

NP-Vollständigkeit



A heißt **polynomiell reduzierbar** auf B („ $A \leq_p B$ “), falls es eine in *polynomieller* Zeit berechenbare totale Funktion $f: \Sigma^* \rightarrow \Sigma^*$ gibt mit $\underline{x} \in A \Leftrightarrow f(\underline{x}) \in B \quad \forall \underline{x} \in \Sigma^*$.

Lemma: a) $A \leq_p B$ und $B \in \mathcal{P} \Rightarrow A \in \mathcal{P}$

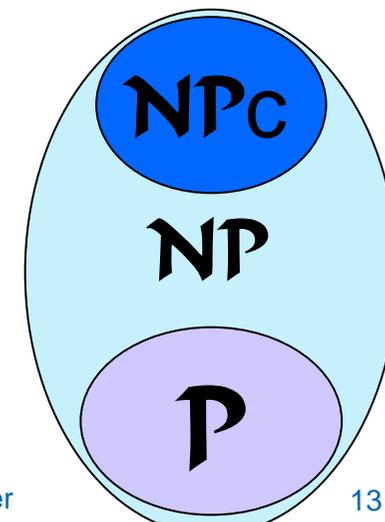
b) $A \leq_p B$ und $B \leq_p C \Rightarrow A \leq_p C$ (*Transitivität*)

L heißt **NP-schwer**, falls für jedes $A \in \mathbf{NP}$ gilt: $A \leq_p L$.

L heißt **NP-vollständig**, falls **NP-schwer** und $L \in \mathbf{NP}$ ist.

Bem: Ist ein L **NP-vollständig** und $L \in \mathcal{P}$,
so folgt $\mathcal{P} = \mathbf{NP}$ (und 1 000 000 \$US)

Korollar: Falls $\mathbf{NP} \neq \mathcal{P}$ gilt, dann sind alle **NP-vollständigen** Sprachen in $\mathbf{NP} \setminus \mathcal{P}$, also insbesondere nicht in \mathcal{P} .



Die Master-Reduktion

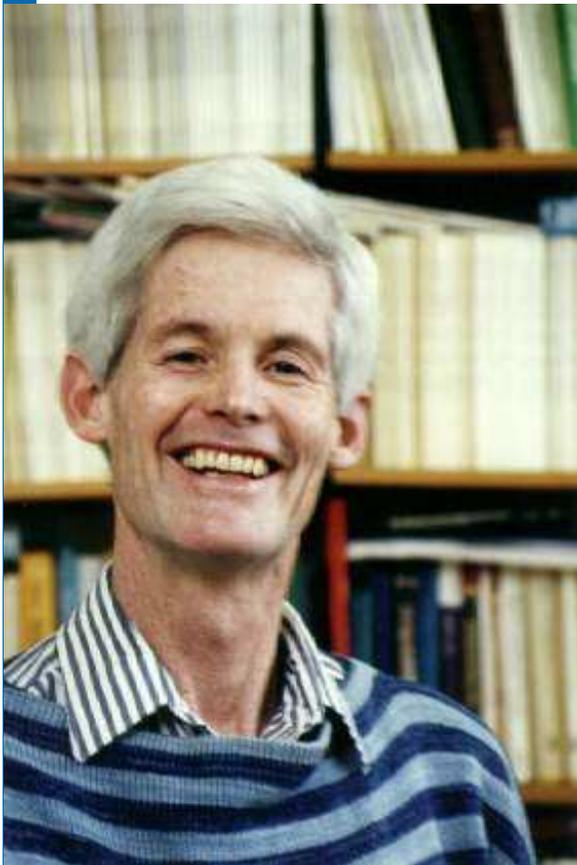


TECHNISCHE
UNIVERSITÄT
DARMSTADT

Komplexitätstheorie

Satz von Cook-Levin (1971/72)

SAT ist NP-vollständig.



