolgekonfig. von K_i $0 \leq i \leq t-1$

  K_t akzeptierend $t \leq p(|w|)$

  $w \notin L$: Konfigurationsfolge existiert nicht

Satz von Cook: Globale Beweisidee

- Berechnung von M ausgedrückt durch Boolesche Formeln in konjunktiver Normalform

  M akzeptiert Eingabe $\Leftrightarrow$ Formel erfüllbar

- Berechnung: Genau $p(|w|)$ Konfigurationen

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

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

Konfigurationen: Variablen

- Aktueller Zustand $Q(i,k)$

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

  $0 \leq i \leq p(|w|)$, $0 \leq k \leq |Q|-1$, $Q = \{q_0, \ldots, q_{|Q|-1}\}$

2. Kopfposition $H(i,j)$

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

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

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

   $S(i,j,k) = 1$, wenn zum Zeitpunkt i an Pos. j Buchstabe a_k steht

   $0 \leq i \leq p(|w|)$, $-p(|w|) \leq j \leq p(|w|)$, $1 \leq k \leq |\Gamma|$, $\Gamma = \{a_1, \ldots, a_{|\Gamma|}\}$

Anz. Var.: $(p(|w|)+1)|Q| + (p(|w|)+1)(2p(|w|)+1) + (p(|w|)+1)(2p(|w|)+1)|\Gamma|$

Konfigurationen: Klauselmenge

- $\forall\, i$ Genau ein $Q(i,k) = 1$
- $\forall\, i$ Genau ein $H(i,j) = 1$
- $\forall\, i\ \forall\, j$ Genau ein $S(i,j,k) = 1$

Klauselmenge nur dann erfüllbar, wenn Variablen Konfiguration beschreiben

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

$O(m^2)$ Klauseln

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

Anfangskonfiguration

Nach Ratephase, da diese nicht von TM-Programm abhängt

- $Q(0,k) = 1$ $\quad q_k$ Anfangszustand nach Ratephase
  $H(0,1) = 1$ $\quad S(0,0,t) = 1$ $\quad a_t$ Trennsymbol

- für $j < 0$
  $$\frac{S(0,j,k_0) \vee S(0,j,k_1) \vee S(0,j,k_2)}{S(0,j,k_2) \vee S(0,j-1,k_2)} \qquad \begin{matrix} a_{k0} = 0 \quad a_{k1} = 1 \quad a_{k2} = B \\ -p(|w|) + 1 \leq j \leq -1 \end{matrix}$$

- $j \geq 1$
  $S(0,j,k_0)$ wenn $w_j = 0$ $\quad S(0,j,k_1)$ wenn $w_j = 1$ $\quad 1 \leq j \leq |w|$
  $S(0,j,k_2)$ $\quad j \geq |w|$

Anz. Klauseln: $3 + p(|w|) + p(|w|) - 1 + |w| + p(|w|) - |w| = O(p(|w|))$

Letzte Konfiguration akzeptierend

- $Q(p(|w|),k^*)$ k^* = Index akzeptierender Zustand

Anz. Klauseln: 1

K_{i+1} Nachfolgekonfiguration von K_i

- Nichtgelesene Speicherzelle unverändert

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

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

- Gelesene Speicherzelle korrekt verändert

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

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

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

K_{i+1} Nachfolgekonfiguration von K_i

- Zustand korrekt verändert

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

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

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

- Kopfposition korrekt verändert

  sei $d(k,l)$ Index mit $\delta(q_k,a_l) = (\ldots, d_{c(k,l)})$ $\quad R=+1 \quad N=0 \quad L=-1$

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

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

  $O(p(|w|)^2)$ Variablen $\quad O(p(|w|)^3)$ Klauseln