Aufgaben zu den Themen **Gewichtspolynome** und **Endliche Körper**

Aufgabe 4.1 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 4.2 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 4.3 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 (5.9). Das zweite Teil der Bemerkung mit $A_i = A_{n-i}$ gilt natürlich nur für binären Codes!)

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

Aufgabe 4.4 Bestimmen Sie das Gewichtspolynom des binären $[23,12,7]$-Golay-Codes. (*Hinweis:* Benutzen Sie Aufgabe 4.2a.)

Aufgabe 4.8 (Bonus-Aufgabe!) 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 selbst-dual 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

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

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

Aufgabe 4.5 Bestimmen Sie den größten gemeinsamen Teiler und die Bézout-Koeffizienten von f und g über den Körper K.

a) $K = \mathbb{F}_2$, $f(x) = x^5 + x^2 + 1$, $g(x) = x^3 + x$.

b) $K = \mathbb{F}_3$, $f(x) = x^5 + x^2 + 1$, $g(x) = x^3 + x$.

c) $K = \mathbb{F}_5$, $f(x) = x^3 + x^2 + x + 1$, $g(x) = x^2 + x$.

Aufgabe 4.6 Finden Sie alle Nustellen des gegebenen Polynoms $f(x) \in K[x]$ für den gegebenen Körper K. Schreiben Sie $f(x) = (x - \alpha_1) \cdots (x - \alpha_k) g(x)$, wobei $\alpha_1, \ldots, \alpha_k$ die Nustellen von $f(x)$ sind, und $g(x)$ **keine** Nulstellen hat. (Die α_i sind nicht unbedingt verschieden.)

Beispiel: $K = \mathbb{R}$, $f(x) = x^5 - x^4 + x^3 - x^2$.
Die Nullstellen sind 0 (zweifach) und 1, und es gilt: $f(x) = x^2(x-1)(x^2+1)$.

a) $K = \mathbb{F}_2$, $f(x) = x^6 + x^5 + x^4 + x^3 + x + 1$.

b) $K = \mathbb{F}_2$, $f(x) = x^5 + x^3 + x + 1$.

c) $K = \mathbb{F}_2$, $f(x) = x^5 + x^4 + x^3 + x^2$.

d) $K = \mathbb{F}_3$, $f(x) = x^4 + x^2 + 1$.

e) $K = \mathbb{F}_3$, $f(x) = x^6 + 2x^5 + x^4 + 2x^3 + x^2 + 2x$.

f) $K = \mathbb{F}_3$, $f(x) = x^5 + x^4 + x^3 + x^2$.

g) $K = \mathbb{F}_5$, $f(x) = x^5 + x^4 + x^3 + x^2$.

h) $K = \mathbb{F}_5$, $f(x) = x^5 + 4x$.

i) $K = \mathbb{F}_7$, $f(x) = x^6 + 3x^5 + 6x^4 + 2x^3 + 2x^2 + 6x + 2$.

j) $K = \mathbb{Q}$, $f(x) = 2x^5 + 3x^4 - 4x^3 - 7x^2 + 2$.

k) $K = \mathbb{R}$, $f(x) = 2x^5 + 3x^4 - 4x^3 - 7x^2 + 2$.

Aufgabe 4.7 Uberprüfen Sie, ob das gegebene Polynom $f \in K[x]$ irreduziebel ist. Finden Sie ein erzeugendes Element α der Multiplikativen Gruppe E^* für $E = K[x]/fK[x]$ und berechnen Sie alle Potenzen von α.

a) $K = \mathbb{F}_3$, $f(x) = x^2 + 1$.

b) $K = \mathbb{F}_2$, $f(x) = x^4 + x^3 + 1$.

c) $K = \mathbb{F}_5$, $f(x) = x^2 + x + 1$ (evtl. mit dem Rechner).

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