Université de Caen/Basse-Normandie
U.F.R. Sciences

École Doctorale SIMEM

THÈSE

présentée par

Fabien Galand

et soutenue
le 1er décembre 2004

en vue de l'obtention du

Doctorat de l'université de Caen
Spécialité informatique
(Arrêté du 25 avril 2002)

Construction de codes $\mathbb{Z}_{p^k}$-linéaires de bonne distance minimale, et schémas de dissimulation fondés sur les codes de recouvrement

Membres du Jury

M. Claude Carlet,	Professeur, Université de Paris 8	(Directeur)
M. Thierry Berger,	Professeur, Université de Limoges	(Rapporteur)
M. Gilles Zémor,	Maître de conférences (HDR), ENST Paris	(Rapporteur)
Mme Caroline Fontaine,	Chargée de recherche, Université de Lille 1	
M. Grigory Kabatiansky,	Chargé de recherche, IITP (Moscou)	
Mme Brigitte Vallée,	Directrice de recherche, Université de Caen	

Remerciements

De nombreuses personnes ont contribué à l'aboutissement de cette thèse. Bien évidemment, elle n'aurait pu voir le jour sans Claude Carlet qui, bien au-delà de la direction scientifique, a su me faire comprendre, au travers de conseils sans nombre, sa pratique de la recherche.

J'ai également profité d'un environnement des plus favorables, le projet CODES, et suis par là même redevable à Pascale Charpin et à Nicolas Sendrier de m'y avoir hébergé le plus naturellement du monde. Ils ont toujours eu à mon égard une bienveillance qui aura été pour moi un véritable soutien.

J'ai mis à contribution l'intégralité des membres permanents du projet en me tournant, à un moment ou à un autre, vers chacun d'eux pour des explications. J'ai tout particulièrement abusé du temps d'Anne Canteaut, d'une disponibilité et d'une rigueur sans failles, ainsi que de celui de Jean-Pierre Tillich dont la pertinence des commentaires ne cessera de m'émerveiller. Ils ont tous deux grandement participé à débroussailler le présent manuscrit et je les prie de m'excuser de ne pas avoir fait un meilleur usage de leurs remarques.

À côté de la science, l'ambiance régnant dans cette équipe, et notamment la bonhomie teintée d'humour de Daniel Augot, s'est avérée une source inépuisable d'énergie. Que dire de ces moments de détente dans la « salle à café », où j'ai pu profiter non seulement des chefs mais aussi de Marion, Cédric T., Cédric L., Emmanuel, Matthieu, Mathieu, de la nombreuse main-d'œuvre occasionnelle et des badauds de passages ? Je n'oublie pas Christelle, qui a été pour moi d'une aide administrative salvatrice, mais qui a surtout constamment le rire aux lèvres.

Bien que n'appartenant pas au projet, Grigory Kabatiansky y est pour moi associé et n'y dépareillerait pas. Sans lui, la seconde partie ma thèse n'existerait pas et cette collaboration m'honore. Sa clarté, sa rigueur et l'ambiance de travail détendue qu'il arrive à créer et qu'il nourrit de ses innombrables plaisanteries, constituent pour moi un véritable modèle.

Bien que peu présent dans l'équipe caennaise d'algorithmique, j'y ai toujours été accueilli chaleureusement par la joyeuse petite bande de doctorants : Aline, Ben, Bruno, Jérémie, Guillaume, Philippe et Régis. Ma sympathie va en particulier à Aline qui n'a pas été avare de son expérience et de sa vision de la recherche. Je remercie Emmanuel pour la même raison.

C'est à Caen que j'ai effectué mon DEA et que j'ai eu la chance de suivre les cours magistraux de Brigitte Vallée. Je lui suis grandement redevable de ces cours, de son implication dans l'obtention de mon financement et de l'intérêt constant qu'elle a manifesté pour le déroulement de ma thèse. Je suis heureux de la voir participer à mon jury.

Je n'aurais pas pu disposer, pour conclure cette thèse, de conditions plus favorables que celles qu'Hubert Comon-Lundh m'a offertes au sein du Laboratoire spécification et vérification, et du département d'informatique de l'École normale supérieure de Cachan. Je l'en remercie et lui présente ici toutes mes excuses pour avoir autant abusé de son indulgence à l'égard de ma situation.

Je suis reconnaissant à Thierry Berger et à Gilles Zémor d'avoir accepté, non seulement de faire partie de mon jury, mais surtout de rapporter ma thèse. La présence de Caroline Fontaine dans ce même jury m'est des plus agréables et ses remarques sur la seconde partie de mon manuscrit m'ont été très profitables.

Enfin, avant de terminer cette série de remerciements, un mot pour ceux qui m'ont permis de garder les pieds sur terre, contre vents et marées et anneaux de Galois. En première ligne, fidèle parmi les fidèles, l'autre-partie-de-la-coloc, Ahmed, qui m'aura supporté, dans presque toutes les acceptions, probablement beaucoup plus qu'il ne l'aurait souhaité. Cette thèse lui doit tant qu'il s'agit un peu de la sienne. Je regrette légèrement de ne pas l'avoir faite sur le béton, il en serait certainement plus fier et pourrait plus facilement y retrouver sa contribution. Loin d'être seul, il fut épaulé dans sa lourde tâche par des hommes de l'ombre, Fabrice, Yann et Yves. Merci à eux et mes plus plates excuses à ceux que j'ai délaissés, notamment Sengdo. D'un soutien plus récent, mais non moins solide, Nathalie. Outre son rôle de correcteur orthographique hors pair, en chair et en os, je lui dois l'intégralité de mes connaissances en latin. Quelle joie de découvrir Cicéron et sa première *Catilinaire* : « Quousque tandem abutere, Catilina, patientia nostra » ! Ces derniers mois auraient été autrement plus éprouvants sans elle.

Le mot de la fin va à ma famille, ma mère, mon père et mon frère bien sûr, mais je pense surtout à mes grands-parents, disparus lors de ma thèse.

Sommaire

Première partie : codes $\mathbb{Z}_{p^k}$-linéaires

Introduction 11

1 Préliminaires 15

2 Codes sur l'anneau $\mathbb{Z}_{p^k}$ 33

3 Codes $\mathbb{Z}_{p^k}$-linéaires 49

4 Codes de Kerdock généralisés 59

5 Relevés des codes de résidus quadratiques 79

6 Construction fondée sur les translatés de codes $\mathbb{Z}_{p^k}$-linéaires 87

Conclusion et perspectives 98

Seconde partie : schémas de dissimulation

Introduction 107

7 Position du problème 111

8 Modèle avec adversaire passif 115

9 Réécriture de travaux précédents 129

10 Modèle avec adversaire actif 139

Conclusion et perspectives 146

Bibliographie 148

Index 156

Table des matières 163

Avant-propos

Ce document comprend deux parties correspondant à deux axes de recherches différents : les codes correcteurs d'erreurs et la stéganographie. Dans notre approche, ces deux axes se rejoignent autour des objets étudiés : les codes. Mais, chaque axe se concentre sur l'étude d'un paramètre spécifique : distance minimale pour la correction d'erreur ; rayon de recouvrement pour la stéganographie.

Ainsi, bien que les thèmes de chaque partie soient nettement distincts, c'est un même objet qui est *in fine* le sujet d'étude, mais sous un éclairage différent à chaque fois. Cela illustre la généralité et la richesse des problèmes survenant avec ces objets pourtant simples.

Les résultats de la première partie ont fait l'objet, pour $\mathrm{p} = 2$, d'une courte présentation dans [Ga03b] et d'un rapport de recherche plus détaillé [Ga03a]. La seconde partie reprend très largement, tout en les précisant, des travaux menés conjointement avec Grigory Kabatiansky, et publiés dans [GK03a, GK03b]. Les exceptions notables sont les sections 8.3 et 8.6, ainsi que le chapitre 9.

Première partie

Construction de codes $\mathbb{Z}_{p^k}$-linéaires de bonne distance minimale

Introduction

L'étude des codes correcteurs d'erreurs trouve son origine dans la transmission d'information. Une source émet des symboles, appartenant à un alphabet Σ, vers un récepteur, et cela au travers d'un canal susceptible de modifier les symboles émis. L'objectif du récepteur est de retrouver exactement les symboles émis. Pour cela, les symboles ne sont pas émis directement sur le canal, ils subissent d'abord un encodage.

Nous allons considérer le cas d'un encodage en blocs dans lequel un bloc de k symboles est encodé en un bloc de $n > k$ symboles qui appartiennent au même alphabet Σ. L'encodage étant une fonction bijective, tous les éléments de Σ^n ne sont pas atteints ; la partie atteinte porte le nom de code, et ses éléments sont appelés les mots de code.

Le paramètre fondamental d'un code en blocs est sa distance minimale, qui mesure sa capacité à corriger les erreurs qui surviennent dans un canal de transmission susceptible de changer un symbole en un autre, tous les changements étant équiprobables (on parle d'un canal symétrique). Cette distance minimale est définie comme le nombre minimal de symboles qui diffèrent entre deux mots de codes. Construire des codes en blocs, d'une longueur n et d'un cardinal M fixés, ayant des distances minimales aussi grandes que possible est un problème important en codage.

Les codes en blocs interviennent dans d'autres domaines d'application que la correction d'erreurs, notamment en cryptographie. Par exemple, Stinson et Massey utilisent dans [SM95] des codes – non linéaires mais systématiques, typiquement les codes de Kerdock et de Preparata – pour construire des fonctions booléennes non linéaires et résilientes. Ce type de fonctions est utilisé dans la construction des chiffrements par flots.

Pour apporter des solutions aux problèmes de théorie des codes, l'alphabet Σ n'est pas quelconque, il est muni d'une structure algébrique afin de faciliter la définition et l'étude des codes. Pendant longtemps, cette structure a été restreinte à celle de corps finis et généralement, dans ce cas, le code se voit imposer une structure d'espace vectoriel, ce qui lui vaut le nom de code linéaire. Ce n'est que relativement récemment que les codes sur des alphabets munis de structures moins restrictives ont commencé à être étudiés intensivement.

Au début des années 1990, dans leur article [HKC+94], Hammons, Kumar, Calderbank, Sloane et Solé donnèrent une construction très simple de certains codes binaires, c'est-à-dire définis sur le corps à deux éléments, non linéaires figurant parmi les meilleurs connus. Il s'agit notamment des codes de Kerdock et de Preparata. Cette construction est également à l'origine de l'explication algébrique d'une curieuse relation entre codes de Kerdock et de Preparata, à savoir leur dualité formelle. Quelques années auparavant, Nechaev, dans [Nec91], avait également donné une construction des codes de Kerdock utilisant l'anneau des entiers modulo 4, $\mathbb{Z}_4$.

L'approche utilisée consiste à construire des codes linéaires sur $\mathbb{Z}_4$ – c'est-à-dire des modules sur $\mathbb{Z}_4$ – puis à les transformer en codes binaires. Les codes ainsi obtenus sont dits $\mathbb{Z}_4$-linéaires. La transformation de codes linéaires sur $\mathbb{Z}_4$ en codes binaires s'opère à l'aide de l'application de Gray qui va de $\mathbb{Z}_4$ dans $\mathbb{Z}_2^2$, étendue coordonnée par coordonnée. C'est en partie grâce aux propriétés de cette application que l'on peut étudier les paramètres des codes binaires ainsi obtenus. Ainsi, on a pu prouver que de tels codes peuvent avoir de bonnes performances. Depuis son apparition, cette technique a très largement fait ses preuves comme en témoignent les travaux de Bonnecaze *et al.*, Calderbank *et al.*, et de Pless et Qian (voir respectivement [BSC95], [CMK+96], [PQ96]), qui présentent des codes $\mathbb{Z}_4$-linéaires figurant toujours parmi les meilleurs codes connus.

Une généralisation de l'application de Gray aux anneaux $\mathbb{Z}_{2^k}$ a été introduite par Carlet dans [Car98]. Elle a ensuite été adaptée, par Greferath et Schmidt dans [GS99], aux anneaux $\mathbb{Z}_{p^k}$ (p premier). Ces généralisations s'accompagnaient des notions de $\mathbb{Z}_{2^k}$ et $\mathbb{Z}_{p^k}$-linéarités et ont déjà permis, conjointement à l'utilisation de la méthode du relèvement de Hensel, la construction de codes meilleurs que ceux connus jusque-là (cf. [GS99] et [DGL+01]).

Dans [Car98], Carlet généralise la famille de codes binaires très performants que sont les codes de Kerdock, dont Hammons *et al.* avaient donné une construction $\mathbb{Z}_4$-linéaire, et établit une borne inférieure sur la distance minimale de ces codes de Kerdock généralisés. La borne obtenue laissait espérer que cette généralisation donnait de bons codes, à condition toutefois que cette dernière fût un peu éloignée de la véritable distance minimale de ces codes. Nous donnons au chapitre 4 une généralisation de cette borne valable pour des codes de Kerdock $\mathbb{Z}_{p^k}$-linéaires et prouvons que ces codes sont cycliques sur $\mathbb{Z}_{p^k}$. Nous donnons ensuite des tables – calculées par ordinateurs – prouvant que la borne est bonne et par voie de conséquence que les codes de Kerdock généralisés ne le sont pas (tout au moins en petite longueur).

D'un autre coté, les résultats de Greferath et Schmidt [GS99], et de Duursma, Greferath, Litsyn et Schmidt [DGL+01], indiquent qu'il est possible de construire de bons codes en utilisant le relèvement de polynômes générateurs de codes cycliques sur $\mathbb{F}_p$ pour obtenir des codes sur l'anneau $\mathbb{Z}_{p^k}$ et en redescendant ces codes sur $\mathbb{F}_p$ par l'application de Gray généra-

lisée. C'est ainsi que nous considérons, au chapitre 5, les codes de résidus quadratiques, qui semblaient *a priori* bien se prêter à ce type de construction : en effet, [BSC95], [CMK+96] et [PQ96] utilisent déjà ces codes avec le relèvement de Hensel sur $\mathbb{Z}_4$, et [DGL+01] et [GS99] les utilisent pour des relèvements à $\mathbb{Z}_8$ et $\mathbb{Z}_9$ respectivement. Ces codes nous ont permis d'obtenir trois nouveaux codes égalant les meilleurs codes linéaires de mêmes longueur et cardinalité. Toutefois, contrairement à nos attentes, les codes obtenus ne surpassent pas les meilleurs codes linéaires.

De plus, dans [DGL+01], Duursma *et al.* utilisent une propriété du code $\mathbb{Z}_8$-linéaire qu'ils obtiennent par relèvement/redescente, pour construire un meilleur code par réunion de ce code $\mathbb{Z}_8$-linéaire et d'un de ses translatés. Au chapitre 6, nous généralisons cette technique à tout code $\mathbb{Z}_{p^k}$-linéaire et nous en déduisons une borne sur les cardinaux de ces codes. Nous verrons que cette borne conduit à de légères améliorations.

Chapitre 1

Préliminaires

Nous introduisons dans ce chapitre deux outils importants pour la suite de notre étude : le relèvement de Hensel et les anneaux de Galois.

Tout d'abord, nous présentons le relèvement de Hensel, qui permet d'obtenir (« relever »), sous certaines conditions, une factorisation d'un polynôme dans l'anneau $\mathbb{Z}_{p^k}[X]$ à partir d'une factorisation dans $\mathbb{Z}_p[X]$. Cela nous servira dans deux cadres différents : en premier lieu, cela permet une construction effective des anneaux de Galois ; en second lieu, le relèvement de Hensel sera une technique de construction de codes cycliques sur $\mathbb{Z}_{p^k}$. Nous illustrons le fonctionnement du relèvement par un algorithme de calcul dans le cas $p = 2$.

Nous abordons ensuite les anneaux de Galois, qui interviendront également à double titre. D'une part, ils constituent un cadre naturel pour l'étude des codes cycliques sur $\mathbb{Z}_{p^k}$, au même titre que les corps finis $\mathbb{F}_{p^k}$ pour les codes cycliques sur $\mathbb{Z}_p$. D'autre part, ils donnent une présentation des codes de Kerdock généralisés semblable à celle des codes de Reed et Muller d'ordre un. La structure d'anneau de Galois généralise les corps finis en conservant de nombreuses propriétés de ces derniers, parmi lesquelles figure l'existence d'un automorphisme de Frobenius ainsi qu'une application trace.

1.1 Relèvement de Hensel

Lemme 1.1 (Lemme de Hensel, [Mac74, chap. XIII, th. 4]) *Soient* p *un nombre premier,* k *un entier supérieur ou égal à 2 et* $P \in \mathbb{Z}_{p^k}[X]$ *un polynôme unitaire, tel que*

$$P \equiv QR \pmod{p} ,$$

pour $Q, R \in \mathbb{Z}_p[X]$*, deux polynômes unitaires premiers entre eux. Alors, il existe un unique couple* $(Q^{(k)}, R^{(k)})$ *de polynômes unitaires de* $\mathbb{Z}_{p^k}[X]$*, tel que*

1. $P = Q^{(k)}R^{(k)}$,
2. $Q^{(k)} \equiv Q \pmod{p}$ *et* $R^{(k)} \equiv R \pmod{p}$,
3. $Q^{(k)}$ *et* $R^{(k)}$ *sont premiers entre eux.*

De plus, on a $\deg\left(Q^{(k)}\right) = \deg(Q)$ *et* $\deg\left(R^{(k)}\right) = \deg(R)$.

L'anneau $\mathbb{Z}_p[X]$ étant factoriel, c'est-à-dire tout polynôme à coefficients dans $\mathbb{Z}_p$ se décomposant de manière unique – à une permutation près – en produit de facteurs irréductibles, on a pour tout polynôme $P \in \mathbb{Z}_{p^k}[X]$:

$$P \equiv f_1^{e_1} \dots f_\ell^{e_\ell} \pmod{p} \ ,$$

où $f_1, \dots, f_\ell$ sont des polynômes irréductibles de $\mathbb{Z}_p[X]$ et $e_1, \dots, e_\ell$ des entiers strictement positifs. Il est donc possible, par récurrence sur le nombre de facteurs, de généraliser le lemme 1.1 afin d'obtenir la factorisation de tout polynôme de $\mathbb{Z}_{p^k}[X]$ à partir de sa factorisation dans $\mathbb{Z}_p[X]$.

