Solut Final 2018

Ex 1

$n=7$, $k=4$, $r=3$; $H(3)$ est de Hamming, donc la matrice de contrôle couvre en colonnes les éléments de $B^r - \{000\}$:

$$H = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$ (3)

- $c' = 0101000$; $Hc' = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}$ = 3è colonne de H (1.5)

donc on a une erreur dans la 3è case et c' se corrige par 0111000. (1.5)

- $c' = 1110010$; $Hc' = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}$ = 2è colonne de H et (1.5)

c' se corrige par : 1010010 (1.5)

- $c' = 1100011 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$ = 6è colonne de H et c' se (1.5)

corrige par : 1100001 (1.5)

Ex2

$H = (v_1, v_2, v_3, v_4, v_5)$; $v_i \in M_{2,1}$ $(r=2)$ (1)

tq $c \cdot {}^tH = 0$ càd (1)

$$\left\{\begin{array}{l} v_1 + v_2 + v_5 = 0 \\ v_2 + v_3 + v_5 = 0 \\ v_3 + v_4 = 0 \end{array}\right. \quad \text{Soit} \quad \left\{\begin{array}{l} v_3 = v_4 \\ v_2 = v_4 + v_5 \\ v_1 = v_4 \end{array}\right.$$ (1)

posons $v_4 = \begin{pmatrix}1\\0\end{pmatrix}$; $v_5 = \begin{pmatrix}0\\1\end{pmatrix}$ (1) (2)

on a $v_1 = \begin{pmatrix}1\\0\end{pmatrix}$; $v_2 = \begin{pmatrix}1\\1\end{pmatrix}$; $v_3 = \begin{pmatrix}1\\0\end{pmatrix}$ (1)

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$ (1)

2) $C^{\perp} = [5,2]$ de matrice génératrice H (2)

B^2	mots de code
0 0	0 0 0 0 0
1 0	$(1\ 0) \cdot H = 1\ 1\ 1\ 1\ 0$
0 1	$(0\ 1) \cdot H = 0\ 1\ 0\ 0\ 1$
1 1	$(1\ 1) \cdot H = 1\ 0\ 1\ 1\ 1$

(4)

3)

info mot : $B^3 = \mathcal{E}$	polynôme associé	code	polynôme associé
0 0 0	0	0	$a = 0$
1 0 0	x^2	1 1 0 0 1	$b = x^4 + x^3 + 1$
0 1 0	x	0 1 1 0 1	$c = x^3 + x^2 + 1$
0 0 1	1	0 0 1 1 0	$d = x^2 + x$
1 1 0	$x^2 + x$	1 0 1 0 0	$e = x^4 + x^2$
1 0 1	$x^2 + 1$	1 1 1 1 1	$f = x^4 + x^3 + x^2 + x + 1$
0 1 1	$x + 1$	0 1 0 1 1	$g = x^3 + x + 1$
1 1 1	$x^2 + x + 1$	1 0 0 1 0	

(4 pts)

d est le polynôme de p.p degré $d^{\circ}(d) = 2 = r$.

(C) est polynomial si $a, b \dots g$ sont des multiples de d

or $b = x^2 \cdot d + 1$ donc n'est pas multiple de d et par suite le code n'est pas polynomial. (2 pts)

Ex3 $g(x) = x^3 + x^2 + x + 1$

1) $n = 5$, $r = 3$. $k = 2$: bits de données
$r = 3$: bits de contrôle (2)

2) $x^5 + 1 = g(x)(x^2 + x) + x$ (2)
$g(x)$ ne divise pas x^5+1 donc (C) n'est pas cyclique (1)

3) $P_m(x) = x^4 + x^3 + x^2 + x = x \cdot g(x)$ donc $g(x)$ (2)
divise $P_m(x)$ et $P_m(x)$ est un polynôme de code
et m est un mot de code (2)

4) $\alpha = 11 \in B^k = B^2$.
Soit m le code de α, $m \in B^n = B^5$.
or $P_m(x) = P_\alpha(x) \oplus R(x)$. (2)
$P_\alpha(x) = x^4 \oplus x^3$; $R(x)$ est le reste de la division de (2)
$P_\alpha(x)$ par $g(x)$:

$P_\alpha(x) = g(x) \cdot x + (x^2 + x)$ (2)

$R(x) = x^2 + x$

$P_m(x) = x^4 + x^3 + x^2 + x$ (2)

$m = 11110$. (2)

5) $P_{m'}(x) = x^4 + x^3 + x + 1$
$= (x^3 + x^2 + x + 1)(x) + x^2 + 1$ (2)

$P_{\sigma(m')}(x) = x^2 + 1 \Rightarrow \sigma(m') = 101 \neq 000$ donc m' n'est pas un mot de code (2)
(2)

Ex4

1) $\{ab, a^2b, aba\}$ 3

2)

