

EXERCICES DU CHAPITRE « INTRODUCTION A LA THEORIE DE L'INFORMATION »

Exercice 1 :

On rappelle la densité de probabilité d'une variable aléatoire Gaussienne :

$$g(x) = \left[\frac{1}{\sqrt{2\pi}\sigma_x} \exp\left(-\frac{(x-\mu_x)^2}{2\sigma_x^2}\right) \right]$$

Montrer que l'entropie différentielle de cette variable aléatoire Gaussienne vaut $\frac{\log_2(2\pi e\sigma_x^2)}{2}$

Solution Exercice 1

$$\begin{aligned} H(X_g) &= - \int g(x) \log_2 g(x) dx = - \int g(x) \log_2 \left[\frac{1}{\sqrt{2\pi}\sigma_x} \exp\left(-\frac{(x-\mu_x)^2}{2\sigma_x^2}\right) \right] dx \\ &= -\log_2 \left[\frac{1}{\sqrt{2\pi}\sigma_x} \right] \int g(x) dx + \frac{\log_2(e)}{2\sigma_x^2} \int (x-\mu_x)^2 g(x) dx \\ &\quad (\text{car } \log_2(t) = \ln(t)/\ln(2) = \ln(t)\log_2(e)) \\ &= -\log_2 \left[\frac{1}{\sqrt{2\pi}\sigma_x} \right] + \frac{\log_2(e)}{2\sigma_x^2} \sigma_x^2 = \frac{\log_2(2\pi e\sigma_x^2)}{2} \end{aligned}$$

Remarque : le résultat est indépendant de la moyenne μ_x de la Gaussienne et ne dépend que de sa variance. D'ailleurs pour toute v.a. $H(X+cste) = H(X)$ en faisant le changement de variable $y=x+cste$ dans la définition de l'entropie différentielle. On peut pour toute v.a changer sa moyenne en la soustrayant et avoir le même résultat d'entropie différentielle.

Exercice 2 :

Montrer que l'entropie différentielle d'une variable aléatoire de variance σ_x^2 fixée, prenant des valeurs réelles quelconques, est maximum pour la variable Gaussienne.

Solution Exercice 2 :

Démonstration : Soit X une variable aléatoire prenant des valeurs réelles quelconques.
D'après la positivité de la divergence de Kullback-Leibler, on a :

$$\int p(x) \log_2 \left(\frac{1}{q(x)} \right) dx \leq \int p(x) \log_2 \left(\frac{1}{p(x)} \right) dx$$

Pour une distribution $q(x)$ Gaussienne de variance σ_x^2 , on trouve donc :

$$\begin{aligned} H(X) &\leq \int p(x) \log_2 \left(\frac{1}{q(x)} \right) dx = \int p(x) \log_2 \left[\frac{1}{\sqrt{2\pi\sigma_x^2}} \exp \left(-\frac{(x-\mu_x)^2}{2\sigma_x^2} \right) \right] dx \\ &= -\log_2 \left[\frac{1}{\sqrt{2\pi\sigma_x^2}} \right] \int p(x) dx + \frac{\log_2(e)}{2\sigma_x^2} \int (x-\mu_x)^2 p(x) dx \\ &= -\log_2 \left[\frac{1}{\sqrt{2\pi\sigma_x^2}} \right] + \frac{\log_2(e)}{2\sigma_x^2} \sigma_x^2 = \frac{\log_2(2\pi e \sigma_x^2)}{2} \text{ CQFD.} \end{aligned}$$

Remarque dans cet exercice comme pour le précédent, peu importe la moyenne de la gaussienne : toutes les distrib gaussiennes de même variance ont la même entropie diff.

Exercice 3 :

Soit un alphabet source dont les probabilités des cinq symboles valent respectivement : $p(a)=1/2$, $p(b)=1/4$, $p(c)=1/8$, $p(d)=1/16=p(e)$.

Quelle est la longueur moyenne d'un codage de Huffman de cette source ?

Comparer cette longueur à l'entropie de la source.

Solution Exercice 3

Je trouve les mots codés :

- a: 0 (1 bit, probabilité 1/2)
- b: 10 (2 bit, probabilité 1/4)
- c: 110 (3 bit, probabilité 1/8)
- d: 1110 (4 bit, probabilité 1/16)
- e: 1111 (4 bit, probabilité 1/16)

La longueur moyenne est donc $L = 1 \cdot 1/2 + 2 \cdot 1/4 + 3 \cdot 1/8 + 4 \cdot 1/16 + 4 \cdot 1/16 = 30/16 = 1.875$ bit.

Il faut alors comparer cette longueur moyenne à l'entropie de la source :

$H = 0.5 \log_2 + 0.25 \log_2 (4) + 0.125 \log_2 (8) + 0.125 \log_2 (16) = 0.5 + 0.5 + 0.375 + 0.5 = 1.875$ bits. Le code de Huffman est parfait dans ce cas, on ne peut pas faire mieux (car les proba sont en $(1/2)^k$)

EXERCICES DU CHAPITRE « INTRODUCTION A LA THEORIE DE L'INFORMATION »

Exercice 1 : Capacité de différents canaux discrets

1. On considère un canal sans mémoire à N_X entrées et N_Y sorties possibles où la transition de l'entrée x_i vers la sortie y_j se produit avec une probabilité de transition p_{ij} . La matrice de transition P à $N_X \times N_Y$ éléments est la matrice dont l'élément sur la ligne i et la colonne j vaut p_{ij} . Un canal est dit complètement symétrique si toutes les lignes contiennent globalement le même jeu de probabilités $\{q_j\}_{j=1}^{N_Y}$ (i.e. toute ligne de P est une permutée des autres lignes) et toutes les colonnes contiennent globalement le même jeu de probabilités $\{r_i\}_{i=1}^{N_X}$ (i.e. toute colonne de P est une permutée des autres colonnes). Montrer que dans un tel cas, $H(Y|X)$ est indépendant des probabilités d'entrée $p(x_i)$ ($i=1 \dots N_X$). En déduire la capacité du canal en fonction de $\{q_j\}_{j=1}^{N_Y}$.

Correction 1-

$$H(Y|X) = \sum_{i=1}^{N_X} p(x_i) H(Y|X=x_i) \quad \text{où} \quad H(Y|X=x_i) = -\sum_{j=1}^{N_Y} p_{ij} \log(p_{ij})$$

mais ici $H(Y|X=x_i) = -\sum_{j=1}^{N_Y} q_j \log(q_j)$ indépendamment de l'indice i .

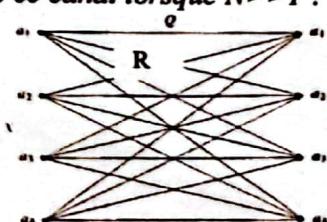
donc $H(Y|X) = -\sum_{i=1}^{N_X} p(x_i) \sum_{j=1}^{N_Y} q_j \log(q_j) = -\sum_{j=1}^{N_Y} q_j \log(q_j)$ est indépendant de $p(x_i)$.

