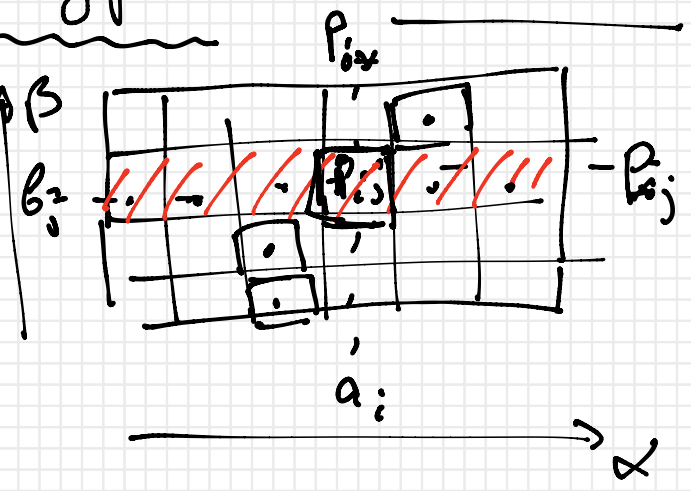
Information theory and crypto. 01/12/20

$H(\alpha|\beta)$

(α,β)



$$\begin{cases} H(\alpha,\beta) = \sum p_{ij} \log \frac{1}{p_{ij}} \\ H(\alpha) = \sum p_{i*} \log \frac{1}{p_{i*}} \\ H(\beta) = \sum p_{*j} \log \frac{1}{p_{*j}} \end{cases}$$

$p_{ij} = Pr[\alpha = a_i \,\&\, \beta = b_j]$

$\sum p_{ij} = 1$

$p_{i*} = \sum_j p_{ij}$

$p_{*j} = \sum_j p_{*j}$

$H(\alpha|\beta=b_j)$ $\quad \beta = b_j$

$$Pr[\alpha = a_i | \beta = b_j] = \frac{Pr[\alpha = a_i \;\beta = b_j]}{Pr[\beta = b_j]}$$

$$H(\alpha|\beta) = \sum_j Pr[\beta = b_j] \cdot H(\alpha|\beta=b_j) \quad \text{Def}$$

$H(\alpha|\beta=b_j) = 0$

Properties

1. $H(\alpha|\beta) \geq 0$
2. $H(\alpha|\beta) = 0 \iff \forall j \; H(\alpha|\beta=b_j) = 0$

$\forall j \; \exists! \, i : Pr[\alpha = a_i | \beta = b_j] > 0$

$\iff$ ② α est une fonction déterministe de β

③ $H(\alpha,\beta) = H(\beta) + H(\alpha|\beta)$

$$\begin{matrix} \| & & \| & & \| \\ \dots & & \dots & & \dots \end{matrix}$$

$$= H(\alpha) + H(\beta|\alpha)$$

④ $H(\alpha|\beta) \leq H(\alpha)$

$H(\alpha|\beta) = H(\alpha) \Leftrightarrow \alpha$ et β sont indep.

$H(\alpha|\beta) = H(\alpha,\beta) - H(\beta)$

$H(\alpha,\beta) - H(\beta) \leq H(\alpha)$

$H(\alpha,\beta) \leq H(\alpha) + H(\beta)$ $=$

Rem.: (α,β,γ) $(\alpha_1, \alpha_2, \dots, \alpha_k)$

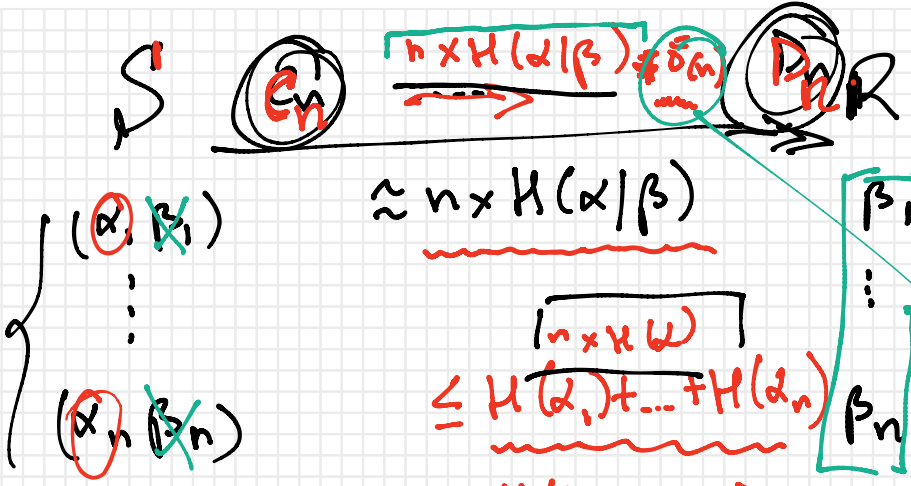
$H(\alpha | \langle\beta,\gamma\rangle)$

