Codes correcteurs

Delphine Boucher

Master 1 de mathématiques fondamentales · Université de Rennes 1
Notes prises par Téofil Adamski (version du 9 avril 2021)

Chapitre 1

Généralités sur les codes correcteurs

1.1 Généralités

L'objectif initial des codes correcteurs est de parer les interférences dans un canal de transmission. On considère un expéditeur et un destinataire communiquant par un canal. L'expéditeur envoie un mot $m \in A^k$ sur un alphabet A. Cependant, il se peut se le destinataire reçoive un message différent m'. On va donc associer au mot m, de manière injective, un code $c \in A^n$ avec $n \geqslant k$. Le destinataire lui recevra une code c' et le surplus des $n-k$ informations va permettre de retrouver le message initial m.

▷ Exemple. On considère un canal de transmission d'informations binaires qui fait au plus une erreur sur un chiffre. Par exemple, l'expéditeur envoie le nombre 1101, mais le destinataire reçoit le nombre 1001. Un bon code correcteur associé au nombre envoyé est donc ce nombre répété trois fois. Avec ce code, on peut savoir si le nombre à l'arrivé est bon.

Définition 1.1. Soit A un ensemble de cardinal $q \in \mathbf{N}^*$. Un *code* sur A de longueur $n \in \mathbf{N}$ est un sous-ensemble de A^n. Le *log-cardinal* d'un code C sur A est la quantité $k \coloneqq \log_q |C|$ et son *taux d'information* est la quantité k/n.

Dans toute la suite, on fixe un ensemble fini A, appelée un *alphabet*. Soit $n \in \mathbf{N}^*$ un entier non nul.

Définition 1.2. Le *poids de Hamming* d'un élément $x \coloneqq (x_1, \dots, x_n) \in A^n$ est l'entier

$$w_{\mathrm{H}}(x) \coloneqq \sharp\{i \in [\![1, n]\!] \mid x_i \neq 0\}.$$

La *distance de Hamming* d'un élément $x \in A^n$ à un élément $y \in A^n$ est l'entier

$$d_{\mathrm{H}}(x, y) \coloneqq w_{\mathrm{H}}(x - y).$$

Proposition 1.3. L'application $d_{\mathrm{H}} \colon A^n \times A^n \longrightarrow \mathbf{N}$ est bien une distance sur A^n.

Définition 1.4. La *distance minimale* d'un code $C \subset A^n$ de longueur n est l'entier

$$d \coloneqq \min_{\substack{x,y \in C \\ x \neq y}} d_{\mathrm{H}}(x, y).$$

Proposition 1.5. Soit $C \subset A^n$ un code de longueur n et de distance minimale $d \in \mathbf{N}$. Soit $y \in A^n$. Alors l'ensemble

$$\{c \in C \mid d_{\mathrm{H}}(y, c) \leqslant t\} \quad \text{avec} \quad t \coloneqq \left\lfloor \frac{d-1}{2} \right\rfloor$$

est soit vide soit un singleton.

Preuve On distingue deux cas. Si tout mot $c \in C$ est à distance supérieure strict à t, alors cet ensemble est vide. On suppose maintenant qu'il existe un mot $c \in C$ tel que $d_{\mathrm{H}}(y, c) \leqslant t$. Soit $c' \in C$ un autre tel mot. Alors l'inégalité triangulaire assure $d_{\mathrm{H}}(c, c') \leqslant 2t < d$ ce qui force $c = c'$. □

Proposition 1.6. Soient $c \in C$ et $y \in A^n$ tels que $d_H(y, c) \leqslant d - 1$. Alors $y = c$ ou $y \notin C$.

L'objectif est de construire des codes de longueur n, de log-cardinal $k \in \mathbf{R}_+$ et de distance minimale $d \in \mathbf{N}$ tel que les quantités k/n et d/n soient grandes. De plus, on souhaite avoir un algorithme de correction/décodage qui est efficace, *i. e.* se fait en temps polynomial.

THÉORÈME 1.7 *(borne de Singleton).* Soit $C \subset A^n$ un code de longueur n, de cardinal $M \in \mathbf{N}$ et de distance minimale $d \in \mathbf{N}$. Soit $k \coloneqq \log_q M$. Alors

$$d \leqslant n - k + 1.$$

Preuve On considère l'application $f\colon C \longrightarrow A^{\lceil k \rceil - 1}$ de projection sur les $\lceil k \rceil - 1$ premières coordonnées. Si elle était injective, alors $\sharp C = \sharp f(C) \leqslant q^{\lceil k \rceil - 1}$, donc $k \leqslant \lceil k \rceil - 1$ ce qui est impossible. On peut donc trouver deux mots distincts $c, c' \in C$ tels que $f(c) = f(c')$. On obtient

$$w_{\mathrm{H}}(c - c') \leqslant n - (\lceil k \rceil - 1) \leqslant n - k + 1$$

ce qui assure la conclusion. □

▷ EXEMPLES. • *Code de répétition.* On considère l'application

$$\varphi\colon \left| \begin{array}{l} \mathbf{F}_2 \longrightarrow \mathbf{F}_2^n, \\ m \longmapsto (m, \dots, m) \end{array} \right.$$

et le code $C \coloneqq \varphi(\mathbf{F}_2)$. Il est de longueur n, de cardinal 2 et de log-cardinal 1.

• *Code de parité.* On considère le code C défini comme l'image de $\mathbf{F}_2^{n-1}$ par l'application

$$\varphi\colon \left| \begin{array}{c} \mathbf{F}_2^{n-1} \longrightarrow \mathbf{F}_2^n, \\ (m_1, \dots, m_{n-1}) \longmapsto (m_1, \dots, m_{n-1}, m_1 + \cdots + m_{n-1}) \end{array} \right.\!\!.$$

Il est de longueur n et de cardinal 2^{n-1}. Trouvons sa distance minimale. Soient $c, c' \in C$. Alors un simple calcul donne $d_{\mathrm{H}}(c, c') = w_{\mathrm{H}}(c - c') \in 2\mathbf{N}$, donc sa distance minimale $d \in \mathbf{N}$ vérifie $d \geqslant 2$.

1.2 Codes linéaires

À un code, on va associer une matrice génératrice et une matrice de contrôle. Cette dernière va nous servir à calculer la distance minimale, à détecter et corriger les erreurs *via* différents algorithmes. Dans la suite, on considère une puissance $q \in \mathbf{N}$ d'un nombre premier et on se place dans le corps $\mathbf{F}_q$.

DÉFINITION 1.8. Soient $k, n \in \mathbf{N}$ des entiers tels que $k \leqslant n \neq 0$. Un *code linéaire* de longueur n et de dimension k est un sous-espace vectoriel de $\mathbf{F}_q^n$ de dimension k.

◇ REMARQUE. Soit $C \subset \mathbf{F}_q^n$ un code linéaire de longueur $n \in \mathbf{N}^*$ et de dimension $k \leqslant n$. Alors il existe une application linéaire injective $\varphi\colon \mathbf{F}_q^k \longrightarrow \mathbf{F}_q^n$ telle que $C = \varphi(\mathbf{F}_q^k)$. Soit $M \in \mathscr{M}_{n,k}(\mathbf{F}_q)$ la matrice de φ dans les bases canoniques. Sa transposée $G \coloneqq {}^{\mathrm{t}}M \in \mathscr{M}_{k,n}(\mathbf{F}_q)$ est la *matrice génératrice* de C. Le code C est ainsi caractérisé par l'égalité

$$C = \{nG \mid n \in \mathbf{F}_q^k\}.$$

DÉFINITION 1.9. La matrice génératrice G de C est sous forme *systématique* lorsqu'elle est de la forme

$$C = \begin{pmatrix} I_k & A \end{pmatrix} \quad \text{avec} \quad A \in \mathscr{M}_{k,n-k}(\mathbf{F}_q).$$

PROPOSITION 1.10. La distance minimale d'un code linéaire C est

$$d = \min_{0 \neq c \in C} w_{\mathrm{H}}(c).$$

NOTATION. On note $[n, k, d]_q$ l'ensemble des codes de longueur $n \in \mathbf{N}^*$, de dimension $k \leqslant n$ et de distance minimale $d \in \mathbf{N}$ sur $\mathbf{F}_q$.

Définition 1.11. Le *dual* d'un code C de $[n,k,d]_q$ de matrice génératrice G est l'orthogonal

$$C^\perp \coloneqq \{x \in \mathbf{F}_q^n \mid \forall c \in C,\ \langle x, c\rangle = 0\}$$

pour le produit scalaire canonique $\langle\ ,\ \rangle$ sur $\mathbf{F}_q^n$. Une *matrice de contrôle* de C est une matrice génératrice de $C^\perp$. On dit que le code C est *auto-dual* si $C^\perp = C$.

Proposition 1.12. Soit C un code $[n,k,d]_q$ de matrice de contrôle H. Alors

$$C \coloneqq \{x \in \mathbf{F}_q^n \mid H\,{}^{\mathrm{t}}x = 0\}.$$

Preuve Soit G sa matrice génératrice. À partir des définitions, on obtient

$$C^\perp = \{x \in \mathbf{F}_q^n \mid G\,{}^{\mathrm{t}}x = 0\},$$

donc $\dim C^\perp = n - k$ puisque $k = \operatorname{rg} G$. Comme la matrice H génère $C^\perp$, on a $\operatorname{rg} H = n - k$. Il suffit alors de montrer qu'une inclusion. Soit $c \in C$. Alors pour tout $y \in C^\perp$, on a $\langle c, y\rangle = 0$ ce qui implique $H\,{}^{\mathrm{t}}c = 0$ et conclut. □

◇ Remarque. On obtient alors $G\,{}^{\mathrm{t}}H = H\,{}^{\mathrm{t}}G = 0$.

▷ Exemples. • *Codes de répétition et de parité.* On reprend l'exemple de code de répétition, *i. e.* l'image par l'application

$$\varphi\colon \left|\begin{array}{l}\mathbf{F}_2 \longrightarrow \mathbf{F}_2^n,\\ m \longmapsto (m,\dots,m).\end{array}\right.$$

Sa matrice génératrice est $G \coloneqq (1 \quad \cdots \quad 1)$ et sa matrice de contrôle est $H \coloneqq (\mathbf{1}_{n-1} \quad I_{n-1})$. Pour le code de parité, sa matrice génératrice est $G' \coloneqq (I_{n-1} \quad \mathbf{1}_{n-1})$ et sa matrice de contrôle est G. Ces deux problèmes sont duaux l'un de l'autre.

• *Code de Hamming de longueur 7.* On considère l'image $C \subset \mathbf{F}_2^7$ par l'application

$$\left|\begin{array}{r}\mathbf{F}_2^4 \longrightarrow \mathbf{F}_2^7,\\ (m_1,m_2,m_3,m_4) \longmapsto (m_1,m_2,m_3,m_4,m_2+m_3+m_4,m_1+m_3+m_4,m_1+m_2+m_4).\end{array}\right.$$

Ses matrices génératrice et de contrôle valent

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

Il est de longueur 7 et de dimension 4. Pour connaître sa distance minimale, on peut faire la liste des mots ou utiliser la matrice H puisque $C = \{x \in \mathbf{F}_2^7 \mid H\,{}^{\mathrm{t}}x = 0\}$. Un mot de poids 1 implique une colonne de H nulle ce qui est impossible. Un mot de poids 2 implique deux mêmes colonnes dans H ce qui est aussi impossible. On note $H_i \in \mathbf{F}_2^3$ les colonnes de H. Comme $H_1 + H_2 + H_3 = 0$, on obtient $(1,1,1,0,\dots,0) \in C$, donc la distance minimale vaut $d \coloneqq 3$.

Théorème 1.13. Soient C un code $[n,k,d]_q$ et H une matrice de contrôle de C. Soit

$$\mathscr{D} = \{j \in [\![1,n]\!] \mid \text{tout ensemble de } j-1 \text{ colonnes de } H \text{ est linéairement indépendant}\}.$$

Alors la distance minimale de C vaut $D \coloneqq \max \mathscr{D}$.

Preuve On suppose qu'il existe $c \in C\backslash\{0\}$ tel que $w_{\mathrm{H}}(c) < D$. Alors $H\,{}^{\mathrm{t}}c = 0$ et $w \coloneqq w_{\mathrm{H}}(c) \leqslant D-1$. On peut écrire $c = (0,\dots,0,\lambda_1,\dots,\lambda_w,0,\dots,0)$ pour des éléments $\lambda_j \in \mathbf{F}_q$ non tous nuls. En considérant les λ_j-ièmes colonnes, il existe $D-1$ colonnes de H linéairement dépendantes ce qui est impossible. Donc $w_{\mathrm{H}}(c) \geqslant D$ pour tout $c \in C$.

Comme $D+1 \notin \mathscr{D}$, il existe D colonnes H_{i_1}, …, H_{i_D} de H linéairement dépendantes. De plus, tout ensemble de $D-1$ colonnes est libre. Par conséquent, il existe $\lambda_1,\dots,\lambda_D \in \mathbf{F}_q^*$ tels que

$$\lambda_1 H_{i_1} + \cdots + \lambda_D H_{i_D} = 0.$$

Le mot $c \coloneqq (0,\dots,0,\lambda_1,\dots,\lambda_D,0,\dots,0)$ où chaque élément λ_j est en position i_j vérifie $w_{\mathrm{H}}(c) = D$. Ceci termine la preuve. □

1.3 Décodage par tableau standard et syndrome

On considère un code C du type $[n, k, d]_q$. Étant donné un mot $y \in \mathbf{F}_q^n$, on souhaite trouver un mot $c \in C$ qui réalise l'infimum $\min_{x \in C} d_{\mathrm{H}}(y, x)$. Cela revient à trouver un mot $e \in \mathbf{F}_q^n$ de poids minimum tel que $y - e \in C$.

1.3.1 Tableau standard

On définit une relation d'équivalence $\mathscr{R}$ sur $\mathbf{F}_q^n$ en décrétant $x \mathscr{R} y$ si et seulement si $x - y \in C$ pour tous mots $x, y \in \mathbf{F}_q^n$. La classe d'équivalence d'un mot $x \in \mathbf{F}_q^n$ est noté $x + C$ et est appelée un *coset*. Un *coset leader* est un mot de plus petit poids dans le coset. On peut remarquer qu'il existe q^{n-k} cosets de taille $q^k = |C|$.

