Introduction à l'algèbre pour les Codes cycliques

A. Bonnecaze

2006-2007

Contents

1 Notes sur ce support de cours

Ce support de cours s'adresse aux étudiants de l'ESIL. Les notions ne sont pas introduites d'une manière mathématique. Ici, il est plus important de savoir construire une structure que de connaitre et comprendre les preuves des théorèmes. Ce support aborde les corps finis et les codes cycliques.
Pour ceux qui veulent aller plus loin, voici une petite bibliographie :

1. O. Papini et J. Wolfmann "Algèbre discrète et codes correcteurs" Springer-Verlag. Mathématiques et applications industrielles.
2. G. Cohen, P. Godlewski et J.L. Dornsetter " Codes correcteurs d'erreurs" Telecom Paris.
3. V. Pless, W.C. Hufman "Handbook of Coding Theory" North-Holland, 1998.

2 Rappels algébriques

Voici quelques rappels concernant les structures algébriques. Ces structures sont très utilisées en codage et en cryptologie. Une structure algébrique est un ensemble muni d'une ou plusieurs opérations. Par exemple l'ensemble des entiers $\mathbf{Z}$ muni de l'addition. Dans ce cas, l'opération est dite binaire car elle agit sur deux éléments de $\mathbf{Z}$.
Les ensembles de nombres les plus utilisés sont : l'ensemble $\mathbf{N}$ des entiers naturels, l'ensemble $\mathbf{Z}$ des entiers relatifs, l'ensemble $\mathbf{Q}$ des rationnels, l'ensemble $\mathbf{R}$ des réels et bien sur l'ensemble $\mathbf{C}$ des complexes. En informatique, on utilise le plus souvent des ensembles finis comme par exemple l'alphabet binaire $\mathbf{F}_2 = \{0, 1\}$.

2.1 Groupes

Un groupe est un ensemble G muni d'une opération binaire sur G notée (par exemple) $*$. Il faut de plus que les propriétés suivantes soient vérifiées :

1. l'opération $*$ doit être associative,
2. G admet un élément identité (ou neutre) e : $\forall a \in G, a * e = e * a = a$,
3. G admet un inverse : $\forall a \in G,\ \exists a^{-1} \in G$ tel que $a * a^{-1} = a^{-1} * a = e$.

On note souvent un groupe comme un triplet $(G, *, e)$, ou plus simplement $(G, *)$ ou même G s'il n'y a pas d'ambiguité sur l'élément neutre et l'opération binaire.
Lorsque $*$ est commutative, on dit que le groupe est commutatif ou abélien.

Remarque 1 *Ici l'opération $*$ représente une opération binaire quelconque. Il ne s'agit pas forcément de la multiplication usuelle.*

En fait, il est assez fréquent que l'on utilise une représentation additive lorsque le groupe est abélien. Dans ce cas, la représentation additive de $a^n = a * a * \cdots * a$ (n facteurs) s'écrit $na = a + a + \cdots + a$ (n termes) et l'inverse de a se note $-a$.

Exemple 2.1 $(\mathbf{R}, +, 0)$ *et* $(\mathbf{R} \setminus \{0\}, \cdot, 1)$ *sont des groupes.*

Il existe aussi des groupes finis. Par exemple $\mathbf{Z}_n$ représente l'ensemble des restes par la division par n (n entier positif) de tous les entiers.

$$\mathbf{Z}_n = \{0, 1, \ldots,\ n-1\}.$$

On note respectivement $a + b$ et ab la somme et le produit usuels de a et b réduits modulo n.

Exemple 2.2 *La structure* $(\mathbf{Z}_4, *, 1)$ *peut être définie par sa table de multiplication :*

$*$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Cette structure ne forme pas un groupe car les éléments 0 *et* 2 *n'admettent pas d'inverse (il n'existe pas de* 1 *sur la ligne ou la colonne correspondant à* 0 *ou* 2*).*

Le groupe additif $(\mathbf{Z}_4, +, 0)$ *peut être défini par sa table d'addition :*

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Il est facile de prouver que

Proposition 2.3 $(\mathbf{Z}_n, +, 0)$ *forme, pour tout n, un groupe. C'est le groupe additif des entiers modulo n.*

Par contre $(\mathbf{Z}_n \setminus \{0\}, *, 1)$ n'est pas un groupe car certains éléments n'ont pas d'inverses. Par exemple dans $\mathbf{Z}_4$, l'élément 2 n'est pas inversible. On a

Proposition 2.4 $(\mathbf{Z}_p \setminus \{0\}, *, 1)$ *forme, pour tout p premier, un groupe. C'est le groupe multiplicatif des entiers modulo p. On le note* $\mathbf{Z}_p^*$.

Preuve La seule difficulté est de montrer que tout élément admet un inverse. Pour cela nous avons besoin du résultat bien connu de Bezout :
Soit p un nombre premier, alors tout entier a avec $0 < a < p$ est premier avec p. De plus, il existe deux entiers u et v tels que $au + pv = 1$ où $0 < u < p$.
Ce résultat nous permet d'écrire que $au = 1 \bmod p$. Ainsi u est l'inverse de a dans $\mathbf{Z}_p^\star$. □

Définition 2.5 *Un groupe fini multiplicatif G est dit cyclique s'il admet un élément a tel que pour tout* $b \in G$, *il existe un entier i tel que* $b = a^i$. *L'élément a est alors appelé un générateur du groupe cyclique. On note* $G =< a >$.

Exemple 2.6

1. $(\mathbf{Z}_4, +, 0)$ *est un groupe additif engendré par* 1 *ou* 3.
2. $(\mathbf{Z}_5^\star, \cdot, 1)$ *est un groupe multiplicatif engendré par* 2 *ou* 3.

Définition 2.7 *Le nombre d'éléments d'un groupe G est appelé l'ordre du groupe (noté* $|G|$*).*

Jeu 2.8 *(des 2 erreurs)*

1. $(\mathbf{R}, \cdot, 1)$ *est un groupe*
2. *l'élément* 2 *est un un générateur de* $(\mathbf{Z}_3^\star, \cdot, 1)$
3. $(\mathbf{Z}_4, \cdot, 1)$ *est un groupe*
4. *le groupe des permutations* S_n *admet* $n!$ *éléments.*

Définition 2.9 *un sous-ensemble non vide H d'un groupe G est un sous-groupe de G si H est un groupe pour la même loi. Si* $H \neq G$, *H est appelé sous-groupe propre de G.*

Si G est un groupe abélien (noté additivement), tout sous-groupe de G contient donc 0. Pour montrer que H est un sous-groupe de G, il faut montrer que

(i) $a+b \in H$ pour tout $a, b \in H$, et

(ii) $-a \in H$ pour tout $a \in H$.

Attention : en notation multiplicative, il faut montrer que $a.b \in H$ et $a^{-1} \in H$ pour tout $a, b \in H$.