Théorème 1.2 (Relèvement de Hensel, [Mac74, chap. XIII, th. 11]) *Soient* p *un nombre premier,* k *un entier supérieur ou égal à 2 et* $P \in \mathbb{Z}_{p^k}[X]$ *un polynôme unitaire. Soit* $P \bmod p = f_1^{e_1} \dots f_\ell^{e_\ell}$ *la factorisation de* P *dans* $\mathbb{Z}_p[X]$*, où* $f_1, \dots, f_\ell$ *sont des polynômes irréductibles et* $e_1, \dots, e_\ell$ *des entiers strictement positifs. Il existe un unique* ℓ*-uplet* $(g_1^{(k)}, \dots, g_\ell^{(k)})$ *de polynômes unitaires de* $\mathbb{Z}_{p^k}[X]$*, tel que*

1. $P = g_1^{(k)} \dots g_\ell^{(k)}$,
2. $g_i^{(k)} \equiv f_i^{e_i} \pmod{p}$,
3. *les* $g_i^{(k)}$ *sont deux à deux premiers entre eux.*

En d'autres termes, les polynômes unitaires de $\mathbb{Z}_{p^k}[X]$ se décomposent – de manière unique – en produits de polynômes du type des $g_i^{(k)}$, *i.e.* qui, réduits modulo p, sont des puissances d'un polynôme irréductible. Cette propriété va nous permettre de définir *le* relevé de Hensel d'un facteur de $X^n - 1$ où n est premier avec p. En effet, dans ce cas, $X^n - 1$ ne comporte que des facteurs simples.

Définition 1.3 (Relevé de Hensel) *Soient* Q *et* R *deux polynômes à coefficients dans* $\mathbb{Z}_p$ *tels que* $X^n - 1 = Q(X)R(X)$ *où* n *est un entier premier avec* p*. On appelle relevé de Hensel d'ordre* k *du polynôme* Q*, le polynôme* $Q^{(k)}$ *du couple* $(Q^{(k)}, R^{(k)})$.

Proposition 1.4 *Soit* $Q \in \mathbb{Z}_p$ *un facteur de* $X^n - 1$*. Son relevé de Hensel d'ordre* k *divise* $X^n - 1$ *dans* $\mathbb{Z}_{p^k}[X]$.

Définition 1.5 (B-polynômes) *Lorsque* Q *est irréductible et primitif, ses relevés sont appelés des B-polynômes* [1].

Le cas le plus important dans la suite est le cas binaire, *i.e.* $p = 2$. La proposition suivante décrit un algorithme itératif de calcul du relevé de Hensel d'un polynôme pour $p = 2$; dans le cas général, on renvoie à l'algorithme 15.10 de [GG99].

Proposition 1.6 (Calcul du relevé de Hensel binaire) *Soient* $Q \in \mathbb{Z}_2[X]$ *un facteur de* $X^{2^m-1} - 1$ *et* $Q^{(k)} \in \mathbb{Z}_{2^k}[X]$ *son relevé de Hensel d'ordre* k. *Posons* $Q^{(k)}(X) = P(X) - I(X)$ *où* P *contient les monômes de degré pair et* I *ceux de degré impair. On a alors* $Q^{(k+1)}(X^2) = \pm(P^2(X) - I^2(X))$, *les opérations étant faites dans* $\mathbb{Z}_{p^{k+1}}[X]$ *et le signe étant choisi pour que* Q^{k+1} *soit unitaire.*

Preuve. Par construction, $P^2(X) - I^2(X)$ n'a que des monômes de degré pair, le polynôme unitaire $f(X) \in \mathbb{Z}_{2^{k+1}}[X]$ tel que $f(X^2) = \pm(P^2(X) - I^2(X))$ est donc bien défini. On a

$$f\left(X^2\right) \equiv P\left(X^2\right) - I\left(X^2\right) \equiv Q\left(X^2\right) \pmod 2$$

car l'application $R(X) \mapsto R^2(X)$ se réduit à $R(X) \mapsto R(X^2)$ sur $\mathbb{Z}_2[X]$. Donc, $f(X) \equiv Q(X) \pmod 2$. Il reste à vérifier que f divise $X^{2^m-1}-1$ dans $\mathbb{Z}_{2^{k+1}}[X]$. Or

$$f\left(X^2\right) = \pm Q^{(k)}(X)Q^{(k)}(-X) \ ,$$

les opérations étant faites dans $\mathbb{Z}_{2^{k+1}}[X]$. Par hypothèse, $Q^{(k)}$ divise $X^{2^m-1}-1$ dans $\mathbb{Z}_{2^k}[X]$. On peut donc écrire

$$X^{2^m-1} - 1 = Q^{(k)}(X)A(X) + 2^k B(X) \ ,$$

où $A(X)$ et $B(X)$ sont deux polynômes de $\mathbb{Z}_{2^{k+1}}[X]$. Cela nous donne également

$$(-X)^{2^m-1} - 1 = Q^{(k)}(-X)A(-X) + 2^k B(-X) \ .$$

Alors

$$\begin{aligned} X^{2^{m+1}-2} - 1 &= \left(X^{2^m-1} - 1\right)\left(X^{2^m-1} + 1\right) \\ &= -\left(X^{2^m-1} - 1\right)\left((-X)^{2^m-1} - 1\right) \\ &= -Q^{(k)}(X)Q^{(k)}(-X)A(X)A(-X) \\ &\qquad - 2^k\left(Q^{(k)}(X)A(X)B(-X) + Q^{(k)}(-X)A(-X)B(X)\right) \ . \end{aligned}$$

[1] Signalons qu'un polynôme dont l'image sur $\mathbb{Z}_p$ est irréductible n'est pas nécessairement un relevé de Hensel, cf. [Wan97, §6.4].

Posons $Q^{(k)}(X) = P(X) - I(X)$, $A(X) = P_a(X) - I_a(X)$ et $B(X) = P_b(X) - I_b(X)$, où $P(X), P_a(X)$ et $P_b(X)$ ne contiennent que les monômes de degré pair et $I(X), I_a(X), I_b(X)$, ceux de degré impair. On a ainsi

$$\begin{aligned}
&Q^{(k)}(X)A(X)B(-X) + Q^{(k)}(-X)A(-X)B(X) \\
&\quad = \Big(P(X) - I(X)\Big)\Big(P_a(X) - I_a(X)\Big)\Big(P_b(-X) - I_b(-X)\Big) \\
&\qquad + \Big(P(-X) - I(-X)\Big)\Big(P_a(-X) - I_a(-X)\Big)\Big(P_b(X) - I_b(X)\Big) \\
&\quad = \Big(P(X) - I(X)\Big)\Big(P_a(X) - I_a(X)\Big)\Big(P_b(X) + I_b(X)\Big) \\
&\qquad + \Big(P(X) + I(X)\Big)\Big(P_a(X) + I_a(X)\Big)\Big(P_b(X) - I_b(X)\Big) \\
&\quad = 2\Big(P(X)P_a(X)P_b(X) - P(X)I_a(X)I_b(X) \\
&\qquad - I(X)P_a(X)I_b(X) + I(X)I_a(X)P_b(X)\Big) \ .
\end{aligned}$$

Donc, on peut écrire

$$X^{2^{m+1}-2} - 1 = Q^{(k)}(X)Q^{(k)}(-X)K(X) + 2^{k+1}L(X) \ ,$$

où $K(X)$ et $L(X)$ sont des polynômes à coefficients dans $\mathbb{Z}_{p^{k+1}}$. Il en résulte que le polynôme $f(X^2) = \pm Q^{(k)}(X)Q^{(k)}(-X)$ divise $X^{2^{m+1}-2} - 1$ dans $\mathbb{Z}_{2^{k+1}}[X]$, donc que $f(X)$ divise $X^{2^m-1} - 1$ dans $\mathbb{Z}_{2^{k+1}}[X]$. □

EXEMPLE 1.7 Dans $\mathbb{Z}_2[X]$, $X^7 - 1$ se factorise sous la forme

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

Posons $Q = Q^{(1)} = X^3 + X + 1 \in \mathbb{Z}_2[X]$ et appliquons la proposition 1.6 pour calculer son relevé d'ordre 3 (un B-polynôme avec notre définition). On a

$$\begin{aligned}
P_1(X) &= 1 && \mod 2 \ , \\
I_1(X) &= -X^3 - X && \mod 2 \ ,
\end{aligned}$$

donc

$$\begin{aligned}
[P_1(X)]^2 &= 1 && \mod 4 \ , \\
[I_1(X)]^2 &= X^6 + 2X^4 + X^2 && \mod 4 \ ,
\end{aligned}$$

d'où,

$$Q^{(2)}\left(X^2\right) = X^6 + 2X^4 + X^2 - 1 \mod 4 \ .$$

Ainsi, le relevé de Hensel d'ordre 2 du polynôme Q est :

$$Q^{(2)}(X) = X^3 + 2X^2 + X - 1 \qquad \bmod 4 \ .$$

De même, pour calculer $Q^{(3)}$ on décompose $Q^{(2)}$ sous la forme :

$$\begin{aligned} P_2(X) &= 2X^2 - 1 && \bmod 4 \ , \\ I_2(X) &= -(X^3 + X) && \bmod 4 \ , \end{aligned}$$

ce qui donne

$$\begin{aligned} [P_2(X)]^2 &= 4X^4 - 4X^2 + 1 && \bmod 8 \ , \\ [I_2(X)]^2 &= X^6 + 2X^4 + X^2 && \bmod 8 \ . \end{aligned}$$

On a donc

$$Q^{(3)}\left(X^2\right) = X^6 - 2X^4 + 5X^2 - 1 \quad \bmod 8 \ ,$$

soit, finalement,

$$Q^{(3)}(X) = X^3 + 6X^2 + 5X + 7 \qquad \bmod 8 \ .$$

On peut alors vérifier que $Q^{(3)}$ est bien un diviseur de $X^7 - 1$ dans $\mathbb{Z}_8[X]$, en effet

$$Q^{(3)}(X)\,(X^4 + 2X^3 + 7X^2 + 5X + 1) = X^7 - 1 \qquad \bmod 8 \ .$$

Bien entendu, $X^4 + 2X^3 + 7X^2 + 5X + 1$ est le relevé de Hensel d'ordre 3 du polynôme $(X^3 + X^2 + 1)(X - 1)$. □

1.2 Anneaux de Galois

Les anneaux de Galois sont une généralisation des corps finis. De même que ces derniers, ils peuvent être définis par une structure d'anneau quotient d'un anneau de polynômes. De nombreuses propriétés résultent directement du fait que les anneaux de Galois sont finis, commutatifs, unitaires et locaux – ce qui signifie que le nombre d'éléments est fini, leur produit est commutatif et admet un élément neutre, et qu'il existe un unique idéal maximal. Toutefois, nous préférons une approche plus concrète et utilisons leur structure d'anneau quotient d'un anneau de polynômes pour obtenir leurs propriétés.

Proposition 1.8 *Soient p un nombre premier, k un entier strictement positif et $P \in \mathbb{Z}_{p^k}[X]$ un B-polynôme de degré m. L'anneau $A = \mathbb{Z}_{p^k}[X]/(P)$ est de caractéristique p^k et de cardinal p^{km}. Les éléments non inversibles forment un idéal engendré par p et cet idéal est le seul idéal maximal de A. De plus, l'anneau quotient $A/(p)$ est un corps fini à p^m éléments.*

PREUVE. La caractéristique et le cardinal de A sont des conséquences directes de sa définition.
On a (cf. [Hun80, th. 2.12])

$$\begin{aligned}\left(\mathbb{Z}_{p^k}[X]/(P)\right)/(p) &\simeq (\mathbb{Z}_{p^k}[X]/(p))/(P \bmod p) \ , \\ &\simeq \mathbb{Z}_p[X]/(P \bmod p) \ .\end{aligned}$$

Or, $P \bmod p$ est irréductible par définition d'un B-polynôme, et son degré est égal à m, donc

$$A/(p) \simeq \mathbb{F}_{p^m} \ . \qquad (*)$$

Rappelons ([Hun80, th. 2.20]) qu'un anneau commutatif et unitaire quotienté par un idéal $\mathcal{I}$ est un corps si et seulement si l'idéal $\mathcal{I}$ est maximal. On déduit donc de (*) que (p) est maximal. Considérons un élément $\alpha \in A$, on vérifie aisément qu'il est inversible si et seulement si $\alpha \bmod p$ est inversible. Ainsi, les éléments non inversibles de l'anneau A sont exactement ceux qui valent 0 modulo p, *i.e.* ce sont les éléments de l'idéal (p). Enfin, considérons un idéal $\mathcal{I} \subset A$. Si $\mathcal{I}$ contient un élément inversible, alors $\mathcal{I} = A$. Dans le cas contraire, il ne contient que des éléments non inversibles et $\mathcal{I} \subset (p)$, (p) est donc le seul idéal maximal, ce qui termine la preuve. □

DÉFINITION 1.9 (ANNEAU DE GALOIS) *On appelle anneau de Galois tout anneau de la forme $\mathbb{Z}_{p^k}[X]/(P)$, où p est un nombre premier, k un entier strictement positif, et $P \in \mathbb{Z}_{p^k}[X]$ un B-polynôme.*

Lorsque $k = 1$, on retrouve le corps fini à $p^{\deg(P)}$ éléments. Si on considère deux B-polynômes P_1, P_2 de même degré, on obtient des anneaux isomorphes. Cela motive la notation suivante :

NOTATION 1.10 (ANNEAU DE GALOIS) *On note $\mathrm{GR}(p^k, m)$ tout anneau de Galois isomorphe à $\mathbb{Z}_{p^k}[X]/(P)$ où $P(X) \in \mathbb{Z}_{p^k}[X]$ est un B-polynôme de degré m. La classe d'équivalence de X est notée x,* i.e. *$x = X \bmod P(X)$. Le B-polynôme définissant $\mathrm{GR}(p^k, m)$ sera systématiquement noté P.*

NOTATION 1.11 *On notera χ le morphisme surjectif de $\mathrm{GR}(p^k, m)$ sur $\mathbb{F}_{p^m}$ qui à un élément $\alpha \in \mathrm{GR}(p^k, m)$ associe sa classe d'équivalence $\chi(\alpha) = \alpha + (p)$.*

PROPOSITION 1.12 *L'élément $x = X \bmod P(X)$ a les propriétés suivantes :*

1. *$\chi(x)$ est un élément primitif de $\mathbb{F}_{p^m}$,*
2. *$P(x) = 0$,*
3. *$x^{p^m-1} = 1$,*
4. *x engendre un groupe multiplicatif d'ordre $p^m - 1$,*

$$\mathcal{T}^* = \left\{1, x, \ldots, x^{p^m-2}\right\} \ .$$

En particulier, tout élément de $\mathcal{T}^*$ est inversible dans $\mathcal{T}^*$.

Les éléments d'un anneau de Galois peuvent être représentés de deux manières différentes, sous forme additive et sous forme multiplicative.

PROPOSITION 1.13 (REPRÉSENTATIONS DES ÉLÉMENTS DE $\mathrm{GR}(p^k, m)$) *Soit* $\alpha \in \mathrm{GR}(p^k, m)$.
Représentation additive : α *s'écrit de manière unique sous la forme*

$$\alpha = \sum_{i=0}^{m-1} \lambda_i X^i \quad \textit{avec } \lambda_0, \ldots, \lambda_{m-1} \in \mathbb{Z}_{p^k} \ .$$

Représentation multiplicative : α *s'écrit de manière unique sous la forme*

$$\alpha = \sum_{j=0}^{k-1} \mu_j p^j \quad \textit{avec } \mu_0, \ldots, \mu_{k-1} \in \mathcal{T} \ ,$$

où $\mathcal{T} = \{0\} \cup \mathcal{T}^*$ *est appelé ensemble de Teichmuller.*

PREUVE. La représentation additive découle directement de la structure d'anneau quotient d'un anneau de Galois. L'existence de la représentation multiplicative est une conséquence directe de l'algorithme de conversion détaillé ci-dessous. L'unicité repose sur le fait que la différence de deux éléments distincts, μ et μ', de $\mathcal{T}$ est inversible. Si l'un des deux est nul, c'est clair. Sinon la différence est du type $X^i - X^j$ pour i et j dans $[0 \ldots p^{m-2}]$, ce qui peut s'écrire $X^{i-j}(1 - X^{j-i})$ et si $i \neq j$, alors les deux termes du produit sont inversibles. De là, notons $\sum_{j=0}^{k-1} \mu_j p^j$ et $\sum_{j=0}^{k-1} \mu'_j p^j$ deux formes multiplicatives d'un même élément α. On a

$$\sum_{j=0}^{k-1} \left(\mu_j - \mu'_j\right) p^j = 0 \pmod{p^k} \ .$$

Cela implique, par réduction modulo p, $\mu_0 - \mu'_0 = 0 \pmod{p}$, donc d'après ce que nous venons de voir $\mu_0 = \mu'_0$. On peut alors mettre p en facteur dans la somme ci-dessus pour obtenir

$$\sum_{j=1}^{k-1} \left(\mu_j - \mu'_j\right) p^{j-1} = 0 \pmod{p^{k-1}} \ .$$

Une réduction modulo p permet d'obtenir l'égalité $\mu_1 = \mu'_1$, et en itérant on obtient l'égalité des deux formes multiplicatives. □

Les calculs avec la représentation additive se font simplement en effectuant les opérations dans $\mathbb{Z}_{p^k}[X]$ et en prenant le reste de la division euclidienne par le B-polynôme P. Pour la représentation multiplicative, ce n'est pas aussi simple : de manière générale, l'addition ou la multiplication de deux formes

multiplicatives n'est pas une forme multiplicative. Une solution consiste à convertir la forme multiplicative en additive, faire l'opération et retourner à la forme multiplicative. Les changements de représentations nécessitent une table donnant la forme additive des éléments du Teichmuller. Cette table s'obtient de manière itérative : en supposant avoir décomposé x^{j-1} sous la forme $\sum_{i=0}^{m-1} a_{j-1,i}x^i$, on a pour $j > m$

$$\begin{aligned} x^j &= x^{j-1} \cdot x \ , \\ &= a_{j-1,0}x + a_{j-1,1}x^2 + \cdots + a_{j-1,m-2}x^{m-1} + a_{j-1,m-1}x^m \ , \\ &= a_{j-1,m-1}a_{m,0} + \sum_{i=1}^{m-1} (a_{j-1,m-1}a_{m,i} + a_{j-1,i-1})x^i \ . \end{aligned}$$

Signalons que la forme additive de x^m est donnée directement par le B-polynôme P, si on pose $P(X) = \sum_{i=0}^{m} c_i X^i$, alors $\sum_i c_i x^i = 0$, d'où

$$x^m = -c_m^{-1} \sum_{i=0}^{m-1} c_i x^i$$

(P étant un B-polynôme de degré m, c_m est nécessairement inversible). On a donc

$$a_{m,i} = -c_m^{-1} c_i \ ,$$

pour tout entier i de $[0, m-1]$. Le passage de la forme multiplicative à la forme additive est alors très simple : soit $\alpha = \sum_{j=0}^{k-1} \mu_j p^j$, il suffit de regarder dans la table la forme additive de μ_j et de remplacer μ_j par cette dernière dans la forme multiplicative de α. En effet, si on pose $\mu_j = \sum u_{j,i}x^i$, on obtient

$$\begin{aligned} \alpha &= \sum_{j=0}^{k-1} \mu_j p^j \\ &= \sum_{j=0}^{k-1} p^j \left(\sum_{i=0}^{m-1} u_{j,i} x^i \right) \\ &= \sum_{i=0}^{m-1} \left(\sum_{j=0}^{k-1} p^j u_{j,i} \right) x^i \ . \end{aligned}$$

Le retour à la forme multiplicative est un peu plus complexe. Il y a deux possibilités :

1. soit $\chi(\alpha)$ est nul, auquel cas α est dans l'idéal (p), donc de la forme $p\alpha'$ pour un certain α' ;
2. soit $\chi(\alpha)$ est non nul. Dans ce cas, $\chi(x)$ étant primitif dans $\mathbb{F}_{p^m}$, il existe un unique entier $i \in [0, p^m - 2]$ tel que $\chi(\alpha) = \chi(x)^i$, *i.e.* $\chi(\alpha - x^i) = 0$

puisque χ est un morphisme d'anneaux. On a donc $\alpha - x^i \in (p)$, ce qui implique que α est de la forme $x^i + p\alpha'$. La recherche de l'entier i peut se faire en utilisant une table dérivée de la table construite ci-dessus en réduisant les coefficients des formes additives modulo p.

