Theoretische Informatik 3

Till Nierhoff

nierhoff@informatik.hu-berlin.de

Institut für Informatik

Humboldt-Universität zu Berlin

27. Mai 2003

Wiederholung

- $\leq_{\mathcal{P}}$ ist transitiv
- Damit kann CNF-SAT auf viele Sprachen in $\mathcal{NP}$ polynomiell reduziert werden

THEOREM COOK, S. WEGENER KAP. 3

CNF-SAT ist $\mathcal{NP}$-vollständig

$\rightarrow$ Liegt eine der Sprachen in $\mathcal{P}$, liegen alle in $\mathcal{P}$.

Wiederholung

- $\leq_{\mathcal{P}}$ ist transitiv
- Damit kann CNF-SAT auf viele Sprachen in $\mathcal{NP}$ polynomiell reduziert werden

THEOREM COOK, S. WEGENER KAP. 3

CNF-SAT ist $\mathcal{NP}$-vollständig

$\rightarrow$ Liegt eine der Sprachen in $\mathcal{P}$, liegen alle in $\mathcal{P}$.

Vermutung: $\mathcal{P} \neq \mathcal{NP}$,

also keine kann in Polynomialzeit entschieden werden

Satz von Cook

Zu zeigen:

- $\textsc{Cnf-Sat} \in \mathcal{NP}$
- $A \in \mathcal{NP} \implies A \leq_{\mathcal{P}} \textsc{Cnf-Sat}$

Satz von Cook

Zu zeigen:

- CNF-SAT $\in \mathcal{NP}$
- $A \in \mathcal{NP} \implies A \leq_{\mathcal{P}}$ CNF-SAT

Beweis ($A \in \mathcal{NP} \implies A \leq_{\mathcal{P}}$ CNF-SAT):

- Rate-TM:
  - nichtdeterministische Phase
  - Konfiguration $K_1(x) = r\Box q_0 x$, x die Eingabe
  - deterministische Phase

Satz von Cook

Zu zeigen:

- $\textsc{Cnf-Sat} \in \mathcal{NP}$
- $A \in \mathcal{NP} \implies A \leq_{\mathcal{P}} \textsc{Cnf-Sat}$

Beweis ($A \in \mathcal{NP} \implies A \leq_{\mathcal{P}} \textsc{Cnf-Sat}$):

- Rate-TM:
  - nichtdeterministische Phase
  - Konfiguration $K_1(x) = r\square q_0 x$, x die Eingabe
  - deterministische Phase
- $N = ([z], \Sigma, \Gamma, \delta, 2, \{z\})$ Rate-TM mit $L(N) = A$
  - $p(n)$-zeitbeschränkt (p ein Polynom)
  - $q_0 = 1$
  - $uzv \vdash uzv$

$\psi_x = \psi(N, x)$

- $x \in \Sigma^* \rightsquigarrow$ CNF-Formel $\psi_x = \psi(N, x)$ mit

  $\psi_x \in$ CNF-SAT $\iff K_1(x) \vdash_N^{p(|x|)} K,\ K$ eine Endkonfiguration

- $f : x \mapsto \psi_x \in \mathcal{P}$

$\psi_x = \psi(N, x)$

- $x \in \Sigma^* \rightsquigarrow$ CNF-Formel $\psi_x = \psi(N, x)$ mit

  $\psi_x \in$ CNF-SAT $\iff K_1(x) \vdash_N^{p(|x|)} K,\;$ K eine Endkonfiguration

- $f : x \mapsto \psi_x \in \mathcal{P}$
- Variablen:
  - $Q(i, k)$, $H(i, j)$, $S(i, j, \ell)$
  - mit $0 \leq i \leq p(|x|)$, $1 \leq k \leq z$, $-p(|x|) \leq j \leq p(|x|)$, $\ell \in \Gamma$

