Université Paris 8
A.A. 2021–2022

Codes Algébriques

Martino Borello

14 avril 2022

Table des matières

Chapitre 1

Codes cycliques

Les codes cycliques sont les codes classiques les plus étudiés de la théorie. Si l'on se donne une longueur n et un corps de base, on dispose d'un choix assez large de codes cycliques, déterminés alors selon leur capacité de correction et/ou leur dimension. Les codes cycliques contiennent les codes les plus performants au niveau des applications, les codes de Bose-Chaudhury-Hocquenghem (codes BCH), pour lesquels on dispose de bons algorithmes de décodage.

1.1 Rappel : Automorphismes et équivalences

Soit S_n le groupe de permutations de $\{1, \ldots, n\}$. On définit une action (à droite) de S_n sur $\mathbb{F}_q^n$, donnée pas

$$x^\sigma := (x_{\sigma^{-1}(1)}, \ldots, x_{\sigma^{-1}(n)})$$

pour tout $x = (x_1, \ldots, x_n) \in \mathbb{F}_q^n$ et $\sigma \in S_n$.

Exemple 1.1. $(x_1, x_2 \ldots, x_n)^{(1,2,\ldots,n)} = (x_n, x_1, \ldots, x_{n-1})$ (*SHIFT*).

Cette action induit une action sur les codes dans $\mathbb{F}_q^n$, donnée par

$$\mathcal{C}^\sigma = \{c^\sigma \mid c \in \mathcal{C}\}$$

pour $\mathcal{C} \subseteq \mathbb{F}_q^n$ et $\sigma \in S_n$.

On a déjà vu (dans le cours d'introduction à la théorie des codes) que

$$\mathrm{wt}(x^\sigma) = \mathrm{wt}(x)$$

pour tout $x \in \mathbb{F}_q^n$ et $\sigma \in S_n$, de manière que les permutations sont des isométries par rapport à la métrique de Hamming.

Définition 1.1. *Soit $\mathcal{C}$ un code dans $\mathbb{F}_q^n$. Un élément $\sigma \in S_n$ est un* automorphisme (*de permutation*) *de $\mathcal{C}$ si $\mathcal{C}^\sigma = \mathcal{C}$.*

L'ensemble $\mathrm{Aut}(\mathcal{C})$ des automorphismes d'un code $\mathcal{C}$ est un sous-groupe de S_n (exercice) appelé *groupe des automorphismes* (de permutation) de $\mathcal{C}$.

Définition 1.2. *Soient $\mathcal{C}_1$ et $\mathcal{C}_2$ deux codes dans $\mathbb{F}_q^n$. Ils sont* équivalents (*par permutation*) *s'il existe $\sigma \in S_n$ telle que*

$$\mathcal{C}_2 = \mathcal{C}_1^{\sigma}.$$

Notation : $\mathcal{C}_1 \sim \mathcal{C}_2$.

Cela est une relation d'équivalence (exercice).

Remarque 1.1. *On n'a pas donné la définition la plus générale d'automorphisme et d'équivalence. Il faudrait prendre en compte toutes les isométries, et non pas seulement les permutations. Toutefois, ces définitions suffisent pour notre cours.*

Exercice 1.1. *Soit $\mathcal{C}$ un code linéaire. Montrer que* $\mathrm{Aut}(\mathcal{C}) = \mathrm{Aut}(\mathcal{C}^{\perp})$.

1.2 Définition et propriétés

Définition 1.3. *Un code linéaire $\mathcal{C} \subseteq \mathbb{F}_q^n$ est* cyclique *si un mot du code shifté est encore un mot du code, i.e. si $(c_1, c_2, \ldots, c_n) \in \mathcal{C}$ implique $(c_n, c_1, \ldots, c_{n-1}) \in \mathcal{C}$.*

Cela équivaut à dire que $(1, 2, \ldots, n)$ est dans $\mathrm{Aut}(\mathcal{C})$ (exercice).

Exemple 1.2. *Le code linéaire $\mathcal{P}_3 := \{(0,0,0), (1,1,0), (1,0,1), (0,1,1)\}$ est cyclique.*

Exercice 1.2. *Montrer que le code linéaire $\mathcal{D}$ avec matrice génératrice*

$$G := \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \end{bmatrix}$$

est cyclique.

Afin d'avoir une description algébrique des codes cycliques, on identifie tout vecteur $c := (c_1, \ldots, c_n) \in \mathbb{F}_q^n$ avec un polynôme $c(x) := c_1 + c_2 x + \cdots + c_n x^{n-1}$ dans $\mathbb{F}_q[x]$, l'anneau des polynômes en x à coefficients dans $\mathbb{F}_q$.

Exemple 1.3. *Le code linéaire $\mathcal{P}_3$ corresponds à l'ensemble de polynômes $\{0, 1 + x, 1 + x^2, x + x^2\}$.*

Pour nos objectifs, on a besoin de considérer $R_n := \mathbb{F}_q[x]/\langle x^n - 1\rangle$, l'ensemble des classes résiduelles de $\mathbb{F}_q[x]$ modulo $x^n - 1$. Tout polynôme de degré inférieur à n appartient à une classe résiduelle distincte, et on peut considérer ce polynôme comme représentant de sa classe résiduelle. Donc (avec un abus de langage) on peut dire que $c(x)$ appartient à R_n.

Remarque 1.2. *R_n est un espace vectoriel de dimension n sur $\mathbb{F}_q$ et on a un isomorphisme ϕ (d'espaces vectoriels) entre $\mathbb{F}_q^n$ et R_n, donné par $\phi : c \mapsto c(x)$. **Dans ce qui suit on va identifier les deux espaces vectoriels**. En plus, R_n est un anneau : on peut faire le produit entre les éléments de R_n en se souvenant que $x^n = 1$ dans R_n. L'espace vectoriel $\mathbb{F}_q^n$ hérite la structure d'anneau à travers l'isomorphisme ϕ. Notons en particulier que multiplier par x dans R_n correspond à un SHIFT dans $\mathbb{F}_q^n$:*

$$x \cdot c(x) = c_1 x + c_2 x^2 + \cdots + c_n x^n = c_n + c_1 x + \cdots + c_{n-1} x^{n-1} = c^{\sigma}(x)$$

avec $\sigma = (1, 2, \ldots, n)$.

Un idéal I de R_n est un sous-groupe additif de R_n tel que pour tout $r(x) \in R_n$ et $i(x) \in I$ on a $r(x) \cdot i(x) \in I$. On peut facilement vérifier que cette définition équivaut au fait que I est un sous-espace linéaire de l'espace vectoriel R_n tel que pour tout $i(x) \in I$ on a $x \cdot c(x) \in I$ (exercice). Cela nous montre le résultat suivant.

Théorème 1.1. *Un code cyclique est un idéal de R_n.*

Un *idéal principal* est composé par tous les multiples, dans R_n, d'un certain polynôme $g(x)$. On le note $\langle g(x) \rangle$ et $g(x)$ est appelé un générateur de l'idéal (il n'est pas unique en général). En vérité, tout idéal de R_n est principal (on dit que R_n est un *anneau principal*). On va le montrer dans le théorème suivant.

Théorème 1.2. *Soit $\mathcal{C}$ un idéal non nul de R_n (c'est-à-dire un code cyclique non trivial).*

a) *Il existe un unique polynôme monique $g(x)$ de degré minimal dans $\mathcal{C}$.*
b) *$\mathcal{C} = \langle g(x) \rangle$, i.e. $g(x)$ est un générateur de $\mathcal{C}$.*
c) *$g(x)$ est un facteur de $x^n - 1$ (dans $\mathbb{F}_q[x]$).*
d) *Tout $c(x) \in \mathcal{C}$ peut être écrit de façon unique comme $c(x) = f(x)g(x)$ dans $\mathbb{F}_q[x]$, avec $\deg(f(x)) < n - \deg(g(x))$.*
e) *Si $g(x) = g_0 + g_1 x + \cdots + g_{r-1} x^{r-1} + g_r x^r$, avec $g_r \neq 0$, alors une matrice génératrice pour $\mathcal{C}$ est*

$$G := \begin{bmatrix} g_0 & g_1 & \cdots & g_{r-1} & g_r & 0 & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & \cdots & g_{r-1} & g_r & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & g_0 & g_1 & \cdots & g_{r-1} & g_r & 0 \\ 0 & \cdots & 0 & 0 & g_0 & g_1 & \cdots & g_{r-1} & g_r \end{bmatrix},$$

de manière que la dimension de $\mathcal{C}$ est $n - r$.

Démonstration.

a) Supposons qu'il y a deux polynômes moniques de degré minimal dans $\mathcal{C}$, disons $f(x)$ et $g(x)$. Leur différence $f(x) - g(x)$ est un polynôme de degré plus petit et cela nous amène à une contradiction, à moins que $f(x) = g(x)$.

b) Soit $c(x) \in \mathcal{C}$. On a que $c(x) = q(x)g(x) + r(x)$ dans $\mathbb{F}_q[x]$, avec soit $r(x) = 0$ soit $\deg(r(x)) < \deg(g(x))$. Or, $r(x) = c(x) - q(x)g(x) \in \mathcal{C}$, ce qui nous amène à une contradiction, à moins que $r(x) = 0$. Ainsi, $c(x) \in \langle g(x) \rangle$.

c) Écrivons $x^n - 1 = h(x)g(x) + r(x)$ dans $\mathbb{F}_q[x]$, avec soit $r(x) = 0$ soit $\deg(r(x)) < \deg(g(x))$. Ainsi, dans R_n on a que $r(x) = -h(x)g(x) \in \mathcal{C}$, ce qui nous amène à une contradiction, à moins que $r(x) = 0$.

d) Par b), tout $c(x) \in \mathcal{C}$, avec $\deg(c(x)) < n$, est égal à $q(x)g(x)$ dans R_n. Alors

$$c(x) = q(x)g(x) + e(x)(x^n - 1) = (q(x) + e(x)h(x))g(x) = f(x)g(x)$$

dans $\mathbb{F}_q[x]$, avec $\deg(f(x)) \leq n - r - 1$, où $r = \deg(g(x))$.

e) Par d), le code $\mathcal{C}$ est composé par le multiples de $g(x)$ par les polynômes de degré $\leq n - r - 1$ (évalues dans $\mathbb{F}_q[x]$ et non pas dans R_n). Il y a $n - r$ vecteurs linéairement indépendants qui sont multiples de $g(x)$, e.g. $g(x), xg(x), \ldots, x^{n-r-1}g(x)$. Les vecteurs correspondants dans $\mathbb{F}_q^n$ sont les lignes de G.

□

Définition 1.4. *Le polynôme $g(x)$ est appelé* le polynôme générateur *du code cyclique $\mathcal{C}$.*

Exemple 1.4. *Le polynôme générateur de $\mathcal{P}_3$ est $g(x) = 1 + x$ et une matrice génératrice pour $\mathcal{P}_3$ est*

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

Exercice 1.3. *Donner le polynôme générateur du code $\mathcal{D}$ introduit dans l'Exercice 1.2 et sa matrice génératrice correspondante.*

Exercice 1.4. *Soit $\mathcal{C}$ l'idéal $\langle x^3+x^2+2x+2 \rangle$ dans $\mathbb{F}_3[x]/\langle x^6-1 \rangle$. En déterminer une matrice génératrice. Quelle est sa distance minimale ?*

Exercice 1.5. *Quel est l'idéal qui décrit le code cyclique*

$$\{(0,0,0,0), (0,1,0,1), (1,0,1,0), (1,1,1,1)\} \subseteq \mathbb{F}_2^4 \ ?$$

Exercice 1.6. *Déterminer le polynôme générateur du plus petit code cyclique dans $\mathbb{F}_2^7$ qui contient le mot $(0,0,1,1,0,1,0)$.*

1.3 Dual d'un code cyclique

Par l'Exercice 1.1, le dual d'un code cyclique est cyclique.

Soit $\mathcal{C}$ un code cyclique avec polynôme générateur $g(x)$. Par le Théorème 1.2 on a que $g(x)$ divise $x^n - 1$ dans $\mathbb{F}_q[x]$. Alors il existe $h(x) \in \mathbb{F}_q[x]$ tel que

$$x^n - 1 = g(x)h(x),$$

qui est appelé *polynôme de contrôle* de $\mathcal{C}$. Son nom vient du fait que pour tout $c(x) \in \mathcal{C}$ ssi $c(x)h(x) = 0$ dans R_n (exercice).

Si le degré de $g(x)$ est égal à r, le degré de $h(x)$ est $n-r$. Soit

$$c(x) = c_0 + c_1 x + \cdots + c_{n-1}x^{n-1} \text{ et } h(x) = h_0 + h_1 x + \cdots + h_{n-r}x^{n-r}.$$

Le coefficient de x^i dans le produit $c(x)h(c)$ est

$$\sum_{i=0}^{n-1} c_i h_{j-i} = 0, \ j \in \{0, \ldots, n-1\} \tag{1.1}$$

où $j-i$ est considéré modulo n.

Théorème 1.3. *Soit $h(x) = h_0 + h_1 x + \cdots + h_{n-r}x^{n-r}$ le polynôme de contrôle d'un code cyclique $\mathcal{C}$. Alors la matrice*

$$H := \begin{bmatrix} 0 & \cdots & 0 & 0 & h_{n-r} & h_{n-r-1} & \cdots & h_1 & h_0 \\ 0 & \cdots & 0 & h_{n-r} & h_{n-r-1} & \cdots & h_1 & h_0 & 0 \\ \vdots & \iddots & \iddots & \iddots & & \iddots & \iddots & & \vdots \\ 0 & h_{n-r} & h_{n-r-1} & \cdots & h_1 & h_0 & 0 & \cdots & 0 \\ h_{n-r} & h_{n-r-1} & \cdots & h_1 & h_0 & 0 & 0 & \cdots & 0 \end{bmatrix}$$

est une matrice de parité pour $\mathcal{C}$.

Démonstration. Par (1.1), on a que $Hc^T = 0$ si $c \in C$. De plus les $n-(n-r) = r$ lignes de H sont linéairement indépendantes, de manière que $Hc^T = 0$ implique que $c \in \mathcal{C}$. Donc H est une matrice de parité pour $\mathcal{C}$. □

Corollaire 1.1. *Soit $h(x)$ le polynôme de contrôle d'un code cyclique $\mathcal{C}$. Alors le code $\mathcal{C}^\perp$ est cyclique avec polynôme générateur*

$$g^\perp(x) = x^{\deg(h(x))} h(x^{-1}).$$

Démonstration. Exercice. □

Ce résultat implique en particulier que le code cyclique avec polynôme générateur $h(x)$ est équivalent (par permutation) à $\mathcal{C}^\perp$.

