Übungsblatt 7

Kryptographie und Kodierungstheorie
WiSe 16/17

Frohe Festtage und einen guten Rutsch ins neue Jahr wünschen Ihnen Nils-Peter Skoruppa und Michael Figelius.

Aufgabe 7.1. Bestimmen Sie alle Untervektorräume C von $\mathbb{F}_2^4$ bis auf Isomorphie und berechnen Sie jeweils $d(C)$ und $R(C)$.

Aufgabe 7.2. Welches Buch erhält man mit der ISBN-10 „3540641c35“? Sie müssen zuerst die achte Stelle c bestimmen!

Aufgabe 7.3. Zeigen Sie, dass (Σ^n, h) ein metrischer Raum ist, wobei Σ^n die Menge der Wörter der Länge n über dem Alphabet Σ ist und h den Hamming-Abstand bezeichne.

Aufgabe 7.4. Sei $B_r(c) := \{w \in \Sigma^n \mid h(c, w) \leq r\}$ der Ball um das Kodewort c mit Radius r. Zeigen Sie die Formel

$$|B_r(c)| = \sum_{i=0}^{r} \binom{n}{i} (a-1)^i,$$

wobei $a = |\Sigma|$ ist.

Aufgabe 7.5. Geben Sie eine Erzeugermatrix und eine Kontrollmatrix eines (15,11)-Hammingkodes an, d.h. einem Kode $H_{15} \subseteq \mathbb{F}_2^{15}$ mit Dimension 11, der die Eigenschaften eines Hammingkodes erfüllt. Welchen Minimalabstand hat H_{15}?

Aufgabe 7.6. Es sei $C \subset \mathbb{F}_2^n$ ein perfekter binärer Kode, der e Fehler korrigiert und den Nullvektor $0 \in C$ enthält. Es sei $\mathcal{P} := \{1, 2, \ldots, n\}$ und wir identifizieren ein Wort $v = v_1 \cdots v_n \in \mathbb{F}_2^n$ mit der Teilmenge $\mathbf{v} = \{i \in \mathcal{P} \mid v_i = 1\}$. Beweisen Sie, dass $(\mathcal{P}, \mathcal{B})$ mit $\mathcal{B} := \{\mathbf{c} \subset \mathcal{P} \mid c \in C, h(0, c) = 2e + 1\}$ ein Steiner-System $S(e + 1, 2e + 1, n)$ bildet.