Coding Theory: Linear Codes and their Dual

A Generic Communication Channel

Transmitter Channel Receiver

Data $\mathbf{x}$ → Encoder → Noise $\mathbf{e}$ → Decoder → Decoded Data $\hat{\mathbf{x}}$

$$\mathbf{x} = (x_1, \ldots, x_k) \in \mathbb{F}_q^k \mapsto \mathbf{c} = \underbrace{(c_1, \ldots, c_n)}_{\text{codeword, } n \geq k} = (x_1, \ldots, x_k) \underbrace{[\mathbf{I}_k | A]}_{\substack{\text{systematic} \\ \text{generator matrix}}} \in \mathbb{F}_q^n$$

Generator matrix

$$\mathcal{C} = \{\mathbf{c} = \mathbf{x}G,\ \mathbf{x} \in \mathbb{F}_q^k\}$$

Parity check matrix

$$\mathcal{C} = \{\mathbf{v} \in \mathbb{F}_q^n,\ H\mathbf{v}^T = \mathbf{0}\}$$

The $(7, 4)$ Hamming code

- Dimension: $k = 4$.
- Length: $n = 7$.
- Alphabet: $\mathbb{F}_2$.
- Encoding given by the generator matrix $G = [\mathbf{I}_4 | A]$, with corresponding parity check matrix $H = [-A^T | \mathbf{I}_{n-k}]$:

$$G = \left[\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right]$$

The $(7,4)$ Hamming code

- Dimension: $k = 4$.
- Length: $n = 7$.
- Alphabet: $\mathbb{F}_2$.
- Encoding given by the generator matrix $G = [\mathbf{I}_4 | A]$, with corresponding parity check matrix $H = [-A^T | \mathbf{I}_{n-k}]$:

$$G = \left[\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right] H = \left[\begin{array}{cccc|ccc} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{array}\right]$$

Dual code $\mathcal{C}^\perp$

Given an (n, k) linear code $\mathcal{C}$ over $\mathbb{F}_q$, $\mathcal{C}^\perp$ is the $(n, n-k)$ linear code generated by the rows of its parity check matrix H.

To have a generator matrix, we simply need a matrix whose rows are independent, they then span the code.

The rows of H ($H = [-A^T|\mathbf{I}_{n-k}]$ in systematic form) are independent.

For $\mathcal{C}$

$\mathcal{C}$ is generated by k basis vectors in $\mathbb{F}_q^n$, placed as rows in G.
$\mathcal{C}$ is the kernel of some H, that is $HG^T\mathbf{x}^T = \mathbf{0}$ for all $\mathbf{x} \in \mathbb{F}_q^k$ and $HG^T = \mathbf{0}$.

For $\mathcal{C}^\perp$

$\mathcal{C}^\perp$ is generated by $n-k$ basis vectors in $\mathbb{F}_q^n$, placed as rows in H.
$\mathcal{C}^\perp$ is the kernel of some $\tilde{G}$, that is $\tilde{G}H^T\mathbf{x}^T = \mathbf{0}$ for all $\mathbf{x} \in \mathbb{F}_q^{n-k}$ and $\tilde{G}H^T = \mathbf{0}$.

For $\mathcal{C}$

$\mathcal{C}$ is generated by k basis vectors in $\mathbb{F}_q^n$, placed as rows in G.
$\mathcal{C}$ is the kernel of some H, that is $HG^T\mathbf{x}^T = \mathbf{0}$ for all $\mathbf{x} \in \mathbb{F}_q^k$ and $HG^T = \mathbf{0}$.

For $\mathcal{C}^\perp$

$\mathcal{C}^\perp$ is generated by $n-k$ basis vectors in $\mathbb{F}_q^n$, placed as rows in H.
$\mathcal{C}^\perp$ is the kernel of some $\tilde{G}$, that is $\tilde{G}H^T\mathbf{x}^T = \mathbf{0}$ for all $\mathbf{x} \in \mathbb{F}_q^{n-k}$ and $\tilde{G}H^T = \mathbf{0}$.

$$HG^T = \mathbf{0},\ H\tilde{G}^T = \mathbf{0} \xRightarrow[\text{dimension}]{\text{kernel}} \tilde{G} = G.$$

Dual code $\mathcal{C}^\perp$

Given an (n, k) linear code $\mathcal{C}$ over $\mathbb{F}_q$, $\mathcal{C}^\perp = \{\mathbf{v} \in \mathbb{F}_q^n,\ \mathbf{c} \cdot \mathbf{v}^T = \mathbf{0} \text{ for all } \mathbf{c} \in \mathcal{C}\}$.

