Informationstheorie, FS 2017
ETH Zürich, Dept. Informatik

Dr. Luis Haug
Nico Gorbach

Übungsblatt 12

Abgabe: Bis Donnerstag, 1. Juni 2017

12.1 [4 + 4 Punkte]

a) Betrachten Sie den linearen Code über $\mathbb{F}_2$, der durch die Parity-Check-Matrix

$$H = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$

definiert wird. Geben Sie für jedes mögliche Syndrom $\sigma \in \mathbb{F}_2^3$ dasjenige kompatible Fehlermuster mit geringstem Hamming-Gewicht an.

b) Gegeben sei ein linearer Code über $\mathbb{F}_2$ für einen binären symmetrischen Kanal $BSC(\varepsilon)$ mit Vertauschungswahrscheinlichkeit $\varepsilon < \frac{1}{2}$. Nehmen Sie an, dass die gesendeten Nachrichten (d.h. die Informationsvektoren $a \in \mathbb{F}_q^K$) gleichverteilt sind. Zeigen Sie, dass dann die Syndromdecodierung anhand geringsten Hamming-Gewichts einen MAP-Decodierer liefert.

12.2 [4 + 4 Punkte]

a) Sei $\mathcal{C} \subset \mathbb{F}_q^N$ ein (nicht unbedingt linearer) Code, der die Korrektur von bis zu e Fehlern erlaubt. Zeigen Sie die Abschätzung

$$M \leq \frac{q^N}{\sum_{j=0}^{e} \binom{N}{j} (q-1)^j}$$

für die Anzahl der Codewörter von $\mathcal{C}$.

b) Zeigen Sie als Anwendung von (a), dass für jedes $r > 1$ unter allen Codes mit $N = 2^r - 1$, die die Korrektur von bis zu einen Fehler erlauben, der entsprechende Hamming-Code die höchste Rate erreicht.

12.3 [8 Punkte]

Wir bezeichnen mit $M_q(N, d)$ die maximale Anzahl an Codewörtern, die ein (nicht unbedingt linearer) Code $\mathcal{C} \subset \mathbb{F}_q^N$ der Länge N und mit Minimaldistanz $\geq d$ haben kann. Zeigen Sie die Ungleichung

$$M_q(N, d) \geq \frac{q^N}{\sum_{j=0}^{d-1} \binom{N}{j} (q-1)^j}.$$

Geben Sie dazu einen Algorithmus an, der im i-ten Schritt ein Codewort aus einer Menge $\mathcal{P}^{i-1}$ potentieller Codewörter auswählt, und dann $\mathcal{P}^i$ erzeugt, indem er die nicht weiter in Frage kommenden Wörter aus $\mathcal{P}^{i-1}$ entfernt.

12.4 [8 Punkte]

Sei $\mathcal{C}$ ein Reed-Solomon-Code über $\mathbb{F}_q$ mit Parametern $\alpha \in \mathbb{F}_q$ und $t \in \mathbb{N}$, d.h. die Codewörter von $\mathcal{C}$ sind genau diejenigen $c \in \mathbb{F}_q^N$, deren Fouriertransformierte die Form $\mathcal{F}_\alpha(c) = (0, \ldots, 0, w_{2t}, \ldots, w_{N-1})$ hat. Zeigen Sie, dass $d_{\min}(\mathcal{C}) = 2t + 1$ ist.