Exercice 2.10 *Soit G un groupe abélien et H un sous-ensemble fini non vide de G tel que $a+b \in H$ pour tout $a, b \in H$. Montrer que H est un sous-groupe.*

Définition 2.11 *Soit G un groupe et $a \in G$. L'ordre de a est le plus petit entier t positif tel que $a^t = 1$. Lorsque t n'existe pas, l'ordre de a est ∞.*

Proposition 2.12 *Soit G un groupe et $a \in G$ un élément d'ordre fini t. Alors $| < a > | = t$.*

Théorème 2.13 *(de Lagrange) Si G est un groupe fini et H un sous groupe de G, Alors $|H|$ divise $|G|$. Ainsi, si $a \in G$, l'ordre de a divise $|G|$.*

Proposition 2.14 *Tout sous-groupe d'un groupe cyclique G est aussi cyclique. En fait, si G est un groupe cyclique d'ordre n, alors pour chaque diviseur d de n, G contient exactement un sous groupe d'ordre d.*

Proposition 2.15 *Soit G un groupe et $a \in G$.*

(i) Si l'ordre de a est t, alors l'ordre de a^k est $t/PGCD(t,k)$.

(ii) Si G est un groupe cyclique d'ordre n et $d|n$, alors G admet exactement $\phi(d)$ éléments d'ordre d. En particulier G admet $\phi(n)$ générateurs.

Exemple 2.16 *Considérons le groupe multiplicatif $\mathbf{Z}_{19}^* = \{1, 2, \ldots, 18\}$ d'ordre 18. Le groupe est cyclique et $\alpha = 2$ est générateur. Les sous-groupes de $\mathbf{Z}_{19}^*$ ainsi que leurs générateurs sont donnés dans le tableau suivant :*

Sous-groupe	*Générateurs*	*Ordre*
$\{1\}$	1	1
$\{1, 18\}$	18	2
$\{1, 7, 11\}$	$7, 11$	3
$\{1, 7, 8, 11, 12, 18\}$	$8, 12$	6
$\{1, 4, 5, 6, 7, 9, 11, 16, 17\}$	$4, 5, 6, 916, 17$	9
$\{1, 2, 3, \ldots, 18\}$	$2, 3, 10, 13, 14, 15$	18

2.2 Corps et anneaux

On a souvent besoin d'avoir deux opérations binaires distinctes : l'addition et la multiplication. On peut alors construire des structures algébriques plus complexes comme les corps ou les anneaux. Ce sont ces structures qui nous intéressent maintenant.
Un corps F est un ensemble d'éléments dans lequel il est possible de faire des additions, soustractions, multiplications et divisions (à l'exception de zero!).
$+$ et $*$ doivent satisfaire les lois de commutativité, associativité et distributivité.
De plus, pour tout $\alpha \in F$, il doit exister $0,\ 1,\ -\alpha,\ \alpha^{-1}$ tel que

$$\begin{array}{cc} 0+\alpha=\alpha & (-\alpha)+\alpha=0 \\ 1*\alpha=\alpha & 0*\alpha=0 \\ \text{et si } \alpha \neq 0 & (\alpha^{-1})*\alpha=1 \end{array}$$

Un corps fini contient un nombre fini d'éléments : C'est son **ordre**. Les corps finis sont appelés **Corps de Galois**.
Un anneau $(F, +, \cdot)$ admet une structure semblable au corps à ceci près que les éléments de $F^\star$ n'admettent pas forcément un inverse multiplicatif. L'ensemble des inversibles d'un anneau forme un groupe (multiplicatif) appelé le groupe des inversible de R.

Exemple 2.17 *L'anneau des entiers modulo p avec p premier :*

$$\mathbf{Z}_p = \{0, 1, \ldots, \ p-1\}.$$

0 est l'élément neutre additif et 1 l'élément neutre multiplicatif. L'ordre de $\mathbf{Z}_p$ est p puisque $\mathbf{Z}_p$ contient p éléments.

La caractéristique d'un anneau est le plus petit entier n tel que $n.1 = 0$. La caractéristique de $\mathbf{Z}_p$ est donc p. Si la caractéristique m d'un corps est non nulle, alors m est premier.
On a vu que $(\mathbf{Z}_n, +, 0)$ et $(\mathbf{Z}_p^\star, *, 1)$ forment des groupes commutatifs pour tout n et tout p premier. On a donc

Proposition 2.18 $(\mathbf{Z}_p, +, \cdot)$ *est un corps si p est premier. Si p n'est pas premier, $(\mathbf{Z}_p, +, \cdot)$ est une anneau.*

Définition 2.19 *Un sous-ensemble F d'un corps E est un sous-corps de E si F est un corps pour les lois de E. Dans ce cas, E est une extension de F.*

2.3 Polynômes

Soit A un anneau, un polynôme f est une expression de la forme

$$f(x) = \sum_{i=0}^{n} a_i x^i = a_0 + a_1 x + \cdots + a_n x^n,$$

où n est un entier positif, les coefficients $a_i, \ 0 \leq i \leq n$ sont des éléments de A et x un symbole appelé une indeterminée.

Définition 2.20 *Soit $f = \sum_{i=0}^{n} a_i x^i$ un polynôme tel que $a_n \neq 0$. Alors f est de degré n (on note $\deg(f) = n$), a_0 est le terme constant et a_n le coefficient de plus haut degré (leading coefficient en anglais).*

On peut définir la somme et le produit de deux polynômes $f = \sum_{i=0}^{n} a_i x^i$ et $g = \sum_{i=0}^{m} b_i x^i$ $(m \leq n)$:

$$f(x) + g(x) = \sum_{i=0}^{n} (a_i + b_i) x^i,$$

et

$$f(x)g(x) = \sum_{k=0}^{n+m} c_k x^k, \text{ où } c_k = \sum_{i+j=k} a_i b_j,$$

où $0 \leq i \leq n$ et $0 \leq j \leq m$.
L'ensemble des polynômes sur A muni de ces deux opérations admet une structure d'anneau noté $A[x]$.
On montre facilement que pour tout $f, g \in F[x]$ (F étant un corps)

$$\deg(f+g) \leq max\{\deg(f), \deg(g)\}, \text{ et } \deg(fg) = \deg(f) + \deg(g).$$

Le polynôme g divise le polynôme f si il existe un polynôme h tel que $f = gh$. Pour éviter tout problème, on ne considère ici que des polynômes à coefficients dans un corps.

Exemple 2.21 *Dans* $\mathbf{F}_2[x]$*, considérons les deux polynômes*
$f = x^7 + x^6 + x^3 + x^2 + x + 1$ *et*
$g = x^4 + x^3 + x^2 + 1$.
Le polynôme g *divise* f *car* $f = gh$ *avec* $h = x^3 + x + 1$.

Théorème 2.22 *Soit* g *un polynôme non nul dans* $F[x]$*. Alors pour tout* $f \in F[x]$ *il existe deux polynômes* q *et* r *de* $F[x]$ *tels que*

$$f = qg + r, \text{ où } \deg(r) < \deg(q).$$

Toujours dans $F[x]$, si d divise f et g et si tout polynôme divisant f et g divise aussi d, alors d est le plus grand diviseur commun de f et g. On note $d = pgcd(f, g)$. Si $pgcd(f, g) = 1$, on dit que f et g sont premiers entre eux.

