14. 12. 2011

(N) ZEIT (n^k) n Input-Länge

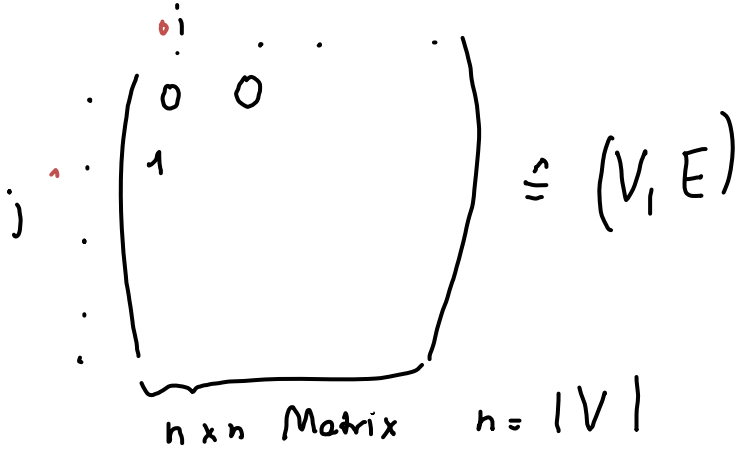
$n \mapsto n^k$ $O^{k \cdot l} \hat{=} \ast l$ Länge l

Kodiere $l \in \mathbb{N}$ " $\log(l)$ ←

Beispiele für Probleme in P

Def (V, E) ist ein (gerichteter) Graph: $V \neq \emptyset$

$E \subseteq V \times V \setminus \{(v,v) \mid v \in V\}$

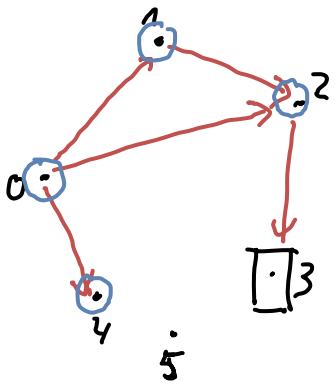


$\hat{=} (V, E)$

$n \times n$ Matrix $n = |V|$

$a_{ij} = 1 \Leftrightarrow (i,j) \in E$

$a_{ij} = 0 \Leftrightarrow (i,j) \notin E$

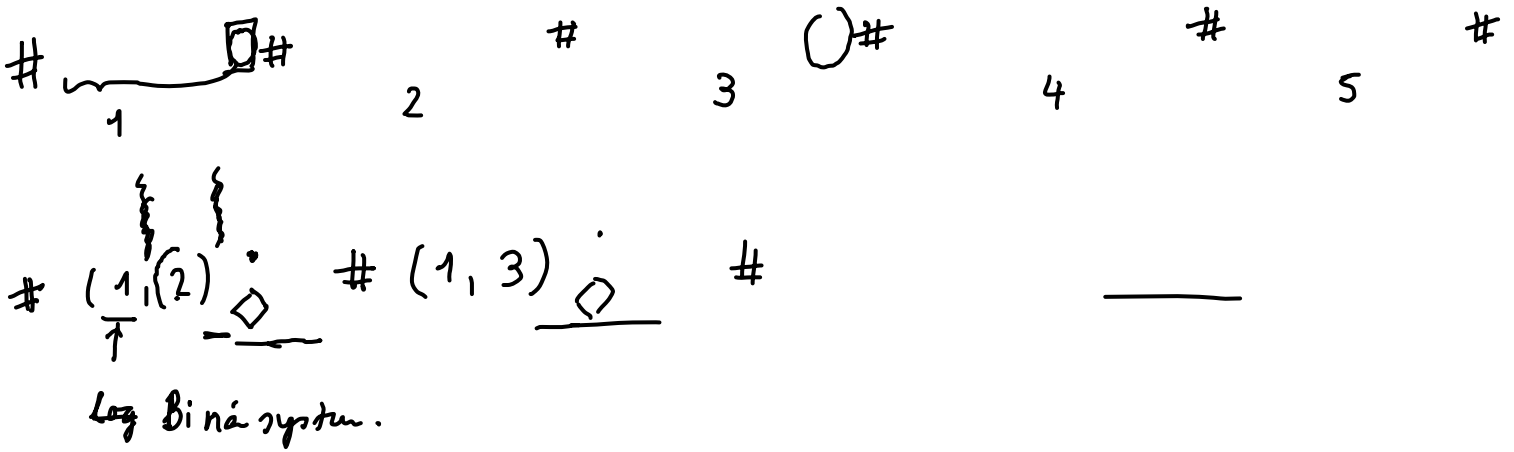


Frage: Gibt es einen Pfad von 0 nach 3 ?