Zu zeigen:

- $\text{SAT} \in \text{NP}$
(schon erledigt)
- Für jedes $L \in \text{NP}$ gilt:
 $L \leq_p \text{SAT}$



Beweisidee

$$\forall L \in \mathbf{NP}: L \leq_p \mathbf{SAT}$$

Sei $L \in \mathbf{NP}$, $N=(Q, \Sigma, \Gamma, \delta, q_0, F)$ eine 1-NTM, Komplexitätstheorie
die L in Zeit $T(n)$ entscheidet für ein Polynom T .

O.B.d.A.: N macht immer genau $T(n)$ Schritte

Aufgabe: Beschreibe eine in polynomieller Zeit berechenbare Funktion f , die bei Eingabe $\underline{w} \in \Sigma^*$ eine Boole'sche Formel $\Phi_{\underline{w}}=f(\underline{w})$ liefert, so dass gilt:

$$N \text{ akzeptiert } \underline{w} \iff \Phi_{\underline{w}} \text{ ist erfüllbar}$$

Idee: Konstruiere Formel Φ so, dass erfüllende Belegungen für Φ zu akzeptierenden Rechnungen von N korrespondieren.

Boole'sche Variablen von Φ und ihre intuitive Bedeutung:

$d_{s,a,t}$: „Nach Schritt t steht in Bandzelle #s das Symbol a “

$h_{s,t}$: „Nach Schritt t steht der Kopf auf Zelle #s“

$z_{q,t}$: „Nach Schritt t ist N im Zustand q “ $a \in \Gamma, q \in Q$

$$s=1..S(|\underline{w}|), \quad t=0\dots T(|\underline{w}|)$$

Konstruiere Formel $\Phi_{\underline{w}}$ so, dass erfüllende Belegungen für Φ zu akzeptierenden Rechnungen von N korrespondieren.

Boole'sche Variablen von Φ und ihre intuitive Bedeutung:

$d_{s,a,t}$: „Nach Schritt t steht in Bandzelle s das Symbol a “ $a \in \Gamma, q \in Q$

$h_{s,t}$: „Nach Schritt t steht der Kopf auf Zelle s “ $s=1..S(|\underline{w}|)$

$z_{q,t}$: „Nach Schritt t ist die Maschine im Zustand q “ $t=0...T(|\underline{w}|)$

$T(n) \cdot S(n) \cdot |\Gamma| + T(n) \cdot S(n) + |Q| \cdot T(n) =$ polynomiell viele Var.en

Jede Rechnung von N gestartet mit \underline{w} kann durch passende Belegung der Var.en beschrieben werden.

Belegungen können aber auch Unsinn beschreiben.

Ziel: Entwerfe KNF Φ , die genau für diejenigen Belegungen der Variablen **wahr** wird, die eine akzeptierende Rechnung von N beschreiben.

Teilformeln von Φ



$$\Phi_{\underline{w}}(V_0, \dots, V_T) := \mathbf{Config}(V_0) \wedge \mathbf{Config}(V_1) \wedge \dots \wedge \mathbf{Config}(V_T) \\ \wedge \mathbf{Start}_{\underline{w}}(V_0) \wedge \mathbf{Succ}(V_0, V_1) \wedge \dots \wedge \mathbf{Succ}(V_{T-1}, V_T) \wedge \mathbf{Akz}(V_T)$$

Boole'sche Variablen von Φ und ihre intuitive Bedeutung:

$d_{s,a,t}$: „Nach Schritt t steht in Bandzelle s das Symbol a “ $a \in \Gamma, q \in Q$
 $h_{s,t}$: „Nach Schritt t steht der Kopf auf Zelle s “ $s=1..S(|\underline{w}|)$
 $z_{q,t}$: „Nach Schritt t ist die Maschine im Zustand q “ $t=0...T(|\underline{w}|)$

V_t := der Teil der Variablen, die zum Rechenschritt $\#t$ gehören
= $\{ d_{s,a,t} : a \in \Gamma, s \leq S \} \cup \{ h_{s,t} : s \leq S \} \cup \{ z_{q,t} : q \in Q \}$

