2016. november 23., szerda 16:25

Problem: How to transfer data reliably over an unreliable channel?

$X \to$ [unreliable channel] $\to Y$

$R := \frac{k}{n}$ data rate (speed)

Channel coding theorem: $R \leq C$: $C = \max_{P(x)} I(X,Y) = \max_{P(x)} H(Y) - H(Y|X)$

How to calculate C?

Characterization of the channel:

$X \in \{\alpha_1, \alpha_2 \dots \alpha_N\}$, $Y = \{\alpha_1 \dots \alpha_N\}$

$P_{ij} = P(Y=\alpha_i | X=\alpha_j) \to P_{yx} = P(Y=y|X=x)$

$\underline{\underline{P}}$

$\sum_y P_{yx} = 1 : \forall x$

"Symmetric channel":

The column vectors of $\underline{\underline{P}}$ are permutations of each other!

$$\begin{pmatrix} 0.1 & 0.2 & 0.7 \\ 0.2 & 0.1 & 0.2 \\ 0.7 & 0.7 & 0.1 \end{pmatrix}$$

$\underline{\underline{P}} \neq \underline{\underline{P}}^T$ ← that would be a symmetric matrix

↳ entropy-column

$$\sum_y P_{yx} \operatorname{ld} \frac{1}{P_{yx}} = \sum_y P(Y=y|X=x) \cdot \operatorname{ld} \frac{1}{P(Y=y|X=x)} = H(\underline{r})$$

$$C = \max_{P(x)} H(Y) - H(Y|X) = \sum_x P(x) \sum_y P(y|x) \operatorname{ld} \frac{1}{P(y|x)} = \left(\sum_x P(x)\right) H(\underline{r})$$

$H(Y)$: $\operatorname{ld}(N)$; $H(Y|X)$: $\sum_x \sum_y P(x,y) \operatorname{ld} \frac{1}{P(y|x)}$; $\sum_x P(x) = 2$

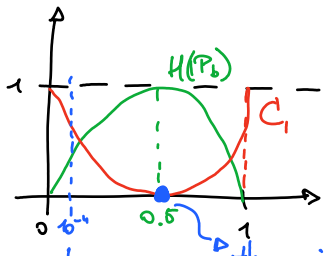
Application – channel capacity of BSC (Binary stochastic channel?)

$\underline{\underline{P}} = \begin{pmatrix} P_{00} & P_{01} \\ P_{10} & P_{11} \end{pmatrix} = \begin{pmatrix} 1-P_b & P_b \\ P_b & 1-P_b \end{pmatrix}$ ← symmetric (in weak and strong sense as well)

↑ probability of transmitting 1 and receiving 0

$P_b = P(Y \neq X)$

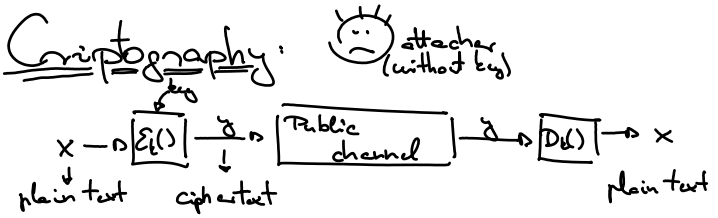
$C = \operatorname{ld} 2 - (1-P_b) \operatorname{ld} \frac{1}{1-P_b} - P_b \operatorname{ld} \frac{1}{P_b} = 1 - H(P_b)$



P_b that is a realistic channel

there is no information transfer possible at that point

Criptography:



Construct: $E_k(x) = y$?

→ $D_k(y) = x$ ⇒ easy if key is known, and "almost imposible" without the key.

Almost imposible: Attacker does not have enough compitation capacity that can decode ciphertext within the time when mensage is valid

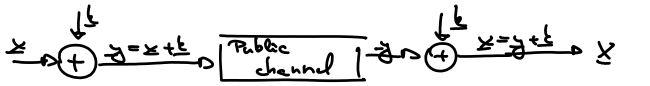
Type of attacks:

→ active: destroy the information by destroying channel ⇒ that is not our concern

→ pasive: get the information out of ciphertext

- ciphertext attacks: $y_k : k = 1 \dots K$
- plain-ciphertext attacks: $(x_k, y_k) : k = 1 \dots K$
- governed plain-ciphertext attacks: $(x_k, y_k) : k = 1 \dots K$

One Time Pad (OTP) – perfect encription



$$P(\underline{Y}=y \mid \underline{X}=x) = P(\underline{Y}=\underline{x}+\underline{k} \mid \underline{X}=\underline{x}) = P(\underline{k}=y+\underline{x}) = \frac{1}{2^N}$$

$$P(\underline{Y}=y) = \sum_x P(\underline{Y}=y \mid \underline{X}=x) P(\underline{X}=x) = \frac{1}{2^N} \sum_x P(\underline{X}=x) = \frac{1}{2^N} \sum_x P(\underline{X}=x) = \frac{1}{2^N} \Rightarrow$$

$$\Rightarrow P(\underline{Y}) = P(\underline{Y} \mid \underline{X}) \rightarrow \underline{X} \text{ and } \underline{Y} \text{ are statistically independent}$$

Commutative encription:

$$E_{k_b}(E_{k_a}(x)) = E_{k_a}(E_{k_b}(x))$$

1) $y_a = E_{k_a}(x) \rightarrow$ transmision

2) $y_b = E_{k_b}(y_a) = E_{k_b}(E_{k_a}(x)) \rightarrow$ transmision

3) $D_{k_a}(y_b) = D_{k_a}(E_{k_b}(E_{k_a}(x))) = D_{k_a}(E_{k_a}(E_{k_b}(x))) = E_{k_b}(x) = y_c \rightarrow$ transmission

4) $D_{k_b}(y_c) = D_{k_b}(E_{k_b}(x)) = x$