Feuille d'exercices n° 3. Codes correcteurs d'erreurs

Exercice 1. — On considère les codes binaires suivants

$$C_1 = \{0000, 1100, 1010, 1001, 0110, 0101, 0011, 1111\} \subset (\mathbb{F}_2)^4 \quad (1)$$
$$C_2 = \{10000, 01010, 00001\} \subset (\mathbb{F}_2)^5 \quad (2)$$
$$C_3 = \{000000, 101010, 010101\} \subset (\mathbb{F}_2)^6. \quad (3)$$

Dire dans chaque cas si le code est linéaire ainsi que le nombre d'erreurs qu'il peut détecter et corriger.

Exercice 2. — 1. Construire un code binaire de 4 mots de longueur 3 et de distance minimum 2.

2. Montrer qu'un code binaire C de longueur 3 et de distance minimum 2 possède au plus 4 mots.

Exercice 3. — Soit n un entier positif. Montrer qu'une condition nécessaire pour qu'il existe un code linéaire binaire parfait 1-correcteur de longueur n est que l'entier n soit de la forme $n = 2^r - 1$, où r est un entier positif.

Exercice 4. — Soit C un code linéaire binaire.

1. Montrer que si C est de longueur 17 et de dimension 7, il ne corrige pas plus d'une erreur.
2. Montrer que si C est de longueur 10 et de distance minimum 3, alors $\#C \leq 93$.

Exercice 5. — Soit C le code linéaire sur $\mathbb{F}_3$ de matrice génératrice

$$G = \begin{pmatrix} 2 & 1 & 0 & 1 & 2 \\ 0 & 2 & 1 & 1 & 1 \end{pmatrix}.$$

1. Montrer que C est systématique et en donner une matrice génératrice normalisée G'.
2. Encoder le message (12) avec G, puis avec G'.
3. Construire une matrice de contrôle de C et calculer sa distance minimale.
   Le code est-il MDS (Maximum Distance Separable) ?
4. On reçoit le message 11102 codé par G. Quel est le message d'origine ? Le mot 12121 est-il un mot de code ? Le décoder sachant qu'il a été encodé par G.

Exercice 6. — Soit C le code linéaire sur $\mathbb{F}_5$ de matrice génératrice

$$G = \begin{pmatrix} 3 & 4 & 1 & 0 \\ 0 & 3 & 4 & 1 \end{pmatrix}.$$

1. Donner le nombre de mots de C.
2. Le code est-il systématique ?
3. Déterminer une matrice de contrôle de C.
4. Calculer la capacité de correction t de C. Le code est-il MDS ?
5. Donner la table de contrôle contenant tous les vecteurs erreurs possibles de poids $\leq t$.
6. Décoder quand c'est possible les mots 3001, 1101 et 2311.

Exercice 7. — Soit C le code de Hamming binaire de longueur 7.

1. Déterminer une matrice génératrice normalisée de C à l'aide de la méthode du pivot de Gauss.
2. En déduire une matrice de contrôle de C.
3. Décoder quand c'est possible les mots 1111111, 1101011, 0110110 et 1111010.

Exercice 8. — Soit C le code linéaire ternaire de matrice génératrice

$$G = \begin{pmatrix} 1 & 0 & 0 & 2 & 2 & 1 \\ 2 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 2 & 0 \\ 0 & 1 & 1 & 2 & 0 & 1 \end{pmatrix}.$$

Montrer que C est systématique, en donner une matrice de contrôle. Quelle est sa distance minimale ?

Exercice 9. — Soit C le code sur $\mathbb{F}_5$ de matrice génératrice G avec

$$G = \begin{pmatrix} 1 & 2 & 3 & 4 & 0 & 4 \\ 1 & 1 & 1 & 1 & 4 & 0 \end{pmatrix}; \quad G' = \begin{pmatrix} 1 & 0 & 4 & 3 & 3 & 1 \\ 0 & 1 & 2 & 3 & 1 & 4 \end{pmatrix}.$$

1. Montrer que G' est une matrice normalisée génératrice du même code C.
2. En déduire une matrice de contrôle.
3. Quelle est la capacité de correction de C ?
4. Décoder les mots 432100 et 411141.