On peut construire le tableau contenant tous les cosets leader c en ligne, les colonnes correspondant aux autres mots de la classe, *i. e.* les mots $c + c_i$ où les mots c_i avec $i \in [\![1, |C| - 1]\!]$ forment une base de C. La tout première case contient donc le mot 0 et les autres cases de la première ligne contiennent les mots c_i. Ce tableau est le *tableau standard*. Soit $y \in \mathbf{F}_q^n$ un mot. On cherche la ligne du tableau où ce mot y apparaît. On lit un coser leader $e \in \mathbf{F}_q^n$ sur la première colonne et il est de poids minimal et vérifie $y - e \in C$.

▷ Exemple. On considère le code sur $\mathbf{F}_2$ de matrice génératrice

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

Pour construire son tableau standard, on énumère tous les mots de poids 1, on recommence avec les mots de poids 2, ... jusqu'à retomber sur un mot déjà obtenu. Son tableau standard est

00000	10110	01011	11101
10000	00110	11011	01101
01000	11110	00011	10101
00100	10010	01111	11001
00010	10100	01001	11111
00001	10111	01010	11100
11000	01110	10011	00101
10001	00111	11010	01100

Si on considère le emot $y \coloneqq 01101$ qui est présent sur la deuxième ligne du tableau, alors il suffit de prendre $e \coloneqq 10000$ et $c \coloneqq 11101$.

1.3.2 Tableau standard simplifié

Soit H une matrice de contrôle de C. Alors pour tous mots $x, y \in \mathbf{F}_q^n$, on a

$$x \mathscr{R} y \quad \Longleftrightarrow \quad H\,{}^{\mathrm{t}}x = H\,{}^{\mathrm{t}}y$$

où la quantité $H\,{}^{\mathrm{t}}x$ est appelée le *syndrome* de x. Le *tableau standard simplifié* est le tableau des syndromes. Soit $y \in \mathbf{F}_q^n$ un mot. Pour répondre au problème posé, on cherche dans le tableau un mot $e \in \mathbf{F}_q^n$ tel que $H\,{}^{\mathrm{t}}e = S \coloneqq H\,{}^{\mathrm{t}}y$. On en déduit que le poids de e est minimal et on a $y - e \in C$.

▷ Exemple. Reprenons l'exemple précédent. Une matrice de contrôle est

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

Alors le tableau standard simplifié est

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

Si on considère le mot $y \coloneqq 01101$, alors son syndrome vaut $S \coloneqq (1,1,0)$ et ce dernier se situe dans la deuxième ligne, donc on prend $e \coloneqq 10000$ qui répond au problème.

1.4 Codes de Hamming

Le but est de construire une famille infinie de codes binaires qui corrigent une erreur et de trouver deux algorithmes de décodage.

1.4.1 Définition

DÉFINITION 1.14. Soit $r \geqslant 2$ un entier. On pose $n \coloneqq 2^r - 1$. On considère la matrice $H \in \mathscr{M}_{r,n}(\mathbf{F}_2)$ dont les colonnes sont les vecteurs non nuls de $\mathbf{F}_2^r$ rangés dans l'ordre suivant : à un entier $j \in [\![1, n]\!]$, on associée le r-uplet $(\varepsilon_j^0, \dots, \varepsilon_j^{r-1}) \in \mathbf{F}_2^r$ tel que

$$\overline{j} = \sum_{i=0}^{r-1} \varepsilon_j^i 2^i$$

et la j-ième colonne de H sera

$$H_j = \begin{pmatrix} \varepsilon_j^0 \\ \vdots \\ \varepsilon_j^{r-1} \end{pmatrix}.$$

Le *code de Hamming* de longueur n est le code $\mathscr{H}_r$ de matrice de contrôle H. La dimension de ce code vaut $2^r - 1 - r$.

Calculons la distance minimale du code C. Il n'y a pas de mot de poids 1 car les colonnes de la matrice H sont non nulles. De même, il n'y a pas de mots de poids 2 car les colonnes sont deux à deux distinctes. Cependant, on a $J_1 + H_2 + H_3 = 0$, donc le mot $(1,1,1,0,\dots,0)$ est un mot de poids 3 du code $\mathscr{H}_r$. Sa distance minimale vaut donc 3.

1.4.2 Décodage/correction

Soit $y = c + e$ un mot avec $c \in \mathscr{H}_r$ et $e \in \mathbf{F}_2^n$ tels que $w_{\mathrm{H}}(e) \leqslant 1$. On souhaite trouver un tel mot c à partir d'un mot donné y. Pour se faire, on utilisera le syndrome. Ce dernier vaut

$$S \coloneqq H\,{}^{\mathrm{t}}y = H\,{}^{\mathrm{t}}c + H\,{}^{\mathrm{t}}e = H\,{}^{\mathrm{t}}e$$

qui est nul si $e = 0$ et qui vaut H_j si $e = (\delta_{j,i})_{i \in [\![1,n]\!]}$.

Premier algorithme

On possède un produit algorithme qui est le suivant.

Entrée : un mot y tel que $y = c + e$ avec $c \in \mathscr{H}_r$ et $w_{\mathrm{H}}(e) \leqslant 1$
Sortie : le mot c
  $S \longleftarrow H\,{}^{\mathrm{t}}y$
  Si $S = 0$, alors
    Retourner y
  Pour $j = 1$ à n, faire

Si $H_j = S$, alors
  $e \longleftarrow (\delta_{j,i})_{i\in[\![1,n]\!]}$
Retourner $y - e$.

Ici, on a corrigé le mot y en le mot c. Si on dispose de la matrice génératrice G, on peut trouver le mot m tel que $c = mG$ en résolvant le système linéaire $xG = c$ d'inconnue $x \in \mathbf{F}_2^n$.

▷ Exemple. On pose $r \coloneqq 3$ et on souhaite corriger le mot $y \coloneqq (1,1,0,1,0,1,0)$. On rappel la matrice de contrôle

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

Son syndrome est $S \coloneqq H\,{}^{\mathrm{t}}y = (1,0,0)$. L'entier correspondant est $j \coloneqq 1$. On peut donc en déduire que le mot corrigé est $c \coloneqq (0,1,0,1,0,1,0)$.

Au passage, comment peut-on trouver la matrice génératrice G de $\mathscr{H}_r$? On cherche une base du noyau de la matrice H et on peut la rechercher sous forme réduite.

1.5 Code de Goley binaire étendu

On considère le code $\mathscr{G}_{24}$ de matrice génératrice $G \coloneqq (I_{12} \quad A)$ où la matrice $A \coloneqq (a_{i,j})_{0\leqslant i,j\leqslant 11}$ est définie par

$$\begin{aligned} &a_{0,0} = 0, \\ &\forall i \in [\![0,11]\!], \quad a_{0,1} = a_{i,0} = 1, \\ &\forall i,j \in [\![1,11]\!], \quad a_{i,j} = b_{i-1,j-1} \end{aligned}$$

et la matrice $B \coloneqq (b_{i,j})_{0\leqslant i,j\leqslant 10}$ vérifie, pour tous $i,j \in [\![1,10]\!]$, le coefficient $b_{i,j}$ vaut 1 si et seulement si l'entier $i+j$ est un carré modulo 11, *i. e.* $i+j \in \{0,1,3,4,5,9\}$. En fait, la matrice G s'écrit

$$G = \left(\begin{array}{cccccccccccc|cccccccccccc} 1&0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1&1&1&1&1&1&1&1 \\ 0&1&0&0&0&0&0&0&0&0&0&0&1&1&1&0&1&1&1&0&0&0&1&0 \\ 0&0&1&0&0&0&0&0&0&0&0&0&1&1&0&1&1&1&0&0&0&1&0&1 \\ 0&0&0&1&0&0&0&0&0&0&0&0&1&0&1&1&1&0&0&0&1&0&1&1 \\ 0&0&0&0&1&0&0&0&0&0&0&0&1&1&1&1&0&0&0&1&0&1&1&0 \\ 0&0&0&0&0&1&0&0&0&0&0&0&1&1&1&0&0&0&1&0&1&1&0&1 \\ 0&0&0&0&0&0&1&0&0&0&0&0&1&1&0&0&0&1&0&1&1&0&1&1 \\ 0&0&0&0&0&0&0&1&0&0&0&0&1&0&0&0&1&0&1&1&0&1&1&1 \\ 0&0&0&0&0&0&0&0&1&0&0&0&1&0&0&1&0&1&1&0&1&1&1&0 \\ 0&0&0&0&0&0&0&0&0&1&0&0&1&0&1&0&1&1&0&1&1&1&0&0 \\ 0&0&0&0&0&0&0&0&0&0&1&0&1&1&0&1&1&0&1&1&1&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&0&1&1&0&1&1&0&1&1&1&0&0&0&1 \end{array}\right).$$

1.5.1 Distance minimale et auto-dualité

Lemme 1.15. Soient $x \coloneqq (x_1,\dots,x_n) \in \mathbf{F}_2^n$ et $y \coloneqq (y_1,\dots,y_n) \in \mathbf{F}_2^n$. On note

$$x * y \coloneqq \sharp\{i \in [\![1,n]\!] \mid x_i = y_i = 1\}.$$

Alors

1. $\langle x,y\rangle = x * y \mod 2$;
2. $\langle x,x\rangle = w_{\mathrm{H}}(x) \mod 2$;
3. $w_{\mathrm{H}}(x+y) = w_{\mathrm{H}}(x) + w_{\mathrm{H}}(x) - 2x * y$.

Preuve 1. Comme on est dans $\mathbf{F}_2$, on a immédiatement

$$\langle x,y\rangle = \sum_{i=1}^{n} x_i y_i = \sum_{x_i=y_i=1} 1 = x * y \mod 2.$$

2. L'égalité est évidente puisque $x * x = w_{\mathrm{H}}(x)$ et on utilise l'égalité précédente.
3. On a

$$\begin{aligned} w_{\mathrm{H}}(x+y) &= \sharp\{i \in [\![1,n]\!] \mid x_i + y_i = 1\} \\ &= \sharp\{i \in [\![1,n]\!] \mid x_i = 1, y_i = 0\} + \sharp\{i \in [\![1,n]\!] \mid x_i = 0, y_i = 1\} \\ &= w_{\mathrm{H}}(x) - \sharp\{i \in [\![1,n]\!] \mid x_i = y_i = 1\} + w_{\mathrm{H}}(y) - \sharp\{i \in [\![1,n]\!] \mid x_i = y_i = 1\} \\ &= w_{\mathrm{H}}(x) + w_{\mathrm{H}}(y). \end{aligned}$$

□

THÉORÈME 1.16. Soient C un code $[n,k,d]_2$ et G une matrice génératrice de C. Pour $i \in [\![0,k-1]\!]$, on note $g_i \in \mathbf{F}_2^n$ la i-ième ligne de G. On suppose que

– pour tous $i,j \in [\![0,k-1]\!]$ tels que $i \neq j$, on a $\langle g_i, g_j \rangle = 0$;
– pour tout $i \in [\![0,k-1]\!]$, on a $w_{\mathrm{H}}(g_i) \equiv 0 \mod 4$.

Alors $C \subset C^\perp$ et la distance minimale $d \in \mathbf{N}$ du code C vérifie $d \equiv 0 \mod 4$.

Preuve Soit $c \in C$. D'après les hypothèses, pour tous $i,j \in [\![0,k-1]\!]$, on a $\langle g_i, g_j \rangle = 0$ dans $\mathbf{F}_2$. Comme les lignes de G engendrent le code C, on obtient $\langle c, c' \rangle = 0$ pour tout mot $c' \in C$. Ceci assure alors $C \subset C^\perp$.

Pour tout entier $r \in \mathbf{N}^*$, on considère la propriété $\mathscr{P}(r)$

$$\text{pour toute partie } I \subset [\![0,k-1]\!] \text{ de cardinal } r, \text{ on a } w_{\mathrm{H}}\Big(\prod_{i\in I}\Big) \equiv 0 \mod 4.$$

Par hypothèse, la propriété $\mathscr{P}(1)$ est vraie. Soit $r \in \mathbf{N}^*$. On suppose $\mathscr{P}(r)$. Soit $I \subset [\![0,k-1]\!]$ une partie de cardinal $r+1$. Soit $i_0 \in I$. On pose

$$x \coloneqq g_{i_0} \quad \text{et} \quad y \coloneqq \sum_{i \in I \setminus \{i_0\}} g_i.$$

Alors le lemme précédent et l'hypothèse $\mathscr{P}(r)$ donnent

$$w_{\mathrm{H}}\Big(\sum_{i\in I} g_i\Big) = w_{\mathrm{G}}(x+y) = w_{\mathrm{H}}(x) + w_{\mathrm{H}}(y) - 2x * y \equiv 0 \mod 4.$$

Cela conclut la récurrence. Ainsi on obtient $d \equiv 0 \mod 4$. □

THÉORÈME 1.17. Le code $\mathscr{G}_{24}$ est un code $[24,12,8]_2$ auto-dual.

Preuve Pour $i \in [\![0,11]\!]$, on note $g_i \in \mathbf{F}_2^{24}$ la i-ième ligne de la matrice G. On a bien $w_{\mathrm{H}}(g_0) = 12 \equiv 0 \mod 4$ et $w_{\mathrm{H}}(g_i) = 8 \equiv 0 \mod 4$ pour tous $i \in [\![1,11]\!]$. Pour tout $i \in [\![1,11]\!]$, on a $\langle g_0, g_i \rangle = 6 = 0$ et, pour tout $i \in [\![2,11]\!]$, on a $\langle g_1, g_i \rangle = 4 = 0$. Par des permutations, on obtient $\langle g_i, g_j \rangle = 0$ pour tous $i,j \in [\![2,11]\!]$. D'après le théorème précédent, en notant $d \in \mathbf{N}$ la distance minimale de $\mathscr{G}_{12}$, on trouve

$$\mathscr{G}_{24} \subset \mathscr{G}_{24}^\perp \quad \text{et} \quad d \equiv 0 \mod 4.$$

Comme $\dim \mathscr{G}_{24} = 12 = 24 - 12 = \dim \mathscr{G}_{12}^\perp$, on obtient l'égalité $\mathscr{G}_{24} = \mathscr{G}_{24}^\perp$ ce qui montre l'auto-dualité.

Vérifions que $d = 8$. En regardant la matrice génératrice, on voit $d \leqslant 4$, donc $d \in \{4,8\}$. Raisonnons par l'absurde et supposons $d = 4$. Alors il existe un mot $c \in \mathscr{G}_{24}$ de poids 4. Comme la matrice G est génératrice, il existe un vecteur $x \in \mathbf{F}_2^{12}$ tel que $c = xG$. Comme la matrice de contrôle H est aussi génératrice puisque le code $\mathscr{G}_{24}$ est auto-dual, il existe un vecteur $y \in \mathbf{F}_2^{12}$ tel que $c = yH$. En exploitant la structure de G et H, on obtient

$$c = (x, xA) = (yA, y), \quad \text{donc} \quad c = (x,y).$$

On peut alors écrire $w_{\mathrm{H}}(c) = w_{\mathrm{H}}(x) + w_{\mathrm{H}}(y) = 4$. Distinguons cinq cas.

