24.2/29

**Ayoub Echchahed**
**(111 274 558)**

**Théorie de l'information**
**GEL-7062**

**Devoir 4**
**Résolution de Problèmes**

**Travail présenté à**
**Mr. Jean-Yves Chouinard**

**Faculté des sciences et de génie**
**Université Laval**
**Hiver 2022**

- **Problème 1 :** 1/3

> **Problème 8.2 :** Calculez et donnez l'expression détaillée de la région de capacité d'un canal à accès multiple avec trois sources, $X_1 \in \{0,1\}$, $X_2 \in \{0,1\}$ et $X_3 \in \{0,1\}$ et
>
> $$Y = X_1 + X_2 + X_3 \text{ mod } 2.$$

$$\boxed{R(\mathcal{S}) \leq I(X(\mathcal{S}); Y | X(\mathcal{S}^c))}$$

- If Y = 0 or Y = 3, sources $X_{1\text{-}3}$ carry no uncertainty
- H (Y) ≤ 2

| $X_1$ | $X_2$ | $X_3$ | Y |
|---|---|---|---|
| 0 | 0 | 0 | 0 |
| 0 | 0 | 1 | 1 |
| 0 | 1 | 0 | 1 |
| 1 | 0 | 0 | 1 |
| 1 | 1 | 0 | 2 |
| 0 | 1 | 1 | 2 |
| 1 | 0 | 1 | 2 |
| 1 | 1 | 1 | 3 |

$R_1 \leq I(X1; Y | X2, X3)$
$\leq H(Y | X2, X3) - H(Y | X2, X3, X1)$
$\leq H(X1)$
$\leq 1$

$R_2 \leq I(X2; Y | X1, X3)$
$\leq H(X2)$
$\leq 1$

$R_3 \leq I(X3; Y | X1, X2)$
$\leq H(X3)$
$\leq 1$

$R_1 + R_2 \leq I(X1, X2; Y|X3)$
$\leq H(Y|X3) - H(Y|X3, X2, X1)$
$\leq H(X1) + H(X2) - I(X1, X2) - H(Y|X3, X2, X1)$
$\leq 1 + 1 - 0 - 0$
$\leq 2$

$R_1 + R_3 \leq I(X1, X3; Y|X2)$
$\leq H(X1) + H(X3) - I(X1, X3) - H(Y|X3, X2, X1)$
$\leq 1 + 1 - 0 - 0$
$\leq 2$

modulo 2 ...

$R_2 + R_3 \leq I(X2, X3; Y|X1)$
$\leq H(X2) + H(X3) - I(X2, X3) - H(Y|X3, X2, X1)$
$\leq 1 + 1 - 0 - 0$
$\leq 2$

$R_1 + R_2 + R_3 \leq I(X1, X2, X3; Y)$
$\leq H(Y)$
$\leq 2$

- **Problème 2 :** 5/5

**Problème 9.1 :** Deux sources corrélées $X$ et $Y$ ont la distribution conjointe suivante :

| $p(x_k, y_j)$ | $y_1$ | $y_2$ | $y_3$ | $y_4$ |
|---|---|---|---|---|
| $x_1$ | $\alpha$ | $\beta$ | $\beta$ | $\beta$ |
| $x_2$ | $\gamma$ | 0 | 0 | 0 |
| $x_3$ | $\gamma$ | 0 | 0 | 0 |
| $x_4$ | $\gamma$ | 0 | 0 | 0 |

avec $\alpha + 3\beta + 3\gamma = 1$, $1 \leq k \leq 4$ et $1 \leq j \leq 4$.

a) Calculez les entropies : $H(X)$, $H(Y)$ et $H(XY)$.

b) Déterminez les entropies conditionnelles suivantes : $H(X|Y)$ et $H(Y|X)$.

c) Déterminez (donnez le détail de vos calculs) la région de débit de Slepian-Wolf pour la compression de ces deux sources.

d) Pour $\alpha = 0.25$, $\beta = 0.15$ et $\gamma = 0.10$, tracez la région de débit et indiquant clairement les valeurs numériques des différents points de la région de débit.

e) Si les deux sources n'étaient pas corrélées, mais avec les mêmes entropies $H(X)$ et $H(Y)$, indiquez quelle serait la région de débit sur ce même graphique.

**a)** 1/1

H (X) = Σ p ($x_k$) log [1 / p ($x_k$)]
= (3β + α) * log [1 / (3β + α)] + 3 [(γ) * log [1 / (γ)]

H (Y) = Σ p ($y_j$) log [1 / p ($y_j$)]
= (3γ + α) * log [1 / (3γ + α)] + 3 [(β) * log [1 / (β)]

H (XY) = - Σ p ($x_k$, $y_j$) * log p ($x_k$, $y_j$)
= - [α * $\log_2$ α] + 3 [ γ * $\log_2$ γ ] + 3 [β * $\log_2$ β ]

**b)** 1/1

H (X|Y) = Σ p ($x_k$, $y_j$) log [1 / p ($x_k$ | $y_j$)]
= Σ p ($x_k$, $y_j$) log [1 / (p ($x_k$, $y_j$) / p ($y_j$)]
= 3 [γ log [1 / (γ / (3γ + α))] + α log [1 / (α / (3γ + α))] il manque un crochet ...