Exemple 1.5. *Le polynôme de contrôle de $\mathcal{P}_3$ est $h(x) = x^2 + x + 1$.*

Exercice 1.7. *Donner le polynôme de contrôle du code $\mathcal{D}$ introduit dans l'Exercice 1.2 et la matrice de parité correspondante.*

Exercice 1.8. *Montrer que le code de longueur 7 sur $\mathbb{F}_2$ avec polynôme générateur x^3+x+1 est le dual du code de longueur 7 sur $\mathbb{F}_2$ avec polynôme générateur $x^4 + x^3 + x^2 + 1$.*

Exercice 1.9. *Soit $\mathcal{C}$ le code cyclique binaire de longueur 15 de polynôme générateur $g(x) = x^4 + x + 1$. Donner une matrice génératrice et une matrice de parité de $\mathcal{C}$ et en trouver la distance minimale. Quel est le code $\mathcal{C}$? Corriger le mot reçu $(0,0,0,0,0,1,1,0,1,1,0,0,0,0,0)$.*

1.4 Construction des codes cycliques

D'après le Théorème 1.2, déterminer tous les codes cycliques sur $\mathbb{F}_q$ de longueur n équivaut à déterminer tous les diviseurs moniques $g(x)$ de $x^n-1 \in \mathbb{F}_q[x]$.

En ce qui suit, on va supposer que $(n,q) = 1$, de manière que q soit dans $(\mathbb{Z}/n\mathbb{Z})^*$ (groupe multiplicatif). Soit m l'ordre de q dans $(\mathbb{Z}/n\mathbb{Z})^*$. On a $q^m = 1 \bmod n$, de manière que n divise $q^m - 1$.

Exercice 1.10. *Soient a, b deux entiers positifs. Montrer que $x^a - 1$ divise $x^b - 1$ dans $K[x]$, avec K un corps quelconque, si et seulement si a divise b dans $\mathbb{Z}$.*

Alors $x^n - 1$ divise $x^{q^m-1} - 1$. On peut montrer (exercice) que $x^n - 1$ ne divise pas $x^{q^s-1} - 1$, pour $s < m$. Rappelons que $\mathbb{F}_{q^m}$ est le corps des racines de $x^{q^m} - x = x \cdot (x^{q^m-1} - 1)$. Donc $\mathbb{F}_{q^m}$ est la plus petite extension de $\mathbb{F}_q$ qui contient les racines de $x^n - 1$ (qui sont appelées *racines n-ièmes de l'unité* sur $\mathbb{F}_q$). L'ensemble des racines n-ièmes de l'unité sur $\mathbb{F}_q$ forment un sous-groupe (cyclique) du groupe multiplicatif (cyclique) $(\mathbb{F}_{q^m})^* = \mathbb{F}_{q^m} - \{0\}$. Soit $\alpha \in \mathbb{F}_{q^m}$ un générateur de ce sous-groupe. Un tel élément est appelé *racine primitive n-ième de l'unité*.

Remarque 1.3. *Supposons $q = 2$ et n pair, de manière que $(n, 2) = 2$. Pour tout m on a que $2^m - 1$ est impair, de manière que n ne peut pas le diviser. Ainsi, il n'existe pas m tel que $x^n - 1$ divise $x^{2^m-1} - 1$. De la même manière, pour tout q et n tel que $(n, q) \neq 1$ on a qu'il n'existe pas m tel que $x^n - 1$ divise $x^{q^m-1} - 1$ (exercice).*

Puisque $\mathbb{F}_{q^m}$ est le corps des racines de $x^{q^m} - x$, on a en particulier

$$x^{q^m-1} - 1 = \prod_{\beta \in (\mathbb{F}_{q^m})^*} (x - \beta)$$

dans $\mathbb{F}_{q^m}[x]$.
Par ailleurs, le polynôme $x^n - 1$ se factorise dans $\mathbb{F}_{q^m}[x]$ comme suit :

$$x^n - 1 = \prod_{i=0}^{n-1} (x - \alpha^i).$$

Lemme 1.1. *Soit T un sous-ensemble de $(\mathbb{F}_{q^m})^*$ et*

$$p(x) = \prod_{\tau \in T} (x - \tau) \in \mathbb{F}_{q^m}[x].$$

On a que $p(x) \in \mathbb{F}_q[x]$ ssi T est stable par l'automorphisme de Frobenius, i.e. ssi $\tau \in T$ implique $\tau^q \in T$.

Démonstration. Puisque $\mathbb{F}_q = \{a \in \mathbb{F}_{q^m} \mid a^q = a\}$, on a que $p(x) \in \mathbb{F}_q[x]$ ssi $p(x)^q = p(x^q)$. Or,

$$p(x)^q = \prod_{\tau \in T} (x - \tau)^q = \prod_{\tau \in T} (x^q - \tau^q) = \prod_{\tau \in T} (x^q - \tau) = p(x^q),$$

ce qui équivaut à T stable par l'automorphisme de Frobenius. □

Définition 1.5. *La* classe cyclotomique *de s modulo n sur $\mathbb{F}_q$ est l'ensemble*

$$C_s := \{s, sq, sq^2, \ldots, sq^{m_s-1}\},$$

où m_s est le plus petit entier positif tel que $sq^{m_s} \equiv s \bmod n$.

C'est utile, mais pas nécessaire, de prendre comme s le plus plus petit entier positif dans C_s. Les classes cyclotomiques forment une partition de $\mathbb{Z}/n\mathbb{Z}$. Notons que $m_1 = \#C_1$ est l'ordre m de q modulo n. Soit S un système de représentants des classes cyclotomiques.

Exemple 1.6. *Soit $n = 9$ et $q = 2$. Alors*

$$C_0 = \{0\}, \quad C_1 = \{1, 2, 4, 8, 7, 5\}, \quad C_3 = \{3, 6\}.$$

On a $m = m_1 = 6$, de manière que $\mathbb{F}_{64}$ est le corps des racines de $x^9 - 1$.

Une conséquence directe des résultats ci-dessus est qu'une factorisation de $x^n - 1$ en facteurs irréductibles dans $\mathbb{F}_q[x]$ est donnée par

$$x^n - 1 = \prod_{s \in S} M_s(x)$$

où

$$M_s(x) = \prod_{j \in C_s} (x - \alpha^j)$$

qui est le *polynôme minimal* de α^j (pour tout $j \in C_s$) sur $\mathbb{F}_q$, c'est-à-dire le polynôme monique dans $\mathbb{F}_q[x]$ de plus petit degré ayant α^j comme racine. Ce polynôme est clairement irréductible dans $\mathbb{F}_q[x]$.

Exemple 1.7. *Soit $n = 9$ et $q = 2$ et soit α une racine primitive 9-ième de l'unité dans $\mathbb{F}_{64}$. Par exemple, si on considère $\mathbb{F}_{64} = \mathbb{F}_2[x]/\langle x^6 + x^3 + 1\rangle$, on peut prendre α comme la racine de $x^6 + x^3 + 1$, c'est-à-dire un élément tel que $\alpha^6 = \alpha^3 + 1$. En effet*

$$\alpha^9 = \alpha^6 \cdot \alpha^3 = (\alpha^3 + 1) \cdot \alpha^3 = \alpha^6 + \alpha^3 = \alpha^3 + 1 + \alpha^3 = 1 \text{ et } \alpha^3 \neq 1.$$

On a

$$\begin{aligned} M_0(x) &= x + \alpha^0 = x + 1 \\ M_1(x) &= (x + \alpha)(x + \alpha^2)(x + \alpha^4)(x + \alpha^8)(x + \alpha^7)(x + \alpha^5) = x^6 + x^3 + 1, \\ M_3(x) &= (x + \alpha^3)(x + \alpha^6) = x^2 + x + 1 \end{aligned}$$

de manière que $x^9 + 1 = (x + 1)(x^6 + x^3 + 1)(x^2 + x + 1)$ est une factorisation de $x^9 + 1$ en polynômes irréductibles sur $\mathbb{F}_2$.

On a donc le résultat suivant.

Théorème 1.4. *Soit $\mathcal{C}$ un code cyclique de longueur n sur $\mathbb{F}_q$, avec polynôme générateur $g(x)$. Soit m l'ordre de q dans $(\mathbb{Z}/n\mathbb{Z})^*$, α une racine primitive n-ième de l'unité dans $\mathbb{F}_{q^m}$ et S un système de représentants des classes cyclotomiques modulo n sur $\mathbb{F}_q$. On a*

$$g(x) = \prod_{t \in T} M_t(x) = \prod_{j \in Z} (x - \alpha^j)$$

où $T \subseteq S$ et $Z := \bigcup_{t \in T} C_t$ est une union de classes cyclotomiques.

Démonstration. Cela suit directement du fait que $g(x)$ est un diviseur (monique) de $x^n - 1$ dans $\mathbb{F}_q[x]$. □

Les racines n-ièmes de l'unité $\{\alpha^j \mid j \in Z\}$ sont appelées les *zéros du code*. Clairement, un élément $c(x) \in R_n$ appartient à $\mathcal{C}$ ssi $c(\alpha^j) = 0$ pour tout $j \in Z$ (exercice). Ainsi, un code cyclique est défini en terme des zéros de $c(x)$.

Exemple 1.8. *On a 8 codes cycliques possibles de longueur 9 sur $\mathbb{F}_2$:*

1. *Le $[9, 9, 1]$ code cyclique $\mathbb{F}_2^9$ avec polynôme générateur 1.*
2. *Le $[9, 8, 2]$ code cyclique avec polynôme générateur $x + 1$. Ceci est le code de parité de longueur 9.*
3. *Le $[9, 3, 3]$ code cyclique avec polynôme générateur $x^6 + x^3 + 1$. Ce code a matrice génératrice*

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

4. *Le $[9, 7, 2]$ code cyclique avec polynôme générateur $x^2 + x + 1$. Ce code a matrice génératrice*

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

5. *Le $[9, 1, 9]$ code cyclique avec polynôme générateur $(x^6+x^3+1)(x^2+x+1)$. Ce code a matrice génératrice*

$$G := \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

6. *Le* $[9,6,2]$ *code cyclique avec polynôme générateur* $(x+1)(x^2+x+1)$. *Ce code a matrice génératrice*

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

7. *Le* $[9,2,6]$ *code cyclique avec polynôme générateur* $(x+1)(x^6+x^3+1)$. *Ce code a matrice génératrice*

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

8. *Le* $[9,0,9]$ *code cyclique nul.*

Notons que le code 8. est le dual du code 1., le code 5. est le dual du code 2., le code 6. est le dual du code 3. est le code 7. est le dual du code 4..

Exercice 1.11. *Montrer que, puisque* $(n,q)=1$, *la factorisation du polynôme* x^n-1 *dans* $\mathbb{F}_q[x]$ *n'a pas de facteurs avec multiplicité plus grande que* 1.

Exercice 1.12. *Soit* k *le nombre des classes cyclotomiques modulo* n *sur* $\mathbb{F}_q$. *Montrer qu'il y a exactement* 2^k *codes cycliques de longueur* n *sur* $\mathbb{F}_q$.

Par le Corollaire 1.1, les zéros du dual d'un code $\mathcal{C}$ sont les inverses des non-zéros de $\mathcal{C}$ (exercice).

Exercice 1.13. *Soit* $n=17$ *et soit* α *une racine primitive* 17*-ième de l'unité dans le corps* $\mathbb{F}_{2^m}$, *où* m *est l'ordre de* 2 *modulo* 17. *Déterminer* m *et les classes cyclotomiques modulo* 17 *sur* $\mathbb{F}_2$. *Quel est le nombre des codes cycliques binaires de longueur* 17 *? Quelle est leur dimension ?*

Exercice 1.14. *Donner la liste des codes cycliques binaires de longueur* 7.

Exercice 1.15 (Solution à p. 191-192 [MWS77])**.** *Soit* $n=2^m-1$ *et* $q=2$. *Soit* α *une racine primitive* n*-ième de l'unité dans* $\mathbb{F}_{2^m}$ *et* $M_1(x)$ *le polynôme (de degré* m*) qui est le produit des* $x-\alpha^j$ *pour* $j \in C_1$, *la classe cyclotomique de* 1 *modulo* n *sur* $\mathbb{F}_2$. *Montrer que le code cyclique* $\mathcal{C}$ *avec polynôme générateur* $M_1(x)$ *est équivalent au code de Hamming* $\mathcal{H}_m$.

Ce dernier exercice implique que tout code de Hamming est équivalent à un code cyclique. On dit souvent, avec un abus de langage, que les codes (binaires) de Hamming sont cycliques.

Remarque 1.4. *Soit* $q=p^t$, *avec* p *premier. Si* $(n,q)\neq 1$, *alors, il existe* $1\leq r\leq t$ *tel que* $(n,q)=p^r$. *Écrivons* $n=p^r\cdot u$, *avec* $(u,q)=1$. *Puisque* $\mathbb{F}_q$ *est un corps de caractéristique* p, *on a que*

$$x^n-1=(x^u)^{p^r}-1^{p^r}=(x^u-1)^{p^r}.$$

Il est possible de factoriser $x^u - 1$ *sur* $\mathbb{F}_q$ *avec la méthode expliquée ci-dessus. Combien de diviseurs a-t-on dans ce cas ?*

Chapitre 2

Les codes BCH

Les codes BCH (Bose-Chaudhuri-Hocquenghem) sont une classe de codes cycliques. Les codes BCH ont été inventés en 1959 par le mathématicien français Alexis Hocquenghem, et indépendamment en 1960 par Raj Bose et D. K. Ray-Chaudhuri. Le nom Bose-Chaudhuri-Hocquenghem (et l'acronyme BCH) découle des initiales des noms des inventeurs (à tort, dans le cas de Ray-Chaudhuri).

L'une des principales caractéristiques des codes BCH est que, lors de la conception du code, il existe un contrôle précis du nombre d'erreurs qui peuvent être corrigées par le code. Un autre avantage des codes BCH est la facilité avec laquelle ils peuvent être décodés, à savoir via une méthode algébrique connue sous le nom de décodage de syndrome.

Les codes BCH sont utilisés dans des applications telles que les communications par satellite, les lecteurs de disques compacts, les DVD, ...

2.1 La borne BCH

Théorème 2.1 (La borne BCH)**.** *Soit $\mathcal{C}$ un code cyclique de longueur n sur $\mathbb{F}_q$, avec polynôme générateur $g(x)$. Soit m l'ordre de q dans $(\mathbb{Z}/n\mathbb{Z})^*$ et α une racine primitive n-ième de l'unité dans $\mathbb{F}_{q^m}$. S'il existe deux entiers $b \geq 0$ et $\delta \geq 2$ tels que*

$$g(\alpha^b) = g(\alpha^{b+1}) = \cdots = g(\alpha^{b+\delta-2}) = 0,$$

i.e. si $\mathcal{C}$ a $\delta - 1$ puissances consécutives de α parmi ses zéros, alors la distance minimale de $\mathcal{C}$ est au moins δ.