Exemple 2.23 *Les polynômes de* $\mathbf{F}_2[x]$
$f = x^2 + x + 1$ *et* $g = x^5 - 1$ *sont-ils premiers entre eux?*

Théorème 2.24 *Avec les mêmes notations, il existe* $u, v \in F[x]$ *tels que*

$$d(x) = u(x)f(x) + g(x)v(x), \text{ avec } u, v \in F[x].$$

Exemple 2.25 *Prenons* $f := x^6 + x^5 + 2\,x^4 + 2\,x^2 + 2$*, et* $g := x^2 + 2\,x + 1$*, deux polynômes sur* $\mathbf{F}_3$*. Alors, on a*

$$f = q_1 g + r_1 \text{ avec } q_1 = x^4 + 2\,x^3 + x \text{ et } r_1 = 2x + 2$$
$$g = q_2 r_1 + r_2 \text{ avec } q_2 = 2x + 2 \text{ et } r_2 = 0.$$

On trouve, $d = 2f + q_1 g = x + 1$.

Définition 2.26 *un polynôme non constant* $f \in F[x]$ *est dit irréductible sur* F *si les seuls polynômes* $(\neq f)$ *qui le divisent sont constants. Sinon, le polynôme* f *est réductible.*

Exemple 2.27 *Le polynôme de* $\mathbf{F}_2[x]$
$f = x^4 - 1$ *est-il irreductible? même question avec* $f = x^3 - 1$.

Théorème 2.28 *Tout polynôme* $f \in F[x]$ *peut s'écrire*

$$f = a f_1^{e_1} f_2^{e_2} \dots f_k^{e_k},$$

où $a \in F$*, les* f_i *sont des polynômes irréductibles unitaires de* $F[x]$ *et les exposants* e_i *des entiers positifs. Cette factorisation est unique.*

Rappelons qu'un polynôme unitaire a son coefficient de plus haut degré égal à 1.

Définition 2.29 *Un élément* a *est une racine (ou un zéro) du polynôme* f *si* $f(a) = 0$.

2.4 Construction d'un corps fini

Jusqu'à présent, nous n'avons introduit qu'un corps ayant p éléments (p premier). Il s'agit de $\mathbf{F}_p$. Dans $\mathbf{F}_p$ les opérations ($+$ et $\cdot$) sont effectuées modulo p.
Comment construire un corps qui admet p^m éléments? En fait, construire un corps qui contient peu d'éléments n'est pas difficile : il suffit de construire les tables de multiplication et d'addition en respectant les contraintes déjà vues. Par exemple, dans la table de multiplication, chaque ligne doit avoir l'élément

neutre. Cela traduit l'existance d'un inverse pour tout élément non nul.
Dans ce qui suit, nous donnons une méthode générale de construction. Nous allons construire le corps $\mathbf{F}_{p^m}$ qui admet p^m éléments.
Soit m un entier positif et $f(x)$ un polynôme irréductible sur $\mathbf{F}_p$ de degré m. On considère un élément α satisfaisant $f(\alpha) = 0$. Posons

$$\mathbf{F}_{p^m} = \{a_0 + a_1\alpha + \cdots + a_{m-1}\alpha^{m-1} \mid a_i \in \mathbf{F}_p\},$$

l'ensemble de tous les polynômes en α de degrés inférieurs à m et à coefficients dans F_p. On peut alors munir cet ensemble des opérations + et $\cdot$.
L'opération + est définie comme l'addition de polynômes dans $\mathbf{F}_p$.
L'opération multiplicative se fait en deux étapes : supposons que l'on veuille calculer $g_1 \cdot g_2$, on va d'abord effectuer une multiplication de polynômes usuelle

$$g_1(\alpha) \cdot g_2(\alpha) = h(\alpha)$$

puis, si le degré de h est supérieur à m, on va le réduire en effectuant une division par f et en considérant le reste r de cette division. Si $\deg(r) < m$ alors $g_1(\alpha) \cdot g_1(\alpha) = r(\alpha)$ sinon on redivise $r(\alpha)$ jusqu'à obtenir un reste dont le degré est inférieur à m. En d'autres termes, on fait les caluls "modulo" le polynôme f, modulo p.

Remarque 2 *Pour simplifier, on note souvent $f \cdot g$ par fg.*

Exemple 2.30 *Calculer $f * g \mod h$ dans $\mathbf{F}_2$ avec $f = x^3 + x^2 + 1$, $g = x^4 + x + 1$ et $h = x^5 + x + 1$.*

Théorème 2.31 *$(\mathbf{F}_{p^m}, +, \cdot)$ est un corps de taille p^m*

Preuve Il est facile de montrer que $(\mathbf{F}_{p^m}, +, \cdot)$ est un anneau contenant p^m éléments. Il reste à montrer que tout élément non nul admet un inverse. Puisque g appartient à $\mathbf{F}_{p^m}$, son degré est inférieur ou égal à $m - 1$. Et puisque f est irréductible, les deux polynômes f et g sont premiers entre eux. On peut donc utiliser Bezout : il existe deux polynômes $u(x)$ et $v(x)$ de $\mathbf{F}_{p^m}[x]$ tels que

$$u(x)f(x) + v(x)g(x) = 1.$$

Si l'on écrit cette égalité en α, puisque $f(\alpha) = 0$, on obtient

$$v(\alpha)g(\alpha) = 1,$$

et en supposant que $\deg(v(\alpha)) < m$ (sinon on réduit modulo f comme précédemment) on a $g^{-1} = v(\alpha)$. □

Le corps $\mathbf{F}_{p^m}$ est appelé une extension finie de $\mathbf{F}_p$ et $\mathbf{F}_p$ est le corps de base. Le corps se note aussi $\mathbf{F}_p[x]/(f(x))$. Si f est réductible, il existe deux polynômes non nuls f_1 et f_2 de $\mathbf{F}_p[x]$ tels que $f = f_1 f_2$. Cela signifie que f_1 et f_2 sont des diviseurs de zéro (donc non inversibles) et $\mathbf{F}_p[x]/(f(x))$ n'est pas un corps.

Exemple 2.32 *Soit $p = 2$ et $f(x) = x^3 + x + 1$ un polynôme irréductible sur $\mathbf{F}_2$. Soit β une racine de $f(x)$. Le corps fini $\mathbf{F}_{2^3}$ est défini par*

$$\mathbf{F}_{2^3} = \{a_0 + a_1\beta + a_2\beta^2 | a_i \in \mathbf{F}_2\}.$$

Les éléments de $\mathbf{F}_{2^3}$ peuvent donc s'écrire comme des triplets (a_0, a_1, a_2) ou des polynômes. De plus, puisque $\mathbf{F}_{2^3}$ est un corps, $\mathbf{F}_{2^3}^\star$ forme un groupe multiplicatif.

On peut montrer que tout corps fini peut être construit comme nous venons de le voir. Cela signifie que tout corps fini F de caractéristique p admet p^m éléments (m étant un entier strictement positif).