H (Y|X) = Σ p ($x_k$, $y_j$) log [1 / p ($y_j$ | $x_k$ )]
= Σ p ($x_k$, $y_j$) log [1 / (p ($x_k$, $y_j$) / p ($x_k$)]
= 3 [β log [1 / (β / (3β + α))] + α log [1 / (α / (3β + α))]

**c)** Hence the Slepian Wolf rate region is:

1/1

$R_1 \geq H(X|Y)$

$\geq 3 [\gamma \log [1 / (\gamma / (3\gamma + \alpha))] + \alpha \log [1 / (\alpha / (3\gamma + \alpha))]]$

$R_2 \geq H(Y|X)$

$\geq 3 [\beta \log [1 / (\beta / (3\beta + \alpha))] + \alpha \log [1 / (\alpha / (3\beta + \alpha))]]$

$R_1 + R_2 \geq H(XY)$

$\geq - [\alpha * \log_2 \alpha] + 3 [\gamma * \log_2 \gamma] + 3 [\beta * \log_2 \beta]$

**d)**

$\beta = 0.15$
$\alpha = 0.25$
$\gamma = 0.10$

$R_1 \geq H(X|Y)$

$\geq 3 [\gamma \log [1 / (\gamma / (3\gamma + \alpha))] + \alpha \log [1 / (\alpha / (3\gamma + \alpha))]]$
$\geq 3 [0.10 \log_2 [1 / (0.10 / (3 (0.10) + 0.25))] + 0.25 \log_2 [1 / (0.25 / (3 (0.10) + 0.25))]]$
$\geq 3 [0.10 \log_2 (5.5)] + 0.25 \log_2 (2.2)$
$\geq 0.7378 + 0.2844$
$\geq 1.02$

$R_2 \geq H(Y|X)$

$\geq 3 [\beta \log [1 / (\beta / (3\beta + \alpha))] + \alpha \log [1 / (\alpha / (3\beta + \alpha))]]$
$\geq 3 [0.15 \log_2 [1 / (0.15 / (3 (0.15) + 0.25))] + 0.25 \log_2 [1 / (0.25 / (3 (0.15) + 0.25))]$
$\geq 3 [0.15 \log_2 (14 / 3)] + 0.25 \log_2 (2.8)$
$\geq 1.3714$

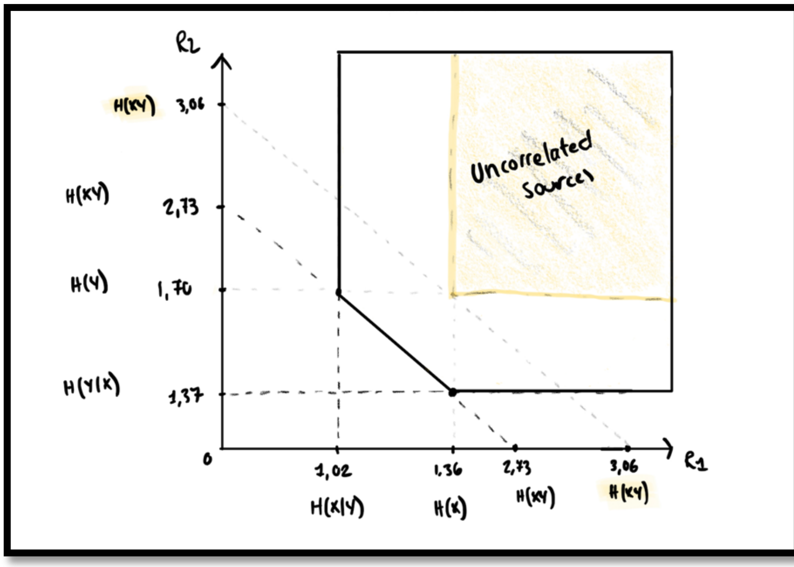
$R_1 + R_2 \geq H(XY)$

$\geq - [\alpha * \log_2 \alpha] + 3 [\gamma * \log_2 \gamma] + 3 [\beta * \log_2 \beta]$
$\geq - [[0.25 * \log_2 0.25] + 3 [0.10 * \log_2 0.10] + 3 [0.15 * \log_2 0.15]]$
$\geq 2.7282$

$H(X) = [3(0.15) + 0.25] * \log[1 / (3(0.15) + 0.25)]$
$+ 3[(0.10) * \log[1 / (0.10)]$
$= 1.36$

$H(Y) = [3(0.10) + 0.25] * \log[1 / (3(0.10) + 0.25)]$
$+ 3[(0.15) * \log[1 / (0.15)]$
$= 1.706$

1/1




**e)** 1/1

$\beta = 0.15$
$\alpha = 0.25$
$\gamma = 0.10$

$R_1 \geq H(X|Y)$
$\geq H(X)$
$\geq (3\beta + \alpha) * \log[1 / (3\beta + \alpha)] + 3[(\gamma) * \log[1 / (\gamma)]$
$\geq (3(0.15) + 0.25) * \log[1 / (3(0.15) + 0.25)] + 3[(0.10) * \log[1 / (0.10)]$
$\geq 1.3568$

