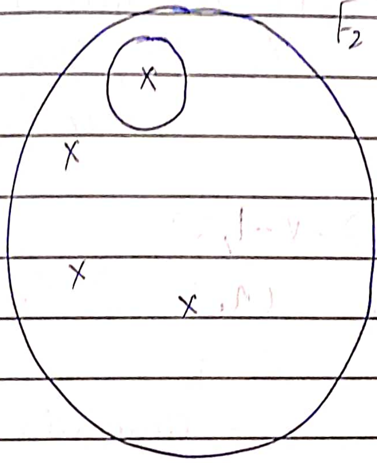
Hamming bound

↳ sphere packing bound.

<u>Bounds</u> for (n, k, d) codes
↳ means inequality.

$\mathbb{F}_2^n$



x → codewords

x → this sphere of t (t-error correcting code)
↳ called a Hamming sphere
↳ How many vectors can this hold?
⇒ set of all vectors which are 1 away from codeword
≡ all vectors differing from this codeword in 1 position → How many ways can this position be picked up?

$$= 1 + \binom{n}{1} + \binom{n}{2} + \dots + \binom{n}{t}$$

All these spheres can't overlap, if they do, the error-correcting codes disappear.
↳ dist betn 2 codewords?
let it be d, then $2t < d$
then largest possible $t = \left\lfloor \frac{d-1}{2} \right\rfloor$

Total of vectors inside hamming spheres of radius t = $\underbrace{2^k}_{\text{codewords}} \left(1+\binom{n}{1}+\dots\binom{n}{t}\right)$

Since the spheres are not overlapping, the total no. of vectors we're counting is less than/equal 2^n.

$$\therefore\ 2^k\left(1+\binom{n}{1}+\dots+\binom{n}{t}\right) \le 2^n$$

↳ codes satisfy this called perfect codes (eg → Hamming code)

eg → $(2^r-1,\ 2^r-r-1,\ 3)$

Repetition code $(n, 1, n) : C_n$

$C_n = \{00\dots0, 11\dots1\}$ → 2 codwords

↳ perfect for n=odd

↳ one is all 0's another is all 1's $2^1 = 2$ codwords

Gilbert - Varshamov bound

↳ not a bound for all codes

↳ existence ~~too~~ result

↳ construct a parity check matrix of r rows & maintain a min dist d

& keeping adding columns till $(n-1)$ columns

& when can n^{th} column be added?

n^{th} column $\neq$ non-zero vector

→ can't be sum of any previous ~~rows~~ columns, or columns.

$$1 + \binom{n-1}{1} + \binom{n-1}{2} + \dots + \binom{n-1}{d-2} < 2^r$$

$\underset{\sim}{uG}H^T = 0$

$\hookrightarrow$ rows of G & H orthogonal to each other

$H = [I_{n-k} \ \vdots \ P^T]$

Syndrome

$$r = (r_0, r_1, ---, r_{n-1})$$
$$= v + e \quad (\text{modulo}-2)$$

$$= (v_0, v_1, ---, v_{n-1}) + (e_0, e_1, ---, e_{n-1})$$

$$= (v_0 + e_0, v_1 + e_1, ---, v_{n-1} + e_{n-1})$$

where binary vector $e = (e_0, e_1, --, e_{n-1})$ = is error pattern

s (syndrome)
$$= (s_0, ---, s_{n-k-1}) = \underset{(1\times n)}{r}\underset{(n\times(n-k))}{H^T}$$

$\hookrightarrow s \neq 0 \Rightarrow$ errors in r

Undetected errors occur when $s = 0$, $\hat{r} \neq r$ & $\underset{\text{error pattern}}{e} \neq 0$

S depends only on "e"

Since

$$S = r \cdot H^T$$

$$= (v+e)H^T$$

$$= \underbrace{vH^T}_{0} + eH^T$$

0 since $v \to$ a valid codeword