Par conséquent maximiser $I(X,Y)=H(Y)-H(Y|X)$ par rapport à $p(x_i)$ revient à maximiser $H(Y)$. $H(Y)$ est max si les y_j sont équiprobables : $p(y_j)=1/N_Y$, ce qui se produit lorsque les $p(x_i)$ le sont également : $p(x_i)=1/N_X$.

On a alors $C = \max \{I(X,Y)\} = \log(N_Y) + \sum q_j \log(q_j)$.

2-

On considère un canal présentant des symétries, comme représenté à la figure suivante pour $N_X = N_Y = N = 4$ et on note $Q=1-p$ la probabilité de non transition, et R toute probabilité qu'un élément se transforme en un élément différent en sortie. Calculer la capacité de ce canal en fonction de N et de p . En déduire la capacité du Canal Binaire Symétrique. Que devient l'expression de la capacité de ce canal lorsque $N \gg 1$?



Correction 2-

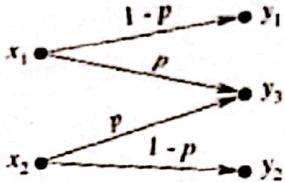
On est dans une configuration particulière traitée à la question 1.

On a $R=p/(N-1)$ et $Q=1-p$ ce qui permet d'obtenir $C=\log(N) + (1-p) \log(1-p) + p \log(p/(N-1))$.

Le CBS s'obtient pour $N=2$: $C_{CBS}=1-H_2(p)$: on retrouve le résultat du cours.

Lorsque $N \gg 1$, on a $C = (1-p) \log N - H_2(p) \rightarrow (1-p) \log N \gg C_{CBS}$

3-On considère à présent un canal sans mémoire à entrée binaire mais on introduit un seuil intermédiaire d'« effacement» lorsque le niveau reçu est perçu comme loin des niveaux binaires attendus. Cet effacement peut être utilisé, soit par une demande de retransmission à l'émetteur de ce qui est perçu comme effacé, soit parce que des



décodeurs, pour lesquels la capacité de correction d'un effacement est double de celle la capacité de correction d'erreur (sans indication d'emplacement), peuvent être mis en place. Ecrire la matrice de transition : le canal est-il totalement symétrique ? Calculer $H(Y/X)$. En déduire et interpréter le sens de la capacité du canal à effacement.

Solution 3-
3- La matrice de transition du canal $P = \begin{pmatrix} 1-p & 0 & p \\ 0 & 1-p & p \end{pmatrix}$ n'est pas totalement symétrique, mais elle l'est sur les lignes (proba p, 1-p, 0)

C'est pourquoi $H(Y|X) = -\sum_{i=1}^{N_x} p(x_i) \sum_{j=1}^{N_y} q_j \log(q_j) = -\sum_{j=1}^{N_y} q_j \log(q_j) = H_2(p)$ est indépendant de $p(x_i)$ donc maximiser $I(X,Y) = H(Y) - H(Y|X)$ par rapport à $p(x_i)$ revient à maximiser $H(Y)$.

En posant $p(y_i) = p_i$, $p(x_1) = \alpha$ (et donc $p(x_2) = 1 - \alpha$), on calcule :

$$\begin{aligned} -H(Y) &= p_1 \log(p_1) + p_2 \log(p_2) + p_3 \log(p_3), \text{ où } p_1 = \alpha(1-p), p_2 = (1-\alpha)(1-p), \text{ et } p_3 = p \\ &= \alpha(1-p) \log(\alpha(1-p)) + (1-\alpha)(1-p) \log((1-\alpha)(1-p)) + p \log(p) \\ &= (1-p) \{ \alpha(\log(\alpha) + \log(1-p)) + (1-\alpha)(\log(1-\alpha) + \log(1-p)) \} + p \log(p) \\ &= (1-p) \{ \alpha(\log(\alpha) + (1-\alpha)\log(1-\alpha) + \log(1-p)) \} + p \log(p) \\ &= (1-p) \{ \alpha(\log(\alpha) + (1-\alpha)\log(1-\alpha)) \} - H(p) \\ &= -(1-p) H(\alpha) - H(p) \quad (\text{E1}) \end{aligned}$$

est maximum en $dH(Y)/d\alpha = 0$ pour $\alpha = 0.5$: symboles d'entrée équiprobables.

(En effet, $dH(Y)/d\alpha = (1-p) d(\alpha(\log(\alpha) + (1-\alpha)\log(1-\alpha)))/d\alpha$ d'après (E1) et on reconnaît dans cette dernière expression l'entropie d'une source binaire de probabilité α : max pour $\alpha = 0.5$. Sinon, si on n'a pas reconnu l'entropie, on dérive et on trouve :

$$(1-p)(1.\log(\alpha) + 1 - \log(1-\alpha) - 1) = 0 \Leftrightarrow \log(\alpha/(1-\alpha)) = 0 \Leftrightarrow \alpha/(1-\alpha) = 1 : \alpha = \frac{1}{2}$$

On trouve alors en remplaçant α par $\frac{1}{2}$, $p(y_1) = p(y_2) = (1-p)/2$ et $p(y_3) = p$
d'où $H(Y) = (1-p) + H_2(p)$

et $C = H(Y) - H(Y|X) = (1-p)$: une fraction p des symboles est perdue.

Remarque : dans cet exercice, contrairement aux exercices déjà vus, le canal n'étant pas totalement symétrique, on ne peut avoir l'équi-répartition des y_i et il faut donc maximiser en dérivant.

Exercice 2 : A propos de la distance de Hamming

On considère des mots codés binaires de longueur n .

1-Montrer que la distance de Hamming constitue bien mathématiquement une distance.

Solution 1-

Directement de la définition de la distance de Hamming, on trouve que $d(\underline{x}, \underline{y}) \geq 0$ (et nulle ssi $\underline{x} = \underline{y}$), $d(\underline{x}, \underline{y}) = d(\underline{y}, \underline{x})$. Le dernier critère de l'inégalité triangulaire est un peu plus ardu mais vient également de la définition :

$$d(\underline{x}, \underline{z}) = \text{card } A_{\underline{x}\underline{z}} = \text{Card} \{ i \mid x_i \neq z_i \}.$$

Soit i_j un quelconque des indices de $A_{\underline{x}\underline{z}}$: $x_{i_j} \neq z_{i_j} \Rightarrow x_{i_j} \neq y_{i_j}$ ou $y_{i_j} \neq z_{i_j}$.

Donc i_j est dans $A_{\underline{x}\underline{y}}$ ou dans $A_{\underline{y}\underline{z}}$ et par conséquent dans $A_{\underline{x}\underline{y}} \cup A_{\underline{y}\underline{z}}$

Donc $A_{\underline{x}\underline{z}}$ est inclus dans $A_{\underline{x}\underline{y}} \cup A_{\underline{y}\underline{z}}$ et

$$\text{Card}(A_{\underline{x}\underline{z}}) \leq \text{Card}(A_{\underline{x}\underline{y}} \cup A_{\underline{y}\underline{z}}) \leq \text{Card}(A_{\underline{x}\underline{y}}) + \text{Card}(A_{\underline{y}\underline{z}})$$

Ceci démontre l'inégalité triangulaire des distances.

