Exercises: Code Equivalence - Day 1 - Solution

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 $\dim(\mathcal{H}(\mathcal{C})) = 0$.

Solution

1. By the definition of parity-check matrix, we have that $H \in \mathbb{F}_q^{(n-k)\times n}$ is of full rank and such that $\ker(H^\top) = \mathcal{C}$. Let us denote the rows of H by h_j for all $j \in \{1,\ldots,n-k\}$. Thus for all $c \in \mathcal{C}$ we have that $\langle c, h_i\rangle = \sum_{j=1}^n c_j h_{i,j} = 0$ for all $j \in \{1,\ldots,n-k\}$ and further, for any $z \in \langle H\rangle$, we find $\lambda_1,\ldots,\lambda_{n-k} \in \mathbb{F}_q$ such that $z = \sum_{j=1}^{n-k}\lambda_j h_j$ and since
$$\langle c, z\rangle = \langle c, \sum_{j=1}^{n-k}\lambda_j h_j\rangle = \sum_{j=1}^{n-k}\lambda_j\langle c, h_j\rangle = 0,$$
we get that $\langle H\rangle \subseteq \mathcal{C}^\perp$.

   Observe that $\mathcal{C}^\perp$ is a linear subspace, as for any $y, y' \in \mathcal{C}^\perp$ we have that
$$\langle y + y', c\rangle = \langle y, c\rangle + \langle y', c\rangle = 0$$
for all $c \in \mathcal{C}$.

As $\langle \cdot, \cdot \rangle$ is a non-degenerate bilinear form, we immediately get that $\dim(\mathcal{C}) + \dim(\mathcal{C}^\perp) = n$ and hence $\dim(\mathcal{C}^\perp) = n - k$.

Since H has rank $n-k$ and $\langle H \rangle \subseteq \mathcal{C}^\perp$, both of dimension $n-k$, we get that $\langle H \rangle = \mathcal{C}^\perp$.

2. By 1. we have seen that $\langle H \rangle = \mathcal{C}^\perp$. We can also apply this to $\mathcal{C}^\perp$: telling us that the dual of the dual $(\mathcal{C}^\perp)^\perp$ is generated by a parity-check matrix of $\mathcal{C}^\perp$. Hence we are looking for a matrix A which is such that $\ker(A^\top) = \mathcal{C}^\perp$. Since $GH^\top = 0$, we get that G is such a matrix.

   Hence G is a parity-check matrix of $\mathcal{C}^\perp$ and thus, $\langle G \rangle = (\mathcal{C}^\perp)^\perp$. As we also know $\langle G \rangle = \mathcal{C}$, we get the claim.

3. To have self-orthogonality, we want to show that every codeword $c \in \mathcal{C}$ also lives in the dual $\mathcal{C}^\perp$. Let $c \in \mathcal{C}$ be an arbitrary codeword, thus there exists $m \in \mathbb{F}_q^k$ such that $c = mG$. As we assumed that $GG^\top = 0$, we get $cG^\top = 0$. By 2. we then know $c \in \mathcal{C}^\perp$.

4. For the first direction, assume that $\mathcal{C} = \mathcal{C}^\perp$, thus $\dim(\mathcal{C}) = k = \dim(\mathcal{C}^\perp) = n - k$ and $n = 2k$ and clearly $\mathcal{C} \subseteq \mathcal{C}^\perp$.

   For the other direction, assume that $n = 2k$ and $\mathcal{C} \subseteq \mathcal{C}^\perp$, then since $\dim(\mathcal{C}) = k$ and $\dim(\mathcal{C}^\perp) = n - k = k$, we get that $\mathcal{C} = \mathcal{C}^\perp$.