Démonstration. Soit $c(x) = c_0 + c_1 x + \cdots + c_{n-1}x^{n-1} \in \mathcal{C}$. Par hypothèse,

$$c(\alpha^b) = c(\alpha^{b+1}) = \cdots = c(\alpha^{b+\delta-2}) = 0,$$

de manière que $H'c^T = 0$, où

$$H' = \begin{bmatrix} 1 & \alpha^b & \alpha^{2b} & \cdots & \alpha^{(n-1)b} \\ 1 & \alpha^{b+1} & \alpha^{2(b+1)} & \cdots & \alpha^{(n-1)(b+1)} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha^{b+\delta-2} & \alpha^{2(b+\delta-2)} & \cdots & \alpha^{(n-1)(b+\delta-2)} \end{bmatrix}.$$

Notons que H' n'est pas forcement la matrice de parité complète de $\mathcal{C}$ (attention : il faut la considérer comme matrice sur $\mathbb{F}_q$, en remplaçant tout entrée de la matrice par la colonne de m élément sur $\mathbb{F}_q$ correspondante).

Supposons qu'il existe un mot non nul de poids inférieur à δ. Soit $A = \{a_1, \ldots, a_{\delta-1}\}$ tel que $c_i \neq 0$ implique $i \in A$ (c'est-à-dire un ensemble de $\delta - 1$ coordonnées contenant le support de c). Alors $H'c^T = 0$ implique que

$$\begin{bmatrix} \alpha^{a_1 b} & \cdots & \alpha^{a_{\delta-1} b} \\ \alpha^{a_1 (b+1)} & \cdots & \alpha^{a_{\delta-1}(b+1)} \\ \vdots & & \vdots \\ \alpha^{a_1(b+\delta-2)} & \cdots & \alpha^{a_{\delta-1}(b+\delta-2)} \end{bmatrix} \begin{bmatrix} c_{a_1} \\ c_{a_2} \\ \vdots \\ c_{a_{\delta-1}} \end{bmatrix} = 0.$$

Ce système a une solution non nulle, de manière que le déterminant de la matrice à gauche est forcement nul. La i-ème colonne est un multiple de $\alpha^{a_i b}$. Ainsi le déterminant de la matrice à gauche est égal à

$$\alpha^{b(a_1+\cdots+a_{\delta-1})} \cdot \begin{vmatrix} 1 & \cdots & 1 \\ \alpha^{a_1} & \cdots & \alpha^{a_{\delta-1}} \\ \vdots & & \vdots \\ (\alpha^{a_1})^{\delta-2} & \cdots & (\alpha^{a_{\delta-1}})^{\delta-2} \end{vmatrix} = \alpha^{b(a_1+\cdots+a_{\delta-1})} \cdot \prod_{i<j} (\alpha^{a_j} - \alpha^{a_i}),$$

l'égalité étant une conséquence de la formule du déterminant d'une matrice de Vandermonde (exercice). Le produit à droite ne peut pas être nul, ce qui nous donne une contradiction. Donc il n'existe pas un mot non nul de poids inférieur à δ. □

Exemple 2.1. *Dans l'Exercice 1.15 on a montré que le code de Hamming binaire $\mathcal{H}_m$ est équivalent à un code cyclique avec polynôme générateur $M_1(x)$, le polynôme minimal de α, racine primitive (2^m-1)-ième de l'unité dans $\mathbb{F}_{2^m}$. Dans la classe cyclotomique de 1 modulo $2^m - 1$ sur $\mathbb{F}_2$ il y a sûrement 1 et 2, de manière que $M_1(\alpha) = M_1(\alpha^2) = 0$. Alors la distance minimale de $\mathcal{H}_m$ est au moins 3 par le Théorème 2.1. On sait $\mathcal{H}_m$ a distance minimale exactement 3.*

Exercice 2.1. *Soit $m \geq 3$ et α une racine primitive (2^m-1)-ième de l'unité dans $\mathbb{F}_{2^m}$. Montrer que α^3 n'est pas une racine du polynôme minimal $M_1(x)$ de α.*

Il y eut nombreux travaux (voir par exemple [HT72, R83, vLW86]) dont le but était l'amélioration de la borne-BCH. Plus précisément, on cherche à mettre en évidence des propriétés combinatoires de l'ensemble des zéros telles que certains outils algébriques puissent s'appliquer, de la même façon que pour le borne BCH.

2.2 Définition des codes BCH

Les codes BCH ont été définis en 1959-1960, dans [H59, BRC60-1, BRC60-2].

Définition 2.1. *Un code cyclique $\mathcal{C}$ de longueur n sur $\mathbb{F}_q$ est un* code BCH de distance construite δ, *avec $2 \le \delta \le n$, s'il existe un entier b tel que son polynôme générateur est égal à*

$$g(x) = \text{ppcm}\{M_b(x), M_{b+1}, \ldots, M_{b+\delta-2}\},$$

i.e. si $g(x)$ est le polynôme monique de plus petit degré sur $\mathbb{F}_q$ qui a $\alpha^b, \alpha^{b+1}, \ldots, \alpha^{b+\delta-2}$ parmi ses zéros, où α est une racine primitive n-ième de l'unité.
Si $b = 1$, il s'agit d'un code BCH au sens strict.
Si $n = q^m - 1$, le code BCH est appelé primitif, *car α est un élément primitif de $\mathbb{F}_{q^m}$.*

Ainsi, un code BCH de distance construite δ a une séquence de $\delta - 1$ puissances successives de α comme zéros, de manière que, par le Théorème 2.1, il a distance minimale au moins δ.

La matrice de parité d'un code BCH de longueur n sur $\mathbb{F}_q$ de distance construite δ, par rapport à l'entier b, est (exercice)

$$H := \begin{bmatrix} 1 & \alpha^b & \alpha^{2b} & \cdots & \alpha^{(n-1)b} \\ 1 & \alpha^{b+1} & \alpha^{2(b+1)} & \cdots & \alpha^{(n-1)(b+1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{b+\delta-2} & \alpha^{2(b+\delta-2)} & \cdots & \alpha^{(n-1)(b+\delta-2)} \end{bmatrix}$$

où α est une racine primitive n-ième de l'unité dans $\mathbb{F}_{q^m}$ et H est considérée comme matrice sur $\mathbb{F}_q$, en remplaçant tout entrée par la colonne de m élément sur $\mathbb{F}_q$ correspondante. Après cette substitution on obtient $m(\delta-1)$ lignes, mais on peut pas dire si elles sont linéairement indépendants. Ainsi, la dimension du code est au moins $n - m(\delta-1)$. On peut résumer ces résultats dans un théorème :

Théorème 2.2. *Un code BCH sur $\mathbb{F}_q$ de longueur n et distance construite δ a paramètres $[n, \ge n - m(\delta-1), \ge \delta]$, où m est l'ordre de q dans $(\mathbb{Z}/n\mathbb{Z})^*$.*

Exemple 2.2. *Comme on a remarqué dans l'Exemple 2.1, les codes de Hamming sont le codes BCH au sens strict de distance construite 3 et de longueur $2^m - 1$ sur $\mathbb{F}_2$.*

Exercice 2.2. *Construire un code BCH de longueur 9 et de distance construite 6 sur $\mathbb{F}_2$.*

Exercice 2.3. *Combien de codes BCH au sens strict de longueur 15 sur $\mathbb{F}_2$ y a-t-il ? Quels sont leurs paramètres ?*

Déterminer la distance minimale vraie des codes BCH est difficile en général. Il est un problème de recherche. Les cas où on sait déterminer cette distance, en sachant la distance construite et la longueur, sont limités. Il s'agit de classes très particulières, comme on peut voir dans le résultat suivant, donné à titre d'exemple.

Théorème 2.3. *Soit $n = \delta s$, avec $2 \leq \delta \leq n$. Alors le code BCH au sens strict de distance construite δ et de longueur n a distance minimale égale à δ.*

Démonstration. On a

$$x^n - 1 = (x^s - 1)\underbrace{\left((x^s)^{\delta-1} + (x^s)^{\delta-2} + \cdots + 1\right)}_{c(x)}.$$

Soit $\mathbb{F}$ le corps de décomposition de $x^n - 1$ et $\alpha \in \mathbb{F}$ une racine primitive n-ième de l'unité. Les racines de $x^n - 1$ sont $1, \alpha, \ldots, \alpha^{n-1}$. Le racines de $x^s - 1$ sont les racines s-ièmes de l'unité, qu'on obtient en prenant les puissances α^l, avec $l \in \{0, \delta, 2\delta, \ldots, (s-1)\delta\}$ (exercice). Ainsi,

$$\alpha, \alpha^2, \ldots, \alpha^{\delta-1}$$

sont des racines de $c(x)$, qui est donc un mot du code BCH au sens strict de distance construite δ. Or, le polynôme $c(x)$ représente clairement un mot de poids δ. □

Exemple 2.3. *On considère les codes BCH au sens strict de longueur $63 = 3^2 \cdot 7$. Les distances construites $3, 7, 9$ et 21 sont les distances minimales des codes concernés.*

On connaît la distance minimale des codes BCH au sens strict, primitifs, de longueur inférieure ou égale à 255, sur $\mathbb{F}_2$ [ACS92].

Il y a une conjecture proposée en 1998 par Pascale Charpin.

Conjecture [C98]. *La distance minimale d'un code BCH au sens strict et primitif de distance construite δ est au plus $\delta + 4$.*

2.3 Les codes de Reed-Solomon

Définition 2.2. *Un* code de Reed-Solomon (*code RS*) *est un code BCH de longueur $q - 1$ sur $\mathbb{F}_q$. On appelle code RS* au sens strict *un code RS qui est un code BCH au sens strict.*

Puisque la longueur de ces codes est $q - 1$, les classes cyclotomiques de q modulo n sont des singletons (exercice). En plus, une racine primitive $(q-1)$-ième de l'unité dans ce cas est un élément primitif de $\mathbb{F}_q$.

Théorème 2.4. *Tous les codes de Reed-Solomon sont MDS et leur distance minimale est égale à leur distance construite.*

Démonstration. Soit $\mathcal{C}$ un code BCH de longueur $q - 1$ sur $\mathbb{F}_q$, de distance construite δ et soit d sa distance minimale. Soit α un élément primitif de $\mathbb{F}_q$. Le polynôme générateur de $\mathcal{C}$ a la forme suivante :

$$g(x) = \prod_{i=0}^{\delta-2} (x - \alpha^{b+i}),$$

pour un certain entier b, puisque les classes cyclotomiques sont des singletons. Ce polynôme a degré $\delta - 1$, de manière qu'il ne peut pas avoir plus de δ coefficients non nuls. Ainsi le poids de $g(x)$ est au plus δ. Puisque $d \geq \delta$, on a $d = \delta$. En plus,

$$d = \deg g(x) + 1 = n - \dim \mathcal{C} + 1,$$

ce qui équivaut à dire que $\mathcal{C}$ est MDS. □

Exercice 2.4. *Le dual d'un code de Reed-Solomon est un code de Reed-Solomon.*

Exemple 2.4. *Soit $q = 7$. On veut construire le code de Reed-Solomon au sens strict de distance minimale $\delta = 4$ dans $\mathbb{F}_7^6$. Notons que 5 est une racine primitive 6-ième de l'unité dans $\mathbb{F}_7$. En effet, $5 \neq 1 \bmod 7$, $5^2 = 4 \neq 1 \bmod 7$, $5^3 = 6 \neq 1 \bmod 7$ et $5^6 = 1 \bmod 7$. Le code avec polynôme générateur*

$$g(x) = (x-5)(x-4)(x-6) = x^3 + 6x^2 + 4x + 6$$

est un code de Reed-Solomon au sens strict de paramètres $[6,3,4]_7$. Son dual a polynôme générateur

$$g^{\perp}(x) = x^3(x^{-1}-1)(x^{-1}-2)(x^{-1}-3) = (1-x)(1-2x)(1-3x) =$$

$$= (-1)(x-1)(-2)(x-4)(-3)(x-5) = (x-1)(x-5)(x-4) = x^3 + 4x^2 + x + 1,$$

qui est encore un code de Reed-Solomon de paramètres $[6,3,4]_7$.

Les deux codes ne sont pas égaux, ni équivalents par permutation (ils le sont dans un sens plus générale).

Classiquement, on construit des nouveaux codes en étendant des codes connus. Cela est une construction standard donnée dans la définition suivante.

Définition 2.3. *Soit $\mathcal{C}$ un code linéaire de longueur n tel qu'il existe un mot $c = (c_1, \ldots, c_n)$ vérifiant*

$$\sum_{i=1}^{n} c_i \neq 0.$$

*L'*extension *du code $\mathcal{C}$ est le code $\mathcal{C}_e$ obtenu en adjoignant à chaque mot $c = (c_1, \ldots, c_n)$ de $\mathcal{C}$ un symbole dit de parité $c_{n+1} = -\sum_{i=1}^{n} c_i$, i.e.*

$$\mathcal{C}_e = \{(c_1, \ldots, c_n, -\sum_{i=1}^{n} c_i) \mid (c_1, \ldots, c_n) \in \mathcal{C}\}.$$

L'extension d'un code linéaire de longueur n (et dimension k) est un code linéaire (exercice) de longueur $n+1$ (et dimension k).

Proposition 2.1. *L'extension $\mathcal{C}_e$ d'un code de Reed-Solomon au sens strict non trivial $\mathcal{C}$ de paramètres $[n,k,d]_q$ est un code MDS de paramètres $[n+1,k,d+1]_q$ (qu'on appelle code RS étendu).*

Démonstration. Le distance minimale augmente de d à $d+1$ si pour tout mot de poids minimal $c(x) \in \mathcal{C}$ on a $c_{n+1} = -\sum_{i=1}^{n} c_i = -c(1) \neq 0$. Mais $c(x) = a(x)g(x)$, avec $g(x)$ le polynôme générateur de $\mathcal{C}$. On a $g(1) \neq 0$, car $\mathcal{C}$ est un code de Reed-Solomon au sens strict non trivial. Si, par l'absurde, $c(1) = 0$, alors $a(1) = 0$ et $c(x)$ appartient donc au code de polynôme générateur $(x-1)g(x)$, qui a distance minimale $d+1$ par la borne BCH. Cela nous donne une contradiction, car $c(x)$ a poids d. □

Soit $\mathcal{C}$ un code de Reed-Solomon au sens strict dans $\mathbb{F}_q^{q-1}$, de distance construite $\delta < q$. Ses zéros sont $\alpha, \alpha^2, \ldots, \alpha^{\delta-1}$, où α est un élément primitif de $\mathbb{F}_q$, et sa dimension est égale à $q - 1 - (\delta - 1) = q - \delta$. Les zéros du dual de $\mathcal{C}$, qui est un code de Reed-Solomon par l'Exercice 2.4, sont les inverses des non-zéros de $\mathcal{C}$, i.e. les inverses de

$$\alpha^{\delta}, \alpha^{\delta+1}, \ldots, \alpha^{q-1},$$

qui sont

$$\alpha^{q-1-\delta} = \alpha^{q-\delta-1}, \alpha^{q-1-(\delta+1)} = \alpha^{q-\delta-2}, \ldots, \alpha^{q-1-(q-1)} = \alpha^{0}.$$

Ainsi, une matrice de parité pour $\mathcal{C}^{\perp}$ (qui est donc une matrice génératrice pour $\mathcal{C}$) est donnée par la matrice $(q-\delta) \times (q-1)$

$$\begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \alpha & \alpha^2 & \cdots & \alpha^{q-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{q-\delta-1} & \alpha^{2(q-\delta-1)} & \cdots & \alpha^{(q-2)(q-\delta-1)} \end{bmatrix}$$

Notons que, pour tout $i \in \{0, \ldots, q-\delta\}$, la ligne $(i-1)$-ème est égale au monôme x^{i-1}, évalué sur $1, \alpha, \ldots, \alpha^{q-2}$. On a donc le résultat suivant.

