if C is a linear code → it admits some efficient algo ($\text{poly}(n)$)

↳ Suppose C is a $\subseteq \mathbb{F}_q^n$ linear code with distance d (Block length of the code)

↳ There is an efficient encoding map $ENC : \mathbb{F}_q^k \to \mathbb{F}_q^n$

→ This encoding map is the multiplication by a generating map G → $ENC : x \to Gx$ and matrix mul we can do in poly time so efficient

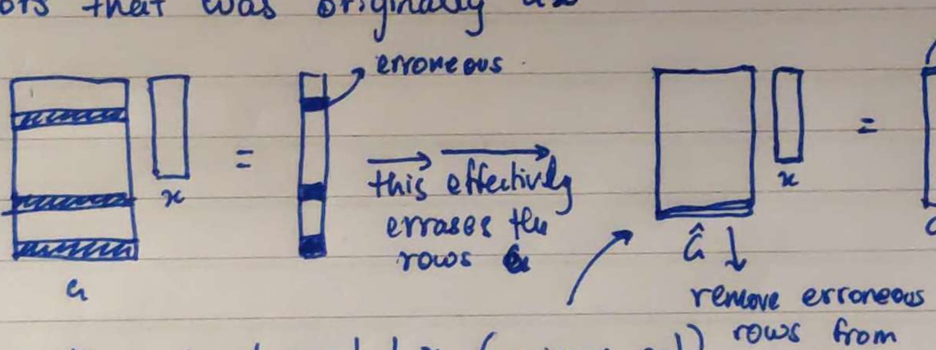
→ detect upto $d-1$ errors in ~~linear~~ poly time

→ One way to do this is through the parity matrix → given $\tilde{c}$ check if $H\tilde{c} = 0$ if so then $\tilde{c}$ is correct else wrong

→ Efficient cause all we need to do is matrix multiplication

→ there is an efficient algo to correct upto $d-1$ erasures

→ Use the generator matrix. Suppose we see some code words with some errors that was originally Gx:



know everything in this vector

The solution x to this system corresponds to the code-word that is consistant with atmost $d-1$ errasures

→ We know there is at most 1 x (unique sol) so we solve the linear system

Now the more important question is for any arbitrary linear code of distance d, can we correct up to $\lfloor \frac{d-1}{2} \rfloor$ errors effectively

→ No

This can be ~~throught~~ thought of as Given $\tilde{c} \in \mathbb{F}_q^n$, $G \in \mathbb{F}_q^{n \times k}$, find $x \in \mathbb{F}_q^k$ that minimises the hamming distance $\Delta(\tilde{c}, Gx)$

↳ This is very similar to the Maximum Likelihood problem which has been proven to be NP-hard