$R_2 \geq H(Y|X)$
$\geq H(Y)$
$\geq (3\gamma + \alpha) * \log[1 / (3\gamma + \alpha)] + 3[(\beta) * \log[1 / (\beta)]$
$\geq (3(0.10) + 0.25) * \log2[1 / (3(0.10) + 0.25)] + 3[(0.15) * \log2[1 / (0.15)]$
$\geq 1.7060$

$R_1 + R_2 \geq H(XY)$
$\geq H(X) + H(Y)$
$\geq 1.3568 + 1.7060$
$\geq 3.0628$

- **Problème 3 :** 5/5

**Problème 9.2 :** Deux sources indépendantes $X$ et $Y$ génèrent des symboles binaires selon des distributions de Bernoulli : $X \sim Bern(0.6)$ et $Y \sim Bern(0.8)$. On forme deux nouvelles variables aléatoires $S$ et $D$ :

$$\begin{aligned} S &= X + Y \\ D &= X - Y \end{aligned}$$

où $S \in \{0, 1, 2\}$ et $D \in \{-1, 0, 1\}$.

a) Calculez les entropies : $H(X)$, $H(Y)$ et $H(XY)$.

b) Calculez les entropies : $H(S)$, $H(D)$ et $H(SD)$.

c) Si on utilise un décodage conjoint, quelle est la région de débit (Slepian-Wolf) de $X$ et $Y$ ?

d) Toujours en utilisant le décodage conjoint, quelle est la région de débit (Slepian-Wolf) de $S$ et $D$ ?

e) Expliquez et comparez les résultats obtenus en c) et d).

- Value 1 with probability p
- Value 0 with probability q = 1 - p

- X ~ Bern (p = 0.6)
- Y ~ Bern (p = 0.8)

- Joint Distribution:

| Variable X | Variable Y | Variable S | Variable D | Probability |
|---|---|---|---|---|
| 0 | 0 | 0 | 0 | (1 - 0.6) (1 - 0.8) = **0.08** |
| 1 | 0 | 1 | 1 | (1 - 0.6) (0.8) = **0.32** |
| 0 | 1 | 1 | -1 | (0.6) (1 - 0.8) = **0.12** |
| 1 | 1 | 2 | 0 | (0.6) (0.8) = **0.48** |

**a)** 1/1

$H(X) = \Sigma\, p(x_k) \log [1 / p(x_k)]$
$= (0.08 + 0.12) \log [1 / (0.08 + 0.12)] + (0.32 + 0.48) \log [1 / (0.32 + 0.48)]$
$= 0.7219$

$H(Y) = \Sigma\, p(y_k) \log [1 / p(y_k)]$
$= (0.08 + 0.32) \log [1 / (0.08 + 0.32)] + (0.12 + 0.48) \log [1 / (0.12 + 0.48)]$
$= 0.97095$

$H(XY) = - \Sigma\, p(x_k, y_j) * \log p(x_k, y_j)$
$= - [(0.08 \log (0.08)) + (0.32 \log (0.32)) + (0.12 \log (0.12)) + (0.48 \log (0.48))]$
$= H(X) + H(Y)$
$= 1.6928$

**b)** 1/1

$H(S) = \Sigma\ p(s_k) \log [1 / p(s_k)]$
$= 0.08 \log [1 / 0.08] + (0.32 + 0.12) \log [1 / (0.32 + 0.12)] + 0.48 \log [1 / 0.48]$
$=$ 1.3209 Sh

$H(D) = \Sigma\ p(d_k) \log [1 / p(d_k)]$
$= 0.12 \log [1 / 0.12] + (0.48 + 0.08) \log [1 / (0.48 + 0.08)] + 0.32 \log [1 / 0.32]$
$=$ 1.3615 Sh

$H(SD) = H(X_{=1}, Y_{=1})$
$= - [(0.6 \log 0.6) + (0.4 \log 0.4) + (0.8 \log 0.8) + (0.2 \log 0.2)]$
$=$ 1.693 Sh

**c)**

1/1

$R1 \geq H(X|Y)$
$\geq H(X)$
$\geq 0.7219$

$R2 \geq H(Y|X)$
$\geq H(Y)$
$\geq 0.97095$

$R1 + R2 \geq H(X, Y)$
$\geq H(X) + H(Y)$
$\geq 1.6928$

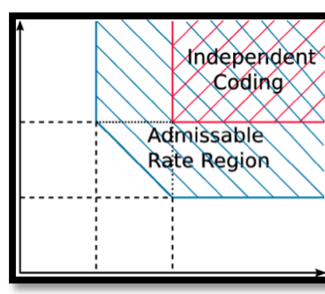
**d)**

$R1 \geq H(S \mid D)$ 1/1
$\geq H(SD) - H(D)$
$\geq 1.693 - 1.3615$
$\geq 0.3315$

$R2 \geq H(D \mid S)$
$\geq H(DS) - H(S)$
$\geq 1.693 - 1.3209$
$\geq 0.3721$

$R1 + R2 \geq H(SD)$
$\geq H(X{=}1) + H(Y{=}1)$
$\geq$ 1.693 Sh

1/1




**e)** For the **independent** variables (X, Y), the Slepian Wolf region is a **4-sided region** (rectangle) as both the entropy & the conditional entropy give the same result for a chosen variable. However, the Slepian Wolf region for the variables (S, D) is a **5-sided region,** and is larger in area than the region for the (X, Y) as the **mutual information between (S, D) is positive.**

Also, R1 + R2 for both c) and d) are the same, which I think can be explained by the fact that the **knowledge of one pair of variables is enough to deduce the value of the other pair**.

