Endow $\mathbb{F}_q^n$ with the symmetric bilinear form:

$$\langle \cdot, \cdot \rangle : \begin{array}{l} \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{F}_q^n \\ (x, y) \mapsto \sum_{i=1}^n x_i y_i \end{array}$$

Definition (Dual code)

For $\mathcal{C} \subseteq \mathbb{F}_q^n$ a code, we define its *dual code* $\mathcal{C}^\perp$ as

$$\mathcal{C}^\perp := \left\{ x \in \mathbb{F}_q^n \mid \forall c \in \mathcal{C}, \langle x, c \rangle = 0 \right\}$$

I. Properties

Prop

Let $\mathcal{C} \subseteq \mathbb{F}_q^n$ be a code with generator matrix G and parity check matrix H.

Then G is a parity check matrix of $\mathcal{C}^\perp$ and H is a generator matrix of $\mathcal{C}^\perp$.

Proof (exercise).
Hint: take note that $G \cdot H^T = 0$: rows of G are orthogonal to rows of H.

Prop

1. $\dim \mathcal{C}^\perp = n - \dim \mathcal{C}$
2. $\left(\mathcal{C}^\perp\right)^\perp = \mathcal{C}$ (immediate from prop. 1)
3. $(\mathcal{C} + \mathcal{D})^\perp = \mathcal{C}^\perp \cap \mathcal{D}^\perp$
4. $(\mathcal{C} \cap \mathcal{D})^\perp = \mathcal{C}^\perp + \mathcal{D}^\perp$

⚠️ In real Euclidean spaces, if $\mathcal{C} \subseteq \mathbb{R}^n$ then: $\mathbb{R}^n = \mathcal{C} \oplus \mathcal{C}^\perp$. **This is not true in $\mathbb{F}_q^n$ with $\langle \cdot, \cdot \rangle$.**

Example

$\mathcal{C} \subseteq \mathbb{F}_2^n$ with generator matrix $G = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$.

Then $\mathcal{C} = \mathcal{C}^\perp$.

Remark. The dual of the **repetition code** is the **parity code**.

II. Metric relation: the McWilliams theorem

Question. Is there a relation between the minimum distances of $\mathcal{C}$ and $\mathcal{C}^\perp$?
No.

Explanation. Minimum distance is not informative enough for this problem.

Definition (Weight enumerator)

Let $\mathcal{C} \subseteq \mathbb{F}_q^n$ a code, its *weight enumerating polynomial* $P_\mathcal{C} \in \mathbb{Z}[X, Y]$ is defined as:

$$P_{\mathcal{C}(x,y)} := \sum_{i=0}^n |\{c \in C \mid w(c) = i\}| x^i y^{n-i}$$

Theorem (McWilliams)
Let $\mathcal{C} \subseteq \mathbb{F}_2^n$ a code. Then:

$$P_{\mathcal{C}^\perp}(x, y) = \frac{1}{|\mathcal{C}|} P(y - x, y + x)$$

The proof rests of the following lemma:

Lemma
Let $f : \mathbb{F}_2^n \to \mathbb{C}$ and denote

$$\hat{f} : \begin{cases} \mathbb{F}_2^n \to \mathbb{C} \\ v \mapsto \sum_{u \in \mathbb{F}_2^n} (-1)^{\langle u, v \rangle} f(u) \end{cases}$$

Let $\mathcal{C} \subseteq \mathbb{F}_2^n$ be a code.

Then:

$$\forall f : \mathbb{F}_2^n \to \mathbb{C}, \sum_{u \in \mathcal{C}^\perp} f(u) = \frac{1}{|\mathcal{C}|} \sum_{v \in \mathcal{C}} \hat{f}(v)$$

Proof.

$$\begin{aligned} (\star) \quad \sum_{v \in \mathcal{C}} \hat{f}(v) &= \sum_{v \in \mathcal{C}} \sum_{u \in \mathbb{F}_2^n} (-1)^{\langle u, v \rangle} f(u) \\ &= \sum_{u \in \mathbb{F}_2^n} f(u) \sum_{v \in \mathcal{C}} (-1)^{\langle u, v \rangle} \end{aligned}$$

Fact:

$$\sum_{v \in \mathcal{C}} (-1)^{\langle u, v \rangle} = \begin{cases} |\mathcal{C}| \text{ if } u \in \mathcal{C}^\perp \\ 0 \text{ otherwise} \end{cases}$$

- If $u \in \mathcal{C}^\perp, \sum_{v \in \mathcal{C}} (-1)^0 = |\mathcal{C}|$
- If $u \notin \mathcal{C}^\perp$, then the map: $\varphi_u : \begin{cases} \mathcal{C} \to \mathbb{F}_2 \\ v \mapsto \langle u, v \rangle \end{cases}$ is a nonzero linear form: $\dim \ker \varphi_u = \dim \mathcal{C} - 1$. Thus:
  - $\langle u, v \rangle = 0$ 2^{k-1} times
  - $\langle u, v \rangle = 1$ $2^k - 2^{k-1} = 2^{k-1}$ times

Back to $(\star)$:

$$\sum_{v \in \mathcal{C}} \hat{f}(v) = \sum_{u \in \mathcal{C}^\perp} f(u) \ |C| \quad \blacksquare$$

Proof of McWilliams theorem.
We will prove $P_{\mathcal{C}^\perp}(x, y) = \frac{1}{|C|} P_{\mathcal{C}}(y - x, y + x)$ for any $(x, y) \in \mathbb{C}^* \times \mathbb{C}^*$.

Algebraic identities prolongation theorem says two bivariate polynomials coinciding on a product of two infinite sets are equal.

Fix $x, y \in \mathbb{C}^* \times \mathbb{C}^*$ and take:

$$f : \begin{cases} \mathbb{F}_2^n \to \mathbb{C} \\ u \mapsto x^{w(u)} y^{n - w(u)} \end{cases}$$

Note that $P_{\mathcal{C}(x,y)} = \sum_{u \in \mathcal{C}} f(u)$.

$$\begin{aligned}
\hat{f}(v) &= \sum_{u \in \mathbb{F}_2^n} (-1)^{\langle u,v \rangle} x^{w(u)} y^{n-w(u)} \\
&= \sum_{(u_1,\ldots,u_n) \in \mathbb{F}_2^n} (-1)^{u_1 v_1} \ldots (-1)^{u_n v_n} x^{u_1} \ldots x^{u_n} y^{1-u_1} \ldots y^{1-u_n} \\
&= \sum_{(u_1,\ldots,u_n) \in \mathbb{F}_2^n} \prod_{i=1}^{n} (-1)^{u_i v_i} x^{u_i} y^{1-u_i} \\
&= \prod_{i=1}^{n} \left(\sum_{t \in \mathbb{F}_2} (-1)^{t v_i} x^t y^{1-t} \right) \\
&= \prod_{i=1}^{n} (y + (-1)^{v_i} x) \\
i.e.\ \hat{f}(v) &= (y+x)^{n-w(v)} (y-x)^{w(v)}
\end{aligned}$$

Now, we can finish the proof using the lemma (skipped on my notes).