Satz von Cook und Levin

$z_{t,j} = 1 \Leftrightarrow$ nach t Schritten: Zustand z_j
$p_{t,i} = 1 \Leftrightarrow$ nach t Schritten: Kopfpos$=i$
$b_{t,i,a} = 1 \Leftrightarrow$ nach t Schritten: Band[i]$=a$

Theorem

SAT ist NP-vollständig.

Beweis (Skizze: SAT ist NP-schwer)

zu zeigen: $\forall_{L \in \mathrm{NP}}\ L \leq_m^p \mathrm{SAT}$.
Sei $L \in \mathrm{NP}$. Dann existiert NTM M mit $L = T(M)$ & Polynom p beschränkt Laufzeit von M.
Sei $M = (Z, \Sigma, \Gamma, \delta, z_1, \square, E)$ mit $\Gamma = \{a_1 = \square, \ldots, a_\ell\}$ und $Z = \{z_1, \ldots, z_k\}$.
Annahme: M hält bei Eingabe $x = x_1 x_2 \ldots x_n \in \Sigma^n$ nach genau $p(n)$ Schritten.
Wir konstruieren eine Polynomzeitreduktion f, sodass gilt $x \in L \Leftrightarrow f(x) := F_M(x) \in \mathrm{SAT}$.
Zu konstruierende Formel $F_M(x)$ besitzt folgende boolesche Variablen:

Var.	Indizes	Bedeutung
$z_{t,j}$	$0 \leq t \leq p(n) \quad 1 \leq j \leq k$	$z_{t,j} = 1 \Leftrightarrow$ nach t Schritten ist M im Zustand z_j
$p_{t,i}$	$0 \leq t \leq p(n) \quad -p(n) \leq i \leq p(n)$	$p_{t,i} = 1 \Leftrightarrow$ nach t Schritten ist Kopf auf Pos. i
$b_{t,i,a}$	$0 \leq t \leq p(n) \quad -p(n) \leq i \leq p(n)$ $a \in \Gamma$	$b_{t,i,a} = 1 \Leftrightarrow$ nach t Schritten befindet sich auf Bandposition i das Zeichen a

Satz von Cook und Levin

$z_{t,j} = 1 \Leftrightarrow$ nach t Schritten: Zustand z_j
$p_{t,i} = 1 \Leftrightarrow$ nach t Schritten: Kopfpos$=i$
$b_{t,i,a} = 1 \Leftrightarrow$ nach t Schritten: Band$[i]=a$

Theorem

SAT ist NP-vollständig.

Beweis (Skizze: SAT ist NP-schwer)

$$F_M(x) := A \wedge T_1 \wedge T_2 \wedge F \wedge R$$

Anfang $A := z_{0,1} \wedge p_{0,0} \wedge \bigwedge_{0 \le i < n} b_{0,i,x_i} \wedge \bigwedge_{-p(n) \le i < 0} b_{0,i,\square} \wedge \bigwedge_{n \le i \le p(n)} b_{0,i,\square}$

Ende $F := \bigvee_{z_j \in E} z_{p(n),j}$

Übergänge $T_1 := \bigwedge_{\substack{0 \le t < p(n) \\ -p(n) \le i \le p(n) \\ 1 \le j \le k \\ a \in \Gamma}} (z_{t,j} \wedge p_{t,i} \wedge b_{t,i,a}) \rightarrow \bigvee_{(z_{j^*}, a^*, \gamma) \in \delta(z_j, a)} (z_{t+1,j^*} \wedge p_{t+1,i+\gamma} \wedge b_{t+1,i,a^*})$

mit $\gamma \in \{-1, 0, 1\}$ (das heißt $L = -1, N = 0, R = 1$)

$$T_2 := \bigwedge_{\substack{0 \le t < p(n) \\ -p(n) \le i \le p(n) \\ a \in \Gamma}} (\overline{p_{t,i}} \wedge b_{t,i,a}) \rightarrow b_{t+1,i,a}$$

Satz von Cook und Levin

$z_{t,j} = 1 \Leftrightarrow$ nach t Schritten: Zustand z_j
$p_{t,i} = 1 \Leftrightarrow$ nach t Schritten: Kopfpos=i
$b_{t,i,a} = 1 \Leftrightarrow$ nach t Schritten: Band[i]=a

Theorem

SAT ist NP-vollständig.

