Übungen zur Informationstheorie und Komplexität

Blatt 7

WS 1999/2000

1. Prove that for random variables $X^n = (X_1, \dots, X_n)$, $Y^n = (Y_1, \dots, Y_n)$, such that $X_1, \dots, X_n$ are i.i.d. and
$$\Pr\{Y^n = y^n | X^n = x^n\} = W^n(y^n|x^n) = W(y_1|x_1) \cdots W(y_n|x_n)$$
with the discrete memoryless channel W, it holds that
$$I(X^n \wedge Y^n) = nI(X_1 \wedge Y_1).$$

2. Let $W : \mathcal{X} \to \mathcal{Y}$ be a discrete memoryless channel and prove that for $\lambda \in (0,1)$ the channel capacities $C(\lambda)$ and $\bar{C}(\lambda)$, requiring maximum and averaged decoding error probability to be bounded by λ, respectively, are equal: $C(\lambda) = \bar{C}(\lambda)$.

3. Two alternative approaches to Gilbert bound. Let in the following n, d be natural numbers.

   (a) In $\{0,1\}^n$ choose M $k-tuples$ $(u_1(m), \dots, u_k(m))$, $m = 1, \dots, M$. Call this collection (a *candidate*) *bad* if for some m all $u_1(m), \dots, u_k(m)$ are within distance $d-1$ from $\{u_i(m') : m' \neq m, i = 1, \dots, k\}$. (Otherwise the candidate is *good* as then some collection $\{u_{i_m}(m) : m = 1, \dots, M\}$ is a code of minimal distance d). Show:

   - The total number of candidates is 2^{nkM}.
   - The number of bad candidates can be bounded by $M(k(M-1)|S^n_{d-1}|)^k \cdot 2^{nk(M-1)}$.
   - Conclude that there is an (n, M, d)–code with
   $$M \geq \left(\frac{2^n}{k|S^n_{d-1}|} \right)^{\frac{k}{k+1}}.$$

   (b) Choose $u_1, \dots, u_M \in \{0,1\}^n$ independently and uniformly. Position i is called *bad* if u_i is within distance $d-1$ from $\{u_1, \dots, u_{i-1}, u_{i+1}, \dots, u_M\}$.

   - Show that
   $$\Pr\{\text{Position } i \text{ is bad}\} \leq \frac{M|S^n_{d-1}|}{2^n}.$$
   - Prove that if $M < \dfrac{1}{2}\dfrac{2^n}{|S^n_{d-1}|}$ there is an (n, M, d)–code. (Hint: consider the random variable counting the number of bad positions to show that with nonzero probability less than half of the positions are bad).

Übung: Mittwoch, 16ct, in U5–135.