Exercice 10. — Soit C le code binaire linéaire de matrice génératrice

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

1. Le code est-il systématique ?
2. Déterminer une matrice de contrôle et la capacité de correction de C.
3. Le code est-il MDS ?
4. Décoder si possible les mots 111110 et 111111.

Exercice 11. — Soit C le code binaire linéaire de matrice génératrice

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

1. Montrer que ce code est systématique. Pourquoi ?
2. Déterminer une matrice de contrôle et la capacité de correction de C.
3. Décoder si possible le mot 110110.

Exercice 12. — Soit p un nombre premier, on considère le code C_p sur $\mathbb{F}_p$, de matrice génératrice

$$G = \begin{pmatrix} 1 & 0 & 0 & 1 & 2 & 2 \\ 0 & 1 & 0 & 0 & 2 & 2 \\ 0 & 0 & 1 & 0 & 1 & 3 \\ 0 & 0 & 0 & 2 & 3 & 2 \end{pmatrix}.$$

1. Quelles sont les longueur et dimension de C_p ? Montrer que $d \leq 3$.
2. Pour $p = 2$, 3, 5, trouver des matrices de contrôle pour C_p et déterminer les distances minimales.
3. Pour $p = 5$, décoder le mot 111234.

Codes cycliques

Exercice 13. — Montrer que le polynôme $X^5 + X^4 + X + 1$ engendre un code cyclique binaire de longueur $n = 8$. En donner une matrice génératrice et une matrice de contrôle.

Exercice 14. — Combien existe-t-il de codes cycliques binaires de longueur 4 ? Donner pour chacun une matrice génératrice et une matrice de contrôle.

Exercice 15. — Montrer que si un code est cyclique, son mot minimal $\widetilde{m} = a_0\, a_1 \dots a_{r-1}\, 1\, 0 \dots 0$ vérifie $a_0 \neq 0$.

Exercice 16. — Le code binaire de matrice génératrice

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

est-il cyclique ?

Exercice 17. — Soit m un mot non nul de $\mathbb{F}_q^n$ et soit C_m le sous-espace vectoriel de $\mathbb{F}_q^n$ engendré par la famille $\{\sigma^i(m) \,|\, i = 0, 1, \dots, n-1\}$.

1. Montrer que
   (a) C_m est un code cyclique de longueur n.
   (b) C_m est le plus petit code cyclique de longueur n sur $\mathbb{F}_q$ contenant le mot m.
   (c) Le polynôme générateur du code C_m est le pgcd des polynômes $X^n - 1$ et $m(X)$.
2. Déterminer le polynôme générateur de C_m lorsque $q = 3$, $n = 9$ et $m = 022011000$.

Exercice 18. — Soit C un code cyclique de longueur n sur $\mathbb{F}_q$, et soit h son polynôme de contrôle. Montrer que pour tout mot $m \in \mathbb{F}_q^n$, on a $(m \in C)$ si et seulement si le polynôme $m(X)h(X)$ est divisible par le polynôme $X^n - 1$.

Exercice 19. — Code binaire de Hamming de longueur $2^r - 1$.
Montrer que le code binaire de Hamming de longueur $2^r - 1$ défini en cours est un code cyclique parfait de dimension $k = 2^s - 1 - s$, de distance minimum $d = 3$ et de polynôme générateur

$$g = \prod_{i=0}^{s-1} (X - \alpha^{2^i}) \in \mathbb{F}_2[X].$$

Exercice 20. — Exemple d'un code de Reed-Solomon.
Soit $\mathbb{F}_8 = \mathbb{F}_2[X]/\langle X^3 + X + 1\rangle$ et soit $\alpha = \overline{X}$.

1. Montrer que α est un élément primitif de $\mathbb{F}_8$.
2. Écrire la table des logarithmes de base α.
3. Soient $g \in \mathbb{F}_8[X]$ le diviseur unitaire de $(X^7 - 1)$ défini par

   $$g = (X - \alpha)(X - \alpha^2).$$

   Montrer que $g = X^2 + \alpha^4 X + \alpha^3$.
4. Écrire une matrice génératrice du code (de Reed-Solomon) C de longueur 7 engendré par g.
5. Déterminer le polynôme de contrôle et une matrice de contrôle de C.
6. En déduire que C est MDS.
7. Corriger le mot reçu $\alpha^3\alpha^2\alpha\alpha^4\alpha\alpha^4 1$.

