Aufgaben zum Thema **Zyklische Codes**

Aufgabe 5.1 Fehlerfang-Methode
Es sei C ein binärer zyklischer $[n,k]$-Code mit Kontrollmatrix H in systematischer Form, also $H = [A^T|I_{n-k}]$. Es bezeichne ferner σ die zyklische Verschiebung um eine Stelle nach rechts und für einen Vektor $y = (y_1, \ldots, y_n)$ bezeichne $s_j(y) = s_H(\sigma^j y) = H(\sigma^j y)^T$ das Syndrom von $\sigma^j y$.

a) Beweisen Sie, dass der folgende Algorithmus (genannt "Fehlerfang") alle Fehler mit Gewicht $\leq \lfloor \frac{n-1}{k} \rfloor$ sowie alle Fehler mit mindestens k nacheinander (auch zyklisch) folgenden Nullen korrigiert:

   Es sei der Vektor y empfangen. Finde nun ein $j \in \{0, \ldots, n-1\}$ mit $\mathrm{wt}(s_j) \leq \lfloor \frac{n-1}{k} \rfloor$, setze $f = (\underbrace{0, \ldots, 0}_{k} | s_j(y)^T)$ und decodiere y zu $c = \sigma^{-j}(\sigma^j y + f)$.

   (*Hinweis:* vgl. mit Aufgabe 3.1b)

b) Wie soll man den Algorithmus aus Teil a) abändern, wenn es für C keine Kontrollmatrix in systematischer Form gibt?

c) Realisieren Sie (Rechner oder Tafel) die Fehlerfang-Methode mit einem zyklischen Code ihrer Wahl.

Aufgabe 5.2 Es sei C ein binärer zyklischer Code der Länge 15 mit Erzeugerpolynom $g(x) = (1+x)m(x)$ mit $m(x) = 1 + x + x^2 + x^3 + x^4$.

a) Zeigen Sie, dass $m(x)$ irreduzibel über $\mathbb{F}_2$ ist.

b) Zeigen Sie, dass C einige Fehler von Gewicht 2 nicht erkennt, was den Satz 7.8 (ii) der Vorlesung widerspricht.

c) Finden Sie den Fehler in dem Beweis des Satzes 7.8 (ii).

Aufgabe 5.3 Zyklische Codes

a) Es sei C ein binärer Code mit Kontrollmatrix $H = [A^T|I_5]$ mit

$$A^T = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 1 \end{pmatrix}.$$

   Zeigen Sie, dass C zyklisch ist, finden Sie das Erzeuger- und das Kontrollpolynom von C und berechnen Sie die Minimaldistanz des Codes. Ist C selbstdual?

b) Es sei C ein ternärer Code mit Kontrollmatrix $H = [A^T|I_4]$ mit

$$A^T = \begin{pmatrix} 2 & 1 & 2 & 2 \\ 1 & 1 & 2 & 0 \\ 0 & 1 & 1 & 2 \\ 1 & 2 & 2 & 2 \end{pmatrix}.$$

   Zeigen Sie, dass C zyklisch ist, und finden Sie das Erzeuger- und das Kontrollpolynom von C. Berechnen Sie die Minimaldistanz des Codes.

c) Zeigen Sie, dass der quatenäre Code D aus Aufgabe 4.8b zyklisch ist, und finden Sie das Erzeuger- und das Kontrollpolynom von D.

Aufgabe 5.4 Sei $g(x)$ ein Erzeugerpolynom eines binäre zyklischen Codes. Zeigen Sie: Genau dann haben alle Codewörter gerades Gewicht, wenn $(x+1)|g(x)$.

Aufgabe 5.5 Beweisen Sie die Existenz eines binären zyklischen $[31, 6]$-Codes mit Minimaldistanz ≥ 15. (*Hinweis:* $\frac{x^{31}+1}{x+1}$ ist ein Produkt von irreduziblen Polynomen von Grad 5 über $\mathbb{F}_2$. Benutzen Sie die BCH-Schranke.)

Aufgabe 3.9 (Diese Aufgabe ist 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. $\tau(x_1, \ldots x_{23}) = (x_1, x_{13}, x_2, x_{14}, \ldots, x_{23}, x_{12})$.

Aufgabe 4.8 Quaternäre Codes

a) Es sei $C = \mathrm{Ham}_4(2)$ und $\widehat{C}$ der erweiterte Code von C. Konstruieren Sie eine Erzeugermatrix von $\widehat{C}$ (starten Sie mit einer Kontrollmatrix von C in systematischer Form) und zeigen Sie: $\widehat{C}$ ist ein $[6, 3, 4]_4$-MDS-Code, der aber nicht selbstdual ist.

b) Es sei D ein quaternärer Code mit Erzeugermatrix

$$G_D = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & x & x+1 & x+1 & x \\ 0 & x & 0 & x & x+1 & x+1 \end{pmatrix}.$$

Zeigen Sie: D ist ebenfalls ein nicht selbst-dualer $[6, 3, 4]_4$-MDS-Code. Zeigen Sie ferner, dass es keine Permutation π existiert mit $D = \pi\widehat{C}$.

c) Wir führen das hermitesche "Skalarprodukt" in $\mathbb{F}_4^6$ ein. Für $u, w \in \mathbb{F}_4^6$ definieren wir

$$\langle u, w \rangle_H = \sum_{i=1}^{6} u_i w_i^2.$$

Zeigen Sie: D ist hermitesch selbstdual (d.h. selbstdual bezüglich des hermiteschen "Skalarproduktes"). Ist auch $\widehat{C}$ hermitesch selbst-dual?

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