LAGRANGE THEOREM

Let $C \in Z_q^n$ is a linear (n, q^k) code. Then

1) every $x \in Z_q^n$ belongs to exactly one coset of C
2) every coset contains exactly q^k vectors from Z_q^n
3) two different cosets do not intersect
4) There are q^{n-k} different cosets

EXAMPLE : $q=2$ $n=4$

$$G = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix} \quad k=2$$

$$C = \{0000, 1011, 0101, 1110\}$$

$$d(C) = 2$$

Cosets of C :

$$0000 + C = C$$

$$1000 + C = \{1000, 0011, 1101, 0110\}$$

$$0100 + C = \{0100, 1111, 0001, 1010\}$$

$$0010 + C = \{0010, 1001, 0111, 1100\}$$

$$1000 + C = 0011 + C$$

$$0010 + C = 1001 + C$$

Any vector with the minimal weight in the coset is called the coset leader

x is the coset leader $\Leftrightarrow$

$x \in a + C$

$\|x\| = \min_{y \in C} \|y\|$

Standard Array is a table representing Z_q^n with q^{n-k} rows and q^k columns

Each row is a coset of C

(C is a first row)

Coset leaders are in the first column.

EXAMPLE. The standard array for (4,4) binary code with $G = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix}$

↓ coset leaders			
C → 0000	1011	0101	1110
1000	0011	1101	0110
0100	1111	0001	1010
0010	1001	0111	1100

Let $\hat{x} = 0011$

To <u>decode</u> first detect that $\hat{x} \in 1000 + C$. Then add the coset leader $\hat{x} + 1000 = 1011$ (correct message)

Coset leaders are error patterns corrected by the code C

For the previous exampee C corrects all single errors except for 0001

Ex. $\hat{x} = 0100$? $x = 0000$ or $x = 0101$

Denote α_i the number of coset leaders of weight i. Then α_i is the number of errors with multiplicity i which is corrected by our code

$$0 \leq \alpha_i \leq \binom{n}{i}$$

If $d(C) = 2\ell + 1$

$$\alpha_i = \binom{n}{i} \quad (i = 1, 2, \ldots, \ell)$$

Consider the probability P_{corr} for error correction by code C $(q=2)$

$$P_{corr} = \sum_{i=0}^{n} \alpha_i \, p^i (1-p)^{n-i}$$

p - is the <u>bit distortion</u> rate

For the previous example

$\alpha_0 = 1$, $\alpha_1 = 3$, $\alpha_2 = \alpha_3 = \alpha_4 = 0$

For $p = 0.01$

$$P_{corr} = (1-p)^4 + 3p(1-p)^3 =$$

$$\approx 0.9897$$

By selecting good C

one can make $P_{corr} \to 1$

as $n \to \infty$

SHANNON'S THEOREM

Let p - is a bit rate distortion for the binary symmetrical channel

denote

$$\mathcal{C}(p) = 1 + p \log_2 p + (1-p) \log_2 (1-p)$$

$$= 1 - H(p)$$

$\mathcal{C}(p)$ is known as a

<u>capacity</u> of the channel

$H(p)$ is ~~entropy~~ <u>entropy</u>