Feb 1 **Def** (Code) A code of block length $\boxed{n}$ over an alphabet Σ is a subset of Σ^n

(Hamming / Image) i.e. $C \subseteq \Sigma^n$, $\bar{c} \in C$ ← codeword

$\boxed{k \le n}$

Alt. view $|C| = M$ $\boxed{q} = |\Sigma|$ ← alphabet size

(Shannon / mapping) $C : \underbrace{[M]}_{\overset{\text{def}}{=}\{1,\dots,M\}} \to \Sigma^n$

Def: Encoding function

dim (C) $= \log_q |C|$ typically $\boxed{k} \overset{\text{def}}{=} \dim(C)$

dimension $\Updownarrow$ $|C| = q^{\dim(C)}$ ← This is an integer $C : \Sigma^{\dim(C)} \to \Sigma^n$

Example: $\Sigma = \{0,1\}$ $q = 2$ (binary codes)

$(k=4, n=5)$

$C_{\oplus} : \{0,1\}^4 \to \{0,1\}^5$

XOR $C_{\oplus}(x_1, x_2, x_3, x_4) = (x_1, x_2, x_3, x_4, x_1 \oplus x_2 \oplus x_3 \oplus x_4)$

$C_{\oplus} \subseteq \{0,1\}^5$ $|C_{\oplus}| = 2^4$ $\dim C_{\oplus} = \log_2 |C_{\oplus}| = \log_2 2^4 = 4$

Repetition code: $q = 2$ $k = 4$, $n = 12$

$C_{3,rep} : \{0,1\}^4 \to \{0,1\}^{12}$

$C_{3,rep}(x_1, x_2, x_3, x_4) = (x_1, x_1, x_1, x_2, x_2, x_2, x_3, x_3, x_3, x_4, x_4, x_4)$

$|C_{3,rep}| = 2^4$

Redundancy: $C : \Sigma^k \to \Sigma^n$

Def 1: $n - k$

$\left.\begin{array}{l} n = 102,\ k = 100 \\ n = 4,\ k = 2 \end{array}\right\} n - k = 2$

$k \le n$

Def (Rate) Rate of C, $R(C) = \frac{k}{n}$

$R(C_{\oplus}) = \frac{4}{5}$

$R(C_{3,rep}) = \frac{4}{12} = \frac{1}{3}$

$0 \le R(C) \le 1$

← more redundancy → less redundancy

High Level goal: Optimal (?) tradeoff between redundancy & error correction?

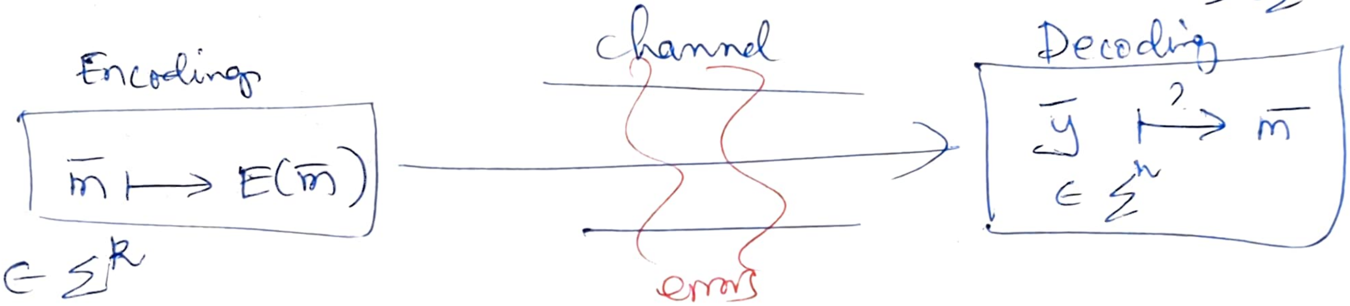
redundancy ↑ rate

error correction ↳ define next

Error Correction

Σ^k if k is an integer.

Def (Encoding function) $C \subseteq \Sigma^n \equiv E : [|C|] \longrightarrow \Sigma^n$



$\overline{m} \in \Sigma^k$

"Reverse" process

Def (Decoding function) $D : \Sigma^n \longrightarrow \Sigma^k$