‹ercice 1. Entropie de la somme de 2 Variables Aléatoires. (2 points)

ient les Variables Aléatoires indépendantes X_1 et X_2 qui suivent une *loi de Bernoulli* avec valeurs $X_i \in \{0,1\}$ et probabilités $\begin{cases} p(X_i=1)=p \\ p(X_i=0)=1-p \end{cases}$ $i=1\cdots2$.

Calculer, en fonction de p, *l'entropie* $H(Y)$ de la Variable Aléatoire $Y=X_1+X_2$. ▯

Dans le cas particulier $p=0.5$, donner la *valeur numérique* de *l'entropie* $H(Y)$. ▯

‹ercice 2. Codage optimal de Huffman. (5 points)

e université doit communiquer par voie télématique une liste de résulats (notes A, B, C, D ou E d'une matière) concernant)0 étudiants. Ces résultats sont les suivants :

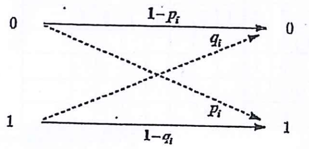
Note	A	B	C	D	E
Nombre d'étudiants	100	150	500	200	50

Calculer *l'entropie* de la source d'information constituée par les résultats. ▯
Construire un *arbre de Huffman* en vue de la compression sans pertes des données. ▯
En déduire un *code de Huffman* associé à chaque note. ▯
Donner la *longueur moyenne* du code de Huffman construit. ▯
Indiquer (en %) le *taux de compression* t réalisé par rapport à une transmission classique (codage ASCII fixe 8 bits caractère A, B, C, D ou E). ▯

‹ercice 3. Canal de transmission asymétrique bruité. (4 points)

source d'information binaire émet les symboles 0 et 1 avec les probabilités $P(0)=p=0.1$ et $)=q=1-p=0.9$. Ces bits sont transmis à un récepteur à travers un canal bruité illustré ci-dessous, avec les abilités d'erreurs de transmission $p_i=0.1$ pour un bit 0, et $q_i=0.6$ pour un bit 1. En notant X et Y les boles respectivement *émis* et *reçus*, calculer les caractéristiques suivantes, en valeurs numériques :

s *entropies* $H(X)$ et $H(Y)$. ▯
s *entropies* $H(X,Y)$, $H(Y|X)$. ▯
information mutuelle moyenne $I(X;Y)$ et la *probabilité*, notée p_e, d'*erreur de transmission d'un symbole*. ▯
capacité C du canal en *absence de bruit*. ▯



‹cice 4. Code cyclique. (5 points)

isidère un code en bloc linéaire, de paramètres $(n,k)=(8,2)$, de matrice génératrice : $\mathbf{G}=\begin{pmatrix}1&0\\1&1\\1&0\\1&1\\1&0\\1&1\\1&0\\1&1\end{pmatrix}$

e la *matrice génératrice* sous forme systématique $\widetilde{\mathbf{G}}$ permettant d'obtenir la *forme systématique* du code. 0.5
ner la *table de code* obtenue par construction systématique du code. 0.5
éduire la *distance minimale* d de ce code. 0.5
bien d'erreurs peut-il toujours *détecter* ? Combien d'erreurs peut-il toujours *corriger* ? ▯
miner la *matrice de contrôle* $\mathbf{H}$ du code. 0.5
e message reçu $\boldsymbol{\omega}^T=(1\ \ 0\ \ 1\ \ 0\ \ 1\ \ 1\ \ 0\ \ 0)$ entaché de 2 erreurs. La correction de ce mot est-elle ? 0.5
correction est possible, donner le *mot-source* issu du décodage de $\boldsymbol{\omega}$. ▯
de construit est un code dit *cyclique*, car lorsqu'on décale un mot-code d'1 bit vers la droite circulairement, on in mot appartenant au code. Un code cyclique s'obtient à partir d'un mot du code particulier dit *mot générateur* itué de n bits $\mathbf{g}=b_{n-1}b_{n-2}\cdots b_1b_0$ tel que tous les mots du code sont *multiples* de $\mathbf{g}$. On associe ment au mot générateur, un polynôme $g(x)=b_{n-1}x^{n-1}+b_{n-2}x^{n-2}+\cdots+b_1x+b_0$ dit *polynôme* *eur* du code et tel que les polynômes associés aux mots du code sont *multiples* de $g(x)$.
le *polynôme générateur* du code. 0.5

