Def (code) A code C of block length $\boxed{n}$ $\boxed{\text{Feb 2}}$
over an alphabet Σ is a subset of Σ^n i.e.

$$C \subseteq \Sigma^n \qquad \bar{c} \in C$$

codeword

Alternative view: $|C| = M$

$$C : [M] \longrightarrow \Sigma^n \qquad \boxed{q} = |\Sigma|$$

$[M] \stackrel{def}{=} \{1, .., M\}$

alphabet size.

Def $\dim(C) = \log_q |C|$ typically use $\boxed{k} \stackrel{def}{=} \dim(C)$

dimension

integer $\Rightarrow$ $C : \Sigma^{\dim(C)} \to \Sigma^n$ $\Rightarrow M = q^k$

Ex! $\Sigma = \{0,1\}$ $q = 2$ (binary codes)

Parity code: $|C_\oplus| = 2^4 \Rightarrow \dim(C_\oplus) = \log_2 2^4 = 4$

$C_\oplus : \{0,1\}^4 \to \{0,1\}^5$ $(n = 5, k = 4)$

EXOR
XOR

$$C_\oplus(X_1, X_2, X_3, X_4) = (X_1, X_2, X_3, X_4, X_1 \oplus X_2 \oplus X_3 \oplus X_4)$$

Repetition Code $C_{3,rep}$: repeat each bit 3 times

$\dim(C_{3,rep}) = 4$ $n = 12$

$$C_{3,rep}(X_1, X_2, X_3, X_4) = (X_1, X_1, X_1, X_2, X_2, X_2, X_3, X_3, X_3, X_4, X_4, X_4)$$

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

Def 1: $n - k$

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

$\to$ Use a relative measure:

Def (rate) Rate of a code C, $R(C) = \dfrac{k}{n}$

$R(C_\oplus) = \dfrac{4}{5}$ $0 \le R \le 1$

more redundancy $\longleftrightarrow$ less redundancy

$R(C_{3,rep}) = \dfrac{1}{3}$

High level goal: optimal$^{??}$ tradeoff between redundancy & error correction

$\uparrow$ rate

if k is an int

Σ^k

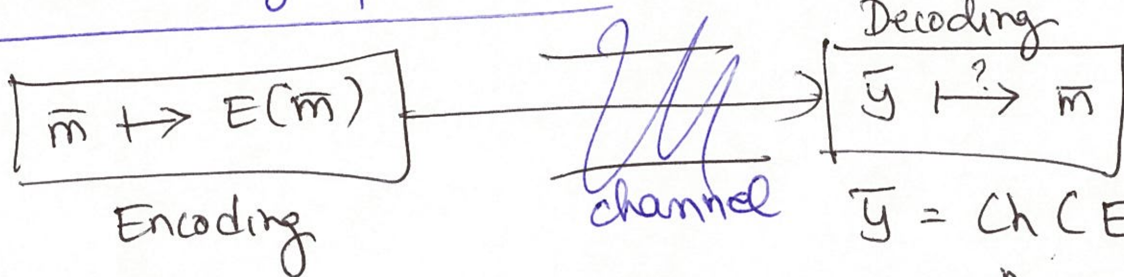
$|||$

Error-correction

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

"Reverse" process

Def (Decoding function): $D: \Sigma^n \to [|C|] \equiv \Sigma^k$



$\bar{y} = Ch(E(\bar{m}))$

$Ch: \Sigma^n \to \Sigma^n$

Capture notion of error correction

Note: You cannot hope to recover from arbitrary errors

Need: Bound how many error Ch can introduce.

Def (Hamming distance) $\bar{u}, \bar{w} \in \Sigma^n$

$\Delta(\bar{u}, \bar{w})$ = # locations where $\bar{u}$ & $\bar{w}$ differ

$|\{i \mid u_i \neq w_i\}|$

$\rightarrow$ notion is oblivious to location of difference

$\Delta(111, 010) = 2 = \Delta(111, 001)$

Def (Error correction): $C \subseteq \Sigma^n$, $1 \leq t \leq n$

C is t-error correcting if $\exists$ a decoding fn D s.t. $\forall \bar{m} \in [|C|]$ & any $\bar{y} = Ch(C(\bar{m}))$ s.t. $\Delta(\bar{y}, C(\bar{m})) \leq t$

$\Rightarrow D(\bar{y}) = \bar{m}$