Soit un Canal Binaire Symétrique (résultant d'un bruit blanc additif de moyenne nulle) de probabilité de transition p ($p \leq 0.5$) sur lequel on transmet successivement n bits d'un mot de code \underline{c} . Soit \underline{r} le mot reçu de n bits, différent en t positions du mot de code émis à cause des transitions dues au canal.

2-Exprimer le plus simplement possible la solution au sens du maximum de vraisemblance en fonction de sa distance de Hamming avec le mot reçu.

Solution 2-

$$\hat{c}_{M'} = \max_{\underline{c}} (p(\underline{r} | \underline{c})) = \max_{\underline{c}} \left(\prod_{i=1}^n p(r_i | c_i) \right) = \max_{\underline{c}} ((1-p)^{n-d(\underline{r}, \underline{c})} p^{d(\underline{r}, \underline{c})})$$

En prenant le log de la quantité entre parenthèses on obtient toujours les maximum et donc $\hat{c}_{M'} = \max_{\underline{c}} (p(\underline{r} | \underline{c})) = \max_{\underline{c}} ((n-d(\underline{r}, \underline{c}) \log(1-p) + d(\underline{r}, \underline{c}) \log(p)) = \max_{\underline{c}} ((n \log(1-p) + d(\underline{r}, \underline{c}) \log(p/1-p))$

Comme $n \log(1-p)$ ne dépend pas de \underline{c} et que $(p/1-p) < 1$ on trouve bien que le max est atteint pour $d(\underline{r}, \underline{c})$ minimum : le mot de code qui diffère en le moins de positions du mot reçu est le mot le plus vraisemblable.

3-Déduire des questions précédentes le lien entre la capacité de correction d'un code et d_{\min} la plus petite distance de Hamming entre deux mots quelconques du code.

Solution 3-

D'après les questions précédentes, on peut garantir de corriger correctement dès lors que tout autre mot \underline{c}' est plus éloigné du mot reçu que le mot émis \underline{c} , et ceci est d'autant plus critique que \underline{c} et \underline{c}' sont proches (au pire d_{\min}).

De l'inégalité triangulaire que l'on a démontré, on a :

$$d(\underline{r}, \underline{c}) + d(\underline{r}, \underline{c}') \geq d(\underline{c}, \underline{c}') = d_{\min}$$

$$\text{donc } d(\underline{r}, \underline{c}') \geq d_{\min} - d(\underline{r}, \underline{c}) \quad (\text{E})$$

- Si d_{\min} est impair $d_{\min} = 2k+1$, on peut corriger $d(\underline{r}, \underline{c}) = t \leq k$ erreurs car d'après (E)

$$d(\underline{r}, \underline{c}') \geq 2k+1 - d(\underline{r}, \underline{c}) = 2k+1 - t \geq k+1 > d(\underline{r}, \underline{c})$$

La capacité de correction s'écrit $e = k = \text{Int}[((2k+1)-1)/2] = \text{Int}[(d_{\min} - 1)/2]$.

- Si d_{\min} est pair $d_{\min} = 2k$, on peut corriger $d(\underline{r}, \underline{c}) = t \leq k-1$ erreurs car d'après (E)

$$d(\underline{r}, \underline{c}') \geq 2k - t \geq k+1 \geq d(\underline{r}, \underline{c})$$

La capacité de correction s'écrit $e = k-1 = \text{Int}[((2k)-1)/2] = \text{Int}[(d_{\min} - 1)/2]$.

Et donc on a bien toujours $e = \text{Int}[(d_{\min} - 1)/2]$.

EXERCICES DU CHAPITRE

« LES CODES BLOCS LINEAIRES »

Exercice 1 :

$$G = \begin{pmatrix} 0011101 \\ 0100111 \\ 1001110 \end{pmatrix}$$

- Trouver une base dans laquelle G soit sous forme systématique.
- En déduire une matrice de contrôle du code. On désire uniquement corriger toutes les erreurs dont le poids est inférieur ou égal à la capacité de correction du code.
Proposer pour cela un tableau de déchiffrement et corriger les mots reçus: $\underline{r}_1=(1101001)$,
 $\underline{r}_2=(0000010)$.

Solution Exercice 1 :

- 1- Si g_1, g_2, g_3 , sont les vecteurs ligne de G , on obtient une matrice sous forme systématique dans la base g_3, g_2, g_1 :

$$\begin{pmatrix} 1001110 \\ 0100111 \\ 0011101 \end{pmatrix}$$

d'où la matrice de contrôle :

$$H = \begin{pmatrix} 1011000 \\ 1110100 \\ 1100010 \\ 0110001 \end{pmatrix}$$

Toutes combinaison de 3 colonnes ou moins de H est non nulle mais par exemple,
 $col1=col4+col5+col6 : d_{min}=4$
Ce code peut donc corriger 1 erreur, mais en détecter 3 (sur 7 symboles transmis).
Une façon alternative est de calculer les 8 mots du code $\underline{c}=\underline{a}G$:
(0000000),(0011101),(0100111),(0111010),
(1001110),(1010011),(1101001),(1110100) et de voir que $w_{min}=4$.
Il s'ensuit le tableau de déchiffrement :

reçu	mot de code
0000000	1001110 1110001 0111010 1101001 1010011 0011101 0100111
0000001	1001111 1110001 0111011 1101000 1010010 0011111 0100101
0000010	1001110 1110010 0111010 1101011 1010001 0011111 0100101
0000100	1001010 1110000 0111110 1101101 1010111 0011001 0100011
0001000	1000110 1111100 0111001 1100001 1011011 0010101 0101111
0010000	1001110 1100100 0111010 1111001 1000011 0011101 0110111
0100000	1101110 1010100 0011101 1000100 1110111 0111101 0000111
1000000	0000110 0110000 0111101 0010001 0010011 1011101 1100111
00000011	1001110 1110001 0111010 1101000 1010000 0011110 0100010
00000101	1001011 1110001 0111110 1101100 1010101 0011001 0100010
00001110	1000100 1110010 0111110 1100000 1011010 0010100 0101110
00011001	1000010 1111100 0111001 1100000 1011101 0010101 0101101
00110000	1101110 1010100 0011101 1000100 1110111 0111101 0000111
0110000	0000110 0110000 0111101 0010001 0010011 1011101 1100111
00011100	1000010 1111100 0111010 1101001 1011111 0010001 0101011
10110001	0000111 0110101 1111010 0101000 0010010 1011100 1100110

En résumé on a une correspondance entre leaders et syndrome suivante :

Leaders	Syndrome	Leaders	Syndrome	Leaders	Syndrome
(0000000)	(000)	(pour 0 transition)			
(0000001)	(0001)	(0000010)	(0010)	(0000100)	(0100)
(0001000)	(1000)	(0010000)	(1101)	(0100000)	(0111)
(1000000)	(1110)	(pour 1 transition sur 7)			
(0000011)	(0011)	(0000101)	(0101)	(0000110)	(0110)
(0001001)	(1001)	(0001010)	(1010)	(0110000)	(1011)
(0001100)	(1100)	(1000001)	(1111)	(parmi 2 transitions sur 7)	

Le mot reçu r_1 est un mot de code, on ne le corrige donc pas.