‹ce 5. Code systématique. (4 points)

ode linéaire $C_{n,k}=C_{7,4}$ qui au vecteur d'information (bits i_1 à i_4) $\mathbf{i}^T=(i_1\ \ i_2\ \ i_3\ \ i_4)$ associe le mot de i_1 à i_4 et c_5 à c_7) $\mathbf{c}^T=(i_1\ \ i_2\ \ i_3\ \ i_4\ \ c_5\ \ c_6\ \ c_7)$ avec $\begin{cases} c_5=i_1+i_3+i_4 \\ c_6=i_1+i_2+i_3 \\ c_7=i_2+i_3+i_4 \end{cases}$.

r la *matrice génératrice* de ce code. ▯
r la *matrice de contrôle* $\mathbf{H}$ de ce code. ▯
$=(1\ \ 0\ \ 1\ \ 0)$, quel est le mot de code associé ? ▯
message $\mathbf{m}^T=(1\ \ 1\ \ 1\ \ 1\ \ 0\ \ 0\ \ 1)$. Est-ce un mot du code ? ▯

Exercice 1. Entropie de la somme de 2 Variables Aléatoires.

1. $Y=\begin{cases} 0 & \text{avec} & p(Y=0)=p(X_1=0 \text{ et } X_2=0)=p(X_1=0)\cdot p(X_2=0)=(1-p)^2 \\ 1 & \text{avec} & p(Y=1)=p(X_1=0 \text{ et } X_2=1)+p(X_1=1 \text{ et } X_2=0)=p(X_1=0)\cdot p(X_2=1)+p(X_1=1)\cdot p(X_2=0)=2p(1-p) \\ 2 & \text{avec} & p(Y=2)=p(X_1=1 \text{ et } X_2=1)=p(X_1=1)\cdot p(X_2=1)=p^2 \end{cases}$

$\rightarrow H(Y)=-(1-p)^2\log_2(1-p)^2-2p(1-p)\log_2[2p(1-p)]-p^2\log_2 p^2$

$\rightarrow \boxed{H(Y)=-2p(1-p)-2p\log_2 p-2(1-p)\log_2(1-p)}$ car $\log_2(2)=1$

2. $\boxed{H(Y)=1.5\,\text{bits/symbole}}$

Exercice 2. Codage optimal de Huffman.

Table des fréquences des notes :

Note	A	B	C	D	E
Nombre d'étudiants	100	150	500	200	50
Fréquence	0.1	0.15	0.5	0.2	0.05

1. *Entropie :*

$\boxed{H=-0.1\log_2(0.1)-0.15\log_2(0.15)-0.5\log_2(0.5)-0.2\log_2(0.2)-0.05\log_2(0.05)\approx 1.92\,\text{bits/symbole}}$

2. *Arbre de Huffman :*

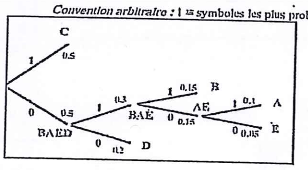
s_i	C	D	B	A	E
p_i	0.5	0.2	0.15	0.1	0.05

s_i	C	D	B	AE
p_i	0.5	0.2	0.15	0.15

s_i	C	BAE	D
p_i	0.5	0.3	0.2

s_i	C	BAED
p_i	0.5	0.5

Convention arbitraire : 1 ≡ symboles les plus probables, 0 ≡ symboles les moins probables



