Übungsblatt 5

Aufgabe 1. Es sei $(A,\cdot)$ eine endliche abelsche Gruppe und $\varphi : A \longrightarrow A,\ x \longmapsto x^2$. Zeigen Sie, dass

(a) φ genau dann injektiv ist, wenn $|A|$ ungerade ist.

(b) Bestimmen Sie die Anzahl der Quadrate von A, falls $|A|$ gerade ist.

(a) *Beweis.* Da A abelsch ist, ist φ ein Gruppenhomorphimsmus. Die Injektivität ist also gleichbedeutend mit $\mathrm{Kern}(\varphi) = \{1\}$. Ist die Gruppenordnung ungerade, so ist nach Lagrange die Ordnung jedes Elements ungleich zwei und somit ist der Kern trivial. Ist andersherum der Kern trivial, so besitzt A kein Element der Ordnung zwei. Da A endlich ist, folgt aus den Sylowsätzen, dass A ungerade Ordnung hat. □

(b) Nach dem Hauptsatz endlich erzeugter abelscher Gruppen gilt $A \cong \bigoplus_{i=1}^t \mathbb{Z}/p_i^{e_i}\mathbb{Z}$, wobei $t \in \mathbb{N}_0$, p_i sind Primzahlen für $1 \le i \le t$ und $e_i \in \mathbb{N}$ für $1 \le i \le t$. Beachte, dass $\bigoplus_{i=1}^t \mathbb{Z}/p_i^{e_i}\mathbb{Z}$ eine abelsche Gruppe bzgl. der Verknüpfung $+$ ist, d.h. die Menge der Quadrate ist $\left\{2x \mid x \in \bigoplus_{i=1}^t \mathbb{Z}/p_i^{e_i}\mathbb{Z}\right\}$. Nun ist genau dann $x = (x_1,\dots,x_t) \in \bigoplus_{i=1}^t \mathbb{Z}/p_i^{e_i}\mathbb{Z}$ ein Quadrat, wenn $x_i \in \mathbb{Z}/p_i^{e_i}\mathbb{Z}$ ein Quadrat für alle $1 \le i \le t$ ist. Nach der vorherigen Teilaufgabe ist für $p_i > 2$ die Anzahl der Quadrate von $\mathbb{Z}/p_i^{e_i}\mathbb{Z}$ genau $p_i^{e_i}$.

Betrachte nun die Komponenten $\mathbb{Z}/p_i^{e_i}\mathbb{Z}$ für $p_i = 2$. Sei $I \subseteq \{1,\dots,t\}$ die maximale Indexmenge mit $p_i = 2$ für $i \in I$. Da A gerade ist und $|A| = \prod_{i=1}^t p_i^{e_i}$ gilt, ist I nicht leer. Die Quadrate von $\mathbb{Z}/2^{e_i}\mathbb{Z}$ für $i \in I$ sind gerade

$$\{2x \mid x \in \mathbb{Z}/2^{e_i}\mathbb{Z}\} = \{[y] \mid 0 \le y < 2^{e_i},\ \text{y ist gerade}\},$$

wobei $[y]$ die Nebenklasse in $\mathbb{Z}/2^{e_i}\mathbb{Z}$ mit Repräsentanten y ist. Offensichtlich ist die rechte Menge in der linken enthalten. Nehme andersherum an, dass es ein $[x] \in \mathbb{Z}/2^{e_i}\mathbb{Z}$ gibt mit $2x = (2k+1) + l \cdot 2^{e_i},\ k,l \in \mathbb{Z}$ und $0 \le 2k+1 < 2^{e_i}$ (mit anderen Worten $2x \equiv 2k+1 \mod 2^{e_i}$). Wir erhalten dadurch die widersprüchliche Aussage $2(x-k) - 1 = l \cdot 2^{e_i}$.

