

## EXERCICES DU CHAPITRE IV

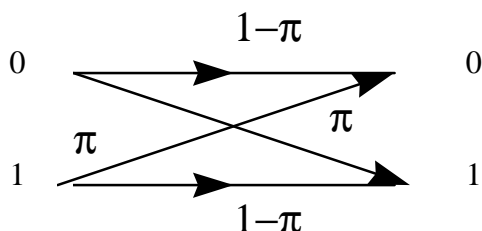
---

### EXERCICE 1

1. On a vu en cours que le code  $C(7, 4)$  est un code parfait. La distance minimum de ce code étant  $d_m = 3$ , il est 1-correcteur. On sait aussi que si plus d'une erreur est commise, alors le principe du décodage à distance minimum induira systématiquement une erreur sur le mot. En conséquence, l'événement  $D_C = \{\text{décision correcte}\}$  s'écrit;

$$D_C = \{\text{aucune erreur sur les 7 éléments binaires}\} \cup \{1 \text{ erreur parmi les 7 éléments binaires}\}$$

Pour effectuer le calcul de  $P\{D_C\}$ , il faut connaître la probabilité d'erreur sur un canal binaire symétrique (par élément binaire).



$$P\{\text{erreur}\} = P\{"0" \text{ émis} \cap "1" \text{ reçu}\} + P\{"1" \text{ émis} \cap "0" \text{ reçu}\}$$

$$P\{\text{erreur}\} = P\{"1" \text{ reçu} / "0" \text{ émis}\}P\{"0" \text{ émis}\} + P\{"0" \text{ reçu} / "1" \text{ émis}\}P\{"1" \text{ émis}\}$$

$$\text{soit } P\{\text{erreur}\} = \pi \times P\{"0" \text{ émis}\} + \pi \times P\{"1" \text{ émis}\} = \pi [P\{"0" \text{ émis}\} + P\{"1" \text{ émis}\}] = \pi$$

On déduit alors;

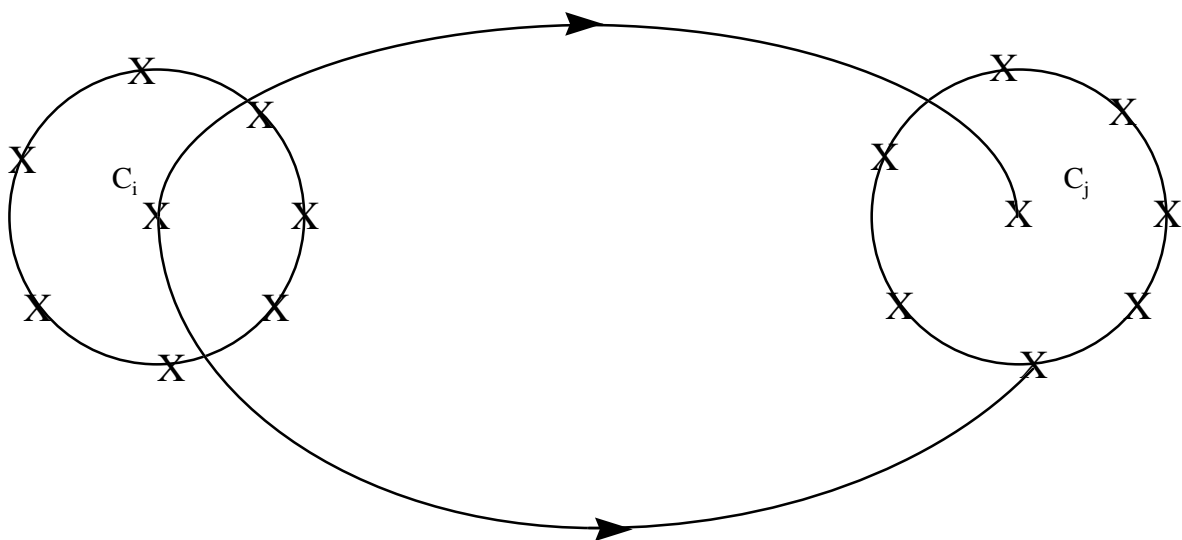
$$P\{D_C\} = (1 - \pi)^7 + C_7^1 \pi (1 - \pi)^6$$

En prenant  $\pi = 0,1$ , on obtient  $P\{D_C\} = 0,85$ .

