Aufgaben zu den Themen **Duale Codes** und **Gewichtspolynome**

Aufgabe 3.1 Syndrom-Decodierer und systematische Form der Kontrollmatrix.

a) Es sei C ein binärer $[n,k,d]$-Code mit $d \geq 2e+1$ und einer Kontrollmatrix H in systematischer Form, d.h. $H = [A^T | I_{n-k}]$, wobei I_k die $k \times k$ Einheitsmatrix bezeichnet. Es sei ferner $y = c + f$ für ein $c \in C$ und $f = (f_1, \ldots, f_n)$ mit $\mathrm{wt}(f) \leq e$ und sei $s = s_H(y) = Hy^T$ das Syndrom von f. Zeigen Sie:

   (i) Ist $\mathrm{wt}(s) \leq e$, so gilt $f_1 = \ldots = f_k = 0$, d.h. die Fehler sind nur in den letzten $n-k$ Bits passiert.

   (ii) Ist $\mathrm{wt}(s) > e$, so existiert ein $i \in \{i, \ldots, k\}$ mit $f_i = 1$, d.h. es ist mindestens ein Fehler in den ersten k Bits passiert.

b) Begründen Sie den folgenden Decodier-Algorithmus (Permutations-Decodierer):

   Es sei $P = \{\pi_1 = \mathrm{id}, \pi_2, \ldots, \pi_s\} \subseteq \mathrm{Aut}(C)$ die Teilmenge der Automorphismen von C, sodass für jeden Fehlervektor f mit $\mathrm{wt}(f) \leq e$ es eine $\pi \in P$ existiert mit $(\pi f)_1 = \ldots = (\pi f)_k = 0$, d.h. πf Einsen nur in den letzten $n-k$ Bits hat.

   Es sei der Vektor y empfangen worden. Berechne $s_{(i)} = H(\pi_i y)^T$ für $\pi_i \in P$ solange, bis $\mathrm{wt}(s_{(j)}) \leq e$ ist.

   Setze $f = (\underbrace{0, \ldots, 0}_{k} | s_{(j)}^T)$ und decodiere y zu $c = \pi_j^{-1}(\pi_j y + f)$.

c) Verfassen Sie einen Permutations-Decodierer für den Hamming-Code $\mathrm{Ham}_2(7)$ mit Kontrollmatrix $H = \left(\begin{smallmatrix} 1&0&1&1&1&0&0 \\ 1&1&1&0&0&1&0 \\ 0&1&1&1&0&0&1 \end{smallmatrix}\right)$ indem Sie $P = \{\mathrm{id}, \sigma, \sigma^4\}$ nehmen. Dabei bezeichnet σ^k eine zyklische Verschiebung um k Stellen nach rechts.

Aufgabe 3.2 Es seien C der ternäre Golay-Code mit Erzeugermatrix G_{11} und $\widehat{C}$ der ternäre erweiterte Golay Code mit Erzeugermatrix G_{12}, wobei

$$G_{11} = \left(\begin{array}{ccccc|ccccc} 1 & & & & & 0 & 1 & -1 & -1 & 1 \\ & 1 & & & & 1 & 0 & 1 & -1 & -1 \\ & & 1 & & & -1 & 1 & 0 & 1 & -1 \\ & & & 1 & & -1 & -1 & 1 & 0 & 1 \\ & & & & 1 & 1 & -1 & -1 & 1 & 0 \\ & & & & & 1 & 1 & 1 & 1 & 1 \end{array}\right) \text{ und } G_{12} = \left(\begin{array}{c|c} & -1 \\ G_{11} & -1 \\ & -1 \\ & -1 \\ & -1 \\ & 0 \end{array}\right).$$

Beweisen Sie dass $\widehat{C}$ ein selbstdualer $[12,6,6]_3$-Code ist und damit C ein $[12,6,5]_3$ perfekter Code ist. (*Hinweis:* Benutzen Sie Aufgabe 3.4b)

Aufgabe 3.3 MDS-Codes

a) Es sei C ein linearer MDS-Code. Zeigen Sie, dass $C^\perp$ auch ein MDS-Code ist.

b) Es sei $K = \{a_1, \ldots, a_q\}$ ein Körper mit $q = 2^\ell$ Elementen. Beweisen Sie, dass

$$G = \begin{pmatrix} 1 & \ldots & 1 & 0 & 0 \\ a_1 & \ldots & a_q & 1 & 0 \\ a_1^2 & \ldots & a_q^2 & 0 & 1 \end{pmatrix}$$

   Erzeugermatrix eines $[q+2, 3, q]$-MDS-Codes ist.

Aufgabe 3.4 Dualität und Dividierbarkeit

a) Es sei C ein binärer 4-dividierbarer Code. Zeigen Sie, dass $C \subseteq C^{\perp}$ ist.

b) Beweisen Sie, dass ein ternärer selbstdualer Code 3-dividierbar ist.

Aufgabe 3.5 Es sei C der binäre $[7, 4, 3]$-Hamming-Code.

a) Bestimmen Sie das Gewichtspolynom von C und $\widehat{C}$.

b) Berechnen Sie für C und $\widehat{C}$ die Wahrscheinlichkeit eines unentdeckten Fehlers sowie die Decodierfehlerwahrscheinlichkeit bei Korrektur eines Fehlers, wenn zur Übertragung ein binär symmetrischer Kanal mit der Symbolfehlerwahrscheinlichkeit $p = 0.01$ benutzt wird.

Aufgabe 3.6 Es sei C ein perfekter $[n, k, d]$-Code über $\mathbb{F}_q$ mit $d = 2e + 1$.

a) Zeigen Sie: ist $q = 2$, so gilt

$$A_d = \frac{\binom{n}{e+1}}{\binom{d}{e}}$$

(*Hinweis:* Es gibt in $\mathbb{F}_2^n$ genau $\binom{n}{e+1}$ Vektoren vom Gewicht $e + 1$. Für $c \in C$ mit $\mathrm{wt}(c) = d$ betrachte man nun die Menge $\{ v \in \mathbb{F}_2^n \mid \mathrm{wt}(v) = e + 1, d(v, c) = e \}$.)

b$^{\#}$) Bestimmen Sie A_d für ein allgemeines q.

Aufgabe 3.7 Bestimmen Sie das Gewichtspolynom des binären $[23, 12, 7]$-Golay-Codes. (*Hinweis:* Benutzen Sie Aufgabe 3.6a.)

Aufgabe 3.8 Es sei C der ternäre $[11, 6, 5]$-Golay-Code.

a) Zeigen Sie, dass $\widehat{C}$ das Gewichtspolynom

$$A(x) = 1 + 264x^6 + 440x^9 + 24x^{12}$$

hat. (*Hinweis:* Benutzen Sie Bemerkung (4.5)a.)

b$^{\#}$) Berechnen Sie A_5 und A_6 der Gewichtsverteilung von C.

Aufgabe$^{\#}$ 3.9 Hamming-Codes

a) Zeigen Sie, dass $\mathrm{Ham}_3(2)$ der einzige selbstduale Hamming Code ist.

b) Bestimmen Sie alle selbstdualen erweiterten Hamming-Codes.

Aufgaben mit # sind etwas schwieriger und sind speziell für M.Sc. Studierenden gedacht. Diese Aufgaben werden in den Übungen nicht besprochen.