Proposition 2.2. *Un code de Reed-Solomon au sens strict $\mathcal{C} \subseteq \mathbb{F}_q^{q-1}$, de distance construite $\delta < q$ est égal à*

$$\mathcal{C} = \{(f(1), f(\alpha), \ldots, f(\alpha^{q-2})) \mid f(x) \in \mathbb{F}_q[x] \text{ de degré } < q - \delta\}.$$

pour α un élément primitif de $\mathbb{F}_q$.

À partir de cette propriété on peut donner une définition plus générale des code de Reed-Solomon (qui inclut la définition précédente) :

Définition 2.4. *Soit $\mathbb{F}_q$ un corps fini et soient $a_1, \ldots, a_n$ n éléments distincts de $\mathbb{F}_q$ (clairement $n \leq q$). Le code linéaire*

$$\mathcal{C} = \{(f(a_1), \ldots, f(a_n)) \mid f(x) \in \mathbb{F}_q[x] \text{ de degré } \leq r\}$$

est appelé code de Reed-Solomon.

Soit $\mathcal{C}$ comme dans la définition ci-dessus. La dimension de $\mathcal{C}$ est clairement $r+1$ (on le voit à partir d'une matrice génératrice - exercice). Puisque un polynôme (non nul) de degré $\leq r$ a au plus r zéros, le poids de tout mot non nul de $\mathcal{C}$ est au moins $n-r$, de manière que la distance minimale d de $\mathcal{C}$ est au moins $n-r$. Mais la borne de Singleton nous donne aussi que $d \leq n-(r+1)+1 = n-r$. Ainsi, le paramètres de $\mathcal{C}$ sont $[n, r+1, n-r]$ et $\mathcal{C}$ est un code MDS.

Exemple 2.5. *Soit $\mathbb{F}_8 = \mathbb{F}_2[x]/\langle x^3+x+1\rangle = \mathbb{F}_2[\alpha]$. On a que α est un élément primitif de $\mathbb{F}_8$. On considère les éléments $0, 1, \alpha, \alpha^2$. Alors le code*

$$\mathcal{C} = \{(f(0), f(1), f(\alpha), f(\alpha^2)) \mid f(x) \in \mathbb{F}_8[x] \text{ de degré } \leq 1\}$$

est un code de Reed-Solomon de paramètres $[4,2,3]_8$. Une matrice génératrice pour $\mathcal{C}$ est

$$G := \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & \alpha & \alpha^2 \end{bmatrix}.$$

Exercice 2.5. *Construire un code de Reed-Solomon de paramètres $[5,3,3]_8$ et en donner une matrice génératrice.*

Avec les codes de Reed-Solomon on a une classe infinie d'exemples de codes MDS. Une question naturel qu'on se pose est la suivante : soit $M(k,q)$ la longueur la plus grande d'un code MDS de dimension k sur $\mathbb{F}_q$. K. A. Bush montre dans [B52] que si $k > q$ alors $M(k,q) = k+1$, i.e. le code MDS le plus long de dimension k sur $\mathbb{F}_q$ a paramètres $[k+1, k, 2]_q$. Les codes de parité sont un exemple de codes avec ces paramètres. Il y a une conjecture, qui est toujours ouverte (même si certains cas ont été montrés), formulée par B. Segre en 1955 et connue comme **Conjecture MDS** :

Conjecture [S55]. *Si $k \leq q$, alors $M(k,q) = q+1$, à exception des cas où q est pair et $k = 3$ ou $k = q-1$, pour lesquels $M(k,q) = q+2$.*

Les codes de Reed-Solomon étendues de longueur $q+1$ sur $\mathbb{F}_q$ sont des exemples de codes MDS de paramètres $[q+1, k, q-k+2]_q$ pour tout $k \leq q$.

Chapitre 3

Décodage des codes algèbriques

D'un point de vue pratique, un code a beaucoup plus d'intérêt s'il existe un algorithme efficace pour le décoder.

3.1 Décodage de Meggitt

On présente ici l'une des versions de l'algorithme conçu par Meggitt en 1960 pour les codes cycliques.

Soit $\mathcal{C}$ un $[n,k,d]_q$ code cyclique et soit $g(x)$ son polynôme générateur, de degré $n-k$. Supposons que $c(x) \in \mathcal{C}$ soit transmis et que $y(x) = c(x) + e(x)$ soit reçu, où $e(x) = e_0 + \ldots + e_{n-1}x^{n-1}$ est le vecteur erreur de poids $\leq \lfloor (d-1)/2 \rfloor$.

Pour tout vecteur $v(x) \in \mathbb{F}_q[x]$, soit $R_{g(x)}(v(x))$ le reste de la division euclidienne de $v(x)$ par $g(x)$, i.e.

$$v(x) = g(x)q(x) + R_{g(x)}(v(x)), \text{ avec } R_{g(x)}(v(x)) = 0 \text{ ou } \deg R_{g(x)}(v(x)) < n-k.$$

Proposition 3.1. *La fonction $R_{g(x)}$ satisfait les propriétés suivantes :*

a) $R_{g(x)}(av(x)+bw(x)) = aR_{g(x)}(v(x))+bR_{g(x)}(w(x))$ *pour tout* $v(x), w(x) \in \mathbb{F}_q[x]$ *et tout* $a, b \in \mathbb{F}_q$ (*i.e.* $R_{g(x)}$ *est un morphisme d'espaces vectoriels*) ;

b) $R_{g(x)}(v(x) + a(x)(x^n - 1)) = R_{g(x)}(v(x))$ (*i.e. le morphisme* $R_{g(x)}$ *"passe au quotient" et donc on peut le définir de* $R_n = \mathbb{F}_q[x]/\langle x^n - 1 \rangle$) ;

c) *si* $v(x) \in R_n$, *on a* $R_{g(x)}(v(x)) = 0$ *ssi* $v(x) \in \mathcal{C}$;

d) *si* $c(x) \in \mathcal{C}$, *on a* $R_{g(x)}(c(x) + e(x)) = R_{g(x)}(e(x))$;

e) *si* $R_{g(x)}(e(x)) = R_{g(x)}(e'(x))$ *et soit* $e(x)$ *soit* $e'(x)$ *ont poids au plus* $\lfloor (d-1)/2 \rfloor$, *alors* $e(x) = e'(x)$;

f) $R_{g(x)}(v(x)) = v(x)$ *si* $\deg v(x) < n - k$.

Démonstration. Exercice. □

Définition 3.1. *Pour tout $v(x) \in R_n$, le polynôme $S(v(x)) := R_{g(x)}(x^{n-k}v(x))$ est appelé le* polynôme syndrome *de $v(x)$.*

Par le point c) de la Proposition 3.1, on a que $S(v(x)) = 0$ ssi $v(x) \in \mathcal{C}$.

Pas 1. On pré-calcule (une seule fois) les polynômes syndrome $S(e(x))$ de toutes les erreurs $e(x) = e_0 + \ldots + e_{n-1}x^{n-i}$ t.q. $\mathrm{wt}(e(x)) \leq \lfloor (d-1)/2 \rfloor$ et $e_{n-1} \neq 0$.
Pas 2. Supposons que $y(x) = c(x) + e(x)$, avec $c(x) \in \mathcal{C}$, soit le vecteur reçu. On calcule le polynôme syndrome $S(y(x))$. Si $S(y(x)) = 0$ alors $y(x) = c(x) \in \mathcal{C}$ et on a fini. Sinon, par le point d) de la Proposition 3.1, on a que $S(y(x)) = S(e(x))$.
Pas 3. Si $S(y(x))$ est dans la liste calculé au pas 1., alors on a trouvé l'erreur $e(x)$ et on peut reconstruire $c(x) = y(x) - e(x)$. Sinon, on va au Pas 4.
Pas 4. On calcule successivement $S(xy(x)), S(x^2y(x)), \ldots$, jusqu'à trouver un polynôme qui est contenu dans la liste calculé au pas 1.. S'il s'agit de $S(x^iy(x))$ et si $e(x)$ est l'erreur correspondante, alors on peut reconstruire $c(x) = y(x) - x^{n-i}e(x)$.

Ce dernier pas est aidé par le résultat suivant (exercice) : si $S(y(x)) = s_0 + \ldots + s_{n-k-1}x^{n-k-1}$, alors

$$S(xy(x)) = xS(y(x)) - s_{n-k-1}g(x).$$

Grâce à la cyclicité, on a réduit la taille de la liste des syndromes par rapport au décodage classique par syndrome. Par exemple, dans l'algorithme classique pour les codes linéaires binaires de longueur n et capacité de correction e on a

$$1 + n + \binom{n}{2} + \ldots + \binom{n}{e}$$

syndromes à calculer, tandis que pour les codes cycliques binaires de de longueur n et capacité de correction e on a

$$1 + (n-1) + \binom{n-1}{2} + \ldots + \binom{n-1}{e-1}$$

syndromes à calculer.
En plus, on réduit aussi la complexité du calcul des syndromes.

Exemple 3.1. *Soit $\mathcal{C}$ le $[15, 7, 5]$ code cyclique avec polynôme générateur $g(x) = 1 + x^4 + x^6 + x^7 + x^8$. Alors la liste des polynômes syndromes est la suivante, où $S(e(x)) = R_{g(x)}(x^8e(x))$:*

$e(x)$	$S(e(x))$	$e(x)$	$S(e(x))$	$e(x)$	$S(e(x))$
x^{14}	x^7	$x^9 + x^{14}$	$x^2 + x^7$	$x^4 + x^{14}$	$x + x^3 + x^4 + x^5 + x^7$
$x^{13} + x^{14}$	$x^6 + x^7$	$x^8 + x^{14}$	$x + x^7$	$x^3 + x^{14}$	$1 + x^2 + x^3 + x^4 + x^7$
$x^{12} + x^{14}$	$x^5 + x^7$	$x^7 + x^{14}$	$1 + x^7$	$x^2 + x^{14}$	$x + x^2 + x^5 + x^6$
$x^{11} + x^{14}$	$x^4 + x^7$	$x^6 + x^{14}$	$x^3 + x^5 + x^6$	$x + x^{14}$	$1 + x + x^4 + x^5 + x^6 + x^7$
$x^{10} + x^{14}$	$x^3 + x^7$	$x^5 + x^{14}$	$x^2 + x^4 + x^4 + x^6 + x^7$	$1 + x^{14}$	$1 + x^4 + x^6$

pour un total de 15 *polynômes syndrome contre* 121 *syndromes de l'algorithme classique.*

Supposons d'avoir reçu $y(x) = 1 + x^4 + x^7 + x^9 + x^{10} + x^{12}$. *On calcule alors* $S(y(x))$, *qui est égal à* $x + x^2 + x^6 + x^7$. *Il n'est pas dans la liste ci-dessus, donc on doit continuer. On calcule*

$$S(xy(x)) = x(x + x^2 + x^6 + x^7) - g(x) = 1 + x^2 + x^3 + x^4 + x^6,$$

qui n'est pas dans la liste. Alors on calcule

$$S(x^2y(x)) = S(x \cdot xy(x)) = x(1 + x^2 + x^3 + x^4 + x^6) - 0 = x + x^3 + x^4 + x^5 + x^7,$$

qui correspond à l'erreur $x^4 + x^{14}$ *dans la liste, de manière que*

$$c(x) = y(x) - (x^2 + x^{12}) = 1 + x^2 + x^4 + x^7 + x^9 + x^{10}$$

est le mot corrigé.

Exercice 3.1. *Soit* $\mathcal{C}$ *le code de l'Exemple 3.1. Décoder* $y(x) = 1 + x + x^6 + x^7 + x^{10} + x^{11}$.

3.2 Décodage de Peterson–Gorenstein–Zierler

Développé initialement par Peterson en 1960 pour les codes BCH binaires, il est généralisé aux codes BCH non-binaires par Gorenstein et Zieler l'année suivante.

Soit $\mathcal{C}$ un code BCH sur $\mathbb{F}_q$ de longueur n et distance construite δ. On suppose, pour simplifier la tractation, que $\mathcal{C}$ soit BCH au sens strict, mais l'algorithme de Peterson–Gorenstein–Zierler fonctionne pour tous les codes BCH. Soit α une racine primitive n-ième de l'unité dans $\mathbb{F}_{q^m}$, avec m, comme d'habitude, qui est l'ordre de q dans $(\mathbb{Z}/n\mathbb{Z})^*$.

Soit $c(x) \in \mathcal{C}$ le mot émis et $y(x) = c(x) + e(x)$ le mot reçu et on suppose que $w := \mathrm{wt}(e(x)) \leq \lfloor (\delta - 1)/2 \rfloor$ (et donc $2w \leq \delta - 1$). Soient $k_1, k_2, \ldots k_w \in \{1, \ldots, n\}$ les w coordonnées (inconnues) où e est non nul. On a

$$e(x) = e_{k_1}x^{k_1} + \ldots + e_{k_w}x^{k_w}$$

(avec les e_{k_i} inconnus). Le but de l'algorithme est déterminer les k_i et les e_{k_i}, qui nous donnent $e(x)$ et par conséquent $c(x) = y(x) - e(x)$. On remarque que déterminer les k_i équivaut à déterminer les puissance α^{k_i}. Pour $i \in \{1, \ldots, w\}$, on appelle

- k_i une *localisation de l'erreur* ;
- $X_i := \alpha^{k_i} \in \mathbb{F}_{q^m}$ le *nombre localisateur de l'erreur correspondent à la localisation* k_i ;
- $E_i := e_{k_i} \in \mathbb{F}_q$ la *valeur de l'erreur à la localisation* k_i.

Le but de l'algorithme est donc déterminer les w couples $(X_i, E_i) \in \mathbb{F}_{q^m} \times \mathbb{F}_q$ pour $i \in \{1, \ldots, w\}$.