Le mot reçu r_2 possède un syndrome dont le leader est \underline{l}_2 et le décodeur délivre donc $\underline{0}$.

Exercice 2 :

Soit un code linéaire transformant des k -uplets binaires en mots codés de longueur n .

Montrer que la distance minimale (et donc la capacité de correction) est limitée par la "borne de Singleton": $d_{\min} \leq n-k+1$.

Solution Exercice 2 :

Tout code est équivalent à un code sous forme systématique.

Si on encode les k bits dont $k-1$ zéros $10\dots0\dots0$, on obtient sous forme systématique les n bits: $10\dots0.0xxxx$: qui a le premier bit et au plus $n-k$ bits de contrôle non nuls, soit au plus $n-k+1$ bits non nuls: $w_{\min} = d_{\min} \leq n-k+1$

Exercice 3 :

Montrer que tous les mots de poids inférieur ou égal à la capacité de correction e peuvent être pris comme leaders dans le tableau de déchiffrement.

Solution Exercice 3 :

Supposons que toutes les configurations de poids $\leq e$ ne puissent pas être prises comme leaders, i.e. ne sont pas sur des lignes distinctes. Donc il existe deux configurations d'erreurs \underline{e}_1 et \underline{e}_2 de poids inférieur ou égal à e sur la même ligne : il existe un mot de code \underline{c}_k tel que :

$$\begin{aligned} \underline{e}_1 &= \underline{e}_2 + \underline{c}_k \text{ soit } \underline{e}_1 - \underline{e}_2 = \underline{c}_k \\ \text{donc } w(\underline{c}_k) &\leq e+e = 2e \end{aligned} \quad (\text{E})$$

or $2e = 2$ Partie entière $[(d_{\min}-1)/2]$

- Si d_{\min} est pair : $d_{\min}=2k$ et donc $2e=2$ Partie entière $[k-1/2]=2(k-1)=d_{\min}-2$

d'après (E), $w(\underline{c}_k) \leq d_{\min}-2$ ce qui est impossible

- Si d_{\min} est impair : $d_{\min}=2k+1$ et donc $2e=2$ Partie entière $[2k/2]=2k=d_{\min}-1$

d'après (E), $w(\underline{c}_k) \leq d_{\min}-1$ ce qui est également impossible.

Par conséquent toutes les configurations de poids inférieur ou égal à e peuvent être prises comme leaders.

EXERCICES DU CHAPITRE « INTRODUCTION AUX CODES ALGEBRIQUES »

Soit $K_3[\alpha]$ l'ensemble des polynômes d'indéterminée α , à coefficients binaires et de degré inférieur ou égal à 3. On considère les opérations modulo le polynôme Π du paragraphe 4.3.

Exercice 1 :

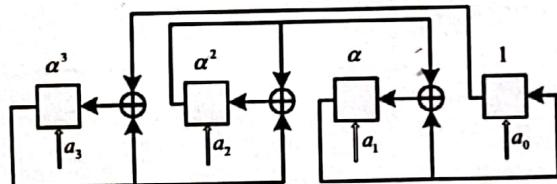
Réaliser un circuit multipliant dans $K_3[\alpha]$ par l'élément α^3 .

Corrigé :

$K_3[\alpha]$ est un ensemble à 16 éléments engendré par le polynôme irréductible $X^4 + X + 1$.

Donc :

$$\begin{aligned}
 a \cdot \alpha^3 &= (a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3) \cdot \alpha^3 \\
 &= a_0\alpha^3 + a_1\alpha^4 + a_2\alpha^5 + a_3\alpha^6 \\
 &= a_0\alpha^3 + a_1(\alpha + 1) + a_2\alpha(\alpha + 1) + a_3\alpha^2(\alpha + 1) \\
 &= a_0\alpha^3 + a_1\alpha + a_1 + a_2\alpha^2 + a_2\alpha + a_3\alpha^3 + a_3\alpha^2 \\
 &= a_1 + a_1\alpha + a_2\alpha + a_2\alpha^2 + a_3\alpha^2 + a_0\alpha^3 + a_3\alpha^3 \\
 &= a_1 + (a_1 + a_2)\alpha + (a_2 + a_3)\alpha^2 + (a_0 + a_3)\alpha^3
 \end{aligned}$$



Exercice 2 :

Le décodeur présenté au paragraphe 4.4 reçoit le mot : $r = (000001000010000)$. Effectuer à la main les opérations pour retrouver le mot émis le plus probable.

Corrigé :

$$r^T H = \begin{pmatrix} \alpha^5 + \alpha^{10} \\ 1+1 \end{pmatrix} = \begin{pmatrix} S_1 \\ S_2 \end{pmatrix}$$

$$I + J = S_1 = \alpha^5 + \alpha^{10} = \alpha + \alpha^2 + 1 + \alpha + \alpha^2 = 1$$

$$S_3 = 0$$

Le syndrome est non nul et S_3 est différent de S_1^3

On a :

$$U = \frac{S_1}{S_1} + S_1^2 = (\alpha^5 + \alpha^{10})^2 = 1$$

$$\begin{aligned}
 \Rightarrow 0 &= X^2 + S_1 X + \left(\frac{S_1}{S_1} + S_1^2 \right) \\
 &= X^2 + X + 1
 \end{aligned}$$

(Remarque : il ne s'agit pas d'une équation à coefficients entiers ou réels, mais bel et bien à coefficients dans un corps de Galois à 16 éléments où 1 (resp. 0) est l'élément neutre pour la multiplication (resp. addition)).

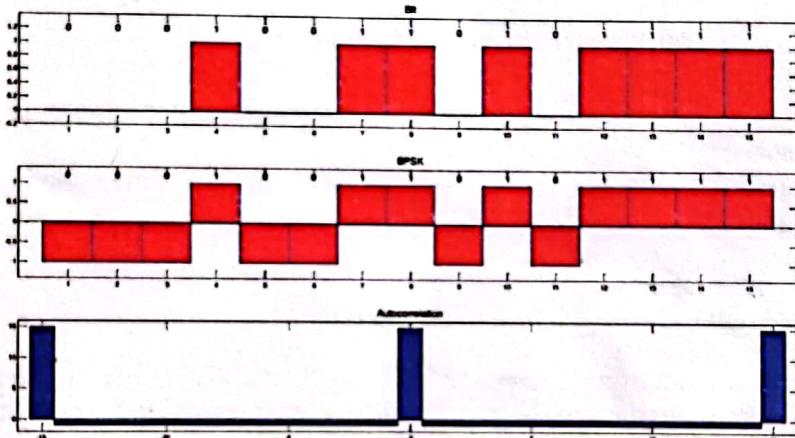
On cherche parmi les éléments du corps de Galois à 16 éléments les racines et on trouve : $X_1 = \alpha^5$ et $X_2 = \alpha^{10}$. Le mot corrigé est donc (0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0).