Exercice 21. — Examen juin 2004

1. Montrer, sans effectuer de division euclidienne, que dans $\mathbb{F}_3[X]$, le polynôme $g = (X-1)^5$ divise le polynôme $X^9 - 1$.
2. Soit C le code cyclique de longueur 9 sur $\mathbb{F}_3$, engendré par le polynôme g.
   (a) Quelle est la dimension de C ?
   (b) Quel est le nombre de mots de C ?
3. Développer le polynôme g dans $\mathbb{F}_3[X]$, en détaillant et justifiant les calculs.
4. Pourquoi la matrice
$$G = \begin{pmatrix} 2 & 2 & 2 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 2 & 2 & 2 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 2 & 2 & 2 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 2 & 2 & 2 & 1 & 1 & 1 \end{pmatrix}$$
est-elle une matrice génératrice du code C ?
5. Montrer que C contient un mot de poids 3.
6. Montrer que le polynôme de contrôle de C est le polynôme
$$h = X^4 + 2X^3 + 2X + 1.$$
7. Déterminer une matrice de contrôle de C.
8. Déterminer la distance minimum du code C et le nombre d'erreurs que C peut corriger.
9. Le mot $m = 121102210$ est reçu.
   (a) Sous l'hypothèse d'au plus une erreur, quel est le mot de code émis ?
   (b) Quel est le message envoyé, sachant qu'il est encodé par la matrice G ?

Corrigés

1. — C_1 est linéaire de dimension 3, il vérifie $d = 2$, il détecte une erreur.
C_2 n'est pas linéaire car il ne contient pas le mot nul, il vérifie $d = 2$, il détecte une erreur.
C_3 n'est pas linéaire, il vérifie $d = 3$, il corrige $\left\lfloor \frac{d-1}{2} \right\rfloor = 1$ erreur.

2. — 1. $C_1 = \{111, 001, 100, 010\}$ ou $C_2 = \{000, 110, 011, 101\}$.

2. Tout mot de ${\mathbb{F}_2}^3$ est à la distance 1 de 111 ou 000, le code C ne peut donc contenir 111 et 000. On en déduit $C = C_1$ ou C_2 puisque $C_1 \cup C_2 = (\mathbb{F}_2)^3$ et que tout mot de C_i est à la distance 1 d'un mot de C_j.

3. — Soit C un code linéaire binaire de longueur n et de dimension k. On sait que $\#C = 2^k$ et que si B est une boule de Hamming de rayon 1, on a $\#B = 1 + n$. Pour que C soit parfait, il est nécessaire qu'il existe un entier positif q tel que $q(1 + n) = 2^k$. On en déduit que $n + 1$ est une puissance de 2.

4. — 1. $2^7 = 128$ et $1 + 17 < 128 < 1 + 17 + \mathcal{C}_2^{17} = 154$.

2. $2^{10} = 1024 \geq (1 + \mathcal{C}_1^{10})(\#C) = 11(\#C)$ d'où $\#C \leq \left\lfloor \frac{1024}{11} \right\rfloor = 93$.

5. — 1. Par la méthode du pivot de Gauss sur les lignes, on obtient $G' = \begin{pmatrix} 1 & 0 & 2 & 1 & 0 \\ 0 & 1 & 2 & 2 & 2 \end{pmatrix}$.

2. $(12)G = 22201$ et $(12)G' = 12021$.

3. $H = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 2 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{pmatrix}$. On a $c_1 = c_3 + 2c_4$, $d = 3$. $n = 5$, $k = 2$ et $d = 3 < n - k + 1 = 4$.

4. $H(11102) = 000$. De $(ab)G = 11102$ on déduit $a = 2$ et $2 + 2b = 1$ d'où $b = 1$, message 21.
$H(12121) = 100 = H(00100)$ le mot envoyé est 12021, encodé par G, le message est 20.

6. — 1. $n = 4$, $k = 2$, donc $\#C = 25$.