Also besitzt die Gruppe $\mathbb{Z}/2^{e_i}\mathbb{Z}$ genau $\frac{1}{2} \cdot 2^{e_i} = 2^{e_i - 1}$ verschiedene Quadrate und somit hat A genau $\prod_{i \in I} 2^{e_i - 1} \cdot \prod_{i \in I^c} p_i^{e_i} = 2^{\sum_{i \in I}(e_i - 1)} \cdot \prod_{i \in I^c} p_i^{e_i} = \frac{|A|}{2^{|I|}}$ verschiedene Quadrate.

Aufgabe 2. (a) Wie erkennt der EAN13-Code das Vertauschen zweier Ziffern?

(b) Konstruieren Sie einen 1-fehlerkorrigierenden linearen binären (7,4)-Code mit der Eigenschaft: Das Syndrom von e_i ist gleich i in dualer Schreibweise.

(a) Für den EAN13-Code $C = \{(c_1,\dots,c_{13}) \mid \sum_{i=0}^6 c_{2i+1} + \sum_{i=1}^6 3c_{2i} = 0\}$ zeigen wir:

(1) Der Code erkennt das Vertauschen zweier Stellen mit geraden oder ungeraden Index nicht.

(2) Der Code entdeckt das Vertauschen einer Stelle mit ungeraden Index mit einer Stellle mit geraden Index, es sei denn ihre Differenz ist fünf.

Die Aussage (1) ist klar. Zu (2): Seien $c = (c_1,\dots,c_{13}) \in C$ und $1 \le i \le 13$ ungerade und $1 \le j \le 13$ gerade. So liefert der Kontrollterm des modifizierten Wortes, dessen i-te und j-te Komponenten vertauscht sind,

$$-3c_j - c_i + 3c_i + c_j = 2(c_i - c_j).$$

Letzeres ist genau dann 0, wenn $c_i - c_j \in \{0, 5\}$.

Der Fall i gerade und j ungerade lässt sich analog beweisen.

(b) Sei $H := \begin{pmatrix} a_{11} & \dots & a_{17} \\ a_{21} & \dots & a_{27} \\ a_{31} & \dots & a_{37} \end{pmatrix}$ die Kontrollmatrix eines $[7,4]_2$-Codes und es soll gelten:

$$\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} a_{11} \\ a_{21} \\ a_{31} \end{pmatrix} = He_1, \quad \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} a_{12} \\ a_{22} \\ a_{32} \end{pmatrix} = He_2, \quad \dots, \quad \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} a_{17} \\ a_{27} \\ a_{37} \end{pmatrix} = He_7.$$

Also gilt $H := \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$, d.h. die Spalten sind gerade die Zahlen eins bis sieben in der dualen Schreibweise. Nun bleibt zu zeigen, dass $C := \mathrm{Kern}(H)$ ein 1-fehlerkorrigierender $[7,4]$-Code ist.

Die Länge ist $n = 7$.

Da der Rang von H offensichtlich drei ist, ist die Dimension des Kerns C $k = 4$.

Die Minimaldistanz ist

$$d(C) = \mathrm{wt}(C) = \min\{r \in \mathbb{N} \mid \text{ es gibt } r \text{ linear abhängige Spalten in } H\} = 3.$$

Somit ist C ein $1 = \left\lfloor \frac{d(C)-1}{2} \right\rfloor$-fehlerkorrigierender Code.

Lemma. *Seien C ein $[n,k,d]$-Code über dem Körper K, $G = (I_k \mid A) \in K^{k\times n}$ und $H = \left(-A^t \mid I_{n-k}\right) \in K^{(n-k)\times n}$, wobei wir mit I die Einheitsmatrix bezeichnen. So ist genau dann G eine Erzeugermatrix von C, wenn H eine Kontrollmatrix von C ist.*

Beweis. Sei G eine Erzeugermatrix von C, so gilt wegen $H \cdot G^t = \left(-A^t \mid I_{n-k}\right) \cdot \begin{pmatrix} I_k \\ A^t \end{pmatrix} = 0$ gerade $C \subseteq \mathrm{Kern}(H)$. Wegen $\dim_K(\mathrm{Kern}(H)) = n - \mathrm{rk}(H) = n - (n-k) = k$ gilt $C = \mathrm{Kern}(H)$. Also ist H eine Kontrollmatrix von C.
Die andere Implikation lässt sich analog beweisen. □