- **Problème 4 :** 4/4

**Problème 9.3 :** Soit $X$ une source d'information binaire suivant une distribution de Bernoulli : $X \sim Bern(\alpha)$. Soit $Z$ une seconde source d'information binaire indépendante de $X$ et de distribution de Bernoulli : $Z \sim Bern(\beta)$. Soit $Y$ une source binaire pour laquelle $Y = X \oplus Z$. On transmet la source $X$ avec un débit $R_X$ et la source $Y$ avec un débit $R_Y$.

a) Écrivez les expressions des entropies : $H(X)$, $H(Z)$ et $H(Y)$ en fonction de $\alpha$ et de $\beta$.

b) Écrivez les expressions des entropies conditionnelles et conjointes en fonction de $\alpha$ et de $\beta$ : $H(X|Y)$, $H(Y|X)$ et $H(XY)$.

c) Donnez la région de débits (Slepian-Wolf) de $X$ et $Y$ en fonction de $\alpha$ et de $\beta$. Décrivez cette région de débits permettant de récupérer $X$ et $Y$.

d) Dessinez la région de débits pour $\alpha = 0.2$ et de $\beta = 0.1$.

- X ~ Bern (α)
- Z ~ Bern (β)
- Y = X ⊕ Z

**a)** 1/1

$H(X) = H(\alpha)$

$H(Z) = H(\beta)$

$H(Y) = H(\alpha * \beta)$ # As we can say Y ~ Bern (α * β) O.K.

$= H(\alpha(1-\beta) + \beta(1-\alpha))$

**b)**

$H(XY) = H(XZ)$ 1/1

$= H(X) + H(Z)$

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

$H(X|Y) = H(X) + H(Z) - H(Y)$

$= H(\alpha) + H(\beta) - H(\alpha*\beta)$

$H(Y|X) = H(\beta)$

**c)** 1/1

$R1 \geq H(X|Y)$

$\geq H(\alpha) + H(\beta) - H(\alpha*\beta)$

$R2 \geq H(Y|X)$

$\geq H(\beta)$

$R1 + R2 \geq H(XY)$

$\geq H(\alpha) + H(\beta)$

As X and Y are not statistically independent like X & Z, the SW region is a **5-sided region** lower bounded on the R1 axis (X) by the conditional entropy of X knowing Y and lower bounded on the R2 axis (Y) by the conditional entropy of Y knowing X. I think this situation can be compared to a noisy communication, where the variable Z represent the noise induced through the channel and we are analyzing the rate at the input and at the output.

**d)**

$\alpha = 0.2$
$\beta = 0.1$

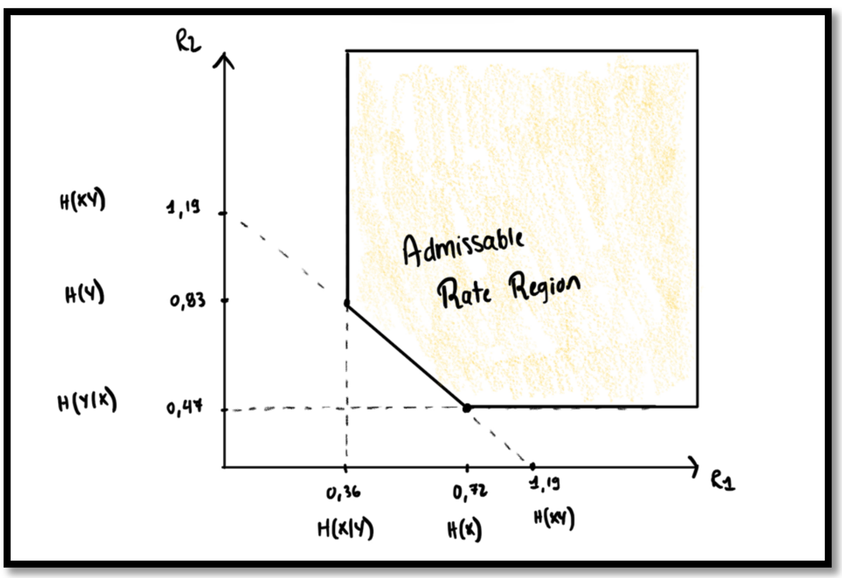
$R_1 \geq H(X|Y)$
$\geq H(\alpha) + H(\beta) - H(\alpha(1-\beta) + \beta(1-\alpha))$
$\geq H(0.2) + H(0.1) - H(0.26)$
$\geq -[(0.2 \log 0.2) + (0.8 \log 0.8)] - [(0.1 \log 0.1) + (0.9 \log 0.9)] + [(0.26 \log 0.26) + (0.74 \log 0.74)]$
$\geq 0.3641$