3. *Code de Huffman associé :*

s_i	A	B	C	D	E
p_i	0.1	0.15	0.5	0.2	0.05
m_i	0101	011	1	00	0100
l_i	4	3	1	2	4

4. *Longueur moyenne du code de Huffman :*

$\boxed{\overline{L}=\sum_{i=1}^{5}p_il_i=4\cdot 0.1+3\cdot 0.15+1\cdot 0.5+2\cdot 0.2+4\cdot 0.05=1.95\,\text{bits/symbole}}$

5. $\boxed{t=\frac{8-1.95}{8}=75.6\%}$

Exercice 3. Canal de transmission asymétrique bruité.

L'énoncé définit les matrices de distributions de probabilités *conditionnelle* $P(Y|X)$ et *marginale* $P_X=P(X)$:

$P(Y|X)=$

$X \setminus Y$	0	1	P_X
0	$1-p_i=0.9$	$p_i=0.1$	$p=0.1$
1	$q_i=0.6$	$1-q_i=0.4$	$q=1-p=0.9$

Le calcul de $H(X,Y)$ requiert la détermination préalable de la distribution *conjointe* $P(X,Y)$:

$$p(x_i,y_j)=p(y_j\,|\,x_i)p(x_i) \qquad i=1,\ldots,n=2 \quad j=1,\ldots,m=2.$$

$P(X,Y)$ permet aussi le calcul de la distribution *marginale* $P_Y=P(Y)$:

$$p(y_j)=\sum_{i=1}^{n=2}p(x_i,y_j) \text{ impliquée dans le calcul de } H(Y).$$

$P(X,Y)=$

$X \setminus Y$	0	1	P_X
0	$(1-p_i)p=0.09$	$p_ip=0.01$	$p=0.1$
1	$q_i(1-p)=0.54$	$(1-q_i)(1-p)=0.36$	$q=1-p=0.9$
P_Y	$(1-p_i)p+q_i(1-p)=0.63$	$p_ip+(1-q_i)(1-p)=0.37$	

1. $\boxed{H(X)=-\sum_{i=1}^{n=2}p(x_i)\log_2[p(x_i)]=-p\log_2(p)-(1-p)\log_2(1-p)\approx 0.469\,\text{bit/symbole}}$.

$\boxed{H(Y)=-\sum_{j=1}^{m=2}p(y_j)\log_2[p(y_j)]=-[(1-p_i)p+q_i(1-p)]\log_2[(1-p_i)p+q_i(1-p)]-[p_ip+(1-q_i)(1-p)]\log_2[p_ip+(1-q_i)(1-p)]=0.951\,\text{bit/symbole}}$.

2.

$\boxed{H(X,Y)=-\sum_{i=1}^{n=2}\sum_{j=1}^{m=2}p(x_i,y_j)\log_2[p(x_i,y_j)]=-(1-p_i)p\log_2[(1-p_i)p]-p_ip\log_2(p_ip)-q_i(1-p)\log_2[q_i(1-p)]-(1-q_i)(1-p)\log_2[(1-q_i)(1-p)]\approx 1.39\,\text{bits/symbole}}$

$\boxed{H(Y|X)=-\sum_{i=1}^{n=2}\sum_{j=1}^{m=2}p(x_i,y_j)\log_2[p(y_j|x_i)]=-(1-p_i)p\log_2(1-p_i)-p_ip\log_2(p_i)-q_i(1-p)\log_2(q_i)-(1-q_i)(1-p)\log_2(1-q_i)\approx 0.921\,\text{bit/symbole}}$

3. $\boxed{I(X;Y)=I(Y;X)=H(X)-H(X|Y)=H(Y)-H(Y|X)=0.03\,\text{bit/symbole}}$.