$H(\alpha_4, \alpha_5, \alpha_7 | \alpha_1, \alpha_9, \alpha_{25})$

$H(\alpha|\beta)$

(α_i, β_i)

i.i.d



Th $\forall \varepsilon > 0 \quad \forall \lambda > H(\alpha|\beta) \quad \exists (C_n, D_n)$

$C_n : (\alpha_1 \beta_1) \ldots (\alpha_n \beta_n) \rightsquigarrow \{0,1\}^{\lceil \lambda \cdot n \rceil}$

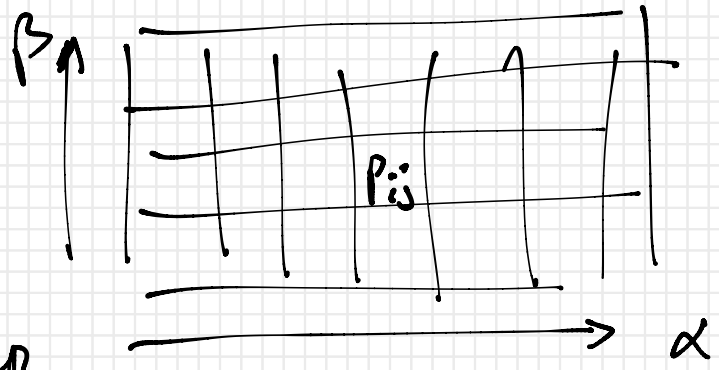
$D_n : \{0,1\}^{\lceil \lambda n \rceil} \times (\beta_1 \ldots \beta_n) \rightsquigarrow (\alpha_1 \ldots \alpha_n)$

$\Pr[\text{error}] < \varepsilon \quad [\to 0 \quad n \to \infty]$

$+ \delta(n)$

Def $I(\alpha:\beta) := H(\beta) - H(\beta|\alpha)$ ← mutual info ≥ 0

"how useful is α to describe β?"



① ≥ 0

$H(\beta) - H(\beta|\alpha) \overset{?}{\geq} 0$

$H(\beta) \overset{?}{\geq} H(\beta|\alpha)$

$= 0 \iff \alpha$ et β sont indep.

② $I(\alpha:\beta) \leq H(\beta)$ ③ $I(\alpha:\beta) \leq H(\alpha)$ ($= I(\beta:\alpha)$)

④ $I(\alpha:\beta) = H(\alpha) + H(\beta) - H(\alpha,\beta) = I(\beta:\alpha)$

$||$ def

$H(\beta) - H(\beta|\alpha) = H(\beta) - (H(\alpha,\beta) - H(\alpha))$

$= H(\alpha) + H(\beta) - H(\alpha,\beta) = H(\alpha) - H(\alpha|\beta)$

$= I(\beta:\alpha)$

Def (α, β, γ)

$p_{ijk} = \text{Prob}[\alpha = a_i \,\&\, \beta = b_j \,\&\, \gamma = c_k]$

$I(\alpha;\beta|\gamma) \overset{\text{def}}{=} H(\beta|\gamma) - H(\beta|\alpha,\gamma)$

$H(\beta|\alpha,\gamma) \equiv$

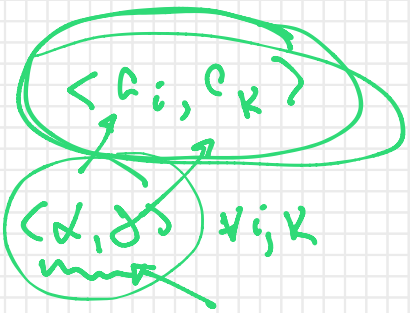
HW $I(\alpha;\beta|\gamma) \overset{(a)}{=} I(\beta:\alpha|\gamma)$