Exemple 2.33 *On veut construire le corps à quatre éléments. On sait que* $4 = 2^2$ *donc le corps de base est* $\mathbf{F}_2$ *et pour construire le corps, il suffit d'obtenir un polynôme irreductible de degré* $m = 2$ *sur* $\mathbf{F}_2$ *(pour cela il existe des tables de polynômes irreductibles dans la littérature).*
Soit $f(x) = x^2 + x + 1$ *un polynôme irréductible sur* $\mathbf{F}_2$ *et soit* β *une racine de* $f(x)$*. La caractéristique du corps est égale à 2, c'est la caractéristique du corps de base. Les éléments de* F_4 *peuvent être représentés par les polynômes de la forme* $a_1 + a_2\beta$*,* a_1 *et* a_2 *étant binaires. On obtient :* $F_4 = \{0, 1, \beta, \beta + 1\}$*. Le corps est totalement défini par sa table d'addition et de multiplication que nous construisons maintenant en notant* $\beta + 1 = \overline{\beta}$

$+$	0	1	β	$\overline{\beta}$
0	0	1	β	$\overline{\beta}$
1	1	0	$\overline{\beta}$	β
β	β	$\overline{\beta}$	0	1
$\overline{\beta}$	$\overline{\beta}$	β	1	0

$\cdot$	0	1	β	$\overline{\beta}$
0	0	1	0	0
1	0	1	β	$\overline{\beta}$
β	0	β	$\overline{\beta}$	1
$\overline{\beta}$	0	$\overline{\beta}$	1	β

Considérons maintenant un corps fini F muni de p^m éléments et $\beta \in F^\star = F \setminus \{0\}$. Alors toute puissance de β appartient aussi à $F^\star$ et comme F est fini, il existe un k et un l tel que $\beta^k = \beta^l$. Cela signifie que $\beta^{k-l} = 1$.

Exemple 2.34 $F = \mathbf{Z}_{11}$, $\beta = 2$. $F^\star$ *s'écrit*

2^0	2^1	2^2	2^3	2^4	2^5	2^6	2^7	2^8	2^9	2^{10}	2^{11}
1	2	4	8	5	10	9	7	3	6	1	2

Donc $\beta^{10} = 1$ *:* β *est une racine dixième de l'unité.*

Définition 2.35 *L'***ordre** *d'un élément* β *non nul dans un corps fini est le plus petit entier* $r \geq 1$ *tel que* $\beta^r = 1$.

Théorème 2.36 *(de l'élément primitif) Tout corps fini* F *de taille* p^m *contient un élément* β *d'ordre* $p^m - 1$*, appelé* **élément primitif** *de* F.

Preuve On sait que puisque F est un corps, $F^\star$ est un groupe multiplicatif d'ordre $p^m - 1$. On va montrer plus précisément que c'est un groupe cyclique engendré par un élément β.
Soit $\beta \in F^\star$ un élément dont l'ordre r est le plus grand parmi tous les éléments du groupe. On a trivialement $r < p^m$. Il est facile de montrer que l'ordre l de tout élément b du groupe divise r. Ainsi, puisque β est racine de l'equation $x^r - 1$, tous les éléments du groupe sont aussi racines de cette même equation et $\prod_{\alpha \in F^\star}(x - \alpha)$ divise $x^r - 1$. Ce qui signifie que $r \geq p^m - 1$. Comme on sait que $r \leq p^m - 1$ on a $r = p^m - 1$. Donc β est d'ordre $p^m - 1$ qui est la taille du groupe multiplicatif $F^\star$ et $F^\star = \{1, \beta, \beta^2, \ldots, \beta^{p^m - 2}\}$. □

Corollaire 2.37 *Tout corps fini de taille* p^m *est de la forme*

$$F = \{0\} \cup \{1, \beta, \beta^2, \ldots, \beta^{p^m - 2}\},\ \beta \in F.$$

Exemple 2.38 $F = \mathbf{Z}_{11} = \{0\} \cup \{1, 2, 2^2, 2^3, 2^4, 2^5, 2^6, 2^7, 2^8, 2^9\}$.

Un polynôme primitif est un polynôme qui contient une racine primitive. Il faut noter que tous les polynômes irréductibles ne sont pas primitifs. Par exemple dans $\mathbf{F}_2[x]$, $P = x^{11}+x^9+x^7+x^6+x^5+x+1$ est irréductible de degré 11 et racine de $x^{23}-1$. Soit β une racine de P, β est d'ordre 23 et non $2^{11}-1 = 2047$ donc β n'est pas une racine primitive de $\mathbf{F}_{2^{11}}$. La donnée de P permet de construire le corps : c'est l'ensemble des polynômes de $\mathbf{F}_2[x]$ "modulo" $P(x)$.
Cependant, d'après le théorème précédent, il existe un élément α d'ordre $2^{11}-1 = 2047$ dont les puissances forment $\mathbf{F}^{\star}_{2^{11}}$. On sait que l'ordre de β divise l'ordre de α. On a $\beta = \alpha^{89}$ car $89 * 23 = 2047$. En résumé, voici deux représentations du corps en fonction de β ou α :

$$\begin{aligned}\mathbf{F}_{2^{11}} &= \{\textstyle\sum_{i=1}^{11} a_i\beta^i,\ a_i \in \mathbf{F}_2\} \\ &= \{0\} \cup \{1, \alpha, \alpha^2, \ldots, \alpha^{2^{11}-2}\}.\end{aligned}$$

Théorème 2.39 *(Fermat) Tout élément β d'un corps F d'ordre p^m satisfait $\beta^{p^m} = \beta$. Ainsi, β est racine de $x^{p^m} = x$ et*

$$x^{p^m} - x = \prod_{\beta \in F} (x - \beta).$$

Définition 2.40 *Le polynôme minimal sur $\mathbf{F}_p$ de β est le polynôme unitaire de plus bas degré $M(x)$ dont les coefficients sont dans $\mathbf{F}_p$ tel que $M(\beta) = 0$.*

Exemple 2.41 *Construction du corps $F_8 = F_{2^3}$. Le corps admet huit éléments donc il contient un élément β d'ordre 7 qui est une racine primitive de l'unité. $F_8 = \{0\} \cup \{1, \beta, \beta^2, \ldots, \beta^6\}$, et β est racine du polynôme $(x^7 - 1)$ mod 2. On a $x^7 - 1 = \prod_{i=1}^{7}(x - \beta^i) = (x^3 + x + 1)(x^3 + x^2 + 1)(x + 1)$. Notons P_1 le polynôme $x^3 + x + 1$ et P_2 son réciproque et choisissons comme générateur β une racine de P_1. Cela veut dire que $P_1(\beta) = 0$ et $\beta^3 = \beta + 1$. Tout élément du corps peut être représenté par un triplet (s'il est vu comme un espace vectoriel de dimension 3 sur F_2) ou un polynôme de degré (au plus) 2 avec $\beta^3 = \beta + 1$.*

triplet $(\beta^2, \beta, 1)$	*polynôme*	*puissance de* β
$(0,0,0)$	0	0
$(0,0,1)$	1	1
$(0,1,0)$	β	β
$(1,0,0)$	β^2	β^2
$(0,1,1)$	$1+\beta$	β^3
$(1,1,0)$	$\beta+\beta^2$	β^4
$(1,1,1)$	$1+\beta+\beta^2$	β^5
$(1,0,1)$	$1+\beta^2$	β^6
$(0,0,1)$	1	$\beta^7 = 1$

En choisissant β racine de P_2, on aurait obtenu un corps isomorphe. Rappelons que deux corps sont dits isomorphes si il existe une application bijective ϕ de E dans F qui preserve l'arithmétique du corps (c.a.d. $\phi(a + b) = \phi(a) + \phi(b)$ et $\phi(ab) = \phi(a)\phi(b)$, $a,\ b \in E$).

Exemple 2.42 *Construction du corps $F_{16} = F_{2^4}$.*
On sait que F_{16} peut s'écrire $F_{16} = \{0\} \cup \{1, \beta, \beta^2, \ldots, \beta^{14}\}$, où β est un élément primitif de F_{16}.

