PARITY CHECK MATRICES.

Syndrome decoding

Let $u = (u_1, \ldots, u_n) \in Z_q^n$

$v = (v_1, \ldots, v_n) \in Z_q^n$

$\langle u, v \rangle = u_1 \cdot v_1 + u_2 \cdot v_2 + \ldots + u_n v_n$

$\langle u, v \rangle \in Z_q$ - scalar product of u and v

If $\langle u, v \rangle 0$ then

$u \perp v$ u is orthogonal to v

EXAMPLE

$\langle 2011, 1210 \rangle = 0$

$\langle 1212, 2121 \rangle = 2$

Th.

1. $\langle u, v \rangle = \langle v, u \rangle$

2. $w, u, v \in Z_q^n \quad ; \lambda, \mu \in Z_q$

$\langle \lambda u + \mu v, w \rangle = \lambda \langle u, w \rangle + \mu \langle v, w \rangle$

Let C is a (n, q^k) code

$C \subseteq Z_q^n$

Then $C^\perp$ (<u>orthogonal</u> to C or <u>dual</u> to C)

$C^\perp = \{ v \in Z_q^n \mid \langle v, u \rangle = 0$ for all $u \in C \}$

Examples 1) $q=2 \quad n=4$

$$C = \begin{matrix} 0000 \\ 1100 \\ 0011 \\ 1111 \end{matrix} \Rightarrow C^{\perp}=C$$

C is self-dual

2) $q=2 \quad n=3$

$$C = \begin{matrix} 000 \\ 101 \\ 011 \\ 110 \end{matrix} \qquad C^{\perp} = \begin{matrix} 000 \\ 111 \end{matrix} \Rightarrow K_{C^{\perp}}=1$$

$$G_C = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix} \Rightarrow K_C = 2$$

T. $(C^{\perp})^{\perp}=C$

T. Let G_C is a generating matrix then

$$v \in C^{\perp} \iff G_C v = 0$$

T: If $\dim C = k_C \Rightarrow$

$$\dim C^\perp = k_{C^\perp} = n - k_C$$

and $C^\perp$ is a (n, q^{n-k_C}) code

Consider a generating matrix for $C^\perp$

$$H = G_{C^\perp}$$

we will call H a <u>parity check</u> matrix for C

$$H = \underbrace{[\quad\quad]}_{n}\}n-k \qquad k = k_C$$

(T.)

$H G^{TR} = O$ – matrix of all zeros

For any $v \in C$

$Hv = 0$ - vector of all zeros

Any code G can be defined by its generating matrix G or check matrix H.

$$C = \{ v \in Z_q^n \mid Hv = 0 \}.$$

FOR $C = \begin{matrix} 0000 \\ 1100 \\ 0011 \\ 1111 \end{matrix}$ $\quad C^{\perp} = C$

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

$$v \in C \qquad H \begin{bmatrix} v_1 \\ v_2 \\ v_3 \\ v_4 \end{bmatrix} = 0 \Rightarrow$$

$$\begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix} \begin{bmatrix} v_1 \\ v_2 \\ v_3 \\ v_4 \end{bmatrix} = \begin{bmatrix} v_1 + v_2 \\ v_3 + v_4 \end{bmatrix} = 0$$

$$\begin{cases} v_1 + v_2 = 0 \\ v_3 + v_4 = 0 \end{cases} \Rightarrow \underline{\text{parity checking}} \text{ equations}$$

EXAMPLE Consider $(n, 2^{n-1})$

binary parity code

FOR THIS code $\mathbb{C}$

$$v \in \mathbb{C} \Leftrightarrow v_1 + v_2 + \dots + v_n = 0 \Leftrightarrow$$

$H = [1\,1\,1 \dots 1]$ $r = n - k = 1$.

(T)

Let $\mathbb{C}$ is (n, q^k) code

and $G = \overbrace{[I_k \mid P]}^{n}\}k$ is

generating matrix for C

Then $H = \overbrace{\left[-P^{TR} \mid I_{n-k}\right]}^{n}\}n-k$

$-P^{TR}$ is transposed P multiplied by (-1)

$H = [-P^{TR} \mid I_{n-k}]$ is a <u>standard</u> form for the check matrix

<u>EXAMPLE</u> $q=2$ $n=7$ $k=4$

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

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

(FOR THE BINARY CASE $\ominus = \oplus$)

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

— codeword of C.