On sait que si $c(x) \in \mathcal{C}$ ssi $c(\alpha^i) = 0$ pour $i \in \{1, \ldots, \delta - 1\}$. Ainsi, $y(\alpha^i) = e(\alpha^i)$ pour $i \in \{1, \ldots, \delta - 1\}$.

Définition 3.2. *On appelle* syndrome *i-ème de $y(x)$ l'élément $S_i = y(\alpha^i) \in \mathbb{F}_{q^m}$, pour $i \in \{1, \ldots, \delta - 1\}$.*

Notons que pour tout $i \in \{1, \ldots, \delta - 1\}$ on

$$S_i = \sum_{j=1}^{w} E_j X_j^i, \tag{3.1}$$

et, si on trouve les nombres localisateurs X_j, ces équations nous donnent un système linéaire qui a comme inconnues les valeurs de l'erreur E_j. Pour déterminer les nombres localisateurs X_j on introduit un nouveau objet.

Définition 3.3. *Le* polynôme localisateur de l'erreur *est le polynôme* (*inconnu*)

$$\sigma(x) = (1 - X_1 x)(1 - X_2 x) \cdots (1 - X_w x) = 1 + \sum_{i=1}^{w} \sigma_i x^i.$$

dont les racines sont les inverses des nombres localisateurs de l'erreur.

En utilisant le fait que les racines de $\sigma(X_i^{-1}) = 0$ et la définition des syndromes on obtient le résultat suivant :

Lemme 3.1.

$$\begin{bmatrix} S_1 & S_2 & S_3 & \cdots & S_w \\ S_2 & S_3 & S_4 & \cdots & S_{w+1} \\ S_3 & S_4 & S_5 & \cdots & S_{w+2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ S_w & S_{w+1} & S_{w+2} & \cdots & S_{2w-1} \end{bmatrix} \begin{bmatrix} \sigma_w \\ \sigma_{w-1} \\ \sigma_{w-2} \\ \vdots \\ \sigma_1 \end{bmatrix} = \begin{bmatrix} -S_{w+1} \\ -S_{w+2} \\ -S_{w+3} \\ \vdots \\ -S_{2w} \end{bmatrix}, \tag{3.2}$$

Démonstration. Pour tout $j \in \{1, \ldots, w\}$ on a

$$\sigma(X_j^{-1}) = 1 + \sigma_1 X_j^{-1} + \cdots + \sigma_w X_j^{-w} = 0.$$

En multipliant par $E_j X_j^{i+w}$, on obtient

$$E_j X_j^{i+w} + \sigma_1 E_j X_j^{i+w-1} + \cdots + \sigma_w E_j X_j^i = 0$$

pour tout $i \in \{1, \ldots, w\}$. Alors

$$\sum_{j=1}^{w} E_j X_j^{i+w} + \sum_{j=1}^{w} \sigma_1 E_j X_j^{i+w-1} + \cdots + \sum_{j=1}^{w} \sigma_w E_j X_j^i = 0,$$

c'est-à-dire, pour tout $i \in \{1, \ldots, w\}$,

$$S_{i+w} + \sigma_1 S_{i+w-1} + \cdots + \sigma_w S_i = 0,$$

ce qui nous donne le système (3.2). □

Ce système nous permettrais de trouver $\sigma(x)$. Il y a deux problèmes : on ne connaît pas la valeur de w et on ne sait pas, a priori, si ce système a une seule solution. Les deux problèmes ont une solution avec ce lemme :

Lemme 3.2. *Soit $\mu \leq \lfloor (\delta-1)/2 \rfloor$ et soit*

$$M_\mu := \begin{bmatrix} S_1 & S_2 & S_3 & \cdots & S_\mu \\ S_2 & S_3 & S_4 & \cdots & S_{\mu+1} \\ S_3 & S_4 & S_5 & \cdots & S_{\mu+2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ S_\mu & S_{\mu+1} & S_{\mu+2} & \cdots & S_{2\mu-1} \end{bmatrix}.$$

Alors M_μ est inversible si $\mu = w$ et singulière si $\mu > w$.

Démonstration. Si $\mu > w$, soient $X_{w+1} = X_{w+1} = \cdots = X_\mu = 0$ et $E_{w+1} = E_{w+1} = \cdots = E_\mu = 0$. On peut montrer facilement que $M_\mu = A_\mu B_\mu A_\mu^T$, avec

$$A_\mu := \begin{bmatrix} 1 & 1 & \cdots & 1 \\ X_1 & X_2 & \cdots & X_\mu \\ \vdots & \vdots & \ddots & \vdots \\ X_1^{\mu-1} & X_2^{\mu-1} & \cdots & X_\mu^{\mu-1} \end{bmatrix} \text{ et } B_\mu := \begin{bmatrix} E_1X_1 & 0 & \cdots & 0 \\ 0 & E_2X_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & E_\mu X_\mu \end{bmatrix}.$$

Ainsi, $\det M_\mu = (\det A_\mu)^2 \det B_\mu$. Clairement, si $\mu > w$, alors $\det B_\mu = 0$. Si $\mu = w$, alors $\det B_\mu \neq 0$ et A_μ est une matrice de Vandermonde, avec les $X_1, \ldots, X_\mu$ distincts, de manière que $\det A_\mu \neq 0$ aussi. □

On a définit tous les objets et énoncé tous les résultats pour pouvoir décrire l'algorithme de Peterson–Gorenstein–Zierler :

Pas 1. On calcule les syndromes S_i pour tout $i \in \{1, \ldots, \delta-1\}$.
Pas 2. Dans l'ordre $\mu = \lfloor (\delta-1)/2 \rfloor$, $\mu = \lfloor (\delta-1)/2 \rfloor - 1, \ldots$ on vérifie si M_μ est singulière et on s'arrête à la première valeur pour laquelle M_μ est inversible. On pose $w = \mu$ et on résout le système (3.2) pour déterminer $\sigma(x)$.
Pas 3. On trouve les racines de $\sigma(x)$ en calculant $\sigma(\alpha^i)$ pour tout $i \in \{0, \ldots, n-1\}$. On inverse les racines pour déterminer les nombres localisateurs X_i.
Pas 4. On résout le système donnes par les équations (3.1) pour obtenir les valeurs E_i.

Pour des remarques par rapport au Pas 4. et d'autres observations par rapport à cet algorithme le lecteur intéressé peut voir les pages 179–183 de [HP10].

Exercice 3.2. *Soit $\mathcal{C}$ le $[15, 7, 5]$ code de l'Exemple 3.1, avec polynôme générateur $g(x) = 1 + x^4 + x^6 + x^7 + x^8$. On considère $\alpha \in \mathbb{F}_{16}$ tel que $\alpha^4 = 1 + \alpha$ comme racine primitive 15-ième de l'unité. Les zéros de $\mathcal{C}$ sont donc $\alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^6, \alpha^8, \alpha^9$ et α^{12}, de manière que $\mathcal{C}$ est un code BCH au sens strict de distance construite δ. Décoder $y(x) = 1 + x + x^5 + x^6 + x^9 + x^{10}$.*

3.3 Décodage de Berlekamp–Massey

L'algorithme de Peterson-Gorenstein-Zierler est efficace par des capacités de correction petites, parce que dans ce cas la matrice au Pas 2. est petite et les calculs sont plus rapides. L'algorithme de Berlekamp-Massey vise à améliorer

le Pas 2. pour rendre l'algorithme efficace pour des capacités de correction plus grandes. Cet algorithme a été introduit par Berlekamp en 1967 et simplifié en 1969 par Massey. Pour plus de détails, le lecteur est renvoyé à [B84].

L'algorithme s'applique aux codes BCH généraux, mais pour simplifier la tractation on va nous restreindre au cas binaire. On utilise donc toute les notations de la Section 3.2 avec cette hypothèse supplémentaire.

L'idée principale est de développer une autre manière de trouver le polynôme localisateur $\sigma(x)$ en substituant au système (3.2) le système donné par les *identités de Newton* :

$$\begin{aligned}
&S_1 + \sigma_1 = 0,\\
&S_2 + \sigma_1 S_1 + 2\sigma_2 = 0,\\
&S_3 + \sigma_1 S_2 + \sigma_2 S_1 + 3\sigma_3 = 0,\\
&\quad\vdots\\
&S_w + \sigma_1 S_{w-1} + \cdots + \sigma_{w-1} S_1 + w\sigma_w = 0,\\
&\text{et pour } j > w\\
&S_j + \sigma_1 S_{j-1} + \cdots + \sigma_w S_{j-w} = 0.
\end{aligned}$$

La preuve du fait que les coefficients σ_i satisfont ces identités peut être trouvé dans [C98, Théorème 3.3]. Il se trouve qu'il suffit de considérer seulement les identités impair qu'on va dénombrer dans la manière suivante (on observe que $i\sigma_i = \sigma_i$ si i est impair) :

$$\begin{aligned}
&(1) \quad S_1 + \sigma_1 = 0,\\
&(2) \quad S_3 + \sigma_1 S_2 + \sigma_2 S_1 + \sigma_3 = 0,\\
&(3) \quad S_5 + \sigma_1 S_4 + \sigma_2 S_3 + \sigma_3 S_2 + \sigma_4 S_1 + \sigma_5 = 0,\\
&\quad\vdots\\
&(\mu) \quad S_{2\mu-1} + \sigma_1 S_{2\mu-2} + \cdots + \sigma_{2\mu-2} S_1 + \sigma_{2\mu-1} = 0,\\
&\quad\vdots
\end{aligned}$$

On définit une séquence de polynômes $\sigma^{(\mu)}(x)$ de degré d_μ

$$\sigma^{(\mu)}(x) = 1 + \sigma_1^{(\mu)} x + \cdots + \sigma_{d_\mu}^{(\mu)} x^{d_\mu}$$

définit comme le polynôme de plus petit degré qui satisfait les μ premières identités de Newton. À tout polynôme $\sigma^{(\mu)}(x)$ on associe un élément, appelé *sa discordance*,

$$\Delta_\mu = S_{2\mu+1} + \sigma_1^{(\mu)} S_{2\mu} + \cdots + \sigma_{2\mu}^{(\mu)} S_1 + \sigma_{2\mu+1}^{(\mu)}$$

qui mesure à quel point $\sigma^{(\mu)}(x)$ est loin de satisfaire la $(\mu+1)$-ième identité.

L'algorithme de Berlekamp-Massey substitue au Pas 2. de l'algorithme de Peterson-Gorenstein-Zierler les pas suivants :

Pas 2.1. On pose $\sigma^{(-1/2)}(x) = \sigma^{(0)}(x) = 1$ et $\Delta_{-1/2} = 1$.
Pas 2.2. Pour tout μ de 0 à $\lfloor(\delta-1)/2\rfloor - 1$ on calcule Δ_μ et :
si $\Delta_\mu = 0$, alors on pose

$$\sigma^{(\mu+1)}(x) := \sigma^{(\mu)}(x),$$

sinon

$$\sigma^{(\mu+1)}(x) := \sigma^{(\mu)}(x) + \Delta_\mu \Delta_\rho^{-1} x^{2(\mu-\rho)} \sigma^{(\rho)}(x),$$

avec $\rho \in \{-(1/2), 0, 1, 2, \ldots, \mu-1\}$ tel que $\Delta_\rho \neq 0$ et $2\rho - d_\rho$ est le plus grand possible.

Le polynôme localisateur de l'erreur $\sigma(x)$ est donc $\sigma^{(\lfloor(\delta-1)/2\rfloor)}(x)$, le dernier polynôme calculé.

Exemple 3.2. *On recalcule le polynôme localisateur de l'erreur pour le vecteur et le code donnés dans l'Exercice 3.2 : on rappelle que $\mathcal{C}$ est le $[15, 7, 5]$ code avec polynôme générateur $g(x) = 1 + x^4 + x^6 + x^7 + x^8$ et on veut décoder $y(x) = 1 + x + x^5 + x^6 + x^9 + x^{10}$. Les syndromes sont $S_1 = y(\alpha) = \alpha^2$, $S_2 = y(\alpha^2) = \alpha^4$, $S_3 = y(\alpha^3) = \alpha^{11}$ et $S_4 = y(\alpha^4) = \alpha^8$. Les identités de Newton qu'on doit considerer sont*

$$(1) \quad \alpha^2 + \sigma_1 = 0,$$
$$(2) \quad \alpha^{11} + \sigma_1 \alpha^4 + \sigma_2 \alpha^2 + \sigma_3 = 0.$$

La table de l'algorithme de Berlekamp-Massey est la suivante :

μ	$\sigma^{(\mu)}(x)$	Δ_μ	d_μ	$2\mu - d_\mu$
$-1/2$	1	1	0	-1
0	1	α^2	0	0
1	$1 + \alpha^2 x$	α	1	1
2	$1 + \alpha^2 x + \alpha^{14} x^2$			

de manière que le polynôme localisateur de l'erreur est $\sigma(x) = 1 + \alpha^2 x + \alpha^{14} x^2$.

Exercice 3.3. *Implémenter l'algorithme avec* MAGMA.

3.4 Décodage de Berlekamp-Welch

L'algorithme de Berlekamp-Welch est un algorithme de décodage efficace des codes de Reed-Solomon. On rappelle qu'un code de Reed-Solomon est défini de la manière suivante : soit $\mathbb{F}_q$ un corps fini et soient $a_1, \ldots, a_n$ n éléments distincts de $\mathbb{F}_q$. Le code de Reed-Solomon de dimension k est défini par

$$\mathcal{C} = \{(f(a_1), \ldots, f(a_n)) \mid f(x) \in \mathbb{F}_q[x] \text{ de degré } \leq k\}.$$

Il peut corriger jusqu'à $t = \lfloor \frac{n-k+1}{2} \rfloor$ erreurs.

Soit $c_f \in \mathcal{C}$ le mot transmis, correspondant au polynôme $f(x)$. Soit $y = (y_1, \ldots, y_n)$ le mot reçu. Supposons qu'il y a eu e erreurs, avec $e \leq t$.

Soit

$$E(x) = \prod_{i : f(a_i) \neq y_i} (x - a_i) = x^e + e_{e-1} x^{e-1} + \ldots + e_1 x + e_0.$$

le *polynôme localisateur*. Clairement, pour tout $i \in \{1, \ldots, n\}$, on a soit $f(a_i) = y_i$ soit $E(a_i) = 0$. Cela se traduit par

$$f(a_i) E(a_i) = y_i E(a_i), \quad i \in \{1, \ldots, n\}.$$

Dans ce système (non-linéaire) à n équation, les inconnus sont les coefficients de f et de E. Soit $F = f \cdot E$, qui est de degré inférieur à $t+k$. On a donc

$$F(a_i) - y_i E(a_i) = 0, \quad i \in \{1, \dots, n\},$$

c'est-à-dire

$$a_i^{t+k-1} F_{t+k-1} + \dots + F_0 - y_i a_i^{e-1} e_{e-1} - \dots - a_i e_1 - e_0 = y_i a_i^e, \quad i \in \{1, \dots, n\}.$$

Il y a n équation pour au plus $k + \frac{n-k+1}{2} - 1 + \frac{n-k+1}{2} = n$ inconnus (c'est-à-dire $\{F_j\}$ et $\{e_j\}$). On peut résoudre le système avec la méthode qu'on veut. Puis, on obtient f en divisant F par E. Tout cela suppose qu'on a bien deviné e. La divisibilité de F par E et la distance de c_f de y (qui doit être inférieure à t) seront des tests pour cela.

