Satz von Cook und Levin

Theorem

SAT ist NP-vollständig.

SAT

<u>I_N</u>: aussagenlogische Formel φ

<u>Q</u>: $\exists$ Belegung β unter der φ zu 1 (wahr) ausgewertet wird

Satz von Cook und Levin

Theorem

SAT ist NP-vollständig.

Beweis (Skizze: SAT ist NP-schwer)

bei Eingabe x macht
M $\leq p(|x|)$ Schritte

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.

Satz von Cook und Levin

Theorem

SAT ist NP-vollständig.

Beweis (Skizze: SAT ist NP-schwer)

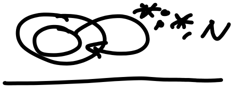
$\ell, k \in \mathbb{N}$

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

Satz von Cook und Levin



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 $Z = \{z_1, \ldots, z_k\}$.

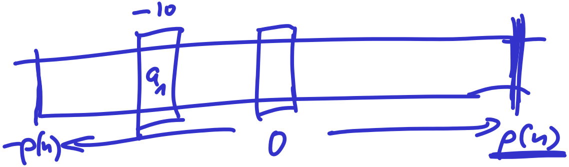
Annahme: M hält bei Eingabe $x = x_1 x_2 \ldots x_n \in \Sigma^n$ nach genau $p(n)$ Schritten.

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:

beschreibt Arbeitsweise von M(x)

Satz von Cook und Levin



$\delta_{t,-10,a_1} = 1$

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 $M = (Z, \Sigma, \Gamma, \delta, z_1, \Box, E)$ mit $\Gamma = \{a_1 = \Box, \ldots, a_\ell\}$ 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
$b_{t,i,a}$	$0 \leq t \leq p(n)$ $\quad -p(n) \leq i \leq p(n)$ $\quad a \in \Gamma$	$b_{t,i,a} = 1 \Leftrightarrow$ 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)

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 $M = (Z, \Sigma, \Gamma, \delta, z_1, \Box, E)$ mit $\Gamma = \{a_1 = \Box, \ldots, a_\ell\}$ 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 $x \in L \Leftrightarrow f(x) := \underline{F_M(x)} \in \mathrm{SAT}$.
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
$b_{t,i,a}$	$0 \leq t \leq p(n)$ $\quad -p(n) \leq i \leq p(n)$ $\quad a \in \Gamma$	$b_{t,i,a} = 1 \Leftrightarrow$ 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)

$$F_M(x) := \underbrace{A}_{\text{Anfang}} \wedge \underbrace{T_1 \wedge T_2}_{\text{Übergänge}} \wedge \underbrace{F}_{\text{Ende}} \wedge \underbrace{R}_{\text{Randbedingungen}}$$

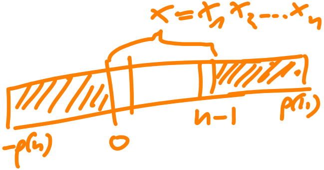
Satz von Cook und Levin

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

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

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

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

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

Ende $F := \bigvee_{z_j \in E} z_{p(n),j}$ $\quad O(1)$

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

$O(p(n) \cdot p(n) \cdot 1 \cdot 1 \cdot 1) = O(p(n)^2)$

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

$T_2 := \bigwedge_{\substack{0 \le t < p(n) \\ -p(n) \le i \le p(n) \\ a \in \Gamma}} (\overline{p_{t,i}} \wedge b_{t,i,a}) \to b_{t+1,i,a}$ $\quad \rightsquigarrow O(p(n)^2)$

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 $R := \underline{R_z} \wedge \underline{R_p} \wedge \underline{R_b}$:

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

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

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

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

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

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

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

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

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

a_1 a_ℓ

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

$$\text{Zustände } R_z := \bigwedge_{0 \le t \le p(n)} \underbrace{\text{genau\_eins}(z_{t,1}, \ldots, z_{t,k})}^{O(k^2)=O(1)} \rightsquigarrow O(p(n))$$

$$\text{Kopfpositionen } R_p := \bigwedge_{0 \le t \le p(n)} \underbrace{\text{genau\_eins}(p_{t,-p(n)}, \ldots, p_{t,p(n)})}^{O(p(n)^2)} \rightsquigarrow O(p(n)^3)$$

$$\text{Bandinhalte } R_b := \bigwedge_{\substack{0 \le t \le p(n)\\ -p(n) \le i \le p(n)}} \underbrace{\text{genau\_eins}(b_{t,i,a_1}, \ldots, b_{t,i,a_\ell})}^{O(1)} \rightsquigarrow O(p(n)^2)$$

$$\text{genau\_eins}(y_1, \ldots, y_q) := \bigvee_{1 \le i \le q} y_i \wedge \bigwedge_{1 \le i < j \le q} \overline{y_i \vee y_j} \rightsquigarrow O(q+q^2) = O(q^2)$$

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:

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:

$$|A| \in O(p(n)) \qquad |F| \in O(1)$$

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:

$$|A| \in O(p(n)) \qquad |F| \in O(1)$$

$$|T_1| \in O((\underline{p(n)})^2) \qquad |T_2| \in O((\underline{p(n)})^2)$$

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:

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

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 $M(x)$

$F_M(x)$ erfüllbar

$\exists$ Belegung die $F_M(x)$ erfüllt $\rightsquigarrow$ $\exists$ Folgekonfigurationsfolge zu akz. Konf.

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 $M(x)$

$$x \in L \Leftrightarrow \text{es gibt akzeptierenden Berechnungspfad im Zustandsgraphen von } M(x)$$

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

Satz v. Savitch
Satz v. Cook

Theorem

TQBF ist PSPACE-vollständig.