PFAD

~~$A \in V$ ist machbar~~

$\hat{B}'$



Größe $O(|V|^3)$

$$PFAD = \{ (V, E, s, t) \mid (V, E) \text{ endl. Graph}, s, t \in V, \text{ es gibt in } (V, E) \text{ einen Pfad von } s \text{ nach } t \}$$

$$\exists\, n \;\; \exists\, s = s_0, \ldots, s_n = t \quad (s_i, s_{i+1}) \in E \quad i = 0, \ldots, n-1$$

$n \leq |V|$

Satz PFAD $\in P$

Beweis:

Wenn ein Input (V, E, s, t) gegeben ist, tue folgendes:

1. Setze Marke auf s
2. Betrachte alle Kanten in $E \subseteq V \times V$: Wenn $a \in V$ markiert ist und $(a, b) \in E$, dann markiere auch b ($\leq |V|$ viele Wdh.)
3. Wiederhole Punkt 2, bis kein neuer Vertex mehr hinzukommt.
4. Wenn t eine Marke trägt, dann akzeptiere (V, E, s, t).
   Sonst lehne ab.

Laufzeit: Inputgröße $\approx |V|^3 \hat{=} n$

$\leq O(n^2)$ Schritte.

Def $n, m \in \mathbb{N} \setminus \{0\}$ heißen relativ prim zueinander, gdw

die größte gemeinsame Teiler 1.

$$RELPRIM = \{ (n, m) \in (\mathbb{N} \setminus \{0\})^2 \mid n, m \text{ relativ zueinander} \}$$

Satz $RELPRIM \in P$

Beweis: $|(n, m)| \hat{=} \log(n) + \log(m) \hat{=} n$, dem Argument der Zeitkomplexitäts

funktion.

1. ~~Ersetze x durch~~ Sei $x < y$. Drehe um. ~~Sei~~
   Sei $x > y$ tue nichts

2. Ersetze x durch $\underbrace{x \bmod y}$. Gehe zu 1, falls $x \bmod y \neq 0$
   $=$ Rest von x beim Teilen durch y

   $x = q \cdot y + r \quad r < y \quad 2 \cdot \log(\max(x, y))$

3. Falls $x = q \cdot y$, $x = q \cdot y \quad q \neq 1$, da $x \neq y$

falls $x = 1$ akzeptiere den Input,
falls $x > 1$, lehne den Input ab.

(x, y) $\quad x > y$

$\vdots$

$x' = r$

$x' < y$

$x' < x - y$

$x \doteq 2^{\log x} = 2^n$

$x_0 = x$ $\quad \underline{x_0} = q \cdot y_0 + \underline{\lceil r_0 \rceil}$

$x_1 = r_0$

$(y_0 \mid r_0$

$\Leftrightarrow y_0 \mid x_0)$

$\underline{x} = q \cdot \underline{y} \qquad q \neq 1$

~~$1 = q$~~

~~$\not\Rightarrow$~~

y teilt x

$y \neq 1$

ex also einen gemeinsamen Teiler $\neq 1$ (nämlich y) von x, y

---

Induktionsbeweis: Der Algorithmus gibt die korrekten Antworten, falls er k mal die Schleife ~~2~~ aufruft. Beweis induktiv über k.

2002 : $PRIM \in P$

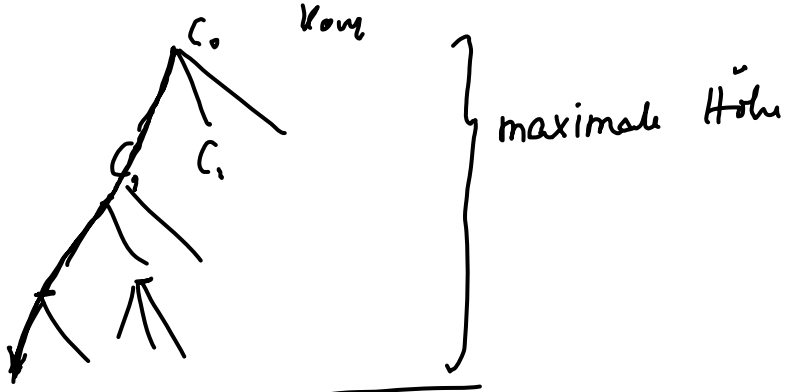
"

