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.

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 die Kolmogorov-Komplexität $K(X)$ durch $K(x) = K_U(x)$.

Eigenschaften der Kolmogorov-Komplexität I

Lemma: Es sei $V = \{0, 1\}$.

1. Es gibt eine Konstante c derart, dass für alle $x \in \{0, 1\}^+$ die Beziehung $K(x) \leq |x| + c$ gilt.
2. Für jede natürliche Zahl n gibt es eine Konstante c derart, dass $2^{n-c} \leq \#(\{x \mid x \in \{0, 1\}^+, K(x) \leq n\}) \leq 2^{n+1}$ gilt.
3. 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.
4. Für $n \in \mathbf{N}$ sei V_n eine endliche Menge mit maximal 2^n Elementen. Ferner sei die Menge $\{(x, n) \mid x \in V_n\}$ rekursiv aufzählbar. Dann existiert eine Konstante c derart, dass dass $K(x) \leq n + c$ für alle $n \in \mathbf{N}$ und alle Elemente $x \in V_n$ gilt.

Eigenschaften der Kolmogorov-Komplexität II

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.

Eigenschaften der Kolmogorov-Komplexität III

Definition: Eine Funktion $F : V^+ \to \mathbf{N}$ heißt von oben rekursiv aufzählbar, falls es eine totale berechenbare Funktion $k : V^+ \times \mathbf{N} \to \mathbf{N}$ gibt, für die

$$k(x,0) \geq k(x,1) \geq k(x,2) \geq \ldots \text{ und } F(x) = \lim_{n \to \infty} k(x,n)$$

für alle $x \in V^+$ gelten.

Lemma: Die Kolmogorov-Komplexität ist von oben rekursiv aufzählbar.

Lemma: Es seien $K' : \{0,1\}^+ \in \mathbf{N}$ eine von oben rekursiv aufzählbare Funktion und C eine Konstante, für die $\#(\{x \mid K'(x) \leq n\}) \leq C2^n$ für alle n erfüllt ist. Dann gibt es eine Konstante c derart, dass $K(x) \leq K'(x) + c$ für alle $x \in \{0,1\}^+$ gilt.

Charakterisierung der Kolmogorov-Komplexität

Satz: Es sei $K' : \{0,1\}^* \to \mathbf{N}$ eine Funktion mit folgenden Eigenschaften:

1. Für jede berechenbare Funktion f gibt es eine Konstante c_f derart, dass
$$K'(f(x)) \leq K'(x) + c_f$$
für alle x gilt, für die $f(x)$ definiert ist.
2. Die Funktion K' ist von oben rekursiv aufzählbar.
3. Es existieren Konstanten c und C derart, dass
$$c2^n \leq \#(\{x \mid x \in \{0,1\}^+,\ K'(x) < n\}) \leq C2^n$$
für alle $n \in \mathbf{N}$ erfüllt ist.

Dann unterscheidet sich K' von der Kolmogorov-Komplexität höchstens um einen konstanten additiven Term.

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

$$\frac{n}{32\log_2(n) \cdot (\log_2(\log_2(n)))^2} \leq \pi(n) \ .$$

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.