Satz (Cook)

$\boxed{\text{SAT ist NP-vollständig}}$

Bew: SAT $\in$ NP: Rate Belegung und überprüfe, ob die Belegung die Formel wahr macht. Kann in poly. Zeit auf NTM abgearbeitet werden. ✓

SAT ist NP-hart: Generische Reduktion. Sei $L \in NP$ beliebig.

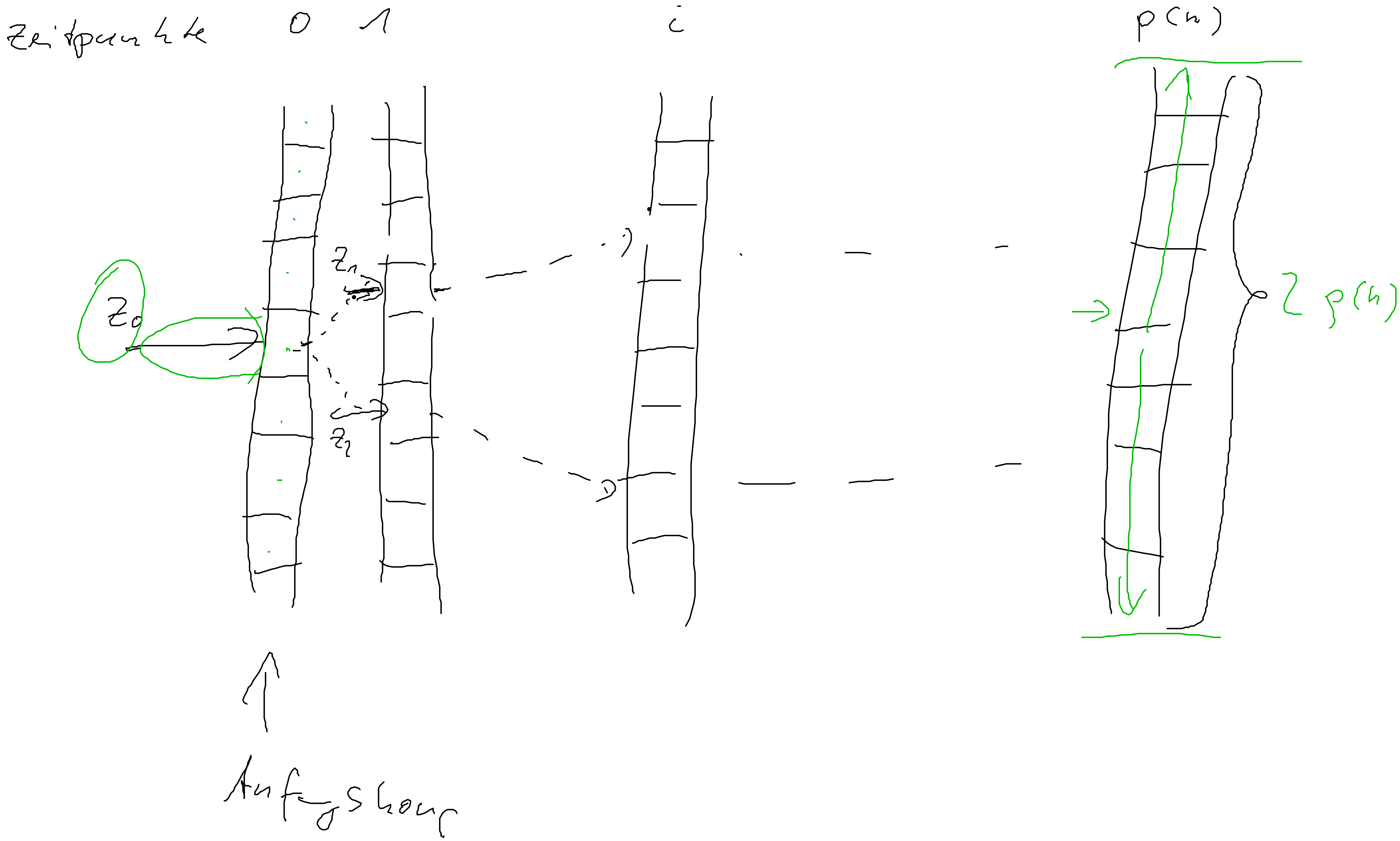
Zu zeigen $L \leq_p SAT$.

Sei M_L die nicht-det. TM, die L akzeptiert mit Laufzeit $p(n)$, wobei n Eingabelänge ist.

die Reduktion beschreibt

Sei $w \in \Sigma^*$ $\longrightarrow$ erzeuge eine Formel F_w mit

$w \in L$ gdw $F_w \in SAT$



Zeitpunkte
0
1
i
p(n)
z_0
z_1
z_2
p(n)

Wir benötigen die folgenden Booleschen Var.:

Zustand	$zu_{t,z}$	$t=0,\dots,p(n)$ $z \in Z$	$zu_{t,z} = T$ gdw. nach genau t Schritten die TM M_L im Zustand z ist.
Kopfpos.	$kp_{t,i}$	$t=0,\dots,p(n)$ $i=-p(n),\dots,0,\dots,p(n)$	$kp_{t,i} = T$ gdw. der Kopf nach genau t Schritten auf Position i steht
Band	$b_{t,i,a}$	$t=0,\dots,p(n)$ $i=-p(n),\dots,+p(n)$ $a \in \Gamma$	$b_{t,i,a} = T$ gdw. nach genau t Schritten hat die Bandzelle mit Index i den Inhalt a.