– Si $w_{\mathrm{H}}(x) = 0$, alors $c = 0$ ce qui est impossible.
– De même, le cas $w_{\mathrm{H}}(x) = 4$ est impossible puisqu'alors $w_{\mathrm{H}}(y) = 0$.
– Si $w_{\mathrm{H}}(x) = 1$, alors c est une ligne de G ce qui est impossible.
– Si $w_{\mathrm{H}}(y) = 1$, alors c est une ligne de H ce qui est impossible.

– On suppose $w_{\mathrm{H}}(x) = 2$. Alors c est une somme de deux lignes de G. Or pour tout $i \in [\![1, 11]\!]$, on a

$$w_{\mathrm{H}}(g_0 + g_i) = w_{\mathrm{H}}(g_0) + w_{\mathrm{H}}(g_i) - 2g_0 * g_i = 12 + 8 - 2 \times 6 = 8 \neq 4$$

et, pour tout $i \in [\![2, 11]\!]$, on a

$$w_{\mathrm{G}}(g_1 + g_i) = 8 + 8 - 2 \times 4 = 8 \neq 4.$$

Ce cas est aussi impossible.

Finalement, on obtient $d = 8$. □

1.5.2 Algorithme de décodage

L'idée est d'exploiter que les matrices G et H sont toutes les deux des matrices de contrôle du code $\mathscr{G}_{24}$. On va utiliser deux syndromes. Pour $i \in [\![0, 11]\!]$, on note $A_i \in \mathbf{F}_2^{12}$ la i-ième colonne de la matrice A.

Théorème 1.18. Soit $c \in \mathscr{G}_{24}$ et $e \coloneqq (x, y) \in \mathbf{F}_2^{12} \times \mathbf{F}_2^{12}$ tel que $w_{\mathrm{H}}(e) \leqslant \lfloor (8-1)/2 \rfloor = 3$. On pose

$$r \coloneqq c + e, \quad S \coloneqq H\,{}^{\mathrm{t}}r \quad \text{et} \quad T \coloneqq G\,{}^{\mathrm{t}}r.$$

Alors l'une des quatre situations suivantes est vérifiée :

(i) si $w_{\mathrm{H}}(S) \leqslant 3$, alors

$$x = 0 \quad \text{et} \quad y = {}^{\mathrm{t}}S\ ;$$

(ii) si $w_{\mathrm{H}}(S) > 3$ et il existe $i \in [\![0, 11]\!]$ tel que $w_{\mathrm{H}}(S + A_i) \in \{1, 2\}$, alors

$$x = \varepsilon_i \coloneqq (\delta_{i,j})_{j \in [\![0,11]\!]} \quad \text{et} \quad y = {}^{\mathrm{t}}S + {}^{\mathrm{t}}A_i\ ;$$

(iii) si $w_{\mathrm{H}}(T) \leqslant 3$, alors

$$x = {}^{\mathrm{t}}T \quad \text{et} \quad y = 0\ ;$$

(iv) si $w_{\mathrm{H}}(T) > 3$ et il existe $i \in [\![0, 11]\!]$ tel que $w_{\mathrm{H}}(T + A_i) \in \{1, 2\}$, alors

$$y = \varepsilon_i \quad \text{et} \quad x = {}^{\mathrm{t}}T + {}^{\mathrm{t}}A_i.$$

Preuve Une matrice de contrôle est $H = (A \quad I_{12})$ de telle sorte que

$$S = A\,{}^{\mathrm{t}}x + {}^{\mathrm{t}}y \quad \text{et} \quad T = {}^{\mathrm{t}}x + A\,{}^{\mathrm{t}}y.$$

(i) On a

$$\begin{aligned} w_{\mathrm{H}}(S) &\geqslant w_{\mathrm{H}}(xA) - w_{\mathrm{H}}(y) \\ &\geqslant w_{\mathrm{H}}(xA) + w_{\mathrm{H}}(x) - w_{\mathrm{H}}(x) - w_{\mathrm{H}}(y) \\ &\geqslant w_{\mathrm{H}}(x, xA) - w_{\mathrm{H}}(e). \end{aligned}$$

Si $x \neq 0$, alors $w_{\mathrm{H}}(S) \geqslant 8 - 3 > 3$.

(ii) On a

$$\begin{aligned} w_{\mathrm{H}}(S + A_i) &= w_{\mathrm{H}}(xA + y + {}^{\mathrm{t}}A_i) \\ &= w_{\mathrm{H}}((x + \varepsilon_i)A + y) \\ &\geqslant w_{\mathrm{H}}((x + \varepsilon_i A)A) - w_{\mathrm{H}}(y) \\ &\geqslant w_{\mathrm{H}}((x + \varepsilon_i)A) + w_{\mathrm{H}}(x + \varepsilon_i) - w_{\mathrm{H}}(x + \varepsilon_i) - w_{\mathrm{H}}(y) \\ &\geqslant w_{\mathrm{H}}((x + \varepsilon_i)G) - w_{\mathrm{H}}(x) - w_{\mathrm{H}}(y) - 1. \end{aligned}$$

Si $x + \varepsilon_i \neq 0$, alors $w_{\mathrm{H}}(S + A_i) \geqslant 8 - 4$, donc $w_{\mathrm{H}}(S + A_i) \notin \{1, 2\}$. De plus, si $w_{\mathrm{H}}(s + A_i) = 0$, alors $x + \varepsilon_i = 0$ et ${}^{\mathrm{t}}(S + A_i) = y$.

On procède identiquement pour les cas (iii) et (iv).

Il reste à montrer qu'un autre cas n'est possible. Raisonnons par l'absurde et supposons qu'aucune des quatre cas n'est satisfait. Alors

$$w_{\mathrm{H}}(S), w_{\mathrm{H}}(T) > 3 \quad \text{et} \quad w_{\mathrm{H}}(S + A_i), w_{\mathrm{H}}(T + A_i) \notin \{1, 2\}, \quad i \in [\![0, 11]\!].$$

Comme $w_{\mathrm{H}}(e) = w_{\mathrm{H}}(x) + w_{\mathrm{H}}(y) \leqslant 3$. Distinguons quatre cas.

– On suppose $w_{\mathrm{H}}(x) = 0$. Alors $w_{\mathrm{H}}(y) \leqslant 3$, donc $w_{\mathrm{H}}(S) \leqslant 3$ ce qui est impossible.

– De même, le cas $w_{\mathrm{H}}(y) = 0$ est impossible.
– On suppose $w_{\mathrm{H}}(x) = 1$. Alors $w_{\mathrm{H}}(y) \leqslant 2$ et il existe $i \in [\![0, 11]\!]$ tel que $x = \varepsilon_i$. On peut écrire

$$w_{\mathrm{H}}(S + A_i) = w_{\mathrm{H}}(A\,{}^{\mathrm{t}}x + {}^{\mathrm{t}}y + A\,{}^{\mathrm{t}}\varepsilon_i) = w_{\mathrm{H}}({}^{\mathrm{t}}y) \in \{1, 2\}$$

ce qui est impossible.
– De même, le cas $w_{\mathrm{H}}(y) = 2$ est impossible.
Ceci conclut la preuve. □

Algorithme de décodage

On peut alors exhiber l'algorithme suivant qui repose sur ce théorème.

Entrée : un mot $y \coloneqq (y_0, \ldots, y_{23})$ tel que $y = c + e$ avec $c \in \mathscr{G}_{24}$ et $w_{\mathrm{H}}(e) \leqslant 3$
Sortie : le mot m

```
T ⟵ G ᵗy
Si w_H(T) ⩽ 3, alors
    x ⟵ ᵗT
Sinon
    Si w_H(T + A_i) ⩽ 2 pour un entier i ∈ ⟦1, 11⟧, alors
        x ⟵ ᵗ(T + A_i)
    Sinon
        S ⟵ ᵗAT
        Si w_H(S) ⩽ 3, alors
            x ⟵ 0
        Sinon
            Si w_H(S + A_i) ⩽ 2 pour un entier i ∈ ⟦1, 11⟧, alors
                x ⟵ ε_i
            Sinon
                Retourner « faux »
m ⟵ (y_0, ..., y_11) + x
Retourner m
```

Chapitre 2

Codes de Reeed-Solomon généralisés et codes de Reed-Muller

2.1 Code GRS

2.1.1 Matrice de contrôle et distance minimale

Définition 2.1. Soit $q \in \mathbf{N}$ une puissance d'un nombre premier. Soient $k, n \in \mathbf{N}$ des entiers tels que $k \leqslant n$. Soient $\alpha_1, \ldots, \alpha_n \in \mathbf{F}_q^*$ des éléments deux à deux distincts. Soient $v_1, \ldots, v_n \in \mathbf{F}_q^*$ d'autres éléments. Le code de Reed-Solomon généralisé du type $[n,k]_q q$, de localisateurs α_1, …, α_n et de multiplicateurs v_1, …, v_n est le code de matrice de contrôle $H \coloneqq VD$ où

$$V \coloneqq \begin{pmatrix} 1 & \cdots & 1 \\ \alpha_1 & \cdots & \alpha_n \\ \vdots & & \vdots \\ \alpha_1^{n-k-1} & \cdots & \alpha_n^{n-k-1} \end{pmatrix} \quad \text{et} \quad D \coloneqq \operatorname{diag}(v_1, \ldots, v_n).$$

Ce code est noté $\mathrm{GRS}_{n,k}(\alpha, v)$.

Vocabulaire. Le vecteur α est le *support* de ce code. On dit que ce code est
– *normalisé* si $v_1 = \cdots = v_n = 1$;
– *primitif* sur $n = q - 1$.

◇ Remarque. – Nécessairement, on a $n \leqslant q - 1$.
– La matrice formée des $n - k$ premières colonnes de H est inversible. En particulier, le code est de dimension k.

▷ Exemples. On considère le code GRS primitif du type $[6,2]_7$, de localisateurs $1, \ldots, 6$ et de multiplicateurs $1, \ldots, 6$. La matrice de contrôle est donc

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 2 & 2 & 4 & 1 \\ 1 & 1 & 6 & 1 & 6 & 6 \end{pmatrix} \begin{pmatrix} 1 & & & & & \\ & 2 & & & & \\ & & 3 & & & \\ & & & 4 & & \\ & & & & 5 & \\ & & & & & 6 \end{pmatrix}.$$

• *Codes de Reed-Solomon.* On suppose $n \mid q - 1$. Soit $\alpha \in \mathbf{F}_q$ une racine n-ième de l'unité. On considère le code de localisateurs $1, \alpha, \ldots, \alpha^{n-1}$ et de multiplicateurs $1, \alpha^{bk}, \ldots, (\alpha^b)^{n-1}$ pour un entier $b \in \mathbf{N}$.

Proposition 2.2. Un code GRS est MDS.

Preuve Soit $C \coloneqq \mathrm{GRS}_{n,k}(\alpha, v)$ un code GRS. On note $d \in \mathbf{N}^*$ sa distance minimale. D'après la borne de singleton, on a $d \leqslant n - k + 1$. Montrons qu'on a en fait l'égalité. On note $H = V \times D$ sa matrice de contrôle associée. Il suffit de montrer que tout ensemble de $n - k$ colonnes de H est libre. Soient $j_1, \ldots, j_{n-k} \in [\![1, n]\!]$ une suite strictement croissante. On note Δ la matrice formée des colonnes j_1, …, j_{n-k} de H. Alors $\Delta = \tilde{V}\tilde{d}$ avec $\tilde{V}_{i,\ell} = \alpha_{j_\ell}^{i-1}$ et $\tilde{D}_{\ell,\ell} = v_{j_\ell}$. La matrice $\tilde{V}$ est une matrice de Vandermonde de la famille $(\alpha_{j_1}, \ldots, \alpha_{j_k})$ où les éléments de cette famille sont deux à deux distincts, donc la matrice Δ est inversible. Cela montre que tout ensemble de $n - k$ colonnes de H est libre. D'où $d \geqslant n - k + 1$. Le code est donc MDS. □

2.1.2 Matrice génératrice et code d'évaluation

PROPOSITION 2.3. Le dual d'un code GRS est un code GRS de mêmes localisateurs.

Preuve Soit $C \coloneqq \mathrm{GRS}_{n,k}(\alpha, v)$ un code GRS. On note $H = VD$ sa matrice de contrôle. On veut montrer qu'il existe un élément $v' \in (\mathbf{F}_q^*)^n$ tel que le code C ait pour matrice génératrice la matrice de contrôle du code $\mathrm{GRS}_{n,n-k}(\alpha, v')$, c'est-à-dire tel que $G\,{}^{\mathrm{t}}H = 0$ avec $G \coloneqq (\alpha_j^{i-1} v'_j)_{1 \leqslant i \leqslant k, 1 \leqslant j \leqslant n}$. Raisonnons par analyse-synthèse. Soit $v' \coloneqq (v'_1, \dots, v'_\ell) \in (\mathbf{F}_q^*)^n$ un tel vecteur. Pour tout $i \in [\![1, k]\!]$ et $j \in [\![1, n-k]\!]$, on a

$$\sum_{\ell=1}^{n} \alpha_\ell^{i-1} v'_\ell \times \alpha_\ell^{j-1} v_\ell = 0, \quad i.\ e. \quad \sum_{\ell=1}^{n} (\alpha_\ell^{i+j-1-1} v_\ell) v'_\ell = 0.$$

Autrement dit, pour tout $s \in [\![1, n-1]\!]$, on a

$$\sum_{\ell=1}^{n} (\alpha_\ell^{s-1} v_\ell) v'_\ell = 0.$$

Cela se réécrit encore $\tilde{H} v' = 0$ avec $\tilde{H} \coloneqq (\alpha_j^{i-1} v_j)_{1 \leqslant i \leqslant n-1, 1 \leqslant j \leqslant k}$. La matrice $\tilde{H}$ est une matrice de contrôle du code $\mathrm{GRS}_{n,1}(\alpha, v)$. Alors $v' \in \mathrm{GRS}_{n,1}(\alpha, v)$. Comme le vecteur a ses composantes tous non nuls, on a aussi $w_{\mathrm{H}}(v') = n$. Réciproquement, comme le code $\mathrm{GRS}_{n,1}(\alpha, v)$ est MDS, on peut trouver un vecteur $v' \in \mathbf{F}_q^n$ tel que $v' \in \mathrm{GRS}_{n,1}(\alpha, v)$ et $w_{\mathrm{H}}(v'it = n$. On peut alors remonter les équivalence et le vecteur v' trouvé satisfait notre souhait initial. □

COROLLAIRE 2.4. Tout code GRS possède une matrice génératrice sous la forme VD pour une matrice V de van der Monde et une matrice G diagonale.