Bemerkung. *Man kann zeigen, dass ein $[n,k]$-Code C bis auf Äquivalenz eine Erzeugermatrix der Form $G = (I_k \mid A)$ mit $A \in K^{k\times(n-k)}$ besitzt.*

Aufgabe 3. Finden Sie die Minimaldistanz eines ternären linearen Codes C mit Erzeugermatrix

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

Wir zeigen, dass die Minimaldistanz des Codes $d(C) = 3$ entspricht. Betrachte dafür die Erzeugermatrix $G' = \begin{pmatrix} 1 & 0 & 2 & 2 \\ 0 & 1 & 2 & 1 \end{pmatrix}$ von C.
Offensichtlich gilt $n = 4$ und $k = 2$. Damit induziert G' mit dem obigen Lemma die Kontrollmatrix

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

Es gilt

$$d(C) = \mathrm{wt}(C) = \min\{r \in \mathbb{N} \mid \text{ es gibt } r \text{ linear abhängige Spalten in } H\}.$$

Die Spalten von H sind paarweise linear unabhängig, aber z.B. $\begin{pmatrix} 1 \\ 1 \end{pmatrix} + 2 \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} + 2 \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} = 0$. Also ist die Minimaldistanz $d(C) = 3$. Die Parameter von C sind somit $[4,2,3]$.

Aufgabe 4. Sei $K = \{a_1, \ldots, a_q\}$ ein Körper mit $q = 2^l$ 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.

Beweis. Wegen der $q+2$ Spalten der Erzeugermatrix ist der erste Parameter $n = q+2$.
Nach Definition bilden die Zeilen ein Erzeugendensystem des linearen Codes C. Da die letzten drei Spalten linear unabhängig sind, sind es auch die drei Zeilen. Somit hat der Code die Dimension drei.
Die erste Zeile von G ist ein Codewort c mit Gewicht $\mathrm{wt}(c) = q$. Somit erhalten wir

$$d(C) = \min_{v \in C \setminus \{0\}} \mathrm{wt}(v) \leq \mathrm{wt}(c) = q.$$

Wir zeigen im Folgenden, dass $d(C) = q$ gilt. Dazu betrachten wir alle 3×3-Minoren von G. Für $1 \leq i < j < r \leq q$ und wegen der Charakteristik zwei erhalten wir also

$$\begin{vmatrix} 1 & 1 & 1 \\ a_i & a_j & a_r \\ a_i^2 & a_j^2 & a_r^2 \end{vmatrix} \neq 0, \qquad \text{(Vandermondsche Determinante)}$$

$$\begin{vmatrix} 1 & 1 & 0 \\ a_i & a_j & 0 \\ a_i^2 & a_j^2 & 1 \end{vmatrix} = \begin{vmatrix} 1 & 1 \\ a_i & a_j \end{vmatrix} = a_j - a_i \neq 0,$$

$$\begin{vmatrix} 1 & 1 & 0 \\ a_i & a_j & 1 \\ a_i^2 & a_j^2 & 0 \end{vmatrix} = \begin{vmatrix} 1 & 1 \\ a_i^2 & a_j^2 \end{vmatrix} = (a_j - a_i)^2 \neq 0 \text{ und}$$

$$\begin{vmatrix} 1 & 0 & 0 \\ a_i & 0 & 1 \\ a_i^2 & 1 & 0 \end{vmatrix} = \begin{vmatrix} 1 & 0 \\ a_i^2 & 1 \end{vmatrix} = 1.$$

Da die obigen Determinanten nicht Null sind, existiert kein Codewort ($\neq 0$) mit Gewicht kleiner oder gleich $q-1$. Mit anderen Worten die (nicht-trivialen) Codewörter haben maximal zwei Einträge gleich Null und somit ist die Minimaldistanz $d(C) = q$. Also bestitzt C die Parameter $[q+2, 3, q]$.
Offensichtlich ist C auch ein MDS-Code, denn $d(C) = q = (q+2) - 3 + 1 = n - k + 1 = n - \log_q(|C|) + 1$. $\square$