2. Nous allons montrer que le canal obtenu en englobant codeur, canal binaire symétrique et décodeur est un canal symétrique. Remarquons tout d'abord que la taille de l'alphabet d'entrée, et par conséquent de sortie, est  $K = 2^4$  (correspondant au nombre de mots binaires contenant 4 éléments binaires d'information). D'autre part, nous allons établir que la probabilité qu'un mot code  $C_i$  soit interprété en un mot code  $C_j$  n'est fonction que de la distance entre  $C_i$  et  $C_j$ .

Considérons à cet effet deux mots code  $C_i$  et  $C_j$  tels que  $d(C_i, C_j) = l$ . On note  $n$  la longueur des mots. La boule fermée centrée sur  $C_i$  (resp.  $C_j$ ) et de rayon  $1 = \text{ent}\left(\frac{d_m - 1}{2}\right)$  contient 8 mots;

- le centre  $C_i$  (resp.  $C_j$ ),
- 7 mots différant de  $C_i$  (resp.  $C_j$ ) par un élément binaire sur sa périphérie.



Pour que  $C_i$  soit interprété en  $C_j$ , trois cas sont possibles:

- $C_i$  est directement transformé en  $C_j$ . La probabilité de cette occurrence est;

$$\underbrace{\pi^l}_{\substack{\text{les } l \text{ éléments binaires} \\ \text{qui diffèrent de } C_i \text{ à } C_j}} \underbrace{(1 - \pi)^{n-l}}_{\substack{\text{les } n-l \text{ autres}}},$$

- $C_i$  est transformé en l'un des mots qui diffèrent de  $C_j$  d'un élément binaire choisi parmi les  $l$  qui diffèrent de  $C_i$  à  $C_j$ . La probabilité correspondante est  $C_i^1 \pi^{l-1} (1 - \pi)^{n-(l-1)}$ ,

-  $C_i$  est transformé en l'un des mots qui diffèrent de  $C_j$  d'un élément binaire choisi parmi les  $n-l$  qui sont identiques de  $C_i$  à  $C_j$ . La probabilité associée est  $C_{n-l}^l \pi^{l+1} (1-\pi)^{n-(l+1)}$ . On obtient donc;

$$P\{C_i \rightarrow C_j\} = \pi^l (1-\pi)^{n-l} + l \pi^{l-1} (1-\pi)^{n-(l-1)} + (n-l) \pi^{l+1} (1-\pi)^{n-(l+1)}$$

On constate que cette grandeur ne dépend que des grandeurs fixées  $n, \pi$  et de la distance  $l = d(C_i, C_j)$ .

Pour construire la ligne  $i$  de la matrice de transition, on part du mot code  $C_i$  et on calcule tous les  $d(C_i, C_j)$ . On a bien sûr pour un mot code  $C_j$ ;

$$d(C_i, C_j) = w(C_i + C_j) = w(C_k)$$

(le code étant linéaire,  $C_i + C_j$  est un mot code que l'on note  $C_k$ )

Si  $C_j'$  désigne un mot code différent de  $C_j$ , alors  $C_i + C_j' \neq C_i + C_j$  (car un code est un sous-groupe additif). Et si on note  $C_k' = C_i + C_j'$ , on aura  $d(C_i, C_j') = w(C_k')$ .

Par conséquent, partant de  $C_i$ , on va décrire tous les poids des mots code. Et on procédera de même pour chaque ligne. Ainsi on peut affirmer que toutes les lignes sont identiques (à des permutations près). Et comme la distance est une grandeur symétrique, les colonnes seront, elles aussi, identiques (à des permutations près).

Donc le canal est symétrique.