◇ REMARQUE. On note $\mathbf{1}_n \coloneqq (1, \dots, 1) \in \mathbf{F}_q^n$. En écrivant le produit mG pour $m \in \mathbf{F}_q^n$, on montre que le code $C \coloneqq \mathrm{GRS}_{n,k}(\alpha, \mathbf{1}_n)$ s'écrit

$$C = \{(f(\alpha_1), \dots, f(\alpha_n)) \mid f \in \mathbf{F}_q[X]_{<k}\}.$$

2.1.3 Algorithme de décodage de Welch-Berklkamp

Soit $C \coloneqq \{(f(\alpha_1), \dots, f(\alpha_n)) \mid f \in \mathbf{F}_q[X]_{<k}\}$ un code GRS. Soit $f \in \mathbf{F}_q[X]_{<k}$. On pose

$$c \coloneqq (f(\alpha_1), \dots, f(\alpha_n)).$$

Soit $e \coloneqq (e_1, \dots, e_n) \in \mathbf{F}_q^n$ tel que $w_{\mathrm{H}}(e) \leqslant t \coloneqq \lfloor (n-k)/2 \rfloor$. On pose $r \coloneqq c + e = (r_1, \dots, r_n)$. Comme toujours, l'objectif est de trouver le polynôme f connaissant le mot r. Pour réaliser cela, on peut adopter une stratégie d'interpolation du polynôme ou utiliser l'algorithme de Welch-Berklkamp.

Donnons l'idée de ce dernier algorithme. On pose $I \coloneqq \{i \in [\![1, n]\!] \mid e_i \neq 0\}$ et $\sigma \coloneqq \prod_{i \in I} (x - \alpha_i)$. Soit $i \in [\![1, n]\!]$. Alors $\sigma(\alpha_i) = 0$ ou $r_i = f(\alpha_i)$, donc $\sigma(\alpha_i)(r_i - f(\alpha_i)) = 0$, donc

$$q(\alpha_i, r_i) = 0 \quad \text{avec} \quad q(x, y) \coloneqq \sigma(x) y - \sigma(x) f(y).$$

L'idée est donc de construire un polynôme $Q(x, y) = Q_0(x) + Q_1(x) y \in \mathbf{F}_q[x, y] \setminus \{0\}$ tel que

$$\forall i \in [\![1, n]\!], \quad Q(\alpha_i, r_i) = 0$$

et on en déduit

$$f(x) = -Q_0(x)/Q_1(x).$$

Soit $Q(x, y) \in \mathbf{F}_q[x, y] \setminus \{0\}$ un tel polynôme. On veut qu'il vérifie le système

$$\begin{cases} \forall i \in [\![1, n]\!], \quad Q(\alpha_i, r_i) = 0, \\ \deg Q_0 \leqslant n - 1 - t, \\ \deg Q_1 \leqslant n - 1 - t - (k-1). \end{cases} \tag{S}$$

Un tel polynôme $Q(x, y)$ existe bien. En effet, il est caractérisé par n équations en N inconnues avec

$$N \coloneqq (n - t) + (n - t - k + 1) = 2n - 2t - k + 1.$$

Or $t \leqslant (n-k)/2$, donc $N \geqslant 2n - (n-k) - k + 1 = n + 1 > n$. Le système (S) est alors sur-déterminé et possède une solution non nulle.

Montrons que $\varphi(x) \coloneqq Q_0(x) + Q_1(x)f(x) = 0$. On a

$$\begin{aligned}\deg\varphi &\leqslant \max(\deg Q_0, \deg Q_1 + \deg f)\\ &\leqslant \max(n-1-t, n-1-t-(k-1)+(k-1)) = n-1-t.\end{aligned}$$

De plus, soit $i \in [\![1,n]\!] \setminus I$. Alors $f(\alpha_i) = r_i$, donc $\varphi(\alpha_i) = Q_0(\alpha_i) + Q_1(\alpha_i)r_i = Q(\alpha_i, r_i) = 0$. Finalement, le polynôme φ admet au moins $n - |I|$ racines. Or $n - |I| \geqslant n - t > \deg\varphi$, donc le polynôme φ est nul.

▷ Exemple. On prend $(q,n,k) = (7,6,2)$. La capacité de correction vaut $t = 2$. On considère le code

$$C \coloneqq \{(f(1),\dots,f(6)) \mid f \in \mathbf{F}_7[X]_{<2}\}.$$

On pose $f \coloneqq 2 - x$. Alors le mot du code C associé est $c_f \coloneqq (1,0,6,5,4,3)$ et on va y ajouter l'erreur $e \coloneqq (0,2,0,3,0,0)$ de sorte à obtenir le mot $r \coloneqq (1,2,6,1,4,3)$. Effectuons l'algorithme : on cherche un polynôme $Q(x,y)$ sous la forme

$$Q(x,y) = Q_0(x) + Q_1(x)y \quad \text{avec} \quad \deg Q_0 \leqslant 3 \quad \text{et} \quad \deg Q_1 \leqslant 2$$

et vérifiant

$$\forall i \in [\![1,6]\!], \quad Q(i, r_i) = 0.$$

On note $Q_0(x) = a_0 + a_1x + a_2x^2 + a_3x^2$ et $Q_1(x) = b_0 + b_1x + b_2x^2$. On obtient le système

$$\left(\begin{array}{cccc|ccc} 1&1&1&1&1&1&1\\ 1&2&3&1&2&4&1\\ 1&3&9&6&6&4&5\\ 1&4&2&1&1&4&2\\ 1&5&4&6&4&6&2\\ 1&6&1&6&3&4&3 \end{array}\right)\left(\begin{array}{c} a_0\\ a_1\\ a_2\\ a_3\\ \hline b_1\\ b_2\\ b_3 \end{array}\right) = 0.$$

On vérifie que le vecteur $(5,6,6,1,1,1,1)$ est solution. On en déduit

$$f(x) = -\frac{5 + 6x + 6x^2 + x^3}{1 + x + x^2} = -(x+5) = 2 - x.$$

2.2 Codes de Reed-Muller

Dans toute la suite, on se place dans le corps $\mathbf{F}_2$.

Définition 2.5. Soient $m \in \mathbf{N}^*$ et $r \in [\![0, 2^m]\!]$. On pose $n \coloneqq 2^m$. Le code de Reed-Muller de paramètre (r,m) est

$$\mathrm{RM}(r,m) \coloneqq \{(f(z_0),\dots,f(z_{n-1})) \mid f \in \mathbf{F}_2[X_0,\dots,X_{m-1}], \deg f \leqslant r\}$$

où les vecteurs z_i avec $i \in [\![0, n-1]\!]$ sont définie par $z_i \coloneqq (\varepsilon_i^0,\dots,\varepsilon_i^{m-1})$ où

$$i = \sum_{j=0}^{m-1} \varepsilon_i^j 2^j.$$

Proposition 2.6. La dimension du code $\mathrm{RM}(r,m)$ est

$$1 + \binom{m}{1} + \cdots + \binom{m}{r}.$$

Preuve On considère l'application

$$\varphi\colon \left|\begin{array}{l}\mathbf{F}_2[X_0,\dots,X_{m-1}]_{\leqslant r} \longrightarrow \mathbf{F}_2^n,\\ \qquad\qquad\qquad f \longmapsto (f(z_0),\dots,f(z_{n-1}))\end{array}\right.$$

Elle induit une application

$$\Theta\colon E_m \coloneqq \frac{\mathbf{F}_2[X_0,\dots,X_{m-1}]_{\leqslant m}}{\langle X_i^2 - X_i \mid i \in [\![0,m-1]\!]\rangle} \longrightarrow \mathbf{F}_2^n$$

qui est injective dont l'image vaut $\mathrm{RM}(m,n)$. De plus, son ensemble de départ E admet pour bases les vecteurs

$$1, \quad X_i, \quad X_iX_j \ (i \neq j), \qquad \ldots, \qquad X_0 \cdots X_{n-1}$$

ce qui en fait un espace vectoriel de dimension

$$\dim_{\mathbf{F}_2} E_m = 1 + \binom{m}{1} + \cdots + \binom{m}{m} = (1+1)^n = \dim_{\mathbf{F}_2} \mathbf{F}_2^n.$$

Il suffit alors de montrer que l'application Θ est surjective pour montrer le résultat. Soit $e \coloneqq e_i \in \mathbf{F}_2^n$ le i-ième vecteur de la base canonique de $\mathbf{F}_2^n$. Soit $I \coloneqq \{j \in [\![0, m-1]\!] \mid \varepsilon_i^j = 1\}$ où

$$i = \sum_{j=0}^{m-1} \varepsilon_i^j 2^j.$$

On pose

$$f \coloneqq \prod_{j \notin I} (1 + X_j) \prod_{j \in I} X_j$$

de sorte que $f(z_i) = 1$ et $f(\alpha) = 0$ pour tout $\alpha \in \mathbf{F}_2^n \setminus \{z_i\}$. Finalement, l'application Θ est bijective, donc l'application induite

$$\Psi \colon E_r \coloneqq \frac{\mathbf{F}_2[X_0, \ldots, X_{m-1}]_{\leqslant r}}{\langle X_i^2 - X_i \mid i \in [\![0, m-1]\!] \rangle} \longrightarrow \mathbf{F}_2^n$$

est injective car $E_r \subset E_m$. On en déduit

$$\dim_{\mathbf{F}_2} \mathrm{RM}(r,m) = \dim_{\mathbf{F}_2} \frac{\mathbf{F}_2[X_0, \ldots, X_{m-1}]_{\leqslant r}}{\langle X_i^2 - X_i \mid i \in [\![0, m-1]\!] \rangle} = 1 + \binom{m}{1} + \cdots + \binom{m}{r}. \qquad \square$$

Chapitre 3

Codes cycliques

3.1 Codes cycliques, générateurs

Définition 3.1. Un code linéaire C de longueur n sur $\mathbf{F}_q$ est *cyclique* si

$$c \coloneqq (c_0, \dots, c_{n-1}) \in C \quad \Longrightarrow \quad c^\pi \coloneqq (c_{n-1}, c_0, \dots, c_{n-2}) \in C.$$

▷ Exemples. Les codes

$$C_1 \coloneqq \{(0, \dots, 0), (1, \dots, 1)\} \text{ et } C_2 \coloneqq \{(0,0,0), (1,0,1), (1,1,0), (0,1,1)\}$$

sont cycliques. Plus généralement, le code

$$C_3 \coloneqq \{(c_1, \dots, c_{n-1}) \in \mathbf{F}_2^n \mid c_0 + \cdots + c_{n-1} = 0\}$$

est cyclique.

Soit C un code linéaire cyclique de longueur n sur $\mathbf{F}_q$. À un mot $c \coloneqq (c_0, \dots, c_{n-1}) \in C$, on associe le polynôme

$$c(X) \coloneqq c_0 + \cdots + c_{n-1}X^{n-1} \in \mathbf{F}_q[X]_{<n}$$

qu'on peut projeter dans l'anneau quotient

$$R_n[X] \coloneqq \mathbf{F}_q[X]/\langle X^n - 1\rangle.$$

Ainsi pour tout $c \in C$, on a $\overline{c^\pi(X)} = \overline{Xc(X)}$. On notera

$$C(X) \coloneqq \{c(X) \mid c \in C\} \in \mathbf{F}_q[X]_{<n} \quad \text{et} \quad \overline{C(X)} \coloneqq \{\overline{c(X)} \mid c \in C\} \subset R_n[X].$$

Lemme 3.2. Le code C est cyclique si et seulement si l'ensemble $\overline{C(X)}$ est un idéal de $R_n[X]$.

Preuve $\Leftarrow$ On suppose que l'ensemble $\overline{C(X)}$ est un idéal de $R_n[X]$. Alors pour tous $u \in \overline{C(X)}$ et $a \in R_n[X]$, on a $au \in \overline{C(X)}$ et, en prenant $a = X$, on obtient $Xu \in \overline{C(X)}$. Il suffit ensuite de prendre $u = c \in C$ ce qui montre que le code C est cyclique.

$\Rightarrow$ On suppose que le code C est cyclique. Pour tout $u \in \overline{C(X)}$, la cyclicité assure $Xu \in \overline{C(X)}$, puis $X^2u \in \overline{C(X)}$ et, en répétant cela, on obtient $\overline{X^iu} \in \overline{C(X)}$ pour tout $i \in \mathbf{N}$. Comme le code est linéaire, tout polynôme multiplié par le polynôme u est donc dans $\overline{C(X)}$. Ce dernier ensemble est ainsi un idéal de $R_n[X]$. □

Théorème 3.3. Soit C un code linéaire cyclique de longueur n sur $\mathbf{F}_q$. Soit $g(X)$ un polynôme unitaire de plus petit degré dans $C(X)$. Soit $r \coloneqq \deg g(X)$. Alors

1. pour tout $c \in C$, on a $g(X) \mid c(X)$ dans $\mathbf{F}_q[X]$;
2. le polynôme $g(X)$ est l'unique polynôme unitaire de degré r dans $C(X)$;
3. on a $g(X) \mid X^n - 1$ dans $\mathbf{F}_q[X]$.

On dit que le polynôme $g(X)$ génère le code C et on note $C = \langle g\rangle_n$.

Preuve 1. Soit $c \in C$. Comme $\mathbf{F}_q$ est un corps, on peut effectuer la division euclidienne de $c(X)$ par $g(X)$: il existe deux polynômes $Q(X)$ et $R(X)$ tels que

$$c(X) = g(X)Q(x) + R(x) \quad \text{avec} \quad \deg R < r.$$

Comme $\overline{g(X)} \in \overline{C(X)}$, on a $\overline{c(X)} - \overline{Q(X)} \cdot \overline{g(X)} = \overline{R(X)} \in \overline{C(X)}$. Comme $\deg R < r < n$, on a nécessairement $R(X) \in C(X)$, donc $R(X) = 0$ ou $\deg R \geqslant r$, donc $R(X) = 0$. D'où $g(X) \mid c(X)$.