5. Any $x \in \mathcal{H}(\mathcal{C})$ is such that $x \in \mathcal{C}$, hence $xH^\top = 0$ and $x \in \mathcal{C}^\perp$, which implies $xG^\top = 0$. Putting both together we get $x \begin{pmatrix} H^\top & G^\top \end{pmatrix} = 0$ and thus $\mathcal{H}(\mathcal{C}) \subseteq \ker\left(\begin{pmatrix} G \\ H \end{pmatrix}^\top\right)$.

   For the other direction we do the same: since any $x \in \ker\left(\begin{pmatrix} G \\ H \end{pmatrix}^\top\right)$ is such that $xG^\top = 0$ and $xH^\top = 0$ we must have $x \in \mathcal{C} \cap \mathcal{C}^\perp$.

6. By 5. We are interested in the dimension of the kernel of the matrix $\begin{pmatrix} G \\ H \end{pmatrix}$, and due to the rank-nullity theorem in its rank. We can assume that G, H are in systematic form, i.e.,
$$G = \begin{pmatrix} \mathrm{Id}_k & A \end{pmatrix}, \quad H = \begin{pmatrix} -A^\top & \mathrm{Id}_{n-k} \end{pmatrix}$$
   and perform row operations to get
$$\begin{pmatrix} G' \\ H' \end{pmatrix}^\top = \begin{pmatrix} \mathrm{Id}_k & A \\ 0 & AA^\top + \mathrm{Id}_{n-k} \end{pmatrix}^\top.$$
   Hence its rank is given by $k + \mathrm{rk}(AA^\top + \mathrm{Id}_{n-k})$. Due to the assumption, that $AA^\top + \mathrm{Id}_{n-k}$ has full rank, we get by rank-nullity
$$\dim(\mathcal{H}(\mathcal{C})) = \dim\left(\ker\left(\begin{pmatrix} G \\ H \end{pmatrix}^\top\right)\right) = n - \mathrm{rk}\left(\begin{pmatrix} G \\ H \end{pmatrix}^\top\right) = n - n = 0.$$

7. For any $c \in \mathcal{C}$, there exists a $m \in \mathbb{F}_q^k$ such that $mG = c$. If c is also in $\mathcal{C}^\perp$, we know that $cG^\top = 0$. This gives: for any $c \in \mathcal{H}(\mathcal{C})$ there exists a $m \in \mathbb{F}_q^k$ such that

$mGG^\top = 0$ and instead of counting $c \in \mathcal{H}(\mathcal{C})$, we count the number of $m \in \mathbb{F}_q^k$ in the kernel of $GG^\top$. Due to the rank-nullity theorem, we get

$$\dim(\ker(GG^\top)) = \dim(\mathrm{im}(GG^\top)) - \mathrm{rk}(GG^\top) = k - k = 0.$$

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 $w \in \{1, \ldots, n\}$ we have that
   $$A_w(\mathcal{C}) = A_w(\mathcal{C}').$$
6. Show that generalized weights are strictly increasing, that is for $r \in \{1, \ldots, k-1\}$ 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 $r \in \{1, \ldots, k\}$ 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?

Solution

1. Let us consider the set S of all linear isometries $\varphi : \mathbb{F}_q^n \to \mathbb{F}_q^n$.

   Clearly, the identity function, id, is a linear isometry.

   As φ is an isometry for a distance function, it has to map 0 to 0, and no other element can be mapped to zero. In fact, if $\varphi(x) = 0$ and $x \neq 0$, we would get that $d(\varphi(x), 0) = 0 \neq d(x, 0)$.

   Hence, $\ker(\varphi) = \{0\}$ and as φ also has to be surjective, we get that φ is a $\mathbb{F}_q$ isomorphism.

   Thus, for all $\varphi \in S$ there also exists φ^{-1}, which is clearly also an isometry:

   $$d(\varphi^{-1}(\varphi(x)), \varphi^{-1}(\varphi(y))) = d(x, y) = d(\varphi(x), \varphi(y)).$$

Hence the inverse of any isometry is also an isometry.

