Übungsblatt 10

Aufgabe 1. Sei C ein binärer $(24, 2^{12}, 8)$-Code, der die 0 enthält. Weiter sei $\mathring{C}$ der in der letzten Koordinate punktierte Code von C.

(a) Zeigen Sie, dass $A_{11} = A_{12} = 1288$, $A_{15} = 506$, $A_{16} = 253$ und $A_{23} = 1$.

(b) Zeigen Sie, dass $4 \mid d(u, v)$ für alle $u, v \in C$.

Beweis. (a) Nach Vorlesung ist $\mathring{C}$ ein perfekter $(23, 2^{12}, 7)$-Code. Offensichtlich ist $A_0 = 1$ und wegen der Minimaldistanz $A_i = 0$ für $1 \le i \le 6$. Wir berechnen im Folgenden A_i für $7 \le i \le 23$. Da $\mathring{C}$ perfekt ist, bilden die 3–Sphären um die Codewörter eine Überdeckung des $\mathbb{F}_2^{23}$.

- Berechnung von A_7: Es gilt
$$\binom{23}{4} = A_7\binom{7}{3},$$
also $A_7 = \frac{\binom{23}{4}}{\binom{7}{3}} = 253$. Im Folgenden zählen wir die Vektoren vom Gewicht 4. Es gibt insgesamt $\binom{23}{4}$ von ihnen und sie befinden sich alle in den 3-Sphären der Codewörter vom Gewicht 7. In den jeweiligen Sphären liegen genau $\binom{7}{3}$ Vektoren vom Gewicht 4.
- Berechnung von A_8: Es gilt
$$\binom{23}{5} = A_8\binom{8}{3} + A_7\binom{7}{2},$$
also $A_8 = \frac{\binom{23}{5} - A_7\binom{7}{2}}{\binom{8}{3}} = 506$. Im Folgenden zählen wir die Vektoren vom Gewicht 5. Es gibt insgesamt $\binom{23}{5}$ viele von ihnen und sie befinden sich alle in den 3-Sphären der Codewörter vom Gewicht 7 und 8. In den 3-Sphären um Codewörter vom Gewicht 8 liegen jeweils $\binom{8}{3}$ Vektoren vom Gewicht 5. In den 3-Sphären um Codewörter vom Gewicht 7 liegen genau $\binom{7}{2}$ Vektoren vom Gewicht 5.
- Berechnung von A_9: Es gilt
$$\binom{23}{6} = A_9\binom{9}{3} + A_8\binom{8}{2} + A_7\binom{7}{1} + A_7\binom{7}{2}\binom{23-7}{1},$$
also $A_9 = 0$.
- Berechnung von A_{10}:
$$\binom{23}{7} = A_{10}\binom{10}{3} + A_9\binom{9}{2} + A_8\binom{8}{1} + A_8\binom{8}{2}\binom{23-8}{1} + A_7\binom{7}{0} + A_7\binom{7}{1}\binom{23-7}{1},$$
also $A_{10} = 0$.
- Berechnung von A_{11}:
$$\begin{aligned}\binom{23}{8} =& A_{11}\binom{11}{3} + A_{10}\binom{10}{2} + A_9\binom{9}{1} + A_9\binom{9}{2}\binom{23-9}{1} + A_8\binom{8}{0} + A_8\binom{8}{1}\binom{23-8}{1} \\ &+ A_7\binom{23-7}{1} + A_7\binom{23-7}{2}\binom{7}{1},\end{aligned}$$
also $A_{11} = 1288$.
- Berechnung von A_{12}:
$$\begin{aligned}\binom{23}{9} =& A_{12}\binom{12}{3} + A_{11}\binom{11}{2} + A_{10}\binom{10}{1} + A_{10}\binom{10}{2}\binom{23-10}{1} + A_9\binom{9}{0} + A_9\binom{9}{1}\binom{23-9}{1} \\ &+ A_8\binom{23-8}{1} + A_8\binom{23-8}{2}\binom{8}{1} + A_7\binom{23-7}{2},\end{aligned}$$
also $A_{12} = 1288$.

Dasselbe Vorgehen liefert die restlichen Werte.

(b) In der Vorlesung wurde gezeigt, dass $4 \mid \mathrm{wt}(c)$ für alle $c \in C$. Sei $u \in C$, so betrachte den Code $C' = u + C$, der dieselben Parameter wie C hat. Nun gilt mit denselben Argumenten wie aus der Vorlesung für $c' = u + v$, dass $4 \mid \mathrm{wt}(c') = d(0, c') = d(0, u + v) = d(u, v)$ für alle $v \in C$.