The usual inner product of vectors $\mathbf{x} = (x_1, \ldots, x_n)$ and $\mathbf{y} = (y_1, \ldots, y_n)$ applies in $\mathbb{F}_q^n$:

$$\mathbf{x} \cdot \mathbf{y}^T = \sum_{i=1}^{n} x_i y_i.$$

We know:

$$\begin{aligned} \mathcal{C}^{\perp} &= \{\mathbf{v} \in \mathbb{F}_q^n,\ \mathbf{c} \cdot \mathbf{v}^T = \mathbf{0} \text{ for all } \mathbf{c} \in \mathcal{C}\} \\ &= \{\mathbf{v} \in \mathbb{F}_q^n,\ \mathbf{x}G \cdot \mathbf{v}^T = \mathbf{0} \text{ for all } \mathbf{x} \in \mathbb{F}_q^k\} \end{aligned}$$

Let $\mathbf{g}_i$, $i = 1, \ldots, k$ be the rows of G. Then $0 = \sum_{i=1}^k x_i \mathbf{g}_i \cdot \mathbf{v}^T$ for any x_i implies $0 = \mathbf{g}_i \mathbf{v}^T$ for every i and

$$\mathcal{C}^{\perp} = \{\mathbf{v} \in \mathbb{F}_q^n,\ G\mathbf{v}^T = \mathbf{0}\}.$$

From $\mathcal{C}$ to $\mathcal{C}^\perp$

Generator matrix of $\mathcal{C}$: G
Parity check matrix of $\mathcal{C}^\perp$: G
Generator matrix of $\mathcal{C}^\perp$: H

From $\mathcal{C}^\perp$ to $\mathcal{C}$

Generator matrix of $\mathcal{C}^\perp$: H
Parity check matrix of $(\mathcal{C}^\perp)^\perp$: H
Generator matrix of $(\mathcal{C}^\perp)^\perp$: G

From $\mathcal{C}$ to $\mathcal{C}^{\perp}$

Generator matrix of $\mathcal{C}$: G
Parity check matrix of $\mathcal{C}^{\perp}$: G
Generator matrix of $\mathcal{C}^{\perp}$: H

From $\mathcal{C}^{\perp}$ to $\mathcal{C}$

Generator matrix of $\mathcal{C}^{\perp}$: H
Parity check matrix of $(\mathcal{C}^{\perp})^{\perp}$: H
Generator matrix of $(\mathcal{C}^{\perp})^{\perp}$: G

- Both definitions of dual are equivalent.
- The dual of $\mathcal{C}^{\perp}$ is $\mathcal{C}$: $(\mathcal{C}^{\perp})^{\perp} = \mathcal{C}$.

Repetition and single parity check codes

A generator matrix (in systematic form) of the repetition code:

$$[1|1\ldots,1].$$

A parity check matrix (in systematic form) over $\mathbb{F}_2$:

$$\left.\begin{bmatrix} 1 & \\ \vdots & \mathbf{I}_{n-k} \\ 1 & \end{bmatrix}\right\} \begin{array}{c}\text{generator matrix}\\ \text{for the single parity}\\ \text{check code}\end{array}$$

A self-orthogonal code $\mathcal{C}$

A code $\mathcal{C}$ which is included in its dual: $\mathcal{C} \subseteq \mathcal{C}^{\perp}$

The $(n, 1)$ repetition code over $\mathbb{F}_2$ is self-orthogonal if n even.

To have $(n-1) \equiv 1 \pmod{2}$, we need n even. Then $c_n = \sum_{i=1}^{n-1} x_i$ for both $(0, \ldots, 0)$ and $(1, \ldots, 1)$, and they are in the single parity check code.

A self-dual code $\mathcal{C}$

A code $\mathcal{C}$ which is equal to its dual: $\mathcal{C} = \mathcal{C}^{\perp}$

The $(4, 2)$ code over $\mathbb{F}_3$ (called tetracode) given by the generator matrix

$$\begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & -1 \end{bmatrix}$$

is self-dual.

The (4,2) tetracode over $\mathbb{F}_3$

$\mathcal{C}^\perp$ has generator matrix H

$$G = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & -1 \end{bmatrix}, \; H = \begin{bmatrix} -1 & -1 & 1 & 0 \\ -1 & 1 & 0 & 1 \end{bmatrix}$$

Rewrite H in systematic form:

$$H \to \begin{bmatrix} -1 & -1 & 1 & 0 \\ 0 & 2 & -1 & 1 \end{bmatrix} \to \begin{bmatrix} -1 & -1 & 1 & 0 \\ 0 & 1 & 1 & 2 \end{bmatrix} \to \begin{bmatrix} -1 & 0 & 2 & 2 \\ 0 & 1 & 1 & 2 \end{bmatrix}$$
$$\to \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 \end{bmatrix} = G$$

The (4,2) tetracode over $\mathbb{F}_3$

$\mathcal{C}^{\perp} = \{\mathbf{v} \in \mathbb{F}_q^n,\ \mathbf{c} \cdot \mathbf{v}^T = \mathbf{0} \text{ for all } \mathbf{c} \in \mathcal{C}\}$.

$$G = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & -1 \end{bmatrix},\ \mathbf{c} = (x_1, x_2, x_1 + x_2, x_1 - x_2)$$

Then for $\mathbf{v} = (v_1, v_2, v_3, v_4) \in \mathbb{F}_3^4$, we want:

$(v_1, v_2, v_3, v_4) \cdot \mathbf{c}^T = v_1 x_1 + v_2 x_2 + v_3(x_1 + x_2) + v_4(x_1 - x_2) = 0.$

This means $v_1 + v_3 + v_4 = 0$ and $v_2 + v_3 - v_4 = 0$. Solve to find $v_3 = v_2 + v_1$ and $v_4 = v_1 - v_2$.

Two definitions of a dual code

self-orthogonal code

self-dual code