

Übungsaufgaben zur Kodierungstheorie

- (4 Punkte) Begründen Sie, ob folgende Codes MDS-Codes sind:
 - der n -fache Wiederholungscode in \mathbb{F}_2^n .
 - der Code $C = \{000, 001, 010, 011\} \subset \mathbb{F}_2^3$,
 - der Code $C = \mathbb{F}_q^n$ ohne Redundanz,
 - der mittels Paritätsregel erweiterte Code $\bar{C} \subset \mathbb{F}_2^{n+1}$ (vgl. Satz 2.11) im Fall $C = \mathbb{F}_2^n$,
 - die Hamming-Codes mit $r = 2$,
 - die Hamming-Codes mit $r \geq 3$,
 - der binäre Golay-Code,
 - der ternäre Golay-Code.
- (4 Punkte) In dieser Aufgabe sollen Sie in mehreren Schritten zeigen, dass für festes q (=eine Primzahlpotenz) und für ungerades $d \in \mathbb{N}$ die Menge

$$\{n \in \mathbb{N} \mid \exists (n, |C|, d)\text{-MDS-Code}\}$$

nach oben beschränkt ist. Das bedeutet, dass die Singleton-Schranke aus Satz 9.1 für großes n (in Relation zu q und d) nicht optimal ist.

Für irgend ein $e \in \mathbb{N}$ mit $e \leq n$ ist der Ball vom Radius e um 0 in \mathbb{F}_q^n bezüglich der Hamming-Metrik die Menge $\{x \in \mathbb{F}_q^n \mid w(x) \leq e\}$. Die Anzahl seiner Elemente ist

$$V_q(n, e) := |\{x \in \mathbb{F}_q^n \mid w(x) \leq e\}| = \sum_{i=0}^e \binom{n}{i} (q-1)^i.$$

- Sei von nun an $d = 2e + 1$. Sei $C \subset \mathbb{F}_q^n$ ein $(n, |C|, d)$ -Code. Zeigen Sie

$$|C| \leq \frac{q^n}{V_q(n, e)}.$$

- Zeigen Sie, dass es zu festem q und d ein $N(q, d) > 0$ gibt, so dass für $n > N(q, d)$ gilt:

$$V_q(n, e) > q^{d-1}.$$

- Folgern Sie

$$\exists \text{ MDS-Code } C \subset \mathbb{F}_q^n \text{ mit } d(C) = d \implies n \leq N(q, d).$$

Bemerkung: Es lohnt sich, diese Aufgabe mit allen 3 oberen Schranken in Kapitel 11 in Beziehung zu setzen.

(Bitte wenden)

3. (8=1+2+1+1+2+1 Punkte) (Alternative Methoden zur Beschreibung von Reed-Solomon Codes)

Sei $\alpha := [x] \in \mathbb{F}_8 - \{0\}$ mit $\mathbb{F}_8 = \mathbb{F}_2[x]/(x^3 + x + 1)$. Wegen $\alpha \neq 1$ ist α ein Erzeugendes der zyklischen Gruppe $(\mathbb{F}_8 - \{0\}, \cdot)$.

Sei $C \subset \mathbb{F}_8^7$ der Reed-Solomon Code im engeren Sinn (also $b = 1$) der Länge $n = 7$, mit dem Erzeugenden α und mit dem designierten Abstand $\delta = n - l = 5$.

- (a) Schreiben Sie in einer Tabelle alle Potenzen $1, \alpha, \alpha^2, \dots, \alpha^6$ von α als Linearkombinationen von $1, \alpha$ und α^2 . Das erleichtert das weitere Rechnen in \mathbb{F}_8 .
- (b) Schreiben Sie das Erzeugerpolynom $g(t)$ und das Polynom $h(t)$ mit $t^7 - 1 = g(t) \cdot h(t)$ als Produkte von Linearfaktoren. Bestimmen Sie die Koeffizienten h_3, h_2, h_1 und h_0 mit $h(t) = h_3t^3 + h_2t^2 + h_1t + h_0$.
- (c) Schreiben Sie die Kontrollmatrix aus Satz 7.4 (c) zum Code C hin. Nennen Sie sie H_1 .
- (d) Schreiben Sie die Kontrollmatrix aus Lemma 10.2 (e) zum Code C hin. Nennen Sie sie H_2 . Hier lassen Sie am besten die Potenzen von α stehen (bloss mit reduzierten Exponenten zwischen 0 und 6).
- (e) In Satz 10.4 ist eine alternative Methode zur Beschreibung von Reed-Solomon Codes im engeren Sinn gegeben. Bestimmen Sie mit Hilfe dieses Satzes eine Basis (v_1, v_2, v_3) von C .
- (f) Rechnen Sie $H_1 \cdot v_j = 0$ und $H_2 \cdot v_j = 0$ für $j = 1, 2, 3$ nach.