Exercises: Code Equivalence - Day 1

Problem 1: Basics of Codes

Let $\mathcal{C}$ be an $[n,k]_q$ linear code with generator matrix $G \in \mathbb{F}_q^{k\times n}$ and parity-check matrix $H \in \mathbb{F}_q^{(n-k)\times n}$.

1. Show that $\langle H \rangle = \mathcal{C}^\perp$.
2. Show that $(\mathcal{C}^\perp)^\perp = \mathcal{C}$.
3. Show that if $GG^\top = 0$, then $\mathcal{C}$ is self-orthogonal.
4. Show that $\mathcal{C}$ is self-dual if and only if $\mathcal{C}$ is self-orthogonal and $n = 2k$.
5. Show that
$$\mathcal{H}(\mathcal{C}) = \ker\left(\begin{pmatrix} G \\ H \end{pmatrix}^\top\right).$$
6. Let G be in systematic form, i.e., $G = \begin{pmatrix} \mathrm{Id}_k & A \end{pmatrix}$ for $A \in \mathbb{F}_q^{k\times(n-k)}$. Show that if $AA^\top + \mathrm{Id}_{n-k}$ is full rank, then $\dim(\mathcal{H}(\mathcal{C})) = 0$.
7. Show that if $GG^\top$ has full rank, then $\dim(\mathcal{H}(\mathcal{C})) = 0$.

Problem 2: Equivalence of Codes

Let $\mathcal{C}, \mathcal{C}'$ be $[n,k]_q$ linear codes with generator matrices G, respectively G'.

1. Show that the linear isometries with respect to some distance function form a group with respect to the composition.
2. Give the automorphism group of $\mathcal{C} = \langle (1,0,0), (0,1,1) \rangle \subseteq \mathbb{F}_2^3$.
3. Let $\varphi \in \mathrm{Aut}(\mathcal{C})$ be a permutation. Show that $\varphi \in \mathrm{Aut}(\mathcal{C} \cap \mathcal{C}^\perp)$.
4. Show that $\mathcal{C}^\perp$ is linearly equivalent to $\mathcal{C}'^\perp$.
   Hint: Use the fact that $G'H'^\top = 0$ and $SGDP = G'$.
5. Show that for all $w \in \{1, \dots, n\}$ we have that
$$A_w(\mathcal{C}) = A_w(\mathcal{C}').$$

6. Show that generalized weights are strictly increasing, that is for $r \in \{1, \dots, k-1\}$ we have $d_r(\mathcal{C}) < d_{r+1}(\mathcal{C})$.
   Hint: Use the subcode $D(\{i\}) = \{d \in \mathcal{D} \mid d_i = 0\}$ and its dual.

7. Show that for all $r \in \{1, \dots, k\}$ we have that

$$d_r(\mathcal{C}) = d_r(\mathcal{C}').$$

8. Consider the code $\mathcal{C}_1 \subseteq \mathbb{F}_3^3$ generated by $G_1 = \begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & 1 \end{pmatrix}$ and the code $\mathcal{C}_2 \subseteq \mathbb{F}_3^3$ generated by $G_2 = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$. Are the two codes linear equivalent, permutation equivalent or not equivalent?

Exercises: Code Equivalence - Day 2

Problem 1: Hermitian Dual

Let $\mathcal{C}$ be an $[n,k]_q$ linear code with generator matrix $G \in \mathbb{F}_q^{k\times n}$ and parity-check matrix $H \in \mathbb{F}_q^{(n-k)\times n}$.

1. Let $H^\star \in \mathbb{F}_q^{(n-k)\times n}$ be a Hermitian parity-check matrix of $\mathcal{C}$. Show that
$$H^\star (G^{p^m})^\top = 0.$$
That is $\mathcal{C}^\star = \ker((G^{p^m})^\top)$.

2. Use
$$\langle x, y\rangle_H = \sum_{i=1}^{n} x_i y_i^{p^m} = (\sum_{i=1}^{n} x_i^{p^m} y_i)^{p^m}$$
to show that $H^\star = H^{p^m}$ is a Hermitian parity-check matrix.