Finally, if $\varphi, \psi \in S$, then $\varphi \circ \psi \in S$ as

$$d(\varphi(\psi(x)), \varphi(\psi(y))) = d(\psi(x), \psi(y)) = d(x, y).$$

2. We first note that the only linear isometries over $\mathbb{F}_2^3$ are permutations $\sigma \in S_3$. We clearly have $\mathrm{id} \in \mathrm{Aut}(\mathcal{C})$ and we can also swap the second and third position, i.e., $(2,3) \in \mathrm{Aut}(\mathcal{C})$.

3. Let $\varphi \in \mathrm{Aut}(\mathcal{C})$ be a permutation. By Proposition 1.34, we know that $\varphi \in \mathrm{Aut}(\mathcal{C}^\perp)$ and hence $\varphi \in \mathrm{Aut}(\mathcal{C} \cap \mathcal{C}^\perp)$.

4. We can follow the same proof as in the lecture:

   Let H, H' be the parity-check matrices for $\mathcal{C}$, respectively $\mathcal{C}'$. Since $G'H'^\top = 0$, we also have $GDPH'^\top = G(H'P^\top D)^\top = 0$. This implies that $H'P^\top D$ is a parity-check matrix for $\mathcal{C}$ and hence there exists some $S \in \mathrm{GL}_q(n-k)$ such that $H = SH'P^\top D$.

   This is enough to show that there exists a monomial transform from $\mathcal{C}^\perp = \langle H \rangle$ to $\mathcal{C}'^\perp = \langle H' \rangle$.

   We can also go further and write $H' = S'HD^{-1}P$, for some $S' \in \mathrm{GL}_q(n-k)$. Thus, the monomial transformation between the duals is $D^{-1}P$, which is not necessarily the original DP.

5. Since $\mathcal{C}_1$ is linearly equivalent to $\mathcal{C}_2$, there exists some isometry $\varphi : \mathcal{C}_1 \to \mathcal{C}_2$. Thus, if we consider the set

$$S_w(\mathcal{C}_1) = \{c \in \mathcal{C}_1 \mid \mathrm{wt}_H(c) = w\}$$

   then

$$\begin{aligned}\varphi(S_w(\mathcal{C}_1)) &= \{\varphi(c) \mid c \in \mathcal{C}_1, \mathrm{wt}_H(c) = w\} \\ &= \{c' \in \mathcal{C}_2 \mid \mathrm{wt}_H(c') = w\} = S_w(\mathcal{C}')\end{aligned}$$

   and hence they have the same size.

6. The fact that $d_{r-1}(\mathcal{C}) \leq d_r(\mathcal{C})$ follows directly from the definition as $d_r(\mathcal{C})$ is the smallest weight of a subcode of dimension r, which also contains subcodes of dimension $r-1$.

   Let $\mathcal{D} \subset \mathcal{C}$ be a subcode of dimension r and weight $d_r(\mathcal{C})$. Let us denote by $S = \mathrm{supp}_H(\mathcal{D})$. For $i \in S$ we consider the subcode

$$D(\{i\}) = \{d \in \mathcal{D} \mid d_i = 0\}.$$

   Clearly,

$$\mathrm{wt}_H(\mathcal{D}(\{i\})) \leq d_r(\mathcal{C}) - 1.$$

   Next, we show that $\mathcal{D}(\{i\})$ has dimension $\dim(\mathcal{D}) - 1 = r - 1$.

For this we consider its dual

$$\mathcal{D}(\{i\})^\perp = \{c \in \mathbb{F}_q^n \mid \langle c, d\rangle = 0 \;\forall\; d \in \mathcal{D}(\{i\})\}.$$

We note that $\dim(\mathcal{D}(\{i\}))$ has to be strictly smaller than $\dim(\mathcal{D}) = r$ as $i \in \mathrm{supp}_H(\mathcal{D})$. Thus $r-1$ is the largest dimension it can be. Similarly, for the dual we have that $\dim(\mathcal{D}^\perp) = n-r$ and $\dim(\mathcal{D}(\{i\})^\perp) > n-r$ and thus $n-r+1$ is the smallest it can be.

