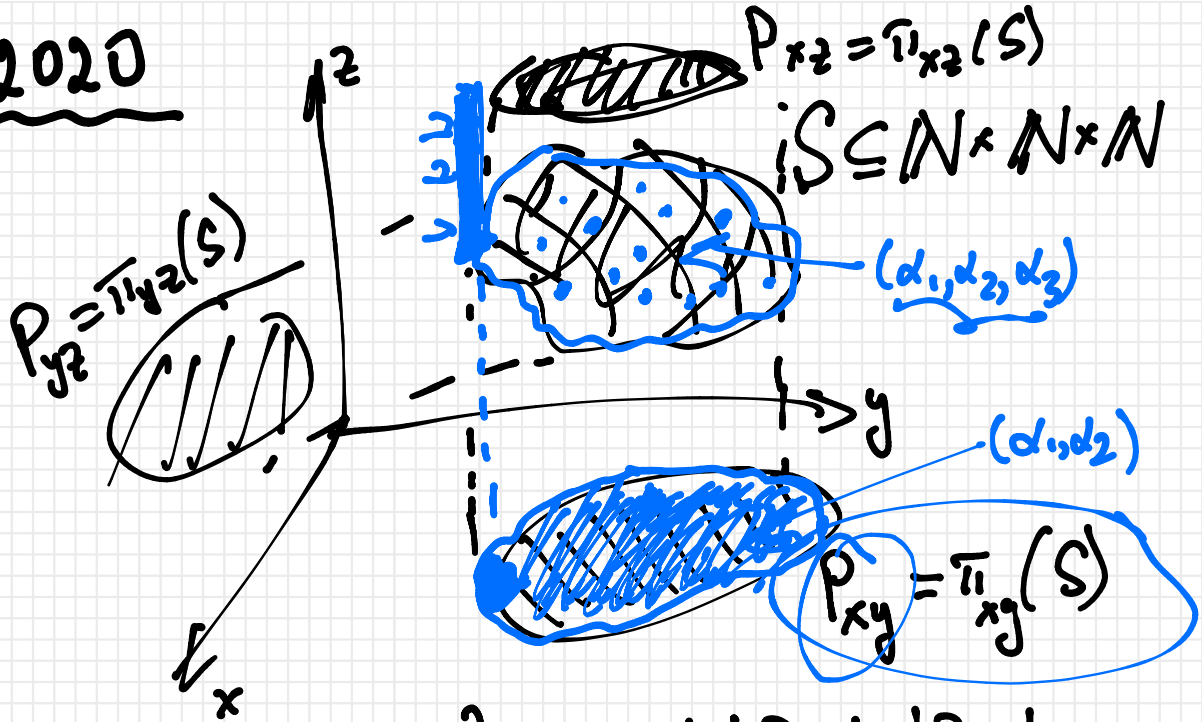
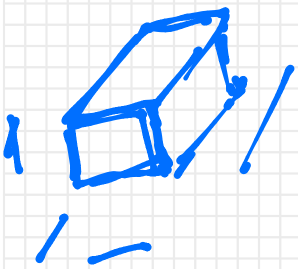
15.12.2020





$$|S|^2 \le |P_{xy}|\cdot|P_{xz}|\cdot|P_{yz}|$$

$$2H(\alpha_1,\alpha_2,\alpha_3) \le H(\alpha_1,\alpha_2)+H(\alpha_1,\alpha_3)+H(\alpha_2,\alpha_3)$$

$(\alpha_1,\alpha_2,\alpha_3)$

$\Downarrow$

point aléatoire de S

1° $S = \{s_1,\dots,s_K\}$

$\underbrace{\tfrac{1}{K} \;\dots\; \tfrac{1}{K}}$

S

$w = (n_i, m_i, \ell_i)$

s_i

$\downarrow \quad \downarrow \quad \downarrow$

$(\alpha_1,\alpha_2,\alpha_3)$

$$H(\alpha_1,\alpha_2,\alpha_3) = \underbrace{\log|S|}_{\log K}$$

$$2\cdot\log|S| = 2H(\alpha_1,\alpha_3,\alpha_3) \overset{2^\circ}{\le} H(\alpha_1,\alpha_2) + H(\alpha_1,\alpha_3) + H(\alpha_2,\alpha_3)$$

$$\wedge\, 3^\circ \qquad \wedge\, 3^\circ \qquad \wedge\, 3^\circ$$

$$\log|P_{xy}| + \log|P_{xz}| + \log|P_{yz}|$$

(a) $2\log|S| \le \log|P_{xy}| + \log|P_{xz}| + \log|P_{yz}|$

(b)