$\overset{(b)}{=} H(\alpha|\gamma) + H(\beta|\gamma) - H(\alpha,\beta|\gamma)$

$\overset{(c)}{=} H(\alpha,\gamma) + H(\beta,\gamma) - H(\alpha,\beta,\gamma) - H(\gamma)$

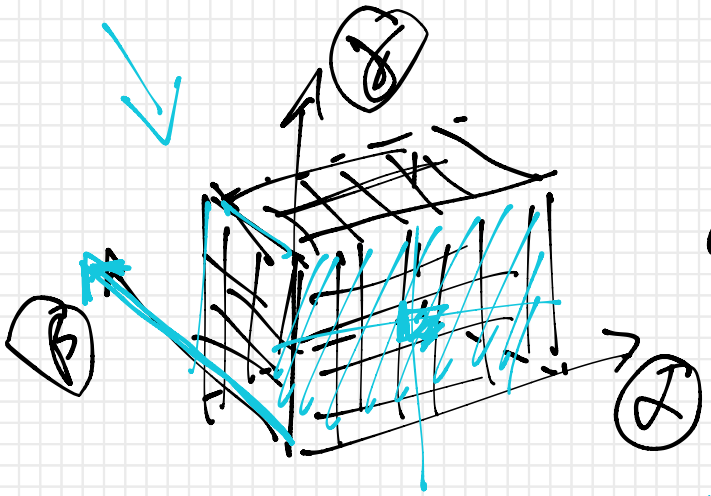
$I(\alpha:\beta|\gamma)$

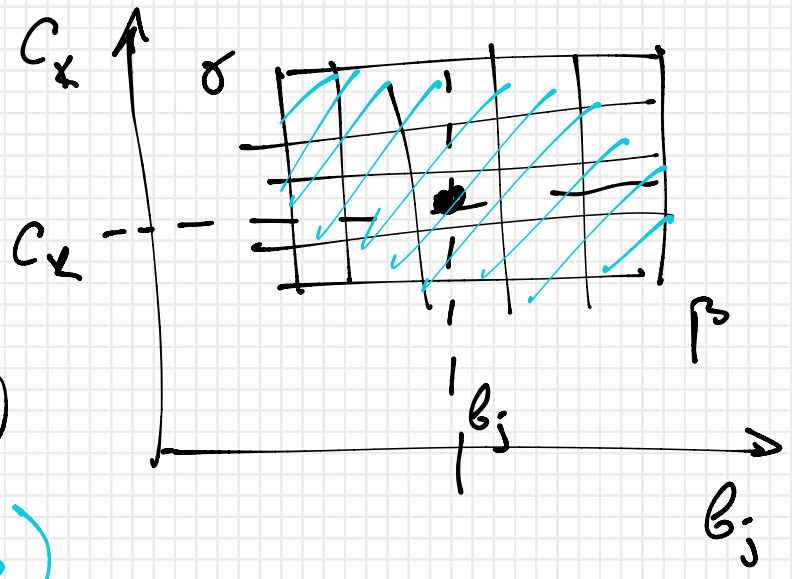
$I(\alpha;\beta|\gamma)$



$H(\beta|\langle\alpha,\gamma\rangle) \equiv$

$\delta \overset{\text{def}}{=} \langle \alpha, \gamma \rangle$





$\langle \alpha, \beta, \gamma \rangle$ $\quad H(\langle \alpha, \beta, \gamma \rangle)$

α
β
γ

$H(\alpha)$
$H(\beta)$
$H(\gamma)$

$H(\langle \alpha, \beta \rangle)$
$H(\langle \alpha, \gamma \rangle)$
$H(\langle \beta, \gamma \rangle)$

