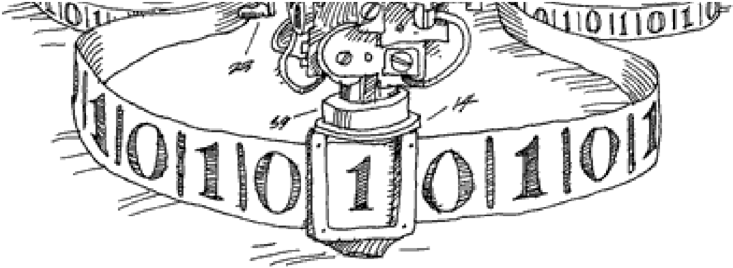
Karlsruher Institut für Technologie

Tutorium Theoretische Grundlagen der Informatik

Simon Bischof

Institut für Kryptographie und Sicherheit



Organisatorisches

- Literaturempfehlung: Michael Sipser, Introduction to the Theory of Computation; in der KIT-Bibliothek Süd im Bereich 1.0, in der Informatik-Bibliothek im Bereich D.Sip.
- Tutorium am 21.12.2012 findet normal statt
- Eulenfest: Mittwoch, 19.12.2012 ab 20:30 beim Infobau

Optimalität der Kolmogorov-Komplexität

- Sei p eine Beschreibungssprache und K_p die zugehörige Beschreibungskomplexität.
- Dann existiert ein c mit $K(w) \leq K_p(w) + c \quad (w \in \{0,1\}^*)$.

nichtkomprimierbare Strings

- Für alle $n \in \mathbb{N}_0$ gibt es nichtkomprimierbare Strings der Länge n.

nichtkomprimierbare Strings

- Für alle $n \in \mathbb{N}_0$ gibt es nichtkomprimierbare Strings der Länge n.
- Fast alle Strings sind nichtkomprimierbar
- Zufällige Strings sind mit hoher Wahrscheinlichkeit nichtkomprimierbar

nichtkomprimierbare Strings

- Für alle $n \in \mathbb{N}_0$ gibt es nichtkomprimierbare Strings der Länge n.
- Fast alle Strings sind nichtkomprimierbar
- Zufällige Strings sind mit hoher Wahrscheinlichkeit nichtkomprimierbar
- Erinnerung: Die Menge der nichtkomprimierbaren Strings ist nicht rekursiv aufzählbar

Komplexitätstheorie

Karlsruher Institut für Technologie

Laufzeit von TM

- Die TM M halte für alle Eingaben.
- $f(n) := \max_{|w|=n} (\text{Anzahl der Berechnungsschritte von } M \text{ bei Eingabe } w)$
  nennt man Laufzeit der TM M.

Die O-Notation

Seien $f, g : \mathbb{N} \to \mathbb{R}^+$. Wir schreiben

- $f \in O(g(n))$ wenn $\exists c, n_0 \in \mathbb{N} \forall n \geq n_0 : f(n) \leq c \cdot g(n)$

Die O-Notation

Karlsruher Institut für Technologie

Seien $f, g : \mathbb{N} \to \mathbb{R}^+$. Wir schreiben

- $f \in O(g(n))$ wenn $\exists c, n_0 \in \mathbb{N} \forall n \geq n_0 : f(n) \leq c \cdot g(n)$
- $f \in o(g(n))$ wenn $\forall c \in \mathbb{R}^+ \exists n_0 \in \mathbb{N}_0 \forall n \geq n_0 : f(n) < c \cdot g(n)$
- Andere Formulierung: $f \in o(g(n))$ wenn $\lim\limits_{n \to \infty} \frac{f(n)}{g(n)} = 0$.

Das Speed-Up-Theorem

- Zu jeder TM gibt es eine sprachäquivalente TM, die um einen konstanten Faktor schneller ist.

Komplexitätsklassen

- Für $t : \mathbb{N} \to \mathbb{N}$ ist $\mathit{TIME}(t(n)) :=$
  $\{L | L$ ist entscheidbar durch eine TM, die bei Eingabelänge n
  $O(t(n))$ Schritte benötigt.$\}$
- Für eine Mehrband-TM M mit Laufzeit $O(t(n))$ ist
  $L(M) \in \mathit{TIME}(O(t^2(n)))$.

Laufzeit einer NTM

Karlsruher Institut für Technologie

- Sei M nichtdeterministische TM, die immer hält und $P(w)$ die Menge der Berechnungspfade bei Eingabe w.
- $f(n) := \max_{|w|=n} \min_{p \in P(w)} (\text{Länge von } p)$

Verifizierer

- Ein Verifizierer für eine Sprache A ist ein Algorithmus V mit $A = \{w | \exists c \in \Sigma^* : V \text{ akzeptiert } (w, c)\}$
- Wenn die Laufzeit von V polynomial in $|w|$: A ist polynomial verifizierbar
- c nennt man Zeuge.

Die Klasse $\mathcal{P}$

- $\mathcal{P} := \bigcup_{k \in \mathbb{N}} \mathit{TIME}(n^k)$
- effizient lösbare Sprachen

Die Klasse $\mathcal{NP}$

Karlsruher Institut für Technologie

- $\mathcal{NP}$: polynomiell verifizierbare Sprachen

Die Klasse $\mathcal{NP}$

Karlsruher Institut für Technologie

- $\mathcal{NP}$: polynomiell verifizierbare Sprachen
- $NTIME(t(n)) := \{L | L \text{ wird von einer NTM in Zeit } O(t(n)) \text{ akzeptiert}\}$
- $\mathcal{NP} = \bigcup_{k \in \mathbb{N}} NTIME(n^k)$

Die Klasse $\mathcal{NP}$

- $\mathcal{NP}$: polynomiell verifizierbare Sprachen
- $\mathit{NTIME}(t(n)) := \{L | L$ wird von einer NTM in Zeit $O(t(n))$ akzeptiert$\}$
- $\mathcal{NP} = \bigcup_{k \in \mathbb{N}} \mathit{NTIME}(n^k)$
- $\mathcal{P} \subseteq \mathcal{NP}$
- Großes Problem der theoretischen Informatik: Ist $\mathcal{P} = \mathcal{NP}$?
  (Vermutung: nein!)

Probleme in $\mathcal{P}$ bzw. $\mathcal{NP}$

In $\mathcal{P}$:

- PATH
- RELPRIME
- EULER-KREIS
- COMPOSITE

In $\mathcal{NP}$ (aber vermutlich nicht in $\mathcal{P}$):

- HAMILTON-KREIS
- CLIQUE
- SUBSET-SUM