Dans les deux cas, on peut écrire $\alpha = \mu_0 + p\alpha'$, avec $\mu_0 \in \mathcal{T}$ et $\alpha' \in \mathrm{GR}(p^k, m)$. L'élément α' étant lui-même dans l'anneau, il est possible de le « décomposer » à son tour sous la forme $\alpha' = \mu_1 + p\alpha''$, ce qui donne pour α : $\mu_0 + p(\mu_1 + p\alpha'')$. En itérant m fois, on obtient pour α une expression de la forme $\sum_{j=0}^{m-1} \mu_j p^j$ qui est nécessairement la forme multiplicative de α puisque cette dernière est unique d'après la proposition 1.13.

Exemple 1.14 On considère $\mathrm{GR}(2^3, 3) = \mathbb{Z}_{2^3}[X]/(7 + 5X + 6X^2 + X^3)$ et on pose $\alpha = 5 + 3x^2$ et $\beta = x$. Nous allons donner les expressions de α et β dans les deux formes et nous allons calculer $\alpha + \beta$ et $\alpha\beta$. Commençons par calculer les deux tables :

$$
\begin{aligned}
x &= & x \\
x^2 &= & x^2 \\
x^3 = -7 - 5x - 6x^2 &= & 1 + 3x + 2x^2 \\
x^4 = x + 3x^2 + 2x^3 = x + 3x^2 - 2(7 + 5x + 6x^2) &= & 2 + 7x + 7x^2 \\
x^5 = x + 7x^2 + 7x^3 &= & 7 + 7x + 5x^2 \\
x^6 = 7x + 7x^2 + 5x^3 &= & 5 + 6x + x^2 \\
x^7 = 5x + 6x^2 + x^3 &= & 1
\end{aligned}
$$

Lorsque l'on quotiente par l'idéal $(2) \subset \mathrm{GR}(2^3, 3)$ on obtient la seconde table :

$$
\begin{aligned}
\chi(x) &= \chi(x) \\
\chi\left(x^2\right) &= \chi\left(x^2\right) \\
\chi\left(x^3\right) &= 1 + \chi(x) \\
\chi\left(x^4\right) &= \chi(x) + \chi\left(x^2\right) \\
\chi\left(x^5\right) &= 1 + \chi(x) + \chi\left(x^2\right) \\
\chi\left(x^6\right) &= 1 + \chi\left(x^2\right) \\
\chi\left(x^7\right) &= 1
\end{aligned}
$$

Ce qui donne

– En représentation additive : α et β étant donnés sous forme additive, on peut directement faire les calculs.

$$\alpha+\beta=\left(5+3x^2\right)+(x) \qquad =5+x+3x^2$$
$$\alpha\beta=\left(5+3x^2\right)(x)=5x+3\left(-7-5x-6x^2\right)=3+6x+6x^2$$

– En représentation multiplicative : commençons par calculer la forme multiplicative de α.

$$\chi(\alpha)=1+\chi\left(x^2\right)$$

donc, grâce à la seconde table,

$$\chi(\alpha)=\chi\left(x^6\right)$$

or, par la première table,

$$\begin{aligned}\alpha-x^6&=5+3x^2-\left(5+6x+x^2\right)\\&=2x+2x^2\\&=2\left(x+x^2\right)\end{aligned}$$

soit

$$\alpha=x^6+2\left(x+x^2\right)\ .$$

En itérant avec $\alpha'=x+x^2$, on a finalement

$$\alpha=x^6+2\left(x^4+2x^5\right)$$

L'élément β est déjà sous forme multiplicative, il n'y donc pas de conversion à faire. La somme $\alpha+\beta$ se fait en utilisant les formes additives, puis en passant à la forme multiplicative par un calcul semblable à celui fait pour α.

$$\begin{aligned}\alpha+\beta&=\left(x^6+2x^4+4x^5\right)+(x)\\&=\left(5+3x^2\right)+(x) && \text{(conversion forme add.)}\\&=5+x+3x^2 && \text{(somme)}\\&=x^5+2x^5+4x^4 && \text{(conversion forme mult.)}\end{aligned}$$

Le calcul du produit est assez simple dans notre exemple puisque le produit des formes multiplicatives est encore une forme multiplicative.

$$\begin{aligned}\alpha\beta&=\left(x^6+2x^4+4x^5\right)(x)\\&=1+2x^5+4x^6\ .\end{aligned}$$

□

Nous allons maintenant présenter l'analogue de l'automorphisme de Frobenius. Pour montrer ses caractéristiques, nous aurons besoin d'une propriété des relevés de Hensel des polynômes irréductibles qui repose sur le lemme suivant :

LEMME 1.15 *Soit* $Q \in \mathbb{Z}_{p^k}[X]$ *un polynôme unitaire tel que* $\chi(Q)$ *soit sans racine multiple, et possède une racine* $\overline{\beta}$ *dans* $\mathbb{F}_{p^m}$ *où* m *désigne un entier strictement positif. Alors il existe un unique élément* $\alpha \in \mathrm{GR}(p^k, m)$ *vérifiant* $Q(\alpha) = 0$ *et* $\chi(\alpha) = \overline{\beta}$.

PREUVE. Nous donnons une preuve reposant sur une généralisation du lemme 1.1. En effet, ce lemme reste vrai si on remplace l'anneau $\mathbb{Z}_{p^k}[X]$ par l'anneau $\mathrm{GR}(p^k, m)$ et le corps fini $\mathbb{Z}_p$ par $\mathbb{F}_{p^m}$. C'est également le cas du théorème 1.2, cf. [Mac74, chap. XIII, th. 4 et 11].
Le polynôme $\chi(Q)$ ayant une racine simple $\overline{\beta} \in \mathbb{F}_{p^m}$, on peut écrire

$$\chi(Q)(X) = (X - \overline{\beta})\,\overline{R}(X) \ ,$$

où $\overline{R}(X) \in \mathbb{F}_{p^m}[X]$ n'admet pas $\overline{\beta}$ pour racine. La généralisation du lemme 1.1 implique

$$Q(X) = (X - \beta + pS(X))\,R(X) \qquad (*)$$

où $S(X), R(X) \in \mathrm{GR}(p^k, m)[X]$ sont unitaires, avec $\chi(R) = \overline{R}$ et où $\beta \in \mathrm{GR}(p^k, m)$ est tel que $\chi(\beta) = \overline{\beta}$. De plus, $X - \beta + pS(X)$ est unitaire et son degré doit être égal à $\deg((X - \overline{\beta})) = 1$. Donc nécessairement $pS(X) = p\beta' \in \mathrm{GR}(p^k, m)$. Si on pose $\alpha = \beta + p\beta'$, l'équation (*) donne

$$Q(X) = (X - \alpha)\,R(X) \ . \qquad (**)$$

Donc, $Q(\alpha) = 0$, prouvant ainsi l'existence d'un élément $\alpha \in \mathrm{GR}(p^k, m)$ vérifiant les conditions du lemme puisque $\chi(\alpha) = \overline{\beta}$.
Pour montrer l'unicité, supposons qu'il existe $\alpha' \in \mathrm{GR}(p^k, m)$ vérifiant $\alpha' \neq \alpha$, $\chi(\alpha') = \overline{\beta}$ et $Q(\alpha') = 0$. Alors (**) implique que $R(\alpha')$ est un diviseur de zéro, d'où $\overline{R}(\overline{\beta}) = 0$, ce qui n'est pas possible. □

PROPOSITION 1.16 *Soit* Q *le relevé de Hensel d'ordre* k *d'un facteur irréductible de* $X^{p^m-1} - 1$. *Le polynôme* Q *a exactement* $d = \deg(Q)$ *racines dans* $\mathrm{GR}(p^k, m)$ *et ces racines sont de la forme* $\alpha, \alpha^p, \ldots, \alpha^{p^{d-1}}$ *où* $\alpha \in \mathcal{T}^*$. *De plus, on a* $\alpha^{p^d} = \alpha$.

PREUVE. Commençons par rappeler qu'un polynôme de degré d, irréductible sur $\mathbb{F}_p[X]$ est simplement scindé dans $\mathbb{F}_{p^d}[X]$ et que si on note $\overline{\alpha}$ l'une de ses racines, l'ensemble des racines du polynôme est simplement

$$\left\{\overline{\alpha}, \overline{\alpha}^p, \ldots, \overline{\alpha}^{p^{d-1}}\right\} \ .$$

Il est clair que toute racine de Q est congrue modulo p à une racine de $\chi(Q)$. Comme, par définition de Q, $\chi(Q)$ est irréductible sur $\mathbb{F}_p$, le lemme 1.15 implique que Q a exactement d racines dans $\mathrm{GR}(p^k, m)$ et que ces racines sont congrues à $\overline{\alpha}, \overline{\alpha}^p, \ldots, \overline{\alpha}^{p^{d-1}}$ modulo p.
Or, nécessairement, les racines de Q sont dans $\mathcal{T}^*$. En effet, si β est une racine de Q, alors β est une racine de $X^{p^{m-1}} - 1$ car $Q \mid X^{p^{m-1}} - 1$. D'autre part, les racines de $X^{p^{m-1}} - 1$ sont exactement les éléments de $\mathcal{T}^*$, car la propriété 4 de la proposition 1.12 implique que ces éléments sont des racines et la propriété d'unicité donnée dans lemme 1.15 implique que ce sont les seules puisque le polynôme $X^{p^{m-1}} - 1$ est simplement scindé sur $\mathbb{F}_{p^m}[X]$.
Il en résulte donc que les d racines de Q sont dans $\mathcal{T}^*$ et qu'elles sont congrues à $\overline{\alpha}, \overline{\alpha}^p, \ldots, \overline{\alpha}^{p^{d-1}}$ modulo p. Comme $\chi(x)$ est primitif sur $\mathbb{F}_{p^m}$, il existe un entier i tel que $\chi(x^i) = \chi(x)^i = \overline{\alpha}$. Posons $\alpha = x^i$. Clairement, α^{p^j} est le seul élément de $\mathcal{T}^*$ congru à $\overline{\alpha}^{p^j}$, $j \in [0, m-1]$, ce qui termine la première partie de la preuve.
L'égalité $\alpha^{p^d} = \alpha$ est vraie modulo p puisque $\overline{\alpha} \in \mathbb{F}_{p^d}$. Or cela implique $ip^d = i \pmod{p^m - 1}$ et par conséquent $x^{ip^d} = x^i$ étant donné que l'élément x est d'ordre $p^m - 1$. On a donc bien $\alpha^{p^d} = \alpha$ dans $\mathrm{GR}(p^k, m)$. □

À l'aide de ce résultat, nous allons montrer que l'application définie par

$$\begin{array}{rccc} \sigma : & \mathrm{GR}(p^k, m) & \longrightarrow & \mathrm{GR}(p^k, m) \\ & \displaystyle\sum_{i=0}^{m-1} \lambda_i x^i & \longmapsto & \displaystyle\sum_{i=0}^{m-1} \lambda_i x^{ip} \qquad \lambda_i \in \mathbb{Z}_{p^k} \end{array}$$

possède des propriétés très proches de l'automorphisme de Frobenius des corps finis.

Théorème 1.17 (Automorphisme de Frobenius) *L'application σ est un automorphisme de l'anneau de Galois $\mathrm{GR}(p^k, m)$ qui laisse invariants les éléments du sous-anneau $\mathbb{Z}_{p^k}$:*

1. $\forall (\alpha, \beta) \in \mathrm{GR}(p^k, m)^2 \qquad \sigma(\alpha + \beta) = \sigma(\alpha) + \sigma(\beta)$,
2. $\forall (\alpha, \beta) \in \mathrm{GR}(p^k, m)^2 \qquad \sigma(\alpha\beta) = \sigma(\alpha)\sigma(\beta)$,
3. *σ est bijective,*
4. $\forall \lambda \in \mathbb{Z}_{p^k} \qquad \sigma(\lambda) = \lambda$.

D'autre part, on a

$$\sigma\left(\sum_{i=0}^{k-1} \mu_i p^i\right) = \sum_{i=0}^{k-1} \mu_i^p p^i \qquad \mu_i \in \mathcal{T} \ .$$

De plus, tout automorphisme de $\mathrm{GR}(p^k, m)$ est une puissance du Frobenius, c'est-à-dire qu'on a

$$\mathcal{A}(p^k, m) = \{\mathrm{Id}, \sigma, \sigma^2, \ldots, \sigma^{m-1}\} \ ,$$

où $\mathcal{A}(p^k, m)$ *est le groupe des automorphismes de* $\mathrm{GR}(p^k, m)$.

PREUVE. De par la définition de σ, on a clairement les propriétés 1 et 4. Prouvons la propriété 2. Soient $\alpha, \beta \in \mathrm{GR}(p^k, m)$. On pose

$$\alpha = P_\alpha(x) = \sum_{i=0}^{m-1} a_i x^i, \quad \beta = P_\beta(x) = \sum_{i=0}^{m-1} b_i x^i \quad \text{et} \quad \alpha\beta = P_{\alpha\beta}(x) = \sum_{i=0}^{m-1} c_i x^i.$$

En d'autres termes, $P_\alpha(X), P_\beta(X), P_{\alpha\beta}(X)$ sont des polynômes de $\mathbb{Z}_{p^k}[X]$ de degré inferieur ou égal à m et $\alpha \equiv P_\alpha(X) \pmod{P(X)}$, où $P(X)$ est le B-polynôme utilisé pour définir l'anneau de Galois, de même pour β et $\alpha\beta$. Avec ces notations, $\sigma(\alpha) = P_\alpha(x^p)$, et la propriété 2 se réécrit

$$P_{\alpha\beta}(x^p) = P_\alpha(x^p)\, P_\beta(x^p) \quad .$$

Or, dans $\mathbb{Z}_{p^k}[X]$, on a

$$P_\alpha(X)P_\beta(X) = P_{\alpha\beta}(X) + Q(X)P(X) \quad ,$$

où $Q(X) \in \mathbb{Z}_{p^k}[X]$. Donc,

$$P_\alpha(x^p)\, P_\beta(x^p) = P_{\alpha\beta}(x^p) + Q(x^p)\, P(x^p) \quad .$$

Par la proposition 1.16, on a $P(x^p) = 0$, et par conséquent la propriété 2 est vérifiée. L'application σ est donc un endomorphisme de $\mathrm{GR}(p^k, m)$.
Soit $\beta = x^j$ un élément de $\mathcal{T}^*$. Par la propriété 2, on a $\sigma(x^j) = \sigma(x)^j = x^{pj}$. Donc pour une forme multiplicative $\sum_{i=0}^{k-1} \mu_i p^i$, on a

$$\begin{aligned} \sigma\left(\sum_{i=0}^{k-1} \mu_i p^i\right) &= \sum_{i=0}^{k-1} \sigma\left(\mu_i p^i\right) \\ &= \sum_{i=0}^{k-1} \sigma(\mu_i)\, \sigma\left(p^i\right) \\ &= \sum_{i=0}^{k-1} \mu_i^p\, p^i \quad . \end{aligned} \tag{*}$$