- *probabilité* p_e d'*erreur de transmission d'un symbole* :

la *probabilité* d'*erreur de transmission d'un symbole* s'obtient à partir de la matrice de probabilités *conjointe* $P(X,Y)$ qui met en jeu à la fois la matrice de *transition* $P(Y|X)$ et la distribution *marginale* P_X :

$\boxed{p_e=P(X=0 \text{ et } Y=1)+P(X=1 \text{ et } Y=0)=p[(X,Y)=(0,1)]+p[(X,Y)=(1,0)]=p_ip+q_i(1-p)=0.55}$

4. Pour un canal sans bruit: $H(X|Y)=0 \rightarrow \boxed{C=\max_{P_X}I(X;Y)=\max_{p\in[0,1]}I(X;Y)=\max_{p\in[0,1]}H(X)=H(X)\big|_{p=0.5}=1\,\text{bit/symbole}}$

Exercice 4. Code cyclique.

$$\mathbf{G}=\begin{array}{cc} c_1 & c_2 \end{array}\begin{pmatrix}1&0\\1&1\\1&0\\1&1\\1&0\\1&1\\1&0\\1&1\end{pmatrix}$$

1. Echelonnage de $\mathbf{G}:\begin{cases}c_1\leftarrow c_1+c_2\\ c_2\leftarrow c_2\end{cases}\rightarrow \boxed{\tilde{\mathbf{G}}=\begin{pmatrix}1&0\\0&1\\1&0\\0&1\\1&0\\0&1\\1&0\\0&1\end{pmatrix}=\begin{pmatrix}\mathbf{I}_k\\ \mathbf{G}'\end{pmatrix}}$ avec $\mathbf{G}'=\begin{pmatrix}1&0\\0&1\\1&0\\0&1\\1&0\\0&1\end{pmatrix}$

2. *Image du code*

#	mot source $\mathbf{m}_i^T$	mot-code $\omega_i^T=(\mathbf{G}\mathbf{m}_i)^T=(\tilde{\mathbf{G}}\mathbf{m}_i)^T=\left[\begin{pmatrix}\mathbf{I}_k\\ \mathbf{G}'\end{pmatrix}\mathbf{m}_i\right]^T=\begin{pmatrix}\mathbf{m}_i\\ \mathbf{G}'\mathbf{m}_i\end{pmatrix}^T=\left[\mathbf{m}_i^T\middle|(\mathbf{G}'\mathbf{m}_i)^T\right]$	distance, poids $d_h(\omega_i,0)=w(\omega_i)$ (= nombre de bits 1 de ω_i)
1	00	00 000000	0
2	01	01 010101	4
3	10	10 101010	4
4	11	11 111111	8

$\hookrightarrow d=4$

3. $\boxed{d=4}$

4. Capacité de détection d'erreurs : $\boxed{e_d=d-1=3}$ Capacité de correction d'erreurs : $\boxed{e_c=E\left[\frac{d-1}{2}\right]=1}$

5. $\mathbf{H}=(\mathbf{G}'|\mathbf{I}_{n-k})\rightarrow \boxed{\mathbf{H}=\begin{pmatrix}1&0&1&0&0&0&0&0\\0&1&0&1&0&0&0&0\\1&0&0&0&1&0&0&0\\0&1&0&0&0&1&0&0\\1&0&0&0&0&0&1&0\\0&1&0&0&0&0&0&1\end{pmatrix}}$

6. La correction de $\omega=(1\ \ 0\ \ 1\ \ 0\ \ 1\ \ 1\ \ 0\ \ 0)^T$ entaché de 2 erreurs n'est pas garantie car la *capacité de correction* est d'1 erreur, mais elle est possible par décodage au sens de minimum de distance de Hamming.

7. *Mot-source* issu du décodage de ω par décodage *au sens de minimum de distance de Hamming* :

$$\begin{cases}d_H(\omega,00\,000000)=4\\ d_H(\omega,01010101)=6\\ d_H(\omega,10101010)=2\\ d_H(\omega,11111111)=4\end{cases}\rightarrow \text{mot-code corrigé}: \omega'=(1\ \ 0\ \ 1\ \ 0\ \ 1\ \ 0\ \ 1\ \ 0)^T\rightarrow \text{mot-source}: \boxed{(1\ \ 0)^T}.$$

8.

