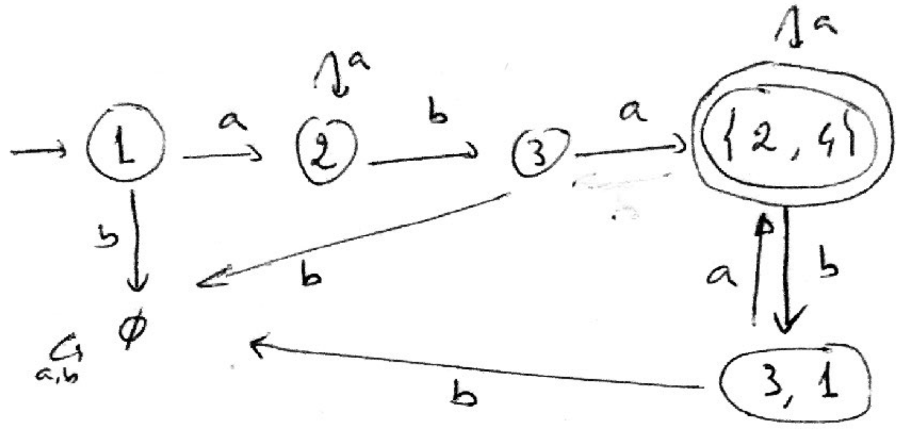
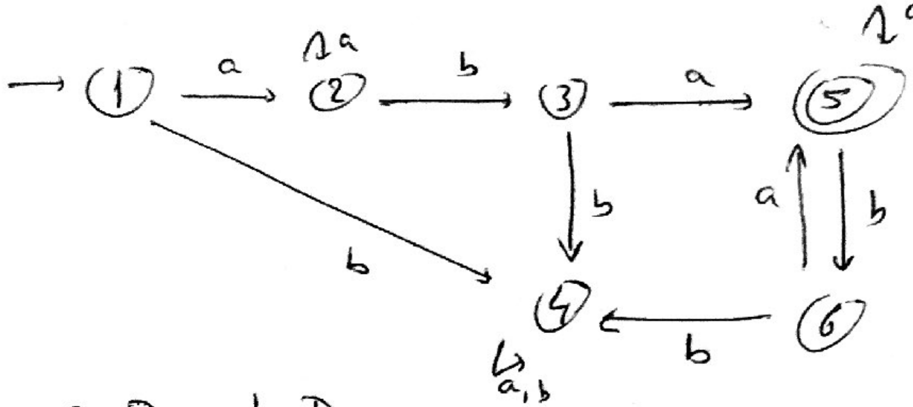
a) $\{ab, a^2b, aba\}$

b)



Ad :



c)

$$\begin{cases} D_1 = a D_2 + b D_4 \\ D_2 = a D_2 + b D_3 \\ D_3 = a D_5 + b D_4 \\ D_5 = \varepsilon + a D_5 + b D_6 \\ D_6 = a D_5 + b D_4 \\ \text{avec } D_4 = \emptyset \end{cases}$$

$D_5 = \varepsilon + (a + ba) D_5 \Rightarrow D_5 = (a+ba)^*$

$D_3 = a(a+ba)^*$; $D_2 = a D_2 + ba(a+ba)^*$

$D_2 = a^* ba(a+ba)^*$.

$L = D_1 = aD_2 = a^+ ba(a+ba)^*$.

d) $E = E_1 \cup E_2 = \{1, 2, 3, 4, 6\} \cup \{5\}$.

$a(1) = 2 \in E_1$ $\quad b(1) = 4 \in E_1$

$a(2) = 2 \in E_1$ $\quad b(2) = 3 \in E_1$

$a(4) = 4 \in E_1$ $\quad b(4) = 4 \in E_1$

$a(6) = 5 \in E_2$ $\quad b(6) = 4 \in E_1$

$a(3) = 5 \in E_2$ $\quad b(3) = 3 \in E_1$

$E_1 = E_{11} \cup E_{12} = \{1, 2, 4\} \cup \{3, 6\}.$

la procedure montre que $1 \nsim 4$

$E_1 = E_{111} \cup E_{112} \cup E_{12} = \{1, 4\} \cup \{2\} \cup \{3, 6\}.$

$\begin{cases} a(3) \in E_2 \\ a(6) \in E_2 \end{cases}$ mais $\begin{matrix} b(3) = 3 \in E_{12} \\ b(6) = 4 \in E_{111} \end{matrix}$ $\quad 3 \nsim 6.$

$E_{12} = E_{121} \cup E_{122} = \{3\} \cup \{6\}$

$E_1 = E_{111} \cup E_{112} \cup E_{121} \cup E_{122} = \{1, 4\} \cup \{2\} \cup \{3\} \cup \{6\}.$

aussi $a(1) = 2 \in E_{112}$ mais:
$a(4) = 4 \in E_{111}$

donc $1 \nsim 4$

$E_1 = \{1\} \cup \{4\} \cup \{2\} \cup \{3\} \cup \{6\}$

$E_2 \{1\} \cup \{4\} \cup \{2\} \cup \{3\} \cup \{6\} \cup \{5\}$

et $\mathcal{A}_d$ est minimal.