2.5 Logarithme de Zech

Lorsque l'on fait des calculs dans les corps finis, il est facile de calculer $\alpha^i\alpha^j$. Il suffit d'additionner les puissances. Par contre, $\alpha^i + \alpha^j$ est plus difficile à déterminer. On peut alors utiliser le logarithme de Zech. Supposons que $i < j$. Alors

$$\alpha^i + \alpha^j = \alpha^i(1 + \alpha^{j-i}).$$

Posons $r = j - i$. On veut calculer $(1 + \alpha^r) = \alpha^s$.
L'entier s est appelé le logarithme de Zech de r, noté $Zech(r)$:

$$\alpha^{Zech(r)} = \alpha^r + 1.$$

Il existe bien sur des tables de logarithmes pour les corps finis les plus utilisés.

Exercice 2.43 *Calculer les tables pour* $\mathbf{F}_8$ *et* $\mathbf{F}_{16}$.

Par cette méthode, il suffit de stocker les $p^m - 2$ logarithmes de Zech pour pouvoir effectuer toutes les additions nécessaires.

2.6 Classes cyclotomiques

Les classes cyclotomiques (cyclotomic cosets en anglais) permettent de déterminer le nombre de facteurs irréductibles de $x^{p^m-1} - 1$ sur F. Connaissant le polynôme minimal d'une racine de $x^{p^m-1} - 1$, elles permettent de trouver tous les polynômes minimaux des racines de $x^{p^m-1} - 1$, c'est à dire tous les facteurs de $x^{p^m-1} - 1$.

Théorème 2.44 *$\beta \in F_{p^m}$ et β^p ont le même polynôme minimal.*

Preuve Soit $M_\beta(x)$ le polynôme minimal de β. $M_\beta(x) = \sum_{i=0}^{d} a_i x^i$, où $d = \deg(M_\beta(x))$ et $a_i \in F_p$. Notons que $a_i = a_i^p$ car a_i est racine de $x^p - x = 0$. On a $M_\beta(\beta) = 0$ et $M_\beta(\beta) = \sum_{i=0}^{d} a_i\beta^i = (\sum_{i=0}^{d} a_i\beta^i)^p = \sum_{i=0}^{d} a_i^p(\beta^p)^i = M(\beta^p)$. Donc β^p est une racine de M_β. Puisque M_β est irreductible, $M_\beta = M_{\beta^p}$. □

Définition 2.45 *Soit $\beta \in F_{p^m}$. Alors les éléments $\beta,\ \beta^p, \ldots,\ \beta^{p^{m-1}}$ sont appelés les conjugués de β pour le corps F_p.*

Tous les conjugués de β ont donc le même polynôme minimal.

Exemple 2.46 *On considère le corps F_{16} avec $p = 2$, $m = 4$ et β admettant pour polynôme minimal $\beta^4 + \beta + 1$. Alors*

$$\left.\begin{array}{ll} \beta & \text{est un zéro de } x^4 + x + 1 \\ \beta^2 & \text{idem} \\ \beta^4 & \text{idem} \\ \beta^8 & \text{idem} \\ \beta^{16} = \beta & \end{array}\right\} \text{4 racines distinctes}$$

Finalement, on peut vérifier par le calcul que

$$x^4 + x + 1 = (x - \beta)(x - \beta^2)(x - \beta^4)(x - \beta^8).$$

Trouver l'ensemble des conjugués de toutes les racines revient à partitionner l'ensemble des puissances de β. Le corps F s'écrit $F = \{0\} \cup \{1, \beta, \beta^2, \ldots, \beta^{p^m-2}\}$ et l'ensemble des puissances de β est tout simplement Z_{p^m-1}.

Définition 2.47 *Soit $a,\ b \in Z_{p^m-1}$. a et b sont dits equivalents (notés $a \equiv b$) si $b = p^i a \ mod\ (p^m - 1)$.*

La relation d'equivalence est reflexive, symétrique et transitive. C_s représente une classe cyclotomique où s est le plus petit entier de la classe :

$$\{s,\ sp,\ sp^2, \ldots,\ sp^{m_s-1}\},$$

où m_s est l'entier le plus petit tel que $p^{m_s} = s \pmod{p^m - 1}$. L'entier s est quelquefois appelé le chef de classe ou en anglais coset leader.

Exemple 2.48 *Quelles sont les classes cyclotomiques modulo* 15 *pour* $p = 2$*?*

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

Théorème 2.49 *Soit $\alpha \in \mathbf{F}_{p^m}$ un élément primitif.*

$$M(\alpha^s)(x) = \prod_{i \in C_s} (x - \alpha^i)$$

Preuve Ce résultat est admis. □

Exercice 2.50 *Soit α une racine primitive de $x^4 + x + 1$ sur $\mathbf{F}_{16}$.*
Déterminer les polynômes minimaux de $1, 3, 5, 7$.

3 Codes cycliques

Les codes cycliques représentent la famille de codes la plus importante. D'un point de vue pratique ce sont les codes les plus utilisés car leur mise en œuvre est facile et ils admettent souvent de bons algorithmes de décodage. D'un point de vue théorique, ils possèdent une structure algébrique (et quelquefois combinatoire) intéressante. Les codes cycliques les plus connus sont les codes de Hamming, BCH, Reed-Solomon, Résidus quadratiques, Kerdock, etc.).

Définition 3.1 *Un code linéaire en bloc C de longueur n sur $F[x]$ est dit cyclique si l'ensemble de ses mots est invariant par décalage circulaire :*

$$(c_0, c_1, \ldots, c_{n-1}) \in C \Rightarrow (c_{n-1}, c_0, c_1, \ldots, c_{n-2}) \in C.$$

Exemple 3.2

i) Le code binaire $C = \{000,\ 101,\ 011,\ 110\}$ est un code cyclique.

ii) Le code binaire $C = \{0000,\ 1001,\ 0110,\ 1111\}$ n'est pas cyclique. Il est cependant équivalent à un code cyclique (il faut échanger les troisième et quatrième coordonnées).

Tout mot $c = (c_0,\ c_1, \cdots,\ , c_{n-1})$ d'un code C sur F peut être identifié à un polynôme $c(x) = c_0 + c_1 x + \cdots + c_{n-1}x^{n-1}$ de $F[x]$. Pour pouvoir construire des codes cycliques, l'anneau à considérer est $R_n = F[x]/(x^n - 1)$. En effet, dans cet anneau, on peut réduire tout polynôme modulo $x^n - 1$ en remplaçant simplement x^n par

1, x^{n+1} par x et ainsi de suite. Le code C est alors un sous ensemble de R_n. Observons ce qu'il se passe lorsque l'on multiplie $c(x)$ par x dans R_n :

$$\begin{aligned} x \,.\, c(x) &= c_0 x + c_1 x^2 + \cdots + c_{n-1} x^n \\ &= c_{n-1} + c_0 x + c_1 x^2 + \cdots + c_{n-2} x^{n-1}. \end{aligned}$$

La multiplication par x correspond à un décalage circulaire. La multiplication par x^m correspond à m décalages circulaires.