2. Le code est systématique car le déterminant $\begin{vmatrix} 3 & 4 \\ 0 & 3 \end{vmatrix} = 9 \equiv 4 \pmod 5$ est non nul dans $\mathbb{F}_5$.

3. Par pivot sur les lignes on obtient
$$G = \begin{pmatrix} 3 & 4 & 1 & 0 \\ 0 & 3 & 4 & 1 \end{pmatrix} \to \begin{pmatrix} 1 & 3 & 2 & 0 \\ 0 & 3 & 4 & 1 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 3 & 4 \\ 0 & 3 & 4 & 1 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 3 & 4 \\ 0 & 1 & 3 & 2 \end{pmatrix} = G'.$$
On en déduit pour matrice de contrôle $H = \begin{pmatrix} 2 & 2 & 1 & 0 \\ 1 & 3 & 0 & 1 \end{pmatrix}$.

4. Il est clair que $d = 3$, $t = 1$, le code est MDS.

5. Si $a \in \mathbb{F}_5^*$, $H(a, 0, 0, 0) = a(21)$, $H(0, a, 0, 0) = a(23)$, etc. La table de correction est constituée des colonnes c_i de H et de leurs multiples.

6. $H(3001) = 14 = 3c_2$, le mot de code émis est donc $3001 - 0300 = 3201$.
$H(1101) = 40 = 4c_3$, le mot de code émis est donc $1101 - 0040 = 1111$.
$H(2311) = 12$, le syndrome n'est pas dans la table, on ne peut pas corriger.

7. — **Code de Hamming binaire de longueur 7**.

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

2. On en déduit
$$H = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

3. $H(1111111) = 000$, le mot de code est 1111111, le message encodé par G est est 1111.
   $H(1101011) = 010$ erreur en 6eme position, message encodé 1101.
   $H(0110110) = 011$, erreur en deuxième position, message encodé 0010.
   $H(1111010) = 101$, erreur en première position, message encodé 0111.

8. — $n = 6$, $k = 4$. Une matrice génératrice normalisée est $G' = \begin{pmatrix} 1 & 0 & 0 & 0 & 2 & 0 \\ 0 & 1 & 0 & 0 & 1 & 2 \\ 0 & 0 & 1 & 0 & 2 & 1 \\ 0 & 0 & 0 & 1 & 0 & 2 \end{pmatrix}$.

Matrice de contrôle $H = \begin{pmatrix} 1 & 2 & 1 & 0 & 1 & 0 \\ 0 & 1 & 2 & 1 & 0 & 1 \end{pmatrix}$, $d = 3$, le code est MDS.

9. — 1. On utilise la méthode du pivot de Gauss sur les lignes pour transformer G en G'.

2. $n = 6$, $k = 2$. $\quad H = \begin{pmatrix} 1 & 3 & 1 & 0 & 0 & 0 \\ 2 & 2 & 0 & 1 & 0 & 0 \\ 2 & 4 & 0 & 0 & 1 & 0 \\ 4 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$.

3. $d = 5$, le code est MDS. $t = 2$.

4. $H(432100) = 0004$, erreur en dernière position, message 432101.
   $H(411141) = 3113 = 3c_1 + c_6$ erreurs en les positions 1 et 6, message 111140.

10. — 1. Le code n'est pas systématique car le bloc 3×3 de gauche de G a un déterminant nul.

2. En permutant les colonnes 1 et 5, 2 et 6 on obtient un code systématique équivalent de matrices génératrice et de contrôle

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

   On obtient H en permutant les colonnes 1 et 5, 2 et 6 de H', ie $H = \begin{pmatrix} 0 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 \end{pmatrix}$.

3. $n = 6$, $k = 3$ et $d = 3$, le code n'est pas MDS.

4. $H(111110) = 101$, erreur sur le 3eme bit, le mot de code émis est 110110 qui correspond à la première ligne de G, le message encodé par G est donc 100.
   $H(111111) = 110$, plus d'une erreur.

11. — 1. Le code est systématique car la sous-matrice matrice carrée 3×3 de gauche de G est inversible.

2. La matrice normalisée est

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

   On a $d = 3$ donc $t = 1$.

3. $H'(110110) = 011 = c_1$, erreur sur le premier bit, le mot de code émis est 010110.