□

Definition. *Seien $t, v, k, \lambda \in \mathbb{N}$ und S eine Menge mit v Elementen, auch* Punkte *genannt, und $\mathcal{B}$ ein System von $k-$elementigen Teilmengen von S, auch* Blöcke *gennant. Das Paar heißt t-(v, k, λ)-*Design*, falls jede t-elementige Teilmenge S in genau λ Blöcken liegt.*

Sei $(S, \mathcal{B})$ ein t-(v, k, λ)-Design. Wir nummerieren die Punkte und Blöcke

$$S = \{s_1, \ldots, s_v\} \text{ und } \mathcal{B} = \{B_1, \ldots, B_b\}.$$

Die Matrix $M = (m_{ij})_{1 \le i \le b, 1 \le j \le v} \in \mathbb{F}_2^{b \times v}$ mit

$$m_{ij} = \begin{cases} 1 & , s_j \in B_j \\ 0 & , sonst \end{cases}$$

heißt Inzidenzmatrix *des t-(v, k, λ)-Designs $(S, \mathcal{B})$.*

Bemerkung. *Eine andere Nummerierung der Punkte und Blöcke führen zu Spalten- und Zeilenvertauschungen.*
In jeder Zeile von M stehen genau k Einsen und $v - k$ Nullen. Sei λ_1 die Anzahl der Blöcke, die einen festen vorgegebenen Punkt enthalten, so steht in der entsprechenden Spalte von M genau λ_1 Einsen und $b - \lambda_1$ Nullen. Das folgende Lemma liefert, dass die Anzahl der Einsen in den Spalten übereinstimmt.

Lemma. *Sei $(S, \mathcal{B})$ ein t-(v, k, λ)-Design, $S_j \subseteq S$ mit $|S_j| = j$, $0 \le j \le t$ und λ_j die Anzahl der Blöcke, die S_j enthalten. So gilt*

$$\lambda_j \binom{k-j}{t-j} = \lambda \binom{v-j}{t-j}.$$

Insbesondere ist λ_j unabhängig der Wahl der Punkte in S_j, $b := \lambda_0 = \lambda \frac{\binom{v}{t}}{\binom{k}{t}}$ ist die Anzahl der Blöcke des Designs und $\lambda_1 = \lambda \frac{\binom{v-1}{t-1}}{\binom{k-1}{t-1}}$ ist die Anzahl der Blöcke die einen festen Punkt enthalten.

Beweis. Im Folgenden bestimmen wir auf zwei verschiedene Arten die Anzahl aller $(t-j)$-elementigen Teilmengen von S, die disjunkt zu S_j und die in einem Block enthalten sind, der S_j beinhaltet.

Einerseits: Wähle einen Block, der S_j enthält, und wähle aus diesem Block genau $t - j$ weitere Punkte. Dies liefert $\binom{k-j}{t-j}$ Möglichkeiten. Dies führt wegen λ_j vielen Blöcken, die S_j enthalten, zu

$$\lambda_j \binom{k-j}{t-j}.$$

Andererseits: Wähle $(t-j)$ beliebige Punkte aus $S \setminus S_j$ und fasse sie in einer Menge U zusammen. Die t-elementige Menge $S_j \cup U$ liegt in genau λ vielen Blöcken. Wir erhalten somit

$$\lambda \binom{v-j}{t-j}.$$

□

Theorem. *Sei $(S, \mathcal{B})$ ein 2-(v, k, λ)-Design mit $b = v$ und $\lambda_1 = k$. So haben je zwei Blöcke genau λ gemeinsame Punkte.*

Beweis. Sei $M \in \mathbb{Z}^{v\times v}$ die Inzidenzmatrix von $(S,\mathcal{B})$ bezüglich einer Nummerierung der Punkte und Blöcke. Der Vektor Me_i gibt an, welche Blöcke den Punkt $s_i \in S$ enthält und somit gibt $(Me_i)^t(Me_j)$ die Anzahl der Blöcke an, die die Punkte $s_i, s_j \in S$ enthalten. Da ein 2-(v,k,λ)-Design gegeben ist, gilt mit $1 \le i,j \le v$

$$(M^t \cdot M)_{i,j} = (Me_i)^t(Me_j) = \begin{cases} \lambda_1 & , i = j \\ \lambda & , sonst. \end{cases}$$

