21. 12. 2011

Satz: Cook SAT ist NP-vollständig

$SAT = \{ \varphi \in \mathcal{L}(A_0, A_1, \dots) \mid$ es gibt eine Belegung v s.d. $\bar{v}(\varphi) = W \}$

$A \subseteq \mathbb{N}$
$A \subseteq \Sigma^*$
} heißt NP-vollst

$A \in NP$ (d.h. es gibt ein NP-Turingmaschine M s.d. $A(M) = A$)

f.a. $B \in NP$ ex. $f_B : \Sigma^* \to \Sigma^*$ polynomial det. berr., s.d.

f.a. $\sigma \in \Sigma^* \mid \sigma \in B \leftrightarrow f(\sigma) \in A$)

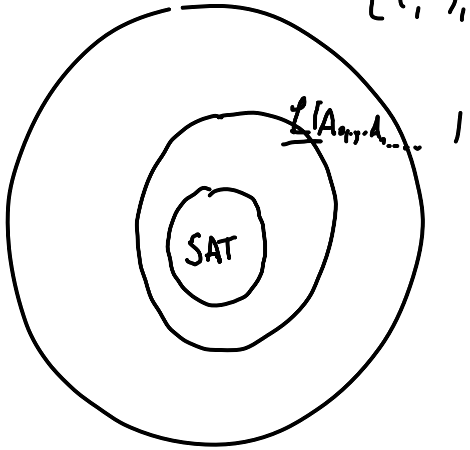
Beweis: 1. Teil $SAT \in NP$

Geg. φ. Errate eine Wahrheitsbel. v auf den Variablen in φ. Berechne (in polynomieller Zeit) $\bar{v}(\varphi)$.