Exercice 3 :

On considère le circuit multipliant dans $K_3[a]$ par l'élément α du paragraphe 4.5.2. Le registre est initialement chargé par 1000 (1 sur le poids faible) et on s'intéresse aux contenus successifs de la bascule de gauche de ce registre (degré zéro). Quelle est la séquence de nombres binaires ainsi générée et quelle est sa période ?

Lorsque ce registre va moduler une modulation BPSK, dont la représentation des symboles en bande de base établit la correspondance entre éléments binaires et symboles réels transmis $0_b \rightarrow -1$ et $1_b \rightarrow +1$, donner la séquence de symboles correspondants en bande de base, puis représenter la fonction d'autocorrélation $\theta_{\text{BPSK}}(i)$ pour $|i| < 16$.

Corrigé :



L'autocorrélation de la séquence est, pour tout retard i , le produit scalaire entre la séquence et d'une version de i décalages (cycliques) de la séquence.

Il suffit donc de compter le nombre A de positions en accord (+1 avec +1 ou -1 avec -1) et celui de positions en désaccord (+1 avec -1 ou -1 avec +1) entre la séquence et sa décalée cyclique :

$$\theta(i) = A - D.$$

L'autocorrélation en forme de Dirac est typique du pseudo-aléatoire. Ce registre est très utilisé à la fois en général pour générer des nombres aléatoires ou du bruit, mais également en pratique pour tout ce qui est système à spectre étalé (TF d'un Dirac qui ressemble au spectre large bande du bruit) : systèmes GPS, Wifi, 3G, IoT...

000100110101111

EXERCICES DU CHAPITRE
« PRINCIPES ELEMENTAIRES SUR LES
CORPS DE GALOIS »

Exercice 1 :

Résoudre dans $\mathbf{G}[2^4] = K_3[\alpha]$:

$$\begin{aligned} \alpha x + \alpha^{11}y &= \alpha^8 & (1) \\ \alpha^3x + \alpha^6y &= \alpha^2 & (2) \end{aligned}$$

Corrigé :

$K_3[\alpha]$ est un corps à 16 éléments engendré par la relation $\alpha^4 = \alpha + 1$

$$\alpha X + \alpha^{11}Y = \alpha^8 \quad (1)$$

$$\alpha^3X + \alpha^6Y = \alpha^2 \quad (2)$$

On peut par exemple utiliser un pivot de Gauss.

En multipliant (2) par α^5 , on obtient $\alpha^8X + \alpha^{11}Y = \alpha^7$ (3). En éliminant Y entre (1) et (3), on a :

$$X = \frac{\alpha^8 + \alpha^7}{\alpha + \alpha^4} = \frac{1 + \alpha^2 + 1 + \alpha + \alpha^3}{\alpha + 1 + \alpha^2} = \frac{\alpha + \alpha^2 + \alpha^3}{1 + \alpha + \alpha^2} = \frac{\alpha^{11}}{\alpha^{10}} = \alpha$$

En remplaçant X par sa valeur α dans (1) ou (2),

$$\Rightarrow Y = \frac{\alpha^{10} + \alpha^2}{\alpha^{13} + \alpha^6} = \frac{1 + \alpha + \alpha^2 + \alpha^3}{1 + \alpha^2 + \alpha^3 + \alpha^2 + \alpha^3} = 1 + \alpha = \alpha^4$$

Toute autre méthode classique (par exemple la méthode des déterminants de Cramer) aurait fonctionné identiquement pour donner le même résultat. C'est l'intérêt de travailler dans un corps.

Exercice 2 :

Dans $\mathbf{G}(16) = K_3[\alpha]$, trouver pour l'élément $\beta = \alpha^6$, l'ordre et les conjugués distincts.

Corrigé :

L'ordre de β est le plus petit entier s tel que $\beta^s = 1$. Au plus, d'après le petit théorème de Fermat, s vaut 15 et de façon générale s est un diviseur de 15 : 1, 3, 5 ou 15.

Or $\beta^1 = \alpha^6$, $\beta^3 = \alpha^{18} = \alpha^3$, $\beta^5 = \alpha^{30} = 1$. L'ordre de β vaut donc 5.

Les conjugués de β sont par définition les puissances 2^i de β :

$$\beta = \alpha^6$$

$$\beta^2 = \alpha^{12}$$

$$\beta^4 = \alpha^{24} = \alpha^9$$

$$\beta^8 = \alpha^{48} = \underline{\alpha^1}$$

(Il ne peut y avoir plus de conjugués par conséquence du petit théorème de Fermat $\beta^{16} = \beta$).

Exercice 3 :

Soit $\mathbf{G}(16)$ construit à partir des relations + et x modulo $1+X+X^4$.

Pour chaque élément de $\mathbf{G}(16)^*$ trouver l'ordre, les conjugués et le polynôme minimal.

Corrigé :

$$\left\{ \alpha, \alpha^2 = \alpha^2, \alpha^3 = \alpha^4, \alpha^5 = \alpha^8 \right\}$$

$$\begin{aligned}
 & (X+\alpha)(X+\alpha^2)(X+\alpha^4)(X+\alpha^8) \\
 &= (X^2 + (\alpha + \alpha^2)X + \alpha^3)(X^2 + (\alpha^4 + \alpha^8)X + \alpha^{12}) \\
 &= (X^2 + \alpha^5 X + \alpha^3)(X^2 + (1 + \alpha + 1 + \alpha^2)X + \alpha^{12}) \\
 &= (X^2 + \alpha^5 X + \alpha^3)(X^2 + \alpha^3 X + \alpha^{12}) \\
 &= X^4 + (\alpha^5 + \alpha^3)X^3 + (\alpha^3 + \alpha^{12} + \alpha^{10})X^2 + (\alpha^{17} + \alpha^8)X + \alpha^{15} \\
 &= X^4 + (\alpha^3 + 1 + \alpha + \alpha^2 + \alpha^3 + 1 + \alpha + \alpha^2)X^2 + (\alpha^2 + 1 + \alpha^2)X + 1 \\
 &= X^4 + X + 1
 \end{aligned}$$

$$\left\{ \alpha^3, (\alpha^3)^2 = \alpha^6, (\alpha^3)^3 = \alpha^{12}, (\alpha^3)^4 = \alpha^9 \right\}$$

$$\begin{aligned}
 & (X+\alpha^3)(X+\alpha^6)(X+\alpha^9)(X+\alpha^{12}) \\
 &= (X^2 + (\alpha^3 + \alpha^6)X + \alpha^9)(X^2 + (\alpha^9 + \alpha^{12})X + \alpha^{21}) \\
 &= (X^2 + (\alpha^3 + \alpha^2 + \alpha^3)X + \alpha^9)(X^2 + (\alpha + \alpha^3 + 1 + \alpha + \alpha^2 + \alpha^3)X + \alpha^6) \\
 &= (X^2 + \alpha^2 X + \alpha^9)(X^2 + \alpha^8 X + \alpha^6) \\
 &= X^4 + (\alpha^2 + \alpha^6)X^3 + (\alpha^9 + \alpha^6 + \alpha^{10})X^2 + (\alpha^{17} + \alpha^8)X + \alpha^{15} \\
 &= X^4 + (\alpha^2 + 1 + \alpha^2)X^3 + (\alpha + \alpha^3 + \alpha^2 + \alpha^3 + 1 + \alpha + \alpha^2)X^2 + (\alpha^2 + \alpha^8)X + 1 \\
 &= X^4 + X^3 + X^2 + (\alpha^2 + 1 + \alpha^2)X + 1 \\
 &= X^4 + X^3 + X^2 + X + 1
 \end{aligned}$$