2. Soit $g'(X) \in C(X)$ un polynôme unitaire de degré r. Alors $\overline{g(X) - g'(X)} \in \overline{C(X)}$, donc $g - g' = 0$ ou $\deg(g - g') \geqslant r$. Comme les polynômes g et g' sont unitaires et de degré r, on a $\deg(g - g') < r$, donc $g = g'$.

3. Effectuons la division euclidienne de $X^n - 1$ par $g(X)$: on écrit

$$X^n - 1 = g(X)Q(X) + R(X) \quad \text{avec} \quad \deg R < r.$$

En passant au quotient, on obtient $\overline{R(X)} = -\overline{g(X)} \cdot \overline{Q(X)} \in \overline{C(X)}$, donc $R(X) \in C(X)$, donc $R = 0$ ou $\deg R \geqslant r$, donc $R = 0$. D'où $g(X) \mid X_{n-1}$. □

Avec le théorème, si un code C est cyclique de longueur n et de polynôme générateur g, on peut donc écrire

$$\overline{C(X)} = \{c(X) \in R_n[X] \mid g(X) \mid c(X)\}.$$

▷ Exemples. – On reprend les exemples précédents. Comme les mots de C_2 correspondent respectivement aux polynômes

$$1 + X^2 = (X + 1)^2, \quad X + 1 \quad \text{et} \quad X + X^2 = X(X + 1),$$

on a $C_2 = \langle X + 1 \rangle_3$. De même, on trouve $C_3 = \langle X + 1 \rangle_n$.

– • *Codes de Reed-Solomon.* Soit $n \in \mathbf{N}^*$ un entier tel que $n \mid q - 1$. Soit $\alpha \in \mathbf{F}_q$ une racine n-ième de l'unité. On considère le code C de Reed-Solomon de localisateurs et de multiplicateurs

$$\alpha \coloneqq (1, \alpha, \ldots, \alpha^{n-1}) \quad \text{et} \quad v \coloneqq (1, \ldots, \alpha^b, \ldots, \alpha^{b(n-1)}).$$

Sa matrice de contrôle vaut

$$H = \begin{pmatrix} 1 & \alpha^b & \alpha^{2b} & \cdots & \alpha^{b(n-1)} \\ 1 & \alpha^{b+1} & \alpha^{2(b+1)} & \cdots & \alpha^{(n-1)(b+1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{b+d-1} & \alpha^{2(b+d-1)} & \cdots & \alpha^{(n-1)(b+d-2)} \end{pmatrix}.$$

Alors pour tout mot $c \in \mathbf{F}_q^n$, on a

$$\begin{aligned} c \in C \quad &\iff \quad H\,{}^{\mathrm{t}}c = 0 \\ &\iff \quad c(\alpha^b) = c(\alpha^{b+1}) = \cdots = c(\alpha^{b+d-1}) = 0 \\ &\iff \quad \forall i \in [\![0, d-2]\!], \quad X - a^{b+i} \mid c(X) \\ &\iff \quad \prod_{i=0}^{d-1} (X - \alpha^{b+1}) \mid c(X). \end{aligned}$$

Le code C est donc un code cyclique de longueur n et de polynôme générateur

$$g(X) \coloneqq \prod_{i=0}^{d-1} (X - \alpha^{b+1}).$$

– Quels sont les codes cycliques binaires de longueur 7 ? Pour répondre à cette question, on factorise le polynôme $X^7 + 1$ en produit d'irréductibles dans $\mathbf{F}_2[X]$: on trouve

$$X^7 + 1 = (X + 1)(X^3 + X + 1)(X^3 + X^2 + 1).$$

Ces facteurs génèrent tous les codes cycliques de longueur 7. On obtient huit codes.

3.2 Matrice génératrice

Soit $C \coloneqq \langle g \rangle_n$ un code cyclique. Trouvons sa matrice génératrice. On a

$$\begin{aligned} C(X) &= \{c(X) \in \mathbf{F}_q[X]_{<n} \mid g(X) \mid c(X)\} \\ &= \{m(X)g(X) \mid m(X) \in \mathbf{F}_q[X], \deg m(X) < k\} \quad \text{avec} \quad k \coloneqq n - r \\ &= \left\{ \sum_{i=0}^{k-1} m_i X^i g(X) \;\middle|\; m_0, \ldots, m_{k-1} \in \mathbf{F}_q^k \right\}. \end{aligned}$$

Ainsi une matrice génératrice est

$$G \coloneqq \begin{pmatrix} g_0 & g_1 & \cdots & g_r & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & \dots & g_r & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & & \ddots & 0 \\ 0 & \cdots & 0 & g_0 & g_1 & \cdots & g_r \end{pmatrix}$$

où $g_r = 1$. Cette matrice est bien de rang k.

3.3 Matrice de contrôle

DÉFINITION 3.4. Le *polynôme de contrôle* d'un code cyclique $C \coloneqq \langle g \rangle_n$ est le polynôme

$$h(X) \coloneqq \frac{X^n - 1}{g(X)}.$$

Pour un mot $c \in C$, on peut écrire $c(X) = m(X)g(X)$ avec $m \in \mathbf{F}_q[X]$ et on obtient

$$c(X)h(X) = m(X)g(X)h(X) \equiv 0 \mod X^n - 1.$$

PROPOSITION 3.5. Soit C un code cyclique $[n,k]_q$ de polynôme générateur g et de polynôme de contrôle $h \coloneqq X^k + \sum_{i=0}^{k-1} h_i X^i$. Alors une matrice de contrôle du code C est

$$H \coloneqq \begin{pmatrix} 1 & h_{k-1} & \cdots & h_0 & 0 & \cdots & 0 \\ 0 & 1 & h_{k-1} & \dots & h_0 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & & \ddots & 0 \\ 0 & \cdots & 0 & 1 & h_{k-1} & \cdots & h_0 \end{pmatrix} \in \mathscr{M}_{n-k,n}(\mathbf{F}_q).$$

◇ REMARQUE. En particulier, son dual $C^\perp$ est cyclique et engendré par le polynôme $h^* \coloneqq X^k h(1/X)$.

Preuve Comme le rang de la matrice H vaut $n-k$, il suffit de montrer

$$\forall c \in C, \quad H\,{}^{\mathrm{t}}c = 0.$$

Soit $c \in C$. Alors $c(X)h(X) \equiv 0 \mod X^n - 1$, donc

$$\sum_{\ell=0}^{n-1+k} u_\ell X^\ell \equiv 0 \mod X^n - 1 \qquad \text{avec} \quad u_\ell \coloneqq \sum_{\substack{0 \leqslant j \leqslant k \\ 0 \leqslant \ell - j < n}} h_j c_{\ell - j}.$$

Réécrivons cette congruence. Modulo $X^n - 1$, on obtient

$$\begin{aligned} \sum_{\ell=0}^{n-1+k} u_\ell X^\ell &\equiv \sum_{\ell=0}^{n-1} u_\ell X^\ell + \sum_{\ell=n}^{n+k-1} u_\ell X^\ell \\ &\equiv \sum_{\ell=0}^{n-1} u_\ell X^\ell + \sum_{\ell=0}^{k-1} u_{\ell+n} X^{\ell+n} \\ &\equiv \sum_{\ell=k}^{n-1} u_\ell X^\ell + \sum_{\ell=0}^{k-1} (u_\ell + u_{\ell+n}) X^\ell. \end{aligned}$$

Comme ce dernier polynôme est de degré strictement inférieur à n, c'est même une égalité, *i. e.*

$$\sum_{\ell=k}^{n-1} u_\ell X^\ell + \sum_{\ell=0}^{k-1} (u_\ell + u_{\ell+n}) X^\ell = 0.$$

On exploite alors la nullité de ses coefficients et on en déduit que, pour tout $\ell \in [\![k, n-1]\!]$, on a

$$u_\ell = 0, \quad \textit{i. e.} \quad \sum_{j=0}^{k} h_j c_{\ell - j} = 0.$$

Ceci montre exactement $H\,{}^{\mathrm{t}}c = 0$. □

▷ Exemple. Considérons le code $C \coloneqq \langle X^3 + X + 1 \rangle_7$ sur $\mathbf{F}^2$. Comme le polynôme $X^7 + 1$ se factorise en

$$X^7 + 1 = (X + 1)(X^3 + X + 1)(X^3 + X^2 + 1).$$

Le polynôme de contrôle est donc

$$h(X) \coloneqq \frac{X^7 + 1}{X^3 + X + 1} = X^4 + X^2 + X + 1.$$

On obtient alors une matrice génératrice et une matrice de contrôle

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

3.4 Polynômes minimaux et factorisation de $X^n - 1$ sur $\mathbf{F}_q$

On va exploiter le fait qu'on ait une bijection entre l'ensemble des codes cycliques $[n, k]_q$ et l'ensemble des diviseurs de $X^n - 1$ de degré $n - k$ sur $\mathbf{F}_q$. Dans la suite, on suppose $\operatorname{pgcd}(n, q) = 1$. Ceci assure que les polynômes $X^n - 1$ et nX^{n-1} sont premiers entre eux, *i. e.* le polynôme $X^n - 1$ est sans facteur carré.

Soit α une racine primitive n-ième de l'unité dans $\mathbf{F}_{q^m}^\times$ où l'entier $m \in \mathbf{N}^*$ est le plus petit entier tel que $n \mid q^m - 1$. Alors on peut écrire

$$X^n - 1 = \prod_{i=0}^{n-1} (X - \alpha^i) \in \mathbf{F}_{q^m}[X].$$

Définition 3.6. La *q-classe cyclotomique modulo* n d'un entier $s \in [\![0, n-1]\!]$ est l'ensemble

$$C_s \coloneqq \{s \mod n, sq \mod n, sq^2 \mod n, \ldots, sq^{m_s - 1} \mod n\} \subset \mathbf{N}$$

où l'entier m_s est le plus petit entier tel que $sq^{m_s} \equiv s \mod n$.

Les classes C_s forment une partition de l'ensemble $[\![0, n-1]\!]$ et on a

$$X^n - 1 = \prod_s M_{a^s}(X) \quad \text{avec} \quad M_{\alpha^s}(X) \coloneqq \prod_{i \in C_s} (X - \alpha^i)$$

où l'entier $s \in [\![0, n-1]\!]$ parcourt l'ensemble des représentants des classes cyclotomiques.

Proposition 3.7. Les polynômes $M_{\alpha^s}(X)$ sont irréductibles sur $\mathbf{F}_q$.

Preuve Soit $s \in [\![0, n-1]\!]$. Montrons d'abord que $M_{\alpha^s}(X) \in \mathbf{F}_q[X]$. On note

$$M_{\alpha^s}(X) = \sum_{i=0}^{m_s} a_i X^i \quad \text{avec} \quad a_i \in \mathbf{F}_{q^m}[X].$$

On cherche à montrer que, pour tout $i \in [\![0, m_s]\!]$, on a $a_i \in \mathbf{F}_q$, c'est-à-dire $a_i^q = a_i$. Il suffit en fait de montrer $M_{\alpha^s}(X)^q = M_{\alpha^s}(X^q)$ puisque

$$M_{\alpha^s}(X)^q = \Big(\sum_{i=0}^{m_s} a_i X^i\Big)^q = \sum_{i=0}^{m_s} a_i^q X^{qi} \quad \text{et} \quad M_{\alpha^s}(X^q) = \sum_{i=0}^{m_s} a_i (X^q)^i = \sum_{i=0}^{m_s} a_i X^{q_i}.$$

Alors on trouve

$$\begin{aligned} M_{\alpha^s}(X)^q &= \prod_{i \in C_s} (X - \alpha^i)^q \\ &= \prod_{i \in C_s} (X^q - \alpha^{iq}) \\ &= \prod_{i \in C_s} (X^q - \alpha^{iq \mod n}) \qquad (\text{car } \alpha^n = 1) \end{aligned}$$

$$= \prod_{j \in C_s} (X^q - \alpha^j) = M_{\alpha^s}(X^q).$$

Ceci conclut que $M_{\alpha^s}(X) \in \mathbf{F}_q[X]$.

Montrons maintenant que le polynôme $M_{\alpha^s}(X)$ est irréductible sur $\mathbf{F}_q$. Soit $f \in \mathbf{F}_q[X]$ un polynôme irréductible unitaire divisant $M_{\alpha^s}(X)$ tel que $f(\alpha^s) = 0$. Alors on trouve $f(\alpha^s)^q = 0$, donc $f(\alpha^{sq}) = 0$. En itérant ce calcul, on obtient

$$f(\alpha^s) = f(\alpha^{sq}) = \cdots = f(\alpha^{sq^{m_s - 1}}),$$

donc $M_{\alpha^s}(X) \mid f(X)$. D'où $f(X) = M_{\alpha^s}(X)$. Ceci montre que le polynôme $M_{\alpha^s}(X)$ est irréductible sur $\mathbf{F}_q$. □

Corollaire 3.8. Le polynôme $X^n - 1$ se factorise sur $\mathbf{F}_q$ sous la forme

$$X^n - 1 = \prod_s M_{\alpha^s}(X).$$

▷ Exemple. Factorisons le polynôme $X^7 + 1$ sur $\mathbf{F}_2$. Le plus petit entier $m \in \mathbf{N}$ tel que $7 \mid 2^m - 1$ est $m = 3$. On se place alors sur le corps

$$\mathbf{F}_{2^3} \simeq \mathbf{F}_2[X]/\langle X^3 + X + 1 \rangle.$$

Soit $\alpha \in \mathbf{F}_{2^3}$ un élément tel que $\alpha^3 + \alpha + 1 = 0$. Comme $\alpha^7 = 1$ et l'entier 7 est premier, l'élément α est une racine primitive septième de l'unité. De plus, on a trois classes cyclotomiques modulo 7

$$C_0 = \{0\}, \quad C_1 = \{1, 2, 4\} \quad \text{et} \quad C_3 \coloneqq \{3, 6, 5\}.$$

On obtient alors la factorisation

$$\begin{aligned} X^7 + 1 &= (X - \alpha^0) \times (X - \alpha)(X - \alpha^2)(X - \alpha^4)) \times [(X - \alpha^3)(X - \alpha^5)(X - \alpha^6) \\ &= (X + 1) \times (X^3 + X + 1) \times (X^3 + X^2 + 1). \end{aligned}$$

Chapitre 4

Codes BCH

4.1 Une famille de codes 2-correcteurs d'erreurs

4.1.1 Un premier code

Soient $r \in \mathbf{N}^*$ et $n \coloneqq 2^r - 1$. Soit $\alpha \in \mathbf{F}_{2^r}$ une racine primitive n-ième de l'unité. Soit C le code binaire de longueur n et de matrice de contrôle

$$H \coloneqq (H_0 \quad \cdots \quad H_{n-1}) \in \mathscr{M}_{r,n}(\mathbf{F}_2)$$

où, pour tout indice $i \in [\![0, n]\!]$, la i-colonne H_i est le vecteur des coordonnées de l'élément α^i dans la base $(1, \alpha, \ldots, \alpha^{r-1})$. Caractérisons les mots de ce code. Soit $c \coloneqq (c_0, \ldots, c_{n-1}) \in \mathbf{F}_2^n$. Alors

$$\begin{aligned} c \in C &\iff H\,{}^{\mathrm{t}}c = 0 \\ &\iff c_0 H_0 + \cdots + c_{n-1} H_{n-1} = 0 \\ &\iff c_0 \alpha^0 + \cdots + c_{n-1}\alpha^{n-1} = 0 \\ &\iff c(\alpha) = 0 \\ &\iff c(\alpha) = c(\alpha^2) = \cdots = c(\alpha^{2^{n-1}}) = 0 \\ &\iff M_\alpha(X) \mid c(X) \end{aligned}$$

où les polynômes $c(X)$ et $M_\alpha(X)$ ont été définis dans le chapitre précédent. Ainsi le code C est le code cyclique binaire de longueur n et de polynôme générateur $P(X) \coloneqq M_\alpha(X)$.