⋮ – $\delta(\ \ ) = \{ (W, q, R),$
$(F, q, R) \}$

$\{ (,), \vee, \wedge, (A_i)_{i \in \mathbb{N}}, \neg \}^*$

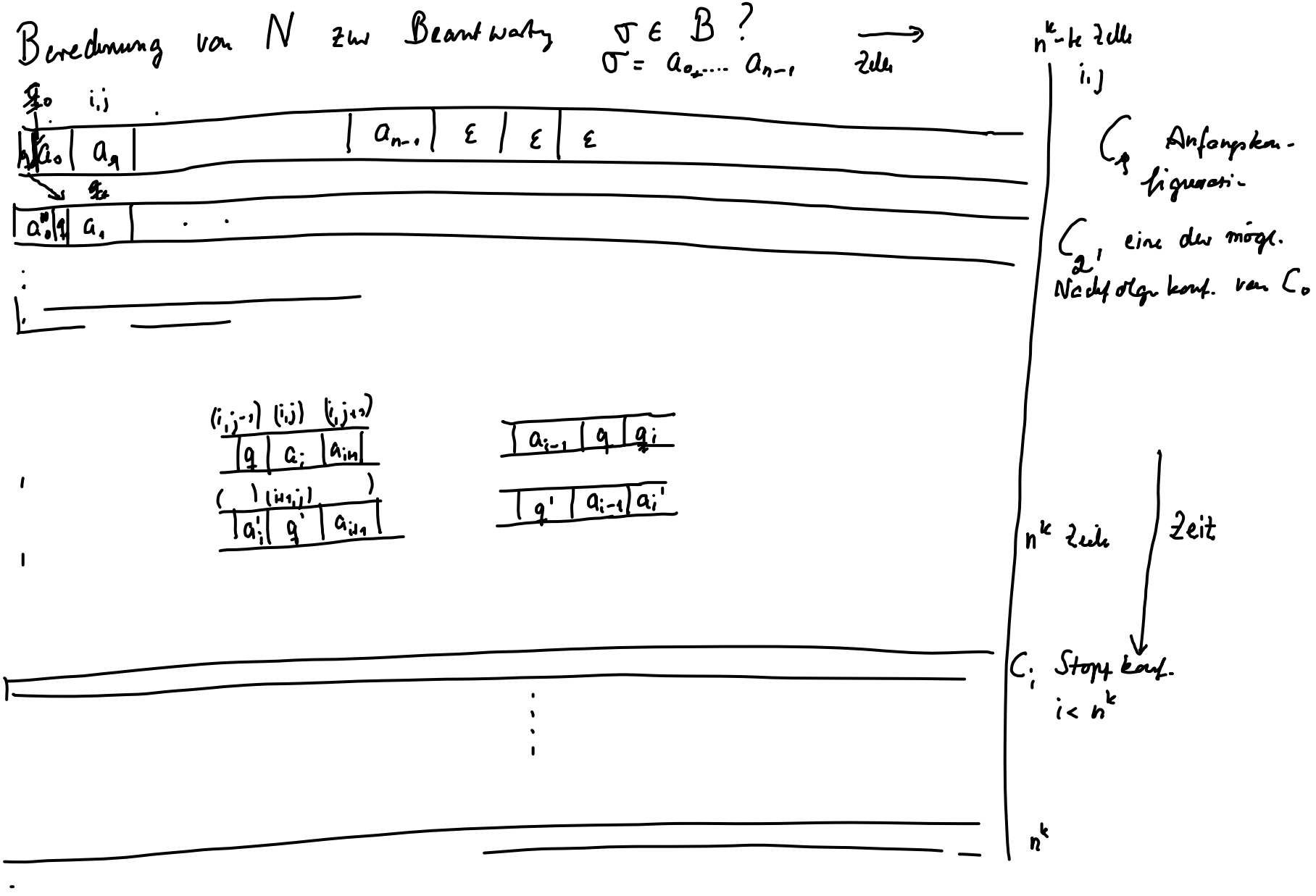
$|\varphi|$ 



Der skizzierte Algorithmus ist in NP.

2. SAT ist NP-hart. Jedes $B \in NP$ lässt sich in polynomieller Zeit auf SAT reduzieren.

Geg. $B \in NP$. Sei N eine n^k-nicht-deterministische TM, o.d.
$B = A(N)$. $B \subseteq \Sigma^*$ $n \longmapsto n^k$


Berechnung von N zur Beantwortung $\sigma \in B$?
$\sigma = a_0 \dots a_{n-1}$
n^k-te Zelle
i, j
C_0 Anfangskonfiguration
C_1 eine der mögl. Nachfolgekonf. von C_0
n^k Zeilen
Zeit
C_i Stopkonf. $i < n^k$
n^k

~~Zeige~~ $w \in \Sigma^*$ beg.

Zeige Definiere $f(w) = \varphi_w \in \mathcal{I}(A, \dots)$

s.d. $w \in A(N) = B \iff ex\ v\ \bar{v}(\varphi_w) = W$

und s.d. f eine deterministisch polynomial ber. Fkt ist.

$\varphi_w = \varphi_{Anfang,w} \wedge \varphi_{Zelle} \wedge \varphi_{Bewegung} \wedge \varphi_{Akz.}$

$\varphi_{Zelle} = \bigwedge_{1 \le i,j \le n^k} \left(\bigvee_{s \in C} x_{i,j,s} \wedge \bigwedge_{\substack{s,t \in C \\ s \neq t}} \neg(x_{i,j,s} \wedge x_{i,j,t}) \right)$ „KNF"

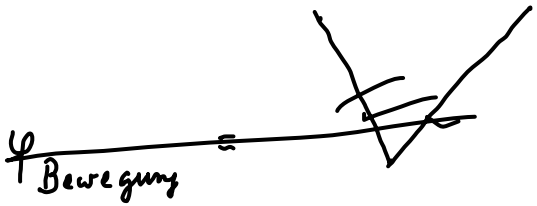
Variable $x_{i,j,s}$, i,j Indizes der Matrix, $s \in Q \cup \Gamma$ von N

Bedeutung $x_{i,j,s}$ ist wahr gdw auf Zelle i,j der „Buchstabe" s steht.

$\varphi_{Anfang,w} = x_{1,1,q_0} \wedge x_{1,2,a_0} \wedge x_{1,3,a_1} \wedge \dots \wedge x_{1,n+1,a_{n-1}} \wedge x_{1,n+2,\varepsilon} \wedge$

$\dots \qquad \dots \qquad \wedge x_{1,n^k,\varepsilon}$ rein Konjunktion

$\varphi_{\text{Akzeptierung}} = \bigvee_{1 \le j \le n^k} x_{n^k, j, q_{ak}}$ ~~DAT~~ reine Disjunktion



Eine Übergangsmatrix $\begin{pmatrix} a & q_1 & b \\ q_2 & a_k & c \end{pmatrix}$ heißt zulässig $:\Leftrightarrow$ $\delta(q_1, a) \ni (q_2, c, k)$

$\begin{pmatrix} a_k & q_1 & b \\ a & c & q_2 \end{pmatrix}$ " $:\Leftrightarrow$ $\delta(q_1, a) \ni (q_2, c, R)$

$\begin{pmatrix} a & q_1 & b \\ a & q_1 & b \end{pmatrix}$ " $:\Leftrightarrow$ $q_1 = q_{ak}$ Stoppzustand

$\begin{pmatrix} a & b & c \\ a & b & c \end{pmatrix}$

$\varphi_{\text{Zul}(i,j)} = \bigvee \left(X_{i,j-1,a_1} \wedge X_{i,j,a_2} \wedge X_{i,j+1,a_3} \wedge X_{i+1,j-1,a_4} \cdots \wedge X_{i+1,j+1,a_6} \right)$

