Lösung 11

Definition Sei $C \leq \mathbb{F}_\ell^N$ ein linearer Code.

- Für $S \subseteq \underline{N}$ bezeichne $\pi_S \colon \mathbb{F}_\ell^N \to \mathbb{F}_\ell^N$ die Projektion auf die Stellen in S, d.h. $\pi_S((x_1,\dots,x_N)) = (y_1\dots,y_N)$ mit $y_i = \begin{cases} x_i & \text{falls } i \in S \\ 0 & \text{falls } i \notin S \end{cases}$.
- $\operatorname{supp}(C) := \{i \in \underline{N} \mid c_i \neq 0 \text{ für ein } (c_1,\dots c_N) \in C\}$ heißt der *Support* von C.
- Der Code C heißt *zerlegbar*, falls es eine Teilmenge $\emptyset \neq S \subsetneq \operatorname{supp}(C)$ gibt so, daß $\pi_S(C)$ und $\pi_{\operatorname{supp}(C)-S}(C)$ Teilcodes von C sind. (In diesem Fall ist $C = \pi_S(C) \perp \pi_{\operatorname{supp}(C)-S}(C)$ eine nichttriviale orthogonale Zerlegung von C.) Andernfalls heißt C *unzerlegbar*.

Lemma
Zu jedem linearen Code $C \leq \mathbb{F}_\ell^N$ existiert eine (bis auf die Reihenfolge) eindeutig bestimmte Partition $\mathcal{S} = (S_1,\dots,S_r)$ von $\operatorname{supp}(C)$ so, daß $\pi_{S_i}(C) \leq C$ unzerlegbar ist für alle $1 \leq i \leq r$. Weiter ist $C = \perp_{i=1}^r \pi_{S_i}(C)$.
Beweis: Existenz: Ist C unzerlegbar, so ist nichts zu zeigen. Andernfalls existiert ein $\emptyset \neq S \subsetneq \operatorname{supp}(C)$ mit $\pi_S(C), \pi_{\operatorname{supp}(C)-S}(C) \leq C$. Dann ist $C = \pi_S(C) \perp \pi_{\operatorname{supp}(C)-S}(C)$. Jetzt iteriert man diese Zerlegung (beachte: Für $T = S$ oder $T = \operatorname{supp}(C) - S$ ist $\operatorname{supp}(\pi_T(C)) = T$). Dieses Verfahren endet, da $1 \leq |S| < \operatorname{supp}(C)$.
Eindeutigkeit: Angenommen, $\mathcal{T} = (T_1,\dots,T_t)$ sei eine weitere solche Partition von $\operatorname{supp}(C)$. Zu $1 \leq i \leq s$ definieren wir $I_i := \{1 \leq j \leq t \mid S_i \cap T_j \neq \emptyset\}$ weiter sei $C_i = \pi_{S_i}(C)$. Sicher ist $|I_i| \geq 1$. Für alle $j \in I_i$ ist $\pi_{S_i \cap T_j}(C_i) = \pi_{S_i}(\pi_{T_j}(C)) \leq \pi_{S_i}(C) = C_i$. Wegen $S_i - T_j = \bigcup_{k \in I_i - \{j\}} S_i \cap T_k$ folgt dann aber auch $\pi_{\operatorname{supp}(C_i)-(S_i \cap T_j)}(C_i) = \pi_{S_i - T_j}(C_i) \leq \bigoplus_{k \in I_i - \{j\}} \pi_{S_i \cap T_k}(C_i) \leq C_i$ stets.
Da $\pi_{S_i}(C)$ unzerlegbar ist, muß $I_j = \{i_j\}$ einelementig sein. Also gilt $S_i \subseteq T_{i_j}$ für alle i. Durch Vertauschen von $\mathcal{S}$ und $\mathcal{T}$ folgt daß auch jedes T_j in genau einem der S_i enthalten ist. Also unterscheiden sich $\mathcal{S}$ und $\mathcal{T}$ nur durch die Reihenfolge ihrer Teilmengen.

