Tutorial 1 ENG

15 September 2021 13:52

IN054

Homework: 6-7 sets 6-8 exercises

↓

1st next week

1st MAX points

→ 85% MAX

→ 75% . .

⋮

Sources of information

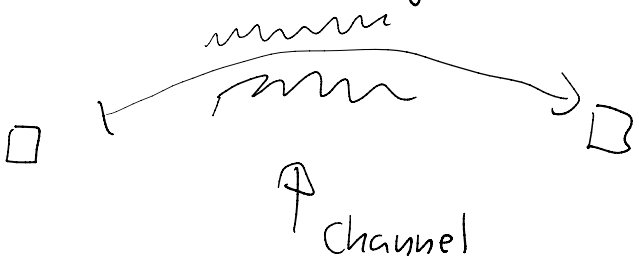
→ Study materials in IS

→ Exercise book

→ Discussion forums in IS

Basics of coding theory

How to send signals reliably over noisy channels?



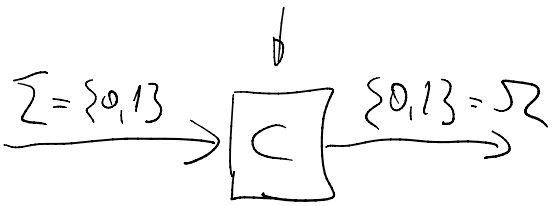
Σ → signal alphabet "input" alphabet

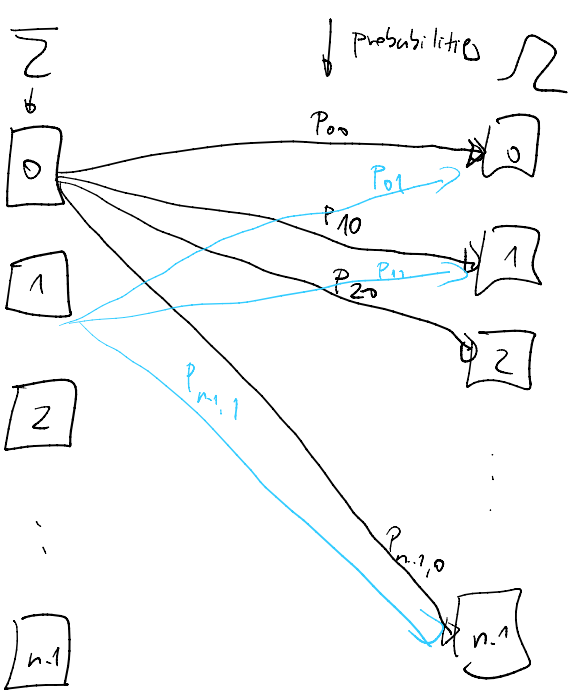
$\Sigma \approx \{0,1\}$

Ω → output alphabet $\Sigma = \Omega$

↓

$\Sigma - Sm12 \longrightarrow Sm12 - \Sigma$





$P_{00} + P_{10} + \dots + P_{n-1,0} = 1$

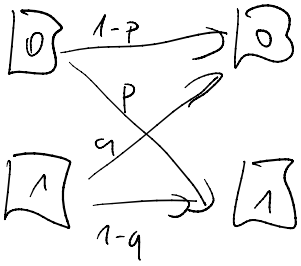
$P_{01} + P_{11} + \dots + P_{n-1,0} = 1$

$P_{0,n-1} + \dots + P_{n-1,n-1} = 1$

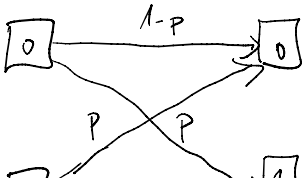
$P_{k|e} = P(k|e)$ ⇝ k was received if e was sent