$R_2 \geq H(Y|X)$
$\geq H(\beta)$
$\geq H(0.1)$
$\geq -[(0.1 \log 0.1) + (0.9 \log 0.9)]$
$\geq 0.469$

$R_1 + R_2 \geq H(XY)$
$\geq H(\alpha) + H(\beta)$
$\geq H(0.2) + H(0.1)$
$\geq -[(0.2 \log 0.2) + (0.8 \log 0.8)] - [(0.1 \log 0.1) + (0.9 \log 0.9)]$
$\geq 1.1909$

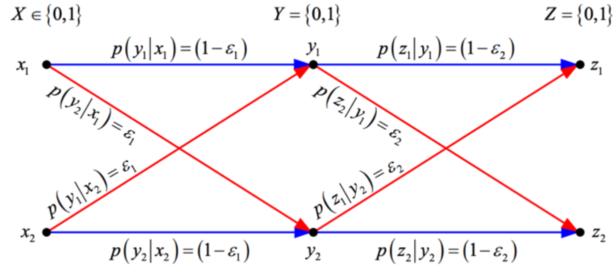
1/1

H (X) = 0.72
H (Y) = 0.83



- **Problème 5 :** 4.2/7

**Problème 10.1 :** La figure ci-dessous montre deux canaux symétriques binaires en cascade.




a) Écrivez l'expression de l'information mutuelle du canal $I(X;Y)$ en fonction de $\epsilon_1$.

b) Écrivez l'expression de l'information mutuelle du canal $I(X;Z)$ en fonction de $\epsilon_1$ de $\epsilon_2$.

c) Donnez capacité du canal $C_{XY}$ pour $\epsilon_1 = 0.1$.

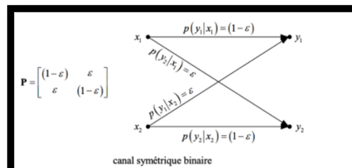
d) Donnez capacité du canal $C_{XZ}$ pour $\epsilon_1 = 0.1$ et $\epsilon_2 = 0.3$.

e) Considérez maintenant qu'il s'agit d'un canal symétrique binaire sous écoute où le canal $X \to Y$ représente le canal légitime entre $X$ (Alice) et $Y$ (Bernard), alors que le canal $X \to Z$ représente le canal dégradé sous écoute entre $X$ et $Z$ (Ève). Écrivez l'expression de la capacité secrète $C_S$ en fonction des information mutuelles $I(X;Y)$ et $I(X;Z)$. Dans ce cas, $C_S$ est obtenue avec une distribution uniforme.

f) Donnez la valeur numérique de la capacité secrète $C_S$ avec $\epsilon_1 = 0.1$ et $\epsilon_2 = 0.3$.

g) À l'aide d'un logiciel, faites également les courbes suivantes :
— $C_{XY}$ pour $0 \leq \epsilon_1 \leq 1$.
— $C_{XZ}$ pour $0 \leq \epsilon_1 \leq 1$ et $0 \leq \epsilon_2 \leq 1$ (graphique 3D).
— $C_S$ pour $0 \leq \epsilon_1 \leq 1$ et $0 \leq \epsilon_2 \leq 1$ (graphique 3D). Expliquez les résultats obtenus.

**a)** 0.5/1




- Symmetrical channel
- Hence input distribution equiprobable: p(x1) = p(x2) = 1/2

H (Y) = 1 Sh
H (E) = - Σ p (yj |xk) log b p (yj |xk)
= - [(1 − ε1) log $_b$ (1 − ε1) + ε1 log $_b$ ε1] *# E as row of the transition matrix*

I (X; Y) = H (Y) - H (Y|X)
= 1 - H (E)
= 1 + [(1 − ε1) log $_b$ (1 − ε1) + ε1 log $_b$ ε1]

dépend de [p(x1),p(x2)]

**b)** 0.5/1

$$P = \begin{bmatrix} 1-\varepsilon_1 & \varepsilon_1 \\ \varepsilon_1 & 1-\varepsilon_1 \end{bmatrix} \begin{bmatrix} 1-\varepsilon_2 & \varepsilon_2 \\ \varepsilon_2 & 1-\varepsilon_2 \end{bmatrix}$$
$$= \begin{bmatrix} (1-\varepsilon_1)(1-\varepsilon_2) + \varepsilon_1 \varepsilon_2 & (1-\varepsilon_1)\varepsilon_2 + \varepsilon_1(1-\varepsilon_2) \\ \varepsilon_1 \cdot (1-\varepsilon_2) + (1-\varepsilon_1)(\varepsilon_2) & \varepsilon_1 \cdot \varepsilon_2 + (1-\varepsilon_1)(1-\varepsilon_2) \end{bmatrix}$$