Cette dernière expression permet de prouver simplement que σ est une bijection (propriété 3). Soient α et β tels que $\sigma(\alpha) = \sigma(\beta)$. Cela implique que $\sigma(\alpha - \beta) = 0$. Posons $\alpha - \beta = \sum_{i=0}^{k-1} \mu_i p^i$. Par unicité de la représentation multiplicative et par (*), on a $\mu_i^p = 0$ pour $i \in [0, k-1]$, donc $\mu_i = 0$ pour $i \in [0, k-1]$, *i.e.* $\alpha = \beta$. Comme nous avons déjà prouvé que σ est un endomorphisme, il en résulte que c'est un automorphisme.
Prouvons la dernière partie du théorème. Notons ψ un automorphisme de $\mathrm{GR}(p^k, m)$. Nécessairement, ψ est l'identité sur $\mathbb{Z}_{p^k}$, car ψ vérifie les égalités $\psi(1) = 1$ et $\psi(\alpha + \beta) = \psi(\alpha) + \psi(\beta)$ par définition d'un automorphisme

d'anneau. Donc nous avons $P(\psi(x)) = \psi(P(x)) = 0$ et par la proposition 1.16, $\psi(x)$ est de la forme x^{p^i}, avec $i \in [0, m-1]$. Il résulte de la propriété 2 que $\psi(\mu) = \mu^{p^i}$ pour tout $\mu \in \mathcal{T}^*$. On a donc finalement

$$\begin{aligned}\psi\left(\sum_{i=0}^{k-1} \mu_i p^i\right) &= \sum_{i=0}^{k-1} \psi(\mu_i)\, p^i \\ &= \sum_{i=0}^{k-1} \mu_i^{p^i}\, p^i \\ &= \sigma^i\left(\sum_{i=0}^{k-1} \mu_i p^i\right) \ ,\end{aligned}$$

ce qui termine la démonstration du théorème. □

Proposition 1.18 (Indépendance linéaire de $\mathcal{A}(p^k, m)$) *Les automorphismes de* $\mathrm{GR}(p^k, m)$ *sont linéairement indépendants sur* $\mathrm{GR}(p^k, m)$, i.e. *pour toute combinaison linéaire à coefficients dans* $\mathrm{GR}(p^k, m)$ *d'automorphismes différents* $\psi_1, \ldots, \psi_n$, *on a*

$$\alpha_1\psi_1 + \cdots + \alpha_n\psi_n = 0 \qquad \Longrightarrow \qquad \alpha_1 = \cdots = \alpha_n = 0 \ .$$

Preuve. Si $n = 1$, le résultat est clair. Soit $n \geq 2$ minimal pour une relation du type

$$\alpha_1\psi_1 + \cdots + \alpha_n\psi_n = 0 \ . \qquad (*)$$

Alors, pour tout y

$$\alpha_1\psi_1(xy) + \cdots + \alpha_n\psi_n(xy) = 0 \ ,$$

soit

$$\alpha_1\psi_1(x)\psi_1 + \cdots + \alpha_n\psi_n(x)\psi_n = 0 \ . \qquad (**)$$

L'élément x étant inversible, $\psi_1(x)$ l'est également et son inverse est simplement $\psi_1(x^{-1})$. En multipliant (**) par $\psi_1(x^{-1})$ et en soustrayant à (*), on obtient pour tout y

$$\sum_{i=1}^{n} \alpha_i \left(1 - \psi_1\left(x^{-1}\right)\psi_i(x)\right)\psi_i(y) = 0 \ ,$$

soit

$$\sum_{i=2}^{n} \alpha_i \left(1 - \psi_1\left(x^{-1}\right)\psi_i(x)\right)\psi_i(y) = 0 \ ,$$

Or, clairement, $\psi_2(x) \neq \psi_1(x)$ (sinon $\psi_2 = \psi_1$) et le coefficient du membre de gauche pour $i = 2$ est non nul, ce qui contredit le caractère minimal de n et conclut la preuve. □

L'automorphisme de Frobenius permet, de manière similaire a ce qui se passe pour les corps finis de définir une application trace : la trace de α est la somme des différentes valeurs prises par les automorphismes de l'anneau, soit

$$\begin{array}{rccc} \mathrm{Tr}: & \mathrm{GR}(p^k, m) & \longrightarrow & \mathrm{GR}(p^k, m) \\ & \alpha & \longmapsto & \displaystyle\sum_{i=0}^{m-1} \sigma^i(\alpha) \end{array}$$

Les trois propriétés suivantes découlent directement du fait que σ est un automorphisme laissant $\mathbb{Z}_{p^k}$ invariant :

1. $\forall \lambda \in \mathbb{Z}_{p^k}, \forall \alpha \in \mathrm{GR}(p^k, m) \qquad \mathrm{Tr}(\lambda\alpha) = \lambda \mathrm{Tr}(\alpha)$,
2. $\forall (\alpha, \beta) \in \mathrm{GR}(p^k, m)^2 \qquad \mathrm{Tr}(\alpha + \beta) = \mathrm{Tr}(\alpha) + \mathrm{Tr}(\beta)$,
3. $\forall \alpha \in \mathrm{GR}(p^k, m) \qquad \mathrm{Tr}(\sigma(\alpha)) = \sigma(\mathrm{Tr}(\alpha)) = \mathrm{Tr}(\alpha)$.

Remarquons que la propriété 3 implique que la trace est à valeurs dans $\mathbb{Z}_{p^k}$. En effet, nous avons :

LEMME 1.19 *Les seuls élements de* $\mathrm{GR}(p^k, m)$ *invariants par* σ *sont ceux de* $\mathbb{Z}_{p^k}$.

PREUVE. Soit $\alpha = \sum_i \mu_i p^i$, $\mu_i \in \mathcal{T}$ tel que $\sigma(\alpha) = \alpha$. Le théorème 1.17 implique

$$\sum_{i=0}^{m-1} \mu_i p^i = \sum_{i=0}^{m-1} \mu_i^p p^i \ .$$

Comme $\mu_i^p \in \mathcal{T}$ et qu'il y a unicité de la forme multiplicative, il en résulte l'égalité $\mu_i = \mu_i^p$ pour tout i dans $[0, m-1]$. Si μ_i est non nul, alors μ_i est dans $\mathcal{T}^*$ et son ordre divise $p-1$. Or il y a au plus $p-1$ éléments dans ce cas. Il y a donc au plus p éléments $\mu \in \mathcal{T}$ vérifiant $\mu = \mu^p$ et par conséquent au plus p^m éléments $\alpha \in \mathrm{GR}(p^k, m)$ tels que $\sigma(\alpha) = \alpha$. Or nous savons déjà que tous les éléments de $\mathbb{Z}_{p^k}$ conviennent (cf. théorème 1.17). Ce sont donc les seuls. □

L'importance de l'application Tr vient du fait qu'elle permet de représenter simplement toutes les formes linéaires :

THÉORÈME 1.20 *Toute application possédant les 3 propriétés ci-dessus,* i.e. *toute forme linéaire du* $\mathbb{Z}_{p^k}$*-module* $\mathrm{GR}(p^k, m)$ *est de la forme* $\beta \mapsto \mathrm{Tr}(\alpha\beta)$ *pour un certain* $\alpha \in \mathrm{GR}(p^k, m)$.

PREUVE. L'anneau $\mathrm{GR}(p^k, m)$ est un $\mathbb{Z}_{p^k}$-module libre de dimension m. En effet, d'après la proposition 1.13, les éléments $1, x, \ldots, x^{m-1}$ sont linéairement indépendants et générateurs. Donc (cf. [Hun80]), l'ensemble de ses formes linéaires est également un $\mathbb{Z}_{p^k}$-module de dimension m. Ainsi, il suffit de trouver une famille libre de m éléments de la forme $\beta \mapsto \mathrm{Tr}(\alpha\beta)$. Prouvons que la famille

$$\left\{ \beta \mapsto \mathrm{Tr}(x^i\beta) \;\middle|\; i \in [0, m-1] \right\}$$

est libre. Posons $T = \left(\mathrm{Tr}(x^i x^j)\right)_{0 \le i,j \le m-1}$, alors

$$\mathrm{Tr}(\alpha\beta) = (a_0, \ldots, a_{m-1}) \cdot T \cdot {}^t(b_0, \ldots, b_{m-1}) \ ,$$

où $\alpha = \sum_{i=0}^{m-1} a_i x^i$ et $\beta = \sum_{i=0}^{m-1} b_i x^i$. Donc on a

$$\begin{aligned} \sum_{i=0}^{m-1} a_i \mathrm{Tr}(x^i\beta) &= \mathrm{Tr}\left(\sum_{i=0}^{m-1} a_i x^i \beta \right) \\ &= \mathrm{Tr}(\alpha\beta) \\ &= (a_0, \ldots, a_{m-1}) \cdot T \cdot {}^t(b_0, \ldots, b_{m-1}) \ . \end{aligned}$$

Ainsi, prouver que la famille considérée est libre revient à prouver que la matrice T est inversible, *i.e.* que $\det(T)$ est inversible. Pour cela, posons $S = \left(\sigma^j(x^i)\right)_{0 \le i,j \le m-1}$. On a alors $T = S \cdot {}^t S$. En effet

$$\begin{aligned} \left(S \cdot {}^t S\right)_{i,j} &= \sum_{k=0}^{m-1} \sigma^k(x^i)\sigma^k(x^j) \\ &= \sum_{k=0}^{m-1} \left(\sigma^k(x^i x^j)\right) \\ &= \mathrm{Tr}(x^i x^j) \ , \end{aligned}$$

car σ^k est dans $\mathcal{A}(p^k, m)$ d'après le théorème 1.17. Or il résulte du lemme 1.18 que $\det(S)$ est inversible : dans le cas contraire, S serait non inversible, *i.e.* il existerait $(\gamma_0, \ldots, \gamma_{m-1}) \in \mathrm{GR}(p^k, m)^m$ non nul tel que

$$(\gamma_0, \ldots, \gamma_{m-1}) \cdot S = 0 \ ,$$

ce qui équivaut à

$$\gamma_0 x^i + \gamma_1 \sigma(x^i) + \cdots + \gamma_{m-1}\sigma^{m-1}(x^i) = 0$$

pour $i \in [0, m-1]$. Donc on aurait

$$\gamma_0 \mathrm{Id} + \gamma_1 \sigma + \cdots + \gamma_{m-1}\sigma^{m-1} = 0 \ ,$$

puisque tout élément de $GR(p^k, m)$ s'écrit de façon unique comme combinaison linéaire sur $\mathbb{Z}_{p^k}$ de $1, x, \ldots, x^{m-1}$. Or, d'après la proposition 1.18 page 28, les σ^i, pour $i \in [0, m-1]$, sont linéairement indépendants. Il y aurait donc une contradiction. Ainsi, on a prouvé que $\det(S \cdot {}^tS) = \det(S)^2$ est inversible, d'où le résultat énoncé. □

Nous terminons cette section par une caractérisation des sous-anneaux de Galois d'un anneau de Galois.

THÉORÈME 1.21 *Posons* $R = GR(p^k, m)$. *Si* A *est un sous-anneau de Galois de* R *alors il est isomorphe à* $GR(p^k, l)$ *où* l *est un diviseur de* m. *Réciproquement, pour tout entier* l *diviseur de* m, R *admet un et un seul sous-anneau isomorphe à* $GR(p^k, l)$.

PREUVE. Soit $A \simeq GR(p^k, l)$ un sous-anneau de R. On a $A/(p) \simeq \mathbb{F}_{p^l}$ qui est un sous-corps de $R/(p) \simeq \mathbb{F}_{p^m}$, et cela implique bien que l est un diviseur de m. Réciproquement, soit l un diviseur de m. Le corps $R/(p) \simeq \mathbb{F}_{p^m}$ a un élément d'ordre p^l. Donc il existe $\zeta \in \mathcal{T}^*$ tel que $\chi(\zeta)$ engendre ${\mathbb{F}_{p^l}}^*$. On vérifie facilement que $\mathbb{Z}_{p^k}[\zeta]$ est isomorphe à $GR(p^k, l)$. De plus, si A est un sous-anneau de R isomorphe à $GR(p^k, l)$, alors $A/(p)$ est le corps $\mathbb{F}_{p^l}$, ce qui implique qu'il existe $\alpha \in GR(p^k, m)$ tel que $\zeta + p \cdot \alpha$ soit un élément de A. Or

$$\begin{aligned}(\zeta + p \cdot \alpha)^{p^{km}} &= \sum_{i=0}^{p^{km}} \binom{p^{km}}{i} p^i \alpha^i \zeta^{p^{km}-i} \\ &= \zeta^{p^{km}}\end{aligned}$$

car p^k divise $\binom{p^{km}}{i} p^i$ pour tout $i > 0$. Mais ζ étant dans $\mathcal{T}^*$, nous avons $\zeta^{p^{km}} = \zeta$, et par conséquent ζ est un élément de A. Il en résulte l'inclusion $\mathbb{Z}_{p^k}[\zeta] \subset A$ et les deux anneaux ayant des cardinaux identiques, on en déduit $\mathbb{Z}_{p^k}[\zeta] = A$. □

Nous allons maintenant utiliser ces objets pour construire et étudier des codes sur l'anneau $\mathbb{Z}_{p^k}$ des entiers modulo une puissance d'un nombre premier.

Chapitre 2

Codes sur l'anneau $\mathbb{Z}_{p^k}$

L'étude de codes ayant pour alphabet un anneau quotient d'entiers n'est certes pas aussi récente qu'il pourrait sembler puisque Blake, Shankar et Spiegel s'y sont intéressés au cours des années 1970, respectivement dans [Bla72, Bla75], [Sha79] et [Spi77, Spi78]. Mais c'est beaucoup plus récemment que ces codes ont fait l'objet d'un important travail de recherche, le point de départ ayant été [HKC+94]. En d'autres termes, la notion de $\mathbb{Z}_4$-linéarité a été une motivation importante dans l'entreprise de cette étude. En fait, de manière plus générale, la théorie des codes sur les anneaux (notamment galoisiens) a profité de ce résultat.

Nous présenterons en détail dans le chapitre suivant la notion de $\mathbb{Z}_{p^k}$-linéarité, mais disons simplement ici que cette notion utilise des codes définis sur l'anneau $\mathbb{Z}_{p^k}$ des entiers modulo une puissance (d'exposant supérieur ou égal à deux) d'un nombre premier. La raison d'être de ce chapitre est donc de donner quelques propriétés de ces codes qui nous seront utiles par la suite, les deux points fondamentaux étant l'existence d'une identité de MacWilliams (qui est l'une des raisons de l'existence du phénomène de dualité formelle) et la structure des codes cycliques sur $\mathbb{Z}_{p^k}$. Nous donnons également la représentation des codes cycliques à l'aide de la fonction trace, ce dont nous nous servirons dans le chapitre 4.

2.1 Codes linéaires sur $\mathbb{Z}_{p^k}$

Définition 2.1 (Code linéaire sur $\mathbb{Z}_{p^k}$) *Un code linéaire de longueur n sur $\mathbb{Z}_{p^k}$ est un sous-module de $\mathbb{Z}_{p^k}{}^n$.*

Contrairement aux espaces vectoriels, les modules n'admettent pas, en général, de base. Ils possèdent toutefois une famille génératrice et donc une matrice génératrice, mais la décomposition des éléments sur cette famille n'est plus nécessairement unique.

Définition 2.2 (Matrice génératrice) *On appelle matrice génératrice d'un code linéaire sur $\mathbb{Z}_{p^k}$ toute matrice de $\mathcal{M}(\mathbb{Z}_{p^k})$ dont les lignes forment une famille génératrice minimale du code.*

Cette matrice peut se mettre sous une forme particulière, si on s'autorise à modifier légèrement le code.

Définition 2.3 (Codes équivalents) *Soient $\mathbf{C}_{p^k}$ et $\mathbf{C}'_{p^k}$ deux codes linéaires sur $\mathbb{Z}_{p^k}$ de matrices génératrices G et G' respectivement. Les codes $\mathbf{C}_{p^k}$ et $\mathbf{C}'_{p^k}$ sont dit équivalents s'il existe une matrice de permutation P telle que*

$$G' = G \cdot P \ .$$

Théorème 2.4 ([CS95, §2]) *Soit $\mathbf{C}_{p^k}$, un code linéaire sur $\mathbb{Z}_{p^k}$. À une permutation des coordonnées près, $\mathbf{C}_{p^k}$ admet une matrice génératrice dite de forme normale*

$$G = \begin{pmatrix} I_{\ell_0} & A_{0,1} & \cdots & \cdots & A_{0,k} \\ 0 & p \cdot I_{\ell_1} & p \cdot A_{1,2} & \cdots & p \cdot A_{1,k} \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & p^{k-1} \cdot I_{\ell_{k-1}} & p^{k-1} \cdot A_{k-1,k} \end{pmatrix} ,$$

où les $A_{i,j}$ sont des matrices $\ell_i \times \ell_j$ à coefficients dans $\{0, \ldots, p-1\} \subset \mathbb{Z}_{p^k}$ et I_{ℓ_i} est la matrice identité de taille ℓ_i. En particulier, le code $\mathbf{C}_{p^k}$ a $\prod_{i=0}^{k-1} p^{(k-i)\,\ell_i}$ éléments.

On définit le produit scalaire sur ${\mathbb{Z}_{p^k}}^n$ par

$$\mathbf{a} \cdot \mathbf{b} = \sum_{i=0}^{n-1} a_i b_i \ ,$$

les opérations étant effectuées dans $\mathbb{Z}_{p^k}$. Ce produit scalaire permet de définir une notion de dualité sur $\mathbb{Z}_{p^k}$.

Définition 2.5 (Code dual sur $\mathbb{Z}_{p^k}$) *Soit $\mathbf{C}_{p^k}$ un code linéaire sur $\mathbb{Z}_{p^k}$, on appelle code dual du code $\mathbf{C}_{p^k}$, et on note $\mathbf{C}^{\perp}_{p^k}$, le sous-module de ${\mathbb{Z}_{p^k}}^n$ défini par*

$$\mathbf{C}^{\perp}_{p^k} = \left\{ \mathbf{a} \;\middle|\; \forall \mathbf{b} \in \mathbf{C}_{p^k}, \quad \mathbf{a} \cdot \mathbf{b} = 0 \right\} \ .$$

Lorsque la matrice génératrice du code $\mathbf{C}_{p^k}$ est sous forme normale, la matrice génératrice du code dual se met sous la forme

$$G^{\perp} = \begin{pmatrix} B_{0,0} & \cdots & \cdots & B_{0,k-1} & I_{\ell_k} \\ p \cdot B_{1,0} & \cdots & p \cdot B_{1,k-2} & p \cdot I_{\ell_{k-1}} & 0 \\ \vdots & \iddots & \iddots & \iddots & \vdots \\ p^{k-1} \cdot B_{k-1,0} & p^{k-1} \cdot I_{\ell_1} & 0 & \cdots & 0 \end{pmatrix} ,$$

où les $B_{i,j}$ sont de dimension $\ell_{k-i} \times \ell_j$ et à coefficients dans $\{0, \ldots, p-1\} \subset \mathbb{Z}_{p^k}$. Cela a la conséquence suivante :

PROPOSITION 2.6 ([CS95, §1]) *Avec les notations du théorème 2.4, le code* $\mathbf{C}_{p^k}^{\perp}$ *a* $\prod_{i=1}^{k} p^{i \cdot l_i}$ *éléments.*

La notion de dualité pour des codes linéaires sur $\mathbb{Z}_{p^k}$ est proche de celle définie pour les codes linéaires (sur un corps fini). Entre autres :

PROPOSITION 2.7 ([CS95, §1]) *Soit* $\mathbf{C}_{p^k}$ *un code linéaire sur* $\mathbb{Z}_{p^k}$. *Le code dual de* $\mathbf{C}_{p^k}^{\perp}$ *est le code* $\mathbf{C}_{p^k}$ *lui-même.*

Autre similarité avec les codes linéaires sur un corps fini : les énumérateurs des poids complets sont liés par une identité de MacWilliams.