Ex 1

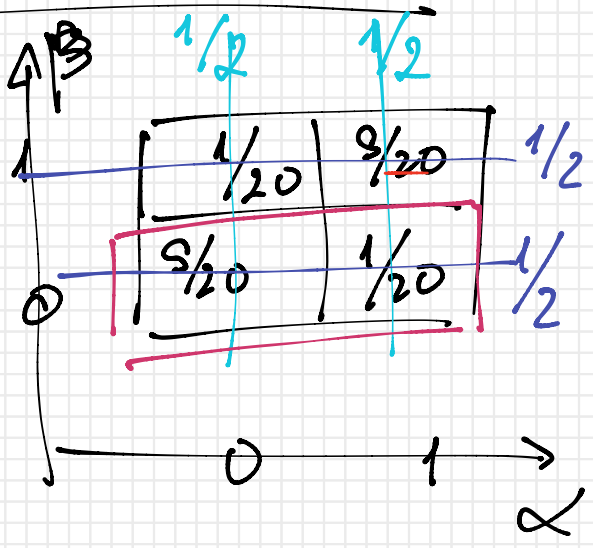
(α, β)

$\Pr[\alpha = 0, \beta = 0] = 9/20$

$\Pr[\alpha = 1, \beta = 0] = 1/20$

$\Pr[\alpha = 0, \beta = 1] = 1/20$

$\Pr[\alpha = 1, \beta = 1] = 9/20$



$\Pr[\alpha = 0] = 1/2$

$\Pr[\alpha = 1] = 1/2$

$\Pr[\beta = 0] = 1/2$

$\Pr[\beta = 1] = 1/2$

$\beta = 0 \Longrightarrow$

$\Pr[\alpha = 0 \mid \beta = 0] = 9/10$

$\Pr[\alpha = 1 \mid \beta = 0] = 1/10$

Ex 2

(α, β, γ)

α, β, γ

$1, 2, 3, 4$

$4 \times 4 \times 4 = 64$

$1 \le \alpha, \beta, \gamma \le 2$

$3 \le \alpha, \beta, \gamma \le 4$

$\Pr[\alpha=1, \beta=1, \gamma=1] = 1/16$

$\Pr[\alpha=2, \beta=1, \gamma=1] = 1/16$

$\Pr[\alpha=2, \beta=2, \gamma=1] = 1/16$

$\Pr[\alpha=1, \beta=2, \gamma=1] = 1/16$

$\Pr[\quad] = 1/16$

$\Pr[\quad] = \vdots$

$\Pr[\quad] = \vdots$

$\Pr[\quad] = \vdots$

$\Pr[\quad]$

$\vdots$

32 16

α: 4
β: 2
γ: 2

16

$\langle \alpha, \beta, \gamma \rangle$

$\Pr[\alpha=1] = 1/4$

$\Pr[\alpha=2] = 1/4$

$\Pr[\alpha=3] = 1/4$

$\Pr[\alpha=4] = 1/4$

(α, β)

$\Pr[\alpha=1, \beta=1] = 1/8$

1	2	1/8
2	1	
2	2	⋮
3	3	⋮
4	3	
3	4	
4	4	

1/8

4	0	0	1/8	1/8
3	0	0	1/8	1/8
2	1/8	1/8	0	0
1	1/8	1/8	0	0
	1	2	3	4

Ex 3 $\langle \alpha, \beta, \gamma \rangle$ $0, 1$ $2 \times 2 \times 2$

$Pr[\alpha = 0, \beta = 0, \gamma = 0] = 1/4$

$Pr[\alpha = 1, \beta = 0, \gamma = 1] = 1/4$

$Pr[\alpha = 0, \beta = 1, \gamma = 1] = 1/4$

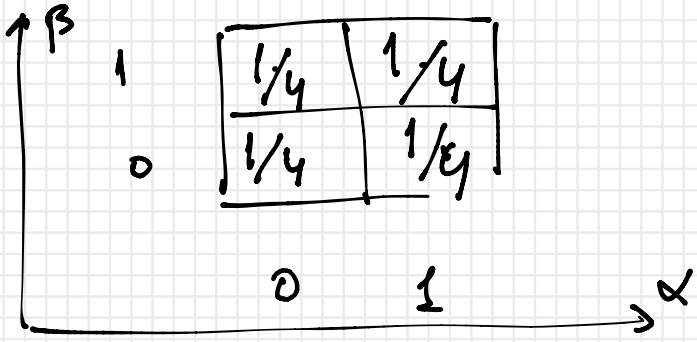
$Pr[\alpha = 1, \beta = 1, \gamma = 0] = 1/4$