$\{ m \in \mathbb{N} \mid m \text{ prim} \}$

⋮

Inputlänge $\log(m)$

2.6 NP-Vollständigkeit und der Satz von Cook



Def Eine Überprüfung für eine $A \subseteq \Sigma^*$ ist ein (deterministischer) Algorithmus V zur Untersuchung von Paaren (w, c), so dass

$$A = \{ w \in \Sigma^* \mid \exists\, c,\ c \in \Gamma^* \text{ s.d. } V \text{ } (w, c) \text{ akzeptiert} \}$$

Wenn V in polynomial Zeit läuft und wenn c polynomial von $|w|$

$$n := |(w, c)| \leq |(w, \underbrace{w \ldots \ldots w}_{\text{polyn}})| \leq |w|^k$$

abhängt, dann sagen wir, dass V eine Überprüfung in polynomial Zeit ist. Ein c, s.d. V (w, c) akzeptiert, heißt Zertifikat für c.

c Suchraum: $\Gamma^{\leq p(|w|)}$ p Polyn.

$$= \{ \sigma \mid \sigma \in \Gamma^* \mid |\sigma| \leq p(|w|) \}$$

Ü

Satz NP ist die Klasse der Probleme, die eine Überprüfung in polynomial Zeit haben.

2.2 $Ü \subseteq NP$ Programm.

2.2. $NP \subseteq Ü$ Korollar des Beweises des Satzes von Cook.

$\delta(x, q)$ Menge

Def Σ Sei ein Alphabet

$\vdots$

$\{0,1\}$ z. B., $\{(,), \wedge, \vee, \neg, A, 0, 1, \bot, T\}$

$f: \Sigma^* \to \Sigma^*$ heißt in polynomialer Zeit berechenbar:

wenn es eine in polynomialer Zeit arbeitende (immer stoppende) TM,

die auf Input w hier $f(w)$ berechnet und auf das Band schreibt.

Bem: Menge $A \subseteq \Sigma^*$ ist berechenbar (Def von vor 5 Wochen) ✓ $\Leftrightarrow$ die charakteristische

Fkt χ_A ist berechenbar nach obiger Def.

$$\chi_A : \Sigma^* \to \{0,1\}$$

$$a \mapsto \begin{cases} 0 & \text{falls } a \notin A \\ 1 & \text{falls } a \in A \end{cases}$$

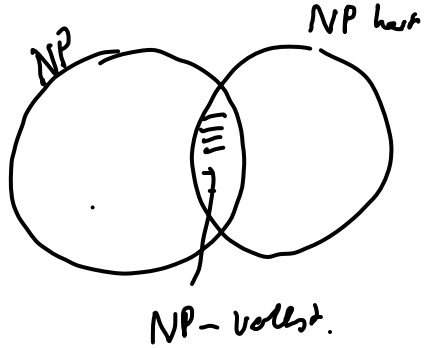
Def: $A, B \subseteq \Sigma^*$

A ist in polynomialer Zeit auf B reduzierbar (in Symbolen: $A \leq_P B$) : gdw. es eine in polynomialer Zeit ber. Fkt $f: \Sigma^* \to \Sigma^*$ gibt s.d. für alle $w \in \Sigma$ gilt:

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

Da f polynomial ber. ist, folgt: $\left(B \in P^{(N)} \text{ und } A \leq_P B\right)$

implizit $A \in P^{(N)}$.



. hart $\Leftrightarrow$ wie Nr 2)

Def: A heißt NP-vollständig : $\Leftrightarrow$

1) $A \in NP$ und

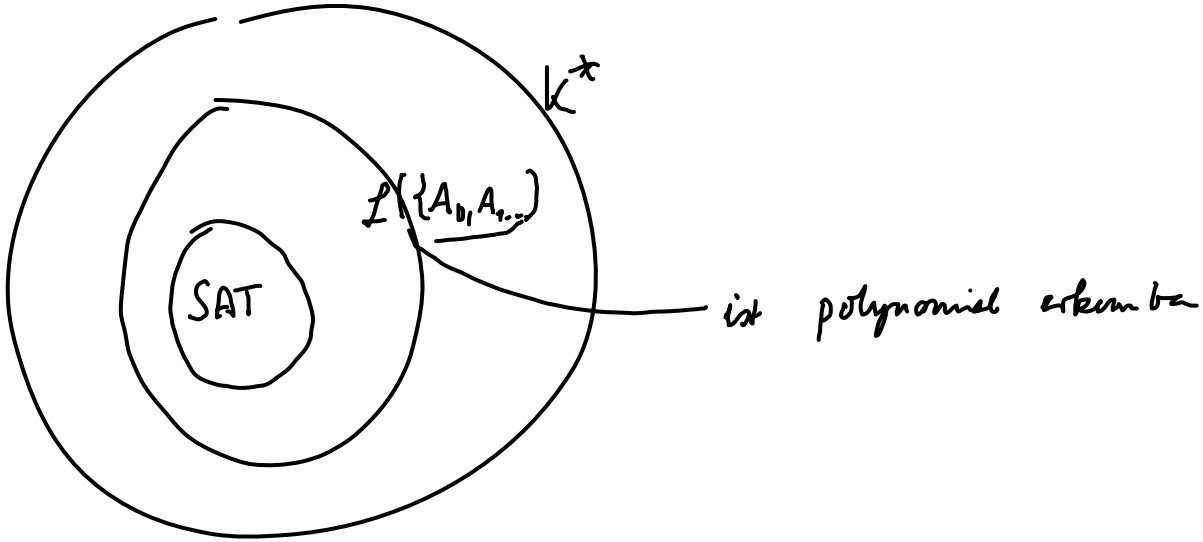
2) für jedes $C \in NP$ gilt: $C \leq_P A$.