$\omega_1=00\,000000$: polynôme correspondant : $\omega_1(x)=0$

$\omega_2=01\,010101$: polynôme correspondant : $\omega_2(x)=x^6+x^4+x^2+1$

$\omega_3=10\,101010$: polynôme correspondant : $\omega_3(x)=x^7+x^5+x^3+x$

$\omega_4=11111111$: polynôme correspondant : $\omega_4(x)=x^7+x^6+x^5+x^4+x^3+x^2+x+1$

$\rightarrow$ **polynôme générateur :** $\boxed{g(x)=\omega_2(x)=x^6+x^4+x^2+1}$ $\begin{cases}\omega_1(x)=0\cdot g(x)\\ \omega_2(x)=1\cdot g(x)\\ \omega_3(x)=x\cdot g(x)\\ \omega_4(x)=(x+1)\cdot g(x)\end{cases}$

(le polynôme générateur est de degré $n-k$)

$\rightarrow$ mot générateur : $\mathbf{g}=01\,010101$ $\begin{cases}\omega_1=0\cdot g\\ \omega_2=1\cdot g\\ \omega_3=10\cdot g\\ \omega_4=11\cdot g\end{cases}$

ω_3															ω_2
1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	
1	0	1	0	1	0	1		1	0						
0	0	0	0	0	0	0	0								

ω_4															ω_2
1	1	1	1	1	1	1	1	1	0	1	0	1	0	1	
1	0	1	0	1	0	1		1	1						
0	1	0	1	0	1	0	1								
	1	0	1	0	1	0	1								
	0	0	0	0	0	0	0								

Exercice 5. Code systématique.

1. Le code est donné sous forme systématique car les mots-codes ont les mots-sources pour préfixes. La matrice génératrice apparaît donc directement sous forme systématique :

$$\mathbf{G}=\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\\1&0&1&1\\1&1&1&0\\0&1&1&1\end{pmatrix}=\begin{pmatrix}\mathbf{I}_k\\ \mathbf{G}'\end{pmatrix}\quad\text{avec } \mathbf{G}'=\begin{pmatrix}1&0&1&1\\1&1&1&0\\0&1&1&1\end{pmatrix}$$

2. $\mathbf{H}=(\mathbf{G}'|\mathbf{I}_{n-k})\rightarrow\boxed{\mathbf{H}=\begin{pmatrix}1&0&1&1&1&0&0\\1&1&1&0&0&1&0\\0&1&1&1&0&0&1\end{pmatrix}}$

3. $\mathbf{i}^T=(1\ \ 0\ \ 1\ \ 0)\rightarrow\boxed{\mathbf{c}^T=\left(\mathbf{i}^T\middle|(\mathbf{G}'\mathbf{i})^T\right)=(1\ \ 0\ \ 1\ \ 0\ \ 0\ \ 0\ \ 1)}$.

car $\mathbf{G}'\mathbf{i}=\begin{pmatrix}1&0&1&1\\1&1&1&0\\0&1&1&1\end{pmatrix}\begin{pmatrix}1\\0\\1\\0\end{pmatrix}=\begin{pmatrix}0\\0\\1\end{pmatrix}$

4. ▪ *méthode du syndrome :* $\mathbf{S}=\mathbf{H}\cdot\mathbf{m}=\begin{pmatrix}1&0&1&1&1&0&0\\1&1&1&0&0&1&0\\0&1&1&1&0&0&1\end{pmatrix}\begin{pmatrix}1\\1\\1\\1\\0\\0\\1\end{pmatrix}=\begin{pmatrix}1\\1\\0\end{pmatrix}\neq 0$