$$\left\{ \alpha^5, (\alpha^5)^2 = \alpha^{10} \right\}$$

$$\begin{aligned}
 & (X+\alpha^5)(X+\alpha^{10}) \\
 &= X^2 + (\alpha^5 + \alpha^{10})X + \alpha^{15} \\
 &= X^2 + (\alpha + \alpha^2 + 1 + \alpha + \alpha^2)X + 1 \\
 &= X^2 + X + 1
 \end{aligned}$$

$$\left\{ \alpha^7, (\alpha^7)^2 = \alpha^{14}, (\alpha^7)^3 = \alpha^{13}, (\alpha^7)^4 = \alpha^{11} \right\}$$

$$\begin{aligned}
 & (X+\alpha^7)(X+\alpha^{11})(X+\alpha^{13})(X+\alpha^{14}) \\
 &= (X^2 + (\alpha^7 + \alpha^{11})X + \alpha^{14})(X^2 + (\alpha^{13} + \alpha^{14})X + \alpha^{27}) \\
 &= (X^2 + (1 + \alpha + \alpha^3 + \alpha + \alpha^2 + \alpha^3)X + \alpha^3)(X^2 + (1 + \alpha^2 + \alpha^3 + 1 + \alpha^3)X + \alpha^{12}) \\
 &= (X^2 + (1 + \alpha^2)X + \alpha^3)(X^2 + \alpha^2 X + \alpha^{12}) \\
 &= (X^2 + \alpha^4 X + \alpha^3)(X^2 + \alpha^2 X + \alpha^{12}) \\
 &= X^4 + (\alpha^2 + \alpha^4)X^3 + (\alpha^{12} + \alpha^3 + \alpha^{10})X^2 + (\alpha^{20} + \alpha^8)X + \alpha^{15} \\
 &= X^4 + (\alpha^2 + 1 + \alpha^2)X^3 + (1 + \alpha + \alpha^2 + \alpha^3 + \alpha^3 + 1 + \alpha + \alpha^2)X^2 + (\alpha^3 + \alpha^8)X + 1 \\
 &= X^4 + X^3 + 1
 \end{aligned}$$

Elément		$\text{ord}(\alpha)$	Conjugués	Polynôme minimal
α	$(\alpha)^{15}=1$	15	{ $\alpha^1, \alpha^2, \alpha^4, \alpha^8$ }	$X^4 + X + 1$
α^2	$(\alpha^2)^{15}=1$	15	{ $\alpha^1, \alpha^2, \alpha^4, \alpha^8$ }	$X^4 + X + 1$
α^3	$(\alpha^3)^5=1$	5	{ $\alpha^3, \alpha^6, \alpha^{12}, \alpha^9$ }	$X^4 + X^3 + X^2 + X + 1$
α^4	$(\alpha^4)^{15}=1$	15	{ $\alpha^1, \alpha^2, \alpha^4, \alpha^8$ }	$X^4 + X + 1$
α^5	$(\alpha^5)^3=1$	3	{ α^5, α^{10} }	$X^2 + X + 1$
α^6	$(\alpha^6)^5=1$	5	{ $\alpha^3, \alpha^6, \alpha^{12}, \alpha^9$ }	$X^4 + X^3 + X^2 + X + 1$
α^7	$(\alpha^7)^{15}=1$	15	{ $\alpha^7, \alpha^{14}, \alpha^{13}, \alpha^{11}$ }	$X^4 + X^3 + 1$
α^8	$(\alpha^8)^{15}=1$	15	{ $\alpha^1, \alpha^2, \alpha^4, \alpha^8$ }	$X^4 + X + 1$
α^9	$(\alpha^9)^5=1$	5	{ $\alpha^3, \alpha^6, \alpha^{12}, \alpha^9$ }	$X^4 + X^3 + X^2 + X + 1$
α^{10}	$(\alpha^{10})^3=1$	3	{ α^5, α^{10} }	$X^2 + X + 1$
α^{11}	$(\alpha^{11})^{15}=1$	15	{ $\alpha^7, \alpha^{14}, \alpha^{13}, \alpha^{11}$ }	$X^4 + X^3 + 1$
α^{12}	$(\alpha^{12})^5=1$	5	{ $\alpha^3, \alpha^6, \alpha^{12}, \alpha^9$ }	$X^4 + X^3 + X^2 + X + 1$
α^{13}	$(\alpha^{13})^{15}=1$	15	{ $\alpha^7, \alpha^{14}, \alpha^{13}, \alpha^{11}$ }	$X^4 + X^3 + 1$
α^{14}	$(\alpha^{14})^{15}=1$	15	{ $\alpha^7, \alpha^{14}, \alpha^{13}, \alpha^{11}$ }	$X^4 + X^3 + 1$
$1 = \alpha^{15}$	$(\alpha^{15})^1=1$	1	{1}	$X + 1$

Remarque :

Le calcul des polynômes minimaux peut paraître fastidieux au premier abord. Il est important d'avoir mené un tel calcul à partir de la définition car on peut être amené à manipuler le calcul de polynômes avec des coefficients dans un corps fini, où aucune simplification n'est possible. Cependant, dans certains cas des simplifications sont possibles.

Tout d'abord, notons que le résultat est toujours un polynôme irréductible à coefficients binaires, ce qui fait un nombre fini de possibilités.

Ainsi pour le polynôme minimal de α^5 , le résultat est un polynôme du second degré $X^2 + aX + b$; mais $b=1$ sinon 0 est racine et le polynôme ne serait plus irréductible ; mais alors pour $X^2 + aX + 1$, $a=1$ sinon 1 serait racine.

Ici, on peut faciliter les calculs pour tous les polynômes minimaux.

Pour { $\alpha^1, \alpha^2, \alpha^4, \alpha^8$ }, on sait que $\alpha^4 + \alpha + 1 = 0$. Donc α est racine de $X^4 + X + 1$ et $X^4 + X + 1$ est le polynôme minimal de α .

Pour { $\alpha^3, \alpha^6, \alpha^{12}, \alpha^9$ }, on sait que $(\alpha^3)^5=1$. Donc α^3 est racine de $X^4 + X + 1 = (X-1)(X^3 + X^2 + X + 1)$ et il s'ensuit que α^3 est racine de $X^4 + X^3 + X^2 + X + 1$ qui est son polynôme minimal.

