$P = NP \Rightarrow N = 1$

Satz (Cook) SAT ist NP-vollständig.

$G(x_1, x_2, \dots, x_n)$ soll wahr sein gdw. genau ein x_i wahr ist.

$$G(x_1, x_2, \dots, x_n) = \bigvee_{i=1}^{n} x_i \wedge \left(\bigwedge_{j=1}^{n-1} \bigwedge_{\ell=j+1}^{n} \neg(x_j \wedge x_\ell) \right)$$

Die Größe von $G(x_1, \dots, x_n)$ ist $O(n^2)$.

Beweis

NP-Härte: Sei $L \in NP$ beliebig. Dann ex. Polynom p und es ex. eine nicht-det. TM M, so dass $L = T(M)$ und $ntime_M(x) \leq p(|x|)$. O.B.d.A. gelte für alle $z_e \in E$: $\delta(z_e, a) \Rightarrow (z_e, a, N)$ $\forall a \in \Gamma$.

Konstruiere Formel F_x, so dass für alle $x \in \Sigma^*$:

$x \in L$ gdw. F_x ist erfüllbar.

Sei $x = x_1 x_2 \dots x_n$.

Sei für M $\Gamma = \{a_1, \dots, a_e\}$ und $Z = \{z_0, \dots, z_q\}$

Wir benutzen die folgenden Booleschen Variablen:

Zustand	$zu_{t,z}$	$t = 0, 1, \dots, p(n)$ $z \in Z$	$zu_{t,z} = 1$ gdw. nach t Schritten die TM M im Zustand z ist. $zu_{5,z_3} = 1$ bedeutet im 5. Schritt ist M im Zustand z_3.
Kopfposition	$kp_{t,i}$	$t = 0, 1, \dots, p(n)$ $i = -p(n), \dots, 0, \dots, p(n)$	$kp_{t,i} = 1$ gdw. M's Kopf ist im Schritt t auf Pos. i
Band	$b_{t,i,a}$	$t = 0, 1, \dots, p(n)$ $i = -p(n), \dots, p(n)$ $a \in \Gamma$	$b_{t,i,a} = 1$ gdw. im Schritt t an Bandposition i das Zeichen a steht.

Man hat

Randbedingung — Transition an Kopfposition

$$F_x = R_{1\times 1} \wedge A_x \wedge T'_{1\times 1} \wedge T''_{1\times 1} \wedge E_{1\times 1}$$

$E_{1\times 1}$ ← Endbedingung

A_x: Anfangsbed.

$T'_{1\times 1}$, $T''_{1\times 1}$: Transition für Restband

$$R_n = \bigwedge_{t=0}^{p(n)} \Big[G\underbrace{\left(zu_{t,z_0}, \dots, zu_{t,z_k}\right)}_{O(1)} \wedge \underbrace{G_{p(n)}\left(kp_{t,-p(n)}, \dots, kp_{t,0}, \dots, kp_{t,p(n)}\right)}_{O(p(n)^2)} \wedge \underbrace{\bigwedge_{i=-p(n)}^{0} G\left(b_{t,i,a_1}, \dots, b_{t,i,a_\ell}\right)}_{O(p(n))} \Big]_{O(1)}$$

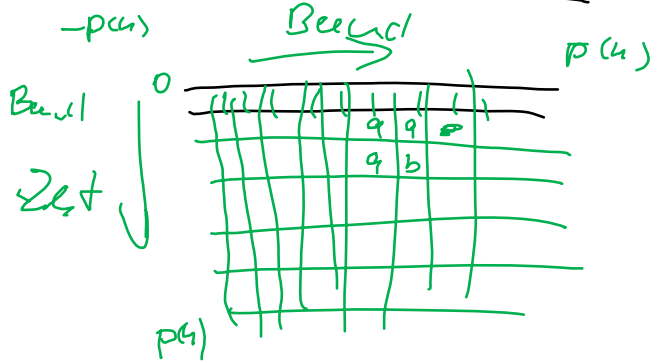
$$A_x = zu_{0,z_0} \wedge kp_{0,1} \wedge \underbrace{\bigwedge_{j=1}^{n} b_{0,j,x_j}}_{O(1)} \wedge \underbrace{\bigwedge_{j=-p(n)}^{0} b_{0,j,\sqcup} \wedge \bigwedge_{j=n+1}^{p(n)} b_{0,j,\sqcup}}_{O(p(n))}$$

- zu_{0,z_0}: zum Zeitpunkt $t=0$ Anfangszustand
- $kp_{0,1}$: Kopfpos. am Anf.
- b_{0,j,x_j}: Eingabewert
- $b_{0,j,\sqcup}$: leere Band

$$T'_n = \bigwedge_{t,z,i,q} \Big[\big(zu_{t,z} \wedge kp_{t,i} \wedge b_{t,i,q} \big) \rightarrow \bigvee_{z',a',y' \text{ mit } \delta(z,a) \ni (z',a',y')} \big(z_{t+1,z'} \wedge kp_{t+1,\, i+B(y')} \wedge b_{t+1,i,a'} \big) \Big]$$

$O(p(n)^2)$

mit $B(y) = \begin{cases} +1, & \text{falls } y = R \\ 0, & \text{falls } y = N \\ -1, & \text{falls } y = L \end{cases}$



$$T''_n = \bigwedge_{t,i,q} \big(\big(\neg kp_{t,i} \wedge b_{t,i,q} \big) \rightarrow b_{t+1,i,q} \big)$$

$$E_n = \bigvee_{z \in E} zu_{p(n),z}$$

z_1	a	z_3	b	L
z_1	a	z_4	c	R
z_2	b	. . .		

Sei nun $x \in L$. Dann ex. eine nicht-det. Rechnung der Länge $p(n)$, die zu einem Zustand $z \in E$ führt: $k_0 \vdash k_1 \vdash \dots \vdash k_{p(n)}$, wenn wir die Variablen in F_x so belegen, das sie der Rechnung entsprechen, dann wird F_x wahr, d.h. F_x ist erfüllbar.

F_x sei erfüllbar. Dann ex. eine Belegung α, die F_x wahr macht. D.h. α macht
- die Randbed. wahr (R_n)
- die Anfangsbed wahr (A_x)
- die Transitionsbed. $(T'_{n,1}, T''_n)$
- die Endbed. wahr (E_n)

D.h. aus α kann eine Konfigurationsfolge extrahiert werden entsprechend der intendierten Belegung der Variablen, die zeigt, dass $x \in L$.

Länge der Teilformeln:

$$|R_n| = O(p(n)^3)$$

$$|A_x| = O(p(n))$$

$$|T'_n| = O(p(n)^2)$$

$$|T''_n| = O(p(n)^2)$$

$$|E_n| = O(1)$$

Da alle Formeln "gleicht" aus M erzeugt werden können,
d.h. die Laufzeit ist polynomiell in n.
D.h. die Reduktion selbst ist polynomiell. $\square$