LINEAR CODES

Let Z_q^n is an n-dim. space over $GF(q)$ q is a power of prime.

Code $C \subseteq Z_q^n$ is <u>linear</u> iff C is a <u>subspace</u>

$$(x, y \in C \Rightarrow x + y \in C$$

$$a \in GF(q), x \in C \Rightarrow ax \in C)$$

If C is a k-dim. subspace of Z_q^n then we will write that C is a (n, q^k) code

$$|C| = q^k$$

Then C has K information digits and n-K check digits

EXAMPLES:

1. Repetition codes are linear
2. PARITY CODES ARE LINEAR.
3. ISBN code is linear.

FOR LINEAR CODES

$$d(x,y) = \|x \ominus y\| \Rightarrow$$

code distance = smallest of weights of the nonzero code-words

Consider (n, q^k) code $C \subseteq \mathbb{Z}_q^n$

C is a k-dim. subspace in $\mathbb{Z}_q^n$. Let $v_1, v_2, \ldots, v_k \in C$ for a basis for C

Consider the matrix

$$G = \underbrace{\begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_k \end{bmatrix}}_{n} \Bigg\} k$$

G is known as a <u>generating matrix</u> for C

The same code C can have many generating matrices

Example $q=2$ $n=5$

$C = \{00000, 01011, 10110, 11101\}$

C is linear $k=2$ $|C| = 2^k = 4$

$G_1 = \begin{bmatrix} 01011 \\ 10110 \end{bmatrix}$, $G_2 = \begin{bmatrix} 01011 \\ 11101 \end{bmatrix}$

$G_3 = \begin{bmatrix} 10110 \\ 11101 \end{bmatrix}$

$G_4 = \begin{bmatrix} 10110 \\ 01011 \end{bmatrix}$