3.1 Polynôme générateur

Définition 3.3 *Le polynôme générateur $g(x)$ d'un code cyclique C est un polynôme non nul unitaire de plus bas degré de C.*

Proposition 3.4 *Le polynôme générateur est unique*

Preuve Supposons que g_1 et g_2 soient deux polynôme générateurs. Alors $g_1 - g_2$ est un polynôme générateur (le code est linéaire) de degré strictement inférieur au degré des g_i. Contradiction. □

Proposition 3.5 *Tout mot d'un code cyclique est un multiple du polynôme générateur. On note $C = \langle g \rangle$.*

Preuve Soit $c(x) \in C$ on effectue la division euclidienne de c par g: $c = ag + r$ avec $\deg(r) < \deg(g)$. Or, le reste r qui est la différence de deux mots du code appartient au code. Si $r \neq 0$, on contredit l'hypothese sur le degré minimum de g. □

Proposition 3.6 *Le polynôme générateur divise $x^n - 1$.*

Preuve On a $x^n - 1 = ag + r$ avec $\deg(r) < \deg(g)$ et on conclut comme précédemment que r doit être nul (après réduction modulo $x^n - 1$). □

3.2 Représentation matricielle

On a vu que tout mot $c \in C$ peut s'obtenir en multipliant g (de degré r) par un polynôme a sans avoir à réduire modulo $x^n - 1$: $c(x) = a(x)g(x)$. Puisque $\deg(c(x)) < n$ et $\deg(g(x)) = r$, on obtient $\deg(a(x)) < n - r$. Utilisons maitenant la notation matricielle. On a

$$c = aG$$

où $c = (c_0, \ldots, c_{n-1})$, $a = (a_0, \ldots, a_{n-r})$ et G est une matrice circulante $(n-r) \times n$ dont la $i$ème ligne ligne contient le mot $x^{i-1}g$

$$G = \begin{bmatrix} g_0 & g_1 & g_2 & \cdots & g_r & & 0 \\ & g_0 & g_1 & \cdots & g_{r-1} & g_r & \\ & & & \cdots & \cdots & & \\ 0 & & g_0 & \cdots & \cdots & & g_r \end{bmatrix}.$$

Son rang est $n - r$. G est une matrice génératrice du code qui a $dim(C)$ lignes. Ainsi $\deg(g) = n - dim(C)$.

3.3 Procédure de codage systématique

On veut coder la séquence de longueur k $u_1, u_2, \ldots, u_k$ avec $u_i \in F$:

u_1 $u_2 \ldots$ u_k

L'idée est de rajouter $n-k$ symboles de manière à obtenir un mot de longueur n qui appartienne au code cyclique C engendré par le polynôme générateur g.

1. On forme le polynôme
$$u(x) = u_1 x^{n-k} + u_2 x^{n-k+1} + \cdots + u_k x^{n-1}$$
La séquence est ainsi décalée de k positions vers la droite :

$0 \ldots 0$	u_1 $u_2 \ldots$ u_k

2. puis on effectue la division euclidienne par le polynôme générateur g du code
$$u(x) = g(x)q(x) + r(x)$$
avec $\deg(r) < \deg(g) = n-k$

3. le polynôme $c(x) = u(x) - r(x)$ est un multiple de $g(x)$. Le mot c appartient donc au code. C'est le mot construit à partir de $u(x)$. Si le code est binaire, on ne prend pas en compte les signes et on obtient :

$r_1 \ldots r_{n-k}$	u_1 $u_2 \ldots$ u_k

Il s'agit d'un codage systématique car les symboles de parité (coefficients de $r(x)$) sont séparés des symboles d'information.

r	u
redondance	information

Lors d'un codage systématique, on peut aussi mettre les bits d'information avant ceux de redondance.

Exemple 3.7 *On veut construire un code de longueur* 7 *sur* $\mathbf{F}_2$. *Le poynôme générateur du code doit diviser* $x^7 - 1$. *On a* $x^7 - 1 = \left(x^3 + x + 1\right)\left(x^3 + x^2 + 1\right)(x + 1)$. *Considérons le code* C *de polynôme générateur* $g(x) = x^3 + x + 1$ *avec matrice génératrice*

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

Pour coder la séquence 1011, *on forme le polynôme*

$$u(x) = x^6 + x^5 + x^3$$

(on décale la séquence de trois positions vers la droite) que l'on divise par g

$$x^6 + x^5 + x^3 = g(x^3 + x^2 + x + 1) + 1$$

le mot

$$c = x^6 + x^5 + x^3 + 1$$

appartient au code C.
Matriciellement, on écrit $c = uG_s$ *avec*

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

La matrice génératrice G_s *est écrite sous forme systématique.*

3.4 Dual d'un code cyclique

Proposition 3.8 *Si* g *est le polynôme générateur de* $C = [n, k]$ *alors* $h := (x^n - 1)/g$ *est le polynôme générateur de* $C^\perp$

Preuve Soit $c \in C$ et $c' \in \langle h \rangle$. On peut écrire $c = ag$ et $c' = a'h$. Ce qui implique que $cc' = aa'gh = 0$ puisque $gh = 0$. donc $\langle h \rangle \subset C^\perp$. Il reste à montrer que $dim(C^\perp) = n - k$ si $dim(C) = k$. On sait que $\deg(h) = n - \deg(g) = k$ donc $dim(h) = n - \deg(h) = n - k$. □

Exemple 3.9 *Construction du code de Hamming* $[7, 4]$.
Soit $C = \langle g \rangle$ *avec* $g = x^3 + x + 1$. *Le polynôme générateur de* $C^\perp$ *est* $(x^3 + x^2 + 1)(x + 1) = x^4 + x^2 + x + 1$.
La matrice génératrice de $C^\perp$ *est*

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

On remarque que les colonnes de la matrice correspondent à tous les 3*-uplets binaires non nuls. Le code* C *est donc le code de Hamming.*

3.5 Construction d'un code cyclique

Pour construire un code cyclique de longueur n, il est utile de connaître la décomposition de $x^n - 1$ en polynômes irréductibles sur le corps de base F :

$$x^n - 1 = \prod_i f_i(x).$$

En l'absence d'un logiciel (maple, magma,...), on peut déterminer les classes cyclotomiques modulo n. Le nombre de classes donne le nombre de facteurs irréductibles. La donnée d'un polynôme irréductible diviseur de $x^n - 1$ permet alors de connaître tous les autres facteurs. Le polynôme générateur du code est un produit d'un certain nombre de facteurs trouvés.

