Transmission de données one-shot

$$M \in \{0,1\}^R \longrightarrow \boxed{\text{enc}} \xrightarrow{X \in \mathcal{X}} \boxed{W} \xrightarrow{Y \in \mathcal{Y}} \boxed{\text{déc}} \longrightarrow \hat{M} \in \{0,1\}^R$$

$$\Pr\left[\hat{M} \neq M\right] \leq 2^{R - I_{\min}(X;Y)_{p \times W}}$$

$p \times W$ ⟶ distribution sur $\mathcal{X}$ selon laquelle on choisit le code.

Pr :

- Le code $\{c(0^R), \ldots, c(1^R)\}$ est choisi au hasard selon p_X $\left(c(m) \in \mathcal{X}\right)$.

- Le décodeur :

$$d(\hat{m}|y) = \frac{2^{\frac{1}{2}S(c(\hat{m});y)}}{\sum_{m'} 2^{\frac{1}{2}S(c(m');y)}}.$$

- On suppose que $M = 0^R$.

$$\Pr\left[\hat{M} \neq 0^R \,\middle|\, Y = y, \mathcal{C} = \{c(0^R), \ldots, c(1^R)\}\right]$$

$$= \frac{\sum_{\hat{m} \neq 0^R} 2^{\frac{1}{2}S(c(\hat{m});y)}}{\sum_{m'} 2^{\frac{1}{2}S(c(m');y)}} \leq \frac{\sum_{\hat{m} \neq 0^R} 2^{\frac{1}{2}S(c(\hat{m});y)}}{2^{\frac{1}{2}S(c(0^R);y)}}$$

$$= 2^{-\frac{1}{2}S(c(0^R);y)} \cdot \sum_{\hat{m} \neq 0^R} 2^{\frac{1}{2}S(c(\hat{m});y)}.$$

⟶ Prenons l'espérance sur $c(\hat{m})$ où $\hat{m} \neq 0^R$:

$$\mathbb{E}_{c(\hat{m}) \sim p_X}\left[2^{\frac{1}{2}S(c(\hat{m});y)}\right]$$

$$S(c(\hat{m});y) = S(c(\hat{m})) + S(y) - S(c(\hat{m}),y)$$

$$= S(c(\hat{m})) - S(c(\hat{m})|y)$$

$$\mathbb{E}_{c(\hat{m})\sim p_x}\left[2^{\frac{1}{2}\left(S(c(\hat{m})) - S(c(\hat{m})|y)\right)}\right]$$

Divergence de Rényi :

$$2^{(\alpha-1)D_\alpha(p\|q)} = \mathbb{E}_{X\sim p}\left[2^{(\alpha-1)\left(S(X)_q - S(X)_p\right)}\right]$$

$$= \mathbb{E}_{c(\hat{m})\sim p_x}\left[2^{-\frac{1}{2}\left(S(c(\hat{m})|y) - S(c(\hat{m}))\right)}\right]$$ → Divergence de Rényi avec $\alpha = \frac{1}{2}$.

$$= 2^{+\frac{1}{2}D_{\frac{1}{2}}(p_x \| p_{X|Y=y})} = 2^{-\frac{1}{2}D_{\frac{1}{2}}(p_{X|Y=y}\|p_x)}$$

Regardons maintenant le terme $2^{-\frac{1}{2}S(c(0^R);y)}$:

$$\mathbb{E}_{c(0^R)\sim p_{X|Y=y}}\left[2^{-\frac{1}{2}S(c(0^R);y)}\right] = 2^{-\frac{1}{2}D_{\frac{1}{2}}(p_{X|Y=y}\|p_x)}$$

$$\Rightarrow \mathbb{E}_{e}\left[2^{-\frac{1}{2}S(c(0^R);y)} \cdot \sum_{\hat{m}\neq 0^R} 2^{\frac{1}{2}S(c(\hat{m});y)}\right]$$