DÉFINITION 2.8 (POLYNÔME ÉNUMÉRATEUR DES POIDS COMPLETS) *Soit* $\mathbf{C}_{p^k}$ *un code linéaire de longueur* n *sur* $\mathbb{Z}_{p^k}$. *Notons* $X^{\mathbf{c}}$ *le monôme, appartenant à* $\mathbb{Z}_{p^k}[X_0, \ldots, X_{p^k-1}]$, *défini par*

$$X^{\mathbf{c}} = \prod_{a \in \mathbb{Z}_{p^k}} X_a^{n_a(\mathbf{c})} \ ,$$

où $n_a(\mathbf{c})$ *désigne le nombre de coordonnées de* $\mathbf{c}$ *égales à* a. *Le polynôme défini par*

$$CW_{\mathbf{C}_{p^k}}(X_0, \ldots, X_{p^k-1}) = \sum_{\mathbf{c} \in \mathbf{C}_{p^k}} X^{\mathbf{c}}$$

est appelé polynôme énumérateur des poids complets du code $\mathbf{C}_{p^k}$.

THÉORÈME 2.9 (IDENTITÉ DE MACWILLIAMS POUR $\mathbb{Z}_{p^k}$) *Soit* $\mathbf{C}_{p^k}$ *un code linéaire sur* $\mathbb{Z}_{p^k}$. *Soit* $\omega = e^{\frac{2i\pi}{p^k}}$, *posons pour tout entier* a

$$\mu_a(X_0, \ldots, X_{p^k-1}) = \sum_{\nu \in \mathbb{Z}_{p^k}} \omega^{\nu \cdot a} X_\nu \ .$$

Les polynômes énumérateurs des poids complets de $\mathbf{C}_{p^k}$ *et de* $\mathbf{C}_{p^k}^{\perp}$, *notés respectivement* $CW_{\mathbf{C}_{p^k}}$ *et* $CW_{\mathbf{C}_{p^k}^{\perp}}$, *vérifient*

$$CW_{\mathbf{C}_{p^k}^{\perp}}(X_0, \ldots, X_{p^k-1}) = \frac{1}{|\mathbf{C}_{p^k}|} CW_{\mathbf{C}_{p^k}}\left(\mu_0(X_0, \ldots, X_{p^k-1}), \ldots, \mu_{p^k-1}(X_0, \ldots, X_{p^k-1})\right) \ .$$

PREUVE. Nous allons prouver cette égalité à l'aide de la transformée de Hadamard. Soit f une fonction définie sur $\mathbb{Z}_{p^k}^n$ et prenant ses valeurs dans $\mathbb{Z}_{p^k}[X_0, \ldots, X_{p^k-1}]$. Sa transformée de Hadamard est par définition

$$\hat{f}(u) = \sum_{v \in \mathbb{Z}_{p^k}^n} \omega^{v \cdot u} f(v) \ .$$

La fonction f et sa transformée $\hat{f}$ vérifient l'égalité de Poisson :

$$\sum_{u \in \mathbf{C}_{p^k}^{\perp}} f(u) = \frac{1}{|\mathbf{C}_{p^k}|} \sum_{u \in \mathbf{C}_{p^k}} \hat{f}(u) \ .$$

En effet,

$$\begin{aligned} \sum_{u \in \mathbf{C}_{p^k}} \hat{f}(u) &= \sum_{u \in \mathbf{C}_{p^k}} \sum_{v \in \mathbb{Z}_{p^k}^n} \omega^{v \cdot u} f(v) \\ &= \sum_{v \in \mathbb{Z}_{p^k}^n} f(v) \sum_{u \in \mathbf{C}_{p^k}} \omega^{v \cdot u} \ . \end{aligned}$$

Or pour tout $v \in \mathbb{Z}_{p^k}^n$, l'application $\phi_v : u \in \mathbf{C}_{p^k} \mapsto u \cdot v$ est une forme linéaire, ce qui implique soit qu'elle est nulle – ce qui signifie par définition que $v \in \mathbf{C}_{p^k}^{\perp}$ – soit qu'elle prend chaque valeur de $\mathbb{Z}_{p^k}$ le même nombre de fois, à savoir $|\mathbf{C}_{p^k}|/|\mathbb{Z}_{p^k}|$. D'où

$$\sum_{u \in \mathbf{C}_{p^k}} \hat{f}(u) = \left(\sum_{v \in \mathbf{C}_{p^k}^{\perp}} f(v) \left| \mathbf{C}_{p^k} \right| \right) + \left(\sum_{v \notin \mathbf{C}_{p^k}^{\perp}} f(v) \frac{|\mathbf{C}_{p^k}|}{p^k} \sum_{a \in \mathbb{Z}_{p^k}} \omega^a \right) \ .$$

Enfin, ω étant une racine primitive p^k-ième de l'unité, la somme $\sum \omega^a$ est nulle et on obtient bien l'égalité de Poisson. Nous allons utiliser cette égalité pour la fonction

$$\begin{aligned} f(\mathbf{c}) &= X^{\mathbf{c}} \\ &= \prod_{i=0}^{n-1} X_{\mathbf{c}_i} = \prod_{a=0}^{p^k-1} X_a^{n_a(\mathbf{c})} \ . \end{aligned}$$

Cette fonction représente la contribution du mot $\mathbf{c}$ à l'énumérateur des poids d'un code contenant $\mathbf{c}$. Soit $CW(X) = \sum_{\mathbf{c} \in \mathbf{C}_{p^k}} f(\mathbf{c})$. Sa transformée de Ha-

damard s'écrit

$$\begin{aligned}
\widehat{f}(\mathbf{c}) &= \sum_{\mathbf{v}\in\mathbb{Z}_{p^k}^n} \omega^{\mathbf{v}\cdot\mathbf{c}} f(\mathbf{v}) \ , \\
&= \sum_{\mathbf{v}\in\mathbb{Z}_{p^k}^n} \prod_{i=0}^{n-1} \omega^{\mathbf{v}_i\cdot\mathbf{c}_i} X_{\mathbf{v}_i} \ , \\
&= \prod_{i=0}^{n-1} \sum_{\nu\in\mathbb{Z}_{p^k}} \omega^{\nu\cdot\mathbf{c}_i} X_\nu \ , \\
&= \prod_{a=0}^{p^k-1} \left(\sum_{\nu\in\mathbb{Z}_{p^k}} \omega^{\nu\cdot a} X_\nu \right)^{n_a(\mathbf{c})} \ .
\end{aligned}$$

Donc, $\widehat{f}$ est obtenue à partir de f par la transformation $X_i \mapsto \mu_i(X_0, \ldots, X_{p^k-1})$. Il suffit alors d'appliquer la formule de Poisson pour obtenir l'égalité de Mac-Williams. □

Cette identité se simplifie considérablement pour les énumérateurs des poids de Hamming. L'énumérateur des poids de Hamming, noté HW, s'obtient à partir de CW par

$$HW_{\mathbf{C}_{p^k}}(X, Y) = CW_{\mathbf{C}_{p^k}}(X, Y, \ldots, Y) \ .$$

Cela conduit à la relation suivante :

THÉORÈME 2.10 *Soit $\mathbf{C}_{p^k}$ un code linéaire sur $\mathbb{Z}_{p^k}$. Alors l'énumérateur des poids de Hamming de $\mathbf{C}_{p^k}$ et de son dual sont liés par*

$$HW_{\mathbf{C}_{p^k}^\perp}(X, Y) = \frac{1}{|\mathbf{C}_{p^k}|} HW_{\mathbf{C}_{p^k}}(X + (p^k - 1)\cdot Y, X - Y) \ .$$

PREUVE. On a

$$HW_{\mathbf{C}_{p^k}^\perp}(X, Y) = CW_{\mathbf{C}_{p^k}^\perp}(X, Y, \ldots, Y) \ .$$

Or

$$\mu_a(X, Y, \ldots, Y) = X + \sum_{\nu=1}^{p^k-1} \omega^{\nu\cdot a} Y \ .$$

Comme ω est une racine p^k-ième de l'unité, on a

$$\sum_{\nu=0}^{p^k-1} (\omega^a)^\nu = \begin{cases} p^k & \text{si } a = 0 \ , \\ 0 & \text{si } a \neq 0 \ , \end{cases}$$

ce qui donne

$$\mu_a(X, Y, \ldots, Y) = \begin{cases} X + (p^k - 1) \cdot Y & \text{si } a = 0 \ , \\ X - Y & \text{si } a \neq 0 \ . \end{cases}$$

Il suffit alors d'appliquer le théorème 2.9. □

2.2 Codes cycliques sur $\mathbb{Z}_{p^k}$

Dans toute cette section, on se restreint au cas où *la longueur* n *des codes est première avec* p.

Définition 2.11 (Code cyclique sur $\mathbb{Z}_{p^k}$) *Un code* $\mathbf{C}_{p^k}$ *de longueur* n *sur l'anneau* $\mathbb{Z}_{p^k}$ *est dit cyclique s'il est linéaire et s'il est invariant par l'application shift définie par*

$$s((a_0, \ldots, a_{n-1})) = (a_{n-1}, a_0, \ldots, a_{n-2}) \ .$$

Un code cyclique sur $\mathbb{Z}_{p^k}$ est donc le pendant exact d'un code cyclique sur $\mathbb{Z}_p$. Ainsi, l'application

$$\begin{array}{rccl} \phi: & \mathbb{Z}_{p^k}{}^n & \longrightarrow & \mathbb{Z}_{p^k}[X]/(X^n - 1) \\ & v = (v_0, \ldots, v_{n-1}) & \longmapsto & \phi(v) = \displaystyle\sum_{i=0}^{n-1} v_i X^i \end{array}$$

est un isomorphisme de modules sur $\mathbb{Z}_{p^k}$ qui envoie les codes cycliques sur $\mathbb{Z}_{p^k}$ sur les idéaux de l'anneau quotient $\mathbb{Z}_{p^k}[X]/(X^n - 1)$. On peut donc assimiler code cyclique sur $\mathbb{Z}_{p^k}$ et idéal de $\mathbb{Z}_{p^k}[X]/(X^n - 1)$. Dans toute la suite, nous noterons $\mathcal{R}$ cet anneau quotient. Comme dans le cas des corps finis, l'anneau $\mathcal{R} = \mathbb{Z}_{p^k}[X]/(X^n - 1)$ est principal. Toutefois, la structure de ses idéaux est plus complexe que celle de $\mathbb{F}_{p^k}[X]/(X^n - 1)$:

Théorème 2.12 (Idéaux de $\mathcal{R}$, [KL97, th. 3.4]) *Soit* $\mathcal{I}$ *un idéal de* $\mathcal{R} = \mathbb{Z}_{p^k}[X]/(X^n - 1)$. *Il existe une unique famille* $\{\widehat{f_i}\} \subset \mathbb{Z}_{p^k}[X]$ *de* $k+1$ *polynômes unitaires deux à deux premiers entre eux, vérifiant* $\widehat{f_0} \cdots \widehat{f_k} = X^n - 1$, *et telle que*

$$\mathcal{I} = \left(f_0,\, p \cdot f_1,\, p^2 \cdot f_2, \ldots,\, p^{k-1} \cdot f_{k-1}\right)$$

où les f_i *sont définies par* $f_i \cdot \widehat{f_i} = X^n - 1$. *D'autre part, l'élément*

$$g = f_0 + p \cdot f_1 + p^2 \cdot f_2 + \cdots + p^{k-1} \cdot f_{k-1}$$

est un générateur de $\mathcal{I}$ *et*

$$|\mathcal{I}| = \prod_{i=0}^{k-1} p^{(k-i)\deg(\widehat{f_i})} \ .$$

COROLLAIRE 2.13 *L'anneau $\mathcal{R}$ a $(k+1)^r$ idéaux distincts, où r désigne le nombre de facteurs irréductibles de X^n-1 dans $\mathbb{Z}_{p^k}[X]$.*

Les idéaux de $\mathcal{R}$, donc les codes cycliques sur $\mathbb{Z}_{p^k}$, étant principaux, il est tentant d'essayer de définir les zéros d'un code, comme pour le cas des corps finis. Autrement dit, de considérer un anneau de Galois dans lequel le polynôme générateur a toutes ses racines, et de nommer celles-ci zéros du code. Nous allons voir qu'avec nos hypothèses il est effectivement possible de considérer un tel anneau. Toutefois, l'existence de diviseurs de zéro rend la situation moins simple. Dans un corps, en dehors de ses racines, un polynôme prend des valeurs inversibles, et par conséquent toutes les contraintes sur les mots du code sont imposées par les zéros du polynôme générateur : les mots du codes sont les multiples du générateur et cela équivaut a considérer qu'un mot est dans le code s'il s'annule sur tous les zéros du générateur. Aucune contrainte n'existe sur les valeurs prises par les mots du code en dehors de ces zéros. Dans notre cas, un polynôme g peut ne pas s'annuler sur un élément β mais prendre pour valeur un élément de la forme $p\cdot\alpha$. Cela implique que les multiples de g ne peuvent pas prendre n'importe quelle valeur en β : si g prend une valeur non inversible, il en sera de même pour tous ces multiples. On est donc amené à considérer comme zéros des éléments n'annulant pas les mots de codes, mais donnant des diviseurs de zéro, et cela afin de pouvoir obtenir une caractérisation des mots de code en fonction des zéros.

Si on note m l'ordre de p modulo n, alors X^n-1 divise $X^{p^m}-1$ et les racines du polynôme X^n-1 sont dans l'anneau $GR(p^k,m)$. Plus précisément, ce sont des éléments de $\mathcal{T}^*$ (cf. lemme 1.15 et proposition 1.16). Les racines des polynômes $\widehat{f_k}$ définis dans le théorème précédent sont donc dans $\mathcal{T}^*$.

DÉFINITION 2.14 *Soit $\mathbf{C}_{p^k}$ un code cyclique de longueur n sur $\mathbb{Z}_{p^k}$. Pour $i\in[0,k-1]$, on note $\mathcal{Z}(i)$ l'ensemble des racines du polynôme $\widehat{f_{k-i}}$. La famille $\mathcal{Z}=\{\mathcal{Z}(0),\dots,\mathcal{Z}(k-1)\}$ est appelée la famille de zéros du code $\mathbf{C}_{p^k}$. Par convention, nous noterons $\mathcal{Z}(k)$ l'ensemble des racines de $\widehat{f_0}$.*

À partir du théorème 2.12, il est facile de voir que, pour tout $\alpha\in\mathcal{Z}(i)$, on a

$$g(\alpha)\in p^{k-i}\mathbb{Z}_{p^k} \text{ et } g(\alpha)\notin p^{k-i+1}\mathbb{Z}_{p^k} \ ,$$

où g est le polynôme générateur défini dans le théorème 2.12. Remarquons que sur $\mathcal{Z}(k)$ le polynôme g ne s'annule pas et ne prend que des valeurs inversibles. Inversement, g est nul en tout point de $\mathcal{Z}(0)$. Lorsque i est strictement compris entre 0 et k, g prend des valeurs parmi les éléments non inversibles, mais non nuls.

Nous allons essentiellement nous intéresser aux idéaux pour lesquels

$$\widehat{f_1}=\widehat{f_2}=\cdots=\widehat{f_{k-1}}=1 \ .$$

Cet intérêt provient du fait que ces idéaux s'obtiennent par relèvement de Hensel des codes cycliques sur $\mathbb{Z}_p$. En effet, le générateur $g(X)$ de tout code cyclique sur $\mathbb{Z}_p$ est un diviseur unitaire de X^n-1 dans $\mathbb{Z}_p[X]$, sans facteur multiple puisque p ne divise pas n. On peut donc lui appliquer le relèvement de Hensel. On obtient ainsi un diviseur (unitaire) $g^{(k)}(X)$ de X^n-1 dans $\mathbb{Z}_{p^k}[X]$ et, d'après le théorème 2.12, un générateur d'un idéal pour lequel $f_0 = g^{(k)}$ et $f_1 = \cdots = f_{k-1} = X^n - 1 \in \mathbb{Z}_{p^k}[X]$.

DÉFINITION 2.15 *Soient* $g(X) \in \mathbb{Z}_p[X]$ *un diviseur de* X^n-1 *et* $g^{(k)}(X) \in \mathbb{Z}_{p^k}(X)$ *son relevé de Hensel d'ordre* k. *Le code* $\mathbf{C}_{p^k} = \left(g^{(k)}(X)\right) \subset \mathcal{R}$ *est appelé le code relevé du code cyclique* $\mathbf{C} = (g(X)) \subset \mathbb{Z}_p[X]/(X^n-1)$. *Le polynôme* $g^{(k)}(X)$ *est appelé* le *générateur du code* $\mathbf{C}_{p^k}$.

Dans ce cas, les zéros du codes sont tous dans $\mathcal{Z}(0)$, et ils sont au nombre de $\deg(g^{(k)})$.

PROPOSITION 2.16 *Soit* $g^{(k)} \in \mathbb{Z}_{p^k}[X]$ *un polynôme unitaire divisant* X^n-1. *La famille*

$$\left\{g^{(k)}(X), Xg^{(k)}(X), \ldots, X^{n-d-1}g^{(k)}(X)\right\}$$

est génératrice du code $\mathbf{C}_{p^k} = (g^{(k)}) \in \mathcal{R}$ *et linéairement indépendante sur* $\mathbb{Z}_{p^k}$, i.e. *c'est une base de* $\mathbf{C}_{p^k}$.