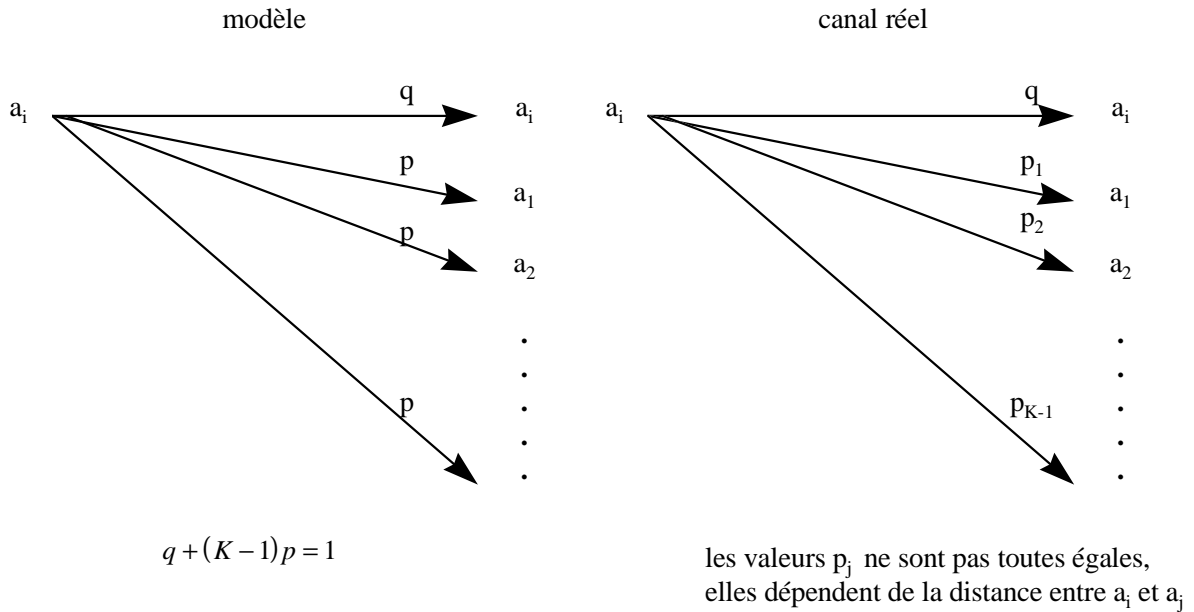
Le problème consiste maintenant à comparer la capacité du canal réel (sans la calculer) avec la capacité du modèle proposé.

Notons que la matrice de transition du modèle, comme celle du canal réel, a ses colonnes identiques (à des permutations près). La conséquence est que la loi de la variable de sortie  $Y$  sera uniforme si la loi de la variable d'entrée  $X$  est uniforme: les canaux étant symétriques, on sait que les capacités sont atteintes pour des lois uniformes sur l'entrée.

$$\text{Ainsi } H_{\text{modèle}}(Y) = H_{\text{canal réel}}(Y)$$

Il reste à comparer  $H_{\text{modèle}}(Y/X)$  et  $H_{\text{canal réel}}(Y/X)$ . En fait, la loi de  $Y$  étant uniforme, il nous suffit de comparer  $H_{\text{modèle}}(Y/X)$  et  $H_{\text{canal réel}}(Y/X = a_i)$ .

Pour le modèle, on choisira  $q$  de telle sorte que  $q = P\{C_i \rightarrow C_i\} = P\{D_C\}$ . On obtient les schémas:



Considérons alors les deux vecteurs de probabilité;

$$(r_i)_{i=1}^K = (q, p, p, \dots, p) \text{ et } (q_i)_{i=1}^K = (q, p_1, p_2, \dots, p_{K-1})$$

L'application du lemme fondamental à ces deux vecteurs donne:

$$\sum_{i=1}^K q_i \log_2 \frac{r_i}{q_i} \leq 0, \text{ soit } \sum_{i=1}^K q_i \log_2 r_i - \sum_{i=1}^K q_i \log_2 q_i \leq 0$$

$$\text{D'où } -\sum_{i=1}^K q_i \log_2 q_i \leq -\sum_{i=1}^K q_i \log_2 r_i = -q \log_2 q - \sum_{i=2}^K q_i \log_2 p$$

$$\text{or } \sum_{i=2}^K q_i = \sum_{j=1}^{K-1} p_j = 1 - q = (K - 1)p = \sum_{i=2}^K p$$

$$\text{donc } -\sum_{i=1}^K q_i \log_2 q_i \leq -q \log_2 q - \sum_{i=2}^K p \log_2 p = -\sum_{i=1}^K r_i \log_2 r_i$$

$$\text{On en déduit } H_{\text{canal réel}}(Y / X = a_i) \leq H_{\text{modèle}}(Y / X = a_i)$$

et puisque  $H_{\text{canal réel}}(Y) = H_{\text{modèle}}(Y)$ , on obtient finalement:

$$\boxed{\text{Capacité (canal réel)} \geq \text{Capacité (modèle)}}$$

En appliquant la formule  $C = \log_2 K - H_2(q) - (1-q)\log_2(K-1)$  établie à l'exercice 4, le calcul numérique (avec  $\pi = 1$ ) de la capacité du modèle conduit à la valeur;

$$C = 4 - (-0,85\log_2 0,85 - 0,15\log_2 0,15) - 0,15\log_2 15$$

$$C = 4 + 0,85\log_2 0,85 + 0,15\log_2 \frac{0,15}{15} = 2,8 \text{ Sh}$$

Cette capacité par utilisation concerne les mots constitués de 7 éléments binaires. Donc la

capacité par élément binaire est;  $C / \text{eb} = \frac{2,8}{7} = 0,4 \text{ Sh / eb}$