Korollar
Sei $C \leq \mathbb{F}_\ell^N$ ein unzerlegbarer linearer Code mit $\operatorname{supp}(C) = \underline{N}$. Ist $D = \{(c_1,\dots,c_k) \in \mathbb{F}_\ell^{Nk} \mid c_i \in C\}$ für ein $k \in \mathbb{N}$, so ist

$$\operatorname{Aut}(D) = \underbrace{\{D \to D,\, (c_1,\dots,c_k) \mapsto (\varphi_1(c_{\sigma(1)}),\dots,\varphi_k(c_{\sigma(k)})) \mid \sigma \in S_k, \varphi_i \in \operatorname{Aut}(C)\}}_{=:\operatorname{Aut}(C) \wr S_k \cong \operatorname{Aut}(C)^k \rtimes S_k}.$$

Beweis: Die Inklusion $\supseteq$ ist klar. Sei umgekehrt $\psi \in \operatorname{Aut}(D)$. Dann ist $\mathcal{S} := (S_1,\dots,S_k)$ mit $S_i = \{(i-1)N+1,\dots,iN\}$ die eindeutig bestimmte Partition von $\operatorname{supp}(C) = \underline{N}$ aus dem obigen Lemma. Weiter ist $(\psi(S_1),\dots,\psi(S_k))$ ebenfalls eine solche Zerlegung. Also existiert ein $\tau \in S_k$ so, daß $\psi(C_i) = C_{\tau(i)}$ stets, wobei $C_i = \pi_{S_i}(D)$. Nach dem bereits gezeigten, existiert ein $\phi \in \operatorname{Aut}(D)$ welches dieselbe Permutation τ auf den C_i induziert. Nachdem man ψ durch $\phi^{-1} \circ \psi$ ersetzt hat, gilt also $\psi(C_i) = C_i$ für alle i. Also ist $\psi|_{C_i} \in \operatorname{Aut}(C_i) \cong \operatorname{Aut}(C)$ stets. Das war zu zeigen.

Aufgabe 1.

Sei $Mass(n,\ell) := \frac{z}{n!} \prod_{j=1}^{n/2-1} (\ell^j + 1)$ mit $z = \begin{cases} 1 & \text{falls } \ell \text{ gerade} \\ 2 & \text{sonst} \end{cases}$ das Maß der selbstdualen Codes in $\mathbb{F}_\ell^{1\times n}$.

(a) Sei $\langle \alpha \rangle = \mathbb{F}_\ell^*$. Wegen $\ell \equiv_4 1$ ist $\frac{\ell-1}{2}$ gerade, also ist $-1 = \alpha^{\frac{\ell-1}{2}}$ ein Quadrat in $\mathbb{F}_\ell^*$. Sei $-1 = a^2$ mit $a \in \mathbb{F}_\ell^*$ und $C = \langle (1,a) \rangle < \mathbb{F}_\ell^{1\times 2}$. Dann ist C selbstdual. Wegen $(a,1) \notin C$ ist $\operatorname{Aut}(C)$ trivial und somit $\frac{1}{|\operatorname{Aut}(C)|} = 1 = Mass(2,\ell)$. Damit folgt die Behauptung.

(b) Sei D der $\mathbb{F}_5$-lineare Code mit Erzeugermatrix $\left(\begin{smallmatrix} 1 & 2 & 0 & 0 \\ 0 & 0 & 1 & 2 \end{smallmatrix}\right)$ (also der Wiederholungscode zu Teil (a)). Dann ist D selbstdual. Nach dem obigen Korollar ist $\operatorname{Aut}(D) = \langle (1,3)(2,4) \rangle \cong C_2$. Wegen $\frac{1}{|\operatorname{Aut}(D)|} = \frac{1}{2} = Mass(4,5)$ folgt die Behauptung.

(c) Sei C der $\mathbb{F}_3$-lineare Code mit Erzeugermatrix $\left(\begin{smallmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 2 & 1 \end{smallmatrix}\right)$. Sicher ist C selbstdual. Der Code C besitzt nur einen Vektor mit 3 Einseinträgen, nämlich $(1,1,1,0)$. Daher ist $\operatorname{Aut}(C) \leq \langle (1,2),(1,2,3)\rangle$. Die Codewörter mit 1 an der letzten Stelle sind $(2,0,1,1), (0,1,2,1), (1,2,0,1)$. Also ist $\operatorname{Aut}(C) \leq \langle (1,2,3)\rangle$. Sei $\varphi = (1,2,3)$. Wegen

$$(0,1,2,1)\varphi = (2,0,1,1) = 2(1,1,1,0) + (0,1,2,1) \in C$$

ist $\operatorname{Aut}(C) = \langle \varphi \rangle$ und somit $\frac{1}{|\operatorname{Aut}(C)|} = \frac{1}{3} = Mass(4,3)$. Damit folgt die Behauptung.

