1 verschieden Entropien – Entropie von Zeichenketten

1.1 Block-Entropie

Die Blockentropie ist die einfachste Berechnungsvorschrift, um die Zufälligkeit einer Zeichenkette auszudrücken. Kann man das nächste Zeichen sicher vorhersagen, so beträgt die Blockentropie 0, ansonsten ist sie größer 0. Der größte Entropiewert bei N Elementen wird durch gleiche Wahrscheinlichkeit der N Ergebnisse erzielt.

Wenn $P\left(W_N\right)$ die Wahrscheinlichkeit ist, ein gegebenes „Wort“ (also eine bestimmte Zeichenkette, zum Beispiel aus Nullen und Einsen oder Buchstaben) mit N Zeichen von der Quelle ausgegeben zu bekommen, dann ist die N-Block-Entropie definiert als:

$$H_N = -\sum_{\{W_N\}} P\left(W_N\right) \ln P\left(W_N\right).$$

Beispiel	Annahme	Block-Entropie	Kompression um
Würfel	$P\left(n\right) = \frac{1}{6}$ für $n = 1..6$	$H_1 = 1,79$	0 %
gezinkter Würfel	$P\left(n\right) = \frac{1}{10}$ für $n = 1..5$, $P\left(6\right) = \frac{1}{2}$	$H_1 = 1,50$	16 %
30 Buchstaben		$H_1 = 3.40$	
deutsches Alphabet	mit Buchstabenhäufigkeit	$H_1 = 2.88$	15 %
deutsches Sprache	Bibel		88 %

Tabelle 1: Zahlenbeispiele für Blockentropie (Kapitel **??**) und Kompressierbarkeit einer so erzeugten Zeichenkette (Kapitel **??**). Bei diesen Beispielen stimmt durch die Unabhängigkeit von der vorhergehenden Sequenz die Block-Entropie mit der Shannon-Entropie überein. Dies gilt nicht für die deutsche Sprache.

1.2 Shannon-Entropie

Claude Elwood Shannon verallgemeinerte diesen Begriff auch auf Zeichenketten, bei denen das nächste Zeichen statistisch von den vorhergehenden abhängt (zum Beispiel ein deutscher Text). Die Shannon-Entropie ist dabei der Grenzwert für unendlich viele bereits bekannte Zeichen und wird über die Blockentropie definiert:

$$h_{\mathrm{Sh}} = \lim_{N\to\infty} \frac{H_N}{N}$$

1.3 Kolmogorov-Sinai-Entropie

Dieses Konzept kann nun auf Trajektorien im Phasenraum erweitert werden, um dynamischen Systemen eine Entropie zuzuweisen. Dafür betrachten wir eine Trajektorie in einem begrenzten Gebiet des Phasenraumes, welches in endliche Zahl an Untergebieten unterteilt sei. Die Unterteilung sei $\mathcal{A}$. In einer Abfolge diskreter Zeiten ($t = \tau \cdot j$, $j = 1, 2, 3, \ldots$) legt die Trajektorie nun eine Sequenz fest, nämlich in welchem Gebiet sie sich jeweils zu den Messzeiten befindet. Dies ist zum Beispiel durch

Poincarè-Abbildungen realisierbar. Die Kolmogorov-Sinai-Entropie (kurz KS-Entropie) ist dann:

$$h_{\mathrm{KS}} = \sup_{\mathcal{A}} h(\mathcal{A}) = \sup_{\mathcal{A}} \frac{1}{\tau} \lim_{N\to\infty} \frac{1}{N} H_N(\mathcal{A})$$

Das heißt, sie ist der obere Grenzewert der Entropie über den Unterteilungen $\mathcal{A}$ des Phasenraumes. Praktisch ist die KS-Entropie in einzelnen Fällen berechenbar, in den meisten nur abschätzbar. Sie ist ein Maß für Chaos: in chaotischem System ist $h_{\mathrm{KS}} = \infty$. Dies entspricht einer vergleichsweise strengen Definition von Chaos.

Die KS-Entropie ist immer kleiner oder gleich der Summe aller positiven Lyapunov-Exponenten. Für typische Hamiltonische Systeme gilt sogar Gleichheit.

2 Algorithmische Komplexität

2.1 Definition

Für eine Sequenz s der Länge N ist $K_{\mathcal{M}}(\mathrm{s})$ definiert als Bitlänge des kürzesten Computerprogramms auf einem Rechner $\mathcal{M}$, welches die Sequenz produziert und danach stoppt. Dies ist bedingt abhängig vom Computer: Verschiedene Computer benötigen zwar unterschiedlich lange Programme, es gibt jedoch sogenannte „universale Rechner“, welche – bis auf eine Übersetzungsvorschrift oder einen kurzen anderen Code unabhängig von der gewünschten Sequenz – immer mit dem kürzesten Code auskommen:

$$K_{\mathcal{U}}(\mathrm{s}) \leq K_{\mathcal{M}}(\mathrm{s}) + C_{\mathcal{MU}}$$

Außerdem gilt für zwei universale Rechner $\mathcal{U}'$ und $\mathcal{U}''$, dass sich ihre Codes unabhängig von der Sequenz maximal um eine feste Anzahl Zeichen unterscheiden:

$$|K_{\mathcal{U}'}(\mathrm{s}) - K_{\mathcal{U}''}(\mathrm{s})| \leq C_{\mathcal{U}'\mathcal{U}''}$$

2.2 Kompression

Das **Shannon-Theorem** stellt nun die Entropie mit der Komplexität (also der möglichen Kompression) in Verbindung: Enthält ein Alphabet m Zeichen, so gibt h_{Sh} ein Maß für die maximale Kompression einer Zeichenkette s aus N Zeichen an:

$$K(\mathrm{s}) \geq \frac{h_{\mathrm{Sh}}}{\log m} N$$

Literatur

[1] Patrizia Castiglione, Massimo Falcioni, Annick Lesne, and Angelo Vulpiani: *Chaos and Coarse Graining in Statistical Mechanics*, Cambridge University Press, Cambridge 2008

[2] Edward Ott: *Chaos in Dynamical Systems*, Cambridge University Press, Cambridge 1993

[3] Marcus Hutter, http://www.scholarpedia.org/article/Algorithmic_complexity, Stand 7. August 2012