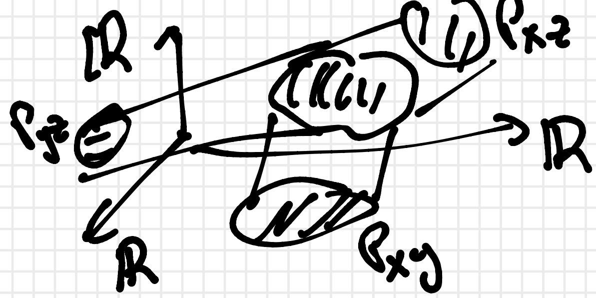
$$\log|S|^2 \le \log\left(|P_{xy}|\cdot|P_{xz}|\cdot|P_{yz}|\right)$$

$$\boxed{|S|^2 \le |P_{xy}|\cdot|P_{xz}|\cdot|P_{yz}|}$$ ← discr.

$(CM^3)^2$ $\underbrace{CM^2 \quad CM^2 \quad CM^2}_{CM^6}$

CM^6

$$(\mu(S))^2 \le \mu(P_{xy})\cdot\mu(P_{xz})\cdot\mu(P_{yz})$$



$S \subseteq \mathbb{R}^3$

$m = (m_1 \ldots m_n)$

$$\boxed{e_i = m_i \oplus k_i} \qquad i = 1 \ldots n$$

$k = (k_1 \ldots k_n)$

$\Pr[k_i = {}^0_1] = 1/2$

$(k_1 \ldots k_n)$: uniforme sur $\{0,1\}^n$

$e = (e_1 \ldots e_n)$

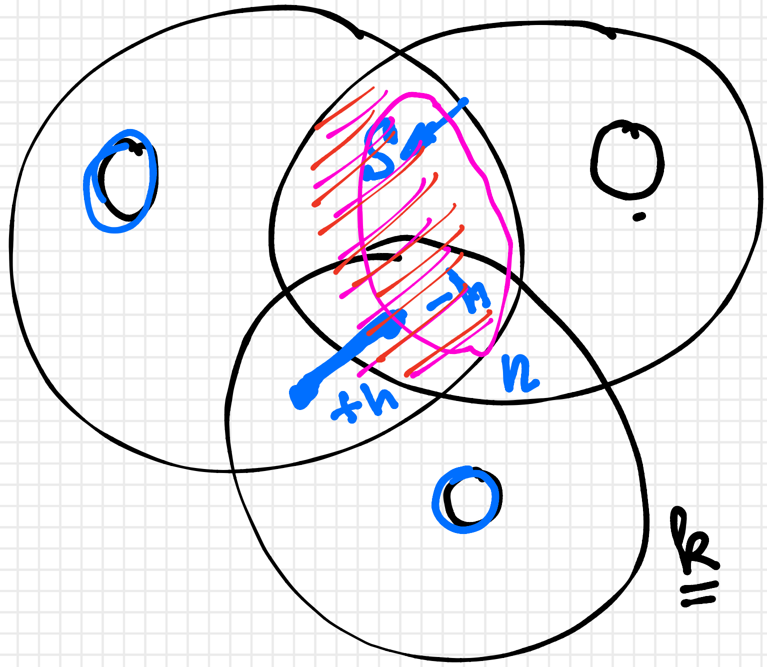
m $e_i := m_i \oplus k_i$

k

?