$\langle \alpha, \beta \rangle$

$\downarrow$

$Pr[\alpha = 0] = 1/2$

$Pr[\alpha = 1] = 1/2$

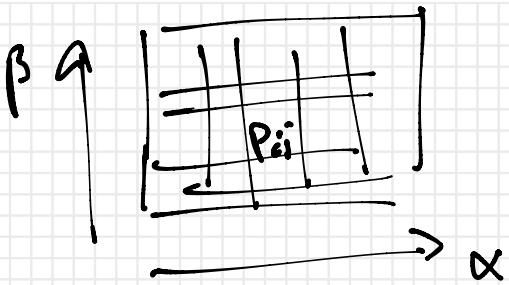


$\langle \alpha, \beta \rangle$

$H(\alpha,\beta)$
$H(\alpha)$
$H(\beta)$

$H(\alpha|\beta)$
$H(\beta|\alpha)$

$I(\alpha:\beta) = I(\beta:\alpha)$



$H(\alpha)$
$H(\beta)$
$H(\alpha,\beta)$

$\rightarrow$

$H(\alpha|\beta) = H(\alpha,\beta) - H(\beta)$

$H(\beta|\alpha) = H(\alpha,\beta) - H(\alpha)$

$I(\alpha:\beta) = H(\alpha) + H(\beta) - H(\alpha,\beta)$

$H(\alpha|\beta)$
$H(\beta|\alpha)$
$I(\alpha:\beta)$

$\rightarrow$

$H(\alpha) = I(\alpha:\beta) + H(\alpha|\beta)$

$H(\beta) = I(\alpha:\beta) + H(\beta|\alpha)$

$H(\alpha,\beta) = I(\alpha:\beta) + H(\alpha|\beta) + H(\beta|\alpha)$

$H(\alpha)$ α $H(\alpha|\beta) \geq 0$ $I(\alpha:\beta)$ $H(\beta|\alpha)$ β $H(\beta)$

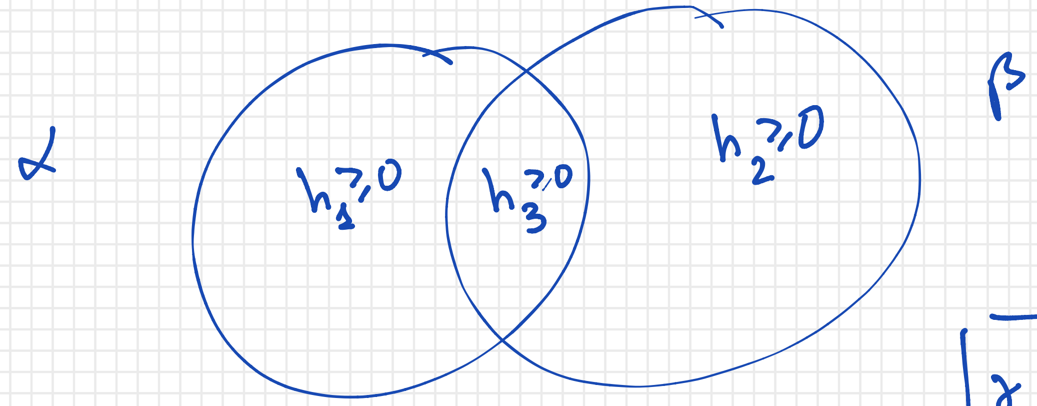
$I(\alpha:\beta) + H(\beta|\alpha)$
$+$
$I(\alpha:\beta) + H(\alpha|\beta)$
$=$
$\leq H(\alpha) + H(\beta)$

$H(\alpha,\beta)$

$I(\alpha:\beta) + H(\alpha|\beta) + H(\beta|\alpha) =$

$H(\alpha,\beta) =$

$H(\alpha|\beta)$
$+$
$H(\beta|\alpha)$
$+$
$I(\alpha:\beta)$



$$\gamma_1 : H(\gamma_1) = h_1 \geq 0$$
$$\gamma_2 : H(\gamma_2) = h_2 \geq 0$$
$$\gamma_3 : H(\gamma_3) = h_3 \geq 0$$

? $\langle \alpha, \beta \rangle$: $\begin{cases} H(\alpha \mid \beta) = h_1 \\ H(\beta \mid \alpha) = h_2 \\ I(\alpha : \beta) = h_3 \end{cases}$

$\alpha \overset{def}{=} \langle \gamma_1, \gamma_3 \rangle$ $\quad H(\alpha) = H(\gamma_1, \gamma_3) = H(\gamma_1) + H(\gamma_3) = h_1 + h_3$ | $\gamma_1, \gamma_2, \gamma_3$ sont indep.