Mit anderen Worten

$$M^t \cdot M = (\lambda_1 - \lambda)E_v + \lambda J,$$

wobei $J = (1)_{v\times v}$ die Einsmatrix ist. Somit erhalten wir mit $k = \lambda_1$

$$M \cdot J = kJ = \lambda_1 J = J \cdot M$$

und damit

$$M \cdot M^t = M\left((\lambda_1 - \lambda)E_v + \lambda J\right)M^{-1} = (\lambda_1 - \lambda)E_v + \lambda M \cdot J \cdot M^{-1} = (\lambda_1 - \lambda)E_v + \lambda J.$$

Mit anderen Worten gilt

$$(M \cdot M^t)_{i,j} = \begin{cases} \lambda_1 & , i = j \\ \lambda & , sonst. \end{cases}$$

Die Eigenschaft $M \cdot M^t = (\lambda_1 - \lambda)E_v + \lambda J$ heißt gerade, dass je zwei Blöcke genau λ gemeinsame Punkte besitzen.
Es fehlt noch der Nachweis der Invertierbarkeit von M. Wir zeigen dafür, dass $M^t \cdot M$ invertierbar ist. Offensichtlich ist $0 \neq \lambda_1 - \lambda$, denn nach dem obigen Lemma gilt für $t = 2$ und $j = 1$

$$\lambda_1(k-1) = \lambda(v-1).$$

Die Zahl $\lambda_1 - \lambda$ ist ein Eigenwert von $M \cdot M^t$ dessen Eigenraum die Dimension $n-1$ hat. Außerdem ist der Einsvektor ein weiterer Eigenvektor zum Eigenwert $(k + (v-1)\lambda) \neq \lambda_1 - \lambda$. Also ist $M^t M$ invertierbar und wegen der Multiplikativität der Determinante ist auch M invertierbar. □

Aufgabe 2. Zeigen Sie, dass es (bis auf Nummerierung der Punkte) genau ein 2-$(11,5,2)$-Design gibt.

Beweis. Wir untersuchen zunächst die Eindeutigkeit. Sei $(S,\mathcal{B})$ ein 2-$(11,5,2)$-Design, so gilt $b = v = 11$, $\lambda_1 = k = 5$ und $t = 2$. Wähle eine Nummerierung der Punkte und der Blöcke, sodass die erste Zeile der Inzidenzmatrix gegeben ist durch $(1,1,1,1,1,0,0,0,0,0,0)$. Nach obigen Satz haben je zwei Blöcke genau zwei gemeinsame Punkte. Nach eventueller Umnummerierung der Punkte, aber nicht der Blöcke, dürfen wir annehmen, dass die zweite Zeile $(1,1,0,0,0,1,1,1,0,0,0)$ ist. Kombinatorische Überlegungen mit Hilfe des obigen Satzes liefert die Inzidenzmatrix

$$M := \begin{pmatrix} 1&1&1&1&1&0&0&0&0&0&0 \\ 1&1&0&0&0&1&1&1&0&0&0 \\ 1&0&1&0&0&1&0&0&1&1&0 \\ 1&0&0&1&0&0&1&0&1&0&1 \\ 1&0&0&0&1&0&0&1&0&1&1 \\ 0&1&1&0&0&0&1&0&0&1&1 \\ 0&1&0&1&0&0&0&1&1&1&0 \\ 0&0&0&0&1&1&0&0&1&0&1 \\ 0&0&1&1&0&1&0&1&0&0&1 \\ 0&0&1&0&1&0&1&1&1&0&0 \\ 0&0&0&1&1&1&1&0&0&1&0 \end{pmatrix}.$$

Die Matrix M liefert insbesondere die Existenz eines 2-$(11,5,2)$-Designs. Eine ausführliche Untersuchung ist in [Eb, Section 2.8] zu finden. □

Aufgabe 3. Sei C ein erweiterter Golay-Code $\mathcal{G}_{24}$. Zeigen Sie, dass $(\Omega, \mathcal{B})$, wobei $\Omega = \{1, \dots, 24\}$ und $\mathcal{B} = \{\mathrm{Tr}(c) \mid c \in \mathcal{G}_{24},\ \mathrm{wt}(c) = 8\}$, ein 5-$(24, 8, 1)$-Design ist.

Beweis. Der binäre Code $\mathcal{G}_{24}$ ist ein perfekter $[24, 12, 8]$-Code mit $A_8 = 759$ Wörter vom Gewicht 8. Die 759 Wörter enthalten in ihren 3-Sphären alle $759\binom{8}{5} = \binom{24}{5}$ Vektoren vom Gewicht 5. Gegeben also eine 5-elementige Teilmenge U von Ω, so befindet sich der dazugehörige Vektor v mit $\mathrm{Tr}(v) = U$ in genau einer 3-Sphäre eines Codeworts c vom Gewicht 8. Also gilt $U \subseteq \mathrm{Tr}(c)$. □

Aufgabe 4. Beweisen Sie, dass der duale Code eines Reed-Solomon-Codes (bis auf Äquivalenz) auch ein Reed-Solomon-Code ist.