<u>Ex2</u>: Soit $\varphi : B^3 \longrightarrow B^6$

$b_1 b_2 b_3 \longrightarrow b_1 b_2 b_3 (b_2 \oplus b_3)(b_3 \oplus b_1)(b_1 \oplus b_2).$

a)

$\oplus$ étant commutative et associative, on vérifie facilement que $\varphi(b_1 b_2 b_3 \oplus a_1 a_2 a_3) = \varphi(b_1 b_2 b_3) \oplus \varphi(a_1 a_2 a_3).$

φ est linéaire ; $G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix}$

B^3	m_i mots de code
000	000000
100	100011
010	010101
001	001110
110	110110
101	101101
011	011011
111	111000

$d = \min w(m_i) = 3$; $n = 6$; $k = 3$; $r = 3$

le nb de bits que le code peut corriger est $t = \frac{d-1}{2} = 1$

$$C_6^0 + C_6^1 = 1 + 6 = 7 \neq 2^r = 8.$$

le code n'est pas parfait donc ce n'est pas un code de Hamming

c) $\Gamma(m_1) = \{ e \in B^6 / \sigma(e) = \sigma(m_1) \}$.

Soit H la matrice de contrôle

$${}^tH = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix};$$

le tableau des syndrômes est

B^3	
000	000000
100	000100
010	000010
001	000001
110	001000
101	010000
011	100000
111	100100

$\sigma(m_1) = 011$

$\sigma(m_2) = 111$

et $e_1 = 100000$ c'est l'unique vecteur erreur

de poids minimal tq $\sigma(e_1) = \sigma(m_1)$

on prend $\Gamma(m_1) = \{e_1\}$.

par contre : $e_2 = 100100$; $e_3 = 010010$; $e_4 = 001001$

sont des vecteurs erreurs de poids minimal / $\sigma(e_i) = \sigma(m_2)$.

on corrige m_1 par $c_1 = m_1 \oplus e_1 = 101110 \oplus 100000 = 001110$.

m_2 peut être corrigé pars

$c_2 = m_2 \oplus e_2$; $c_3 = m_2 \oplus e_3$; $c_4 = m_2 \oplus e_4$

$c_2 = 011011$; $c_3 = 101101$; $c_4 = 110110$.

) la proba de se tromper en corrigeant m_1 c'est de choisir

un des 7 mots de code autre que $c_1 = 001110$.

$$P = \sum_{\substack{i=1 \\ i \neq 4}}^{8} P(m_i) = p^3q^3 + p^4q^2 + p^4q^2 + p^3q^3 + p^3q^3 + p^3q^3 + p^4q^2$$

$$= 4p^3(1-p)^3 + 3p^4(1-p)^2.$$

Ex3 :

a) $x^3 . P(x) = G(x)\,Q(x) \oplus R(x)$

avec : $Q(x) = a_1 x^4 \oplus a_2 x^3 \oplus (a_1 \oplus a_3) x^2 + (a_1 \oplus a_2 \oplus a_4) x + (a_1 \oplus a_2 \oplus a_3 \oplus a_5)$

$R(x) = (a_2 + a_3 + a_4) x^2 \oplus (a_3 \oplus a_4 \oplus a_5) x + (a_1 \oplus a_2 \oplus a_3 \oplus a_5)$