Exemple 3.3. *Soit*

$$\mathcal{C} = \{(f(0), f(1), \dots, f(6)) \mid f(x) \in \mathbb{F}_7[x] \text{ de degré } \leq 2\}$$

le code de Reed-Solomon de paramètres $[7,3,5]_7$. *On a* $t = 2$. *Soit*

$$f = 3x^2 + 2x + 1,$$

de manière que

$$c_f = (1,6,3,6,1,2,2)$$

soit le mot transmis. Supposons que

$$y = (1,5,3,6,3,2,2)$$

soit le mot reçu (ici l'erreur est dans la deuxième et dans la cinquième coordonnée). On commence en supposant $e = 2$, *de manière que*

$$E(x) = (x-1)(x-4) = x^2 + e_1 x + e_0 = x^2 + 2x + 4$$

qui n'est pas connu. On a

$$F(x) = (3x^2+2x+1)(x^2+2x+4) = 3x^4+x^3+3x^2+3x+4 = F_4x^4+F_3x^3+F_2x^2+F_1x+F_0,$$

qui n'est pas connu, et il a degré inférieur à $2+3$. *On a*

$$F(0) - y_1 E(0) = 0,$$

c'est-à-dire

$$F_0 + 6e_0 = 0.$$

Puis

$$F(1) - y_2 E(1) = 0,$$

c'est-à-dire

$$F_4 + F_3 + F_2 + F_1 + F_0 + 2(1 + e_1 + e_0),$$

etc., d'où le système

$$\begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 0 & 6 \\ 1 & 1 & 1 & 1 & 1 & 2 & 2 \\ 2 & 1 & 4 & 2 & 1 & 1 & 4 \\ 4 & 6 & 2 & 3 & 1 & 3 & 1 \\ 4 & 1 & 2 & 4 & 1 & 2 & 4 \\ 2 & 6 & 4 & 5 & 1 & 4 & 5 \\ 1 & 6 & 1 & 6 & 1 & 2 & 5 \end{bmatrix} \begin{bmatrix} F_4 \\ F_3 \\ F_2 \\ F_1 \\ F_0 \\ e_1 \\ e_0 \end{bmatrix} = \begin{bmatrix} 0 \\ 5 \\ 5 \\ 5 \\ 6 \\ 1 \\ 2 \end{bmatrix}$$

d'où $F(x) = 3x^4 + x^3 + 3x^2 + 3x + 4$ *et* $E(x) = x^2 + 2x + 4$. *Si on divise* $F(x)$ *par* $E(x)$ *on trouve* $f(x)$ *avec reste* 0.

Exercice 3.4. *Soit* $\mathcal{C}$ *comme dans l'Exemple 3.3. Utiliser l'algorithme de Berlekamp-Welch pour corriger le mot reçu* $y = (0, 3, 0, 6, 1, 3, 1)$.

Exercice 3.5. *Implémenter l'algorithme avec* MAGMA.

Chapitre 4

Codes en métrique rang

La théorie de la métrique rang a été introduite par Delsarte comme alternative à la métrique de Hamming en 1978 [D78] et puis développée par Gabidulin en 1985 [G85], qui a montré l'existence d'une famille de codes atteignant une borne analogue à la borne du Singleton, et décodables en un temps polynomial. Les codes en métrique rang ne sont pas facilement utilisables pour la détection et la correction des erreurs, car les canaux de communication réels introduisent rarement une erreur qui soit modélisée efficacement en métrique rang.

Cependant, les outils de cette métrique sont adaptés au codage réseau : ce dernier est un domaine de recherche qui a vu le jour dans une série d'articles entre la fin des années 1990 et le début des années 2000. Le concept de codage réseau linéaire est toutefois antérieur à cette période. En 1978, un schéma visant à améliorer le débit d'une communication bidirectionnelle par satellite a été proposé. Dans ce schéma, deux utilisateurs en communication transmettaient leurs flux de données à un satellite, combinant les deux flux en les additionnant modulo 2 et diffusant ensuite le flux combiné. Chacun des deux utilisateurs, à la réception du flux diffusé, peut décoder l'autre flux en utilisant les informations de son propre flux.

Plus récemment, les codes en métrique rang ont été étudié pour leurs possibles applications à la cryptographie basée sur les codes.

Dans ce chapitre, on va introduire les notions de base de cette théorie. Pour tout résultat sans preuve, on renvoie le lecteur à [G19] et aux références qui y figurent.

4.1 Premières définitions

Soient n, m des entiers positifs. On indique avec $\mathbb{F}_q^{n\times m}$ l'ensemble des matrices $n \times m$ à coefficients dans $\mathbb{F}_q$.

Définition 4.1. *La fonction*

$$d_R : \mathbb{F}_q^{n\times m} \times \mathbb{F}_q^{n\times m} \to \mathbb{Z}, \qquad (A, B) \mapsto \operatorname{rank}(A - B)$$

est une distance (exercice), appelée distance rang. *Le rang est la fonction poids correspondante.*
Un code (de matrices) en métrique rang *est un $\mathbb{F}_q$-sous-espace $\mathcal{C} \subseteq \mathbb{F}_q^{n\times m}$.*

Une classe de codes en métrique rang qui a reçu beaucoup d'attention est celle de codes vectoriels en métrique rang.

Définition 4.2. *Le* poids rang *d'un vecteur $v = (v_1, \dots, v_n) \in \mathbb{F}_{q^m}^n$ est défini par*

$$\operatorname{rank}(v) = \dim\langle v_1, \dots, v_n\rangle_{\mathbb{F}_q},$$

au quel on peut associer la distance

$$d_R : \mathbb{F}_{q^m}^n \times \mathbb{F}_{q^m}^n \to \mathbb{Z}, \qquad (u, v) \mapsto \operatorname{rank}(u - v).$$

Un code vectoriel en métrique rang *est un $\mathbb{F}_{q^m}$-sous-espace $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$.*

Tout code vectoriel peut être regardé comme un code (de matrices) en métrique rang, en choisissant une base de $\mathbb{F}_{q^m}$ sur $\mathbb{F}_q$ et en mettant les coefficients en ligne.

Définition 4.3. *Soit $\Gamma = \{\gamma_1, \gamma_2, \dots, \gamma_m\}$ une base de $\mathbb{F}_{q^m}$ sur $\mathbb{F}_q$ et soit $v \in \mathbb{F}_{q^m}^n$. On définit $\Gamma(v) \in \mathbb{F}_q^{n\times m}$ par*

$$v_i = \sum_{j=1}^{m} \Gamma_{i,j}(v)\gamma_j,$$

pour tout $i \in \{1, \dots, n\}$. Pour un code vectoriel $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$, l'ensemble

$$\Gamma(\mathcal{C}) = \{\Gamma(c) \mid c \in \mathcal{C}\}$$

est appelé code en métrique rang associé à $\mathcal{C}$ par rapport à Γ.

On va illustrer cela avec un exemple.

Exemple 4.1. *Soit $\mathcal{C} = \langle(1, \alpha)\rangle \subseteq \mathbb{F}_8^2$, où $\mathbb{F}_8 = \mathbb{F}_2[\alpha]$ avec $\alpha^3 = \alpha + 1$. Soit $\Gamma = \{1, \alpha, \alpha^2\}$ une base de $\mathbb{F}_8$. Alors la matrice associée à $(1, \alpha)$ dans la base Γ est*

$$\Gamma((1, \alpha)) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}.$$

Si on veut une base pour $\mathcal{C}$ comme $\mathbb{F}_2$-sous-espace de $\mathbb{F}_2^{2\times 3}$ on peut multiplier $(1, \alpha)$ par α et par α^2. On obtien donc

$$\Gamma(\mathcal{C}) = \left\langle \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix} \right\rangle \subseteq \mathbb{F}_2^{2\times 3}.$$

Lemme 4.1. *La fonction $v \mapsto \Gamma(v)$ est une isométrie $\mathbb{F}_q$-linéaire. En particulier, si $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ est un code vectoriel de dimension k sur $\mathbb{F}_{q^m}$, alors $\Gamma(\mathcal{C})$ est un code en métrique rang de dimension mk sur $\mathbb{F}_q$.*

Démonstration. Exercice. □

Définition 4.4. *La* distance minimale *d'un code en métrique rang* $0 \neq \mathcal{C} \subseteq \mathbb{F}_q^{n\times m}$ *est l'entier positif*

$$d_R(\mathcal{C}) = \min_{0\neq c\in\mathcal{C}} \operatorname{rank}(c).$$

La distance minimale *d'un code vectoriel en métrique rang* $0 \neq \mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ *est l'entier positif*

$$d_R(\mathcal{C}) = \min_{0\neq c\in\mathcal{C}} \operatorname{rank}(c).$$

On dit qu'un code vectoriel en métrique rang $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ *a paramètres* $[n,k,d]_{q^m/q}$ *si* k *est sa dimension sur* $\mathbb{F}_{q^m}$ *et* d *est sa distance minimale.*

Comme dans la métrique de Hamming, on a une borne de Singleton, montré dans [D78, Theorem 5.4].

Théorème 4.1. *Soit* $\mathcal{C} \subseteq \mathbb{F}_q^{n\times m}$ *code en métrique rang. Alors*

$$\dim_{\mathbb{F}_q} \mathcal{C} \leq \max\{n,m\}(\min\{n,m\} - d_R(\mathcal{C}) + 1).$$

Si $\mathcal{C}$ est un $[n,k,d]_{q^m/q}$ code vectoriel alors

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

Cela suit clairement du Théorème 4.1 si $n \leq m$ et il est facile de le vérifier pour tout n, m.

Définition 4.5. *Un code* $\mathcal{C} \subseteq \mathbb{F}_q^{n\times m}$ *en métrique rang est un MRD code* (maximum rank distance code) *si*

$$\dim_{\mathbb{F}_q} \mathcal{C} = \max\{n,m\}(\min\{n,m\} - d_R(\mathcal{C}) + 1).$$

Un $[n,k,d]_{q^m/q}$ *code vectoriel en métrique rang est dit MRD si* $k = n - d + 1$.

Exercice 4.1. *Soit* $\mathcal{C} \subseteq \mathbb{F}_q^{n\times m}$ *un code métrique rang et* $\Gamma = \{\gamma_1, \ldots, \gamma_m\}$ *une base de* $\mathbb{F}_{q^m}$ *sur* $\mathbb{F}_q$.

1. *Montrer que, si* $n \leq m$, *alors* $\mathcal{C}$ *est MRD ssi* $\Gamma(\mathcal{C})$ *est MRD.*
2. *Montrer que, si* $n > m$, 0 *et* $\mathbb{F}_{q^m}^n$ *sont les seuls codes vectoriels MRD.*

4.2 Dualité et identités de MacWilliams

On peut définir le dual d'un code vectoriel en métrique rang de façon identique que pour un code en métrique de Hamming (en effet, cela ne dépend en aucune manière de la métrique). Par contre, on a une notion de dual pour les codes de matrices.

Définition 4.6. *Le dual d'un code* $\mathcal{C} \subseteq \mathbb{F}_q^{n\times m}$ *est*

$$\mathcal{C}^\perp := \{M \in \mathbb{F}_q^{n\times m} \mid \operatorname{Tr}(MN^T) = 0 \text{ pour tout } N \in \mathcal{C}\}.$$

Exercice 4.2. *Soient* $\Gamma = \{\gamma_1, \dots, \gamma_m\}$ *et* $\Gamma' = \{\gamma'_1, \dots, \gamma'_m\}$ *deux bases de* $\mathbb{F}_{q^m}$ *sur* $\mathbb{F}_q$ *telles que*

$$\mathrm{Tr}_{q^m/q}(\gamma_i \gamma'_j) = \delta_{i,j}.$$

(c'est-à-dire deux bases orthogonales*). Montrer que*

$$\Gamma(\mathcal{C})^\perp = \Gamma'(\mathcal{C}^\perp)$$

pour tout $\mathcal{C} \subseteq \mathbb{F}_q^{n\times m}$.

Exercice 4.3. *Trouver* Γ' *et* $\Gamma'(\mathcal{C}^\perp)$ *pour le code de l'Exemple 4.1.*

Définition 4.7. *Soit* $\mathcal{C} \subseteq \mathbb{F}_q^{n\times m}$ *un code en métrique rang. La* distribution des poids *de* $\mathcal{C}$ *est la collection de nombres naturels*

$$A_i(\mathcal{C}) = \#\{M \in \mathcal{C} \mid \mathrm{rank}(M) = i\},$$

pour $i \in \{0, \dots, \min\{m, n\}\}$.

Théorème 4.2 (Identités de MacWilliams)**.** *Soit* $\mathcal{C} \subseteq \mathbb{F}_q^{n\times m}$ *un code en métrique rang. Pour tout* $\ell \in \{0, 1, \dots, \min\{m, n\}$ *on a*

$$\sum_{i=0}^{\min\{m,n\}-\ell} A_i(\mathcal{C}) \begin{bmatrix} \min\{m,n\} - i \\ \ell \end{bmatrix}_q = \frac{\#C}{q^{\max\{m,n\}\cdot\ell}} \sum_{j=1}^{\ell} A_j(\mathcal{C}^\perp) \begin{bmatrix} \min\{m,n\} - j \\ \ell - j \end{bmatrix}_q$$

où

$$\begin{bmatrix} a \\ b \end{bmatrix}_q = \begin{cases} 0 & \text{si } a < 0, b < 0, \text{ ou } b > a, \\ 1 & \text{si } b = 0 \text{ et } a \geq 0, \\ \frac{(q^a-1)\cdots(q^{a-b+1}-1)}{(q^b-1)\cdots(q-1)} & \text{autrement.} \end{cases}$$

Ce dernier est appelé q-ième coefficient de Gauss.

