Übungsblatt 9

Aufgabe 1. Sei C ein linearer binärer Code der Länge n mit $C \subseteq C^\perp$. Beweisen Sie:

(a) (i) $(1,\dots,1) \in C^\perp$.

(ii) Ist C selbstdual, so gibt es für alle $i = 0,\dots,n$ eine Bijektion zwischen der Menge der Codewörter vom Gewicht i und der Menge der Codewörter vom Gewicht $n-i$.

(b) Sei C ein binärer 4-dividierbarer Code. Zeigen Sie, dass $C \subseteq C^\perp$.

Beweis. (a) (i) Sei $c = (c_1,\dots,c_n) \in C$, so gilt wegen $C \subseteq C^\perp$

$$0 = \langle c, c\rangle = \sum_{i=1}^{n} c_i^2 = \sum_{i=1}^{n} c_i = \sum_{i=1,\ c_i\neq 0}^{n} 1 = \langle c, (1,\dots,1)\rangle.$$

Folglich ist $(1,\dots,1) \in C^\perp$.

(ii) Sei $A_i := \{c \in C \mid \mathrm{wt}(c) = i\}$ die Menge der Codewörter vom Gewicht i für $0 \le i \le n$. Wegen $(1,\dots,1) \in C^\perp = C$ und $\mathrm{wt}(c) + \mathrm{wt}(c+(1,\dots,1)) = n$ für alle $c \in C$ ist die folgende Abbildung wohldefiniert

$$\varphi_i : A_i \longrightarrow A_{n-i},\ c \longmapsto c + (1,\dots,1)$$

mit $0 \le i \le n$. Wegen $\varphi_i \circ \varphi_{n-i} = \mathrm{id} = \varphi_{n-i} \circ \varphi_i$ ist φ_i auch eine Bijektion.

(b) Seien $c, d \in C$, so gilt

$$\mathrm{wt}(c+d) = \mathrm{wt}(c) + \mathrm{wt}(d) - 2|\mathrm{Tr}(c) \cap \mathrm{Tr}(d)|.$$

Da C 4-dividierbar ist, ist $|\mathrm{Tr}(c) \cap \mathrm{Tr}(d)|$ gerade. Also gilt mit $c = (c_1,\dots,c_n)$ und $d = (d_1,\dots,d_n)$

$$\langle c, d\rangle = \sum_{i=1}^{n} c_i d_i = \sum_{i \in \mathrm{Tr}(c)\cap\mathrm{Tr}(d)} 1 = |\mathrm{Tr}(c) \cap \mathrm{Tr}(d)| \cdot 1 = 0.$$

□

Aufgabe 2. (a) Konstruiere für alle k und q mit $q \equiv 0 \mod 2$ oder $q \equiv 1 \mod 4$ einen selbstdualen $[2k, k, 2]$-Code über $\mathbb{F}_q$.

(b) Sei C ein $[2k, k, d]$-Code über dem Körper K mit Erzeugermatrix $G = (E_k \mid A)$, wobei $A \in K^{k\times k}$ ist. Zeigen Sie, dass C genau dann selbstdual ist, wenn $AA^t = -E_k = A^t A$ ist.

(a) Zunächst überlegen wir uns, dass in beiden Fällen -1 ein Quadrat in $\mathbb{F}_q$ ist. Für $q \equiv 0 \mod 2$ gilt $q = 2^m$ für ein $m \in \mathbb{N}$ und somit ist $\mathbb{F}_2$ der Primkörper von $\mathbb{F}_q$. In diesem Fall gilt $-1 = 1 = 1^2$.

Ist $q \equiv 1 \mod 4$, so gilt $4 \mid q-1$. Da die Gruppe $\mathbb{F}_q^\star$ zyklisch der Ordnung $q-1$ ist, existiert ein Element $\langle a\rangle = \mathbb{F}_q^\star$ und somit können wir $x = a^{\frac{q-1}{4}}$ setzen. Das Polynom $X^2 - 1 = (X+1)(X-1)$ hat über $\mathbb{F}_q$ genau zwei Lösungen und wegen $x^2 \neq 1$ und $x^4 = 1$ folgt $x^2 = -1 \in \mathbb{F}_q$.

