Aufgaben zu den Themen **Duale Codes** und **LDPC-Codes**

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 $\mathrm{Ham}_2(7)$, indem Sie $P = \{\mathrm{id}, \sigma^3, \sigma^6\}$ nehmen. Dabei bezeichnet σ^k eine zyklische Verschiebung um k Stellen nach rechts.

Aufgabe 3.2 Es sei C der binäre Code zur Konrollmatrix

$$H = \left(\begin{array}{cccccccccccccccc}
1 & 1 & 1 & 1 & & & & & & & & & & & & \\
 & & & & 1 & 1 & 1 & 1 & & & & & & & & \\
 & & & & & & & & 1 & 1 & 1 & 1 & & & & \\
 & & & & & & & & & & & & 1 & 1 & 1 & 1 \\
\hline
1 & & & & 1 & & & & 1 & & & & 1 & & & \\
 & 1 & & & & 1 & & & & 1 & & & & 1 & & \\
 & & 1 & & & & 1 & & & & 1 & & & & 1 & \\
 & & & 1 & & & & 1 & & & & 1 & & & & 1 \\
\hline
1 & & & & & 1 & & & & & 1 & & & & & 1 \\
 & 1 & & & & & 1 & & & & & 1 & 1 & & & \\
 & & 1 & & & & & 1 & 1 & & & & & 1 & & \\
 & & & 1 & 1 & & & & & 1 & & & & & 1 &
\end{array}\right).$$

a) Zeigen Sie, dass C ein $[16, 6, 6]$-Code ist.

b) Zeichnen Sie den Expander-Graphen zu H und bestimmen Sie einen möglichst großen Ausdehnungsfaktor für $\alpha = \frac{1}{4}$.

c) Decodieren Sie 1100101001100001.
   Seien Sie in der Lage, ein beliebiges Wort zu decodieren.

Aufgabe 3.3 Es seien C der ternäre Golay-Code mit Erzeugermatrix G_{11} und $\widehat{C}$ der ternäre erweiterte Golay Code mit Erzeugermatrix G_{12}, wobei

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

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 3.4 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 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 3.6 Es sei E der Expander aus Beispiel (4.5) der Vorlesung und C der zugehörige Expander-Code.

a) Zeigen Sie, dass für $\alpha = \frac{2}{9}$ jedes $\delta < \frac{3}{2}$ als Ausdehnungsfaktor gewählt werden kann.

b) Beweisen Sie, dass C ein $[9,4,4]$-Code ist.

c) Decodeiren Sie das empfangene Wort $v = 101110101$, indem Sie zunächst x_2 flippen. Der Algorithmus liefert dann ein Codewort, welches nicht notwendigerweise das Gesendete ist. Was ist der Grund?

Aufgabe$^\#$ 3.7 Hamming-Codes

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

b) Bestimmen Sie alle selbstdualen erweiterten Hamming-Codes.

Aufgabe$^\#$ 3.8 Sei $\mathrm{RM}(r,m)$ der binäre Reed-Muller-Code r-ter Ordnung.
Zeigen Sie: $\mathrm{RM}(r,m)^\perp = \mathrm{RM}(m-r-1,m)$ für alle $0 \leq r < m$.

Aufgabe 3.9 (Diese Aufgabe ist **freiwillig** und nur mit dem Rechner zu lösen.)
Es sei C der binäre Golay Code.

a) Geben Sie eine Erzeugermatrix $G = [I_{12}|A]$ und eine Kontrollmatrix $H = [A^T|I_{11}]$ in systematischer Form an und realisieren Sie den Syndrom-Decodierer für C.

b) Realisieren Sie den Permutations-Decodierer (siehe Aufgabe 3.1) für C, indem Sie

$$P = \left\{ \sigma^i \tau^j \,\middle|\, 0 \leq i \leq 22, j \in \{0,1,2,10\} \right\}$$

nehmen. Dabei bezeichnet σ die zyklische Verschiebung um eine Stelle nach rechts und $\tau : i \mapsto [12(i-1) \bmod 23]+1$, d.h. $\tau(x_1, \ldots x_{23}) = (x_1, x_{13}, x_2, x_{14}, \ldots, x_{23}, x_{12})$.

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