TQBF & PSPACE $= \bigcup_{k \in \mathbb{N}} \text{DSPACE}(n^k)$

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

TQBF & PSPACE

Theorem

TQBF ist PSPACE-vollständig.

Beweis (Skizze: TQBF ist PSPACE-schwer)

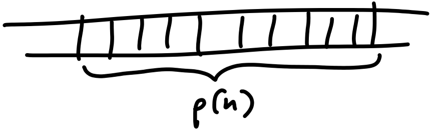
zu zeigen: $\forall_{L \in \mathrm{PSPACE}}\ L \leq_m^p \mathrm{TQBF}$.
Sei $L \in \mathrm{PSPACE}$. Dann existiert DTM M mit $L = T(M)$, platzbeschränkt durch Polynom p.
Sei $M = (Z, \Sigma, \Gamma, \delta, z_1, \square, E)$ mit $\Gamma = \{a_1 = \square, \ldots, a_\ell\}$ und $Z = \{z_1, \ldots, z_k\}$.

TQBF & PSPACE

Theorem

TQBF ist PSPACE-vollständig.

Beweis (Skizze: TQBF ist PSPACE-schwer)



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

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

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

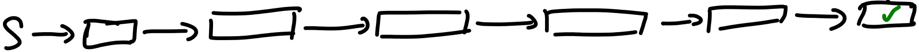
Sei $\mathcal{K}_x$ die Menge aller möglichen Konfigurationen von M bei Eingabe x

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 $\wedge\ \mathrm{reach}_x(S, T, k \cdot p(n) \cdot |\Gamma|^{p(n)})$

$\Rightarrow$ $\Leftarrow$

#Konfigurationen $= |\mathcal{K}_x|$



reach(S, T, 31) = 1

TQBF & PSPACE

Theorem

TQBF ist PSPACE-vollständig.

Beweis (Skizze: TQBF ist PSPACE-schwer)

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

Sei $L \in \mathrm{PSPACE}$. 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 $Z = \{z_1, \ldots, z_k\}$.

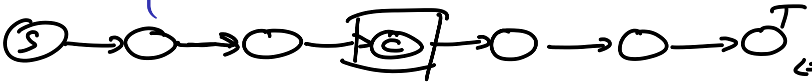
Sei $\mathcal{K}_x$ die Menge aller möglichen Konfigurationen von M bei Eingabe x

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 $\wedge\ \mathrm{reach}_x(S, T, k \cdot p(n) \cdot |\Gamma|^{p(n)})$

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

$$\mathrm{reach}_x(Q, R, j) := \begin{cases} R \text{ ist Folgekonfiguration von } Q \ \vee (R = Q) & \text{falls } j = 1 \\ \exists_{C \in \mathcal{K}_x}\ \mathrm{reach}_x(Q, C, \lfloor j/2 \rfloor) \wedge \mathrm{reach}_x(C, R, \lceil j/2 \rceil) & \text{falls } j > 1 \end{cases}$$



$\mathrm{reach}_x(S,T,6)$
$\Leftrightarrow \exists C\ \mathrm{reach}_x(S,C,3) \wedge \mathrm{reach}_x(C,T,3)$

$s(j) = 2 \cdot s(j/2)$ $s(1) = O(1)$

$\rightsquigarrow s(j) = j$

TQBF & PSPACE

Theorem

TQBF ist PSPACE-vollständig.

Beweis (Skizze: TQBF ist PSPACE-schwer)

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

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 $\wedge\ \mathrm{reach}_x(S, T, k \cdot p(n) \cdot |\Gamma|^{p(n)})$ → exponentiell in n!!!

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

$$\mathrm{reach}_x(Q, R, j) := \begin{cases} R \text{ ist Folgekonfiguration von } Q \ \vee (R = Q) & \text{falls } j = 1 \\ \exists_{C \in \mathcal{K}_x}\ \mathrm{reach}_x(Q, C, \lfloor j/2 \rfloor) \wedge \mathrm{reach}_x(C, R, \lceil j/2 \rceil) & \text{falls } j > 1 \end{cases}$$

$\forall D, D' \in K_x$ reach $(D, D', j/2)$ für $D = Q$ & $D' = C$ → reach $(D, D', j/2)$ für $D = C$ & $D' = R$

$\rightsquigarrow |\mathrm{reach}_x(Q, R, j)| \approx 2 \cdot |\mathrm{reach}_x(Q, R, \lceil j/2 \rceil)| \approx j \rightsquigarrow$ ✗

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 $M(x)$

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

$\leadsto |\text{reach}_x(Q, R, j)| \approx 2 \cdot |\text{reach}_x(Q, R, \lceil j/2 \rceil)| \approx j \leadsto$ ✗

TQBF & PSPACE

Zusammenbruch PH falls nur konstant viele Quantorenwechseln

Theorem

TQBF ist PSPACE-vollständig.

Beweis (Skizze: TQBF ist PSPACE-schwer)

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

Sei $L \in \mathrm{PSPACE}$. 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 ($x \in L$) $\Leftrightarrow \exists_{T \in \mathcal{K}_x}\ T$ akzeptierend $\wedge\ \mathrm{reach}_x(S, T, k \cdot p(n) \cdot |\Gamma|^{p(n)})$ $\rightarrow \log(*) \in p(n)^{O(1)}$

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

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

$\rightsquigarrow |\mathrm{reach}_x(Q, R, j)| \approx O(\overset{p(n)}{\cancel{1}}) + |\mathrm{reach}_x(Q, R, \lceil j/2 \rceil)| \in O(\log j \cdot p(n))$ ✓