PREUVE. Clairement, tous les éléments de l'idéal $(g^{(k)})$ s'écrivent sous la forme de combinaisons linéaires sur $\mathbb{Z}_{p^k}$ des éléments de la famille considérée. Montrons qu'elle est linéairement indépendante sur $\mathbb{Z}_{p^k}$. Posons

$$g^{(k)}(X)h^{(k)}(X) = X^n - 1$$

et supposons l'existence d'un $(n-d)$-uplet $(a_i) \in \mathbb{Z}_{p^k}^{n-d}$ tel que

$$\sum_{i=0}^{n-d-1} a_i X^i g^{(k)}(X) = 0 \in \mathcal{R} \ .$$

Alors $A(X) = \sum_i a_i X^i$ est un multiple de $h^{(k)}$, or $\deg(h^{(k)}) = n-d$ et $\deg(A) \leq n-d-1$. Donc $A(X) = 0$, c'est-à-dire $(a_i) = 0$. Les coefficients de toutes combinaisons linéaires valant zéro sont nécessairement nuls et par conséquent la famille est libre. □

COROLLAIRE 2.17 *Posons* $g^{(k)} = \sum_{i=0}^{d} g_i^{(k)} X^i$. *La matrice*

$$G = \begin{pmatrix} g_0^{(k)} & g_1^{(k)} & \ldots & g_d^{(k)} & 0 & \ldots\ldots & 0 \\ 0 & g_0^{(k)} & g_1^{(k)} & \ldots & g_d^{(k)} & 0 & \ldots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & \ldots & 0 & g_0^{(k)} & g_1^{(k)} & \ldots & g_d^{(k)} & 0 \\ 0 & \ldots\ldots & & 0 & g_0^{(k)} & g_1^{(k)} & \ldots & g_d^{(k)} \end{pmatrix}$$

est une matrice génératrice (de dimension $n \times (n-d)$) du code $\mathbf{C}_{p^k} = (g^{(k)}) \in \mathcal{R}$, et $\mathbf{C}_{p^k}$ a $p^{k(n-d)}$ mots de code.

Soit $h^{(k)}$ le quotient de $X^n - 1$ par $g^{(k)}$. Pour tout mot de code $c(X)$, on a clairement $c(X)h^{(k)}(X) = 0 \in \mathcal{R}$.

DÉFINITION 2.18 (POLYNÔME DE CONTRÔLE) *Soit $g^{(k)} \in \mathbb{Z}_{p^k}[X]$ un polynôme unitaire diviseur $X^n - 1$. Le polynôme $h^{(k)}(X) = (X^n - 1)/g^{(k)}(X)$ est appelé polynôme de contrôle du code $\mathbf{C}_{p^k} = (g^{(k)})$.*

De même que pour les corps finis, le dual de $(g^{(k)})$ est cyclique. Le code dual est engendré par le polynôme réciproque de $h^{(k)}$ défini par

$$\begin{aligned}\widetilde{h^{(k)}}(X) &= \frac{1}{h_0} X^{n-d} h^{(k)}\left(X^{-1}\right) \ , \\ &= \frac{1}{h_0} \sum_{i=0}^{n-d} h^{(k)}_{n-d-i} X^i \ ,\end{aligned}$$

où $h^{(k)}(X) = \sum_{i=0}^{n-d} h_i X^i$.

PROPOSITION 2.19 *Soient $\mathbf{C}_{p^k} = (g^{(k)}) \subset \mathcal{R}$ un code cyclique et $h^{(k)}$ son polynôme de contrôle. Le code dual $\mathbf{C}^{\perp}_{p^k}$ est cyclique, engendré par le polynôme réciproque de $h^{(k)}$. Par conséquent, la matrice*

$$G^{\perp} = \begin{pmatrix} h^{(k)}_{n-d} & h^{(k)}_{n-d-1} & \cdots\cdots & h^{(k)}_0 & 0 & \cdots\cdots\cdots\cdots & 0 \\ 0 & h^{(k)}_{n-d} & h^{(k)}_{n-d-1} & \cdots\cdots & h^{(k)}_0 & 0 & \cdots \ 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots \ \vdots \\ 0 & \cdots\cdots & 0 & h^{(k)}_{n-d} & h^{(k)}_{n-d-1} & \cdots\cdots & h^{(k)}_0 \ 0 \\ 0 & \cdots\cdots\cdots\cdots & & 0 & h^{(k)}_{n-d} & h^{(k)}_{n-d-1} & \cdots \ h^{(k)}_0 \end{pmatrix}$$

est une matrice génératrice (de dimension $n \times d$) du code dual $\mathbf{C}^{\perp}_{p^k}$ et ce dernier a pour cardinal $|\mathbf{C}^{\perp}_{p^k}| = p^{kd}$.

PREUVE. La preuve de l'égalité $\mathbf{C}^{\perp}_{p^k} = (\widetilde{h^{(k)}})$ est semblable à celle qu'on peut donner pour les corps finis (cf. [MS96, chap. 7 §4, th. 4]). Il suffit ensuite d'appliquer le corollaire 2.17. □

Nous avons choisi de singulariser le générateur unitaire divisant $X^n - 1$ lorsque cela est possible, mais il existe un autre type de générateur possédant des propriétés intéressantes dans les codes engendrés par un diviseur de $X^n - 1$: les idempotents.

DÉFINITION 2.20 (IDEMPOTENT) *Soit* $e(X) \in \mathbb{Z}_{p^k}[X]$. *Le polynôme* e *est un idempotent de* $\mathcal{R}$ *si on a*

$$e^2(X) \equiv e(X) \pmod{X^n - 1} \ .$$

THÉORÈME 2.21 (IDEMPOTENT GÉNÉRATEUR) *Soit* $g^{(k)}$ *un diviseur unitaire de* $X^n - 1$. *Le code cyclique* $\mathbf{C}_{p^k} = (g^{(k)}) \subset \mathcal{R}$ *admet un unique idempotent générateur* $e(X)$. *De plus, tout mot* $c(X) \in \mathbf{C}_{p^k}$ *est caractérisé par l'égalité*

$$c(X)e(X) \equiv c(X) \pmod{X^n - 1} \ . \qquad (*)$$

PREUVE. Soit $h^{(k)}$ le polynôme de contrôle de $\mathbf{C}_{p^k}$. Les polynômes $g^{(k)}$ et $h^{(k)}$ étant premiers entre eux, il existe un couple $(u(X), v(X)) \in (\mathbb{Z}_{p^k}[X])^2$ tel que

$$g^{(k)}(X)u(X) + h^{(k)}(X)v(X) = 1 \ .$$

Posons $e(X) = g^{(k)}(X)u(X)$. Alors

$$e(X) = 1 - h^{(k)}(X)v(X)$$

et

$$\begin{aligned} e^2(X) &= e(X) - e(X)h^{(k)}(X)v(X) \\ &= e(X) - g^{(k)}(X)h^{(k)}(X)u(X)v(X) \\ &\equiv e(X) \pmod{X^n - 1} \ . \end{aligned}$$

Ainsi, $e(X)$ est bien un idempotent. D'autre part, on a

$$\begin{aligned} g^{(k)}(X)e(X) &= g^{(k)}(X) - g^{(k)}(X)h^{(k)}(X)v(X) \\ &\equiv g^{(k)}(X) \pmod{X^n - 1} \ . \end{aligned}$$

Cela implique l'inclusion $(g^{(k)}) \subset (e)$. L'inclusion inverse résulte directement de la définition de e comme étant égal au produit $g^{(k)}(X)u(X)$. D'où $\mathbf{C}_{p^k} = (g^{(k)}) = (e)$, *i.e.* e est un générateur du code $\mathbf{C}_{p^k}$. La relation (*) signifie que e est un élément neutre pour le groupe $(g^{(k)})$ muni de la multiplication ; cette loi étant commutative, il est nécessairement unique. Terminons la preuve en démontrant la dernière assertion du théorème qui est une simple conséquence des résultats que nous venons d'obtenir. Soit $c(X) \in \mathbb{Z}_{p^k}$ vérifiant $c(X) \equiv c(X)e(X) \pmod{X^n - 1}$. Clairement $c(X) \in (e(X)) = \mathbf{C}_{p^k}$. Réciproquement, soit $c(X) \in \mathbf{C}_{p^k}$, alors $c(X) \equiv b(X)e(X) \pmod{X^n - 1}$ pour un certain $b(X) \in \mathbb{Z}_{p^k}[X]$. Or

$$\begin{aligned} c(X)e(X) &\equiv b(X)e^2(X) \pmod{X^n - 1} \\ &\equiv b(X)e(X) \pmod{X^n - 1} \\ &\equiv c(X) \pmod{X^n - 1} \ , \end{aligned}$$

ce qui conclut la preuve. □

EXEMPLE 2.22 Le polynôme $g^{(3)}(X) = 7 + 5X + 6X^2 + X^3$ divise $X^7 - 1$ dans $\mathbb{Z}_8[X]$ (voir l'exemple 1.7 page 18), donc $(g^{(3)})$ admet un idempotent générateur $e(X)$. Notons $h^{(3)}$ le polynôme de contrôle correspondant à $g^{(3)}$. On a

$$(2X^3 + 6X^2 + 7X + 4)g^{(3)}(X) + (6X^2 + 2X + 5)h^{(3)}(X) = 1 \ .$$

Nous avons calculé cette relation par l'algorithme 15.10 de [GG99] à l'aide du logiciel MAGMA. D'après la preuve du théorème ci-dessus,

$$\begin{aligned} e(X) &= (2X^3 + 6X^2 + 7X + 4)g^{(3)}(X) \\ &= 2X^6 + 2X^5 + 5X^4 + 2X^3 + 5X^2 + 5X + 4 \ . \end{aligned}$$

On a

$$\begin{aligned} e^2(X) &= 4X^{12} + 4X^9 + 5X^8 + 4X^7 + 2X^6 + 6X^5 + 5X^4 + 2X^3 + X^2 \\ &\equiv 2X^6 + 2X^5 + 5X^4 + 2X^3 + 5X^2 + 5X + 4 \pmod{X^7 - 1} \\ &\equiv e(X) \pmod{X^7 - 1} \ . \end{aligned}$$

Vérifions que le produit par $e(X)$ laisse les mots du code invariants :

$$\begin{aligned} g^{(3)}(X)e(X) &= 2X^9 + 6X^8 + 3X^7 + X^3 + 4X^2 + 7X + 4 \\ &\equiv X^3 + 6X^2 + 5X + 7 \equiv g^{(3)}(X) \pmod{X^7 - 1} \ . \end{aligned}$$

Tout mot du code s'exprimant comme un multiple de $g^{(3)}(X)$ et ce dernier étant invariant par produit par $e(X)$, on a bien que $e(X)$ est un générateur de $(g^{(3)})$. □

Le générateur idempotent est en fait un élément neutre pour la multiplication dans le code $\mathbf{C}_{p^k}$, *i.e.* non seulement $\mathbf{C}_{p^k}$ est un idéal, mais c'est anneau (attention, ce n'est pas un sous-anneau de $\mathcal{R}$ puisque les éléments neutres sont différents). Les idempotents générateurs ont plusieurs intérêts. Par exemple, d'un point de vue algorithmique, ils permettent de tester l'appartenance d'un mot au code par une simple multiplication dans $\mathcal{R}$ plutôt que par une division, ce qui est plus rapide (cf. §9.7 de [GG99]). Sur un plan plus théorique, Pless et Qian dans [PQ96] utilisent les idempotents pour énumérer l'ensemble des codes cycliques de longueur 7 sur $\mathbb{Z}_4$. Pour des exemples de l'utilisation des idempotents dans le cas des corps finis, nous renvoyons au chapitre 8 de [MS96].

2.3 Polynôme de Mattson-Solomon

Un outil classique pour étudier les propriétés d'un code cyclique sur un corps fini est la transformée de Fourier discrète des mots de code, qu'il est

d'usage, en théorie des codes, de représenter sous la forme du polynôme de Mattson-Solomon. Les résultats exposés dans cette section, que nous avons retrouvés indépendamment, sont présentés dans un cadre légèrement plus général dans [RS94a] – l'anneau est $\mathbb{Z}_m$, où m est un entier quelconque – mais sans introduire le polynôme de Mattson-Solomon. Ces résultats sont étendus aux codes abéliens sur $\mathbb{Z}_m$, qui étendent les codes cycliques, dans [RS94b], toujours sans mention du polynôme de Mattson-Solomon. Blackford et Ray-Chaudhuri, dans [BR00], utilisent une approche fondée sur le polynôme de Mattson-Solomon et valable pour les codes cycliques sur l'anneau $\mathrm{GR}(p^k, m)$. Dans notre cas, nous nous intéressons au codes cycliques sur $\mathbb{Z}_{p^k}$ et nous utilisons la définition suivante :

DÉFINITION 2.23 (POLYNÔME DE MATTSON-SOLOMON) *Soient n un entier premier avec p, et $\mathbf{c}$ un mot de ${\mathbb{Z}_{p^k}}^n$. On note m l'ordre de p modulo n. Soit ζ un élément d'ordre n dans $\mathcal{T}^* \subset \mathrm{GR}(p^k, m)$. On appelle polynôme de Mattson-Solomon du mot $\mathbf{c}$ le polynôme défini par*

$$M_{\mathbf{c}}(X) = \sum_{j=0}^{n-1} M_j X^j \ ,$$

où

$$M_j = \sum_{i=0}^{n-1} c_i \cdot \left(\zeta^{n-j}\right)^i \ .$$

Le coefficient de X^j, M_j, est donc simplement l'évaluation du mot $\mathbf{c}$, vu comme un élément de $\mathbb{Z}_{p^k}[X]$, en ζ^{n-j}, donc en ζ^{-j} puisque ζ est une racine n-ième de l'unité. De façon usuelle pour ce type de transformation, il existe une transformation inverse :

$$\begin{aligned} M_{\mathbf{c}}(\zeta^j) &= \sum_{i=0}^{n} \mathbf{c}\left(\zeta^{n-i}\right) \cdot \left(\zeta^j\right)^i \ , \\ &= \sum_{i=0}^{n} \sum_{l=0}^{n} c_l \left(\zeta^{n-i}\right)^l \left(\zeta^j\right)^i \ , \\ &= \sum_{l=0}^{n} c_l \sum_{i=0}^{n} \zeta^{i(j-l)} \ , \\ &= n \cdot c_j \ , \end{aligned}$$

puisque pour $j \neq l$, ζ^{j-l} est une racine n-ième de l'unité différente de 1, ce qui implique $\sum_i \zeta^{i(j-l)} = 0$. Si la longueur n est première avec p, n est inversible et on peut écrire

$$\mathbf{c} = n^{-1}\left(M_{\mathbf{c}}\left(\zeta^0\right), \ldots, M_{\mathbf{c}}\left(\zeta^{n-1}\right)\right) \ .$$

Cependant, la transformation qui, à un mot de $\mathbb{Z}_{p^k}^n$, associe son polynôme de Mattson-Solomon n'est pas une surjection de $\mathbb{Z}_{p^k}^n$ dans le sous anneau de $GR(p^k, m)[X]$ des polynômes dont le degré est au plus $n-1$ – il suffit de comparer les cardinaux. En fait, quel que soit le mot $\mathbf{c}$, le coefficient M_j est un élément de $\mathbb{Z}_{p^k}[\zeta^{-j}]$. Or ζ^{-j} est racine d'un certain facteur irréductible $P \in \mathbb{Z}_{p^k}[X]$ de X^n-1. Notons m_j le degré de P. Le polynôme P est irréductible de degré m_j. Nous avons donc

$$\mathbb{Z}_{p^k}[\zeta^{-j}] \simeq \mathbb{Z}_{p^k}[X]/(P) \simeq GR(p^k, m_j) \ .$$

Le coefficient M_j ne peut donc pas prendre n'importe quelle valeur dans $GR(p^k, m)$, mais est restreint au sous-anneau $GR(p^k, m_j)$.

D'autre part, en appliquant l'automorphisme de Frobenius aux M_j, on obtient

$$\sigma(M_j) = \mathbf{c}(\zeta^{-jp}) = M_{jp \bmod n}$$

puisque σ se réduit à l'identité sur $\mathbb{Z}_{p^k}$ et à l'élévation à la puissance p sur $\mathcal{T}$.

THÉORÈME 2.24 *Soient $\mathbf{C}_{p^k}$ un code cyclique de longueur n sur $\mathbb{Z}_{p^k}$ et $\mathbf{c}$ un mot de code. Les coefficients du polynôme de Mattson-Solomon de $\mathbf{c}$ vérifient*

1. $M_j \in GR(p^k, m_j)$;
2. $M_{jp \bmod n} = \sigma(M_j)$;
3. $\zeta^{-j} \in \mathcal{Z}(i) \Longrightarrow M_j \in p^{k-i}GR(p^k, m_j)$.

De plus, il y a bijection entre les mots du code et l'ensemble des polynômes de $GR(p^k, m)[X]$ de degré au plus $n-1$ vérifiant les trois conditions précédentes.

PREUVE. Nous avons déjà vu les conditions 1 et 2. Pour prouver la troisième, rappelons que nous avons $M_j = \mathbf{c}(\zeta^{-j})$. Or $\mathbf{c}$ est un multiple du polynôme générateur de $\mathbf{C}_{p^k}$, et si $\zeta^{-j} \in \mathcal{Z}(i)$ alors $g(\zeta^{-j}) \in p^{k-i}GR(p^k, m)$. En ajoutant la contrainte due à la première condition, on obtient bien l'implication énoncée.

Pour prouver le caractère bijectif, ayant déjà noté l'existence d'une transformation réciproque de $\mathbf{c} \mapsto M_{\mathbf{c}}$, nous avons l'injectivité. Par conséquent, il est suffisant de montrer que le cardinal de l'ensemble des polynômes satisfaisant les trois conditions du théorème est égal à celui du code.

La famille $\{\mathcal{Z}(i)\}$, $i \in [0, k]$, est une partition des racines n-ièmes de l'unité et on peut définir l'application z de $[0, n-1]$ dans $[0, n-1]$ qui, à j, associe l'entier $z(j)$ tel que $\zeta^{-j} \in \mathcal{Z}(z(j))$.