Corollaire 4.1. *Soit* $\mathcal{C} \subseteq \mathbb{F}_q^{n\times m}$ *un code en métrique rang. Alors* $\mathcal{C}$ *est MRD ssi* $\mathcal{C}^\perp$ *est MRD.*

Lemme 4.2. *Soit* $\mathcal{C} \subseteq \mathbb{F}_q^{n\times m}$ *un code en métrique rang. Alors*

$$\dim_{\mathbb{F}_q} \mathcal{C} + \dim \mathcal{C}^\perp = mn.$$

En outre,

$$d_R(\mathcal{C}) + d_R(\mathcal{C}^\perp) \leq \min\{m, n\} + 2$$

et on a l'égalité ssi $\mathcal{C}$ *est MRD.*

Démonstration. La première égalité est triviale.
Pour montrer l'inégalité, on suppose $n \leq m$ sans perte de généralité. Par le Théorème 4.1 on a

$$\dim_{\mathbb{F}_q} \mathcal{C} \leq m(n - d_R(\mathcal{C}) + 1)$$

et

$$mn - \dim_{\mathbb{F}_q} \mathcal{C} = \dim_{\mathbb{F}_q} \mathcal{C}^\perp \leq m(n - d_R(\mathcal{C}^\perp) + 1).$$

c'est-à-dire

$$\dim_{\mathbb{F}_q} \mathcal{C} \geq m(1 - d_R(\mathcal{C}^\perp)).$$

d'où l'inégalité. La deuxième partie suit du Corollaire 4.1. □

4.3 Polynômes linéarisés et codes de Gabidulin

Les polynômes linéarisés (ou linéaires) forment un anneau non-commutatif et nous servirons pour définir les codes de Gabidulin. Ils sont appelés aussi q-polynômes et ils ont été introduits en 1933 par Ore comme exemple de polynômes tordus.

Définition 4.8. *Un polynôme $p(x) \in \mathbb{F}_{q^m}[x]$ est un* polynôme linéarisé *s'il est de la forme*

$$p(x) = p_0 x^{[0]} + p_1 x^{[1]} + \dots p_r x^{[r]},$$

où $x^{[i]} = x^{q^i}$ et $p_r \neq 0$. On dit que r est le q-degré de $p(x)$. L'ensemble des polynôme linéarisés sur $\mathbb{F}_{q^m}$ est indiqué $\mathbb{L}_{q^m}[x]$.

Notons que, si $p(x) \in \mathbb{L}_{q^m}[x]$, l'application $\mathrm{ev}_{p(x)} : \mathbb{F}_{q^m} \to \mathbb{F}_{q^m}$, $a \mapsto p(a)$ est $\mathbb{F}_q$-linéaire (exercice).

Une q-matrice de Vandermonde, ou matrice de Moore, associée à un vecteur $(a_1, \dots, a_n) \in \mathbb{F}_{q^m}^n$ est une matrice dans $\mathbb{F}_{q^m}^{s\times n}$ définie par

$$\mathcal{M}_{s,q}(a) := \begin{bmatrix} a_1^{[0]} & a_2^{[0]} & \dots & a_n^{[0]} \\ a_1^{[1]} & a_2^{[1]} & \dots & a_n^{[1]} \\ \vdots & \vdots & \ddots & \vdots \\ a_1^{[s-1]} & a_2^{[s-1]} & \dots & a_n^{[s-1]} \end{bmatrix}$$

On peut montrer que, si $n = s$, le déterminant de $\mathcal{M}_{s,q}(a)$ est différent de zéro ssi $a_1, a_2, \dots, a_n$ sont indépendants sur $\mathbb{F}_q$.

On peut maintenant donner la définition des codes introduits par Gabidulin en [G85].

Définition 4.9. *Un code (vectoriel en métrique rang) de Gabidulin de longueur $n \leq m$ et dimension k sur $\mathbb{F}_{q^m}$ associé à un vector $g \in \mathbb{F}_{q^m}^n$ tel que* $\mathrm{rank}(g) = n$, *noté $\mathcal{G}_{n,k}(g)$, est un code dont une matrice génératrice est*

$$G = \mathcal{M}_{k,q}(g).$$

De façon complètement équivalente (exercice), on peut définir

$$\mathcal{G}_{n,k}(g) = \{(p(g_1), \dots, p(g_n)) =: p(g) \mid p(x) \in \mathbb{L}_{q^m}[x]_{<k}\},$$

où $\mathbb{L}_{q^m}[x]_{<k}$ est l'ensemble de polynômes linéarisés de q-degré inférieur à k.

Théorème 4.3. *Tout code de Gabidulin est MRD, c'est-à-dire $\mathcal{G}_{n,k}(g)$ est un $[n, k, n-k+1]_{q^m/q}$ code en vectoriel en métrique rang.*

Démonstration. L'ensemble des racines d'un polynôme linéarisé $p(x)$ est un $\mathbb{F}_q$-sous-espace de $\mathbb{F}_{q^m}$ (en effet c'est le noyau de l'application d'évaluation) et si le q-degré est inférieur à k, sa dimension est au plus $k-1$.

Un mot de $\mathcal{G}_{n,k}(g)$ est l'évaluation d'un polynôme $p(x)$ sur une base de $\mathbb{F}_{q^m}$ sur $\mathbb{F}_q$, de manière que (graçe au Théorème du rang)

$$\mathrm{rank}(p(g)) = n - \dim \ker \mathrm{ev}_{p(x)} \geq n - k + 1.$$

L'énoncé suit de la borne du Théorème 4.1. □

Annexe A

Corrigé des exercices

A.1 Codes cycliques

Exercice A.1.1. *Soit $\mathcal{C}$ un code linéaire. Montrer que* $\mathrm{Aut}(\mathcal{C}) = \mathrm{Aut}(\mathcal{C}^\perp)$.

Solution. Si $\sigma \in \mathrm{Aut}(\mathcal{C})$, alors $\sigma^{-1} \in \mathrm{Aut}(\mathcal{C})$. Soit $h \in \mathcal{C}^\perp$. On a $\langle h^\sigma, c\rangle = \langle h, c^{\sigma^{-1}}\rangle = 0$ pour tout $c \in \mathcal{C}$, de manière que $h^\sigma \in \mathcal{C}^\perp$, ce qui implique $\sigma \in \mathrm{Aut}(\mathcal{C}^\perp)$. Donc $\mathrm{Aut}(\mathcal{C}) \subseteq \mathrm{Aut}(\mathcal{C}^\perp)$. L'autre inclusion suit du fait que $(\mathcal{C}^\perp)^\perp = \mathcal{C}$.

Exercice A.1.2. *Montrer que le code linéaire $\mathcal{D}$ avec matrice génératrice*

$$G := \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \end{bmatrix}$$

est cyclique.

Solution. Une matrice de parité de $\mathcal{D}$ est

$$H := \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix},$$

d'où on obtient facilement que $\mathcal{D}^\perp$ est cyclique. Par l'exercice précèdent, $\mathcal{D}$ est cyclique aussi.

Exercice A.1.3. *Donner le polynôme générateur du code $\mathcal{D}$ introduit dans l'Exercice A.1.2 et sa matrice génératrice correspondante.*

Solution. En faisant la somme de la première ligne avec la troisième ligne de G on obtient $c = (1,0,1,0,0,0,0,0)$ qui correspond à $c(x) = x^2 + 1 \in \mathcal{D}$. Ni 1, ni x,

ni $x+1$ sont dans $\mathcal{D}$ (on le voit facilement à partir de la matrice G). Donc x^2+1 est le polynôme monique de degré minimal dans $\mathcal{D}$ et il est donc son polynôme générateur. La matrice génératrice correspondante est

$$\begin{bmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \end{bmatrix}.$$

Exercice A.1.4. *Soit $\mathcal{C}$ l'idéal $\langle x^3+x^2+2x+2\rangle$ dans $\mathbb{F}_3[x]/\langle x^6-1\rangle$. En déterminer une matrice génératrice. Quelle est sa distance minimale ?*

Solution. Notons que $x^6-1=(x^3+x^2+2x+2)(x^3+2x^2+2x+1)$, de manière que tout polynôme dans $\mathcal{C}$ est divisible par x^3+x^2+2x+2 dans $\mathbb{F}_3[x]$. Ainsi x^3+x^2+2x+2 est le polynôme générateur de $\mathcal{C}$. Donc une matrice génératrice de $\mathcal{C}$ est

$$G := \begin{bmatrix} 2 & 2 & 1 & 1 & 0 & 0 \\ 0 & 2 & 2 & 1 & 1 & 0 \\ 0 & 0 & 2 & 2 & 1 & 1 \end{bmatrix},$$

qu'on peut réduire en forme systématique :

$$G' := \begin{bmatrix} 1 & 0 & 0 & 2 & 2 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 2 & 2 \end{bmatrix},$$

pour obtenir qu'une matrice de parité pour $\mathcal{C}$ est

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

On observe qu'il n'y a pas de colonnes nulles, ni égales dans H, de manière que la distance minimale de $\mathcal{C}$ est au moins 3. Puisque la deuxième ligne de G' a poids 3, la distance minimale de $\mathcal{C}$ est 3.

Exercice A.1.5. *Quel est l'idéal qui décrit le code cyclique*

$$\{(0,0,0,0),(0,1,0,1),(1,0,1,0),(1,1,1,1)\} \subseteq \mathbb{F}_2^4 \ ?$$

Solution. C'est l'idéal $\langle x^2+1\rangle$.

Exercice A.1.6. *Déterminer le polynôme générateur du plus petit code cyclique dans $\mathbb{F}_2^7$ qui contient le mot $(0,0,1,1,0,1,0)$.*

Solution. Soit $\mathcal{C}$ le plus petit code cyclique dans $\mathbb{F}_2^7$ qui contient le mot $x^5 + x^3 + x^2$. Alors $x^3 + x + 1 \in \mathcal{C}$ et donc $\langle x^3 + x + 1 \rangle \subseteq \mathcal{C}$. Puisque $\mathcal{C}$ est le plus petit code cyclique, $\mathcal{C} = \langle x^3 + x + 1 \rangle$. Notons que $x^7 + 1 = (x^3 + x + 1)(x^4 + x^2 + x + 1)$ de manière que tout polynôme dans $\mathcal{C}$ est divisible par $x^3 + x + 1$ dans $\mathbb{F}_2[x]$. Ainsi $x^3 + x + 1$ est le polynôme générateur de $\mathcal{C}$ et une matrice génératrice pour $\mathcal{C}$ est

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

Exercice A.1.7. *Donner le polynôme de contrôle du code $\mathcal{D}$ introduit dans l'Exercice A.1.2 et la matrice de parité correspondante.*

Solution. On a $x^8 + 1 = (x^2 + 1)(x^6 + x^4 + x^2 + 1)$, de manière que $h(x) = x^6 + x^4 + x^2 + 1$ est le polynôme de contrôle. La matrice de parité correspondante est

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

Exercice A.1.8. *Montrer que le code de longueur 7 sur $\mathbb{F}_2$ avec polynôme générateur $x^3 + x + 1$ est le dual du code de longueur 7 sur $\mathbb{F}_2$ avec polynôme générateur $x^4 + x^3 + x^2 + 1$.*

Solution. Le code $\mathcal{C}$ de longueur 7 sur $\mathbb{F}_2$ avec polynôme générateur $g(x) = x^3 + x + 1$ a polynôme de contrôle égal à $h(x) = x^4 + x^2 + x + 1$, car $x^7 + 1 = (x^3 + x + 1)(x^4 + x^2 + x + 1)$. Ainsi, le dual de $\mathcal{C}$ a polynôme générateur

$$g^\perp(x) = x^4(x^{-4} + x^{-2} + x^{-1} + 1) = x^4(x^3 + x^5 + x^6 + 1) = 1 + x^2 + x^3 + x^4.$$

Exercice A.1.9. *Soit $\mathcal{C}$ le code cyclique binaire de longueur 15 de polynôme générateur $g(x) = x^4 + x + 1$. Donner une matrice génératrice et une matrice de parité de $\mathcal{C}$ et en trouver la distance minimale. Quel est le code $\mathcal{C}$? Corriger le mot reçu $(0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0)$.*

Solution. Une matrice génératrice est

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

En plus, $x^{15} + 1 = (x^4 + x + 1)(x^{11} + x^8 + x^7 + x^5 + x^3 + x^2 + x + 1)$, de manière que une matrice de contrôle est

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

Dans H il n'y a pas de colonnes nulles, ni égales. La cinquième colonne est la somme de la première et la deuxième, de manière que la distance minimale est 3. Puisque les colonnes de H sont tous les vecteurs non nuls de $\mathbb{F}_2^4$, on a que $\mathcal{C}$ est équivalent au code de Hamming $\mathcal{H}_3$.

$$\begin{aligned}(0,0,0,0,0,1,1,0,1,1,0,0,0,0,0)H^T &= (0,1,0,1)\\ &= (0,0,0,0,0,0,0,0,1,0,0,0,0,0,0)H^T,\end{aligned}$$

de manière que le mot corrigé est $(0,0,0,0,0,1,1,0,0,1,0,0,0,0,0)$.

Exercice A.1.10. *Soient a, b deux entiers positifs. Montrer que $x^a - 1$ divise $x^b - 1$ dans $K[x]$, avec K un corps quelconque, si et seulement si a divise b dans $\mathbb{Z}$.*

Solution. Pour tout $c \in \mathbb{N}$, $x^a - 1$ divise

$$x^{ac} - 1 = (x^a)^c - 1 = (x^a - 1)(x^{a(c-1)} + \ldots + 1).$$

Soit $b = ac + r$, avec $0 \leq r < a$. On a

$$x^b - 1 = x^{ac+r} - 1 = x^{ac+r} - x^r + x^r - 1 = x^r(x^{ac-1} - 1) + x^r - 1.$$

Alors $x^a - 1$ divise $x^b - 1$ ssi $x^r - 1 = 0$, c'est-à-dire ssi a divise b.

Exercice A.1.11. *Montrer que, puisque $(n, q) = 1$, la factorisation du polynôme $x^n - 1$ dans $\mathbb{F}_q[x]$ n'a pas de facteurs avec multiplicité plus grande que 1.*

Solution. Supposons que $x^n - 1 = a(x)^2 b(x)$, avec $a(x)$ de degré supérieur à 1. La dérivée de $x^n - 1$ est

$$nx^{n-1} = 2a(x)a'(x)b(x) + a(x)^2 b'(x) = a(x)(\ldots).$$

Puisque $\mathbb{F}_q[x]$ est un anneau factoriel, on a que x divise $a(x)$, ce qui équivaut à $a(0) = 0$, ce qui nous donne une contradiction, puisque

$$0 = a(0)^2 b(0) \neq 0^n - 1 = -1.$$

Exercice A.1.12. *Soit k le nombre des classes cyclotomiques modulo n sur $\mathbb{F}_q$. Montrer qu'il y a exactement 2^k codes cycliques de longueur n sur $\mathbb{F}_q$.*

Solution. Soit $\phi : \mathcal{C} \mapsto g(x)$ l'application qui associe à tout code cyclique son polynôme générateur. Cela est une application bijective de l'ensemble des codes cycliques à l'ensemble des diviseurs de $g(x)$, par le Théorème 1.2. Donc le nombre des codes cycliques de longueur n sur $\mathbb{F}_q$ est égal au nombre des diviseurs de $x^n - 1$ dans $\mathbb{F}_q[x]$. Par l'exercice précédent, si $(n, q) = 1$ le facteurs de $x^n - 1$ dans $\mathbb{F}_q[x]$ sont distingués. En plus, on a vu que le facteurs irréductibles de $x^n - 1$ sont en bijection avec les classes cyclotomiques modulo n sur $\mathbb{F}_q$. Alors il y a

une bijection entre les diviseurs de $x^n - 1$ et les sous-ensembles de l'ensemble des classes cyclotomiques (à tout diviseur $g(x)$ de $x^n - 1$ on associe l'ensemble des classes correspondantes aux facteurs irréductibles de $g(x)$). Cela implique que le nombre des diviseurs de $x^n - 1$ (et donc des codes cycliques de longueur n sur $\mathbb{F}_q$) est égal à la cardinalité de l'ensemble des parties de l'ensemble des classes cyclotomiques, c'est-à-dire 2^k.