La capacité du canal binaire symétrique de probabilité d'erreur  $\pi = 0,1$  vaut;

$$C_{CBS} = 1 - H_2(0,1) = 0,531 \text{ Sh / eb}$$

## EXERCICE 2

1. La distance minimum étant 3, le code est 1-correcteur. Si on note  $n$  la longueur des mots et  $k$  le nombre d'éléments binaires de contrôle, on sait d'après le cours que l'on doit vérifier la relation:  $2^k = 1 + n$ .

Soit alors  $m = n - k$  le nombre d'éléments binaires d'information contenus dans un mot code. Comme les mots source d'origine ( $S_1$ ) comportent 3 éléments binaires d'information, l'extension d'ordre  $r$  concernera  $3r$  éléments binaires d'information. On a donc  $n = 3r + k$  et la relation à vérifier devient  $2^k = 3r + k + 1$ . En raisonnant pas à pas sur les valeurs de  $k$ , on obtient;

k	$3r = 2^k - (k + 1)$	caractère possible
1	$2 - 2 = 0$	impossible
2	$4 - 3 = 1$	impossible
3	$8 - 4 = 4$	impossible
4	$16 - 5 = 11$	impossible
5	$32 - 6 = 26$	impossible
6	$64 - 7 = 57$	possible $r = 19$

Il faut prendre l'extension d'ordre 19.

2. Les mots code comportent 57 éléments binaires d'information et 6 éléments binaires de contrôle, soit une longueur de 63 éléments binaires. Le code étant parfait, on sait que s'il se produit plus d'une erreur, alors il y aura erreur systématique sur le mot décodé.

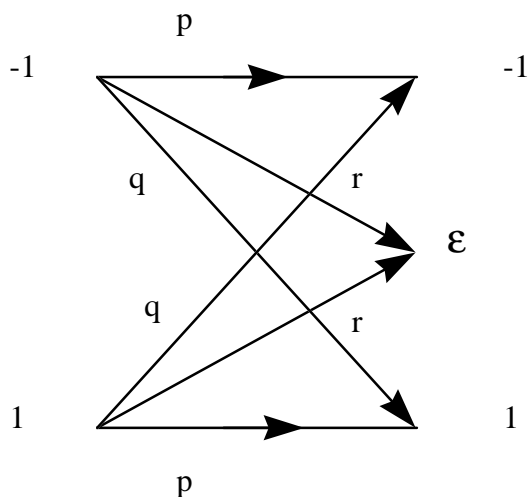
$$P\{\text{décodage correct}\} = P\{0 \text{ erreur sur les } 63 \text{ eb}\} + P\{1 \text{ erreur sur les } 63 \text{ eb}\}$$

$$P\{\text{décodage correct}\} = (1 - p)^{63} + 63p(1 - p)^{62}$$

En prenant  $p = 0,08$ , on obtient  $P\{\text{décodage correct}\} = 0,03389$

### EXERCICE 3

Rappelons les probabilités de transition du canal utilisé:



$$p = Q\left(\frac{A - \sqrt{E_b}}{\sigma}\right), \quad q = Q\left(\frac{A + \sqrt{E_b}}{\sigma}\right) \text{ et } r = 1 - p - q$$

$$A = \sqrt{E_b}, \quad \sigma = \sqrt{\frac{N_0}{2}} \text{ et } \sqrt{\frac{2E_b}{N_0}} = 2,236$$