Par la deuxième condition, nous savons que tous les coefficients dont les indices appartiennent à une même classe cyclotomique de p modulo n sont uniquement déterminés dès que nous en connaissons un seul. Donc, si on note S une classe cyclotomique, et s son plus petit élément, $S = \{s, sp, \ldots, sp^{l}\} \subset$

$\mathbb{Z}_n$, connaître M_s permet d'obtenir tous les M_j pour $j \in S$. Mais, la troisième condition implique que M_s est dans $p^{k-z(s)}\mathrm{GR}(p^k, m_s)$. Le nombre de polynômes correspondant à ces conditions est donc

$$\prod_s \left| p^{k-z(s)}\mathrm{GR}(p^k, m_s) \right| = \prod_s p^{z(s)\cdot m_s}$$

où s parcourt un ensemble de représentants des classes cyclotomiques de p modulo n. Or m_s est le degré du facteur irréductible de $X^n - 1$ ayant ζ^{-s} comme racine. Donc, par la proposition 1.16, c'est également le cardinal de la classe de s. D'autre part, on a $z(s) = z(j)$ pour tout élément j dans la même classe que s. Cela permet donc d'écrire le cardinal recherché sous la forme

$$\begin{aligned}\prod_s p^{z(s)\cdot m_s} &= \prod_{j=0}^{n-1} p^{z(j)} \\ &= \prod_{i=0}^{k} p^{(n-i)|\mathcal{Z}(i)|} \\ &= \prod_{i=0}^{k} p^{(n-i)\deg \widehat{f_i}} \quad .\end{aligned}$$

Par le théorème 2.12, le cardinal du code $\mathbf{C}_{p^k}$ est $\prod_i (p^{n-i})^{|\mathcal{Z}(i)|}$, les deux cardinaux sont donc égaux, ce qui achève la preuve de la bijectivité. □

Nous allons maintenant utiliser le polynôme de Mattson-Solomon pour représenter les mots d'un code cyclique à l'aide d'applications faisant intervenir la fonction trace. Par définition du polynôme de Mattson-Solomon, on a $M(X) = \sum_{j=0}^{n-1} M_j X^j$, ce que l'on peut écrire en utilisant la deuxième propriété du théorème précédent

$$M(X) = \sum_s \mathrm{Tr}_{m_s}\left(M_s X^s\right) \quad ,$$

où s parcourt un ensemble de représentants des classes cyclotomiques de p modulo n, et avec Tr_{m_s} désignant la trace de $\mathrm{GR}(p^k, m_s)$, $\mathrm{Tr}_{m_s} = \mathrm{Id} + \sigma + \ldots + \sigma^{m_s-1}$. Dans cette expression, les M_s ne varient pas librement dans $\mathrm{GR}(p^k, m)$, mais dans un idéal de $\mathrm{GR}(p^k, m_s)$ dépendant des zéros du code. On peut la réécrire pour faire apparaître les racines n-ièmes n'appartenant pas à $\mathcal{Z}(0)$ – la troisième propriété du théorème 2.24 implique que les coefficients M_j correspondant aux éléments $\zeta^{-j} \in \mathcal{Z}(0)$ sont nuls.

Pour tout élément $\zeta^a \in \mathcal{Z}(i)$ on a $\sigma(\zeta^a) \in \mathcal{Z}(i)$. L'automorphisme de Frobenius σ permet donc de partitionner les $\mathcal{Z}(i)$ en classes d'équivalence.

Nous noterons $\mathcal{Z}_\ell(i)$ la réunion des classes incluses dans $\mathcal{Z}(i)$ dont le cardinal est égal à ℓ. Cela équivaut à dire que l'ensemble $\mathcal{Z}_\ell(i)$ contient tous les éléments de $\mathcal{Z}(i)$ dont le degré du polynôme minimal est ℓ. Donc l'ensemble $\mathcal{Z}_\ell(i)$ ne peut être non vide que lorsque ℓ divise m, où m est l'ordre de p modulo n. Nous noterons $\overline{\mathcal{Z}_\ell(i)}$ un système de représentants des logarithmes des éléments de cette union de classe. Autrement dit,

$$\mathcal{Z}_\ell(i) = \left\{ \zeta^{jp^a} \mid j \in \overline{\mathcal{Z}_\ell(i)}, a \in [0, m-1] \right\} \ .$$

On a alors

$$M(X) = \sum_{i=1}^{k} \sum_{\ell | m} \mathrm{Tr}_\ell \left(\sum_{s \in \overline{\mathcal{Z}_\ell(i)}} M_s X^s \right) \ ,$$

avec $M_s \in p^{k-i}\mathrm{GR}(p^k, \ell)$. Introduisons l'application d'évaluation π^* qui à une application f de $\mathrm{GR}(p^k, m)$ à valeurs dans $\mathbb{Z}_{p^k}$ associe le n-uplet

$$\pi^*(f) = \left(f(x^0), f(x), \ldots, f\left(x^{n-2}\right) \right) \ .$$

En utilisant la formule $M_{\mathbf{c}}(\zeta^j) = n^{-1} \cdot \mathbf{c}(\zeta^j)$, on peut décrire le code comme l'image par π^* des applications

$$\beta \mapsto \sum_{i=1}^{k} \sum_{\ell | m} \mathrm{Tr}_\ell \left(\sum_{s \in \overline{\mathcal{Z}_\ell(i)}} \lambda_s^{(\ell,i)} \beta^s \right) \ ,$$

où les $\lambda_s^{(\ell,i)}$ sont dans $p^{k-i}\mathrm{GR}(p^k, \ell)$.

Proposition 2.25 *Soit $\mathbf{C}_{p^k}$ un code cyclique de longueur n. Le code est l'image par l'application d'évaluation π^* de l'ensemble*

$$\left\{ \beta \mapsto \sum_{i=1}^{k} \sum_{\ell | m} \mathrm{Tr}_\ell \left(\sum_{s \in \overline{\mathcal{Z}_\ell(i)}} \lambda_s^{(\ell,i)} \beta^s \right) \ \middle| \ \lambda_s^{(\ell,i)} \in p^{k-i}\mathrm{GR}(p^k, \ell) \right\} \ .$$

Exemple 2.26 Rappelons (cf. Exemple 1.7) qu'on a sur $\mathbb{Z}_2[X]$

$$X^7 - 1 = (X+1)(X^3 + X + 1)(X^3 + X^2 + 1) \ ,$$

ce qui donne sur $\mathbb{Z}_8[X]$,

$$X^7 - 1 = (X+7)(X^3 + 6X^2 + 5X + 7)(X^3 + 3X^2 + 2X + 7) \ .$$

Posons $P(X) = X^3 + 6X^2 + 5X + 7$ et considérons le code cyclique $\mathbf{C}_{2^3}$ engendré par P. Son polynôme de contrôle est

$$\begin{aligned} h(X) &= (X^7 - 1)/P \\ &= (X+7)(X^3 + 3X^2 + 2X + 7) \\ &= X^4 + 2X^3 + 7X^2 + 5X + 1 \ . \end{aligned}$$

Avec les notations du théorème 2.12, on a

$$\begin{aligned}\widehat{f_0} &= h \ , \\ \widehat{f_1} = \widehat{f_2} &= 1 \ , \\ \widehat{f_3} &= P \ .\end{aligned}$$

Dans $GR(8,3) \simeq \mathbb{Z}_8[X]/(P(X))$, l'élément $x = X \pmod{P(X)}$ est racine de P, de même que les éléments x^2 et x^4. Les racines de h sont donc

$$\mathcal{Z}(3) = \{x^3, x^6, x^5\} \cup \{x^0\} \ .$$

Pour simplifier l'écriture, remarquons que $x^6 = x^{-1}$. Donc $\mathcal{Z}(3)$ contient une classe de longueur 3, celle de x^{-1} et une de longueur 1, celle de 1. Cela donne

$$\begin{aligned}\mathcal{Z}_3(3) &= \{x^{-1}, x^{-2}, x^{-4}\} & \overline{\mathcal{Z}_3(3)} &= \{-1\} \\ \mathcal{Z}_1(3) &= \{x^0\} & \overline{\mathcal{Z}_1(3)} &= \{0\}\end{aligned}$$

Comme $\widehat{f_1} = \widehat{f_2} = 1$, on a $\mathcal{Z}(1) = \mathcal{Z}(2) = \emptyset$. Donc l'expression de la proposition 2.25 donne

$$\beta \mapsto \mathrm{Tr}_3\left(\lambda_{-1}^{3,3}\beta\right) + \mathrm{Tr}_1\left(\lambda_0^{1,3}\right) \ .$$

L'application Tr_1 n'étant autre que l'identité, en notant simplement Tr la trace de $GR(8,3)$, on obtient la forme suivante pour les mots du code :

$$\mathbf{c} = \pi^*\left(\beta \mapsto \mathrm{Tr}\left(\lambda_{-1}\beta\right) + \lambda_0\right) \ ,$$

soit

$$\mathbf{c} = \left(\mathrm{Tr}\left(\lambda_{-1}\right) + \lambda_0, \mathrm{Tr}\left(\lambda_{-1}x\right) + \lambda_0, \ldots \mathrm{Tr}\left(\lambda_{-1}x^6\right) + \lambda_0\right)$$

où λ_{-1} est un élément de $GR(8,3)$, car $-1 \in \overline{\mathcal{Z}_3(3)}$ et λ_0 est dans $GR(8,1) = \mathbb{Z}_8$ puisque $0 \in \overline{\mathcal{Z}_1(3)}$.

□

Comme l'illustre l'exemple précédent, dans certains cas la représentation des mots de code par la trace est très simple. Une première simplification de l'expression générale énoncée dans la proposition 2.25 est obtenue en considérant les codes construits par relèvement de Hensel. Alors seuls les ensembles $\mathcal{Z}(0)$ et $\mathcal{Z}(k)$ sont non vides, et on évite la première sommation sur i. L'étape suivante consiste à réduire $\mathcal{Z}(k)$ au minimum, c'est-à-dire à une seule classe d'équivalence. Cela revient à relever des codes irréductibles sur $\mathbb{Z}_p$, à savoir des codes cycliques dont le polynôme de contrôle est irréductible. Les mots du code relevé sont alors de la forme

$$\mathbf{c} = \pi^*\left(\beta \mapsto \mathrm{Tr}_{m_s}\left(\lambda \cdot \beta^{-s}\right)\right)$$

avec $\lambda \in GR(p^k, m_s)$. Ce cas très particulier va nous servir au chapitre 4 où nous prouverons que les codes de Kerdock généralisés peuvent être construit en utilisnt des codes de ce types.

Chapitre 3

Codes $\mathbb{Z}_{p^k}$-linéaires

Nous avons présenté dans le chapitre précédent les codes sur les anneaux d'entiers modulo une puissance d'un nombre premier. Notre but étant de construire des codes sur $\mathbb{Z}_p$, il nous reste à traiter de la transformation des codes sur $\mathbb{Z}_{p^k}$ en codes sur $\mathbb{Z}_p$. Toutefois, nous cherchons à respecter deux contraintes : nous souhaitons conserver d'une part le cardinal du code et d'autre part sa distance minimale. Nous avons donc besoin d'une isométrie. Ce premier point fait l'objet de la section 3.1. L'approche retenue est essentiellement celle de [Car98] généralisée à p^k, donnant un cas particulier de l'application de Greferath et Schmidt presentée dans [GS99]. Précisons dès maintenant que l'isométrie ainsi construite permet de retrouver l'application de Gray introduite dans [HKC+94] pour $\mathbb{Z}_4$ et plusieurs fois reprise depuis lors.

Par la suite, nous donnons les principales propriétés des codes $\mathbb{Z}_{p^k}$-linéaires que l'application de Gray généralisée permet de construire. Un point important est l'existence d'une relation de type MacWilliams entre un code $\mathbb{Z}_{p^k}$-linéaire et le dual de son relevé, relation qui donne lieu, dans le cas particulier de $\mathbb{Z}_4$, à la notion de dualité formelle, c'est-à-dire au fait que deux codes non linéaires puissent avoir des énumérateurs des poids qui satisfassent la relation de MacWilliams.

3.1 Application de Gray généralisée

À l'origine, le code de Gray est un ordre sur les séquences binaires de longueur fixée n, permettant d'énumérer toutes ces séquences en ne modifiant qu'un seul bit pour passer d'une séquence à la suivante. Le cas qui va nous intéresser directement est celui des séquences de longueur deux, pour lequel

on a le code de Gray suivant :

$$0 \mapsto 00$$
$$1 \mapsto 01$$
$$2 \mapsto 11$$
$$3 \mapsto 10$$

On appelle application de Gray, et nous noterons Ψ, l'application allant de $\mathbb{Z}_{2^2}$ dans $\mathbb{Z}_2^2$, qui à un entier inférieur ou égal à 3 associe la séquence binaire de longueur 2 correspondante.

En théorie des codes, l'intérêt principal de l'application de Gray est qu'elle permet de construire une *isométrie* entre $\mathbb{Z}_4$ et $\mathbb{Z}_2^2$, *i.e.* une application bijective conservant les distances. Pour obtenir cette isométrie, on munit $\mathbb{Z}_2^2$ du poids de Hamming et $\mathbb{Z}_4$ du poids de *Lee*, noté w_L, que l'on définit par

$$0 \overset{w_L}{\longmapsto} 0$$
$$1 \longmapsto 1$$
$$2 \longmapsto 2$$
$$3 \longmapsto 1$$

Rappelons qu'il est possible d'associer simplement une distance à un poids en définisant la distance entre deux éléments a et b comme étant le poids de leur différence. La distance de Lee entre a et b est alors $w_L(a-b)$. On a alors

PROPOSITION 3.1 ([HKC+94, §II.D, TH. 1]) *L'application de Gray est une isométrie de* $(\mathbb{Z}_4, w_L)$ *dans* $(\mathbb{Z}_2^2, w_H)$, i.e.

1. *c'est une bijection,*
2. $\forall (a,b) \in \mathbb{Z}_4^2 \qquad d_L(a,b) = d_H(\Psi(a), \Psi(b))$.

w_L	$\mathbb{Z}_4$	Ψ	$\mathbb{Z}_2^2$	w_H
0	0	$\longmapsto$	00	0
1	1	$\longmapsto$	01	1
2	2	$\longmapsto$	11	2
1	3	$\longmapsto$	10	1

FIG. 3.1 – Application de Gray.

Cette isométrie est à l'origine de l'explication de la dualité formelle de certains codes binaires non linéaires tels les Kerdock et Preparata (cf. [HKC+94]). On a donc cherché à généraliser l'application de Gray à $\mathbb{Z}_{2^k}$.

Malheureusement, quel que soit le poids w dont on munit $\mathbb{Z}_{2^k}$, il n'existe pas d'isométrie entre $(\mathbb{Z}_{2^k}, w)$ et $(\mathbb{Z}_2^k, w_H)$ pour $k \geq 3$ comme l'a montré Sălăgean-Mandache dans [Săl99]. Pour obtenir une généralisation de Ψ définie sur $\mathbb{Z}_{2^k}$ conservant les distances, il faut agrandir l'ensemble d'arrivée. Ainsi, la généralisation introduite par C. Carlet dans [Car98] est à valeurs dans $\mathbb{Z}_2^{2^{k-1}}$.

Le principe de cette généralisation consiste à utiliser le code de Reed et Muller d'ordre 1 en $k-1$ variables (c'est-à-dire les fonctions booléennes affines en $k-1$ variables) comme ensemble d'arrivée pour Ψ en utilisant l'écriture en base 2 des éléments de $\mathbb{Z}_{2^k}$ pour définir la correspondance.

Cette approche s'étend naturellement à l'anneau $\mathbb{Z}_{p^k}$ si l'on utilise le code généralisé de Reed et Muller d'ordre 1 en $k-1$ variables sur $\mathbb{Z}_p$. Afin de présenter cette généralisation, on introduit l'application d'évaluation $\pi : \mathbb{Z}_p[Y_1, \ldots, Y_{k-1}] \to \mathbb{Z}_p^{p^{k-1}}$ qui, à un polynôme P, associe le p^{k-1}-uplet défini par

$$\pi(P) = \left(P(\mathbf{x}_0), \ldots, P\left(\mathbf{x}_{p^{k-1}-1}\right)\right) \quad ,$$

avec $\mathbb{Z}_p^{p^{k-1}} = \{\mathbf{x}_0, \ldots, \mathbf{x}_{p^{k-1}-1}\}$.

L'application π dépend de l'ordre choisi pour les $\mathbf{x}_i$. Cependant, c'est au poids de Hamming de $\pi(P)$ que nous allons nous intéresser et celui-ci est indépendant de l'ordre des $\mathbf{x}_i$. Toutefois, lorsqu'un ordre explicite sera nécessaire, comme c'est le cas dans les exemples 3.2 et 3.6, nous utiliserons l'ordre lexicographique inverse. Cela revient à dire que l'élément $\mathbf{x}_i$ est le p^{k-1}-uplet correspondant à l'écriture en base p de l'indice i (le coefficient de degré p^{k-1} étant à la coordonnée 0).

Exemple 3.2 On prend $p = 2$, $k = 4$ et $P(Y_1, Y_2, Y_3) = Y_1 + Y_3$.

	$\mathbf{x}_0$	$\mathbf{x}_1$	$\mathbf{x}_2$	$\mathbf{x}_3$	$\mathbf{x}_4$	$\mathbf{x}_5$	$\mathbf{x}_6$	$\mathbf{x}_7$
Y_1	0	0	0	0	1	1	1	1
Y_2	0	0	1	1	0	0	1	1
Y_3	0	1	0	1	0	1	0	1
$\pi(P)$	0	1	0	1	1	0	1	0

Le polynôme multivarié P a donc pour image par π le vecteur $\pi(P) = (0,1,0,1,1,0,1,0)$. □

Définition 3.3 (Code généralisé de Reed et Muller) *On appelle code généralisé de Reed et Muller d'ordre r en m variables sur $\mathbb{Z}_p$ l'image par π des éléments de $\mathbb{Z}_p[Y_1, \ldots, Y_m]$ de degré au plus égal à r :*

$$\mathrm{GRM}(r, m) = \left\{\pi(P) \;\middle|\; P \in \mathbb{Z}_p[Y_1, \ldots, Y_m] \text{ et } \deg(P) \leq r\right\} \quad .$$

L'application π associe à un polynôme multivarié un élément de $\mathbb{Z}_p^{p^{k-1}}$. Il reste à associer les éléments de $\mathbb{Z}_{p^k}$ aux polynômes multivariés. La composition des deux applications donnera alors une application de $\mathbb{Z}_{p^k}$ dans $\mathbb{Z}_p^{p^{k-1}}$

qui sera la généralisation de l'application de Gray. Pour cela, on définit l'application $\rho : \mathbb{Z}_{p^k} \to \mathbb{Z}_p[Y_1, \ldots, Y_{k-1}]$ telle que pour tout $a = \sum_{i=1}^{k} a_i p^{i-1}$,

$$\rho(a) = a_1 Y_1 + \cdots + a_{k-1} Y_{k-1} + a_k \ .$$

L'application de Gray généralisée Ψ est alors définie comme la composition $\pi \circ \rho$. Ainsi Ψ est une bijection de $\mathbb{Z}_{p^k}$ dans $\mathrm{GRM}(1, k-1)$.