$\beta \overset{def}{=} \langle \gamma_2, \gamma_3 \rangle$

$$H(\beta) = H(\gamma_2) + H(\gamma_3) = h_2 + h_3$$

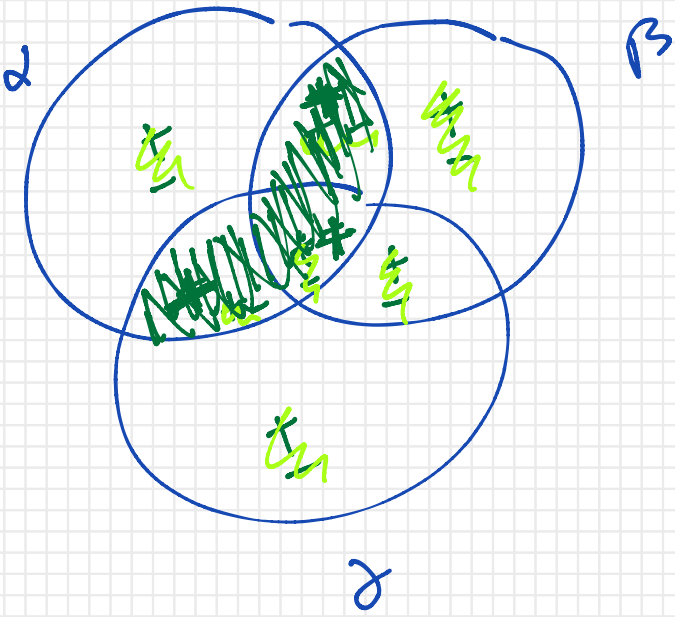
$$H(\alpha, \beta) = H(\langle \gamma_1, \gamma_2, \gamma_3, \cancel{\gamma_3} \rangle) = H(\gamma_1) + H(\gamma_2) + H(\gamma_3) = h_1 + h_2 + h_3$$

$\langle \alpha, \beta, \gamma \rangle$

$H(\alpha)$
$H(\beta)$
$H(\gamma)$
$H(\alpha,\beta)$
$H(\alpha,\gamma)$
$H(\beta,\gamma)$
$H(\alpha,\beta,\gamma)$

$H(\alpha|\beta)$ ...
$H(\alpha|\beta\gamma)$ ...
$H(\alpha\beta|\gamma)$ ...

$I(\alpha:\beta)$
$I(\alpha:\gamma)$
$I(\beta:\gamma)$
$I(\alpha,\beta:\gamma)$ ...
$I(\alpha:\beta|\gamma)$ ...