Voyons un algorithme de décodage. Soit $y = c + e$ avec $c(X) = m(X)P(X)$ et $w_{\mathrm{H}}(e) \leqslant 1$. Cette dernière condition dit que le polynôme $e(X)$ est soit nul soit égale à un monôme X^j. Avec notre caractérisation, on a

$$y(\alpha) = e(\alpha) = \begin{cases} 0 & \text{si } e = 0, \\ \alpha^j & \text{sinon.} \end{cases}$$

On peut alors en déduire un algorithme.

Entrée : un mot $y = c + e$ avec $c(X) = m(X)P(X)$ et $w_{\mathrm{H}}(e) \leqslant 1$
Sortie : le polynôme $m(X)$

```
S ⟵ y(α)
Si s = 0, alors
    Rendre y(X)/P(X)
Sinon
    Déterminer l'indice j ∈ [[0, n − 1]] tel que S = α^j
    Rendre (y(X) − X^j)/P(X).
```

4.1.2 Un second code

Soit C le code cyclique binaire de longueur n et de polynôme générateur $G(X) \coloneqq M_\alpha(X)M_{\alpha^3}(X)$. Autrement dit, pour un mot $c \in \mathbf{F}_2^n$, on a

$$c \in C \iff c(\alpha) = c(\alpha^3) = 0.$$

Trouvons également un algorithme de décodage. Soit $y = c+e$ avec $c(X) = m(X)G(X)$ et $w_{\mathrm{H}}(e) \leqslant 2$. En procédant identiquement, on obtient

$$S_1 \coloneqq y(\alpha) = e(\alpha) \quad \text{et} \quad S_3 \coloneqq y(\alpha^3) = e(\alpha^3).$$

On distingue maintenant trois cas.

– Si $w_{\mathrm{H}}(e) = 0$, alors $S_1 = S_3 = 0$.
– Si $w_{\mathrm{H}}(e) = 1$, alors on peut écrire $e(X) = X^j$ et on a $S_1 = \alpha^j$ et $S_3 = \alpha^{3j} = S_1^3$.
– On suppose désormais $w_{\mathrm{H}}(e) = 2$. On peut écrire $e(X) = X^i + X^j$ avec $i \neq j$. Alors $S_1 = \alpha^i + \alpha^j$ et $S_3 = \alpha^{3i} + \alpha^{3j}$. Comme on est en caractéristique deux, on a

$$\begin{aligned} S_1^3 &= \alpha^{3i} + \alpha^{2i}\alpha^j + \alpha^i\alpha^{2j} = \alpha^{3j} \\ &= S_3 + \alpha^i\alpha^j S_1. \end{aligned}$$

En notant $\sigma(Z) \coloneqq Z^2 + S_1 Z + (S_1^3 + S_3)/S_1 \in \mathbf{F}_{2^r}[Z]$, on a $\sigma(\alpha^i) = \sigma(\alpha^j) = 0$.

On en déduit l'algorithme

Entrée : un mot $y = c + e$ avec $c(X) = m(X)P(X)$ et $w_{\mathrm{H}}(e) \leqslant 1$
Sortie : le polynôme $m(X)$

```
S_1 ⟵ y(α)
S_3 ⟵ y(α^3)
Si S_1 = S_3 = 0, alors
    Rendre y(X)/G(X)
Si S_3 = S_1^3, alors
    Déterminer l'indice j ∈ ⟦0, n−1⟧ tel que S_1 = α^j
    Rendre (y(X) − X^j)/G(X)
Sinon
    σ(Z) ⟵ Z^2 + S_1 Z + (S_1^3 + S_3)/S_1
    Déterminer les indices i, j ∈ ⟦0, n−1⟧ avec i ≠ j tels que σ(α^i) = σ(α^j) = 0
    Rendre (y(X) − X^i − X^j)/G(X).
```

◇ Remarque. En fait, les polynômes $P(X)$ et $G(X)$ n'ont pas été choisis au hasard : ils vérifient

$$\begin{aligned} P(X) &= M_\alpha(X) = \mathrm{ppcm}(M_\alpha(X), M_{\alpha^2}(X)), \\ G(X) &= M_\alpha(X) M_{\alpha^3}(X) = \mathrm{ppcm}(M_\alpha(X), M_{\alpha^2}(X), M_{\alpha^3}(X), M_{\alpha^4}(X)). \end{aligned}$$

4.2 Définition et propriétés

Définition 4.1. Soit q une puissance d'un nombre premier. Soit $n \in \mathbf{N}^*$. On suppose $\mathrm{pgcd}(q, n) = 1$. Soit m l'ordre multiplicatif de q modulo n. Soit $\alpha \in \mathbf{F}_{q^m}$ un élément d'ordre multiplicatif m. Soient $b \in \mathbf{N}$ et $\delta \in [\![2, n]\!]$. Le code BCH de longueur n sur $\mathbf{F}_q$, associé à α et b, de distance prescrite δ est le code cyclique de longueur n sur $\mathbf{F}_q$ de polynôme générateur

$$\mathrm{ppcm}(M_{\alpha^b}(X), \ldots, M_{\alpha^{b+\delta-2}}(X)) \in \mathbf{F}_q[X].$$

Si $b = 1$, on dit que ce code est strict. Si $n = q^m - 1$, on dit que ce code est primitif.

▷ Exemple. On considère les codes BCH stricts primitifs binaires de longueur 15. Pour cela, on construit d'abord le corps $\mathbf{F}_{2^4}$ comme

$$\mathbf{F}_{2^4} \simeq \mathbf{F}_2[X]/\langle X^4 + X + 1\rangle.$$

Soit $\alpha \in \mathbf{F}_{2^4}$ le classe $\overline{X}$ dans $\mathbf{F}_{2^4}$. On vérifie qu'il s'agit bien d'une racine primitive quinzième de l'unité. On cherche les codes BCH stricts primitifs binaires associé à la racine α et de distance prescrite δ.

– Si $\delta = 2$, alors le polynôme générateur est $g \coloneqq M_\alpha$.
– Si $\delta = 3$, alors $g = \mathrm{ppcm}(M_\alpha, M_{\alpha^2}) = M_\alpha$.
– Si $\delta = 4$, alors $g = \mathrm{ppcm}(M_\alpha, M_{\alpha^2}, M_{\alpha^3})$. On calcule le polynôme M_{α^3}. Les 2-classes cyclotomiques modulo 15 sont

$$\begin{aligned} C(0) &= \{0\}, \\ C(1) &= \{1, 2, 4, 8\}, \\ C(3) &= \{3, 6, 12, 9\}, \\ C(5) &= \{5, 10\}, \end{aligned}$$

$$C(7) = \{7, 14, 13, 11\}.$$

On en déduit

$$\begin{aligned} M_{\alpha^0} &= X + 1, \\ M_{\alpha^1} &= X^4 + X + 1, \\ M_{\alpha^3} &= X^4 + X^3 + X^2 + X + 1, \\ M_{\alpha^5} &= X^2 + X + 1, \\ M_{\alpha^7} &= X^4 + X^3 + 1. \end{aligned}$$

Finalement, on trouve $g = (X^4 + X + 1)(X^4 + X^3 + X^2 + X + 1)$.
– Si $\delta \in \{6, 7\}$, alors $g = (X^4 + X + 1)(X^4 + X^3 + X^2 + X + 1)(X^2 + X + 1)$.
– Si $\delta \in \{8, \dots, 15\}$, alors $g = X^{14} + \cdots + X + 1$.

THÉORÈME 4.2 *(de la borne BCH).* Un code BCH de distance prescrite δ est de distance minimale supérieure ou égale à δ.

Preuve Raisonnons par l'absurde et supposons que le code possède un mot c de poids $w \in [\![1, \delta - 1]\!]$. Notons

$$c(X) = c_{a_1} X^{a_1} + \cdots + c_{a_w} X^{a_w}.$$

On sait que $c(\alpha^b) = \cdots = c(\alpha^{b+\delta-2}) = 0$, donc $c(\alpha^b) = \cdots = c(\alpha^{b+w-1}) = 0$. Sous forme matricielle, ces dernières égalités s'écrivent

$$\begin{pmatrix} \alpha^{ba_1} & \cdots & \alpha^{ba_w} \\ \alpha^{(b+1)a_1} & \cdots & \alpha^{(b+1)a_w} \\ \vdots & \ddots & \vdots \\ \alpha^{(b+w-1)a_1} & \cdots & \alpha_{(b+w-1)a_w} \end{pmatrix} \begin{pmatrix} c_{a_1} \\ c_{a_2} \\ \vdots \\ c_{a_w} \end{pmatrix} = 0.$$

Pour $i \in [\![1, w]\!]$, on note $\rho_i \coloneqq \alpha^{a_i}$. Alors

$$A \begin{pmatrix} c_{a_1} \\ c_{a_2} \\ \vdots \\ c_{a_w} \end{pmatrix} = 0 \qquad \text{avec} \qquad A \coloneqq \begin{pmatrix} 1 & \cdots & 1 \\ \rho_1 & \cdots & \rho_w \\ \vdots & \ddots & \vdots \\ \rho_1^{w-1} & \cdots & \rho_w^{w-1} \end{pmatrix} \begin{pmatrix} \rho_1^b & & & \\ & \rho_2^b & & \\ & & \ddots & \\ & & & \rho_w^b \end{pmatrix}.$$

Or les éléments ρ_i sont tous non nuls, donc la matrice A est inversible ce qui conduit à avoir $c = 0$. Ceci étant impossible par hypothèse, le code ne possède pas de mots de poids inférieur strictement à la distance prescrite δ. □

4.3 Algorithme de décodage des codes BCH

Soit C un code BCH strict sur $\mathbf{F}_q$, de longueur n, de distance prescrite $\delta \coloneqq 2t + 1$ et associé à une racine primitive n-ième $\alpha \in \mathbf{F}_{q^m}$ de l'unité. C'est le code cyclique de longueur n généré par le polynôme

$$g \coloneqq \operatorname{ppcm}(M_\alpha(X), \dots, M_{\alpha 2t}(X)) \in \mathbf{F}_q[X].$$

Soit $y \coloneqq mg + e$ avec $m, e \in \mathbf{F}_q[X]$, $\deg m + \deg g < n$, $\deg e < n$ et $r \coloneqq w_{\mathrm{H}}(e) \leqslant t$. On cherche le mot m tout en connaissant le mot y. Notons

$$e = \sum_{j=1}^{r} Y_j x^{i_j} \quad \text{avec} \quad 0 \leqslant i_1 < \cdots < i_r \leqslant n - 1 \quad \text{et} \quad Y_j \in \mathbf{F}_q^\times.$$

DÉFINITION 4.3. Le *polynôme syndrome* associé au mot y est

$$S(z) \coloneqq \sum_{j=1}^{2t} S_j z^{j-1} \in \mathbf{F}_{q^m}[z]$$

où $S_j := y(\alpha^j)$ pour tout $j \in [\![1, 2t]\!]$. Le *polynôme localisateur d'erreurs* est

$$\sigma(z) := \prod_{j=1}^{r}(1 - X_j z).$$

On remarque qu'il est de degré inférieur à égal à la capacité de correction t. Le *polynôme évaluateur d'erreurs* est

$$w(z) := \sum_{i=1}^{r} X_i Y_i \frac{\sigma(z)}{1 - X_i z}.$$

THÉORÈME 4.4 *(équation clé).* On a

$$S(z)\sigma(z) \equiv w(z) \mod z^{2t}.$$

Preuve On a

$$\begin{aligned} S(z)\sigma(z) &= \sigma(z) \sum_{j=1}^{2t} \Big(\sum_{i=1}^{r} Y_i X_i^j \Big) z^{j-1} \\ &= \sum_{i=1}^{r} X_i Y_i \sum_{j=1}^{2t} (X_i z)^{j-1} \sigma(z). \end{aligned}$$

Or

$$(1 - X_i z) \sum_{j=1}^{2t} (X_i z)^{j-1} \equiv 1 \mod z^{2t}.$$

On en déduit

$$\begin{aligned} S(z)\sigma(z) &\equiv \sum_{i=1}^{r} X_i Y_i \frac{\sigma(z)}{1 - X_i z} \mod z^{2t} \\ &\equiv w(z) \mod z^{2t}. \end{aligned}$$

□

L'idée de l'algorithme est d'utiliser l'algorithme d'Euclide étendu pour trouver une identité de Bézout, celle apparaissant dans l'équation clé.

THÉORÈME 4.5 *(algorithme d'Euclide étendu).* Soient $a, b \in \mathbf{F}_{q^m}[z]$ deux polynômes non tous nuls. On considère les suites $(r_i)_{i\in\mathbf{N}}$, $(u_i)_{i\in\mathbf{N}}$ et $(v_i)_{i\in\mathbf{N}}$ de $\mathbf{F}_{q^m}[z]$ telles que

- on ait $(r_0, r_1, u_0, u_1, v_0, v_1) = (a, b, 1, 0, 0, 1)$;
- pour tout $i \in \mathbf{N}$, si $r_i \neq 0$,
  - le polynôme r_{i+1} est le reste de la division euclidienne de r_{i-1} par r_i ;
  - on ait $u_{i+1} = u_{i-1} - q u_i$ et $v_{i+1} = v_{i-1} - q v_i$ où le polynôme q est le reste.