Le code linéaire  $C(7, 4)$  a une distance minimum  $d_m = 3$ . En vertu d'une proposition énoncée dans le cours, ce code peut à la fois remplir  $\rho$  effacements et corriger  $t$  erreurs si;

$$\rho + 1 \leq d_m \tag{1}$$

$$\text{et } 2t \leq d_m - \rho - 1 \tag{2}$$

En remplaçant  $d_m$  par 3, (1) et (2) deviennent;

$$\rho \leq 3 - 1 = 2 \tag{1}$$

$$2t \leq 3 - 1 - \rho \tag{2}$$

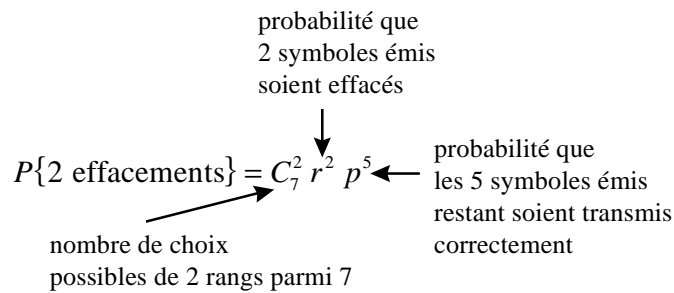
$\rho = 2 \Rightarrow t = 0$  le code peut remplir 2 effacements,

$\rho = 1 \Rightarrow t = 0$  le code peut remplir 1 effacement,

$\rho = 0 \Rightarrow t = 1$  le code peut corriger 1 erreur.

On est donc à même de calculer la probabilité pour qu'un mot code soit correctement restitué (on note  $D_C$  cet événement).

$$P\{D_C\} = P\{2 \text{ effacements}\} + P\{1 \text{ effacement}\} + P\{1 \text{ erreur}\}$$



De la même façon, on obtient:

$$P\{1 \text{ effacement}\} = C_7^1 r p^6$$

et  $P\{1 \text{ erreur}\} = C_7^1 q p^5$

soit 
$$P\{D_C\} = C_7^2 r^2 p^5 + C_7^1 r p^6 + C_7^1 q p^5$$

Application numérique

$$p = Q(0) = \frac{1}{2}, \quad q = Q\left(2\sqrt{\frac{2E_b}{N_0}}\right) = Q(2 \times 2,236) = Q(4,472)$$

La table de Gauss donne  $Q(4,4) = 54 \times 10^{-7}$   
 $Q(4,5) = 34 \times 10^{-7}$

Par interpolation linéaire, on obtient:

$$q = 54 \times 10^{-7} + \frac{(54 \times 10^{-7} - 34 \times 10^{-7}) \times 0,72}{1} = 6,84 \times 10^{-6}$$

$$r = 1 - [0,5 + 6,84 \times 10^{-6}] \approx 0,5$$

Finalement:

$$P\{D_c\} = \frac{7!}{5!2!} \left(\frac{1}{2}\right)^2 \left(\frac{1}{2}\right)^5 + 7 \times \frac{1}{2} \times \left(\frac{1}{2}\right)^6 + 7 \times 6,84 \times 10^{-6} \left(\frac{1}{2}\right)^5$$

soit  $\boxed{P\{D_c\} = 0,21875}$

#### EXERCICE 4

1. On constate que les deux premiers éléments binaires des mots code correspondent aux éléments binaires d'information. Donc le code est systématique.

Si on note  $\overline{a_1 a_2 c_1 c_2 c_3}$  les mots code ( $a_1 a_2$  représentent les éléments binaires d'information et  $c_1 c_2 c_3$  les éléments binaires de contrôle), on a;

$$c_1 = a_1 + a_2 \quad [2]$$

$$c_2 = a_1$$

$$c_3 = a_1 + a_2 \quad [2]$$

La matrice génératrice s'écrit:  $G = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \\ 1 & 0 \\ 1 & 1 \end{pmatrix}$

et la matrice de l'orthogonal du code est  $H = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$

On déduit de ce qui précède la matrice de contrôle:

$$H^T = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$

2. Pour construire la table de décodage, il faut recenser tous les syndromes possibles.  $H^T$  est une matrice  $3 \times 5$  et les séquences reçues possibles sont des matrices  $5 \times 1$ . Les produits  $H^T z$  sont de dimension  $3 \times 1$ . Ils sont au nombre de  $2^3 = 8$ .

Calculons les syndromes;

le syndrome de 00000 est 000

„ „ „ 00001 „ 001

„ „ „ 00010 „ 010

„ „ „ 00100 „ 100

„ „ „ 01000 „ 101

„ „ „ 10000 „ 111

Il y a donc 5 configurations (les cinq possibles) de une erreur qui peuvent être corrigées.