$$\left\{P_{k|e}\right\}_{\substack{k \in \Omega \\ e \in \Sigma}}$$

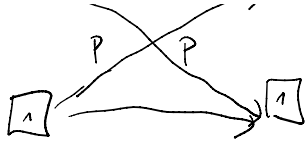
$\Sigma = \Omega = \{0,1\}$

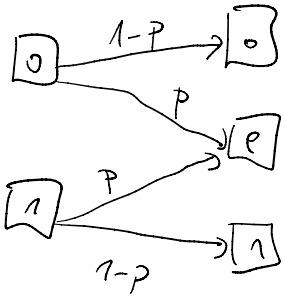


⇝ binary channel



⇝ binary symmetric channel



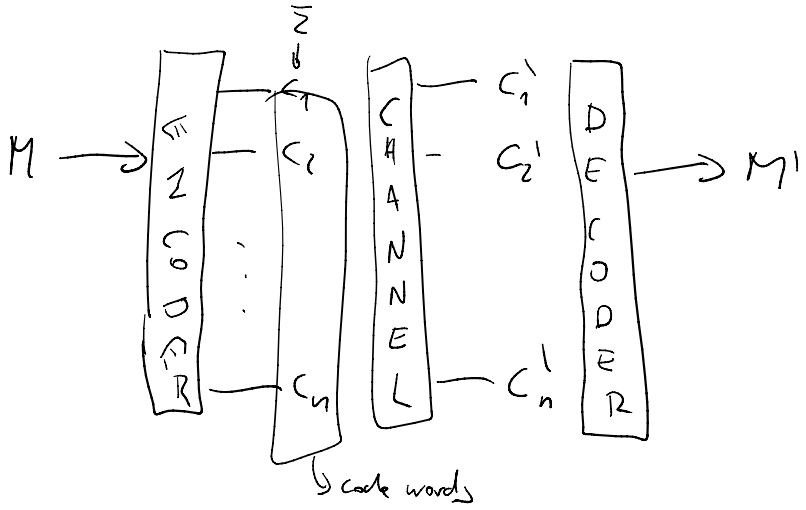


0' message not received !

Binary channel

How to send messages

messages = strings of signals



BSC w.p. of error $p < 1/2$

$M = \{0,1\}$ Enc: $0 \to 0$ $\in M$ $\in \Sigma$

$1 \to 1$

$\in M$ $\in \Sigma$

$0 \xrightarrow{1-p} 0$

$1 \xrightarrow{p} 0$

if you receive '0' how do you decode it?

'0' $\in \Sigma \to 0 \in M$ ← this is more probable

'1' $\in \Sigma \to 1 \in M$!

$0 \in \Omega \rightarrow 0 \in '1'$ ← this is more probable,

$'1' \in \Omega \rightarrow 1 \in M$ because $\boxed{1-p > p}$

Principle of maximum likelyhood

$M \in \{0,1\}$ $\quad \overset{\in M}{0} \rightarrow 000 \in \Sigma^3$ ENCODER $\quad \{000, 100, 010, 001\} \rightarrow '0'$ DECODER

$\Sigma \in \{0,1\}$ $\quad 1 \rightarrow 111 \in \Sigma^3$ $\quad \{111, 110, 101, 011\} \rightarrow '1'$

$\in M$

$$P(000 \mid 001) = (1-p) \cdot (1-p) \cdot p \overset{\text{in } b}{\text{ or }}$$

$$P(111 \mid 001) = p \cdot p \cdot (1-p)$$

Repetition code ~ repeat the message bit $2\ell+1$ times

achieves arbitrarily low probability of wrong decoding.

$M \in \{0,1\}$ $\quad$ ENC $\quad$ DEC $\in R$

$\Sigma \in \{0,1\}$ $\quad 0 \rightarrow \underbrace{0 \dots 0}_{2\ell+1 = n}$ $\quad \#'1' \geq \ell+1 \rightarrow 1 \in M$

$\Omega \in \{0,1\}$ $\quad 1 \rightarrow \underbrace{1 \dots 1}_{2\ell+1}$ $\quad \#'1' < \ell+1 \rightarrow 0 \in M$

$p < 1/2$

$$\Pr(\text{correct decoding}) = \sum_{i \in 0}^{\ell} \binom{2\ell+1}{i} p^{i} (1-p)^{2\ell+1-i}$$

'000 0'

i errors can happen in this many positions

$$\lim_{\ell \to \infty} \Pr(\text{correct decoding}) = 1$$

$$\frac{\#\text{Messages}}{\#\text{channel uses per message} = \text{length of codewords}} = \frac{2^{\ell}}{2\ell+1} \underset{\ell \to \infty}{=} 0$$

Hamming distance

$\Omega = \Sigma = \{0,1\}$

$C_i = \{0,1\}^n \qquad C_i \in C \qquad C \subseteq \{0,1\}^n$

C - code

C_i - code word

$\text{Ham}(c_i, c_j)$ the number of positions in which c_i and c_j differ

$\in \{1, 2, 3, 4\}$

Ex. 1.1 $C = \{10001, 00110, 11010, 01101\}$

$\text{Ham}(10001, 00110) = 4$ $\quad \text{Ham}(00110, 11010) = 3$

$\text{Ham}(10001, 11010) = 3$ $\quad \text{Ham}(00110, 01101) = 3$

$\text{Ham}(10001, 01101) = 3$ $\quad \text{Ham}(11010, 01101) = 4$

$n = 5$ length of codewords

$M = 4$ number of codewords

} efficiency

$d = 3$ minimum distance $\rightsquigarrow$ the larger the distance, the more errors are necessary for wrong decoding

more errors are less likely than ...

errors are necessary for wrong decoding
more errors are less likely than less errors

Error detection: if at most $d-1$ errors happen, then an error is detected: output is not a codeword

Error correction → $d = 2t+1$ then code can correct up to t errors.