$SAT = \{\varphi \in \mathcal{L}(\{A_0, A_1, \ldots\}) \mid \varphi \text{ ist erfüllbar}\} \subseteq \mathcal{L}(\{A_0, A_1, \ldots\})$

$\subseteq \underbrace{\{(,), A, \vee, \wedge, 0, 1, \neg\}^*}_{K}$

$\vdots$

satisfiability

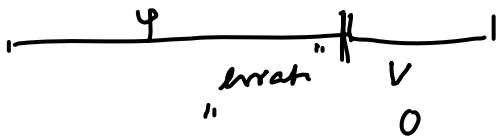


Offen: $P \neq NP$?

(äquivalent $SAT \in P$?)

Satz von Cook 1976: SAT ist NP-vollst.

Beweis: 1) $SAT \in NP$.



$\delta(\quad) = 1$

Berechn $\bar{v}(\varphi)$ (in polynomial Zeit)

)*(

(

.

.

A_i

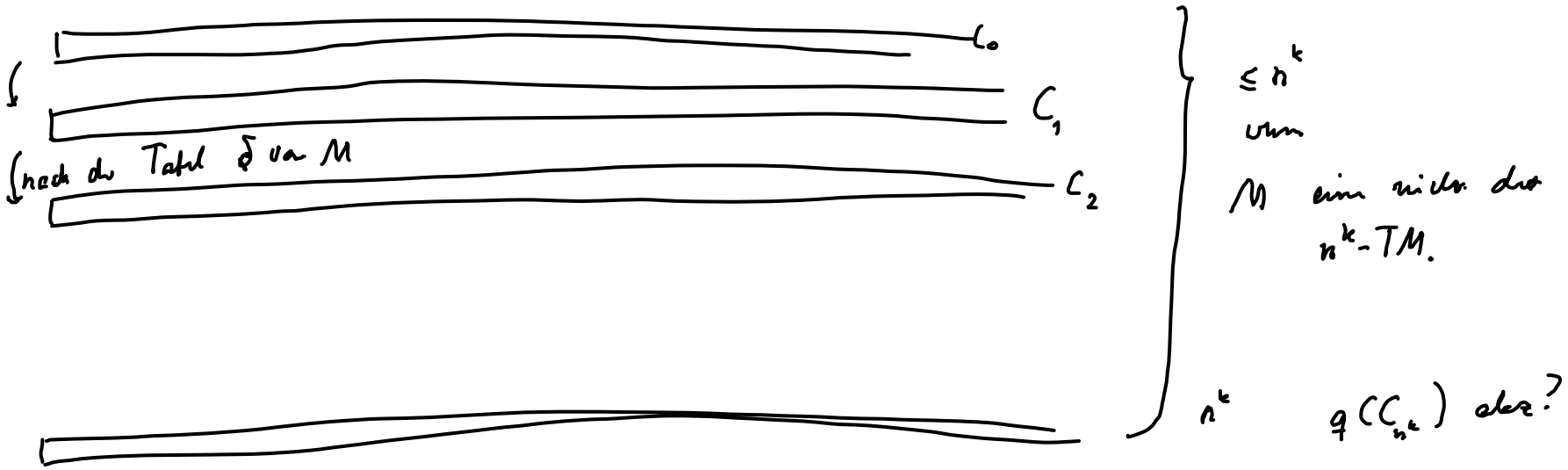
↑

log i

Sei $A \in NP$ mit einer nicht-det. polynomialen TM M_A.

Zu zeigen: $A \leq_p SAT$.

$a \in A \leftrightarrow$ $f(a)$ erfüllbare aussagenlog. Formel.



$w \in A$ wird durch M korrekt entschieden