Nun sei

$$F_w = \underbrace{\overset{\text{Anfangsbed.}}{A_w} \wedge \underset{\text{Randbed.}}{R_{|w|}}} \wedge \underbrace{\underset{\text{Transitionsbed. für Band an der Kopfpos.}}{T'_{|w|}} \wedge \underset{\text{Transitionsbed. für Restband}}{T''_{|w|}}} \wedge \underline{\overset{\text{Endbedingung}}{E_{|w|}}}$$

$w = x_1 x_2 \dots x_n$

$O(p(n))$

$$A_w = zu_{0,z_0} \wedge kp_{0,1} \wedge \bigwedge_{j=1}^{n} b_{0,j,x_j} \wedge \bigwedge_{j=-p(n)}^{0} b_{0,j,\square} \wedge \bigwedge_{j=n+1}^{p(n)} b_{0,j,\square}$$

$$\underset{O(p(n)^3)}{R_n} = \bigwedge_{t=0}^{p(n)} \Big[\overset{O(1)}{G(zu_{t,z_0}, \dots, zu_{t,z_k})} \wedge \overset{O(p(n)^2)}{\underset{O(1)}{G(kp_{t,-p(n)}, \dots, kp_{t,p(n)})}} \wedge \underbrace{\bigwedge_{i=-p(n)}^{p(n)} G(b_{t,i,a_1}, \dots, b_{t,i,a_\ell})}_{O(p(n))} \Big]$$

$$T_h' = \bigwedge_{t,z,i,a} \Big[(zu_{t,z} \wedge kp_{t,i} \wedge b_{t,i,a}) \rightarrow$$

$O(p(n)^2)$ $O(1)$

$$\Big(\bigvee_{\substack{z',a',y' \text{ m.d.} \\ \delta(z,a) \ni (z',a',y')}} (\boxed{zu_{t+1,z'}} \wedge kp_{t+1,\, i+B(y')} \wedge \underline{b_{t+1,i,a'}}) \Big) \Big]$$

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

$O(p(n)^2)$

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

$$E = \bigvee_{z \in E} zu_{p(n),z} \leftarrow O(1)$$

unter der Voraussetzung, dass die TM in einem Endzustand bleiben kann, wenn sie ihn erreicht hat.

Sei $w \in L$. Dann ex. eine nicht-det. erfolgreiche Rechnung auf M_L mit der Länge $p(n)$, d.h. nach $p(n)$ Schritte sind wir im Zustand $z \in E$: $k_0 \vdash k_1 \vdash \dots \vdash k_{p(n)}$.
Wenn wir die Var. in F_w so belegen, dass sie der intendierte Bedeutung entsprechen, dann wird jeder Teil von F_w wahr werden. D.h. F_w ist erfüllbar.

Sei F_w erfüllbar ist. D.h. es gibt eine Belegung α, die F_w wahr macht. D.h. unser α macht:

- die Anfangsbed. wahr (A_n)
- die Randbed wahr ($R_{|w|}$)
- die Transitionsbed. wahr ($T'_{|w|}$, $T''_{|w|}$)
- die Endbed. wahr ($E_{|w|}$)

D.h. aus der Belegung kann eine Konfigurationsfolge erzeugt werden $k_0 \vdash k_1 \dots \vdash k_{p(n)}$, die einer erfolgreiche Rechnung entspricht, d.h. $w \in L$.

Länge der Teilformeln (in Abhängigkeit von der Länge von w)

$$|A_w| = O(p(|w|))$$

$$|R_{|w|}| = O(p(|w|)^3)$$

$$|T'_{|w|}| = |T''_{|w|}| = O(p(|w|)^2)$$

$$|E_{|w|}| = O(1)$$

Alle Formeln können bei gegebener Maschine M_L und w direkt hingeschrieben werden, d.h. die Laufzeit der Reduktion ist auch polynomial. $\square$

Spezialisierungen von SAT

CNF/DNF-SAT

Gegeben: Eine Formel der Aussagenlogik F in konjunktiver Normalform (CNF) ($\hat{=} \bigwedge(\bigvee l_{i,j})$) bzw. disjunktiver Normalform (DNF) ($\hat{=} \bigvee(\bigwedge l_{i,j})$).

Gefragt: Ist F erfüllbar?

DNF-SAT $\in$ P $\rightarrow$ trivialer Algorithmus

$$\boxed{(\underset{T}{\overset{\shortparallel}{a}} \wedge \underset{T}{\overset{\shortparallel}{b}} \wedge \underset{T}{\overset{\shortparallel}{c}})} \vee \boxed{(a \wedge b \wedge \neg a)}$$

3CNF-SAT (meist als 3SAT bez.)

CNF-SAT, wobei max. 3 Literale pro Klausel.

Bsp: $(a \vee b) \wedge (d \vee \neg e \vee \neg c)$

$\cancel{(a \vee b \vee c \vee d)}$

3CNF-SAT $\leq_p$ SAT

Satz 3CNF-SAT ist NP-vollständig.

Bew: 3CNF-SAT $\in$ NP ✓

NP-Härte: Reduktion von SAT auf 3CNF-SAT ($\leq_p$)

Gegeben eine Formel F über Var. $\{x_1, \dots, x_n\}$, erzeuge 3CNF Formel F' mit:

$$F \in \text{SAT} \quad \text{gdw} \quad F' \in \text{3CNF-SAT}$$

1. Versuch: Normalisiere F und erzeuge die CNF-Formel.

Die CNF (und DNF) einer Formel kann exponentiell größer sein als die Ursprungsformel! Geht nicht!