Clearly, any $c \in \mathcal{D}^\perp$ also lives in $\mathcal{D}(\{i\})^\perp$, as any $c \in \mathcal{D}^\perp$ is also such that $\langle c, d\rangle = 0$ for all $d \in \mathcal{D}(\{i\})$. We also note that e_i, the ith standard vector is in $\mathcal{D}(\{i\})^\perp$ and thus

$$\mathcal{D}^\perp \cup \langle e_i\rangle \subseteq \mathcal{D}(\{i\})^\perp.$$

We note that $e_i \notin \mathcal{D}^\perp$, as $i \in \mathrm{supp}_H(\mathcal{D})$, there exists some $c \in \mathcal{D}$ with $c_i \neq 0$, hence $\langle e_i, c\rangle = c_i \neq 0$. Thus, we get that

$$\dim(\mathcal{D}^\perp \cup \langle e_i\rangle) = n-r+1,$$

and hence

$$\mathcal{D}^\perp \cup \langle e_i\rangle = \mathcal{D}(\{i\})^\perp,$$

which in turn gives that $\dim(\mathcal{D}(\{i\})) = r-1$.

Thus,

$$d_{r-1}(\mathcal{C}) \leq \mathrm{wt}_H(\mathcal{D}(\{i\})) \leq d_r(\mathcal{C}) - 1 < d_r(\mathcal{C}).$$

7. Let $\varphi \in (\mathbb{F}_q^\times)^n \rtimes S_n$ be such that $\varphi(\mathcal{C}_1) = \mathcal{C}_2$ and let $\mathcal{D}$ be any subcode of $\mathcal{C}_1$, then $\varphi(\mathcal{D})$ is a subcode of $\mathcal{C}_2$.

   As $\mathrm{wt}_H(\mathcal{D}) = \mathrm{wt}_H(\varphi(\mathcal{D}))$, we immediately get

$$\begin{aligned} d_r(\mathcal{C}_1) &= \min\{\mathrm{wt}_H(\mathcal{D}) \mid \mathcal{D} \subset \mathcal{C}_1, \dim(\mathcal{D}) = r\} \\ &= \min\{\mathrm{wt}_H(\varphi(\mathcal{D})) \mid \varphi(\mathcal{D}) \subset \varphi(\mathcal{C}_1), \dim(\varphi(\mathcal{D})) = r\} \\ &= d_r(\varphi(\mathcal{C}_1)) = d_r(\mathcal{C}_2). \end{aligned}$$

8. For this we use 4. that is we check whether their duals are equivalent. We compute

$$H_1 = \begin{pmatrix} 1 & 2 & 1 \end{pmatrix}, \quad \text{and} \quad H_2 = \begin{pmatrix} 2 & 0 & 1 \end{pmatrix}.$$

   As these codes $\mathcal{C}_1^\perp$ and $\mathcal{C}_2^\perp$ have a different minimum distance: $d(\mathcal{C}_1^\perp) = 3$ and $d(\mathcal{C}_2^\perp) = 2$, they are not equivalent.

Exercises: Code Equivalence - Day 2 - Solution

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 $\dim(\mathcal{H}^\star(\mathcal{C})) = 0$.

