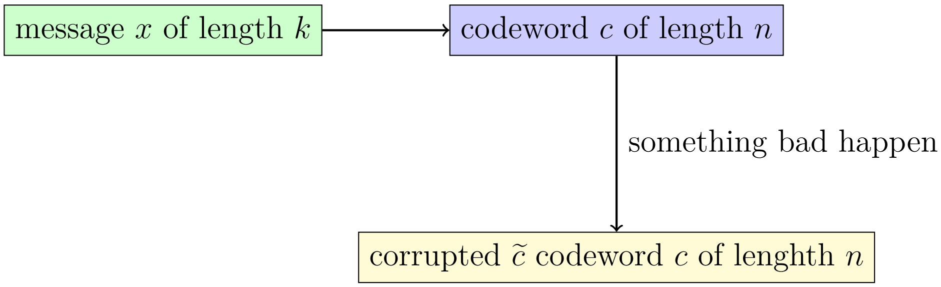
algebraic-coding-theroy-part01

XuGuoqiang

2022-11-26

Introduction


message x of length k
codeword c of length n
something bad happen
corrupted $\tilde{c}$ codeword c of lenghth n

Goal: Given $\tilde{c}$, recover x

Examples:

- Communication. Message corrupted in a noisy channel.
- Storage. SSD read, write, electrical, mechanical errors...

Goals:

- Handling Something Bad
- Recovering Info About x
- Minimize Overhead, $\frac{k}{n}$ As Large As Possible

- Doing All The Things Efficiently Possible

Question: What is hand-off between all the goals?

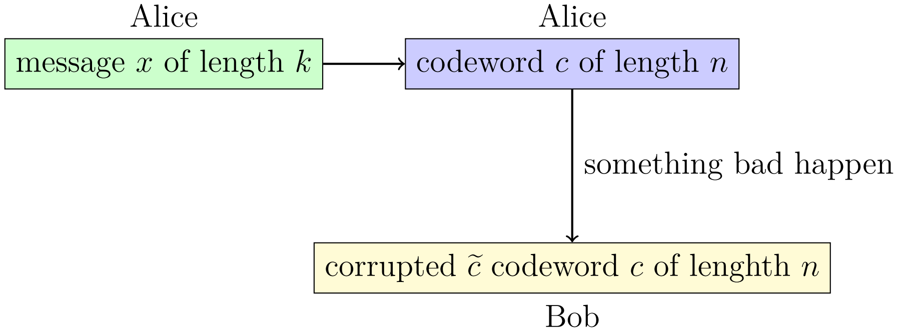
Basics

Definition:
A code C of blocklength n over an Alphabet Σ is $C \subseteq \Sigma_n$. The elements $c \in C$ are codewords.

Examples:

1. $C = \{HELLOWORLD, BRUNCHTIME, ALLTHETIME\}$ is a code of blocklength 10 over $\Sigma = \{A, B, C, \dots, Z\}$.
2. $C = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix}$ is a code of blocklength 4 over $\Sigma = \{0, 1\}$.

Relation to Alice and Bob


Alice
message x of length k
Alice
codeword c of length n
something bad happen
corrupted $\tilde{c}$ codeword c of lenghth n
Bob

Consider $ENC(\{0,1\}^3) \mapsto \{0,1\}^4$

$$\boxed{\{x_1, x_2, x_3\} \quad \mapsto \quad \{x_1, x_2, x_3, (x_1 \ + \ x_2 \ + \ x_3) \text{ mod } 2\}}$$

Example: $ENC(\{0,1,1\}) = (0,1,1,0)$

This Code can correct one ERASURE.
Example: $(0, X, 0, 1)$. X must be 1.

Definition:
ERASURE: You know which bit got lost, but you don't know the value.

This Code can detect one ERROR.
Example: $(0, 0, 0, 1)$

Definition:
ERROR: You know one bit is wrong, but you don't know which one.

More Definitions

Definition:
The HAMMING DISTANCE between x, y $\in \Sigma_n$ is $\triangle(x, y) = \Sigma_1^n \mathbf{1}\{x_i \neq y_i\}$