

63

## LAGRANGE THEOREM

Let  $C \in \mathbb{Z}_q^n$  is a linear  $(n, q^k)$  code. Then

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

(84)

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 :

$$0000 + C = C$$

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

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

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

$$1000 + C = 0011 + C$$

$$0010 + C = 1001 + C$$

(85)

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

~~rep~~ representing  $\mathbb{Z}_q^n$  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  $\hat{x} = 0011$

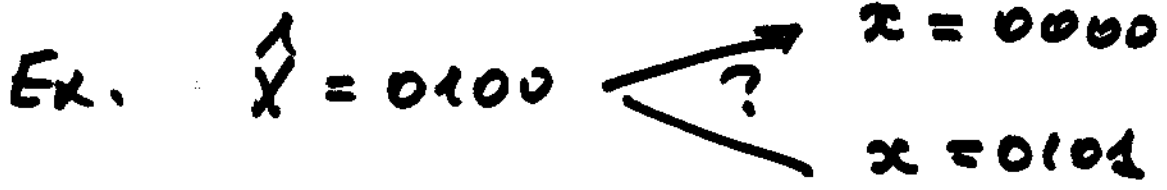
To decode first detect that

$\hat{x} \in 1000 + C$ . Then add the coset leader  $\hat{x} + 1000 = 1011$

correct message

Coset leaders are error patterns corrected by the code C

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



88

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

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

$$\text{If } d(C) = 2l + 1$$

$$\alpha_i = \binom{n}{i} \quad (i = 1, 2, \dots, l)$$

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

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

$p$  is the bit distortion rate  
For the previous example

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

For  $p = 0.01$

$$P_{\text{corr}} = (1-p)^4 + 3p(1-p)^3 = \approx 0.9897$$

(90)

By selecting good  $C$   
one ~~just~~ can make  $P_{\text{err}} \rightarrow 1$   
as  $n \rightarrow \infty$

### SHANNON'S THEOREM

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

denote

$$\begin{aligned} \mathcal{L}(p) &= 1 + p \log_2 p + (1-p) \log_2 (1-p) \\ &= 1 - H(p) \end{aligned}$$



$\zeta(p)$  is known as a capacity of the channel

$K(p)$  is ~~entropy~~ entropy