$\begin{pmatrix} a_1 & a_2 & a_3 \\ a_4 & a_5 & a_6 \end{pmatrix}$ | zulässig

$\leq \sum_{\substack{a \in \Gamma \\ q \in Q}} |\delta(a,q)|$

$\leq |\Gamma \times Q \times \{R, L\}|$

$\varphi_{\text{Zul}(i,j)}$ $\quad |\Gamma|^2 \cdot |Q|^2 \cdot 2$

$\varphi_{\text{Berg}} = \bigwedge_{\substack{1 \leq i < n^k \\ 1 < j < n^k}}$ ($\bigvee$ 6 ei. Konjunkt.) KNF

$1 \leq i < n^k$, j $\quad (a_1 \ldots a_6)$ zul. Konjunktion

$\varphi_W = \varphi_{\text{Anf,kW}} \wedge \varphi_{\text{Zelle}} \wedge \varphi_{\text{Akzept}} \wedge \varphi_{\text{Berg}}$

φ_W ist erfüllbar $\Leftrightarrow$ $w \in$ ~~Alt~~ $A(N)$ $\Leftrightarrow$ es gibt $C_1, \ldots, C_\ell$, $\ell \leq n^k$

s.d. $(C_i)_i$ eine akzeptierende Konf.folge ist.

"$\Leftarrow$" nehme die Einträge $X_{i,j,s}$ längs $C_1, \ldots, C_\ell, \underbrace{C_\ell, \ldots, C_\ell}_{n^k - \ell}$

" $V(X_{i,j,s}) = W \Leftrightarrow$ auf Zelle (i,j) steht s

Sei $\bar{v}: \{x_{i,j,s} \mid 1 \leq i,j \leq n^k, s \in Q \cup T\} \to \{W, F\}$

o.d. $\bar{v}(\varphi_w) = W$.

$\Rightarrow$ es gibt $C_0, \dots, C_{n^k}$ $C_i \vdash C_{i+1}$ entspricht δ von N oder

$C_i = C_{i+1}$ und $q(C_i)$ ist ein Stoppstand.

$f: w \mapsto \varphi_w$ ist also eine Reduktion von B auf SAT

$w \in B \iff f(w) \in SAT$.

f ist in polynomieller Zeit berechenbar.

φ_{Anfang} hat Länge n^k und $w \mapsto \varphi_{Anfang,w}$

ist in $O(n^k)$ berechenbar.

$\varphi_{2 Zelle}$: Größen von w aus, ist dies eine konstante Fkt.

$|\varphi_{2 Zelle}| \leq O(n^k \cdot n^k \cdot (|Q| + |\Gamma|^2))$

$|\varphi_{\text{Akzeptierg}}| \leq O(n^k)$

$|\varphi_{\text{Bewegg}}| = O\left(n^k \cdot n^k \cdot 6 \cdot (Q^2 + T^2)\right) = O(n^{2k})$ □

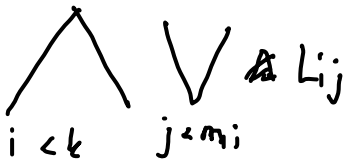
Korollar aus dem Beweis:

$\{\varphi \text{ KNF} \mid \varphi \text{ erfüllbar}\}$ ist NP-vollständig.

Beweis: φ_w muss noch ein bisschen umgewandelt werden s.d. φ_w KNF.

Korollar aus dem Korollar:

3-SAT ist NP-vollständig.



Def 3-SAT = $\{\varphi$ KNF $\mid$ alle Disjunktionen in φ haben ≤ 3 Literale$\}$

2-SAT " ≤ 2

Bew: $\bigwedge \bigvee_{j \le m_i} L_{ij}$

$B_1 \vee \dots \vee B_5 \vee B_n$ sei ein Konjunktionsglied

$$\varphi_{3\text{-KNF}} := (B_1 \vee B_2 \vee \underbrace{C_1}_{W}) \wedge (\underbrace{\neg C_1}_{F} \vee B_3 \vee \underbrace{C_2}_{W}) \wedge (\underbrace{\neg C_2}_{W} \vee B_4 \vee C_3)$$

$$\wedge (\underbrace{\neg C_3}_{W} \vee B_5 \vee \underbrace{C_4}_{W}) \wedge \dots \wedge (\underbrace{\neg C_{n-3}}_{\text{neu } W} \vee B_{n-1} \vee B_n)$$

es gibt kein w mit $w(B_i) = F$ für alle i o.d.
$\overline{w}(\varphi_{3\text{-KNF}}) = W$.