Solution

1. If $H^\star$ is a Hermitian parity-check matrix, then any $x \in \mathcal{C}^\star$ can be written as $x = mH^\star$ for some $m \in \mathbb{F}_q^{n-k}$. Similarly, for any $y \in \mathcal{C}$, there exists some $m' \in \mathbb{F}_q^k$ such that $y = m'G$. Since any $x \in \mathcal{C}^\star$ is such that $x(y^{p^m})^\top = 0$ for all $y \in \mathcal{C}$, we get that $mH^\star((m'G)^{p^m})^\top = 0$ or equivalently, $H^\star(G^{p^m})^\top = 0$

2. From
$$\sum_{i=1}^{n} x_i y_i^{p^m} = (\sum_{i=1}^{n} x_i^{p^m} y_i)^{p^m}$$
we get (similarly to 1.) that $((H^\star)^{p^m} G^\top)^{p^m} = 0$, which implies that $(H^\star)^{p^m} G^\top = 0$ and thus, $(H^\star)^{p^m}$ is a parity-check matrix of $\mathcal{C}$. Hence, given a parity-check matrix H, we can construct $H^\star = H^{p^m}$, as then $(H^\star)^{p^m} = (H^{p^m})^{p^m} = H^{p^{2m}} = H$.

3. Recall from 2. that if $\mathcal{C} = \ker(H^\top)$ then a Hermitian parity-check matrix is given by H^{p^m}. Thus, if we apply this to $\mathcal{C}^\star = \ker((G^{p^m})^\top)$, we get that a Hermitian parity-check matrix of $\mathcal{C}^\star$ is given by $G^{p^{2m}} = G$, that is $\langle G \rangle = (\mathcal{C}^\star)^\star$. As $\langle G \rangle = \mathcal{C}$, we get the claim.

4. In order for $x \in \mathbb{F}_q^n$ to be in $\mathcal{H}^\star(\mathcal{C}) = \mathcal{C} \cap \mathcal{C}^\star$, we need that $x \in \mathcal{C} = \ker(H^\top)$, that is $xH^\top = 0$. As we also need $x \in \mathcal{C}^\star = \ker((G^{p^m})^\top)$, from which we get the condition $x(G^{p^m})^\top = 0$. Thus, any $x \in \mathcal{H}^\star(\mathcal{C})$ must be in the kernel of $\begin{pmatrix} G^{p^m} \\ H \end{pmatrix}^\top$.

5. Let $\mathcal{C} = \langle G \rangle$ with Hermitian parity-check matrix $H^\star$ and $\mathcal{C}' = \langle G' \rangle$, with Hermitian parity-check matrix $H'^\star$, such that there exists a $n \times n$ permutation matrix P and a diagonal matrix $D = \operatorname{diag}(d)$ with $d \in (\mathbb{F}_q^\star)^n$, with $GDP = G'$.

   From 2. we recall that $G'((H'^\star)^{p^m})^\top = 0$, hence
$$GDP((H'^\star)^{p^m})^\top = G((H'^\star)^{p^m} P^\top D)^\top = G((H'^\star P^\top D^{p^m})^{p^m})^\top = 0,$$
   which implies that $H'^\star P^\top D^{p^m}$ is a Hermitian parity-check matrix of $\mathcal{C}$ and hence there exists some invertible $S \in \mathrm{GL}_q(n-k)$ with $SH^\star = H'^\star P^\top D^{p^m}$, or equivalently, $SH^\star (D^{p^m})^{-1} P = H'^\star$ and hence $\mathcal{C}'$ is linearly equivalent to $\mathcal{C}'^\star$.

6. Recall that $A^\star = (G^{p^m})^\top (G(G^{p^m})^\top)^{-1} G$. Hence for a different choice SG, we get
$$\begin{aligned} ((SG)^{p^m})^\top (SG((SG)^{p^m})^\top)^{-1} SG &= (S^{p^m} G^{p^m})^\top (SG(S^{p^m} G^{p^m})^\top)^{-1} SG \\ &= (G^{p^m})^\top (S^{p^m})^\top (SG(G^{p^m})^\top (S^{p^m})^\top)^{-1} SG \\ &= (G^{p^m})^\top (S^{p^m})^\top ((S^{p^m})^\top)^{-1} (G(G^{p^m})^\top)^{-1} S^{-1} SG \\ &= (G^{p^m})^\top (G(G^{p^m})^\top)^{-1} G = A^\star. \end{aligned}$$