$m_i := e_i \oplus k_i$

k



$$c = m \oplus k$$

$$\Updownarrow$$

$$m \oplus k \oplus e = \underbrace{(0 \ldots 0)}_{n}$$

$$1^\circ \quad H(e|m,k) = 0$$

$$H(m|e,k) = 0$$

$$H(k|m,e) = 0$$

$$n = H(k) = 0 + 0 + n$$

$$H(m) = 0 + 0 + S = S \leq n$$

$$H(e) = \underbrace{S - h + n} \leq \underbrace{n}$$

$$\Updownarrow$$

$$S - h \leq 0$$

$$\Updownarrow$$

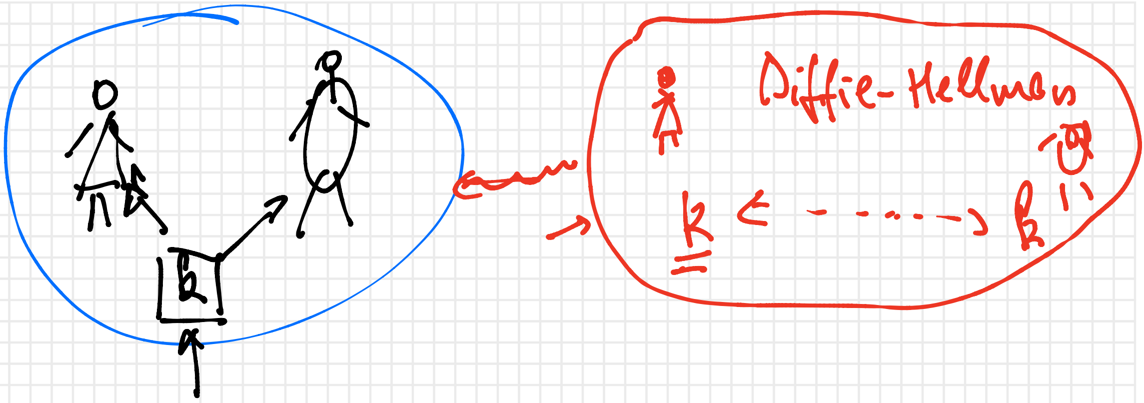
$$I(m:e) \leq 0$$

$$= 0$$

$$\rightarrow \boxed{I(m:e) = 0}$$

Vernam

1°



2°

$e_i = m_i \oplus k_i$

$m_i = k_i \oplus e_i$

e_i

$|k| = \#\text{bit dans } m$

$m \xrightarrow{\text{Huffman}} m'$

$e_i = m'_i \oplus k_i$

$m'_i = e_i \oplus k_i \rightarrow m$

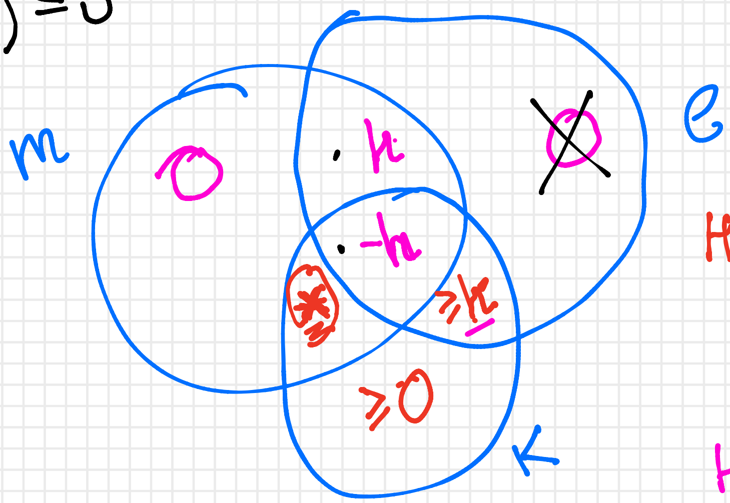
$|m'| \approx H(m)$

$|k| \approx H(m)$

Th (m,k,e) [Shannon]

- 1° $H(m \mid k,e)=0$
- 2° ~~$H(e \mid m,k)=0$~~
- 3° $I(m:e)=0$

$\Rightarrow H(k) \geq H(m)$



$$H(k) = * + (-h) + \cdots + \cdots$$

$$\vee\!\!/$$

$$H(m) = 0 + * + h - h$$