Pour { α^5, α^{10} }, $(X-\alpha^5)(X-\alpha^{10})=X^2 + X + 1$, sinon 0 ou 1 serait racine et le polynôme minimal de degré 2 ne serait pas irréductible.

Pour { $\alpha^7, \alpha^{14}, \alpha^{13}, \alpha^{11}$ }, on sait que $\alpha^{15}=1$, soit $\alpha^7=\alpha^{-8}$. Par conséquent, le polynôme minimal de α^7 est celui de α^8 (soit $X^4 + X + 1$) à coefficients retournés : $X^4 + X^3 + 1$. En effet si β est racine de $a_n X^n + a_{n-1} X^{n-1} + a_{n-2} X^{n-2} + \dots + a_0$, $a_n \beta^n + a_{n-1} \beta^{n-1} + a_{n-2} \beta^{n-2} + \dots + a_0 = 0$, en divisant

par β^n , on obtient $a_n + a_{n-1} \beta^{-1} + a_{n-2} \beta^{-2} + \dots + a_0 \beta^{-n} = 0$. Cela signifie bien que β^{-1} (l'inverse de β) est racine du polynôme à coefficients renversés du polynôme dont β est racine.

EXERCICES DU CHAPITRE « CODES CORRECTEURS ALGEBRIQUES »

Exercice 1 :

On note $C(n, k)$ l'ensemble des codes linéaires binaires de longueur n , fabriqués à partir de k -uplets.

1- Ecrire sous deux formes distinctes les éléments du corps de Galois engendré par le polynôme $X^5 + X^2 + 1$.

En déduire les caractéristiques (d_{min} , polynôme générateur, longueur avant et après codage) d'un code cyclique C de longueur $n=31$ qui puisse corriger deux erreurs.

2- Donner un schéma électronique permettant le codage, et un schéma électronique permettant la détection d'erreurs pour le code C .

3- On considère parmi les k -uplets à coder, ceux commençant par z bits égaux à 0 (z est un entier). Soit C' le sous ensemble du code C obtenu en ne considérant que les k -uplets précédents (à z zéros en tête). Montrer que l'on peut considérer C' comme un code de même capacité de détection que C avec C' élément de $C(n-z, k-z)$. Comment utiliser les circuits de la question 3-2 précédente pour coder et détecter les erreurs avec C' ?

Corrigé :

$$-1 - P(X) = X^5 + X^2 + 1 \Rightarrow \alpha^5 = \alpha^2 + 1 \text{ et } \alpha^{31} = 1$$

$$\begin{aligned} \alpha \cdot \alpha &= (a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 + a_4\alpha^4) \cdot \alpha \\ &= a_0\alpha + a_1\alpha^2 + a_2\alpha^3 + a_3\alpha^4 + a_4\alpha^5 \\ &= a_0\alpha + a_1\alpha^2 + a_2\alpha^3 + a_3\alpha^4 + a_4(\alpha^2 + 1) \\ &= a_4 + a_0\alpha + (a_1 + a_2)\alpha^2 + a_3\alpha^3 + a_4\alpha^4 \end{aligned}$$

5 coord. binaires	Représentation polynomiale	α^i	i
1 0 0 0 0	1	1	0
0 1 0 0 0	α	α	1
0 0 1 0 0	α^2	α^2	2
0 0 0 1 0	α^3	α^3	3
0 0 0 0 1	α^4	α^4	4
1 0 1 0 0	$1 + \alpha^2$	α^5	5
0 1 0 1 0	$\alpha + \alpha^3$	α^6	6
0 0 1 0 1	$\alpha^2 + \alpha^4$	α^7	7
1 0 1 1 0	$1 + \alpha^2 + \alpha^3$	α^8	8
0 1 0 1 1	$\alpha + \alpha^3 + \alpha^4$	α^9	9
1 0 0 0 1	$1 + \alpha^4$	α^{10}	10
1 1 1 0 0	$1 + \alpha + \alpha^2$	α^{11}	11
0 1 1 1 0	$\alpha + \alpha^2 + \alpha^3$	α^{12}	12
0 0 1 1 1	$\alpha^2 + \alpha^3 + \alpha^4$	α^{13}	13
1 0 1 1 1	$1 + \alpha^2 + \alpha^3 + \alpha^4$	α^{14}	14
1 1 1 1 1	$1 + \alpha + \alpha^2 + \alpha^3 + \alpha^4$	α^{15}	15
1 1 0 1 1	$1 + \alpha + \alpha^3 + \alpha^4$	α^{16}	16

1	1	0	0	1	$1+\alpha+\alpha^4$	α^{17}	17
1	1	0	0	0	$1+\alpha$	α^{18}	18
0	1	1	0	0	$\alpha+\alpha^2$	α^{19}	19
0	0	1	1	0	$\alpha^2+\alpha^3$	α^{20}	20
0	0	0	1	1	$\alpha^3+\alpha^4$	α^{21}	21
1	0	1	0	1	$1+\alpha^2+\alpha^4$	α^{22}	22
1	1	1	1	0	$1+\alpha+\alpha^2+\alpha^3$	α^{23}	23
0	1	1	1	1	$\alpha+\alpha^2+\alpha^3+\alpha^4$	α^{24}	24
1	0	0	1	1	$1+\alpha^3+\alpha^4$	α^{25}	25
1	1	1	0	1	$1+\alpha+\alpha^2+\alpha^4$	α^{26}	26
1	1	0	1	0	$1+\alpha+\alpha^3$	α^{27}	27
0	1	1	0	1	$\alpha+\alpha^2+\alpha^4$	α^{28}	28
1	0	0	1	0	$1+\alpha^3$	α^{29}	29
0	1	0	0	1	$\alpha+\alpha^4$	α^{30}	30

Pour corriger t=2 erreurs, il faut un polynôme ayant $2t=4$ puissances consécutives $\{\alpha^1, \alpha^2, \alpha^3, \alpha^4\}$. Il faut alors calculer le polynôme minimal de α^1 ($\alpha^2, \alpha^4, \dots$) et celui de α^3 . Pour calculer le polynôme minimal P_1 de α , (dont les conjugués sont les puissances 1, 2, 4, 8 et 16 de α), écrivons que α est racine de ce polynôme à coefficients binaires:

$$P_1(\alpha) = \alpha^5 + b\alpha^4 + c\alpha^3 + d\alpha^2 + e\alpha + 1$$

$$\begin{aligned} &= \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 1 \end{pmatrix} + b \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} + c \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} + d \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} + e \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \\ &= \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 1 \end{pmatrix} + \begin{pmatrix} b \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ c \\ 0 \\ 0 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \\ d \\ 0 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \\ 0 \\ e \\ 0 \end{pmatrix} \\ &= \begin{pmatrix} b \\ c \\ d \\ e \\ 0 \end{pmatrix} \\ &\Rightarrow \begin{pmatrix} b \\ c \\ d \\ e \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \Rightarrow P_1(X) = X^5 + X^2 + 1 \end{aligned}$$

On procède de même pour le polynôme minimal de α^3 .