$\rightarrow \boxed{\mathbf{m}\text{ non mot-code}}$

▪ *méthode directe :* $\mathbf{m}^T\overset{?}{=}\left(\mathbf{i}^T\middle|(\mathbf{G}'\mathbf{i})^T\right)$; $\mathbf{i}^T=(1\ \ 1\ \ 1\ \ 1)\rightarrow\mathbf{G}'\mathbf{i}=\begin{pmatrix}1&0&1&1\\1&1&1&0\\0&1&1&1\end{pmatrix}\begin{pmatrix}1\\1\\1\\1\end{pmatrix}=\begin{pmatrix}1\\1\\1\end{pmatrix}\neq\begin{pmatrix}0\\0\\1\end{pmatrix}$

$\rightarrow \boxed{\mathbf{m}\text{ non mot-code}}$

Entropie : $H(X)=-\sum_{i=1} p_i \log_2(p_i)$
avec $\log_2=\frac{\ln x}{\ln 2}$
Dans le cas d'une distrib uniforme $H(Y)=\log_2(2)=1$

Inégalité de Kraft
Un code sans préfixe (= instantané) de longueurs de mots données $(l_1,l_2,\dots,l_n)$ existe ssi $\sum_{i=1} d^{-l_i}\geq 1$
où d taille de l'alphabet du canal, et n la taille de la source ($d=2$ pr canal binaire)

Méthode de Huffman :
On trie les caractères de la source par proba décroissante.

s_i	a	e	i	c	g	j	h	d	f	b
p_i	0,2	0,15	0,15	0,1	0,1	0,1	0,05	0,05	0,05	0,05

On regroupe les 2 caractères les ⊖ probables (les plus petits).
On obtient :

s_i	a	e	i	c	g	j	fh	b	d
p_i	0,2	0,15	0,15	0,1	0,1	0,1	0,1	0,05	0,05

etc..
Jusqu'à :

s_i	ajeic	gfhbd
p_i	0,6	0,4

On en déduit l'arbre qui fournit un code optimal sans préfixe.

Théorème Borne inférieure :
Soit une source S d'alphbt $\Omega_s=\{s_1,\dots,s_n\}$, de taille n et de distribution de probabilités $P_s=\{p_1,\dots,p_n\}$. Soit un canal d'alphbt binaire $\Omega_c=\{0,1\}$, donc de taille $d=2$, sans bruit, stationnaire et sans mémoire. Soit un code déchiffrable $\{m_1,\dots,m_n\}$ de longueurs de mots $\{l_1,\dots,l_n\}$.
Alors la longueur moyenne des mots de code vérifie $\bar{L}=\sum_{i=1}^{n} p_i l_i\geq\frac{H(S)}{\log_2(d)}$
L'égalité n'est possible que si $\forall i=1,\dots,n$, $p_i=d^{-l_i}=2^{-l_i}$

Taux de compression (%) : $\frac{NC-C}{NC}=1-\frac{C}{NC}$
avec NC : taille des données non compressées
C : taille des données compressées

Taux de compression (autre méthode) :
$t=\frac{8-\bar{L}}{8}$ si encodé en 8 bits

Modélisation mathématique d'un canal

• Distribution marginale
$$\begin{cases}P_X=P(X):\{x_i\}_{i=1}^{n}\rightarrow[0,1]\quad x_i\mapsto p(x_i)=\sum_{j=1}^{m}p(x_i,y_j)\\ P_Y=P(Y):\{y_j\}_{j=1}^{m}\rightarrow[0,1]\quad y_j\mapsto p(y_j)=\sum_{i=1}^{n}p(x_i,y_j)\end{cases}$$

Exemple :

X\Y	y_1	y_2	P_X
x_1	0,25	0	0,25
x_2	0,1	0,3	0,4
x_3	0,1	0,25	0,35
P_Y	0,45	0,55	

Alphabet $\Omega_X\{x_1,x_2,x_3\}$ de taille $n=3$
$\Omega_Y\{y_1,y_2\}$ de taille $m=2$