$$= 2^{-\frac{1}{2}D_{\frac{1}{2}}(p_{X|Y=y}\|p_x)} \cdot (2^R - 1) \cdot 2^{-\frac{1}{2}D_{\frac{1}{2}}(p_{X|Y=y}\|p_x)}$$

$$\leq 2^{R - D_{\frac{1}{2}}(p_{X|Y=y}\|p_x)}$$

→ Prenons l'espérance sur Y :

$$\mathbb{E}_Y\left[2^{R - D_{\frac{1}{2}}(p_{X|Y=y} \| p_X)}\right]$$

$$\boxed{\begin{array}{l}\text{Information mutuelle de Rényi :} \\ 2^{\frac{\alpha-1}{\alpha} I_\alpha(X;Y)} = \mathbb{E}_Y\left[2^{\frac{\alpha-1}{\alpha} D_\alpha(p_{X|Y=y} \| p_X)}\right]\end{array}}$$

On est dans cette situation pour $\alpha = \frac{1}{2}$:

$$= 2^R \cdot 2^{-I_{\frac{1}{2}}(X;Y)} = 2^{R - I_{\frac{1}{2}}(X;Y)} = 2^{R - I_{min}(X;Y)}$$

$$\boxed{I_{min}(X;Y) := I_{\frac{1}{2}}(X;Y)}$$

$\square$

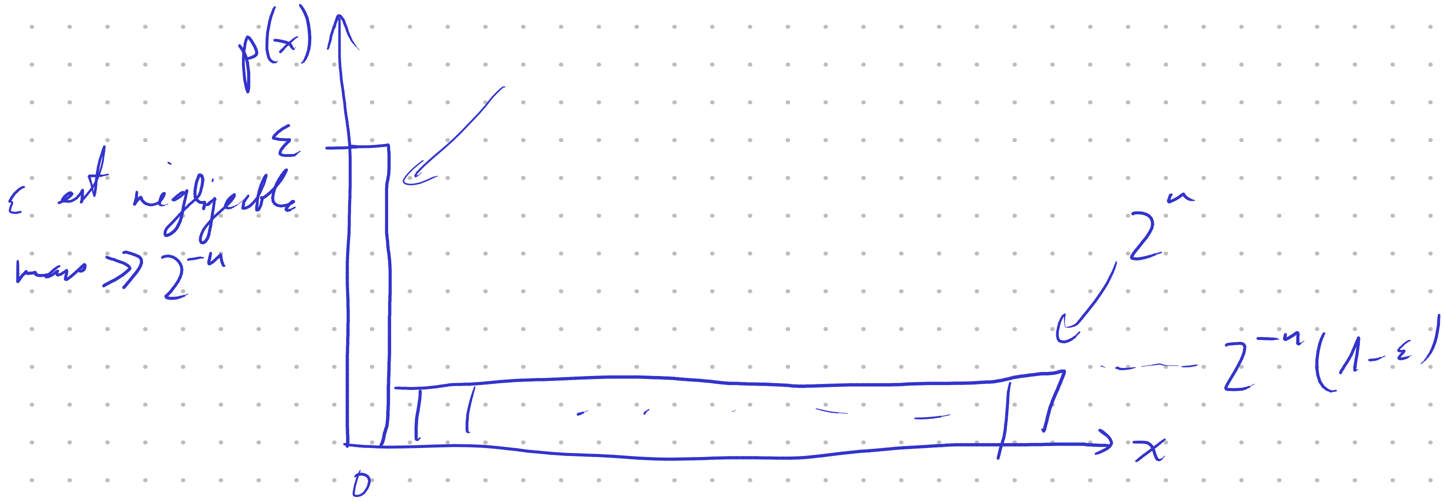
Compression : $\Pr[\text{erreur}] \leq 2^{-(R - H_{max}(X|Y))}$

Extraction d'aléa : $\|(\text{cas réel}) - (\text{cas idéal})\|_1 \leq 2^{\frac{1}{2}(k - H_{min}(X|Y))}$

Transmission de donnée : $\Pr[\text{erreur}] \leq 2^{R - I_{min}(X;Y)}$.

