Literatur

Norbert Blum : Einführung in Formale Sprachen, Berechenbarkeit, Informations- und Lerntheorie. Oldenbourg-Verlag München, Wien, 2007

Juraj Hromkovic : Theoretische Informatik – Berechenbarkeit, Komplexitätstheorie, Algorithmik, Kryptographie. Eine Einführung, Teubner-Verlag, Stuttgart, 2. Aufl., 2004

Definition der Kolmogorov-Komplexität I

Definition: Die Komplexität $K_A(x)$ eines Wortes $x \in V^+$ bezüglich des Algorithmus A ist die Länge der kürzesten Eingabe $p \in \{0,1\}^+$ mit $A(p) = x$, d.h. in formalisierter Form

$$K_A(x) = \min\{|p| \mid p \in \{0,1\}^+,\ A(p) = x\}.$$

Falls kein p mit $A(p) = x$ existiert, so setzen wir $K_A(x) = \infty$.

Definition: Ein Algorithmus A_1 ist asymptotisch nicht schlechter als ein Algorithmus A_2, wenn es eine Konstante c_{A_2} so gibt, dass

$$K_{A_1}(x) \leq K_{A_2}(x) + c_{A_2}$$

für alle $x \in V^*$ gilt.

Universelle Algorithmen I

Mit $\langle M \rangle$ und $\langle w \rangle$ bezeichnen wir die Beschreibungen der Turing-Maschine $M = (X, Z, z_0, Q, \delta)$ und $w \in X^+$ durch Binärwörter.

Definition: Eine Turing-Maschine $M = (\{0,1\}, Z', z_0', Q', \delta')$ heißt universell, wenn sie für jede Eingabe $\langle N \rangle \langle w \rangle$
– den Wert $\langle f_N(w) \rangle$ berechnet, falls $f_N(w)$ definiert ist und
– nicht stoppt, falls N auf w nicht stoppt.

Satz: Es gibt universelle Turing-Maschinen.

Universelle Algorithmen II

Es sei V ein Alphabet mit mindestens zwei Buchstaben. Ferner sei $\mathcal{Z}_V$ die Menge aller Turing-Maschinen N mit $f_N : \{0,1\}^+ \to V^+$, d.h. die Maschinen aus $\mathcal{Z}_V$ stoppen nur auf nichtleeren Wörtern über $\{0,1\}$ und geben nur nichtleere Wörter über V aus.

Definition: Eine Turing-Maschine $M = (\{0,1\} \cup V, Z', z_0', Q', \delta')$ heißt universell für $\mathcal{Z}_V$, wenn sie für jede Eingabe $\langle N \rangle w$ mit $N \in \mathcal{Z}_V$ und $w \in \{0,1\}$ den Wert $f_N(w)$ berechnet.

Satz: Für jedes Alphabet V mit mindestens zwei Buchstaben gibt es für $\mathcal{Z}_V$ universelle Turing-Maschinen.

Von nun ab einfach ,,universell" anstelle von ,,universell für $\mathcal{Z}_V$"

Definition der Kolmogorov-Komplexität II

Satz: Es sei U ein universeller Algorithmus und $x \in V^*$. Dann gilt

$$K_U(x) \leq K_A(x) + c_A$$

für jeden Algorithmus A, wobei c_A eine nur von A (und nicht von x) abhängende Konstante ist (d.h. U ist asymptotisch nicht schlechter als jeder andere Algorithmus A).

Definition: Es sei U ein (fest gewählter) universeller Algorithmus. Dann definieren wir für $x \in V^+$ die Kolmogorov-Komplexität $K(x)$ durch $K(x) = K_U(x)$.

Für eine Zahl natürliche Zahl n sei $bin(n)$ die Binärdarstellung von n.

Definition: Für eine Zahl natürliche Zahl n setzen wir $K(n) = K(bin(n))$.

Eigenschaften der Kolmogorov-Komplexität I

Lemma:
Es gibt eine Konstante c derart, dass für alle $x \in \{0,1\}^+$ die Beziehung $K(x) \leq |x| + c$ gilt.

Lemma:
Für jede natürliche Zahl n gibt es eine Konstante c derart, dass

$$2^{n-c} \leq \#(\{x \mid x \in \{0,1\}^+, K(x) \leq n\}) < 2^{n+1}$$

gilt.

Folgerung:
Für jede natürliche Zahl n gibt es ein Wort $x \in \{0,1\}^+$ der Länge n mit $K(x) \geq n$.

Eigenschaften der Kolmogorov-Komplexität II

Lemma:
Für jede berechenbare Funktion f gibt es eine Konstante c_f derart, dass für alle x, für die $f(x)$ definiert ist, $K(f(x)) \leq K(x) + c_f$ gilt.

Lemma:
Für jede berechenbare Funktion $h : V^+ \to \mathbf{N}$ mit $h(x) \leq K(x)$ für alle $x \in V^+$ gibt es eine Konstante C derart, dass $h(x) \leq C$ für alle $x \in V^*$ gilt.

Folgerung:
Die Kolmogorov-Komplexität ist keine berechenbare Funktion.

Primzahlsatz

$\pi(n)$ sei die Anzahl der Primzahlen p mit $p \leq n$

A. M. Legendre (1752–1833) und C. F. Gauss (1777–1855) vermuteten, dass $\pi(n)$ angenähert $n/\ln(n)$ ist

P. L. Tschebyscheff (1821–1894) zeigte $0.929 \leq \frac{\pi(n)}{n/\ln(n)} \leq 1,106$.

J. S. Hadamard (1865–1963) und Ch. J. de la Vallee Poussin (1866–1962) bewiesen 1896, dass $\lim_{n\to\infty} \frac{\pi(n)}{n/\ln(n)} = 1$ gilt

Satz: Für unendlich viele $n \in \mathbf{N}$ gilt

$$\frac{n}{64 \log_2(n) \cdot (\log_2(\log_2(n)))^2} \leq \pi(n) \ .$$

Ein Lemma

Lemma:
Es sei $n_1, n_2, n_3, \ldots$ eine unendliche Folge natürlicher Zahlen mit den Eigenschaften

$$n_i \leq n_{i+1} \quad \text{und} \quad K(n_i) \geq \frac{\lceil \log_2(n_i) \rceil}{2}.$$

Weiterhin sei q_i, $i \geq 1$, die größte Primzahl, die die Zahl n_i teilt. Dann ist die Menge $Q = \{q_i \mid i \geq 1\}$ unendlich.