12. — 1. $n = 6$ et $k = 4$, on en déduit $d \leq 3$, (Borne de Singleton).

2. $\quad G_2 = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} \sim G_2' = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}.$

$$H_2' = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix} \sim H_2 = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}; \, d = 1.$$

$$G_3 = \begin{pmatrix} 1 & 0 & 0 & 1 & 2 & 2 \\ 0 & 1 & 0 & 0 & 2 & 2 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 2 & 0 & 2 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 & 1 & 2 & 2 \\ 0 & 1 & 0 & 0 & 2 & 2 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 & 0 & 2 & 1 \\ 0 & 1 & 0 & 0 & 2 & 2 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \end{pmatrix}$$

$$H_3 = \begin{pmatrix} 1 & 1 & 2 & 0 & 1 & 0 \\ 2 & 1 & 0 & 2 & 0 & 1 \end{pmatrix}; \, d = 2.$$

$$G_5 = \begin{pmatrix} 1 & 0 & 0 & 1 & 2 & 2 \\ 0 & 1 & 0 & 0 & 2 & 2 \\ 0 & 0 & 1 & 0 & 1 & 3 \\ 0 & 0 & 0 & 2 & 3 & 2 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 & 1 & 2 & 2 \\ 0 & 1 & 0 & 0 & 2 & 2 \\ 0 & 0 & 1 & 0 & 1 & 3 \\ 0 & 0 & 0 & 1 & 4 & 1 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 & 0 & 3 & 1 \\ 0 & 1 & 0 & 0 & 2 & 2 \\ 0 & 0 & 1 & 0 & 1 & 3 \\ 0 & 0 & 0 & 1 & 4 & 1 \end{pmatrix}.$$

$$H_5 = \begin{pmatrix} 2 & 3 & 4 & 1 & 1 & 0 \\ 4 & 3 & 2 & 4 & 0 & 1 \end{pmatrix}; \, d = 3.$$

3. $H_5(111234) = 41 = 4c_4$, erreur en 4eme position, le mot de code émis est donc $111234 - 000400 = 111334$.

13. — Dans $\mathbb{F}_2[X]$, on a $X^8 - 1 = X^8 + 1 = (X^5 + X^4 + X + 1)(X^3 + X^2 + X + 1)$, le polynôme $X^5 + X^4 + X + 1$ est bien un diviseur de $X^8 - 1$. Le polynôme de contrôle est $X^3 + X^2 + X + 1$. On en déduit les matrices génératrice et de contrôle

$$G = \begin{pmatrix} 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \end{pmatrix} \quad \text{et} \quad H = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

14. — Dans $\mathbb{F}_2[X]$, on a $X^4 - 1 = (X - 1)^4$, les diviseurs propres de $X^4 - 1$ sont $(X - 1)^i = (X + 1)^i$ pour $i = 1, 2, 3$. Les codes correspondants sont de dimension $4 - i$.

– Pour $i = 1$, on a $g = 1 + X$, $h = (1 + X)^3 = X^3 + X^2 + X + 1$ et $k = 3$ d'où

$$G_1 = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix} \quad \text{et} \quad H_1 = \begin{pmatrix} 1 & 1 & 1 & 1 \end{pmatrix}$$

– Pour $i = 2$, on a $g = (1 + X)^2 = 1 + X^2$, $h = g$ et $k = 2$ d'où

$$G_2 = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix} \quad \text{et} \quad H_2 = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$$

– Pour $i = 3$, on a $g = (1 + X)^3 = 1 + X + X^2 + X^3$, $h = 1 + X$ et $k = 1$ d'où

$$G_3 = \begin{pmatrix} 1 & 1 & 1 & 1 \end{pmatrix} \quad \text{et} \quad H_3 = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}$$

15. — Si $a_0 = 0$, le mot de code $a_1 \dots a_{r-1}00\dots0$ obtenu par décalage à gauche de $\widetilde{m}$ possède un zéro de plus à droite que $\widetilde{m}$ qui n'est donc pas minimal.

16. — Non, le polynôme $1 + X + X^2$ ne divise pas $X^5 - 1$ dans $\mathbb{F}_2[X]$.