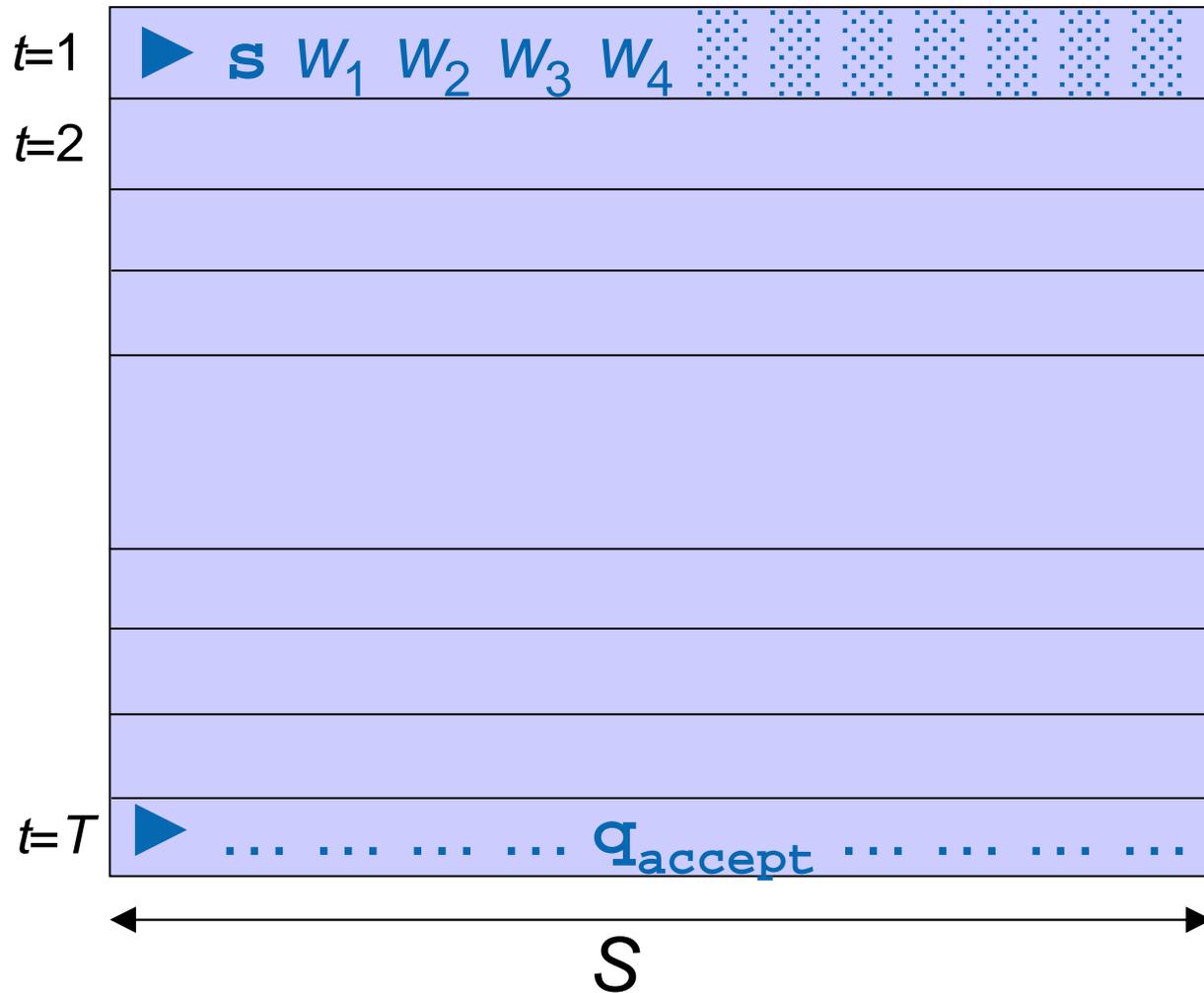
$\mathbf{Config}(V_t)$: wird **wahr** genau für die Belegungen von V_t ,
die eine Konfiguration beschreiben.

$\mathbf{Succ}(V_t, V_{t+1})$: wird **wahr** genau für die Belegungen von $V_t \cup V_{t+1}$,
die Konfigurationen K und K' beschreiben mit $K \vdash K'$.