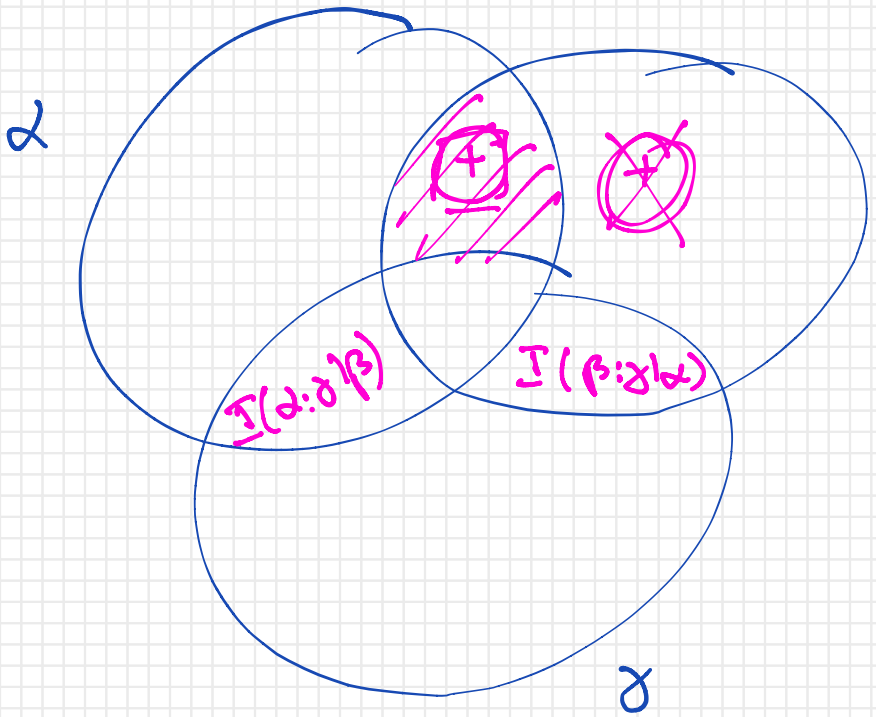


$H(\alpha|\beta) = H(\alpha,\beta) - H(\beta)$

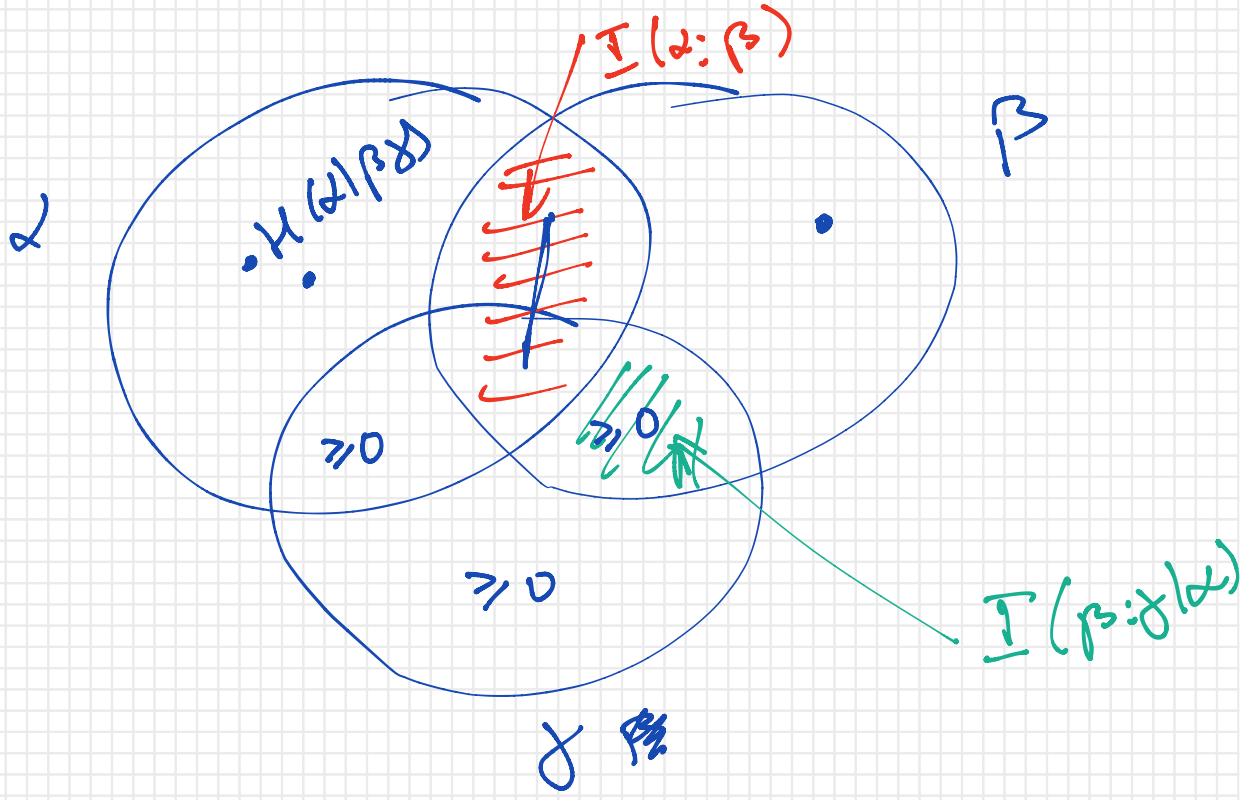
$H(\alpha|\beta\gamma) = H(\alpha,\beta\gamma) - H(\beta,\gamma)$