17. — 1. (a) Il est clair que le code C_m est de longueur n.

Le code C_m est cyclique car le décalage σ commute avec l'addition et la multiplication par un scalaire, c'est-à-dire que si a et $b \in \mathbb{F}_q$, et m_1 et $m_2 \in {\mathbb{F}_q}^n$, on a $\sigma(am_1 + bm_2) = a\sigma(m_1) + b\sigma(m_2)$.

(b) Si un code cyclique C contient le mot m, il contient tous les mots décalés de m, donc $C_m \subseteq C$.

(c) Soit g_m le polynôme générateur de C_m. On sait que g_m divise les polynômes $X^n - 1$ et $m(X)$, il divise donc leur pgcd g'_m. Le code cyclique C'_m engendré par le polynôme g'_m contient m car g'_m divise $m(X)$, donc $C_m \subseteq C'_m$. Comme le mot associé à g_m appartient à C_m donc à C'_m , on en déduit que g'_m divise g_m. Les deux polynômes g'_m et g_m étant unitaires, ils sont égaux.

2. On a $m(X) = X^5 + X^4 + 2X^2 + 2X$ et $g_m = \text{pgcd}\,(X^9 - 1, m(X)) = (X-1)^3 = 2 + X^3$.

18. — Soit g le polynôme générateur de C. On sait que $m \in C$ si et seulement si le polynôme $m(X)$ est divisible par g, on écrit $m(X) = g(X)r(X)$ avec $r(X) \in \mathbb{F}_q[X]$, ce qui équivaut à

$$h(X)m(X) = h(X)g(X)r(X) = (X^n - 1)r(X).$$

19. — **Code de Hamming binaire de longueur $2^s - 1$.** L'application linéaire u est surjective puisque les α^i constituent tous les éléments non nuls de $\mathbb{F}_{2^s}$. On en déduit que $C = Ker(u)$ est de dimension $k = n - s = 2^s - 1 - s$.

Une boule de Hamming de rayon 1 est de cardinal $n + 1 = 2^s$. Comme $d \geq 3$, la réunion boules de Hamming de rayon 1 centrées en les 2^k éléments de C possède

$$2^k\, 2^s = 2^{2^s - 1 - s}\, 2^s = 2^{2^s - 1} = 2^n = \#{\mathbb{F}_2}^n,$$

c'est-à-dire que $\mathbb{F}_2^n$ est égal à la réunion de ces boules. Le code est donc parfait.

Soit $x \in \mathbb{F}_2^n$ un mot de poids 2, il existe un mot de code m tel que $d_H(x, m) \leq 1$, et comme $w(m) \geq 3$, on en déduit $w(m) = 3$, donc $d = 3$.

Soit H une matrice de contrôle de C. Chacune des $2^s - 1$ colonnes de H appartient à $\mathbb{F}_2^s \setminus \{0\}$ et ces colonnes sont toutes distinctes.

Le code C est cyclique car

$$u(x_1, \ldots, x_{n-1}, x_0) = \sum_{k=0}^{n-2} x_{k+1}\, \alpha^k + x_0 \alpha^{n-1} = \alpha^{-1} u(x_0, x_1, \ldots, x_{n-1}).$$

Il est clair que $g(X)^2 = g(X^2)$, on en déduit que $g \in \mathbb{F}_2[X]$.

Le mot $m = g_0, g_1, \ldots, g_{s-1}, 1, \underbrace{0, \ldots, 0}_{n-s}$ associé au polynôme g est dans C puisque $u(m) = g(\alpha) = 0$.

Il résulte du théorème **6.22** du cours que m est le mot minimal de C donc que g en est le polynôme générateur.

20. — **Code de Reed-Solomon**

1. On a $\alpha^3 = \alpha + 1 \neq 1$, α est donc un élément primitif, en effet tout élément de $\mathbb{F}_8^*$ autre que 1 est un élément primitif car $\#\mathbb{F}_8^* = 7$ est un nombre premier.
2. On a $\alpha^3 = 1 + \alpha$, $\alpha^4 = \alpha + \alpha^2$, $\alpha^5 = 1 + \alpha + \alpha^2$, $\alpha^6 = 1 + \alpha^2$, $\alpha^7 = 1$.
3. Le polynôme $X^7 - 1$ admet pour racines simples toutes les puissance de α.