7. For any $c \in \mathcal{C}$, there exists a $m \in \mathbb{F}_q^k$ such that $mG = c$. If c is also in $\mathcal{C}^\star$, we know that $c(G^{p^m})^\top = 0$. This gives: for any $c \in \mathcal{H}^\star(\mathcal{C})$ there exists a $m \in \mathbb{F}_q^k$ such that $mG(G^{p^m})^\top = 0$ and instead of counting $c \in \mathcal{H}^\star(\mathcal{C})$, we count the number of $m \in \mathbb{F}_q^k$ in the kernel of $G(G^{p^m})^\top$. Due to the rank-nullity theorem, we get
$$\dim(\ker(G(G^{p^m})^\top)) = \dim(\operatorname{im}(G(G^{p^m})^\top)) - \operatorname{rk}(G(G^{p^m})^\top) = k - k = 0.$$

Problem 2: Sums in finite fields

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

Solution

If $(q-1) \mid \ell$, then there exists a positive integer m such that $m(q-1) = \ell$ and

$$\sum_{\alpha \in \mathbb{F}_q^\star} \alpha^\ell = \sum_{\alpha \in \mathbb{F}_q^\star} \alpha^{m(q-1)} = \sum_{\alpha \in \mathbb{F}_q^\star} (\alpha^{q-1})^m = \sum_{\alpha \in \mathbb{F}_q^\star} 1 = q-1.$$

On the other hand, if $(q-1) \nmid \ell$, then for any primitive element $a \in \mathbb{F}_q^\star$, we have that $a^\ell \neq 1$. Multiplying by a introduces a bijection $\varphi_a : \mathbb{F}_q^\star \to \mathbb{F}_q^\star, \alpha \mapsto a\alpha$. Thus,

$$\sum_{\alpha \in \mathbb{F}_q^\star} \alpha^\ell = \sum_{\alpha \in \mathbb{F}_q^\star} (a\alpha)^\ell = a^\ell \sum_{\alpha \in \mathbb{F}_q^\star} \alpha^\ell.$$

Since $a^\ell \neq 1$, we must have $\sum_{\alpha \in \mathbb{F}_q^\star} \alpha^\ell = 0$.

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

$$(\lambda \otimes G)^{(\ell)} = \lambda^\ell \otimes G^{(\ell)}.$$

Solution

1. Let $c \in \mathcal{C}^{(2)}$, then there exist $c_1, c_2 \in \mathcal{C}$ such that $c = c_1 * c_2$. Hence we have $m_1, m_2 \in \mathbb{F}_q^k$ such that $c_1 = m_1 G = \sum_{i=1}^k m_{1,i} g_i$ and $c_2 = m_2 G = \sum_{i=1}^k m_{2,i} g_i$.

   Thus,

$$\begin{aligned} c = m_1 G * m_2 G &= (\sum_{i=1}^k m_{1,i} g_{i,1} \cdot \sum_{i=1}^k m_{2,i} g_{i,1}, \dots, \sum_{i=1}^k m_{1,i} g_{i,n} \cdot \sum_{i=1}^k m_{2,i} g_{i,n}) \\ &= (\sum_{i,j=1}^k (g_{i,1} g_{j_1})(m_{1,i} m_{2,j}), \dots, \sum_{i,j=1}^k (g_{i,n} g_{j_n})(m_{1,i} m_{2,j})) \\ &= M G^{(2)}, \end{aligned}$$

   where $M = (m_{1,1} m_{2,1}, m_{1,1} m_{2,2}, \dots, m_{1,k} m_{2,k})$.

