5.2 Linear codes

finite field $\mathbb{F}_q$

a polynomial $f(x)$ in $\mathbb{F}_q$

$$f(x) = \sum_{i=0}^{d-1} c_i x^i \quad \Leftarrow \text{degree } d-1$$

$\boxed{\text{Thm: A polynomial of degree } d \text{ has at most } d \text{ roots!}}$

Linear code: c_1 and c_2 are codewords, then

$c_1 + c_2$ is also a codeword

$c_1 \in \mathbb{F}_q^n$ $\quad$ $c_2 \in \mathbb{F}_q^n$

$c_1 + c_2$ is elementwise addition, addition on each element defined by the field

- A codebook forms a subspace of the vector space $\mathbb{F}_q^n$

- An $[n, k]_q$-code is a code in $\mathbb{F}_q^n$ that forms a k-dimensional subspace, $1 \le k \le n$

  rate of the code: $\dfrac{\log|C|}{n \log|\Sigma|} = \dfrac{k}{n}$

- An $[n, k, d]_q$-code is $[n, k]_q$-code with minimal distance d.

- Singleton bound: $|C| \le q^{n-d+1}$

  $\Leftrightarrow k \le n - d + 1 \Leftrightarrow \underline{\underline{k + d \le n + 1}}$

… to describe a subspace:

- There are two ways to

Def.: Let C be an $[n,k]_q$-code. A matrix $G \in F_q^{n\times k}$ is said to be a generator matrix for C if its columns span C.

The matrix fixes an association between messages $x \in F_q^k$ and codewords $c = Gx$.

Def. Let C be an $[n,k]_q$ code. A matrix $H \in F_q^{(n-k)\times n}$ is said to be a parity check matrix for C if $Hc = 0$ for all $c \in C$.
(The rows of H span the orthogonal complement of C.)

Example: Binary repetition code with $n=3$ $(k=1)$.

$$G = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}. \quad H \in F_q^{2\times 3}, \quad H_1 = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$$

$$H_2 = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}$$

Example: $[7,4,3]_2$ - Hamming code

Message: $x_1 x_2 x_3 x_4$ (4 bits)

Codeword: $x_1, x_2, x_3, x_4, x_2 \oplus x_3 \oplus x_4, x_1 \oplus x_3 \oplus x_4, x_1 \oplus x_2 \oplus x_4$

$G \in F_2^{7\times 4}$ $\qquad$ $H \in F_2^{3\times 7}$

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ \ldots \end{pmatrix} \qquad H = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ \ldots \end{pmatrix}$$

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

Lemma: For any linear code

$$d(C) = \min_{\substack{c,c' \in C \\ c \neq c'}} \delta(c,c') = \min_{\substack{c \in C \\ c \neq 0}} \delta(c).$$

Proof: $\delta(c,c') = \delta(c-c',0)$ $\square$

The Hamming code is optimal!

Hamming bound $|C| \leq \dfrac{2^n}{\sum_{i=0}^{\lceil \frac{d-1}{2} \rceil} \binom{n}{i}}$

$n=7$, $|C| = 2^4$, $d=3$:

$$\Rightarrow 2^4 \leq \frac{2^7}{1+7} = 2^4 \Rightarrow \text{perfect code}$$

Def. The dual of a binary $[n,k]$-code C, the $[n,n-k]$-code $C^\perp$, is the space spanned by all codewords $c' \in F_q^n$ s.t.

$$\sum_{i=1}^n c_i c_i' = 0 \quad \text{for all } c$$

$$\Rightarrow G^\perp = H^T, \quad H^\perp = G^T.$$

5.3 Reed-Solomon codes

Family of codes with 3 parameters

q : alphabet size

n : block length

k : message length

with $k < n \leq q$

1) In this code a message $m = (m_0, m_1, m_2, \dots m_{k-1}) \in \mathbb{F}_q^k$ is first mapped to a polynomial

$$p_m(x) = \sum_{i=0}^{k-1} m_i x^i \quad \text{of degree } k-1$$

2) The codewords for m are obtained by evaluating $p_m(x)$ at n different points $x_1, x_2, \dots x_n$.

$$G = \begin{pmatrix} 1 & x_1 & x_1^2 & \dots & x_1^{k-1} \\ 1 & x_2 & x_2^2 & & \vdots \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & x_n & x_n^2 & \dots & x_n^{k-1} \end{pmatrix}$$

Thm: The above code has minimal distance $d = n-k+1$.

Proof: From Singleton bound $d \leq n-k+1$!

We need to show that $\delta(c) \geq n-k+1$ for all $c \in C$, $c \neq 0$.

$\Rightarrow$ It suffices to show that # zeros in c is smaller or equal to $k-1$

This follows since $p_m(x)$ can have at most $k-1$ roots! $\square$

Example: $q = 2^2$, $n = 4$ and $k = 2$ $(x_1 = 0, x_2 = 1, x_3 = 2, x_4 = 3)$

$0011 = \{0, 3\} \longrightarrow 3 + 0x \longrightarrow \{3, 3, 3, 3\} = 11111111$

$1010 = \{2, 2\} \longrightarrow 2 + 2x \longrightarrow \{2, 0, 1, 3\} = 10000111$

$\vdots$

$\Rightarrow$ we get a $[8, 4, 3]_2$-code