Beh: $B_1 \vee \dots \vee B_n$ ist erfüllbar gdw.

$\varphi_{3\text{-KNF}}$ erfüllbar.

ausführlich: (es gibt $v: \{B_1, \dots, B_n\} \to \{W, F\}$ $\overline{v}(B_1 \vee \dots \vee B_n) = W$)

gdw (es gibt $w: \{B_1, \dots, B_n, C_1, \dots, C_{n-3}\} \to \{W, F\}$ $\overline{w}(\varphi_{3\text{-KNF}}) = W$)

$\Rightarrow$: $v(B_i) = W$ dann bestimme w, $w(B_i) = v(B_i)$, $w(C_j)$ nach oben beschriebener Strategie.

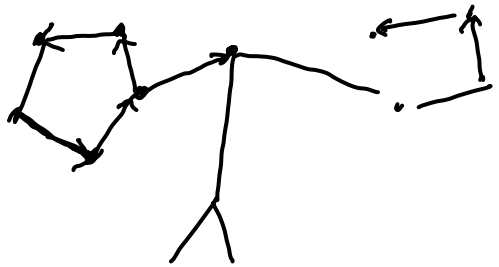
$\Leftarrow$ Sei $\bar{w}(\varphi_{3KNF}) = W$

Satz 2-SAT ist in P.

Beispiele für Mengen in NP:

Def: Sei $(V, E) = G$ ein gerichteter Graph.

Ein Hamiltonpfad von G ist ein Pfad in G, der jeden Punkt genau einmal enthält.



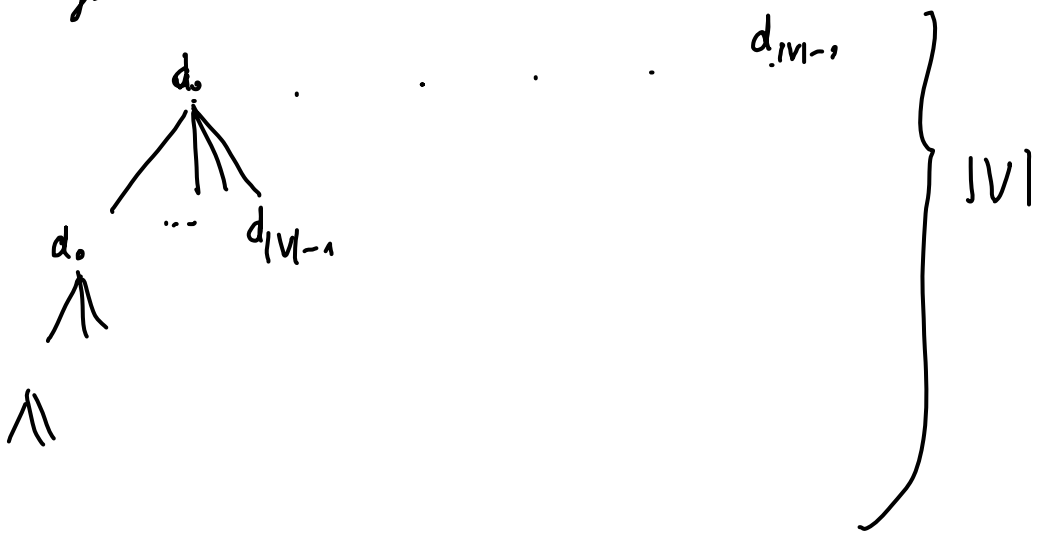
$$HAMPFAD := \{ (V, E, s, t) \mid \text{es gibt einen Hamiltonpfad von } s \text{ nach } t \text{ in } (V, E), \text{ gerichteter Graph}, s, t \in V \}$$

Algorithmus: HAMPFAD $\in$ NP

1. „Errate Zertifikat $c = (c_0, \dots, c_{|V|-1})$, $c_i \in V$." $|V|$ Möglichkeiten
2. Prüfe, ob $(c_i, c_{i+1}) \in E$. Wenn ja, gehe zu 3, wenn nein, lehne c ab
3. Prüfe ob für $i,j \in \{0,\dots,|V|-1\}$, $i \neq j$ $c_i \neq c_j$. (Injektive Funktionen von V nach V sind auch surjektiv.)
4. Prüfe ob für jedes $v \in V$ ein $c_i = v$ ist)

Wenn ja, akzeptiere, wenn nein, lehne c ab. „Errate nächstes c."

Bei deterministischer Simulation.



Beh: HAMPFAD ist NP-hart.

1. Möglichkeit: B nicht-det n^k-abzählbar

$B = A(N)$

2. Möglichkeit $3\text{-SAT} \leq_P$ HAMPFAD