

4. ÜBUNG

1/5

Lösungsideen:

- G14: Input: x (ist ja in poly-Zeit berechenbar)
- Rate $y_1, \dots, y_{|x|}$
 - Prüfe, ob y_i paarweise verschieden
 - Prüfe, ob $y_i \in L$ (LEMP)
 - Prüfe, ob ein $y_i = x$
- } REJECT
- ANSONSTEN: ACCEPT

G16:

- a) Sei f der μ -Isomorphismus, durch μ_1 -Zeit-beschränkt.
Dann $|f(x)| \leq \mu_1(|x|)$. Da f injektiv ist, folgt
 $C_{L_1}(n) \leq C_{L_2}(\mu_1(n))$ für $|x| = n$

- b) Sei S eine dünn besetzte Sprache, d.h. $C_S(n) \leq p(n)$.
Aus $S \cong_{\mu} \text{SAT}$ folgt nach a) die Existenz eines
Polynoms g mit $C_{\text{SAT}}(n) \leq C_S(g(n)) \leq p(g(n))$.
Damit wäre also auch $C_{\text{SAT}}(n)$ Polynomiell
beschränkt, doch SAT ist nach der Vorlesung
nicht dünn besetzt! $\perp$

G15:

- a)
- Aus $P=NP$ würde folgen, daß es endliche NP -vollständige Sprachen gibt.
 - Eine endliche Sprache kann nicht bijektiv auf eine unendliche (z.B. SAT) abgebildet werden.
 - Somit: $P=NP$ widerlegt die Isomorphievermutung
 - Somit: Aus der Isomorphievermutung folgt $P \neq NP$

b) Sei x eine SAT-Formel und y ein boolesches Wort.

$$P_{SAT}(x, y) := x \wedge \underbrace{(\exists v_1 \neg \exists) \wedge u^{y_1} \wedge \dots \wedge u^{y_k}}_{\text{frische Variablen}}$$

$\underbrace{\hspace{10em}}_{\text{erlaubt Rekonstruktion von } y}$

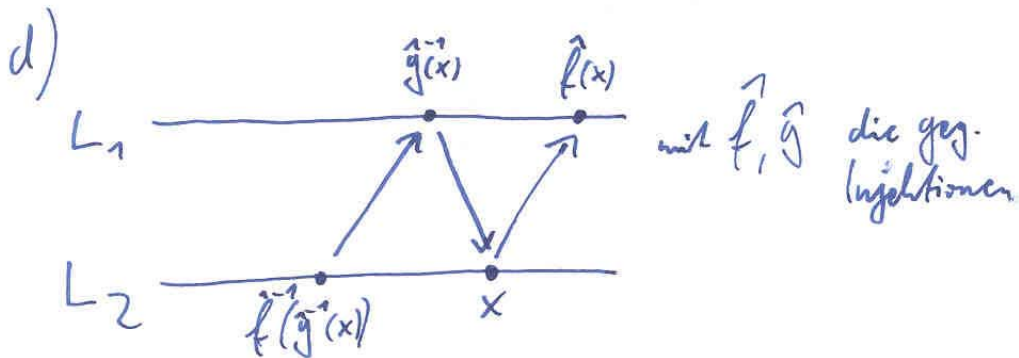
615

3/5

- c) Aus der NP-vollständigkeit folgt die Existenz einer polynomiell berechenbaren Reduktion g , welche L_1 auf L_2 reduziert.

$$f(x) := p_{L_2}(g(x), x)$$

erfüllt dann alle gewünschten Eigenschaften



Wir konstruieren:

$$h(x) := \begin{cases} \hat{f}(x) & \text{Kette endet unten} \\ \hat{g}^{-1}(x) & \text{Sonst} \end{cases}$$

"Kette endet unten": Von x aus gehen wir abwechselnd mit $\hat{g}^{-1}$ und $\hat{f}^{-1}$ zurück. Da beide Funktionen echt verlängert sind, muß diese Kette nach maximal $|x|$ -Schritten enden (entweder "oben" mit $\hat{g}^{-1}$ oder "unten" mit $\hat{f}^{-1}$).

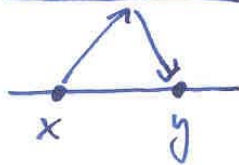


615

4/5

d) $\rightarrow$ Injektivität:- $x \neq y$ aber $h(x) = h(y)$.- Da f injektiv ist, folgt

$$h(x) = f(x) = \hat{g}(\hat{y}) = h(y)$$

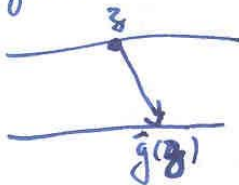


Somit liegen x und y auf der gleichen Kette. Widerspruch, da dann $h(x)$ und $h(y)$ beide durch $\hat{f}$ oder $\hat{g}$ definiert sind.

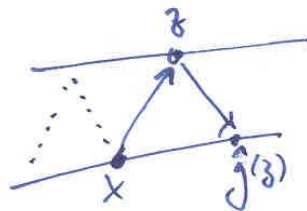
Surjektivität:

$$z \in L_2$$

1. Fall:

 z ist Ende einer Kette:dann aber $h(\hat{g}(z)) = z$

2. Fall

 z ist nicht Ende einer Kette:

dann entweder

 $h(x) = z$ oder $h(\hat{g}(z)) = z$
 je nachdem wie die Kette endet.

5/5

6 15:

e) Folgt unmittelbar aus

b), c), d)

sowie der NP-vollständigkeit von SAT.