- Symmetrical channel
- Input distribution equiprobable: p(x1) = p(x2) = 1/2

H (Z) = 1 Sh
H (E) = - Σ p (yj |xk) log b p (yj |xk)
= - [(1 − ε) log $_b$ (1 − ε) + ε1 log $_b$ ε] *# E as row of the transition matrix*

The two cascaded BSC channels can be viewed as a single BSC channel with an overall loss parameter ε = ε1(1 - ε2) + ε2 (1 - ε1)

I (X; Z) = H (Z) - H (Z|X) = H (Z) - H (E)
= 1 + [(1 − ε) log $_b$ (1 − ε) + ε log $_b$ ε]
= 1 + [(1 − [ε1(1 - ε2) + ε2 (1 - ε1)]) log $_b$ (1 − [ε1(1 - ε2) + ε2 (1 - ε1)]) + [ε1(1 - ε2) + ε2 (1 - ε1)] log $_b$ [ε1(1 - ε2) + ε2 (1 - ε1)]]

dépend de [p(x1),p(x2)]

**c)** $\varepsilon 1 = 0.1$

$C = \text{Max } I(X;Y)$
$= 1 + [(1 - 0.1) \log_2 (1 - 0.1) + 0.1 \log_2 0.1]$
$= 1 + [-0.1368 - 0.33219]$
$= 0.5310$ Sh 1/1

**d)** $\varepsilon_1 = 0.1$ & $\varepsilon_2 = 0.3$

The two cascaded BSC channels can be viewed as a single BSC channel with an overall loss parameter $\varepsilon$:

$\varepsilon = \varepsilon 1(1 - \varepsilon 2) + \varepsilon 2 (1 - \varepsilon 1)$
$\varepsilon = 0.1 (1 - 0.3) + 0.3 (1 - 0.1)$
$\varepsilon = 0.34$

$C = \text{Max } I(X;Y)$
$= 1 + [(1 - \varepsilon) \log_b (1 - \varepsilon) + \varepsilon \log_b \varepsilon]$
$= 1 + [(1 - 0.34) \log_b (1 - 0.34) + 0.34 \log_b 0.34]$
$= 1 + [(0.66) \log_2 (0.66) + 0.26 \log_2 0.26]$
$= 1 + [-0.9009]$
$= 0.0991$Sh 0/1

**e)**

**Définition** *(Capacité secrète d'un canal sous écoute dégradé $C_S$* : La capacité secrète d'un canal sous écoute, discret et sans mémoire, dégradé est donnée par :

$$C_S = \max_{X \to Y \to Z} [I(X;Y) - I(X;Z)]$$

- Uniform distribution

1/1

$C_S = \max I(X;Y) - I(X;Z)$
$= [1 + [(1 - \varepsilon 1) \log_b (1 - \varepsilon 1) + \varepsilon 1 \log_b \varepsilon 1]] - [1 + [(1 - [\varepsilon 1(1 - \varepsilon 2) + \varepsilon 2 (1 - \varepsilon 1)]) \log_b (1 - [\varepsilon 1(1 - \varepsilon 2) + \varepsilon 2 (1 - \varepsilon 1)]) + [\varepsilon 1(1 - \varepsilon 2) + \varepsilon 2 (1 - \varepsilon 1)] \log_b [\varepsilon 1(1 - \varepsilon 2) + \varepsilon 2 (1 - \varepsilon 1)]]]$

**f)** 0.5/1

$\varepsilon 1 = 0.3$
$\varepsilon 2 = 0.1$

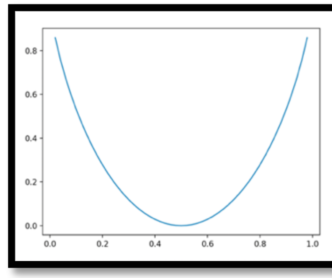
$C_S = \max I(X;Y) - I(X;Z)$
$= [1 + [(1 - \varepsilon 1) \log_b (1 - \varepsilon 1) + \varepsilon 1 \log_b \varepsilon 1]] - [1 + [(1 - [\varepsilon 1(1 - \varepsilon 2) + \varepsilon 2 (1 - \varepsilon 1)]) \log_b (1 - [\varepsilon 1(1 - \varepsilon 2) + \varepsilon 2 (1 - \varepsilon 1)]) + [\varepsilon 1(1 - \varepsilon 2) + \varepsilon 2 (1 - \varepsilon 1)] \log_b [\varepsilon 1(1 - \varepsilon 2) + \varepsilon 2 (1 - \varepsilon 1)]]]$

$= [1 + [(1 - 0.3) \log_b (1 - 0.3) + 0.3 \log_b 0.3]] - [1 + [(1 - [0.3 (1 - 0.1) + 0.1 (1 - 0.3)]) \log_b (1 - [0.3 (1 - 0.1) + 0.1 (1 - 0.3)]) + [0.3(1 - 0.1) + 0.1 (1 - 0.3)] \log_b [0.3 (1 - 0.1) + 0.1 (1 - 0.3)]]]$

