Aufgaben zum Thema **Zyklische Codes**

Aufgabe 4.1 Zyklische Codes

a) Es sei C der binäre 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) Es sei C der quatenäre Code mit Erzeugermatrix

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

finden Sie das Erzeuger- und das Kontrollpolynom von C.

Aufgabe 4.2 CRC-Codierung
Sei K ein Körper. Ein Polynom $m \in K[x]$ heißt *primitiv*, falls es irreduzibel ist und $\left({}^{K[x]}/_{m(x)K[x]}\right)^* = \langle x \rangle$ gilt. Sei im Folgenden $K = \mathbb{F}_2$.

a) Zeigen Sie, dass $m_1(x) = x^4 + x^3 + x^2 + x + 1$ irreduzibel aber nicht primitiv und $m_2(x) = x^4 + x + 1$ primitiv ist. (Sie dürfen auch äquivalente Definitionen von "primitiv" verwenden.)

b) Seien C_1 bzw. C_2 der zyklische $[15, 10]$-Code mit Erzeugerpolynom

$$g_1(x) = (x+1)m_1(x) \text{ bzw. } g_2(x) = (x+1)m_2(x).$$

Erklären Sie anhand dieser Codes, wie CRC-Codierung und Decodierung (Fehlererkennung) funktioniert. Zeigen Sie, dass C_1 einige Fehler von Gewicht 2 nicht erkennt.

c) Für die CRC-Codierung braucht man die tatsächlichen zyklischen Codes nicht. Benutzen Sie das Polynom $g_2(x)$ zur CRC-Codierung der Nachricht $a(x) = (10101)$, dabei soll das erzeugte "Codewort" c die Länge 10 haben. Angenommen, c wird dreimal versendet, und es sind $y_1 = c + (1111000000)$, $y_2 = c + (1000010011)$ sowie $y_3 = c + (0010010101)$ empfangen worden. Werden die Fehler in allen drei Fällen erkannt?

Aufgabe 4.3 Sei $g(x)$ ein Erzeugerpolynom eines binären zyklischen Codes C. Zeigen Sie: Genau dann haben alle Codewörter von C gerades Gewicht, wenn $(x+1)|g(x)$.

Aufgabe 4.4 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 4.5 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?

Als #-Aufgabe bleibt Aufgabe 3.9 vom Blatt 3.

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.