(d) Sei $D = \{(c,d) \mid c,d \in C\}$ wobei C den Code aus Teil (c) bezeichne. Sicher ist D selbstdual. Aus dem obigen Korollar ist $\operatorname{Aut}(D) \cong C_3 \wr S_2$. Wegen $\frac{1}{|\operatorname{Aut}(D)|} = \frac{1}{3^2\cdot 2} = \frac{1}{18} = Mass(8,3)$ folgt die Behauptung.

Aufgabe 2.

(a) Wir behaupten $|O_{2n}^-(\mathbb{F}_\ell)| = 2\ell^{n(n-1)}(\ell^n+1)\prod_{i=1}^{n-1}(\ell^{2i}-1)$.

Der Fall $n=1$ wurde bereits in Blatt 11 Aufgabe 3b bewiesen. Sei nun $n>1$ und $(E,q) = H \perp V$ mit $H \cong \mathbb{H}$ und $V \cong \mathbb{H}^{n-1} \perp (\mathbb{F}_{\ell^2}, N)$. Sei (h_1,h_2) eine Basis von H mit $q(h_1) = q(h_2) = 0$ und $b_q(h_1,h_2) = 1$. Für einen Teilraum F von E sei ferner $S(F) = \{x \in F - \{0\} \mid q(x) = 0\}$.

Wir setzen $U_1 = \operatorname{Stab}_{O(E,q)}(h_1)$ und $U_2 = \operatorname{Stab}_{U_1}(h_2)$. Aus dem Bahnenlemma folgt dann $|O_{2n}^-(\mathbb{F}_\ell)| = |O(E,q)\cdot h_1|\cdot|U_1| = |O(E,q)\cdot h_1|\cdot|U_1\cdot h_2|\cdot|U_2|$.

Wir bestimmen nun die drei Faktoren getrennt:

$|U_2|$: Sei $\varphi \in U_2$. Dann ist $\varphi|_H = \mathrm{id}_H$ und $\varphi(V) \perp H$. Also $\varphi(V) = V$. Damit ist $\tau\colon U_2 \to O(V)$, $\varphi \mapsto \varphi|_H$ wohldefiniert. Wegen $\varphi|_H = \mathrm{id}_H$ ist τ injektiv. Umgekehrt setzt jedes Element aus $O(V)$ nach dem Fortsetzungssatz von Witt zu einem Element in $O(E,q)$ fort. Also ist τ auch surjektiv und damit $|U_2| = |O(V)| = |O_{2(n-1)}^-(\mathbb{F}_\ell)|$.

$|U_1\cdot h_2|$: Nach dem Wittschen Fortsetzungssatz ist $U_1\cdot h_2 = \{x \in E \mid q(x) = 0 \text{ und } b_q(h_1,x) = 1\}$. Sei nun $x := ah_1 + bh_2 + v$ mit $a,b \in \mathbb{F}_\ell$ und $v \in V$. Dann gilt also

$$\begin{aligned} x \in U_1\cdot h_2 &\iff b_q(x,h_1) = 1 \text{ und } q(x) = 0 \\ &\iff b = 1 \text{ und } ab + q(v) = 0 \\ &\iff (a,b) = (-q(v),1) \end{aligned}$$

Also ist $|U_1\cdot h_2| = |V| = \ell^{2(n-1)}$.