Soit $N \in \mathbf{N}$ le plus petit entier tel que $r_{N+1} = 0$. Alors

- $r_N = \operatorname{pgcd}(a, b)$;
- pour tout $i \in [\![0, N+1]\!]$, on a $r_i = a u_i + b v_i$;
- pour tout $i \in [\![0, N+1]\!]$, on a $\deg v_i = \deg a - \deg r_{i-1}$;
- pour tout $i \in [\![0, N+1]\!]$, les polynômes u_i et v_i sont premiers entre eux.

Preuve On l'admet. □

THÉORÈME 4.6. On considère les suites $(r_i)_{i\in\mathbf{N}}$, $(u_i)_{i\in\mathbf{N}}$ et $(v_i)_{i\in\mathbf{N}}$ de $\mathbf{F}_{q^m}[z]$ associées aux polynômes z^{2t} et $S(z)$. Soit $j \in \mathbf{N}$ un entier tel que $\deg r_{j-1} \geqslant t$ et $\deg r_j < t$. Alors

$$\sigma(z) = \frac{v_j(z)}{v_j(0)} \quad \text{et} \quad w(z) = \frac{r_j(z)}{v_j(0)}.$$

Preuve Grâce au précédent théorème, on trouve

$$r_j(z) = z^{2t} u_j(z) + S(z) v_j(z),$$

$$w(z) = z^{2t}\lambda(z) + S(z)\sigma(z) \quad \text{avec} \quad \lambda \in \mathbf{F}_{q^m}[z].$$

Une combinaison linéaire donne alors

$$r_j(z)\sigma(z) - v_j(z)w(z) = z^{2t}(u_j(z)\sigma(z) - \lambda(z)v_j(z)).$$

On sait que

$$\deg r_j < t, \quad \deg \sigma \leqslant t \quad \text{et} \quad \deg w < t.$$

De plus, ce même théorème donne $\deg v_j = \deg z^t - \deg r_{j-1} \leqslant t$. Par conséquent, le polynôme z^{2t} divise le polynôme $r_j(z)\sigma(z) - v_j(z)w(z)$ qui est de degré strictement inférieur à $2t$. On en déduit

$$r_j(z)\sigma(z) - v_j(z)w(z) = 0 \quad \text{et} \quad u_j(z)\sigma(z) - \lambda(z)v_j(z) = 0. \qquad (*)$$

Ceci donne $\sigma(z) \mid v_j(z)w(z)$. Or on remarque que les polynômes $\sigma(z)$ et $w(z)$ sont premiers entre eux, donc le lemme de Gauss implique $\sigma(z) \mid v_j(z)$. De même, grâce à la seconde égalité $(*)$, on trouve $v_j(z) \mid \sigma(z)$. On peut alors trouver un élément $\mu \in \mathbf{F}_{q^m}$ tel que $\sigma(z) = \mu v_j(z)$. Or $\sigma(0) = 1$, donc $\mu = 1/v_j(0)$. Avec les égalités $(*)$, on trouve également $w(z) = r_j(z)/v_j(0)$. ce qui conclut. □

On peut à présent donner un algorithme de décodage basé sur ce théorème.

Entrée : des polynômes y et g, une racine α et un entier t avec $y = mg + e$ et $w_{\mathrm{H}}(e) \leqslant t$
Sortie : le polynôme m

> $S_i \longleftarrow y(\alpha^i)$ pour $i \in [\![1, 2t]\!]$
> $S \longleftarrow \sum_{i=1}^{2t} S_i z^{i-1}$
> Déterminer les polynômes σ et w solutions de l'équation clé avec l'algorithme d'Euclide étendu
> Calculer les entiers $i_1, \ldots, i_r \in [\![0, n-1]\!]$ tels que $\sigma(\alpha^{-i_j}) = 0$ pour tout $j \in [\![1, r]\!]$
> Calculer les éléments $Y_1, \ldots, Y_r$ à l'aide du polynôme w
> $e \longleftarrow \sum_{j=1}^{r} Y_j X^{i_j}$
> $c \longleftarrow y - e$
> Retourner c/g

▷ Exemple. On considère un code BCH strict de longueur 15, de distance prescrite 5, binaire et associé à une racine primitive quinzième $\alpha \in \mathbf{F}_{2^4}$ de l'unité définie par la relation $\alpha^4 + \alpha^3 + 1 = 0$. Son polynôme générateur est

$$g \coloneqq \mathrm{ppcm}(M_\alpha, M_{\alpha^2}, M_{\alpha^3}, M_{\alpha^4}).$$

Comme on est en caractéristique deux, les trois polynômes M_α, M_{α^2} et M_{α^4} sont tous égaux au polynôme $X^4 + X^3 + 1$. De plus, l'élément α^3 est une racine du polynôme

$$X^5 - 1 = (X - 1)(X^4 + X^3 + X^2 + X + 1).$$

Comme $\alpha^3 \neq 1$, on en déduit $M_{\alpha^3} = X^4 + X^3 + X^2 + X + 1$. D'où

$$g = (X^4 + X^3 + 1)(X^4 + X^3 + X^2 + X + 1).$$

On considère le mot reçu

$$y \coloneqq X^{12} + X^{11} + X^8 + X^7 + X^6 + X^5 + X^4 + 1.$$

On peut l'écrire sous la forme $y = mg + e$ avec $w_{\mathrm{H}}(e) \leqslant 2$ et $\deg m < 7$.

Appliquons le premier algorithme de décodage trouvé (cf. page 19), spécifique au cas $t = 2$. On calcul $S_1 \coloneqq y(\alpha) = \alpha^5$ et $S_3 \coloneqq y(\alpha^3) = \alpha^{13}$. Le polynôme

$$P(z) \coloneqq z^2 + S_1 z + \frac{S_3 + S_1^3}{S_1} = z^2 + \alpha^5 z + \alpha^2$$

admet les éléments α^8 et α^9 pour racines. On en déduit $e = X^8 + X^9$.

Chapitre 5

Codes de Goppa

5.1 Définition et matrice de contrôle

Soient $n, m \in \mathbf{N}^*$ et q une puissance d'un nombre premier.

Définition 5.1. Soit $L \coloneqq (\gamma_0, \dots, \gamma_{n-1}) \in \mathbf{F}_{q^m}^n$ un n-uplet tel que les éléments γ_i soient distincts deux à deux. Soit $g \in \mathbf{F}_{q^m}[z]$ un polynôme tel que $g(\gamma_i) \neq 0$ pour tout $i \in [\![0, n-1]\!]$. Le *code de Goppa* de support L et de polynôme de Goppa g est l'ensemble

$$\Gamma(L, g) \coloneqq \Big\{(c_0, \dots, c_{n-1}) \in \mathbf{F}_q^n \;\Big|\; \sum_{i=0}^{n-1} c_i \frac{1}{z - \gamma_i} \equiv 0 \mod g\Big\}.$$

▷ Exemple. Soit $\alpha \in \mathbf{F}_{2^3}$ tel que $\alpha^3 + \alpha + 1 = 0$. Les coordonnées du vecteur $L \coloneqq (1, \alpha, \alpha^2, \alpha^4)$ sont deux à deux distinctes. On considère le polynôme $g \coloneqq z - \alpha^3$. Pour tout $i \in \{0, 1, 2, 4\}$, on a

$$g(z) = z - \alpha^i + g(\alpha^i), \quad \text{donc} \quad \frac{1}{g(\alpha^i)}(z - \alpha^i) \equiv 0 \mod g.$$

On en déduit que les inverses des polynômes $z - \alpha^i$ modulo g sont

$$\begin{aligned} z - 1 &\longleftrightarrow \alpha^6 && \text{car } g(1) = \alpha, \\ z - \alpha &\longleftrightarrow 1 && \text{car } g(\alpha) = 1, \\ z - \alpha^2 &\longleftrightarrow \alpha^2 && \text{car } g(\alpha^2) = \alpha^5, \\ z - \alpha^3 &\longleftrightarrow \alpha && \text{car } g(\alpha^6) = \alpha^6. \end{aligned}$$

Pour tout mot $c \coloneqq (c_0, c_1, c_2, c_3) \in \mathbf{F}_2^4$, on obtient alors

$$c \in \Gamma(L, g) \iff c_0\alpha^6 + c_1 + c_2\alpha^2 + c_3\alpha = 0.$$

Théorème 5.2. On a

$$\Gamma(L, g) = \{c \in \mathbf{F}_q^n \mid \tilde{H}\,{}^{\mathrm{t}}c = 0\}$$

où $\tilde{H} \coloneqq VD \in \mathscr{M}_{r,m}(\mathbf{F}_{q^m})$ avec $r \coloneqq \deg G$ et

$$V \coloneqq \begin{pmatrix} 1 & \cdots & 1 \\ \gamma_0 & \cdots & \gamma_{n-1} \\ \vdots & \ddots & \vdots \\ \gamma_0^{r-1} & \cdots & \gamma_{n-1}^{r-1} \end{pmatrix} \quad \text{et} \quad D \coloneqq \operatorname{diag}(1/g(\gamma_0), \dots, 1/g(\gamma_{n-1})).$$

Autrement dit, on a

$$\Gamma(L, g) = \mathrm{GRS}_{n,n-r}(L, (1/g(\gamma_0), \dots, 1/g(\gamma_{n-1}))) \cap \mathbf{F}_q^n.$$

Preuve Soit $c \coloneqq (c_0, \dots, c_{n-1}) \in \mathbf{F}_q^n$. Pour tout $i \in [\![0, n-1]\!]$, on a

$$(z - \gamma_i)\frac{g(z) - g(\gamma_i)}{z - \gamma_i} \equiv -g(\gamma_i) \mod g,$$

donc

$$c \in \Gamma(L, g) \iff \sum_{i=0}^{n-1} c_i \frac{1}{z - \gamma_i} \equiv 0 \mod g$$

$$\iff \quad \underbrace{\sum_{i=0}^{n-1} c_i h_i \frac{g(z)-g(\gamma_i)}{z-\gamma_i}}_{\deg < \deg g} \equiv 0 \mod g \quad \text{avec} \quad h_i \coloneqq 1/g(\gamma_i)$$

$$\iff \quad \sum_{j=0}^{n-1} c_j h_j \frac{g(z)-g(\gamma_j)}{z-\gamma_j} = 0.$$

Notons le polynôme g sous la forme $g = \sum_{k=0}^{r} g_k z^k$ avec $g_r \neq 0$. Pour tout $j \in [\![0, n-1]\!]$, on a

$$\begin{aligned}\frac{g(z)-g(\gamma_j)}{z-\gamma_j} &= \sum_{k=0}^{r} g_k \frac{z^k-\gamma_j^k}{z-\gamma_j} \\ &= \sum_{k=0}^{r} g_k \sum_{i=0}^{k-1} z^i \gamma_i^{k-1-i} \\ &= \sum_{i=0}^{r-1} \Big(\sum_{k=i+1}^{r} g_k \gamma_j^{k-1-i} \Big) z^i.\end{aligned}$$

Il vient alors que

$$\begin{aligned} c \in \Gamma(L,g) \quad &\iff \quad \sum_{i=0}^{n-1} \Big(\sum_{j=0}^{n-1} \Big[\sum_{k=i+1}^{r} g_k \gamma_j^{k-1-i} \Big] h_j c_j \Big) z^i = 0 \\ &\iff \quad \forall i \in [\![0, r-1]\!], \quad \sum_{j=0}^{n-1} \Big[\sum_{k=0}^{r-1-i} g_{k+i+1} \gamma_j^k \Big] h_j c_j = 0. \end{aligned}$$

Remarquons que le terme

$$\sum_{k=0}^{r-1-i} g_{k+i+1} \gamma_j^k$$

est le coefficient (i,j) de la matrice

$$G \coloneqq \begin{pmatrix} g_r & 0 & \cdots & \cdots & 0 \\ g_{r-1} & g_r & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ g_0 & \cdots & g_{r-1} & g_r & 0 \end{pmatrix} \begin{pmatrix} 1 & \cdots & 1 \\ \gamma_0 & \cdots & \gamma_{n-1} \\ \vdots & \ddots & \vdots \\ \gamma_0^{r-1} & \cdots & \gamma_{n-1}^{r-1} \end{pmatrix}$$

de telle sorte que

$$c \in \Gamma(L,g) \quad \iff \quad GVD\,{}^{\mathrm{t}}c = 0.$$

Or $g_r \neq 0$, donc la matrice est inversible et on a bien

$$c \in \Gamma(L,g) \quad \iff \quad H\,{}^{\mathrm{t}}c = 0. \qquad \square$$

▷ Exemple. Reprenons l'exemple précédent. En posant

$$V = (1 \quad 1 \quad 1 \quad 1) \quad \text{et} \quad D \coloneqq \operatorname{diag}(\alpha^6, 1, \alpha^2, \alpha),$$

une matrice de contrôle du code $\Gamma(L,g)$ est la matrice VD.