$$P_3(X) = (X + \alpha^1)(X + \alpha^6)(X + \alpha^{12})(X + \alpha^{24})(X + \alpha^{17})$$

$$= X^5 + bX^4 + cX^3 + dX^2 + eX + 1$$

$$= X^5 + X^4 + X^3 + X^2 + 1$$

$$\begin{aligned}
 P_1(\alpha^3) &= \alpha^{15} + b\alpha^{12} + c\alpha^9 + d\alpha^6 + e\alpha^3 + 1 \\
 &= \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} + b \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \end{pmatrix} + c \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} + d \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \end{pmatrix} + e \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \\
 &= \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} + \begin{pmatrix} 0 \\ b \\ b \\ b \\ 0 \end{pmatrix} + \begin{pmatrix} c \\ c \\ c \\ 0 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ d \\ d \\ 0 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \\
 &= \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} + \begin{pmatrix} 1+c \\ 1+b+c+d+e \\ 1+b \\ 1+b+c+d \\ 0 \end{pmatrix} = 0 \\
 \Rightarrow \begin{pmatrix} b \\ c \\ d \\ e \end{pmatrix} &= \begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \end{pmatrix} \Rightarrow P_1(X) = X^5 + X^4 + X^3 + X^2 + 1
 \end{aligned}$$

⇒ Pour t=2, le polynôme générateur est :

$$\begin{aligned}
 g(X) &= P_1(X)P_2(X) \\
 &= (X^5 + X^4 + X^3 + X^2 + 1)(X^5 + X^4 + X^3 + X^2 + 1) \\
 &= X^{10} + X^9 + X^8 + X^7 + X^5 \\
 &\quad + X^7 + X^6 + X^5 + X^4 + X^2 \\
 &\quad + X^5 + X^4 + X^3 + X^2 + 1 \\
 &= X^{10} + X^9 + X^8 + X^6 + X^5 + X^3 + 1
 \end{aligned}$$

Ce code cyclique encode k=n- degré(g)=31-10=21 bits en n=31 après codage n=31 ; il corrige t=2 erreurs et donc possède une distance minimale supérieure ou égale à 5.

Remarques :

i/

31 étant un nombre premier (puissance de 2 première : nombre dit de Mersenne), tous les éléments (différents de l'élément neutre 1) ont pour ordre exactement 31 (et donc pas un de ses diviseurs). Par conséquent à part pour le polynôme minimal de α , on ne peut pas faire de simplifications comme celles pour le corps à 16 éléments ($15=5*3$ éléments non nuls) avec les ordres.

Pour α , on sait que par construction $\alpha^5 = \alpha^2 + 1$.

Donc α est racine de $P(X) = X^5 + X^2 + 1$ qui est bien le polynôme minimal calculé précédemment.

ii/

Le calcul des autres polynômes minimaux donne :

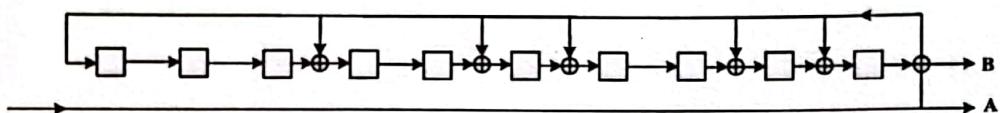
$$\begin{aligned}
 P_2(X) &= (X + \alpha^3)(X + \alpha^{10})(X + \alpha^{20})(X + \alpha^9)(X + \alpha^{11}) \\
 &= X^5 + X^4 + X^2 + X + 1
 \end{aligned}$$

$$\begin{aligned}
 P_3(X) &= (X + \alpha^7)(X + \alpha^{14})(X + \alpha^{21})(X + \alpha^{23})(X + \alpha^{19}) \\
 &= X^5 + X^4 + X^2 + X + 1
 \end{aligned}$$

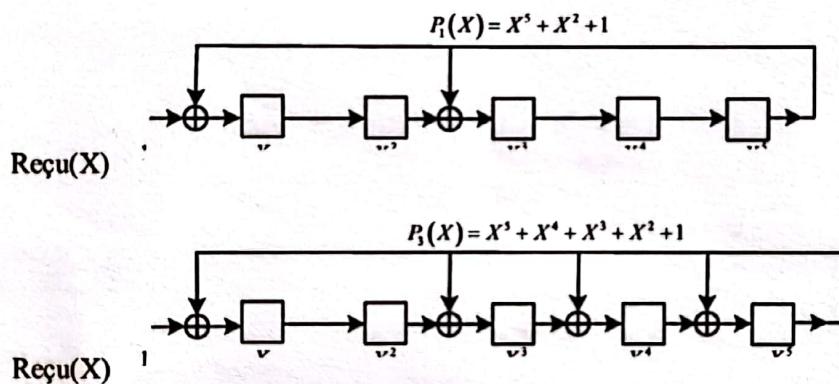
$$P_{11}(X) = (X + \alpha^{11})(X + \alpha^{22})(X + \alpha^{13})(X + \alpha^{26})(X + \alpha^{21}) \\ = X^5 + X^4 + X^3 + X + 1$$

$$P_{12}(X) = (X + \alpha^{19})(X + \alpha^{10})(X + \alpha^{20})(X + \alpha^{27})(X + \alpha^{23}) \\ = X^5 + X^3 + 1$$

-2- Le circuit pour l'encodage est un circuit diviseur par $g(X)$ en n -degré(g)=31-10=21 coups d'horloge, qui aux 21 bits d'information rajoute les 10 coefficients du reste :



Pour détecter les erreurs, il faut diviser le mot reçu par les polynômes minimaux du polynôme générateur et vérifier si tous les coefficients des restes sont nuls ou pas. Si un seul contenu de ces $2*5=10$ bascules est non nul le polynôme reçu n'est pas un multiple des polynômes minimaux et les erreurs sont détectées. Les deux circuits diviseurs (en $n=31$ coups d'horloge) sont :



-3-

En ne considérant que le sous-ensemble C' des mots ayant z bits à zéro en tête, on a toujours des mots de code, c'est-à-dire ayant une distance d_{\min} entre eux et donc au moins une capacité de correction identique t à celle du code.

On peut encore utiliser puisque les mots de C' sont des mots de code les circuits codeurs et décodeurs de la question précédente ; de plus, comme les z premiers bits sont à zéro, il ne se passe rien dans ses circuits pendant z coups d'horloge. Donc en faisant directement rentrer les $k-z$ bits non nuls dans le circuit encodeur (pendant $n-k-z$ coups d'horloge) et dans le circuit décodeur (pendant $n-z$ coups d'horloge), on obtiendra exactement le même résultat. Il est même donc alors inutile de transmettre ces z bits à zéro, connus et n'apportant aucune information réelle. Le code C' qui transforme $k'=k-z$ bits en $n'=n-z$ avec le codeur précédent et les décodeur avec le décodeur précédent est capable de corriger t erreurs. Nous en déduisons qu'il n'est pas nécessaire que la longueur d'un code soit contrainte à une longueur de la forme $n=2^k - 1$, mais que toute longueur n' devient possible (car $n'=2^k - 1 - z$ où z est un entier quelconque).