$|O(E,q)\cdot h_1|$: Jedes Element in $S(E)$ erzeugt einen scharf primitiven Teilaum von E. Nach dem Wittschen Fortsetzungssatz folgt daher wiederum $S(E) = O(E,q)\cdot h_1$. Sei nun $x := ah_1 + bh_2 + v \in S(E)$ mit $a,b \in \mathbb{F}_\ell$ und $v \in V$. Wegen $0 = q(x) = ab + q(v)$ ist $S(E)$ die Vereinigung der folgenden drei disjukten Mengen:

$$\begin{aligned} X_1 &= \{\lambda h_i \mid i \in \{1,2\},\ \lambda \in \mathbb{F}_\ell^*\} \\ X_2 &= \{ah_1 + bh_2 + v \mid v \in S(V),\ a,b \in \mathbb{F}_\ell,\ ab = 0\} \\ X_3 &= \{ah_1 + bh_2 + v \mid v \in V,\ q(v) \neq 0,\ a,b \in \mathbb{F}_\ell,\ ab = -q(v)\} \end{aligned}$$

Also ist

$$\begin{aligned} |S(E)| &= |X_1| + |X_2| + |X_3| \\ &= 2(\ell-1) + (2\ell-1)\cdot|S(V)| + (|V| - |S(V)| - 1)\cdot(\ell-1) \\ &= \ell - 1 + |S(V)|\cdot\ell + (\ell-1)\ell^{2n-2}\,. \end{aligned}$$

Für $k \geq 1$ sei $a_k = |S((\mathbb{F}_{\ell^2},N) \perp \mathbb{H}^{k-1})|$ und wir setzen $x_k = a_k - \ell^{2k-1} + 1$. Wegen $|S(V)| = a_{k-1}$ folgt aus der soeben gezeigten Identität die Rekursionsgleichung $x_k = \ell x_{k-1}$. Da $(\mathbb{F}_{\ell^2},N)$ anisotrop ist, ist $a_1 = 0$ also $x_1 = 1-\ell$. Damit folgt

$$|S(E)| = a_n = x_n + \ell^{2n-1} - 1 = \ell^{n-1}(1-\ell) + \ell^{2n-1} - 1 = (\ell^n+1)(\ell^{n-1}-1)\,.$$

Setzen wir nun alles zusammen, so folgt wie behauptet

$$\begin{aligned} |O_{2n}^-(\mathbb{F}_\ell)| &= (\ell^n+1)(\ell^{n-1}-1)\cdot\ell^{2(n-1)}\cdot|O_{2(n-1)}^-(\mathbb{F}_\ell)| \\ &= (\ell^n+1)(\ell^{n-1}-1)\cdot\ell^{2(n-1)}\cdot 2\ell^{(n-1)(n-2)}(\ell^{n-1}+1)\prod_{i=1}^{n-2}(\ell^{2i}-1) \\ &= 2\ell^{n(n-1)}(\ell^n+1)\prod_{i=1}^{n-1}(\ell^{2i}-1) \end{aligned}$$

(b) Wir behaupten $|O_{2n+1}(\mathbb{F}_\ell)| = z\ell^{n^2}\prod_{i=1}^{n-1}(\ell^{2i}-1)$ mit $z=1$ falls ℓ gerade und $z=2$ sonst.

Sei $(E,q)\cong[1]\perp\mathbb{H}^n$. Wieder führen wir eine Induktion nach n. Im Fall $n=0$ besitzt jedes $e\in E$ nur zwei mögliche Bilder unter $O(E,q)$ nämlich e und $-e$. Also ist $O(E,q)=\{\pm\mathrm{id}_E\}$.

Sei nun $n\geq 1$. Wieder schreiben wir $(E,q)=H\perp V$ mit $H\cong\mathbb{H}$ und $V\cong[1]\perp\mathbb{H}^{n-1}$. Sei (h_1,h_2) eine Basis von H mit $q(h_1)=q(h_2)=0$ und $b_q(h_1,h_2)=1$. Für einen Teilraum F von E sei ferner $S(F)=\{x\in F-\{0\}\mid q(x)=0\}$.

Wir setzen $U_1=\mathrm{Stab}_{O(E,q)}(h_1)$ und $U_2=\mathrm{Stab}_{U_1}(h_2)$. Dann folgt wiederum $|O_{2n+1}(\mathbb{F}_\ell)| = |O(E,q)\cdot h_1|\cdot|U_1\cdot h_2|\cdot|U_2|$ mit $|U_2|=|O_{2n-1}(\mathbb{F}_\ell)|$ und $|U_1\cdot h_1|=|V|=\ell^{2n-1}$. Es verbleibt daher $|O(E,q)\cdot h_1|=|S(E)|$ zu bestimmen.