Intéressons-nous maintenant aux configurations de 2 erreurs.

Le syndrome de 00011 est 011 disponible

„ „ „ 00110 „ 110 disponible

„ „ „ 01100 „ 001 déjà utilisé

„ „ „ 11000 „ 010 déjà utilisé

„ „ „ 10100 „ 011 déjà utilisé

„ „ „ 10010 „ 101 déjà utilisé

„ „ „ 10001 „ 110 déjà utilisé

„ „ „ 01010 „ 111 déjà utilisé

„ „ „ 01001 „ 100 déjà utilisé

„ „ „ 00101 „ 111 déjà utilisé

Donc sur les  $C_5^2 = 10$  configurations de deux erreurs, deux peuvent être corrigées.

Les huit syndromes possibles ayant un antécédent, le code peut corriger toutes les configurations de une erreur et deux configurations de deux erreurs.

Table de décodage

syndromes	séquences z	nombre d'erreurs
000	00000	pas d'erreur
001	00001	1 erreur
010	00010	1 erreur
011	00011	2 erreurs
100	00100	1 erreur
101	01000	1 erreur
110	00110	é erreurs
111	10000	1 erreur

L'utilisation de la table de décodage se traduira par une décision correcte sur un mot code si aucune erreur ne s'est produite ou si une erreur s'est produite ou encore si l'une des deux configurations de deux erreurs apparaissant dans la table est survenue.

Si  $p$  désigne la probabilité d'erreur sur le canal bi aire symétrique, on obtient;

$$P\{\text{décision correcte}\} = (1-p)^5 + 5p(1-p)^4 + 2p^2(1-p)^3$$

## EXERCICE 5

1. Il faut vérifier que la condition du deuxième théorème de Shannon est satisfaite.

L'entropie de la source  $S$  par symbole est:  $H(S) = H_2(0,98) = 0,141$  Sh .

La capacité du canal par utilisation est  $C = 1 - H_2(0,05) = 0,713$  Sh .

Débit d'entropie de  $S$ :  $H' = 300 \times 10^3 \times 0,141 = 42300$  Sh / sec .

Capacité du canal par unité de temps:  $C' = 0,713 \times 280 \times 10^3 = 199640$  Sh / sec .

On vérifie  $H' < C'$ , on peut donc théoriquement transmettre le contenu de la source avec une probabilité d'erreur aussi petite que souhaitée.

2. La source étant sans mémoire, si  $L$  est l'ordre d'extension, on sait qu'il existe un code préfixe dont le nombre moyen d'éléments binaires  $\bar{n}$  utilisés pour représenter un élément binaire source vérifie;

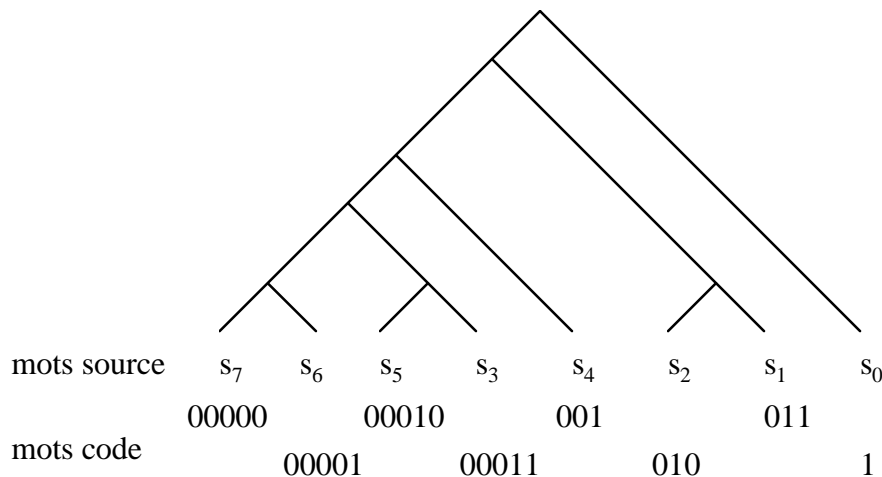
$$H(S) \leq \bar{n} < H(S) + \frac{1}{L}$$

Si on veut obtenir une réduction du débit initial d'au moins 50%, il ne faut pas que  $\bar{n}$  dépasse 0,5 puisqu'à un élément binaire source, il correspond (en moyenne)  $\bar{n}$  éléments binaires code. L doit donc vérifier:  $0,141 + \frac{1}{L} < 0,5$ , soit  $\frac{1}{L} < 0,359$ , c'est-à-dire  $L > 2,78$ . Il faut donc prendre l'extension d'ordre 3.

