

Informations- und Codierungstheorie
13. Übungsblatt für den 27. Jänner 2009

Wir besprechen am 27.1. auch die Beispiele 1 und 5 vom 12. Übungsblatt.

1. Sei $c_3 > c_2 > 0$. Zeigen Sie

$$\lim_{n \rightarrow \infty} (1 - 2^{-nc_2})^{2^{nc_3}} = 0.$$

2. Sei $p \in [0, \frac{1}{2}]$, sei Ω ein Wahrscheinlichkeitsraum, und seien $X : \Omega \rightarrow \{1, 2\}$, $Y : \Omega \rightarrow \{1, 2\}$ Zufallsvariablen mit

$$P[X = i \& Y = j] = \frac{1}{2}A(i, j),$$

wobei $A = \begin{pmatrix} 1-p & p \\ p & 1-p \end{pmatrix}$. Wir konstruieren nun durch $2n$ faire Münzwürfe zwei Folgen \mathbf{x}, \mathbf{y} in $\{1, 2\}^n$. Zeigen Sie, dass für die Wahrscheinlichkeit p , dass $(\mathbf{x}, \mathbf{y})^T$ gemeinsam typisch für $X \otimes Y$ zum Parameter β ist, gilt:

$$p \leq 2^{n(-I(X;Y)+\beta)}.$$

Hinweis: Das ist besser als die Schranke aus Lemma 4.37.

Aus den Sätze von Shannon kann man auch Resultate für das *diskrete Kugelpackungsproblem* herleiten.

Seien dazu $\mathbf{x} = (x_1, \dots, x_n) \in \{0, 1\}^n$ und $\mathbf{y} = (y_1, \dots, y_n) \in \{0, 1\}^n$. Die *Hamming-Distanz* von \mathbf{x} und \mathbf{y} ist definiert durch

$$d(\mathbf{x}, \mathbf{y}) = |\{i \in \{1, 2, \dots, n\} : x_i \neq y_i\}|,$$

also als die Anzahl der Stellen, an denen sich \mathbf{x} und \mathbf{y} unterscheiden.

Für einen Code $\mathcal{C} = (\mathbf{x}^{(1)}, \mathbf{x}^{(2)}, \dots, \mathbf{x}^{(s)}) \in (\{0, 1\}^n)^s$ ist die Minimaldistanz von \mathcal{C} gegeben durch

$$d_{\min}(\mathcal{C}) = \min \{d(\mathbf{x}^{(i)}, \mathbf{x}^{(j)}) \mid i \neq j\}.$$

3. Sei $n \in \mathbb{N}$, sei $p \in [0, 1]$, und sei $\varepsilon > 0$. Wir nehmen an, dass wir einen Code $\mathcal{C} = (\mathbf{x}^{(1)}, \mathbf{x}^{(2)}, \dots, \mathbf{x}^{(s)}) \in (\{0, 1\}^n)^s$ mit Minimaldistanz $d_{\min}(\mathcal{C}) \geq 2np + 1$ haben. Bauen Sie aus diesen s Codewörtern ein Übertragungssystem für Nachrichten mit $\lfloor \log_2(s) \rfloor$ Bits und n -maliger Verwendung des Kanals $\begin{pmatrix} 1 - (p - \varepsilon) & (p - \varepsilon) \\ (p - \varepsilon) & 1 - (p - \varepsilon) \end{pmatrix}$, sodass die Bitfehlerrate $p_B(n)$ die Eigenschaft $\lim_{n \rightarrow \infty} p_B(n) = 0$ erfüllt. *Hinweis:* Für große n ist es sehr unwahrscheinlich, dass np Bits bei der Übertragung umfallen.

4. (Bonus) Sei $A(n, d)$ das maximale $s \in \mathbb{N}_0$, sodass es einen binären Code der Länge n mit Minimaldistanz $\leq d$ gibt. (Bsp.: $(A(n, 0) = \infty, A(n, 1) = 2^n, A(n, n) = 2)$). Zeigen Sie

$$(1) \quad \limsup_{n \rightarrow \infty} \frac{\log_2(A(n, 2np + 1))}{n} \leq 1 - H(p).$$

Hinweis: Es reicht, dass für alle ε gilt:

$$\limsup_{n \rightarrow \infty} \frac{\log_2(A(n, 2np + 1))}{n} \leq 1 - H(p - \varepsilon).$$

5. (Bonus) Folgern Sie aus der Ungleichung (1), dass für alle $\delta \in [0, 1]$ gilt:

$$\limsup_{n \rightarrow \infty} \frac{\log_2(A(n, n\delta))}{n} \leq 1 - H\left(\frac{\delta}{2}\right).$$