Exemple 3.10 *Combien peut-on construire de codes cycliques* $[31, 21]$ *sur* $\mathbf{F}_2$ *?*
Il suffit de déterminer les classes cyclotomiques modulo 31. *Il existe* 7 *classes cyclotomiques, chacune con-*

tenant 5 *éléments.*

$$C_0 = \{0\}$$
$$C_1 = \{1, 2, 4, 8, 16\}$$
$$C_3 = \{3, 6, 12, 24, 17\}$$
$$C_5 = \{5, 10, 20, 9, 18\}$$
$$C_7 = \{7, 14, 28, 25, 19\}$$
$$C_{11} = \{11, 22, 13, 26, 21\}$$
$$C_{23} = \{23, 15, 30, 29, 27\}$$

Il existe 6 *facteurs de degré* 5 *et un facteur de degré* 1 *:* $(x-1)$*. Le polynôme générateur d'un code* $[31, 21]$ *doit être de degré* 10*. Il y a* $\binom{6}{2} = 15$ *possibilités. Pour pouvoir factoriser effectivement* $x^{31} - 1$ *il faut connaître un polynôme irréductible de degré* 5 *(en effet* $31 = 2^5 - 1$*). Il existe des tables qui donnent des polynômes irréductibles ou primitifs de degré donné sur* $\mathbf{F}_2$*.*

4 Les codes de Hamming

Ils ont été construits par R. Hamming dans l'immédiate après guerre Pour des raisons pratiques : éviter que l'exécution de ses programmes soit arrêtée par des erreurs de transmission. Ils permettent de corriger une erreur et détecter deux erreurs. Les codes de Hamming représente une famille de codes dont le premier élément est le code de longueur 7 de paramètres $[7, 4, 3]$. Plus généralement, les paramètres d'un code H_m sont $[n = 2^m - 1, k = n - m, d = 3]$. Il peut être défini par sa matrice de contrôle dont les colonnes sont tous les $m-$tuples distincts non nuls.
Soit α une racine primitive de $\mathbf{F}_{2^m}$, alors $1, \alpha, \alpha^2, \ldots, \alpha^{2^m-2}$ sont tous distincts et peuvent être représentés par tous les $m-$tuples non nuls. Ainsi, la matrice de contrôle d'un code de Hamming peut s'écrire

$$H = [1, \alpha, \alpha^2, \ldots, \alpha^{2^m-2}].$$

Exemple 4.1 *Pour* $m = 3$*,* $H = [1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6]$ *qui peut se traduire en*

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

où $\alpha \in \mathbf{F}_{2^3}$ *satisfait* $\alpha^3 + \alpha + 1 = 0$*.*
Soit $c = (1, 1, 0, 1, 0, 0, 0)$*, que vaut* Hc^T *?*

On a

$$c = (c_0, c_1, \ldots, c_{n-1}) \in H_m$$
$$\Leftrightarrow$$
$$Hc^T = 0$$
$$\Leftrightarrow$$
$$\textstyle\sum_{i=0}^{n-1} c_i \alpha^i = 0$$
$$\Leftrightarrow$$
$$c(\alpha) = 0 \text{ où } c(x) = c_0 + c_1 x + \cdots + c_{n-1} x^{n-1}.$$

Donc $c \in H_m \quad \Leftrightarrow \quad M^{(1)}(x) \mid c(x)$ et H_m consiste en tous les multiples de $M^{(1)}(x)$.
On vient de montrer que H_m est un code cyclique de polynôme générateur $g(x) = M^{(1)}(x)$.

Exemple 4.2 *La matrice génératrice de H_3 peut s'écrire*

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

si le polynôme générateur est $1 + x + x^3$. Les racines du polynôme générateur sont appelées des zéros du code.

Exercice 4.3 *Soit H la matrice de contrôle d'un code C cyclique binaire avec*

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \dots & \alpha^{2^m-2} \\ 1 & \alpha^3 & \alpha^6 & \dots & \alpha^{3(2^m-2)} \end{bmatrix}$$

et α une racine primitive de $\mathbf{F}_{2^m}$.
Calculer le polynôme générateur du code.

Réponse :

$$\begin{gathered} c = (c_0, c_1, \dots, c_{n-1}) \in C \\ \Leftrightarrow \\ Hc^T = 0 \\ \Leftrightarrow \\ \textstyle\sum_{i=0}^{n-1} c_i\alpha^i = 0 \text{ et } \sum_{i=0}^{n-1} c_i\alpha^{3i} = 0 \\ \Leftrightarrow \\ c(\alpha) = 0 \text{ et } c(\alpha^3) = 0 \\ \Leftrightarrow \\ M^{(1)}(x) \mid c(x) \text{ et } M^{(3)}(x) \mid c(x) \\ \Leftrightarrow \\ ppcm(M^{(1)}M^{(3)}) \mid c(x). \end{gathered}$$

Les polynômes $M^{(1)}$ et $M^{(3)}$ sont distincts et irréductibles donc $c \in C \Leftrightarrow M^{(1)}M^{(3)} \mid c(x)$.

5 Les codes BCH

Ils ont été découverts par Hocquenghem, Bose et Ray-Chaudhuri (d'où le nom de BCH). Ils représentent une famille très importante de codes. D'un point de vue pratique Ils s'encodent et se décodent facilement. Supposons que l'on désire un code de longueur n qui corrige t erreurs sur $\mathbf{F}_q$ (n premier avec q). Alors, on peut construire un code BCH de paramètres $[n, k, 2t + 1]$.

Définition 5.1 *Un code BCH sur $\mathbf{F}_q$ de longueur n et distance construite δ est le plus grand code possible ayant comme zéros*

$$\beta^b, \beta^{b+1}, \dots, \beta^{b+\delta-2},$$

où $\beta \in \mathbf{F}_{q^m}$ est une racine primitive de l'unité, b un entier positif et m l'ordre multiplicatif de q modulo n.

Il existe deux cas importants :

1. $b = 1$ appelé en anglais *narrow-sense BCH code.*

2. Si $n = q^m - 1$ on parle de code BCH primitif.

Proposition 5.2 *La distance construite δ est une borne inférieure de la distance minimale d.*

Preuve Le mot $c(x)$ appartient à $\langle g \rangle$ si $c(\beta^j) = 0$ pour $b \leq j \leq b + \delta - 2$. Matriciellement cela signifie que $cH^T = 0$ avec

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

Il faut remarquer que les lignes de la matrice ne sont pas forcément linéairement indépendantes. De plus, on pourrait remplacer les β^j par des vecteurs colonne à m composantes sur $\mathbf{F}_q$.
Il faut montrer que si $cH^T = 0$ et $c \neq 0$ alors le poids de c est strictement supérieur à δ. D'une manière equivalente, cela signifie que n'importe quelles $\delta - 1$ colonnes de H sont linéairement indépendantes sur $\mathbf{F}_q$. Soient $\beta^{j_1 b}$, $\beta^{j_2 b}, \dots,$ $\beta^{j_{\delta-1} b}$ les termes du haut de ces colonnes. Le determinant

$$\Delta = \begin{bmatrix} \beta^{j_1 b} & \beta^{j_2 b} & \dots & \beta^{j_{\delta-1} b} \\ \beta^{j_1 (b+1)} & \beta^{j_2 (b+1)} & \dots & \beta^{(j_{\delta-1})(b+1)} \\ \vdots & & & \\ \beta^{j_1 (b+\delta-2)} & \beta^{j_2 (b+\delta-2)} & \dots & \beta^{(j_{\delta-1})(b+\delta-2)} \end{bmatrix}$$

est de Vandermonde. Donc le determinant est de la forme

$$\Delta = \beta^{\sum_k j_k b} \prod_{u>v} (\beta^{j_u} - \beta^{j_v}) \neq 0.$$

Le determinant est non nul car β est une racine primitive $n$ième de l'unité. □

δ est appelée distance BCH, notée d_{BCH}.