Lissage ("Smoothing")

→ Peut-on récupérer les théorèmes i.i.d via les thms one-shot ?



→ Extraction d'aléa :

$$2^{-H_2(X)} = \mathbb{E}\left[2^{-S(X)}\right]$$
$$= \sum_x \left[p(x)^2\right]$$
$$= \varepsilon^2 + 2^n(1-\varepsilon)^2\, 2^{-2n}$$
$$= \varepsilon^2 + (1-\varepsilon)^2 \cdot 2^{-n} \geq \varepsilon^2$$

$\Rightarrow H_2(X) \leq 2\log\frac{1}{\varepsilon} \ll n$.

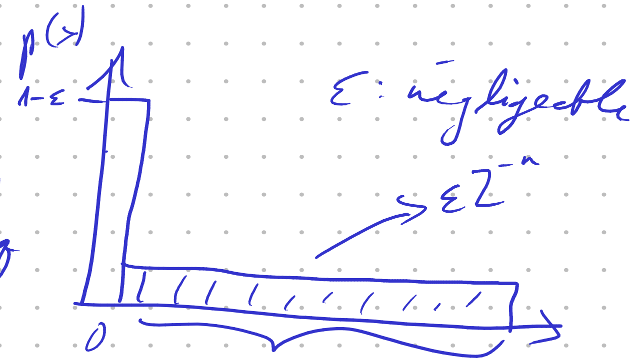
→ Pourtant, on doit pouvoir extraire $\approx n$ bits, car l'évènement que $x=0$ a une probabilité négligeable.

→ On définit des versions "lissées" des mesures one-shot :

$\varepsilon \in (0,2)$:

$$\tilde{H}^{\varepsilon}_{min}(X|Y)_p := \max_{q : \|q-p\|_1 \leq \varepsilon} H_{min}(X|Y)_q$$

$$\tilde{H}^{\varepsilon}_{max}(X|Y)_p := \min_{q : \|q-p\|_1 \leq \varepsilon} H_{max}(X|Y)_q$$



$$\tilde{I}^{\varepsilon}_{\min}(X;Y)_p = \max_{q : \|q-p\|_1 \leq \varepsilon} I_{\min}(X;Y)_q .$$

Extraction alea: $\|p_{ZYH} - u_Z \times q_Y \times u_H\|_1 \leq \|p_{ZYH} - q_{ZYH}\|_1$

$+ \|q_{ZYH} - u_Z \times q_Y \times u_H\|_1$

On choisit q t.q. $\tilde{H}^{\varepsilon}_{\min}(X|Y)_p = H_{\min}(X|Y)_q$.

et $\|p-q\|_1 \leq \varepsilon$

$\leq \varepsilon + 2^{\frac{1}{2}(k - \tilde{H}^{\varepsilon}_{\min}(X|Y)_p)}$.

Compression : Soit q_{XY} t.q. $\|q-p\|_1 \leq \varepsilon$ et $\tilde{H}^{\varepsilon}_{\max}(X|Y)_p = H_{\max}(X|Y)_q$

$r_{XY\tilde{X}\tilde{Y}}$ t.q. $\Pr[(X,Y) \neq (\tilde{X},\tilde{Y})] = \frac{\varepsilon}{2}$

et $r_{XY} = p_{XY}$ $r_{\tilde{X}\tilde{Y}} = q_{\tilde{X}\tilde{Y}}$.