$\mathbf{Start}_{\underline{w}}(V_0)$: wird **wahr** genau für Belegung, die $q_0 \underline{w}$ beschreibt.

$\mathbf{Akz}(V_T)$ **wahr** für Belegung, die einen akz. Endzustand beschreibt

Skizze zum Beweis



Start(V_1, \underline{w})

Succ(V_1, V_2)

Succ(V_2, V_3)

T

Succ(V_{T-1}, V_T)

Akz(V_T)

Config(V_1) $\wedge \dots \wedge$ Config(V_T)

Gibt es so eine
Belegung?

Gibt es solch eine Rechnung auf der NTM?

Config(V), Start $_{\underline{w}}$, Akz



wahr für Belegungen, die eine Konfiguration beschreiben

$$V = \{ d_{s,a} : a \in \Gamma, s \leq S \} \cup \{ h_s : s \leq S \} \cup \{ z_q : q \in Q \}$$

$d_{s,a}$: „in Bandzelle #s steht das Symbol a“

h_s : „Kopf steht auf Zelle #s“

z_q : „N ist in Zustand q“

Abkürzung $\text{uniq}(x_1, \dots, x_r) := (x_1 \vee \dots \vee x_r) \wedge \bigwedge_{i \neq j} (\neg x_i \vee \neg x_j)$

wahr \Leftrightarrow genau ein x_i ist **wahr**, Länge $O(r^2)$.

Config(V) :=

$$\text{uniq}(h_1, \dots, h_S) \wedge \text{uniq}(z_q : q \in Q) \wedge \bigwedge_{s \leq S} \text{uniq}(d_{s,a} : a \in \Gamma)$$

hat Länge $O(S^2 + |Q|^2 + S \cdot |\Gamma|^2) = O(S^2)$, da NTM N fixiert.

$$\text{Start}_{\underline{w}}(V) := h_1 \wedge z_{q_0} \wedge d_{1,w_1} \wedge \dots \wedge d_{n,w_n} \wedge d_{n+1,B} \wedge \dots \wedge d_{S,B}$$

$$\text{Akz}(V) := z_{q_+} \quad \text{Länge } O(S)$$

Start $_{\underline{w}}$ (V) : wird **wahr** genau für Belegung, die $q_0 \underline{w}$ beschreibt.

Succ(V_t, V_{t+1})



wahr genau für die Belegungen, die aufeinanderfolgende Konfigurationen beschreiben

Abkürzungen: „ $x=y$ “ $\Leftrightarrow (x \vee \neg y) \wedge (\neg x \vee y)$

$Y_{s,q,a,p,b,L} := „(h_{s,t} \wedge z_{q,t} \wedge d_{s,a,t}) \Rightarrow (z_{p,t+1} \wedge d_{s,b,t+1} \wedge h_{s-1,t+1)“$

$Y_{s,q,a,p,b,N}(V_t, V_{t+1})$ und $Y_{s,q,a,p,b,R}(V_t, V_{t+1})$ analog

„Kopf steht auf Bandzelle #s oder Zelle #s bleibt unverändert“

$$\text{Succ}(V_t, V_{t+1}) := \bigwedge_{s \leq S} \bigwedge_{a \in \Gamma} (h_{s,t} \vee „d_{s,a,t} = d_{s,a,t+1}“)$$
$$\wedge \bigwedge_{s \leq S} \bigvee_{(p,b,X) \in \delta(q,a)} Y_{s,q,a,p,b,X}(V_t, V_{t+1})$$

$d_{s,a,t}$: „Nach Schritt t steht in Bandzelle s das Symbol a “ $a \in \Gamma, q \in Q$
 $h_{s,t}$: „Nach Schritt t steht der Kopf auf Zelle #s“ $s=1..S$
 $z_{q,t}$: „Nach Schritt t ist die Maschine im Zustand q “ $t=0..T$

Zusammenfassung des Beweises



$\text{Config}(V_t)$: wird **wahr** genau für die Belegungen von V_t ,
die eine Konfiguration beschreiben.

$\text{Succ}(V_t, V_{t+1})$: wird **wahr** genau für die Belegungen von $V_t \cup V_{t+1}$,
die Konfigurationen K und K' beschreiben mit $K \vdash K'$.