$b_1 = a_2 \oplus a_3 \oplus a_4$; $b_2 = a_3 \oplus a_4 \oplus a_5$; $b_3 = a_1 \oplus a_2 \oplus a_3 \oplus a_5$

b) i) on a $\varphi(a_1 a_2 a_3 a_4 a_5) = a_1 a_2 a_3 a_4 a_5 b_1 b_2 b_3$

$G = (\varphi(e_i))$ avec $e_i = 0 \dots 0 \overset{i}{1} 0 \dots 0 \in B^8$

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

ii) la matrice engendrée par G est

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

$$\longrightarrow \begin{array}{c} \begin{pmatrix} 1&0&0&0&0&0&0&1 \\ 0&1&0&0&0&1&0&1 \\ 0&0&1&0&0&1&1&1 \\ 0&0&0&1&0&1&1&0 \\ 0&0&0&0&1&0&1&1 \end{pmatrix} \end{array} \begin{array}{l} l_1 \oplus l_3 \oplus l_4 \oplus l_5 \\ \to l_2 \oplus l_4 \oplus l_5 \\ l_3 \oplus l_5 \\ l_4 \\ l_5 \end{array}$$

c)

$$\begin{array}{l|l} X^8 \oplus 1 & X^3 \oplus X \oplus 1 \\ \cline{2-2} X^8 \oplus X^6 \oplus X^5 & X^5 \oplus X^3 \oplus X^2 \oplus X \\ \hline X^6 \oplus X^5 \oplus 1 & \\ X^6 \oplus X^4 \oplus X^3 & \\ \hline X^5 \oplus X^4 \oplus X^3 \oplus 1 & \\ X^5 \oplus X^3 \oplus X^2 & \\ \hline X^4 \oplus X^2 \oplus 1 & \\ X^4 \oplus X^2 \oplus X & \\ \hline 0 & \end{array}$$

$G(x)$ divise $X^n \oplus 1$ donc le code est cyclique

$P_m(x) = x^6 \oplus x^5 \oplus x^3 \oplus x^2 \oplus 1$

$\sigma(m)$ est le reste de la division de $P_m(x)$ par $g(x)$

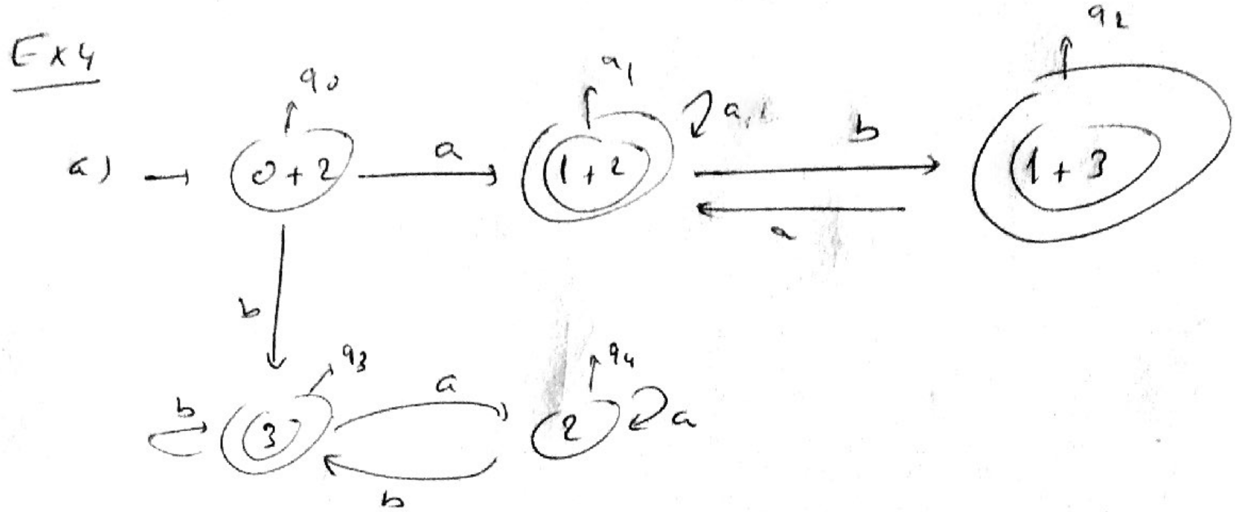
$P_m(x) = G(x)\,(x^3 \oplus x^2 \oplus x \oplus 1) \oplus x^2$

$R(x) = x^2$ d $\sigma(m) = 100 \neq 0$

donc m n'est pas un mot de code

Exo4

a)



b)

$q_0 \xrightarrow{b} q_3 \xrightarrow{a} q_4 \xrightarrow{b} q_3 \xrightarrow{b} q_3 \xrightarrow{a} q_2 \xrightarrow{a} q_2$, $m_1 \notin L(A)$.

$q_0 \xrightarrow{b} q_3 \xrightarrow{a} q_2 \xrightarrow{b} q_3 \xrightarrow{b} q_3 \xrightarrow{a} q_2 \xrightarrow{a} q_2 \xrightarrow{b} q_3 \xrightarrow{b} q_3 \xrightarrow{b} q_3$; $m_2 \in L(A)$

c)