$= 0.1187 - 0.07518$
$= 0.04352$ X

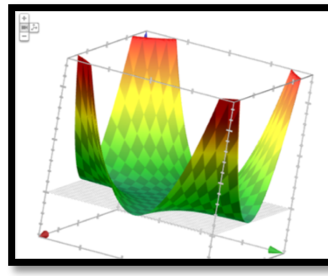
**g)** 0.7/1

- **$C_{XY}$ pour 0 <= ε1 <= 1**




*0 <= ε <= 1*
*C = 1 + [(1 − ε) log $_b$ (1 − ε) + ε log $_b$ ε]*

- **$C_{XZ}$ pour 0 <= ε1 <= 1 & 0 <= ε2 <= 1**

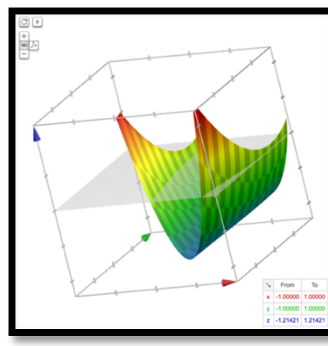


*0 <= ε1 <= 1*
*0 <= ε2 <= 1*

$C_{XZ}$ = 1 + [(1 − [ε1(1 - ε2) + ε2 (1 - ε1)]) log $_b$ (1 − [ε1(1 - ε2) + ε2 (1 - ε1)])
+ [ε1(1 - ε2) + ε2 (1 - ε1)] log $_b$ [ε1(1 - ε2) + ε2 (1 - ε1)]]

- **$C_S$ pour 0 <= ε1 <= 1 & 0 <= ε2 <= 1**

X



*0 <= ε1 <= 1*
*0 <= ε2 <= 1*

$C_S$ = **[**1 + [(1 − ε1) log $_b$ (1 − ε1) + ε1 log $_b$ ε1]**] -**
[1 + [(1 − [ε1(1 - ε2) + ε2 (1 - ε1)]) log $_b$ (1 − [ε1(1 - ε2) + ε2 (1 - ε1)]) + [ε1(1 - ε2) + ε2 (1 - ε1)] log $_b$ [ε1(1 - ε2) + ε2 (1 - ε1)]]]

- **Explanation**

When it comes to the Secret Capacity $C_s$, it is maximised when ε1 tends near 0 or 1 while ε2 tends near 0 or 1 too. On the other hand, it is minimized strongly when ε1 equal 0.5, whatever ε2 value.

This can be explained by the fact that we compute the Secret Capacity $C_s$ by maximising the difference between the mutual information of the channel $C_{XY}$ & $C_{XZ}$, and by putting the ε1 = 0.5, the $C_{XY}$ capacity via the mutual information formula [1 - H (E)] is minimized as we increase the entropy of the error term.

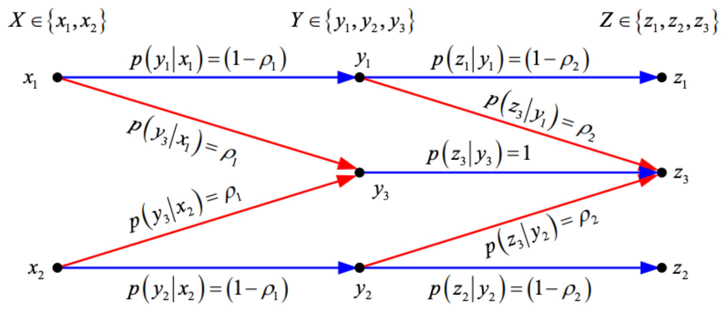
On the other hand, if we keep the ε1 uncertainty low by approaching 0 or 1, we are in the first step of maximizing our Secret Capacity $C_s$. The second step is to make ε2 as close as possible to 0 or 1 too, as unlike the first term of our equation that we searched to maximized, we are now trying to minimize the I (X; Z) term, which is done by having **both** the error approaching 0 or 1 as it gives in the Mutual Information formula 1 + [(1 − ε) log $_b$ (1 − ε) + ε log $_b$ ε] an error term that again minimize uncertainty as we can see below.

**Max: {0,0} {0,1} {1,0} {1,1}**

ε = ε1(1 - ε2) + ε2 (1 - ε1)
ε = 0 (1 - 0) + 0 (1 - 0) = **0**
ε = 1(1 - 0) + 0 (1 - 1) = **1**
ε = 1 (1 - 1) + 1 (1 - 1) = **0**
ε = 0 (1 - 1) + 1 (1 - 0) = **1**

- **Problème 6 :** 5/5

**Problème 10.2 :** La figure ci-dessous montre un canal symétrique binaire sous écoute où le canal $X \to Y$ représente le canal légitime entre $X$ (Alice) et $Y$ (Bernard), alors que le canal $X \to Z$ représente le canal dégradé sous écoute entre $X$ (Alice) et $Z$ (Ève).




a) Donnez l'expression de la capacité du canal légitime $C_{XY}$ en fonction de $\rho_1$.

b) Écrivez l'expression de la capacité du canal sous écoute $C_{XZ}$ en fonction de $\rho_1$ et de $\rho_2$.

c) Donnez l'expression de la capacité secrète $C_S$ en fonction des information mutuelles $I(X;Y)$ et $I(X;Z)$. Dans ce cas, $C_S$ est obtenue avec une distribution uniforme.

d) Donnez la valeur numérique de la capacité secrète $C_S$ avec $\rho_1 = 0.3$ et $\rho_2 = 0.1$.

e) À l'aide d'un logiciel, faites un graphique de la capacité secrète $C_S$ en fonction des probabilités $\rho_1$ et $\rho_2$ et interprétez le graphique obtenu.