Exercice 5.3 *Montrer que le code de Hamming H_m est un code BCH pouvant corriger 1 erreur.*

5.1 Codes BCH corrigeant deux erreurs

Pour pouvoir corriger deux erreurs, il faut que la distance minimale soit au moins égale à 5. Essayons de construire un code BCH primitif binaire avec $b = 1$ de longueur $n = 2^m - 1$. Soit β une racine primitive $n$ième de l'unité et soit C ce code. Par définition, C est le plus grand code ayant comme zéros $\beta, \beta^2, \beta^3, \beta^4$. Le polynôme générateur est donc $M^{(1)}M^{(3)}$ avec $\deg(M^{(1)}) = m$ (puisque β est primitive) et $\deg(M^{(3)}) \leq m$. On a $k = n - \deg(g)$ donc $k \geq n - 2m$. Les paramètres du code sont donc $[n = 2^m - 1, k \geq n - 2m, d \geq 5]$.

Considérons le code C BCH de paramètres $[15, 7, 5]$. Choisissons comme racine primitive, la racine de $x^4 + x + 1$

$$\begin{aligned} g(x) &= g_1(x)g_3(x) \\ &= (x^4 + x + 1)(x^4 + x^3 + x^2 + x + 1) \ . \\ &= x^8 + x^7 + x^6 + x^4 + 1 \end{aligned}$$

1. Montrons que $d = d_{BCH}$
   On sait que $d \geq d_{BCH}$ et de plus que le poids de $g(x)$ est exactement 5. $g(x)$ appartient au code donc $d = 5$.

2. Construire la matrice de contrôle

$$H = \begin{bmatrix} 1 & \beta & \beta^2 & \dots & \beta^{14} \\ 1 & \beta^3 & \beta^6 & \dots & \beta^{12} \end{bmatrix}.$$

C'est donc une matrice 8×15. On prend $\beta^4 = (0011)^T$ et on obtient

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

3. Décodage
Supposons que l'on reçoive $y = (010001100010111)$. Soit c le mot effectivement envoyé et e l'erreur, on a $y = c + e$. La première chose à faire est de calculer son syndrome $S(y) = Hy = (01001001)$. Il faut ensuite l'étudier de la manière suivante

   (a) $S(y) \neq 0$ donc $y \notin C$.
   Posons $y = c + e$ avec $e \neq 0$ l'inconnue.

   (b) Si l'equation $y = c + e$ admet une solution de poids 1 (c.a.d. $w(e) = 1$), alors nécessairement, il existe une colonne h_i de la matrice H telle que $S(y) = S(e) = h_i$. On a $S(y) = (01001001) = (\beta^2, \beta^{14})^T$ qui ne correspond pas à une colonne de H. Donc $w(e) \geq 2$.

   (c) Cherchons maintenant une solution avec $W(e) = 2$. On a $S(e) = h_i + h_j$ et il faut résoudre le système

$$\begin{cases} \beta^i + \beta^j = \beta^2 \\ \beta^{3i} + \beta^{3j} = \beta^{14} \end{cases}$$

   Elevons au cube la première equation : on a
   $\beta^{3i} + \beta^{3j} + \beta^{i+j}(\beta^i + \beta^j) = \beta^6$
   qui se simplifie en
   $\beta^{14} + \beta^{i+j}\beta^2 = \beta^6$.
   Donc $\beta^{i+j} = (\beta^6 + \beta^{14})/\beta^2 = \beta^4 + \beta^{12} = (1100)^T = \beta^6$.
   On connait maintenant $\beta^i + \beta^j$ et β^{i+j} donc β^i et β^j sont solutions de $x^2 + \beta^2 x + \beta^6 = 0$. Une recherche exhaustive donne β et β^5 comme solution. Il faut donc corriger le deuxième et sixième bits de y pour obtenir le mot de code.

Exercice 5.4 *Avec le code précédent, décoder* $y = (101010010001011)$ *puis écrire un programme qui corrige jusqu'à deux erreurs tout mot recu.*

D'autres techniques de décodage seront présentées dans la troisième partie du module.

Exercice 5.5 *Construire une matrice génératrice d'un code BCH de longueur* 13 *sur* $\mathbf{F}_3$ *et de distance construite* 3.

6 Les codes de Reed-Solomon

Les codes de Reed-Solomon (RS) sont des codes BCH sur $\mathbf{F}_q$ de longueur $q-1$ ($q \neq 2$). Leur utilisation dans les lecteurs de CD et DVD à permis d'obtenir une qualité de son et d'image excellente.

Puisque l'alphabet est $\mathbf{F}_q$, les polynômes sont totalement réductibles. $x^{q-1}-1 = \prod_{\beta \in \mathbf{F}_q^\star}(x-\beta)$ et le polynôme minimal de α^i est $M^{(i)}(x) = x - \alpha^i$. Ainsi un code RS de longueur $q-1$ et distance construite δ a pour polynôme générateur

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

Généralement $b = 1$.

Exercice 6.1 *Soit $\mathbf{F}_4 = \{0, 1, \alpha, \beta = \alpha^2\}$ avec $\alpha^2+\alpha+1 = 0$. On veut construire un code de RS de longueur 3 avec $\delta = 2$ et $b = 2$. Le polynôme générateur est $g(x) = x - \beta$.*

1. *Enumérer le code*
2. *déterminer ses paramètres $[n, k, d]$ et vérifier que $d = n - k + 1$.*

Exercice 6.2 *Calculer une matrice génératrice du code de RS sur $\mathbf{F}_5$ avec $\delta = 3$.*

La dimension d'un code RS est $k = n - \deg(g) = n - \delta + 1$ et $\delta = \deg(g) + 1$. On a donc $\delta = n - k + 1$ et $d \geq \delta$. Or la borne de Singleton donne $n - k \geq d - 1$ donc $d = \delta$. Les codes qui admettent cette propriété sont dits MDS (Maximum Distance Separable en anglais).

6.1 Image binaire des codes de Reed-Solomon

Lorsque $q = p^m$, les éléments de $\mathbf{F}_q$ peuvent être représentés par des $m-$tuples d'éléments de $\mathbf{F}_p$. Ainsi, un code RS de paramètres $[n, k, d]$ sur $\mathbf{F}_q$ devient un code binaire de paramètres $[n' = mn, k' = mk, d' \geq d]$. En particulier, les codes RS construits sur des extensions de $\mathbf{F}_2$ admettent souvent des images binaires ayant de très bons paramètres. Ces images binaires sont des codes linéaires mais ne sont pas en général cycliques.

Exercice 6.3 *Reprenons l'exercice précédent concernant le code RS sur $\mathbf{F}_4$ de longueur 3. On utilise l'application ϕ de $\mathbf{F}_4$ dans $(\mathbf{F}_2)^2$ définie par $\phi(0) = 00$, $\phi(1) = 01$, $\phi(\alpha) = 10$, $\phi(\beta) = 11$. On obtient un code de paramètres $[6, 4, 2]$.*
Enumérer le code et vérifier les paramètres. Le code est-il cyclique?

Définition 6.4 *Un paquet d'erreur de longueur b est un vecteur dont les seuls éléments non nuls vivent parmi b composantes consécutives et dont la première et la dernière composante sont non nulles.*

L'image binaire des codes de RS est intéressante pour corriger des paquets d'erreurs. En effet, un paquet de longueur b peut affecter au plus r symboles adjacents de $\mathbf{F}_q$, avec

$$(r-2)m \leq b \leq (r-1)m + 1.$$

Ces paquets peuvent être corrigés si d est bien plus grand que r.