Sei $A = x \cdot E_k$ mit $x = 1$, wenn $q \equiv 0 \mod 2$ und für $q \equiv 1 \mod 4$ sei $x = a^{\frac{q-1}{4}}$. Sei C der Code über $\mathbb{F}_q$ mit Erzeugermatrix $G = (E_k \mid A)$, so hat C offensichtlich die Parameter $[2k, k]$. Eine Kontrollmatrix von C lautet nach dem Lemma von der Lösung 5

$$H = \left(-A^t \mid E_k\right) = \left(-A \mid E_k\right).$$

Offensichtlich gibt es zwei linear abhängige Spalten, woraus $d(C) = 2$ folgt.

Wegen $A \cdot A^t = A^t \cdot A = \mathrm{diag}(x^2,\dots,x^2) = -E_k$ ist nach (b) der Code C selbstdual.

(b) *Beweis.* Ist C selbstdual, so ist G sowohl eine Erzeuger- als auch Kontrollmatrix von C. Also gilt

$$0 = G \cdot G^t = (E_k \mid A) \begin{pmatrix} E_k \\ A^t \end{pmatrix} = E_k \cdot E_k + A \cdot A^t.$$

Also ist $A \cdot A^t = -E_k$. Da nach Satz 12.2 aus der Vorlesung auch $G' = \left(-A^t \mid E_k\right)$ sowohl eine Kontroll- als auch Erzeugermatrix von C ist, gilt analog $A^t \cdot A = -E_k$.

Ist andersherum $A \cdot A^t = -E_k$ und G eine Erzeugermatrix von C, so gilt $G \cdot G^t = A \cdot A^t + E_k = 0$, d.h. $C \subseteq \ker(G)^t = C^\perp$. Die Matrix $G' = \left(-A^t \mid E_k\right)$ ist eine Erzeugermatrix von $C^\perp$. Analog gilt somit $C^\perp \subseteq (C^\perp)^\perp = C$. □

Aufgabe 3. Zeigen Sie, dass der $[4, 2, 3]$-Hamming-Code der einzige selbstduale Hamming-Code ist.

Beweis. Eine Kontrollmatrix des $\mathrm{Ham}_3(2)$ ist

$$H = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 \end{pmatrix}$$

und eine Erzeugermatrix lautet

$$G = \begin{pmatrix} 2 & 2 & 1 & 0 \\ 2 & 1 & 0 & 1 \end{pmatrix}.$$

Die Zeilen sind paarweise und zu sich selbst orthogonal

$$\langle (2,2,1,0), (2,1,0,1) \rangle = \langle (2,2,1,0), (2,2,1,0) \rangle = \langle (2,1,0,1), (2,1,0,1) \rangle = 0,$$

d.h. $\mathrm{Ham}_3(2) \subseteq \mathrm{Sim}_3(2)$. Aus Dimensionsgründen stimmen die beiden Codes überein.
Alternativ kann man Aufgabe 2(b) benutzen, um die Selbstdualität von $\mathrm{Ham}_3(2)$ zu verifizieren.

Sei $\mathrm{Ham}_q(k)$ ein selbstdualer $[n = \frac{q^r-1}{q-1}, k, 3]$-Hamming-Code über $\mathbb{F}_q$, so sind die Parameter von $\mathrm{Ham}_q(k) = \mathrm{Sim}_q(k)$ nach Vorlesung $[n = 2k, k, 3] = [2k, k, q^{r-1}]$. Insbesondere gilt $q^{r-1} = 3$, woraus $q = 3$ und $r = 2$ folgen.