Exercice A.1.13. *Soit $n = 17$ et soit α une racine primitive 17-ième de l'unité dans le corps $\mathbb{F}_{2^m}$, où m est l'ordre de 2 modulo 17. Déterminer m et les classes cyclotomiques modulo 17 sur $\mathbb{F}_2$. Quel est le nombre des codes cycliques binaires de longueur 17 ? Quelle est leur dimension ?*

Solution. On a $2^1 \equiv 2 \bmod 17$, $2^2 \equiv 4 \bmod 17$, $2^4 \equiv -1 \bmod 17$ et $2^8 \equiv 1 \bmod 17$, de manière que $m = 8$. On a

$$C_0 = \{0\}, \quad C_1 = \{1, 2, 4, 8, 16, 15, 13, 9\}, \quad C_3 = \{3, 6, 12, 7, 14, 11, 5, 10\}.$$

Il y a trois classes cyclotomiques, donc par l'exercice précédent, on a $2^3 = 8$ codes cycliques binaires de longueur 17. On a que $M_0(x)$ a degré 1, tandis que $M_1(x)$ et $M_3(x)$ ont degré 8. Le code avec polynôme générateur M_0 a dimension $17 - 1 = 16$, les codes avec polynôme générateur $M_1(x)$ ou $M_3(x)$ ont dimension $17 - 8 = 9$, les codes avec polynôme générateur $M_0(x)M_1(x)$ ou $M_0(x)M_3(x)$ ont dimension $17 - 9 = 8$, le code avec polynôme générateur $M_1(x)M_3(x)$ a dimension $17 - 16 = 1$. Finalement, il y a $\mathbb{F}_2^{17}$, qui a dimension 17, et le code nul, qui a dimension 0.

Exercice A.1.14. *Donner la liste des codes cycliques binaires de longueur 7.*

Solution. On a $2^1 \equiv 2 \bmod 7$ et $2^3 \equiv 1 \bmod 7$, de manière que $m = 3$. Soit α une racine primitive 7-ième de l'unité dans $\mathbb{F}_8$. Par exemple, si on considère $\mathbb{F}_8 = \mathbb{F}_2[x]/\langle x^3 + x + 1\rangle$, on peut prendre comme α la racine de $x^3 + x + 1$, c'est-à-dire un élément tel que $\alpha^3 = \alpha + 1$. En effet

$$\alpha^7 = \alpha \cdot (\alpha^3)^2 = \alpha \cdot (\alpha + 1)^2 = \alpha \cdot (\alpha^2 + 1) = \alpha^3 + \alpha = \alpha + 1 + \alpha = 1.$$

Les classes cyclotomiques modulo 7 sur $\mathbb{F}_2$ sont

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

On a

$$\begin{aligned} M_0(x) &= x + \alpha^0 = x + 1 \\ M_1(x) &= (x + \alpha)(x + \alpha^2)(x + \alpha^4) = \ldots = x^3 + x + 1, \\ M_3(x) &= (x + \alpha^3)(x + \alpha^6)(x + \alpha^5) = \ldots = x^3 + x^2 + 1 \end{aligned}$$

de manière que $x^7 + 1 = (x + 1)(x^3 + x + 1)(x^3 + x^2 + 1)$ est une factorisation de $x^7 + 1$ en polynômes irréductibles sur $\mathbb{F}_2$. Les 8 codes cycliques binaires de longueur 7 sont donc

1. Le $[7, 7, 1]$ code cyclique $\mathbb{F}_2^7$ avec polynôme générateur 1.

2. Le $[7,6,2]$ code cyclique avec polynôme générateur $x+1$. Ceci est le code de parité de longueur 7.
3. Le $[7,4,3]$ code cyclique avec polynôme générateur x^3+x+1. Ce code a matrice génératrice

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

4. Le $[7,4,3]$ code cyclique avec polynôme générateur x^3+x^2+1. Ce code a matrice génératrice

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

5. Le $[7,1,7]$ code cyclique avec polynôme générateur $(x^3+x+1)(x^3+x^2+1)$. Ce code a matrice génératrice

$$G := \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

6. Le $[7,3,4]$ code cyclique avec polynôme générateur $(x+1)(x^3+x^2+1)$. Ce code a matrice génératrice

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

7. Le $[7,3,4]$ code cyclique avec polynôme générateur $(x+1)(x^3+x+1)$. Ce code a matrice génératrice

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

8. Le $[7,0,0]$ code cyclique nul.

Notons que le troisième et le quatrième code sont équivalents au code de Hamming $\mathcal{H}_3$.

A.2 Les codes BCH

Exercice A.2.1. *Soit $m \geq 3$ et α une racine primitive (2^m-1)-ième de l'unité dans $\mathbb{F}_{2^m}$. Montrer que α^3 n'est pas une racine du polynôme minimal $M_1(x)$ de α.*

Solution. La classe cyclotomique C_1 de 1 modulo $2^m - 1$ contient sûrement 1 et 2. Si α^3 est une racine de $M_1(x)$, alors 3 aussi est dans C_1. Cela implique, pour la borne BCH, que le code qui a polynôme générateur $M_1(x)$ a distance minimale au moins 4. Mais ce code, comme on a vu, est $\mathcal{H}_m$, qui a distance minimale 3. Donc α^3 n'est pas une racine de $M_1(x)$.

Exercice A.2.2. *Construire un code BCH de longueur* 9 *et de distance construite* 6 *sur* $\mathbb{F}_2$.

Solution. Pour le faire, il faut considérer 5 puissances successives d'une racine primitive 9-ième de l'unité dans $\mathbb{F}_{64}$. Or, les classes cyclotomiques modulo 9 sont

$$C_0 = \{0\}, \quad C_1 = \{1, 2, 4, 8, 7, 5\}, \quad C_3 = \{3, 6\}.$$

Donc on peut considérer $C_0 \cup C_1$ (ce qui donne le $[9, 2, 6]$ code avec polynôme générateur $(x + 1)(x^6 + x^3 + 1)$), $C_1 \cup C_3$ (ce qui donne le $[9, 1, 9]$ code avec polynôme générateur $(x^6 + x^3 + 1)(x^2 + x + 1)$) ou encore $C_0 \cup C_1 \cup C_3$ (ce qui donne le code trivial).

Exercice A.2.3. *Combien de codes BCH au sens strict de longueur* 15 *sur* $\mathbb{F}_2$ *y a-t-il ? Quels sont leurs paramètres ?*

Solution. Les classes cyclotomiques modulo 15 sont

$$C_0 = \{0\},\ C_1 = \{1, 2, 4, 8\},\ C_3 = \{3, 6, 9, 12\},\ C_5 = \{5, 10\},\ C_7 = \{7, 11, 13, 14\}.$$

Donc $M_1(x)$, $M_1(x)M_3(x)$, $M_1(x)M_3(x)M_5(x)$, $M_1(x)M_3(x)M_5(x)M_7(x)$ et $M_1(x)M_3(x)M_5(x)M_7(x)M_0(x)$ sont les 5 polynômes générateurs possibles. Les paramètres sont, respectivement, $[15, 11, 3]$ (code de Hamming), $[15, 7, \geq 5]$ (qui a forcement distance minimale 5, par le Théorème 2.3), $[15, 5, \geq 7]$, $[15, 1, 15]$ (code de répétition) et $[15, 0, 15]$ (code trivial). Pour calculer la distance minimale vraie du troisième, il faut calculer le polynôme générateur et la matrice génératrice. En le faisant, on obtient que la distance minimale est 7.

Annexe B

Quelques exemples d'utilisation de MAGMA

Exemple B.1. *Programme pour construire tous les codes cycliques de longueur n sur $\mathbb{F}_q$.*

```
liste_des_codes_cycliques:=function(n,q);
    if n  in Integers() and q in Integers() and IsPrimePower(q)
    and n ge 1 and Gcd(n,q) eq 1 then
        L:=[];
        K<a>:=GF(q);
        P<x>:=PolynomialRing(K);
        F:=Factorisation(x^n-1);
        for s in Subsets({1..#F}) do
            g:=P!1; for i in s do g:=g*F[i][1]; end for;
            L:=L cat [CyclicCode(n,g)];
        end for;
        return L;
    else
        print("erreur dans les parametres"); return 0;
    end if;
end function;
```

Output de `liste_des_codes_cycliques(4,3);`

```
[
    [4, 3, 2] Cyclic Linear Code over GF(3)
    Generator matrix:
    [1 0 0 1]
    [0 1 0 2]
    [0 0 1 1],
    [4, 4, 1] Cyclic Linear Code over GF(3),
```

```
    [4, 1, 4] Cyclic Linear Code over GF(3)
    Generator matrix:
    [1 1 1 1],
    [4, 3, 2] Cyclic Linear Code over GF(3)
    Generator matrix:
    [1 0 0 2]
    [0 1 0 2]
    [0 0 1 2],
    [4, 2, 2] Cyclic Linear Code over GF(3)
    Generator matrix:
    [1 0 1 0]
    [0 1 0 1],
    [4, 0, 4] Cyclic Linear Code over GF(3),
    [4, 1, 4] Cyclic Linear Code over GF(3)
    Generator matrix:
    [1 2 1 2],
    [4, 2, 2] Cyclic Linear Code over GF(3)
    Generator matrix:
    [1 0 2 0]
    [0 1 0 2]
]
```

Exemple B.2. *Programme pour construire les classes cyclotomiques modulo n sur $\mathbb{F}_q$.*

```
classes_cylotomiques:=function(n,q);
CC:={};
for s in [0..n-1] do
    C:={};
    for i in [0..n-1] do
        C:=C join {s*q^i mod n};
    end for;
    CC:=CC join {C};
end for;
return CC;
end function;
```

Exemple B.3. *Programme sur le décodage de Peterson–Gorenstein–Zierler.*

```
q:=2;
n:=51;
m:=Min({i:i in [1..n]|q^i mod n eq 1});
delta:=11;

F<beta>:=GF(q^m);
alpha:=beta^((q^m-1) div n);
Cl:=[];
for j in [1..n-1] do
Cl[j]:={j*q^i mod n:i in [0..n]};
end for;
PF<xx>:=PolynomialRing(F);
P<x>:=PolynomialRing(GF(q));
Z:={}; for i in [1..delta-1] do Z:=Z join Cl[i]; end for;
p:=1; for j in Z do p:=p*(xx-alpha^j); end for;
p:=P!p;
C:=CyclicCode(n,p);

c:=Polynomial(ElementToSequence(Random(C)));
e:=[0:i in [1..n]];
for i in [1..(delta-1) div 2] do
e[Random([1..n])]:=1;
end for;
e:=P!Polynomial(e);
y:=c+e;

S:=[Evaluate(y,alpha^i):i in [1..delta-1]];

M:=function(mu,S);
s:=[];
for j in [0..mu-1] do
s:=s cat S[1+j..mu+j];
end for;
return Matrix(F,mu,mu,s);
end function;

for j in [0..(delta-1) div 2] do
mu:=(delta-1) div 2-j;
if Determinant(M(mu,S)) ne 0 then w:=mu; break; end if;
end for;

sigma_inverse:=-M(mu,S)^-1*Matrix(F,w,1,S[w+1..2*w]);
sigma:=1;
for j in [0..w-1] do sigma:=sigma+sigma_inverse[w-j][1]*xx^(j+1); end for;
```

```
X:=[r[1]^-1:r in Roots(sigma)];
K:=[Log(alpha,t):t in X];

ee:=0; for k in K do ee:=ee+x^k; end for;

c eq y-ee;
```

Bibliographie

[ACS92] D. Augot, P. Charpin et N. Sendrier. *Studying the locator polynomials of minimum weight codewords of BCH-codes.* IEEE Trans. Inf. Theory, 38(3) :960–973, May 1992.

[B84] E. R. Berlekamp. *Algebraic Coding Theory.* Laguna Hills, CA : Aegean Park Press, 1984.

[BRC60-1] R.C. Bose et D.K. Ray-Chauduri. *On a class of error correcting binary group codes.* Inform. and Control, Mars 1960.

[BRC60-2] R.C. Bose et D.K. Ray-Chauduri. *Further results on error correcting binary group codes.* Inform. and Control, Septembre 1960.

[B52] K.A. Bush. *Orthogonal arrays of index unity.* Ann. Math. Statistics, 23 :426–434, 1952.

[C98] P. Charpin. *Open problems on cyclic codes.* In : V.S. Pless, W.C. Huffman (Eds.), Handbook of Coding Theory, vol. I, pp. 963–1063 (Chapter 11), Elsevier, 1998.

[D78] P. Delsarte. *Bilinear forms over a finite field, with applications to coding theory.* Journal of Combinatorial Theory, Series A, 25(3), 226–241, 1978

[G85] E.M. Gabidulin. *Theory of codes with maximum rank distance.* Problems of Information Transmission, 21(1) : 1–12, 1985.

[G19] E. Gorla. *Rank-metric codes.* arXiv :1902.02650.

[HT72] C.R.P. Hartmann et K.K. Tzeng. *Generalizations of the BCH-bound.* Information and Control, 20 :489–498, 1972.

[H59] A. Hocquenghem. *Codes Correcteurs d'Erreurs.* Chiffres, 1959.

[HP10] W.C. Huffman et V. Pless. *Fundamentals of error-correcting codes.* Cambridge university press, 2010.

[MWS77] F.J. MacWilliams et N.J.A. Sloane. *The Theory of Error Correcting Codes.* Elsevier 1977.

[R83] C. Roos. *A new lower bound for the minimum distance of a cyclic code.* IEEE Trans. Inform. Theory, vol.IT-29 :330–332, 1983.

[S55] B. Segre. *Curve razionali normali e k-archi negli spazi finiti.* Ann. Mat. Pura Appl. (4), 39 :357–379, 1955.

[vLW86] J.H. van Lint et R.M. Wilson. *On the minimum distance of cyclic codes.* IEEE Trans. Inform. Theory, IT-32 :23–40, 1986.