Maximum likely hood: 1. receive $y \in \Sigma^n$
2. Calculate $\forall c_i \in C$ $Hamm(y, c_i)$
3.) Decode as c_i with smallest $Hamm(c_i, y)$

Ex. 1.6
decode 10101 $C = \{10001, 00110, 11010, 01101\}$

$Hamm(10101, 10001) = 1$ ✓
$Hamm(10101, 01101) = 2$
$Hamm(10101, 11010) = 3$
$Hamm(10101, 01101) = 4$

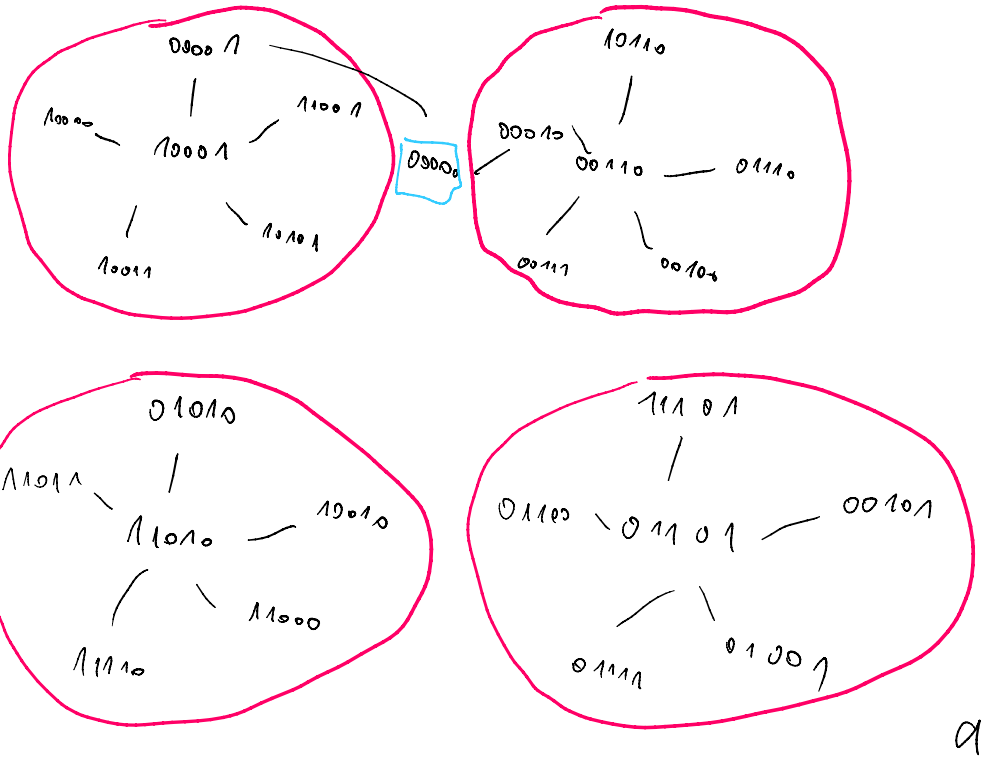
$A_q(n, M)$ = the largest n of a code with M codewords of lenght n.

↓
alphabet size
$q = ?$

Sphere packing bound $C = \{10001, 00110, 11010, 01101\}$

Sphere packing bound

$C = \{10001, 00110, 11010, 01101\}$



$q = 2k+1$

$$M \cdot \left(\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \binom{n}{2} \right) \leq 2^n$$

$=$

↓

Perfect code

Code equivalence

C_1 and C_2 are equivalent iff

C_1 can be constructed from C_2 by a string of following operations:

1.) permutation of the positions of the code

2.) permutation of symbols in a fixed position

$C_0 = \{10001, 01101, 00110, 11010\}$

$C_1 = \{01001, 10101, 00110, 11010\}$

$C_2 = \{00001, 11101, 01110, 10010\}$