Beweis (Skizze: SAT ist NP-schwer)

$$F_M(x) := A \wedge T_1 \wedge T_2 \wedge F \wedge R$$

Randbedingungen $R := R_z \wedge R_p \wedge R_b$:

$$\text{Zustände } R_z := \bigwedge_{0 \le t \le p(n)} \text{genau\_eins}(z_{t,1}, \ldots, z_{t,k})$$

$$\text{Kopfpositionen } R_p := \bigwedge_{0 \le t \le p(n)} \text{genau\_eins}(p_{t,-p(n)}, \ldots, p_{t,p(n)})$$

$$\text{Bandinhalte } R_b := \bigwedge_{\substack{0 \le t \le p(n) \\ -p(n) \le i \le p(n)}} \text{genau\_eins}(b_{t,i,a_1}, \ldots, b_{t,i,a_\ell})$$

$$\text{genau\_eins}(y_1, \ldots, y_q) := \bigvee_{1 \le i \le q} y_i \wedge \bigwedge_{1 \le i < j \le q} \overline{y_i \vee y_j}$$

Satz von Cook und Levin

$z_{t,j} = 1 \Leftrightarrow$ nach t Schritten: Zustand z_j
$p_{t,i} = 1 \Leftrightarrow$ nach t Schritten: Kopfpos=i
$b_{t,i,a} = 1 \Leftrightarrow$ nach t Schritten: Band[i]=a

Theorem

SAT ist NP-vollständig.

Beweis (Skizze: SAT ist NP-schwer)

$$F_M(x) := A \wedge T_1 \wedge T_2 \wedge F \wedge R$$

Formelgröße:

$$|A| \in O(p(n)) \qquad |F| \in O(1)$$
$$|T_1| \in O((p(n))^2) \qquad |T_2| \in O((p(n))^2)$$
$$|\text{genau\_eins}(y_1, \ldots, y_q)| \in O(q^2) \qquad |R| \in O((p(n))^3)$$

Korrektheit:

Beobachtung: $F_M(x)$ modelliert akzeptierenden Berechnungspfad im Zustandsgraphen von $M(x)$

$x \in L \Leftrightarrow$ es gibt akzeptierenden Berechnungspfad im Zustandsgraphen von $M(x)$
$\Leftrightarrow F_M(x)$ erfüllbar

TQBF & PSPACE

Theorem

TQBF ist PSPACE-vollständig.

Beweis (Skizze: TQBF ist PSPACE-schwer)

zu zeigen: $\forall_{L \in \text{PSPACE}}\ L \leq_m^p \text{TQBF}$.

Sei $L \in$ PSPACE. Dann existiert DTM M mit $L = T(M)$, platzbeschränkt durch Polynom p.

Sei $M = (Z, \Sigma, \Gamma, \delta, z_1, \square, E)$ mit $\Gamma = \{a_1 = \square, \ldots, a_\ell\}$ und $Z = \{z_1, \ldots, z_k\}$.

Sei $\mathcal{K}_x$ die Menge aller möglichen Konfigurationen von M bei Eingabe x

Sei $S \in \mathcal{K}_x$ die Startkonfiguration von M bei Eingabe x. Argument ähnlich zu Satz v. Savitch:

M akzeptiert $x \Leftrightarrow \exists_{T \in \mathcal{K}_x}\ T$ akzeptierend $\wedge\, \text{reach}_x(S, T, k \cdot p(n) \cdot |\Gamma|^{p(n)})$

$\text{reach}_x(Q, R, j) \hat{=}$es gibt einen Q-R-Pfad der Länge $\leq j$ im Konfigurationsgraph von $M(x)$

$$\text{reach}_x(Q, R, j) := \begin{cases} R \text{ ist Folgekonfiguration von } Q \vee (Q = R) & \text{falls } j = 1 \\ \exists_{C \in \mathcal{K}_x} \forall_{D, D' \in \mathcal{K}_x} \left((D = Q \wedge D' = C) \vee (D = C \wedge D' = R)\right) & \\ \qquad \rightarrow \text{reach}_x(D, D', \lceil j/2 \rceil) & \text{falls } j > 1 \end{cases}$$

$\rightsquigarrow |\text{reach}_x(Q, R, j)| \approx O(1) + |\text{reach}_x(Q, R, \lceil j/2 \rceil)| \in O(\log j) \rightsquigarrow$ ✓