2. Recall that any codeword in $\mathcal{C}^{(2)}$ is of the form $c = c_1 * c_2$ for $c_1, c_2 \in \mathcal{C}$. Since $c_1 DP, c_2 DP \in \mathcal{C}'$we get that $(c_1 DP) * (c_2 DP) \in \mathcal{C}'^{(2)}$. Now we observe that

$$(c_1 DP) * (c_2 DP) = (c_1 D * c_2 D) P = (c_1 * c_2) D^2 P \in \mathcal{C}'^{(2)}.$$

3. Let us consider $\mathcal{C} \subseteq \mathbb{F}_3^3$ generated by $G = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 2 \end{pmatrix}$. We compute the parity-check matrix as

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

   Hence the hull of $\mathcal{C}$ is given by the kernel of

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

   By elementary row operations, we find the systematic form to be

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

   that is $\mathcal{C}^\perp \subseteq \mathcal{C}$ and hence $\mathcal{C}^\perp = \mathcal{H}(\mathcal{C})$. If we compute the square code of this hull, we get a code generated by

$$H^{(2)} = \begin{pmatrix} 1 & 1 & 1 \end{pmatrix}.$$

   On the other hand, if we compute the square code $\mathcal{C}^{(2)}$, generated by

$$G^{(2)} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 0 & 2 \\ 0 & 1 & 1 \end{pmatrix},$$

   we see that $\mathcal{C}^{(2)} = \mathbb{F}_3^3$ and hence $(\mathcal{C}^{(2)})^\perp = \{0\}$. Thus,

$$\mathcal{H}(\mathcal{C}^{(2)}) = \{0\} \neq \mathcal{H}(\mathcal{C})^{(2)} = \langle (1,1,1) \rangle.$$

4. We first compute

$$G^{(2)} = \begin{pmatrix} 1 & 0 & 4 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 4 & 0 \end{pmatrix}, \quad G'^{(2)} = \begin{pmatrix} 1 & 1 & 0 & 4 \\ 0 & 4 & 0 & 0 \\ 0 & 1 & 4 & 0 \end{pmatrix}.$$

Then we compute

$$B = G^{(2)}(G^{(2)})^\top = \begin{pmatrix} 3 & 4 & 1 \\ 4 & 1 & 4 \\ 1 & 4 & 2 \end{pmatrix} = G'^{(2)}(G'^{(2)})^\top.$$

Next, we compute its inverse

$$B^{-1} = \begin{pmatrix} 3 & 3 & 0 \\ 3 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}.$$

Now we can compute

$$A = (G^{(2)})^\top B^{-1} G^{(2)} = \begin{pmatrix} 3 & 0 & 0 & 3 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 3 & 0 & 0 & 3 \end{pmatrix}$$

$$A' = (G'^{(2)})^\top B^{-1} G'^{(2)} = \begin{pmatrix} 3 & 0 & 0 & 2 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 2 & 0 & 0 & 3 \end{pmatrix}.$$

Hence, we can find $P^\top D^2 A D^2 P = A'$ for several D, P in particular for $D^2 = \operatorname{diag}(1, 4, 4, 4)$, and $P = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$. Checking again with G, G' we get $D = \operatorname{diag}(4, 2, 3, 2)$ and $\sigma = (2, 3)$.

5. As a small counterexample we can consider $\mathbb{F}_3$ with the generator matrix

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

Then for $\lambda = (1, 2)$ we get

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

and

$$(\lambda \otimes G)^{(2)} = \begin{pmatrix} 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 2 & 2 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

On the other hand,

$$G^{(2)} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 0 & 2 \\ 0 & 1 & 1 \end{pmatrix}$$

and

$$\lambda \otimes (G^{(2)}) = \begin{pmatrix} 1 & 2 & 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 & 2 & 1 \\ 0 & 0 & 1 & 2 & 1 & 2 \end{pmatrix}$$

which do not give the same code.