- $x \in \Sigma^* \rightsquigarrow$ CNF-Formel $\psi_x = \psi(N, x)$ mit

  $$\psi_x \in \textsc{Cnf-Sat} \iff K_1(x) \vdash_N^{p(|x|)} K,\ K \text{ eine Endkonfiguration}$$

- $f : x \mapsto \psi_x \in \mathcal{P}$
- Variablen:
  - $Q(i, k)$, $H(i, j)$, $S(i, j, \ell)$
  - mit $0 \le i \le p(|x|)$, $1 \le k \le z$, $-p(|x|) \le j \le p(|x|)$, $\ell \in \Gamma$
- Klauseln:
  - $Q(i, k)$, $H(i, j)$, $S(i, j, \ell)$ beschreiben Konfiguration ($=: K_i$)

$\psi_x = \psi(N, x)$

- $x \in \Sigma^* \rightsquigarrow$ CNF-Formel $\psi_x = \psi(N, x)$ mit

  $\psi_x \in$ CNF-SAT $\iff K_1(x) \vdash_N^{p(|x|)} K$, K eine Endkonfiguration

- $f : x \mapsto \psi_x \in \mathcal{P}$
- Variablen:
  - $Q(i, k)$, $H(i, j)$, $S(i, j, \ell)$
  - mit $0 \leq i \leq p(|x|)$, $1 \leq k \leq z$, $-p(|x|) \leq j \leq p(|x|)$, $\ell \in \Gamma$
- Klauseln:
  - $Q(i, k)$, $H(i, j)$, $S(i, j, \ell)$ beschreiben Konfiguration ($=: K_i$)
  - $Q(0, k)$, $H(0, j)$, $S(0, j, \ell)$ beschreiben $K_1(x) = r\Box q_0 x$

$\psi_x = \psi(N, x)$

- $x \in \Sigma^* \rightsquigarrow$ CNF-Formel $\psi_x = \psi(N, x)$ mit

  $\psi_x \in$ CNF-SAT $\iff K_1(x) \vdash_N^{p(|x|)} K,\ K$ eine Endkonfiguration

- $f : x \mapsto \psi_x \in \mathcal{P}$
- Variablen:
  - $Q(i, k)$, $H(i, j)$, $S(i, j, \ell)$
  - mit $0 \leq i \leq p(|x|)$, $1 \leq k \leq z$, $-p(|x|) \leq j \leq p(|x|)$, $\ell \in \Gamma$
- Klauseln:
  - $Q(i, k)$, $H(i, j)$, $S(i, j, \ell)$ beschreiben Konfiguration ($=: K_i$)
  - $Q(0, k)$, $H(0, j)$, $S(0, j, \ell)$ beschreiben $K_1(x) = r\Box q_0 x$
  - $K_{p(|x|)}$ ist Endkonfiguration

$\psi_x = \psi(N, x)$

- $x \in \Sigma^* \rightsquigarrow$ CNF-Formel $\psi_x = \psi(N, x)$ mit

  $$\psi_x \in \textsc{Cnf-Sat} \iff K_1(x) \vdash_N^{p(|x|)} K,\ K \text{ eine Endkonfiguration}$$

- $f : x \mapsto \psi_x \in \mathcal{P}$
- Variablen:
  - $Q(i, k)$, $H(i, j)$, $S(i, j, \ell)$
  - mit $0 \leq i \leq p(|x|)$, $1 \leq k \leq z$, $-p(|x|) \leq j \leq p(|x|)$, $\ell \in \Gamma$
- Klauseln:
  - $Q(i, k)$, $H(i, j)$, $S(i, j, \ell)$ beschreiben Konfiguration ($=: K_i$)
  - $Q(0, k)$, $H(0, j)$, $S(0, j, \ell)$ beschreiben $K_1(x) = r\square q_0 x$
  - $K_{p(|x|)}$ ist Endkonfiguration
  - $K_i \vdash_N K_{i+1}$