Beweis. Sei

$$G = \begin{pmatrix} 1 & \dots & 1 \\ a_1 & \dots & a_n \\ \vdots & & \vdots \\ a_1^{k-1} & \dots & a_n^{k-1} \end{pmatrix}$$

die Erzeugermatrix eines $[n, k, n-k+1]$ Reed-Solomon-Codes C über dem Körper mit q Elementen. Betrachte die Matrix

$$S = \begin{pmatrix} 1 & \dots & 1 \\ a_1 & \dots & a_n \\ \vdots & & \vdots \\ a_1^{n-2} & \dots & a_n^{n-2} \end{pmatrix} \in \mathbb{F}_q^{(n-1)\times n}.$$

Es gilt $\mathrm{rk}(S) = n-1$ und somit $\dim(\mathrm{Kern}(S)) = 1$. Sei $v = (v_1, \dots, v_v)^t \in \mathrm{Kern}(S) \setminus \{0\}$, so zeigen wir im Folgenden, dass $v_i \neq 0$ für alle $1 \leq i \leq n$. Angenommen, $v_i = 0$ für ein i, so entsteht durch Streichen der i-ten Spalte von S die Matrix $\widehat{S} \in \mathbb{F}_q^{(n-1)\times(n-1)}$. Es gilt $\widehat{v} = (v_1, \dots, v_{i-1}, v_{i+1}, \dots, v_n) \in \mathrm{Kern}(\widehat{S})$. Allerdings ist $\widehat{S}$ invertierbar, woraus $v = 0$ folgt.
Sei nun $v = (v_1, \dots, v_n)^t \in \mathrm{Kern}(S) \setminus \{0\}$, so gilt mit

$$M := \begin{pmatrix} v_1 & a_1 v_1 & a_1^2 v_1 & \dots & a_1^{n-k-1} v_1 \\ \vdots & & & & \vdots \\ v_n & a_n v_n & a_n^2 v_n & \dots & a_n^{n-k-1} v_n \end{pmatrix} \in \mathbb{F}_q^{n\times(n-k)}$$

gerade $G \cdot M = 0$. Die Spalten von M liegen also im $\mathrm{Kern}(G) = C^\perp$. Für die ersten $n-k$-Zeilen von M ist

$$\det \begin{pmatrix} v_1 & a_1 v_1 & a_1^2 v_1 & \dots & a_1^{n-k-1} v_1 \\ \vdots & & & & \vdots \\ v_{n-k} & a_{n-k} v_{n-k} & a_{n-k}^2 v_{n-k} & \dots & a_{n-k}^{n-k-1} v_{n-k} \end{pmatrix} = v_1 \cdots v_{n-k} \cdot \det \begin{pmatrix} 1 & a_1 & \dots & a_1^{n-k-1} \\ \vdots & & & \vdots \\ 1 & a_{n-k} & \dots & a_{n-k}^{n-k-1} \end{pmatrix} \neq 0.$$

Also ist $\mathrm{rk}(M) = n-k$. Da $\dim(C^\perp) = n-k$, bilden die Spalten von M eine Basis von $C^\perp$, d.h. $M^t = \begin{pmatrix} v_1 & \dots & v_n \\ a_1 v_1 & \dots & a_n v_n \\ \vdots & & \vdots \\ a_1^{n-k-1} v_1 & \dots & a_n^{n-k-1} v_n \end{pmatrix} \in \mathbb{F}_q^{(n-k)\times n}$ ist eine Erzeugermatrix von $C^\perp$. Da $v_i \neq 0$ für alle i, ist M^t äquivalent zu

$$\begin{pmatrix} 1 & \dots & 1 \\ a_1 & \dots & a_n \\ \vdots & & \vdots \\ a_1^{n-k-1} & \dots & a_n^{n-k-1} \end{pmatrix}$$

und somit ist $C^\perp$ äquivalent zu einem Reed-Solomon Code. □

References

[Eb] Wolfgang Ebeling, *Lattices and codes, A course partially based on lectures by Friedrich Hirzebruch*. Third edition. Advanced Lectures in Mathematics. Springer Spektrum, Wiesbaden, 2013. xvi+167 pp.