6. Let $\lambda = (1, \alpha, \ldots, \alpha^{q-2})$ and let

$$G = \begin{pmatrix} g_{1,1} & g_{1,2} & \cdots & g_{1,n} \\ g_{2,1} & g_{2,2} & \cdots & g_{2,n} \\ \vdots & \vdots & & \vdots \\ g_{k,1} & g_{k,2} & \cdots & g_{k,n} \end{pmatrix}.$$

We note that $\mathcal{C}^{(\ell)} = \mathcal{C} * \mathcal{C}^{(\ell-1)}$ and hence proceed by induction. For $\ell = 2$, we get The closure $\lambda \otimes \mathcal{C}$ is then generated by

$$\lambda \otimes G = \begin{pmatrix} g_{1,1} & \alpha g_{1,1} & \cdots & \alpha^{q-2} g_{1,1} & \cdots & g_{1,n} & \alpha g_{1,n} & \cdots & \alpha^{q-2} g_{1,n} \\ \vdots & \vdots & & \vdots & & \vdots & \vdots & & \vdots \\ g_{k,1} & \alpha g_{k,1} & \cdots & \alpha^{q-2} g_{k,1} & \cdots & g_{k,n} & \alpha g_{k,n} & \cdots & \alpha^{q-2} g_{k,n} \end{pmatrix}.$$

Hence the square of the closure is generated by $(\lambda \otimes G)^{(2)}$ being

$$\begin{pmatrix} g_{1,1}^2 & \alpha^2 g_{1,1}^2 & \cdots & \alpha^{2(q-2)} g_{1,1}^2 & \cdots & g_{1,n}^2 & \alpha^2 g_{1,n}^2 & \cdots & \alpha^{2(q-2)} g_{1,n}^2 \\ \vdots & \vdots & & \vdots & & \vdots & \vdots & & \vdots \\ g_{k,1}^2 & \alpha^2 g_{k,1}^2 & \cdots & \alpha^{2(q-2)} g_{k,1}^2 & \cdots & g_{k,n}^2 & \alpha^2 g_{k,n}^2 & \cdots & \alpha^{2(q-2)} g_{k,n}^2 \end{pmatrix}.$$

On the other hand, the square code of $\mathcal{C}$ is generated by

$$G^{(2)} = \begin{pmatrix} g_{1,1}^2 & g_{1,2}^2 & \cdots & g_{1,n}^2 \\ g_{1,1}g_{2,1} & g_{1,2}g_{2,2} & \cdots & g_{1,n}g_{2,n} \\ \vdots & \vdots & & \vdots \\ g_{k,1}^2 & g_{k,2}^2 & \cdots & g_{k,n}^2 \end{pmatrix}.$$

Thus, $\lambda^2 \otimes G$ is

$$\begin{pmatrix} g_{1,1}^2 & \alpha^2 g_{1,1}^2 & \cdots & \alpha^{2(q-2)} g_{1,1}^2 & \cdots & g_{1,n}^2 & \alpha^2 g_{1,n}^2 & \cdots & \alpha^{2(q-2)} g_{1,n}^2 \\ \vdots & \vdots & & \vdots & & \vdots & \vdots & & \vdots \\ g_{k,1}^2 & \alpha^2 g_{k,1}^2 & \cdots & \alpha^{2(q-2)} g_{k,1}^2 & \cdots & g_{k,n}^2 & \alpha^2 g_{k,n}^2 & \cdots & \alpha^{2(q-2)} g_{k,n}^2 \end{pmatrix}.$$

Now for ℓ we get that

$$\langle (\lambda \otimes G)^{(\ell)} \rangle = (\lambda \otimes \mathcal{C})^{(\ell)} = (\lambda \otimes \mathcal{C}) * (\lambda \otimes \mathcal{C}^{(\ell-1)}),$$

by the induction hypothesis, we have that

$$(\lambda \otimes \mathcal{C}^{(\ell-1)}) = \langle \lambda^{\ell-1} \otimes G^{(\ell-1)} \rangle$$

and hence

$$(\lambda^{\ell-1} \otimes G^{(\ell-1)}) * (\lambda \otimes G) = \lambda^{\ell} \otimes G^{(\ell)}.$$