3. Show that $(\mathcal{C}^\star)^\star = \mathcal{C}$.

4. Show that
$$\mathcal{H}^\star(\mathcal{C}) = \ker\left(\begin{pmatrix} G^{p^m} \\ H \end{pmatrix}^\top\right).$$

5. Let $\mathcal{C} \subset \mathbb{F}_q^n$ be linearly equivalent to $\mathcal{C}'$. Show that $\mathcal{C}^\star$ is linearly equivalent to $(\mathcal{C}')^\star$. *Hint:* Use again that $G((H^\star)^{p^m})^\top = 0$ and $GDP = G'$.

6. Let $\mathcal{C} \subset \mathbb{F}_q^n$ be permutation equivalent to $\mathcal{C}'$. Show that $\mathcal{H}^\star(\mathcal{C})$ is permutation equivalent to $\mathcal{H}^\star(\mathcal{C}')$.

7. Show that $A^\star$ is independent on the choice of G.

8. Show that if $G(G^{p^m})^\top$ has full rank, then $\dim(\mathcal{H}^\star(\mathcal{C})) = 0$.

Problem 2: Sums in finite fields

Let q be a prime power and ℓ be a positive integer, then
$$\sum_{\alpha\in\mathbb{F}_q^\star} \alpha^\ell = \begin{cases} 0 & \text{if } (q-1)\nmid \ell, \\ -1 & \text{if } (q-1)\mid \ell. \end{cases}$$

Problem 3: Square Codes

Let $\mathcal{C}$ be an $[n,k]_q$ linear code with generator matrix $G \in \mathbb{F}_q^{k\times n}$ and parity-check matrix $H \in \mathbb{F}_q^{(n-k)\times n}$.

1. Let $\mathcal{C}$ be generated by $G = \begin{pmatrix} g_1 \\ \vdots \\ g_k \end{pmatrix} \in \mathbb{F}_q^{k\times n}$. Then $\mathcal{C}^{(2)}$ is generated by
$$G^{(2)} = \begin{pmatrix} g_1 * g_1 \\ \vdots \\ g_1 * g_k \\ \vdots \\ g_k * g_k \end{pmatrix} \in \mathbb{F}_q^{\binom{k+1}{2}\times n}.$$
2. Let $\mathcal{C}, \mathcal{C}'$ be two $[n,k]_q$ linear codes and $\varphi = (D,P) \in (\mathbb{F}_q^\star)^n \rtimes S_n$ be such that $\varphi(\mathcal{C}) = \mathcal{C}'$. Then $\varphi' = (D^2, P) \in (\mathbb{F}_q^\star)^n \rtimes S_n$ is such that
$$\varphi'(\mathcal{C}^{(2)}) = \mathcal{C}'^{(2)}.$$
3. Let $\mathcal{C}$ be a $[n,k]_q$ linear code. Show that $\mathcal{H}(\mathcal{C})^{(2)} \neq \mathcal{H}(\mathcal{C}^{(2)})$.
4. Reduce the following LEP instance to GI using the square code:
$$G = \begin{pmatrix} 1 & 0 & 2 & 1 \\ 0 & 1 & 3 & 0 \end{pmatrix} \in \mathbb{F}_5^{2\times 4}$$
and
$$G' = \begin{pmatrix} 4 & 1 & 0 & 2 \\ 0 & 4 & 2 & 0 \end{pmatrix}.$$
5. Let α be a primitive element in $\mathbb{F}_q$. Define $\lambda = (1, \alpha, \ldots, \alpha^{q-2})$. Show that
$$(\lambda \otimes \mathcal{C})^{(2)} \neq \lambda \otimes \mathcal{C}^{(2)}.$$
6. Show that
$$(\lambda \otimes G)^{(\ell)} = \lambda^\ell \otimes G^{(\ell)}.$$