**a)**

**Théorème** *(capacité d'un canal symétrique) :*
La capacité $C$ d'un canal symétrique de matrice de transition **P** est atteinte avec une source équiprobable $X \sim$ **p**, c.-à-d. $p(x_k) = \frac{1}{K}, \forall k$. Cette capacité est donnée par :

$$C = \left[\sum_{j=1}^{J} p(y_j|x_k) \log_b p(y_j|x_k)\right] + \log_b J$$

- Legitimate Channel
- Symmetrical Channel
- Erasure probability = $\rho_1$

$$P = \begin{bmatrix} (1-\rho_1) & — & \rho_1 \\ — & (1-\rho_1) & \rho_1 \end{bmatrix}$$

$C_{XY} = \sum p(y_j | x_k) \log_2 p(y_j | x_k) + \log_2 (J)$
$= [(1 - \rho_1) \log_2 (1 - \rho_1)] + 1$
$= 1 - \rho_1$

1/1

**b)**

- Wiretapped Channel (degraded)
- Symmetrical Channel
- Erasure probability = $(\rho_1 + \rho_2 - \rho_1\rho_2)$

$$P = \begin{bmatrix} (1-\rho_1)(1-\rho_2) & — & (1-\rho_1)(\rho_2) + (\rho_1)(1) \\ — & (1-\rho_1)(1-\rho_2) & (1-\rho_1)(\rho_2) + (\rho_1)(1) \end{bmatrix}$$

$C_{XZ} = \sum p(y_j | x_k) \log_2 p(y_j | x_k) + \log_2 (J)$
$= [(1 - (\rho_1 + \rho_2 - \rho_1\rho_2) \log_2 (1 - (\rho_1 + \rho_2 - \rho_1\rho_2))] + 1$
$= 1 - \rho_1 - \rho_2 + \rho_1\rho_2$
$= (1 - \rho_1)(1 - \rho_2)$

1/1

**c)**

**Définition** *(Capacité secrète d'un canal sous écoute dégradé $C_S$* : La capacité secrète d'un canal sous écoute, discret et sans mémoire, dégradé est donnée par :

$$C_S = \max_{X \to Y \to Z} [I(X;Y) - I(X;Z)]$$

- Uniform distribution

$C_S$ = max I (X; Y) - I (X; Z)
= $[1 - \rho 1] - [(1 - \rho 1)(1 - \rho 2)]$

1/1

**d)**

$\rho_1 = 0.3$
$\rho_2 = 0.1$

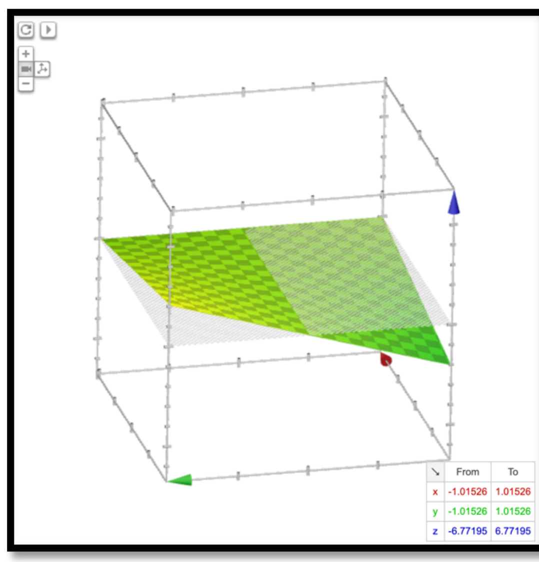
$C_S$ = max I (X; Y) - I (X; Z)
= $[1 - \rho 1] - [(1 - \rho 1)(1 - \rho 2)]$
= $[1 - 0.3] - [(1 - 0.3)(1 - 0.1)]$
= 0.07 1/1

**e)**

- **Secret Capacity ($C_S$) in function of $\rho_1$ et $\rho_2$**

$C_S = [1 - \rho 1] - [(1 - \rho 1)(1 - \rho 2)]$

1/1




- **Interpretation**:

As we can see on the graph, the Secret Capacity (Cs) is **maximised when we set the erasure probability ρ2 to 1 and set ρ1 to 0.** Additionally, we can observe that the Secret Capacity ($C_S$) will move toward 0 as the value of ρ2 approach 0 and/or the value of ρ1 approach 1. Again, this can be explained by the fact that when we try to maximise the difference between I (X; Y) & I (X; Z) to optimize (Cs), we first need the **highest first component of our formula** [1 − ρ1], which need **ρ1 minimized**. Then, we need the **smallest value for our second part**, which is [(1 − ρ1) (1 − ρ2)], obtained by the **highest ρ2 possible**.

**Max: {ρ1 = 0; ρ2 = 1}**