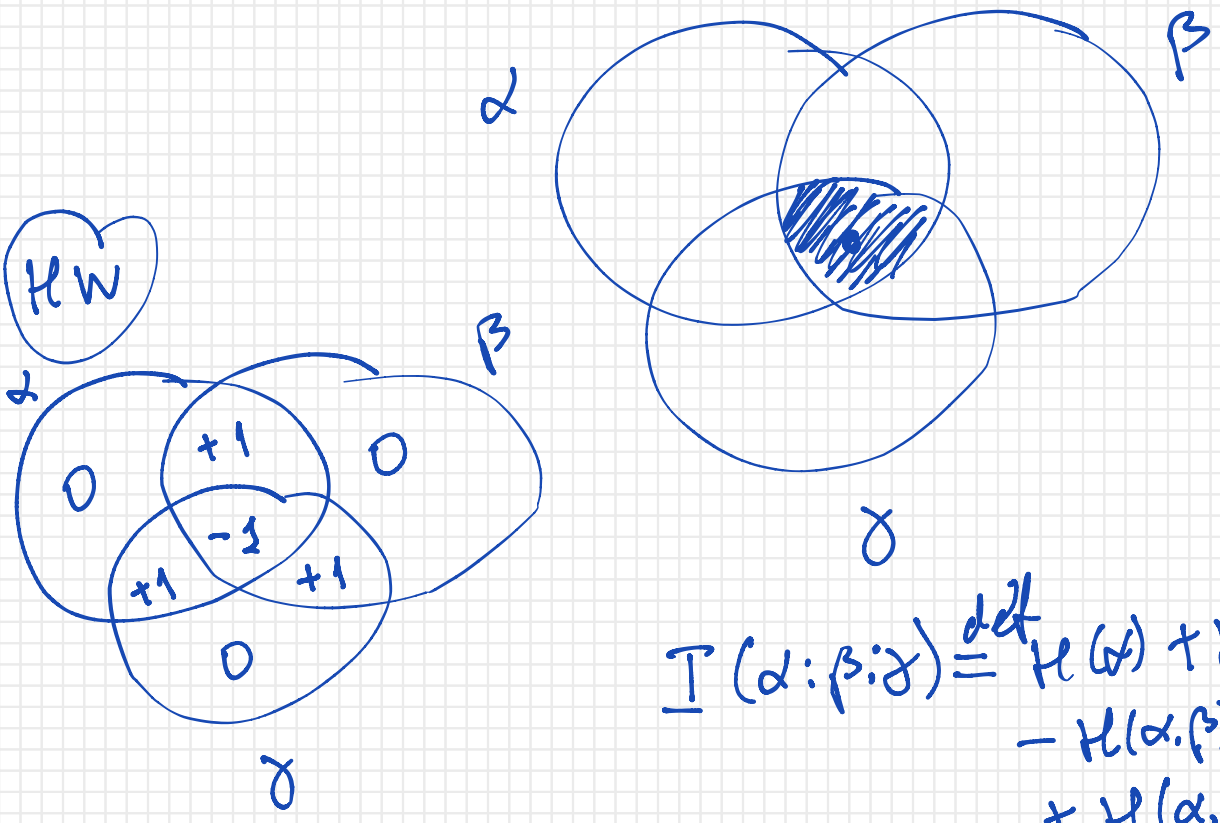
$I(\alpha:\beta) =$

$I(\alpha:\beta\gamma) = H(\alpha) + H(\beta\gamma) - H(\alpha,\beta,\gamma)$



$I(\alpha:\beta|\gamma) \stackrel{\text{def}}{=} H(\beta|\gamma) - H(\beta|\alpha\gamma)$





$$\underline{I}(\alpha:\beta:\gamma) \stackrel{\text{def}}{=} H(\alpha)+H(\beta)+H(\gamma) - H(\alpha,\beta)-H(\alpha,\gamma)-H(\beta,\gamma) + H(\alpha,\beta,\gamma)$$