WOLFGANG K. SEILER
Tel. 2515

A5, C201

3. November 2004

2. Übungsblatt Kryptologie

Aufgabe 1: *(6 Punkte)*
Eine Quelle mit Alphabet $A = \{x_1, \ldots, x_n\}$ und Wahrscheinlichkeit p_i von $x_i \in A$ sende eine große Anzahl m von Zeichen aus. Dann kann man, ohne einen großen Fehler zu machen, davon ausgehen, daß das Zeichen x_i unter diesen m Zeichen $p_i m$-mal vorkommt und daß diese Zahl ganz ist. Somit können wir davon ausgehen, daß für jedes $x_i \in A$ bekannt ist, wie oft es vorkommt; unbekannt ist „nur" die Reihenfolge der Zeichen. Zeigen Sie:

a) Es gibt $\dfrac{m!}{(p_1 m)! \cdots (p_n m)!}$ verschiedene Möglichkeiten, diese Zeichen anzuordnen.

Lösung: Es gibt $N!$ Möglichkeiten, die Reihenfolge von N Buchstaben festzulegen; hiervon sind allerdings alle diejenigen uninteressant, die nur Buchstaben miteinander vertauschen, die ohnehin schon gleich sind. Für den i-ten Buchstaben, der $p_i m$-mal vorkommt, sind dies $(p_i m)!$ Stück. Somit gibt es nur $\dfrac{m!}{(p_1 m)! \cdots (p_n m)!}$ verschiedene Möglichkeiten.

b) $\lim\limits_{m\to\infty} \dfrac{1}{m} \log_2 \dfrac{m!}{(p_1 m)! \cdots (p_n m)!}$ ist gleich der Entropie der Quelle.
(Hinweis: Nach der STIRLINGschen *Formel ist* $\log_2 N! = N \log_2 N - \frac{N}{\ln 2} + \frac{\log_2 N}{2} + O(1)$, *wobei* $O(1)$ *einen Term bezeichnet, der für* $N \to \infty$ *beschränkt bleibt.)*

Lösung: Nach der STIRLINGschen Formel ist

$$\begin{aligned}
&\log_2 \frac{m!}{(p_1 m)! \cdots (p_n m)!} \\
&= m \log_2 m - (p_1 m) \log_2 (p_1 m) - \cdots - (p_n m) \log_2 (p_n m) \\
&\quad - \frac{m}{\ln 2} + \frac{p_1 m}{\ln 2} + \cdots + \frac{p_n m}{\ln 2} \\
&\quad + \frac{\log_2 m}{2} - \frac{\log_2 (p_1 m)}{2} - \cdots - \frac{\log_2 (p_n m)}{2} + O(1) \\
&= m \log_2 m (1 - p_1 - \cdots - p_n) - m (p_1 \log_2 p_1 + \cdots + p_n \log_2 p_n) - \frac{m(1 - p_1 - \cdots - p_n)}{\ln 2} \\
&\quad + \frac{1-n}{2} \log_2 m + O(1) \\
&= -m \sum_{i=1}^{n} p_i \log_2 p_i + \frac{1-n}{2} \log_2 m + O(1)\,,
\end{aligned}$$

denn $1 - \sum\limits_{i=1}^{m} p_i = 0$. Somit ist

$$\frac{1}{m} \log_2 \frac{m!}{(p_1 m)! \cdots (p_n m)!} = -\sum_{i=1}^{n} p_i \log_2 p_i + \frac{1-n}{2} \cdot \frac{\log_2 m}{m} + \frac{O(1)}{m}\,,$$

was für $m \to \infty$ gegen die Entropie $-\sum\limits_{i=1}^{m} p_i \log_2 p_i$ konvergiert.