5.2 Distance minimale et dimension

Théorème 5.3. Le distance minimale $d \in \mathbf{N}^*$ du code $\Gamma(L,g)$ vérifie

$$d \geqslant r+1 \quad \text{avec} \quad r \coloneqq \deg g.$$

Preuve Le théorème précédent nous donne

$$\Gamma(L,g) = \mathrm{GRS}_{n,n-r}((\gamma_0, \ldots, \gamma_{n-1}), (h_0, \ldots, h_{n-1})) \cap \mathbf{F}_q^n$$

où le code GRS, noté C, apparaissant est du type $[n, n-r, r+1]_q$. Comme $\Gamma(L,g) \subset C$, on obtient la conclusion. $\square$

THÉORÈME 5.4. Le dimension du code $k \in \mathbf{N}^*$ du code $\Gamma(L,g)$ vérifie

$$k \geqslant n - rm.$$

Preuve Reprenons sa matrice de contrôle $\tilde{H} \in \mathscr{M}_{r,n}(\mathbf{F}_{q^m})$. Elle est de rang r. Notons

$$\tilde{H} = (\tilde{H}_{i,j})_{0 \leqslant i \leqslant r-1, 0 \leqslant j \leqslant n-1}.$$

Soit $c \coloneqq (c_0, \ldots, c_{n-1}) \in \mathbf{F}_q^n$. Alors

$$c \in \Gamma(L,g) \quad \iff \quad \forall i \in [\![0, r-1]\!], \quad \sum_{j=0}^{n-1} \tilde{H}_{i,j} c_j = 0.$$

Soit $(\beta_0, \ldots, \beta_{m-1})$ une base du $\mathbf{F}_q$-espace vectoriel $\mathbf{F}_{q^n}$. Pour tous $i \in [\![0, r-1]\!]$ et $j \in [\![0, n-1]\!]$, on écrit

$$\tilde{H}_{i,j} = \sum_{\ell=0}^{m-1} \tilde{H}_{i,j,\ell} \beta_\ell.$$

On peut donc écrire

$$\begin{aligned} c \in \Gamma(L,j) \quad &\iff \quad \forall i \in [\![0, r-1]\!], \quad \sum_{\ell=0}^{m-1} \Big(\sum_{j=0}^{n-1} \tilde{H}_{i,j,\ell} c_j \Big) \beta_\ell = 0 \\ &\iff \quad \forall i \in [\![0, r-1]\!], \ \forall \ell \in [\![0, m-1]\!], \quad \sum_{j=0}^{n-1} \tilde{H}_{i,j,\ell} c_j = 0. \end{aligned}$$

Définissons la matrice par blocs

$$H \coloneqq \begin{pmatrix} (\tilde{H}_{0,j,\ell})_{0 \leqslant j \leqslant n-1, 0 \leqslant \ell \leqslant m-1} \\ \vdots \\ (\tilde{H}_{r-1,j,\ell})_{0 \leqslant j \leqslant n-1, 0 \leqslant \ell \leqslant m-1}. \end{pmatrix} \in \mathscr{M}_{mr,n}(\mathbf{F}_q).$$

de telle sorte que

$$c \in \Gamma(L,g) \quad \iff \quad H \, {}^{\mathrm{t}}c = 0.$$

Comme $\operatorname{rg} H \leqslant mr$, le théorème est montré. □

▷ EXEMPLE. On reprend l'exemple précédent. Une matrice de contrôle du code $\Gamma(L,g)$ est la matrice

$$\tilde{H} \coloneqq (\alpha^6 \quad 1 \quad \alpha^2 \quad \alpha).$$

La famille $(1, \alpha, \alpha^2)$ est une base du $\mathbf{F}_2$-espace vectoriel $\mathbf{F}_{2^3}$. Soit $c \coloneqq (c_0, c_1, c_2, c_3) \in \mathbf{F}_2^4$. Alors

$$\begin{aligned} c \in \Gamma(L,g) \quad &\iff \quad c_0 \alpha^6 + c_1 + c_2 \alpha^2 + c_3 \alpha = 0 \\ &\iff \quad c_0(1 + \alpha^2) + c_1 + c_2 \alpha^2 + c_3 \alpha = 0 \\ &\iff \quad (c_0 + c_1) + c_3 \alpha + (c_0 + c_2) \alpha^2 = 0 \\ &\iff \quad \begin{cases} c_0 + c_1 = 0, \\ \qquad c_3 = 0, \\ c_0 + c_2 = 0 \end{cases} \\ &\iff \quad \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \end{pmatrix} = 0 \end{aligned}$$

Remarquons que les colonnes de cette dernière matrice sont respectivement les coordonnées des vecteurs α^6, 1, α^2 et α. Finalement, on trouve

$$\Gamma(L,g) = \{(0,0,0,0), (1,1,1,0)\}.$$

PROPOSITION 5.5. On se place dans le cas $q = 2$ et on suppose que le polynôme est sans facteur

carré dans $\mathbf{F}_{2^m}[z]$ et de degré r. Alors la distance minimale $d \in \mathbf{N}^*$ du code $\Gamma(L, g)$ vérifie

$$d \geqslant 2r + 1.$$

Preuve Il suffit de montrer que $\Gamma(L, g) = \Gamma(L, g^2)$ et d'appliquer le théorème. Comme $g \mid g^2$, on peut écrire $\Gamma(L, g^2) \subset \Gamma(L, g)$. Montrons l'inclusion réciproque. Soit $c \coloneqq (c_0, \ldots, c_{n-1}) \in \Gamma(L, g)$. Alors

$$\sum_{i=0}^{n-1} c_i \frac{1}{z - \gamma_i} \equiv 0 \mod g.$$

On pose

$$f \coloneqq \prod_{c_i \neq 0} (z - \gamma_i).$$

En multipliant la dernière égalité par ce polynôme, on trouve

$$\sum_{c_i \neq 0} \frac{f}{z - \gamma_i} \equiv 0 \mod g,$$

donc $f' \equiv 0 \mod g$. La réciproque est également vraie. Cela implique $g \mid f'$. Écrivons

$$f = \sum_{i=0}^{d} a_i z^i.$$

En le dérivant, on obtient

$$f' = \sum_{0 \leqslant 2j+1 \leqslant d} a_{2j+1} z^{2j}.$$

Comme on travaille dans le corps $\mathbf{F}_{2^m}$, on a

$$\begin{aligned} f' &= \sum_{0 \leqslant 2j+1 \leqslant d} a_{2j+1}^{2^m} z^{2j} \\ &= \Big(\sum_{0 \leqslant 2j+1 \leqslant d} a_{2j+1}^{2^{m-1}} z^j \Big)^2. \end{aligned}$$

Ainsi le polynôme f' est un carré d'un polynôme et il est divisible par le polynôme g qui est sans facteur carré. Par conséquent, on a $g^2 \mid f'$, donc $c \in \Gamma(L, g^2)$ grâce à l'équivalence montrée précédemment. D'où $\Gamma(L, g) = \Gamma(L, g^2)$. Comme $\deg g^2 = 2r$, il ne reste plus qu'à utiliser le théorème précédent. □

5.3 Algorithme de décodage

Soient $L \coloneqq (\gamma_0, \ldots, \gamma_{n-1}) \in \mathbf{F}_{q_m}^n$ un n-uplet d'éléments deux à deux distincts et $g \in \mathbf{F}_{q^m}[z]$ un polynôme ne s'annulant sur aucun élément γ_i. On note $r \coloneqq \deg g$. On souhaite déterminer un algorithme de décodage pour le code

$$\Gamma(L, g) = \mathrm{GRS}_{n,n-r}(L, (1/g(\gamma_0), \ldots, 1/g(\gamma_{n-1}))) \cap \mathbf{F}_q^n.$$

On note $k \in \mathbf{N}$ sa dimension. Soient $m \in \mathbf{F}_q^k$ un mot, G une matrice génératrice du code et $e \in \mathbf{F}_q^n$ un mot tel que $w_{\mathrm{H}}(e) \leqslant \lfloor r/2 \rfloor$. On considère le mot

$$y \coloneqq mG + e = (y_0, \ldots, y_{n-1}).$$

Notons

– le polynôme syndrome du mot y

$$S \coloneqq \sum_{i=0}^{n-1} \frac{y_i}{z - \gamma_i} \mod g \ ;$$

– le polynôme localisateur d'erreurs

$$\sigma \coloneqq \prod_{i \in I} (z - \gamma_i) \quad \text{avec} \quad I \coloneqq \{i \in [\![1, n]\!] \mid e_i \neq 0\} \ ;$$

– le polynôme évaluateur d'erreurs

$$w \coloneqq \sum_{i\in I} e_i \prod_{\substack{j\in I\\ j\neq i}} (z-\gamma_j) = \sum_{i\in I} e_i \frac{\sigma}{z-\gamma_i}.$$

PROPOSITION 5.6. On a

$$\deg \sigma \leqslant t \coloneqq \lfloor r/2 \rfloor \quad \text{et} \quad \deg w < t.$$

De plus, pour tout indice $i \in I$, on a

$$w(\gamma_i) = e_i \prod_{j\neq i} (\gamma_i - \gamma_j).$$

En particulier, les polynômes σ et w sont premiers entre eux.

THÉORÈME 5.7 *(équation clef).* Ces polynômes vérifient

$$S\sigma \equiv w \mod g.$$

Preuve On calcul

$$\begin{aligned} S\sigma &\equiv \sum_{i=0}^{n-1} \frac{y_i}{z-\gamma_i}\sigma \mod g \\ &\equiv \Big(\sum_{i=0}^{n-1} \frac{c_i}{z-\gamma_i} + \sum_{i=0}^{n-1} \frac{e_i}{z-\gamma_i}\Big)\sigma \mod g \\ &\equiv \sum_{i\in I} \frac{e_i}{z-\gamma_i}\sigma \mod g \qquad \text{car } c \in \Gamma(L,g) \\ &\equiv w \mod g. \end{aligned}$$

□

Comme pour les codes GRS, on peut en déduire un algorithme de décodage utilisant l'équation clef et l'algorithme d'Euclide étendu.

Chapitre 6

Cryptosystème de McEliece

6.1 Cryptosystème à clef publique

On considère un envoyeur Alice et un destinateur Bob. On va supposer que le canal de transmission est parfait. Cependant, Charles peut écouter le canal. On souhaite alors crypter les messages de telle sorte que Charles ne puissent pas intercepté les messages.

Définition 6.1. Un *cryptosystème* est un 5-uplet (P, C, K, E, D) où
– l'élément P est un ensemble, appelé l'*espaces des messages en clair* ;
– l'élément C est un ensemble, appelé l'*espaces des messages chiffrés* ;
– l'élément K est un ensemble, appelé l'*espaces des clefs* ;
– l'élément E est une famille d'applications $E_k \colon C \to C$ indicée par l'ensemble K, appelées les *fonctions de chiffrement* ;
– l'élément D est une famille d'applications $D_k \colon C \to P$ indicée par l'ensemble K, appelées les *fonctions de déchiffrement*.

Étant donné un cryptosystème, à chaque clef $e \in K$ est associée une clef $d \in K$ telle que

$$\forall m \in P, \quad D_d(E_e(m)) = m.$$

L'utilisation des cryptosystèmes se déroulent entre quatre étapes :
– la construction des clefs ;
– le chiffrement : on transforme un message m en le message $c \coloneqq E_e(m)$;
– le déchiffrement : on transforme le message c en le message $D_d(c) = m$;
– la vérification de la sécurité.

6.2 Cryptosystème de McEliece

Génération des clefs. Soit C un code $[n, k, d]_q$ de matrice génératrice G décodant jusqu'à t erreurs en temps polynomial. Soient $S \in \mathrm{GL}_k(\mathbf{F}_q)$ une matrice inversible et $P \in \mathscr{M}_n(\mathbf{F}_q)$ une matrice de permutation. Notons

$$G' \coloneqq SGP \in \mathscr{M}_{k,n}(\mathbf{F}_q).$$

Cette matrice G' sera appelée la *clef publique* et le triplet (G, S, P) sera appelé la *clef privée*.

Chiffrement. Soit $m \in \mathbf{F}_q^k$ un mot représentant le message en clair. On lui associe le *cryptogramme* $c \coloneqq mG' + e$ avec $w_{\mathrm{H}}(e) \leqslant t$.

Déchiffrement. On calcul alors $cP^{-1} = (mS)G + eP^{-1}$ où le mot $(ms)G$ est dans le code C et le mot eP^{-1} est de poids $w_{\mathrm{H}}(e)$. On décode ainsi le mot $y \coloneqq cP^{-1}$ dans le code C et on retrouve le mot mS, puis le mot S puisque la matrice S est connue du destinataire.

◇ Remarque. Dans la pratique, on utilisera un code de Goppa irréductible

6.3 Exemple

Soit $a \in \mathbf{F}_{2^3}$ un élément tel que $a^3 = a+1$. Considérons le code $C \coloneqq \Gamma(L, z)$ avec $L \coloneqq (a, \dots, a^7)$. Ce code est l'ensemble des mots $c \in \mathbf{F}_2^7$ tels que $H\,{}^{\mathrm{t}}c = 0$ avec $\tilde{H} \coloneqq VD$ où

$$V = (1 \quad 1 \quad 1 \quad 1 \quad 1 \quad 1 \quad 1) \quad \text{et} \quad D \coloneqq \mathrm{diag}(a^6, a^5, a^4, a^3, a^2, a, 1).$$

Autrement dit, on a

$$\tilde{H} = (a^6 \quad a^5 \quad a^4 \quad a^3 \quad a^2 \quad a \quad 1).$$

On écrit maintenant les éléments a^i dans la base $(1, a, a^2)$ pour obtenir la matrice de contrôle

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

On en déduit une matrice génératrice

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

On considère maintenant les matrices

$$S \coloneqq \begin{pmatrix} 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix} \in \mathrm{GL}_4(\mathbf{F}_2) \quad \text{et} \quad P \coloneqq (2 \quad 6 \quad 1 \quad 7 \quad 3 \quad 4 \quad 5).$$

On calcule alors la matrice

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

La distance minimale du code C est supérieur à $1 + 2 \deg z = 3$ puisque le polynôme z est sans facteur carré et le code est binaire.

On considère le mot $m \coloneqq (1, 0, 1, 1)$. Pour l'erreur $e \coloneqq (0, 0, 0, 0, 1, 0, 0)$, le cryptogramme vaut

$$c \coloneqq mG' + e = (0, 1, 0, 0, 0, 0, 1).$$

On calcul le mot $y \coloneqq cP^{-1} = (0, 0, 0, 0, 1, 1, 0)$. Décodons-le avec l'algorithme d'Euclide étendu. Son syndrome vaut

$$\begin{aligned} S &= \sum_{i=0}^{6} \frac{y_i}{z - a^i} \mod z^2 \\ &= \frac{1}{z - a^5} + \frac{1}{z - a^6} \mod z^2 \\ &= \frac{z^2 - a^{10}}{z - a^5} \frac{1}{a^{10}} + \frac{z^2 - a^{12}}{z - a^6} \frac{1}{a^{12}} \\ &= (z + a^5)a^4 + (z + a^6)a^2 \\ &= az + a^4. \end{aligned}$$

Appliquons l'algorithme d'Euclide étendu aux polynômes z^2 et S. On a successivement

$$\begin{aligned} z^2 &= z^2 \times 1 + S \times 0, \\ S &= z^2 \times 0 + S \times 1, \\ a^6 &= z^2 \times 1 + S \times (a^6 z + a^2) \end{aligned}$$

de telle sorte que

$$S \times (z + a^3) \equiv 1 \mod z^2.$$

Le polynôme localisateur d'erreur est $\sigma \coloneqq z + a^3$. Comme $\sigma(a^3) = 0$, on en déduit

$$eP^{-1} = (0, 0, 1, 0, 0, 0, 0).$$

Comme $y = (mS)G + eP^{-1}$, on en déduit $(mS)G = (0, 0, 1, 0, 1, 1, 0)$, donc $mS = (0, 0, 1, 0)$ et on retrouve bien le mot m.

Pour l'attaquant, il est facile de retrouver le mot m à partir du mot intercepté c. En effet, on calcul une matrice de contrôle associé à la matrice G' qui est

$$H' \coloneqq \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

On trouve $H' \, {}^{\mathrm{t}}c = (1, 0, 0)$, donc l'erreur est en position 5.