

Theoretische Grundlagen der Informatik

Tutorium 11

Institut für Kryptographie und Sicherheit



Wiederholung: Kolmogorov Komplexität

Eine minimale Beschreibung eines Wortes w heißt Kolmogorow-Komplexität $K(w)$

- Also: $\forall d(w) : |d(w)| \geq |K(w)|$
- Die Länge von $K(w)$ ist abhängig von der Struktur von w

Falls $|K(w)| \geq |w|$ heißt das Wort unkomprimierbar.

Wiederholung: Kolmogorov Komplexität

Beispiel:

Geben Sie eine möglichst gute obere Schranke für die Kolmogorow-Komplexität von $x = 0^n$ an!

Beispiel:

Geben Sie eine möglichst gute obere Schranke für die Kolmogorow-Komplexität von $x = 0^n$ an!

- n ist die Anzahl an Nullen

Beispiel:

Geben Sie eine möglichst gute obere Schranke für die Kolmogorow-Komplexität von $x = 0^n$ an!

- n ist die Anzahl an Nullen
- n lässt sich binär kodieren mit $\log_2(n)$ viel Platz

Beispiel:

Geben Sie eine möglichst gute obere Schranke für die Kolmogorow-Komplexität von $x = 0^n$ an!

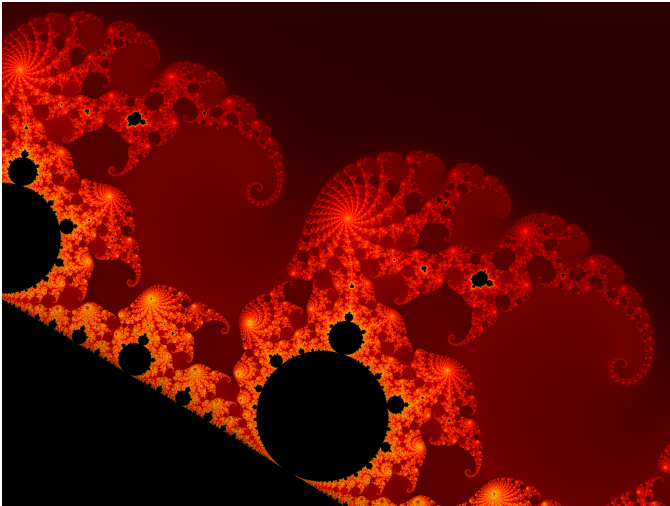
- n ist die Anzahl an Nullen
- n lässt sich binär kodieren mit $\log_2(n)$ viel Platz
- $K(x) \leq \log_2(n) + c$, wobei c die *konstante* Größe einer Turingmaschine ist, die in Bezug auf das Problem bei *jeder* möglichen Kodierung als Eingabe die Ausgabe x liefert.

Beispiel:

Geben Sie eine möglichst gute obere Schranke für die Kolmogorow-Komplexität von $x = 0^n$ an!

- n ist die Anzahl an Nullen
- n lässt sich binär kodieren mit $\log_2(n)$ viel Platz
- $K(x) \leq \log_2(n) + c$, wobei c die *konstante* Größe einer Turingmaschine ist, die in Bezug auf das Problem bei *jeder* möglichen Kodierung als Eingabe die Ausgabe x liefert.

Vorsicht: Aufpassen, in Abhängigkeit wovon eine obere Schranke angegeben werden soll.



Die Kolmogorov-Komplexität einer Zeichenkette $x \in \{0, 1\}^n$ ist immer größer als $\log_2(n)$

Das Hamilton-Kreis Problem ist NP-vollständig

In der Klasse NP liegen nicht-entscheidbare Probleme

Das Vertex-Cover Problem ist NP-vollständig

Semi-entscheidbare Sprachen sind unter Komplementbildung abgeschlossen

Nichtdeterministische endliche Automaten sind echt mächtiger als deterministische

Zu jeder CH-2-Sprache gibt es eine CH-1-Grammatik

Um zu zeigen, dass ein Problem Π NP-vollständig ist, genügt es, ein NP-schweres Problem auf Π zu reduzieren.

Kolmogorov Directions



WHEN PEOPLE ASK FOR STEP-BY-STEP DIRECTIONS, I WORRY THAT THERE WILL BE TOO MANY STEPS TO REMEMBER, SO I TRY TO PUT THEM IN MINIMAL FORM.



Dieses Werk ist unter einem "Creative Commons Namensnennung-Weitergabe unter gleichen Bedingungen 3.0 Deutschland"-Lizenzvertrag lizenziert. Um eine Kopie der Lizenz zu erhalten, gehen Sie bitte zu <http://creativecommons.org/licenses/by-sa/3.0/de/> oder schreiben Sie an Creative Commons, 171 Second Street, Suite 300, San Francisco, California 94105, USA.

Davon ausgenommen sind das Titelfeld, welches aus der März-April 2002 Ausgabe von American Scientist erschienen ist und ohne Erlaubnis verwendet wird, sowie das KIT Beamer Theme. Hierfür gelten die Bestimmungen der jeweiligen Urheber.