Review Week 01

CODING THEORY
Yuri . Bazlov @
manchester. ac. uk

2022-09-26

Information, channels and errors

Alphabet F: a finite set
Symbol: an element of F
Information: a long sequence of symbols

What is $\mathbb{F}_2 = \{0, 1\}$
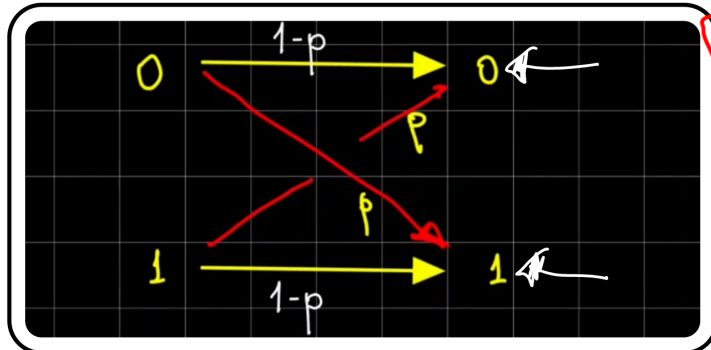
Model of information transmission: noisy channel

SENDER $\xrightarrow{x}$ CHANNEL $\xrightarrow{y}$ RECEIVER
NOISE
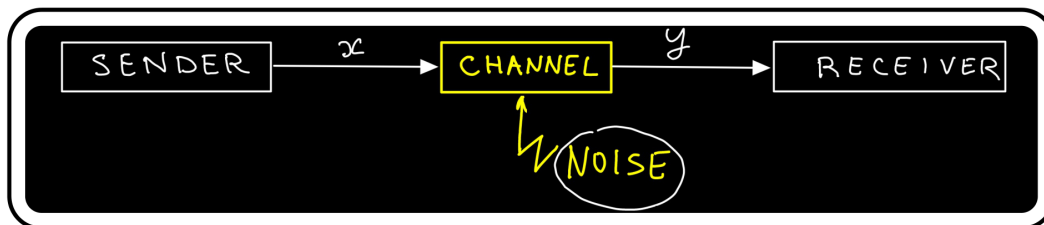
What event is *symbol error*?

$$y \neq x$$

The BSC(p) channel ← **MEMORYLESS** $0 \leq p < \frac{1}{2}$

0 $\xrightarrow{1-p}$ 0
p
p
1 $\xrightarrow{1-p}$ 1

N bits transmitted; probability of 0 errors?

"bit" = an element of $\mathbb{F}_2$
= "binary symbol"

$$(1-p)^N$$

Challenge

Send 80,000 bits via BSC(0.01). P(zero errors)? E(# of times need to resend until 0 errors)?

$$(1 - 0.01)^{80000}$$

$$\left(1 + \frac{x}{n}\right)^n \xrightarrow{n \to \infty} e^x$$

$$n \simeq 80000$$

$$\frac{x}{n} = -0.01 \Rightarrow x = -0.01 \times 80000$$
$$= -800$$

$$(1 - 0.01)^{80000} \approx e^{-800} \quad < 10^{-100}$$

$$e^{-8} < \frac{1}{10}$$

What is a code and how does it *detect* errors?

$$F^n = \{ (x_1, \ldots, x_n) : \quad x_i \in F, \ \forall i = 1, \ldots, n \}$$

$$\text{Code (of length } n \text{) is} \quad C \subseteq F^n, \quad C \neq \emptyset.$$

Worked examples: $E_3 = \{ 000, 011, 101, 110 \} \subseteq \mathbb{F}_2^3$ } binary codes of length 3

$Rep(3, \mathbb{F}_2) = \{ 000, 111 \}$

Detected and undetected errors

| SENDER | Codeword sent $\underline{c} \in C$ → | CHANNEL | received word $\underline{y} \in F^n$ → | RECEIVER |

DETECTED
ERROR:
$\underline{y} \notin C$

Assume that the codeword 111 of $Rep(3, \mathbb{F}_2)$ is sent. Describe the following events and give examples:

- no error ——————— $y = 111$
- detected error ——————— 010 as $010 \notin Rep(3, \mathbb{F}_2)$
- undetected error ——— 000

The Hamming distance

$F = \{1, 2, 3\}$

$$d(\underline{x}, \underline{y}) = \#\{ i : \ 1 \leq i \leq n, \quad x_i \neq y_i \}$$

$d(123, 321) =$
123
321 $d = 2$
X ✓ X

Correcting errors

A decoder for C is a function $\text{DECODE} : F^n \rightarrow C$ such that $\text{DECODE}(\underline{y})$ is a nearest neighbour of $\underline{y}$ in C.

| SENDER | Codeword sent $\underline{c} \in C$ → | CHANNEL | received word $\underline{y} \in F^n$ → | → | RECEIVER |

Draw all 3-bit binary words and show how each word is DECODEd to a codeword of $Rep(3, \mathbb{F}_2)$.

RECEIVED 101 ⟶ DECODE to 111

Challenge: can an undetected error be corrrected?