• Distribution conditionnelle $P(X|Y)$ et $P(Y|X)$
$$p(x_i|y_j)=\frac{p(x_i,y_j)}{p(y_j)}\qquad p(y_j|x_i)=\frac{p(x_i,y_j)}{p(x_i)}$$
$i=1,\dots,n\qquad j=1,\dots,m$

$$P(X|Y)=\begin{pmatrix}0{,}25/0{,}45 & 0/0{,}55\\ 0{,}1/0{,}45 & 0{,}3/0{,}55\\ 0{,}1/0{,}45 & 0{,}25/0{,}55\end{pmatrix}\qquad P(Y|X)=\begin{pmatrix}0{,}25/0{,}25 & 0/0{,}25\\ 0{,}1/0{,}4 & 0{,}3/0{,}4\\ 0{,}1/0{,}35 & 0{,}25/0{,}35\end{pmatrix}$$

• Distribution conjointe de X et Y : $P(X,Y)$
$$p(x_i,y_j)=p(y_j|x_i)\,p(x_i)\quad i=1\dots n,\ j=1\dots m$$

Entropie conjointe $H(X,Y)=-\sum_{i=1}^{n}\sum_{j=1}^{m}p(x_i,y_j)\log_2[p(x_i,y_j)]$

Entropie conditionnelle $H(X|Y)=-\sum_{i=1}^{n}\sum_{j=1}^{m}p(x_i,y_j)\log_2[p(x_i|y_j)]$

Information mutuelle $=I(X;Y)=I(Y,X)=H(Y)-H(Y|X)=H(X)-H(X|Y)$

Méthode codage RLE (RUN LENGTH ENCODING)
Consiste à établir des couples (nb, c) où nb est le nbre de caractères de la séquence, et c ce caractère.
Ex : NNNBBGGG $\rightarrow$ (3,N)(2,B)(3,G)
RLE + Huffman :
On tire une table des fréquences des couples obtenus

Couple	n couples
Nb occurence	2
Fréquence P_i	2/n

On en tire l'entropie, ainsi que l'arbre de Huffman

Pour l'exemple ci-dessous :
$$G'=\begin{pmatrix}1&0&1&1\\0&1&1&1\\1&1&0&1\\1&1&1&0\end{pmatrix}$$

Codage de Canal
Distance minimale d'un code : Nombre de modif à faire pour passer d'un mot à l'autre (2 mots normalement). Ex : $w_1=000$, $w_2=111$.
Distance minimale $d=3$ car $\begin{matrix}0&0&0\\ \downarrow&\downarrow&\downarrow\\ 1&1&1\end{matrix}$ 3 chgmnts
Capacité de détection $e_d=d-1=2$ ici
Capacité de correction $e_c=E\left[\frac{d-1}{2}\right]=1$ ici
Code linéaire : $w=G\,m$ matrice génératrice, $\dim G=n\times k$ (~~ligne~~ ligne colonne)
mot code (000 - 111), mot-source (0-1)

Forme systématique de G :
$$\tilde{G}=\begin{pmatrix}I_k\\ \hline G'\end{pmatrix}\leftarrow \text{identité de rang } k$$
Pour obtenir cette matrice $\tilde{G}$ on échelonne G autant de fois qu'il faut.

Ensemble des mots-code

	2^k mots-source m	mots-code : $w=m^T|(G'm)^T$	distance nbre de bits 1 ds le mot code
1	0000	0000 (m) 0000 ($G'm$)	0
2	1000	1000 1011	4
3	0100	0100 0111	4
⋮	⋮	etc ⋮	⋮

distance minimale du code = plus petit poids non nul
Capacité de détection : $e_d=d-1$
Capacité de correction : $e_c=E\left[\frac{d-1}{2}\right]$