Error Correcting codes:

① Code up a message into a sequence of binary digits. (a,b,c) [If the message is longer, can send it in blocks of 3 digits].

② Want to transmit it over a noisy channel & errors are auto corrected.

(A) If $\exists$ at most one error for every 9 bits transmitted then can do the following:

Send (a,b,c,a,b,c,a,b,c). If one # is changed, it can be recovered.
If 2 are changed $\Rightarrow$ recovery may not be possible.

(B) Let $F = \{0,1\}$. Pick $v_1, v_2, v_3 \in F^n$ "cleverly", & L.I.

Transmit $u = av_1 + bv_2 + cv_3$. $\leftarrow$ a sequence of n binary digits.

① Note $\{v_1, \dots v_3\}$ L.I. $\Rightarrow \{v_1, \dots v_3\}$ is a basis of $\operatorname{span}\{v_1, v_2, v_3\} = C$

Thus given any $u \in \operatorname{span}\{v_1, v_2, v_3\}$, $\exists!$ a,b,c s.t. $u = av_1 + bv_2 + cv_3$.

$\Rightarrow$ After receiving u, the original message can be recovered.

② Detecting errors: If $\exists$ at most one bit which is corrupted then

$$r = u + e_i \quad \text{(for some } i \in \{1, \dots n\}\text{)}.$$

(r: what you receive; u: transmitted)

Suppose we chose $\{v_1, v_2, v_3\}$ s.t. $e_i \notin \operatorname{span}\{v_1, v_2, v_3\} = C$.

Then $u + e_i \notin C$ [Pf: Say $u + e_i = c \in C \Rightarrow u + e_i - c \in C \Rightarrow\Leftarrow$].

So if $r \notin C$ you know an error occurred.

③ Correcting errors: Let $c = r + e_j$.

(c: corrected message; r: received msg)

Want to choose C s.t. $\exists!$ j s.t. $r + e_j \in C$ (& have $j = i$, done).

This choice would $\Rightarrow$ error correction is possible

$r + e_j \in C \iff u + (e_i + e_j) \in C \iff e_i + e_j \in C$.

To summarize: Transmit $u = av_1 + bv_2 + cv_3$. $C = \operatorname{span}\{v_1, v_2, v_3\}$. $\{v_1, v_2, v_3\}$ L.I.

① Given u can recover a,b,c.

② $e_i \notin C$ $\forall i$ $\Rightarrow$ can detect one error.

③ $e_i + e_j \notin C$ $\forall i \neq j$ $\Rightarrow$ can correct one error!

Eg: $n = 6$. $v_1 = \begin{pmatrix} 1\\1\\1\\0\\0\\0 \end{pmatrix}$ $v_2 = \begin{pmatrix} 1\\0\\0\\1\\1\\0 \end{pmatrix}$ $v_3 = \begin{pmatrix} 1\\0\\1\\0\\1\\0 \end{pmatrix}$

$$C = \left\{ \begin{pmatrix} 0\\0\\0\\0\\0\\0 \end{pmatrix}, \begin{pmatrix} 1\\1\\1\\0\\0\\0 \end{pmatrix}, \begin{pmatrix} 1\\0\\0\\1\\1\\0 \end{pmatrix}, \begin{pmatrix} 1\\0\\1\\0\\1\\0 \end{pmatrix}, \begin{pmatrix} 0\\1\\1\\1\\1\\0 \end{pmatrix}, \begin{pmatrix} 0\\1\\0\\1\\0\\1 \end{pmatrix}, \begin{pmatrix} 0\\0\\1\\0\\1\\1 \end{pmatrix}, \begin{pmatrix} 1\\1\\0\\0\\1\\1 \end{pmatrix} \right\}.$$

So can transmit a 3 digit message using 6 digits & if at most one error occurs, it can be corrected.

Remark: Once v_1, v_2, v_3 are suitably chosen, the process of coding & decoding can be done by multiplying by a certain matrix.