Wie bereits zuvor ist $|S(E)|=\ell-1+|S(V)|\cdot\ell+(\ell-1)\ell^{2n-2}$. Für $k\geq 0$ sei $a_k=|S([1]\perp\mathbb{H}^{k-1})|$ und $x_k=a_k-\ell^{2k-1}+1$. Dann gilt wiederum $x_n=\ell x_{n-1}$ aber im Gegensatz zu Teil (a) ist nun $a_0=S([1])=0$ und somit $x_0=0$. Also ist $x_k=0$ für alle $k\in\mathbb{N}$. Damit wird $|S(E)|=a_n=\ell^{2n}-1$.

Setzen wir nun alles zusammen, so folgt wie behauptet:

$$\begin{aligned}|O_{2n+1}(\mathbb{F}_\ell)| &= (\ell^{2n}-1)\cdot\ell^{2n-1}\cdot|O_{2n-1}(\mathbb{F}_\ell)|\\ &= (\ell^{2n}-1)\cdot\ell^{2n-1}\cdot z\ell^{(n-1)^2}\prod_{i=1}^{n-2}(\ell^{2i}-1)\\ &= z\ell^{n^2}\prod_{i=1}^{n-1}(\ell^{2i}-1)\end{aligned}$$

Aufgabe 3.

(a) Wir führen Induktion nach s. In den Fällen $s\in\{0,1\}$ ist nichts zu zeigen. Sei nun $s\geq 2$.

Im Fall $V_s\in\bigcup_{i=1}^{s-1}V_i$ folgt aus der Induktionsvoraussetzung bereits

$$\bigcup_{i=1}^{s}V_i=\bigcup_{i=1}^{s-1}V_i\neq V\,.$$

Im Fall $V_1\leq V_s$ folgt ebenfalls aus der Induktionsvoraussetzung

$$\bigcup_{i=1}^{s}V_i=\bigcup_{i=2}^{s}V_i\neq V\,.$$

Also dürfen wir annehmen, daß es ein $v\in V_s-\bigcup_{i=1}^{s-1}V_i$ und ein $w\in V_1-V_s$ gibt. Wir behaupten nun, daß es für jedes $1\leq i\leq s$ höchstens ein $\lambda_i\in K$ gibt mit $w+\lambda_i v\in V_i$.

Beweis: Angenommen es ist $\lambda\in K$ mit $w+\lambda v\in V_s$. Dann folgt $w=(w+\lambda v)-\lambda v\in V_s$ was der Wahl von w widerspricht. Also existiert kein solcher Skalar λ.

Angenommmen, es gibt $\lambda,\mu\in K$ mit $w+\lambda v,\ w+\mu v\in V_i$ für ein $i\leq s-1$. Dann ist $V_i\ni(w+\lambda v)-(w+\mu v)=(\lambda-\mu)v$. Wegen $v\notin V_i$ folgt $\lambda=\mu$. Damit ist die Behauptung bewiesen.

Also ist $|\{\lambda\in K\mid w+\lambda v\in\bigcup_{i=1}^{s}V_i\}|\leq s<|K|$. Daher existiert ein $\lambda\in K$ mit $w+\lambda v\notin\bigcup_{i=1}^{s}V_i$.

(Hinweis: Wir haben sogar $|\{\lambda\in K\mid w+\lambda v\in\bigcup_{i=1}^{s}V_i\}|\leq s-1$ gezeigt. D.h. Teil (a) ist auch richtig im Fall $s=|K|<\infty$.)

(b) Sei $U=\langle V-\bigcup_{i=1}^{s}V_i\rangle$. Es genügt zu zeigen, daß $V_j\in U$ für alle $1\leq j\leq s$. Sei dazu $w\in V_j$. Nach (a) existiert ein $v\in V-\bigcup_{i=1}^{s}V_i$. Wie in Teil (a) folgt, daß es für jedes $1\leq i\leq s$ höchstens ein $\lambda_i\in K$ mit $w+\lambda_i v\in V_i$ gibt. Wegen $s<|K|$ existiert daher ein $\lambda\in K$ mit $w+\lambda v\notin\bigcup_{i=1}^{s}V_i$. Also ist $w+\lambda v\in U$ und somit auch $w=(w+\lambda v)-\lambda v\in U$.