Review Week 03

2022-10-10

Announcement:
Week 03 feedback → Blackboard (by 9 am Monday 17 OCT)
Reminder: Week 05 COURSEWORK!

Linear codes

- **The alphabet: a finite field $\mathbb{F}_q$. IF $q = p$ is a prime, $\mathbb{F}_p = \{0, 1, \ldots, p-1\}$.**
  - **Every non-zero symbol λ has a multiplicative inverse λ^{-1}; e.g., in $\mathbb{F}_{11}$, $2^{-1} =$** 6
- **The weight of a vector: for $\underline{v} \in \mathbb{F}_q^n$, $w(\underline{v}) = d(\underline{v}, \underline{0})$ (*the number of non-zero symbols in $\underline{v}$*); $d(\underline{u}, \underline{v}) = w(\underline{u} - \underline{v})$**

in $\mathbb{F}_{11}$: $2 \times 6 = 12 = 1$

- **Linear code: a subspace of the space $\mathbb{F}_q^n$**
- **The weight of the code: $w(C) = \min\{w(\underline{v}) : \underline{v} \in C, v \neq \underline{0}\}$ for $C \subseteq \mathbb{F}_q^n$. One has $w(C) = d(C)$ for linear C.**

defined unless $C = \{\underline{0}\}$ NULL CODE

- **Examples: the trivial code, the repetition code**
  - **Write the parameters of these codes:**

Trivial code $\mathbb{F}_q^n = \{(v_1, \ldots, v_n) \mid v_i \in \mathbb{F}_q\}$ LINEAR

$M = q^n$ $k = n$ $[n, n, 1]_q$-code

$d = w(\mathbb{F}_q^n) = 1$ as $1000\cdots0 \in \mathbb{F}_q^n$

$\mathrm{Rep}(n, \mathbb{F}_q) = \{(a, a, \ldots, a) \mid a \in \mathbb{F}_q\}$ Linear

$M = q$, $k = 1$, $[n, 1, n]_q$

The binary even weight code E_n

- $E_n = \{\underline{v} \in \mathbb{F}_2^n : w(\underline{v}) \text{ is even}\}$
- $E_n = \{(x_1, x_2, \ldots, x_n) \in \mathbb{F}_2^n : x_1 + x_2 + \cdots + x_n = 0 \text{ in } \mathbb{F}_2\}$ ← equivalent definition of En
- **As we can see, E_n is defined by a single *checksum***
- $E_3 = \{$ 000, 011, 101, 110 $\}$
- **Encoder for E_3. ENCODE: $\mathbb{F}_2^2 \to E_3$, ENCODE $((x_1, x_2)) = ($** $x_1, x_2, x_1 + x_2$ **$)$**
  - **appends the parity check bit**

Generating a linear code by a matrix

- **A $k \times n$ matrix G with linearly independent rows generates an $[n, k, d]_q$ linear code C**
- **The code is the image of ENCODE on $\mathbb{F}_q^k$, $\mathrm{ENCODE}(\underline{u}) = \underline{u}G$**
- **Row operations can change the matrix G, but do not change the code generated by G. *The code is the row space of G.***

$$C = \{ \underline{u}G \mid \underline{u} \in \mathbb{F}_q^k \} \qquad G = \begin{bmatrix} \underline{r_1} \\ \vdots \\ \underline{r_k} \end{bmatrix} \quad \underline{r_i} \in \mathbb{F}_q^n$$

$$\underline{u} = (u_1, \dots, u_k) \qquad \underline{u}G = u_1 \underline{r_1} + u_2 \underline{r_2} + \dots + u_k \underline{r_k}$$

The generator matrix in standard form

$$k \left\{ \left[\underbrace{\begin{matrix} 1 & & 0 \\ & 1 & \\ & & 1 \\ 0 & & \ddots \; 1 \end{matrix}}_{k \text{ columns}} \;\middle|\; \underbrace{\begin{matrix} * & \cdots \\ \cdots & * \end{matrix}}_{n-k} \right] \right.$$

This is $G = [\, I_k \mid A \,]$ for some $k \times (n-k)$ matrix A:

To find a generator matrix of C in standard form *if it exists*, bring any generator matrix to reduced row echelon form.

Example. Write down a generator matrix in standard form for E_3 without any calculations.

$$E_3 = \{000, 011, 101, 110\} \qquad M = 4, \quad k = \log_2 4 = 2$$

$$\underbrace{\boxed{G}}_{n} \Big\} k = \#\text{rows of } G = \text{inf. dim. of } C = \dim(C)$$

$$G = \left[\begin{matrix} \underbrace{\begin{matrix} 1 & 0 \\ 0 & 1 \end{matrix}}_{\text{standard form!}} & \begin{matrix} 1 \\ 1 \end{matrix} \end{matrix} \right]$$

Ex Check that G indeed generates E_3.

Example. A ternary code C is generated by $G = \begin{bmatrix} 2 & 2 & 2 & 0 \\ 2 & 0 & 1 & 1 \end{bmatrix}$. Find a generator matrix in standard form by (a) listing all codevectors; (b) bringing G to RREF. Find the parameters of C and determine if C is perfect/MDS.

Easy or difficult? Given a generator matrix of C over $\mathbb{F}_q$, find the parameters of C

- n
- k
- d (*important*)

Example. Bring the following matrix over $\mathbb{F}_2$ to standard form. Show that the weight of the code it generates is at least 2.

$$G = \begin{bmatrix} 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 \end{bmatrix}$$

$\mathbb{F}_3$

$$G = \begin{bmatrix} 2 & 2 & 2 & 0 \\ 2 & 0 & 1 & 1 \end{bmatrix} \xrightarrow{r_1 *= 2}$$

Bring G to standard form:

$$\longrightarrow \begin{bmatrix} 1 & 1 & 1 & 0 \\ 2 & 0 & 1 & 1 \end{bmatrix} \xrightarrow{r_2 += r_1} \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 2 & 1 \end{bmatrix}$$

$$\xrightarrow{r_1 -= r_2} \left[\begin{array}{cc|cc} 1 & 0 & 2 & 2 \\ 0 & 1 & 2 & 1 \end{array}\right]$$

Standard form $\longrightarrow$