□

Lemma. *Sei C ein ternärer selbstdualer Code, so ist C 3-dividierbar.*

Beweis. Sei n die Länge von C, so gilt für $c = (c_1, \ldots, c_n) \in C$

$$0 = \langle c, c \rangle = \sum_{j=0}^{n} c_i^2 = \sum_{j=0,\ c_j \neq 0}^{n} 1 = \mathrm{wt}(c)1.$$

Somit gilt $3 \mid \mathrm{wt}(c)$. □

Aufgabe 4. Sei $\widehat{C}$ ein ternärer Code mit Erzeugermatrix

$$G = \begin{pmatrix} 1 & & & & & 1 & 1 & 1 & 1 & 1 & 0 \\ & 1 & & & & 0 & 1 & -1 & -1 & 1 & -1 \\ & & 1 & & & 1 & 0 & 1 & -1 & -1 & -1 \\ & & & 1 & & -1 & 1 & 0 & 1 & -1 & -1 \\ & & & & 1 & -1 & -1 & 1 & 0 & 1 & -1 \\ & & & & & 1 & 1 & -1 & -1 & 1 & 0 & -1 \end{pmatrix} = (E_6 \mid A)$$

Zeigen Sie:

(a) $\widehat{C}$ ist ein selbstdualer Code.

(b) $\widehat{C}$ hat die Parameter $[12, 6, 6]$.

(c) Löschen der letzten Koordinate in $\widehat{C}$ liefert einen $[11, 6, 5]$-Code C.

(d) C ist perfekt.

Beweis. (a) Die Zeilen G sind paarweise (und zu sich selbst orthogonal), d.h. $\widehat{C} \subseteq \widehat{C}^{\perp}$. Offensichtlich gilt $\dim_{\mathbb{F}_3}(\widehat{C}) = 6$ und damit $\dim_{\mathbb{F}_3}(\widehat{C}^{\perp}) = 12 - 6 = 6$. Wir erhalten somit $\widehat{C} = \widehat{C}^{\perp}$.

Alternativ gilt wegen

$$A \cdot A^t = -E_6 = A^t \cdot A$$

nach Aufgabe 2(b) die Selbstdualität von C.

(b) Offensichtlich gilt $n = 12$ und $k = 6$. Das Gewicht der ersten Zeile von G ist 6, also gilt $3 \leq d(\widehat{C}) \leq 6$.

Da $\widehat{C}$ selbstdual ist, ist G nach der Satz 12.2 aus der Vorlesung eine Kontrollmatrix von $\widehat{C}$. Die Minimaldistanz lautet somit nach Satz 8.6 aus der Vorlesung

$$d(\widehat{C}) = \min\{r \in \mathbb{N} \mid \text{ es gibt } r \text{ linear abhängige Spalten von } G\}.$$

Angenommen $d(\widehat{C}) < 6$, so existieren drei linear abhängige Spalten G_i, G_j, G_k mit $i < j < k$, d.h. $\pm G_i \pm G_j = G_k$. Es gilt $j \geq 7$, denn aus $i < j \leq 6$ würde $\pm G_i \pm G_j \neq G_k$ folgen. Direktes Nachrechnen liefert, dass eine Linearkombination der Spalten G_j, G_k für $7 \leq j < k$ keinen kanonischen Einheitsvektor liefert (keine der ersten sechs Spalten), d.h. $i \geq 6$ und somit $7 \leq i < j < k$. Allerdings bilden die letzten sechs Spalten von G, wegen $A \cdot A^t = -E_6$, eine Basis von $\mathbb{F}_3^6$ und sind daher linear unabhängig. Also gilt $d(\widehat{C}) = 6$.

(c) Offensichtlich gilt $n = 11$, $k = 6$ und $5 \leq d(C) \leq 6$. Die zweite Zeile der Matrix G hat Gewicht 6. Durch Streichen der letzten Komponente hat das entsprechende induzierte Codewort aus C Gewicht 5. Also gilt $d(C) = 5$.

(d) Wir rechnen die Kugelpackungsgleichung nach. Für $|C| = 3^6$ gilt

$$|\mathbb{F}_3^{11}| = 3^{11} = 3^6 \cdot 3^5 = 3^6 \sum_{j=0}^{2} \binom{11}{j} 2^j = |C| \sum_{j=0}^{2} \binom{11}{j} (3-1)^j.$$

□