3. Calculons les probabilités des huit mots de l'extension d'ordre 3 de S.

désignation des mots	mots source	probabilités
$s_0$	000	$(0,98)^3 = 0,941$
$s_1$	001	$(0,98)^2 \times 0,02 = 0,019$
$s_2$	010	0,019
$s_3$	011	$0,98 \times (0,02)^2 = 3,92 \times 10^{-4}$
$s_4$	100	0,019
$s_5$	101	$3,92 \times 10^{-4}$
$s_6$	110	$3,92 \times 10^{-4}$
$s_7$	111	$8 \times 10^{-6}$

Représentons l'arbre de Huffman



La longueur moyenne d'un mot code (correspondant à un mot source de longueur 3) est;

$$\bar{n}_3 = 5 \times 1,184 \times 10^{-3} + 3 \times 3 \times 0,019 + 1 \times 0,941 \approx 1,118$$

A un élément binaire source, il correspond  $\frac{1,118}{3} = 0,3726$  élément binaire code.

La réduction du débit binaire est de l'ordre de 73%.

Le débit binaire  $D_s'$  de la nouvelle source est;

$$D_s' = 300 \times 10^3 \times 0,3726 = 111,78 \text{ kbits/sec.}$$

Le débit d'utilisation du canal étant de 280 kbits/sec, on a  $\frac{280}{111,78} \approx 2,5$ . Cela veut dire qu'il faut ajouter 1,5 élément binaire de contrôle à 1 élément binaire d'information, soit 3 éléments binaires de contrôle à 2 éléments binaires d'information.

4. On sait que si la distance minimum est  $d_m$ , le code peut corriger  $t = \text{ent}\left(\frac{d_m - 1}{2}\right)$  erreurs.

La plus petite valeur de  $d_m$  qui donne  $t = 1$  est 3.

5. On va donc construire un code de distance minimum 3. Le code étant systématique, la partie "haute" de la matrice génératrice est l'identité de dimension 2. Ensuite il faut ajouter deux "1" sur chaque colonne (sinon la distance minimum ne serait pas 3). Après des considérations identiques à celles développées dans l'exemple du cours, on obtient;

$$G = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 0 \\ 1 & 1 \\ 0 & 1 \end{pmatrix}$$

Les deux vecteurs de base ont un poids égal à 3 et leur somme est de poids 4.

6. En multipliant G par les quatre vecteurs d'information possibles, on obtient;

mots code	poids
00000	0
01011	3
10110	3
11101	4

7. D'après le cours, on déduit;

$$H = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \text{ soit } H^T = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

D'où la table de décodage;

syndromes	séquences z
000	00000
001	00001
010	00010
011	01000
100	00100
101	11000
110	10000
111	10001

Il reste deux valeurs de syndromes libres après avoir affecté un syndrome à toutes les configurations de une erreur. Donc deux configurations de deux erreurs peuvent être corrigées.

Par conséquent, il ne s'agit pas d'un code parfait, car on sait que pour un tel code t-correcteur, s'il y a plus de t erreurs, il y a erreur systématique sur le mot décodé.

8. Soit  $D_c = \{\text{décision correcte sur un mot code}\}$

$$P\{D_c\} = P\{\text{pas d'erreur} \cup 1 \text{ erreur} \cup 2 \text{ erreurs localisées}\}$$

$P\{D_c\} = (1-p)^5 + 5(1-p)^4 p + 2p^2(1-p)^3$  où p est la probabilité d'erreur par élément binaire sur le canal.

On a donc  $P\{\text{erreur sur mot décodé}\} = 1 - P\{D_c\}$ .

Si on transmettait directement sur le canal les mots de l'extension d'ordre 2 de S', on aurait;

$$P\{D_c\} = (1-p)^2, \text{ soit } P\{\text{erreur}\} = 1 - (1-p)^2.$$

Pour  $p = 5\%$ , l'application numérique conduit à;

probabilité d'erreur avec codage = 0,018

probabilité d'erreur sans codage = 0,097.