$\text{Start}_{\underline{w}}(V_0)$: wird **wahr** genau für Belegung, die $q_0 \underline{w}$ beschreibt.

$\text{Akz}(V_T)$ **wahr** für Belegung, die einen akz. Endzustand beschreibt

Jeweils berechenbar aus \underline{w} in polynom. Zeit

$$\Phi_{\underline{w}}(V_0, \dots, V_T) := \text{Config}(V_0) \wedge \text{Config}(V_1) \wedge \dots \wedge \text{Config}(V_T) \\ \wedge \text{Start}_{\underline{w}}(V_0) \wedge \text{Succ}(V_0, V_1) \wedge \dots \wedge \text{Succ}(V_{T-1}, V_T) \wedge \text{Akz}(V_T)$$

Berechenbar in polynom. Zeit und gilt:

N akzeptiert $\underline{w} \iff \Phi_{\underline{w}}$ ist erfüllbar



NP-vollständige Probleme

Def. (Erinnerung): A heißt **NP-vollständig**, falls
 $A \in \mathbf{NP}$ und für jedes $L \in \mathbf{NP}$ gilt: $L \leq_p A$

Cook-Levin: **SAT** ist **NP-vollständig**.

Wissen: $\mathbf{CLIQUE} \equiv_p \mathbf{IS} \leq_p \mathbf{SAT} \equiv_p \mathbf{3SAT} \leq_p \mathbf{IS}$.

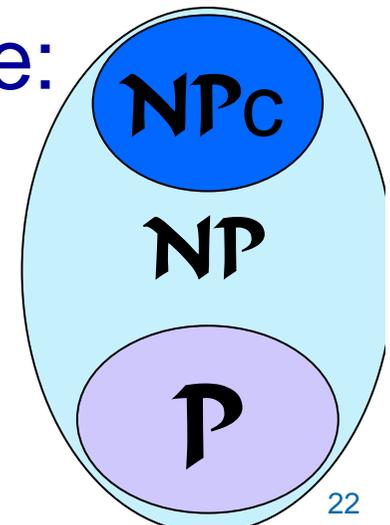
\Rightarrow auch **CLIQUE**, **IS**, **3SAT** sind **NP-vollständig**

Lemma. Sei A **NP-vollständig** und gelte:

- $B \in \mathbf{NP}$

- $A \leq_p B$

Dann ist auch B **NP-vollständig**.



SubsetSum NP-vollständig

$$\{ \langle a_1, \dots, a_N, b \rangle \mid a_1, \dots, a_N, b \in \mathbb{N}, \exists \alpha_1, \dots, \alpha_N \in \{0, 1\} : b = \sum_i a_i \cdot \alpha_i \}$$

SubsetSum \in NP \checkmark Zeige: 3SAT \leq_p SubsetSum

In polynom. Zeit: 3KNF $\Phi \rightarrow X \subseteq \mathbb{N}$ und $b \in \mathbb{N}$ mit:
 \exists erfüllend. Belegung von $\Phi \Leftrightarrow \exists Y \subseteq X: b = \sum_{a \in Y} a$

Bsp $\Phi = (x_1 \vee \neg x_3 \vee x_5) \wedge (\neg x_1 \vee x_5 \vee x_4) \wedge (\neg x_2 \vee \neg x_2 \vee \neg x_5)$

$v_1 :=$	100	10000	$v_1' :=$	010	10000	$b :=$	444	11111
$v_2 :=$	000	01000	$v_2' :=$	002	01000	$c_1 :=$	100	00000
$v_3 :=$	000	00100	$v_3' :=$	100	00100	$d_1 :=$	200	00000
$v_4 :=$	010	00010	$v_4' :=$	000	00010	$c_2 :=$	010	00000
$v_5 :=$	110	00001	$v_5' :=$	001	00001	$d_2 :=$	020	00000
						$c_3 :=$	001	00000

m Klauseln in n Var. $\rightarrow 2n+2m+1$ Werte à $n+m$ Dez.ziffern