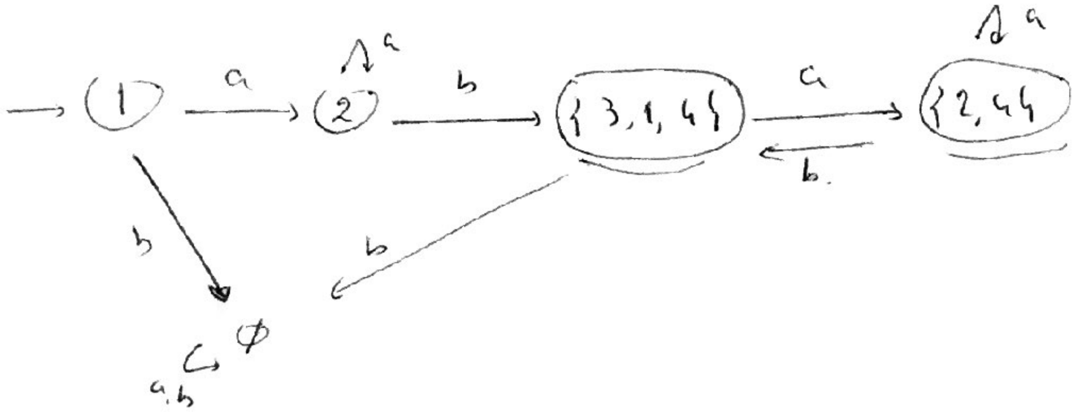
δ	1	2	3	4
a	2	2	–	4
b	–	3	–	–
ε	–	–	1, 4	–

2

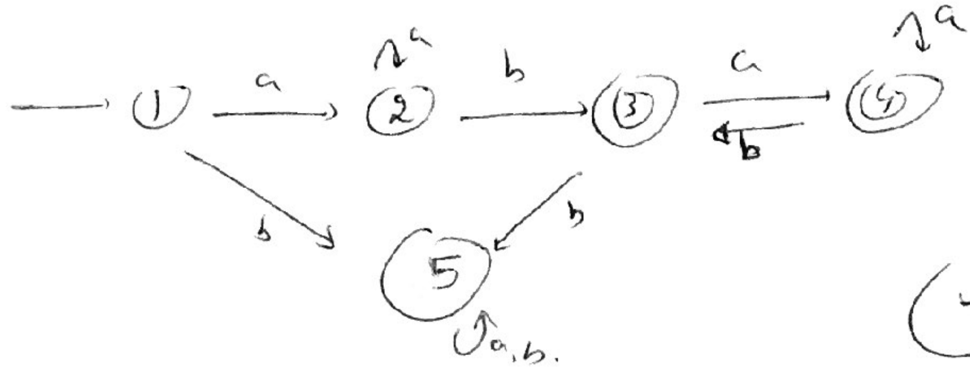
3)

δ	1	2	{3, 1, 4}	2, 4
a	2	2	2, 4	2, 4
b	$\emptyset$	{3, 1, 4}	$\emptyset$	{3, 1, 4}

4



(B):



5

4) $\partial_5 = \emptyset$.

$$\begin{cases} \partial_1 = a\,\partial_2 \\ \partial_2 = a\,\partial_2 + b\,\partial_3 \\ \partial_3 = a\,\partial_4 + \varepsilon \\ \partial_4 = b\,\partial_3 + a + a\,\partial_4 = b\,\partial_3 + \partial_3 = (b+\varepsilon)\,\partial_3 \end{cases}$$

4

$$\partial_3 = a(b+\varepsilon)\,\partial_3 + \varepsilon$$

$$\partial_3 = (a(b+\varepsilon))^* = (ab+a)^*$$

$$\partial_2 = a\,\partial_2 + b(ab+a)^*$$

$$\partial_2 = a^* b(ab+a)^*$$

$$\partial_1 = a^+ b(ab+a)^*$$

$$L = a^+ b(ab+a)^*.$$

4

5) les langages de départ sont tous différents donc on n'a pas d'états équivalents et par suite 3 est minimal.

3

5 (6)

1) $AB = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 1 \\ 0 & 2 & 0 \\ 1 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 2 & 0 \\ 2 & 2 & 2 \\ 0 & 2 & 0 \end{pmatrix} = 2A.$ (3)

$BA = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 2 & 0 \\ 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 2 & 0 \\ 2 & 2 & 2 \\ 0 & 2 & 0 \end{pmatrix} = 2A.$ (3)

$A^2 = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 3 & 1 \\ 1 & 1 & 1 \end{pmatrix} = A + B$ (3)

2) $n=1$: $(2+1)A + (1-1)B = 3A = 3.A^1$ (2)

la pté est vraie pour $n=1$; supposons que

$3A^n = [2^n - (-1)^n]A + [2^{n-1} + (-1)^n]B$ (2)

$3A^{n+1} = 3.A^n.A = [2^n-(-1)^n]A^2 + [2^{n-1}+(-1)^n]BA$

$= [2^n-(-1)^n](A+B) + [2^{n-1}+(-1)^n](2A)$

$= [2^n-(-1)^n + 2^n + 2(-1)^n]A + [2^n-(-1)^n]B$

$= [2^{n+1} + (-1)^n]A + [2^n + (-1)^{n+1}]B$

$= [2^{n+1} - (-1)^{n+1}]A + [2^n + (-1)^{n+1}]B$ cqfm.

(4)

7

$|C| = -1 \neq 0$ donc C est inversible et 3

$C^{-1} = \frac{1}{|C|}\, {}^t\mathrm{Cof}(C) = \frac{1}{|C|}\, \mathrm{Cof}(C)$ car C est sym 2

$$C^{-1} = -\begin{pmatrix} -1 & 0 & 1 \\ 0 & 0 & -1 \\ 1 & -1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & -1 \\ 0 & 0 & 1 \\ -1 & 1 & 0 \end{pmatrix}.$$ 2