$$\Pr_{(X,Y)\sim p}[\text{erreur}] \leq \Pr_{(X,Y)\sim r}\left[\text{erreur}_{(X,Y)} \wedge (X,Y) = (\tilde{X},\tilde{Y})\right]$$

$$+ \Pr_{(X,Y)\sim r}\left[\text{erreur} \wedge (X,Y) \neq (\tilde{X},\tilde{Y})\right]$$

$$\leq \Pr_{(X,Y)\sim q}[\text{erreur}] + \frac{\varepsilon}{2}$$

$$\leq 2^{\tilde{H}^{\varepsilon}_{\max}(X|Y) - R} + \frac{\varepsilon}{2} .$$

Transmission de données : p_{XY}, q_{XY} et $r_{XY\tilde{X}\tilde{Y}}$ comme précédemment

$$\Pr_{(X,Y)\sim p}[\text{erreur}] \leq \Pr_{(X,Y)\sim r}[\text{erreur} \wedge (X,Y)=(\tilde{X},\tilde{Y})]$$
$$+ \Pr_{(X,Y)\sim r}[\text{erreur} \wedge (X,Y)\neq(\tilde{X},\tilde{Y})]$$

$$\leq \ldots$$
$$\leq \Pr_{(X,Y)\sim q}[\text{erreur}] + \frac{\varepsilon}{2}$$
$$\leq 2^{R-\tilde{I}^{c}_{min}(X;Y)} + \frac{\varepsilon}{2}.$$

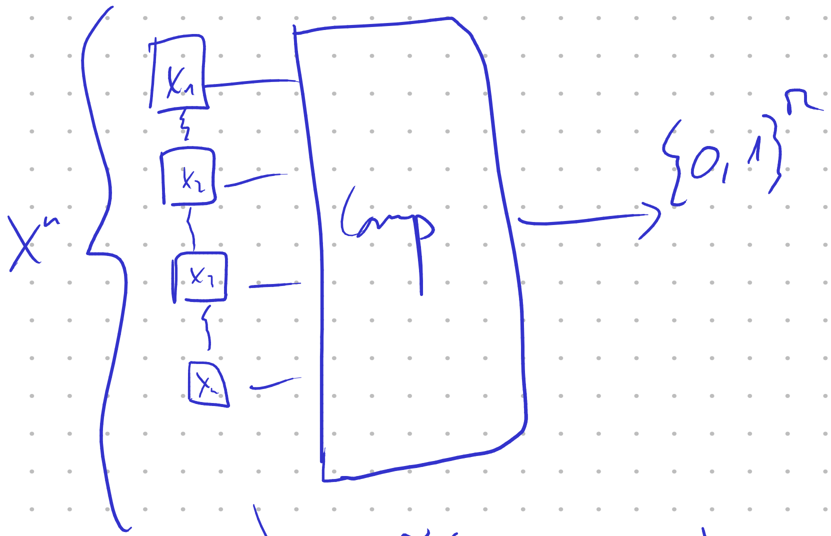
Pour récupérer les théorèmes iid à partir des méthodes one-shot, on doit montrer que :

$(X^n, Y^n) \sim$ iid :

dépend de $|\mathcal{X}|, \varepsilon$

$$\tilde{H}^{\varepsilon}_{min}(X^n|Y^n) \approx nH(X|Y) \qquad \geq nH(X|Y) - O(\sqrt{n})$$
$$\tilde{H}^{\varepsilon}_{max}(X^n|Y^n) \approx nH(X|Y) \qquad \leq nH(X|Y) + O(\sqrt{n})$$
$$\tilde{I}^{\varepsilon}_{min}(X^n;Y^n) \approx nI(X;Y) \qquad \geq nI(X;Y) - O(\sqrt{n}).$$

$$\geq nH(X|Y) - \sqrt{n}\left(\frac{\ln 2}{2}\,\mathbb{E}[S(X)^2] + \log\frac{2}{\varepsilon}\right)$$



$\tilde{H}^{\varepsilon}_{min/max}(X^n)$

$H^{\varepsilon}_{min}(X^n) \geq$ (processus d'échantillonage).