   On utilise la table des logarithmes de base α pour montrer que

$$g = (X - \alpha)(X - \alpha^2) = X^2 + (\alpha + \alpha^2)X + \alpha^3 = X^2 + \alpha^4 X + \alpha^3.$$

4. Le code C est de longueur 7 et de dimension 5 sur $\mathbb{F}_8$. Il possède $8^5 = 2^{15} = 32\,768$ mots.

Une matrice génératrice est donnée par

$$G = \begin{pmatrix} \alpha^3 & \alpha^4 & 1 & 0 & 0 & 0 & 0 \\ 0 & \alpha^3 & \alpha^4 & 1 & 0 & 0 & 0 \\ 0 & 0 & \alpha^3 & \alpha^4 & 1 & 0 & 0 \\ 0 & 0 & 0 & \alpha^3 & \alpha^4 & 1 & 0 \\ 0 & 0 & 0 & 0 & \alpha^3 & \alpha^4 & 1 \end{pmatrix}.$$

5. On détermine le polynôme de contrôle h à l'aide de la table de logarithmes

$$h = (X-1)(X-\alpha^3)(X-\alpha^4)(X-\alpha^5)(X-\alpha^6) = X^5 + \alpha^4 X^4 + X^3 + \alpha^5 X^2 + \alpha^5 X + \alpha^4.$$

Une matrice de contrôle est donnée par

$$H = \begin{pmatrix} 1 & \alpha^4 & 1 & \alpha^5 & \alpha^5 & \alpha^4 & 0 \\ 0 & 1 & \alpha^4 & 1 & \alpha^5 & \alpha^5 & \alpha^4 \end{pmatrix}.$$

6. L'examen de H indique $d = 3$, le code est MDS.
7. $H(\alpha^3\alpha^2\alpha\alpha^4\alpha\alpha^4 1) = (\alpha^5, \alpha) = \alpha c_2$, erreur en position 2, le mot de code émis est donc

$$\alpha^3\alpha^2\alpha\alpha^4\alpha\alpha^4 1 - 0\alpha 00000 = \alpha^3\alpha^4\alpha\alpha^4\alpha\alpha^4 1.$$

21. — 1. Tout polynôme $P \in \mathbb{F}_3[X]$ vérifie, pour tout $i \in \mathbb{N}$, $P(X^{3^i}) = [P(X)]^{3^i}$, en particulier $X^9 - 1 = (X-1)^9$, multiple de $g = (X-1)^5$.

2. Le polynôme g est un diviseur de degré 5 de $X^9 - 1$, le code cyclique C de longueur 9 qu'il engendre est donc un espace vectoriel de dimension $9 - 5 = 4$ sur le corps $\mathbb{F}_3$, on en déduit qu'il possède $3^4 = 81$ mots.
3. $(X-1)^5 = (X-1)^3(X-1)^2 = (X^3-1)(X^2-2X+1) = (X^3-1)(X^2+X+1)$
$= X^5 + X^4 + X^3 + 2X^2 + 2X + 2$.
4. Résulte de 3.
5. La différence des deux premières lignes de la matrice G est le mot 200200200 de poids 3.
6. $h = (X-1)^4 = (X-1)(X-1)^3 = (X-1)(X^3-1) = X^4 + 2X^3 + 2X + 1$.
7. Il en résulte qu'une matrice de contrôle de C est la matrice

$$H = \begin{pmatrix} 1 & 2 & 0 & 2 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & 0 & 2 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 2 & 0 & 2 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 2 & 0 & 2 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 2 & 0 & 2 & 1 \end{pmatrix}.$$

8. Il n'existe pas deux colonnes de H linéairement dépendantes, il en résulte $d \geq 3$. On sait d'autre part (question 5.) que $d \leq 3$. On a donc $d = 3$. Le code C corrige $\left\lfloor \dfrac{d-1}{2} \right\rfloor = 1$ erreur.
9. On vérifie que le syndrome $H(m)$ de m est égal à la première colonne de H.
Le mot de code émis est donc $121102210 - 100000000 = 021102210$. Le message émis est 0110.