EXEMPLE 3.4 On prend $k = 4$ et $p = 2$. L'élément $5 \in \mathbb{Z}_{2^4}$ s'écrit

$$1 \cdot 1 + 0 \cdot 2 + 1 \cdot 2^2 + 0 \cdot 2^3 \ ,$$

donc $\rho(5) = 1 \cdot Y_1 + 0 \cdot Y_2 + 1 \cdot Y_3 + 0$. Finalement, par l'exemple 3.2, on a

$$\Psi(a) = (0, 1, 0, 1, 1, 0, 1, 0) \ .$$

□

Le code $\mathrm{GRM}(1, k-1)$ n'a que trois poids de Hamming : 0 pour le polynôme nul, p^{k-1} pour les polynômes constants non nuls, et $(p-1)p^{k-2}$ pour tous les autres polynômes de degré 1. Définissons le poids homogène d'un élément $a \in \mathbb{Z}_{p^k}$, que nous noterons $w_{\mathrm{hom}}(a)$, par $w_H(\Psi(a))$. On a alors

$$w_{\mathrm{hom}}(a) = \begin{cases} 0 & \text{si } a = 0, \\ (p-1)p^{k-2} & \text{si } a \not\equiv 0 \pmod{p^{k-1}}, \\ p^{k-1} & \text{si } a \equiv 0 \pmod{p^{k-1}}. \end{cases}$$

PROPOSITION 3.5 *L'application de Gray généralisée définie par* $\Psi = \pi \circ \rho$ *conserve les distances entre* $(\mathbb{Z}_{p^k}, w_{\mathrm{hom}})$ *et* $(\mathbb{Z}_p^{p^{k-1}}, w_H)$, i.e.

$$\begin{aligned} \forall (a, b) \in \mathbb{Z}_{p^k}^2 \qquad d_{\mathrm{hom}}(a, b) &= w_H(\Psi(a - b)) \\ &= d_H(\Psi(a), \Psi(b)) \ . \end{aligned}$$

PREUVE. Par définition, la distance homogène entre a et b est le poids homogène de la différence, $w_{\mathrm{hom}}(a-b)$. Or le poids homogène est simplement le poids de Hamming de l'image par Ψ. Nous cherchons donc à prouver l'égalité

$$w_H(\Psi(a - b)) = w_H(\Psi(a) - \Psi(b)) \ .$$

Comme π est linéaire, on a $\Psi(a) - \Psi(b) = \pi(\rho(a) - \rho(b))$. Par ailleurs, le nombre de zéros d'un polynôme multivarié non nul, P, de degré au plus 1, et par conséquent le poids de Hamming de son image par π, est caractérisé de manière unique par son degré. Ainsi, l'égalité précédente équivaut à

$$\deg(\rho(a - b)) = \deg(\rho(a) - \rho(b)) \ . \qquad (*)$$

Pour prouver (*), nous examinons les trois cas possibles :

1. si $a = b$, alors l'égalité est clairement vérifiée ;
2. si $a - b \equiv 0 \pmod{p^{k-1}}$, alors $\rho(a-b)$ est un polynôme constant. Mais, $\rho(a) - \rho(b)$ est également un polynôme constant puisque les écritures en base p de a et de b ne diffèrent que pour le coefficient de p^{k-1} et que par conséquent $\rho(a)$ et $\rho(b)$ ne diffèrent que d'une constante ;
3. enfin, si $a - b \not\equiv 0 \pmod{p^{k-1}}$, alors $\rho(a-b)$ n'est pas constant. Il en est de même pour $\rho(a) - \rho(b)$. En effet il existe $i \in [0, k-2]$ tel que les coefficients de p^i des écritures en base p de a et de b soient différents. Le monôme Y_{i+1} a donc un coefficient non nul dans $\rho(a) - \rho(b)$.

□

Lorsque $k = p = 2$, cette généralisation correspond bien à l'application de Gray vue précédemment dans le cas particulier de $\mathbb{Z}_4$, et la distance homogène coïncide alors avec la distance de Lee. Toujours avec $p = 2$ mais $k \geq 3$, nous obtenons la proposition 1 de [Car98, §II]. Dans la suite, nous noterons également Ψ l'application de $\mathbb{Z}_{p^k}^n$ vers $\left(\mathbb{Z}_p^{p^{k-1}}\right)^n = \mathbb{Z}_p^{n \cdot p^{k-1}}$ étendant l'application de Gray généralisée coordonnée par coordonnée.

EXEMPLE 3.6 Explicitons l'application de Gray généralisée sur $\mathbb{Z}_4$ et $\mathbb{Z}_8$. Sur $\mathbb{Z}_4$, nous avons $p = 2$ et $k = 2$, $\rho(a)$ est un polynôme en $k - 1 = 1$ variable de degré au plus 1, $\Psi(a)$ est donc un mot binaire de longueur $2^{k-1} = 2$.

$a = a_1 + 2a_2$	0	1	2	3
$a_1 a_2$	00	10	01	11
$\rho(a)$	0	Y_1	1	$Y_1 + 1$

Avec l'ordre lexicographique inverse

	x_0	x_1
Y_1	0	1

on obtient

a	0	1	2	3
$\Psi(a)$	00	01	11	10
$w_H(\Psi(a))$	0	1	2	1

• $p = 2$ et $k = 3$: $\rho(a)$ est un polynôme en $k - 1 = 2$ variables de degré au plus 1, $\Psi(a)$ est le mot binaire associé de longueur $2^{k-1} = 4$.

a	0	1	2	3	4	5	6	7
$a_1a_2a_3$	000	100	010	110	001	101	011	111
$\rho(a)$	0	Y_1	Y_2	Y_1+Y_2	1	Y_1+1	Y_2+1	Y_1+Y_2+1

Avec l'ordre lexicographique inverse

	x_0	x_1	x_2	x_3
Y_1	0	0	1	1
Y_2	0	1	0	1

on obtient

a	0	1	2	3	4	5	6	7
$\Psi(a)$	0000	0011	0101	0110	1111	1100	1010	1001
$w_H(\Psi(a))$	0	2	2	2	4	2	2	2

□

Remarque 3.7 Il existe d'autres généralisations de l'application de Gray : celle de Greferath et Schmidt (cf. [GS99]) qui étend celle présentée dans cette section à tout anneau commutatif local, principal et fini ; et celle de Kuzmin et Nechaev (cf. [KN92, KN94]), qu'ils appellent Reed-Solomon map, qui définit une isométrie entre $GR(p^2, m)$ et un code de longueur p^m sur $\mathbb{F}_{p^m}$, le code de Reed-Solomon de dimension 2.

3.2 Codes $\mathbb{Z}_{p^k}$-linéaires

L'application de Gray généralisée introduite à la section précédente permet de construire, à partir d'un code défini sur $\mathbb{Z}_{p^k}$ de longueur n, un code sur $\mathbb{Z}_p$ (non nécessairement linéaire) de longueur $n \cdot p^{k-1}$.

Définition 3.8 (Code $\mathbb{Z}_{p^k}$-linéaire) *Un code binaire $\mathcal{C}$ est $\mathbb{Z}_{p^k}$-linéaire si c'est l'image par l'application de Gray généralisée Ψ d'un code $\mathbf{C}_{p^k}$ linéaire sur $\mathbb{Z}_{p^k}$. Dans ce cas, le code $\mathbf{C}_{p^k}$ est appelé code relevé de $\mathcal{C}$.*

Définition 3.9 (Code $\mathbb{Z}_{p^k}$-cyclique) *Un code $\mathcal{C}$ est $\mathbb{Z}_{p^k}$-cyclique s'il est $\mathbb{Z}_{p^k}$-linéaire et si son code relevé est cyclique sur $\mathbb{Z}_{p^k}$.*

La première des deux définitions est susceptible de créer une ambiguïté. En effet, un code relevé peut désigner deux types de codes : soit l'antécédent par l'application de Gray généralisée d'un code $\mathbb{Z}_{p^k}$-linéaire (cf. les deux définitions précédentes) ; soit un code cyclique sur $\mathbb{Z}_{p^k}$ obtenu en appliquant le relèvement de Hensel au générateur d'un code cyclique binaire (Définition 2.15). Le contexte rendra claire l'interprétation pertinente.

Les propriétés de Ψ rendent les codes $\mathcal{C} = \Psi(\mathbf{C}_{p^k})$ et $\mathbf{C}_{p^k}$ très proches.

PROPOSITION 3.10 *Soit $\mathcal{C} = \Psi(\mathbf{C}_{p^k})$ un code $\mathbb{Z}_{p^k}$-linéaire. On a les propriétés suivantes :*

1. *le code $\mathcal{C}$ est distance-invariant, c'est-à-dire tout translaté du code selon un mot de code à la même distribution des poids que $\mathcal{C}$;*
2. *les codes $\mathcal{C}$ et $\mathbf{C}_{p^k}$ ont même distribution des poids, $\mathbb{Z}_p$ étant muni du poids de Hamming et $\mathbb{Z}_{p^k}$ du poids homogène (cf. §3.1).*

La distance-invariance des codes $\mathbb{Z}_{p^k}$-linéaires justifie que l'on s'intéresse uniquement au poids minimal. En effet, un corollaire de cette propriété est que le poids minimal d'un code $\mathbb{Z}_{p^k}$-linéaire est égal à sa distance minimale.

L'application de Gray généralisée étant injective, le code $\mathcal{C}$ a le même cardinal que son relevé, en particulier son cardinal est une puissance de p (cf. théorème 2.4).

DÉFINITION 3.11 (DIMENSION) *Soit $\mathcal{C}$ un code $\mathbb{Z}_{p^k}$-linéaire (n, M). On appelle dimension de $\mathcal{C}$ le logarithme en base p du cardinal de $\mathcal{C}$,* i.e. $\log_p(M)$.

NOTATION 3.12 (PARAMÈTRES) *Nous noterons $\{n, \ell, d\}_p$ les paramètres d'un code $\mathbb{Z}_{p^k}$-linéaire de longueur n, cardinal p^ℓ et de distance minimale d. En l'absence d'ambiguïté, nous écrirons simplement $\{n, \ell, d\}$.*

Il convient de remarquer qu'un code $\mathbb{Z}_{p^k}$-linéaire n'est pas, en général, linéaire sur $\mathbb{Z}_p$ (cf. [HKC+94, Car98, DGL+01, GS99]). Compte-tenu de cette remarque sur la non-linéarité, en général, des codes $\mathbb{Z}_{p^k}$-linéaires, la notion usuelle de dual, définie pour les codes linéaires sur un corps fini, n'a pas de signification dans ce cadre. La notion pertinente est celle de $\mathbb{Z}_{p^k}$-dualité, qui utilise la dualité entre codes relevés, et donc, au final, la dualité sur l'anneau $\mathbb{Z}_{p^k}$.

DÉFINITION 3.13 ($\mathbb{Z}_{p^k}$-DUAL) *Soit $\mathcal{C} = \Psi(\mathbf{C}_{p^k})$ un code $\mathbb{Z}_{p^k}$-linéaire. On appelle code $\mathbb{Z}_{p^k}$-dual de $\mathcal{C}$, et on note $\mathcal{C}_\perp$, l'image par l'application de Gray généralisée du dual de $\mathbf{C}_{p^k}$,* i.e.

$$\mathcal{C}_\perp = \Psi\left(\mathbf{C}_{p^k}^\perp\right) \quad .$$

Toutefois, cette notion se comporte moins bien que la dualité dans le cas linéaire. Par exemple, elle ne donne pas lieu, en général, à une relation de « type MacWilliams » entre des codes $\mathbb{Z}_{p^k}$-duaux, et cela malgré l'existence d'une identité de MacWilliams pour les codes relevés (cf. théorème 2.9). La $\mathbb{Z}_{p^k}$-dualité est tout de même intéressante car elle permet d'obtenir la distribution des poids du $\mathbb{Z}_{p^k}$-dual grâce au polynôme des poids *symétrisés* du code *relevé* $\mathbf{C}_{p^k}$ (à défaut du simple énumérateur des poids de Hamming du code $\mathcal{C}$ comme dans le cas linéaire). De manière plus prosaïque : on peut obtenir la distribution des poids de $\mathcal{C}_\perp$ mais cela demande plus d'information sur $\mathcal{C}$ que dans le cas linéaire.

Définition 3.14 (Polynôme énumérateur des poids symétrisés) *Soit $\mathbf{C}_{p^k}$ un code linéaire de longueur n sur $\mathbb{Z}_{p^k}$. On appelle polynôme énumérateur des poids symétrisés le polynôme homogène de degré n en trois variables, défini par*

$$SW_{\mathbf{C}_{p^k}}(X,Y,Z) = \sum_{\mathbf{c}\in\mathbf{C}_{p^k}} X^{n_z(\mathbf{c})}Y^{n_{nd}(\mathbf{c})}Z^{n_d(\mathbf{c})} \ ,$$

où $n_z(\mathbf{c}), n_{nd}(\mathbf{c}), n_d(\mathbf{c})$ désignent respectivement le nombre de coordonnées de $\mathbf{c}$ nulles, non divisibles par p^{k-1}, et divisibles par p^{k-1} mais non nulles. Le triplet $(n_z(\mathbf{c}), n_{nd}(\mathbf{c}), n_d(\mathbf{c}))$ est appelé poids symétrisé du mot $\mathbf{c}$.

Clairement, ce polynôme s'obtient à partir de $CW_{\mathbf{C}_{p^k}}(X_0,\ldots,X_{p^k-1})$, le polynôme énumérateur des poids complets du code $\mathbf{C}_{p^k}$, en remplaçant X_0 par X, X_i par Y pour $i \not\equiv 0 \pmod{p^{k-1}}$ et par Z pour $i \equiv 0 \pmod{p^{k-1}}$ non nul.

Théorème 3.15 (Distributions des poids de codes $\mathbb{Z}_{p^k}$-duaux) *Soit $\mathcal{C} = \Psi(\mathbf{C}_{p^k})$ un code $\mathbb{Z}_{p^k}$-linéaire de longueur n. On a l'égalité suivante :*

$$\begin{aligned} &HW_{\mathcal{C}_\perp}(X,Y) \\ &\quad = \frac{1}{|\mathcal{C}|} SW_{\mathbf{C}_{p^k}}\Big(X^{p^{k-1}} + (p-1)\cdot Y^{p^{k-1}} + (p^k-p)X^{p^{k-2}}Y^{(p-1)p^{k-2}}, \\ &\qquad\qquad X^{p^{k-1}} - Y^{p^{k-1}}, X^{p^{k-1}} + (p-1)\cdot Y^{p^{k-1}} - pX^{p^{k-2}}Y^{(p-1)p^{k-2}}\Big) \ , \end{aligned}$$

où $HW_{\mathcal{C}_\perp}$ désigne le polynôme énumérateur des poids de Hamming de $\mathcal{C}_\perp$,

$$HW_{\mathcal{C}_\perp}(X,Y) = \sum_{\mathbf{c}\in\mathcal{C}\perp} X^{n-w_H(\mathbf{c})}Y^{w_H(\mathbf{c})} \ .$$

Preuve. Le polynôme énumérateur des poids de Hamming du code $\mathcal{C}_\perp$ s'obtient à partir de l'énumérateur des poids complets de son relevé par la transformation Γ :

$$\begin{array}{rcll} X_0 & \mapsto & X^{p^{k-1}} & , \\ X_i & \mapsto & X^{p^{k-2}}Y^{(p-1)\cdot p^{k-2}} & \text{pour } i \not\equiv 0 \pmod{p^{k-1}} \ , \\ X_i & \mapsto & Y^{p^{k-1}} & \text{pour } i \not\equiv 0, i \equiv 0 \pmod{p^{k-1}} \ . \end{array}$$

Pour simplifier l'écriture, on pose $A = X^{p^{k-1}}, B = X^{p^{k-2}}Y^{(p-1)\cdot p^{k-2}}$, et $C = Y^{p^{k-1}}$. Or, pour tout entier a on a

$$\begin{aligned}
\mu_a(\Gamma(X_0),\ldots,\Gamma(X_{p^k-1})) &= \sum_{\nu\in\mathbb{Z}_{p^k}} \omega^{\nu\cdot a}\Gamma(X_\nu) \\
&= A + \sum_{\substack{p^{k-1}|\nu \\ \nu\neq 0}} \omega^{\nu\cdot a}C + \sum_{\substack{\nu\in\mathbb{Z}_{p^k} \\ p^{k-1}\not|\nu}} \omega^{\nu\cdot a}B \\
&= A - C \\
&\quad + \sum_{p^{k-1}|\nu} \omega^{\nu\cdot a}C - \sum_{p^{k-1}|\nu} \omega^{\nu\cdot a}B \\
&\quad + \sum_{\nu\in\mathbb{Z}_{p^k}} \omega^{\nu\cdot a}B \\
&= A - C \\
&\quad + C\cdot\sum_{\ell=0}^{p-1}\left(\omega^{p^{k-1}\cdot a}\right)^\ell - B\cdot\sum_{\ell=0}^{p-1}\left(\omega^{p^{k-1}\cdot a}\right)^\ell \\
&\quad + B\sum_{\nu\in\mathbb{Z}_{p^k}} \omega^{\nu\cdot a}\ .
\end{aligned}$$

Donc, nous avons trois cas :

1. si $a = 0$, clairement on a

$$\mu_a(\Gamma(X_0),\ldots,\Gamma(X_{p^k-1})) = A + (p-1)C + \left(p^k - p\right)B\ ;$$

2. si $a \not\equiv 0 \pmod{p}$, alors les sommes

$$\sum_{l=0}^{p-1}\left(\omega^{p^{k-1}\cdot a}\right)^l$$

et

$$\sum_{\nu\in\mathbb{Z}_{p^k}} \omega^{\nu\cdot a}$$

sont nulles, respectivement parce que $\omega^{p^{k-1}\cdot a}$ est une racine p-ième de l'unité différente de 1 et que ω^a est une racine p^k-ième de l'unité différente de 1. D'où

$$\mu_a(\Gamma(X_0),\ldots,\Gamma(X_{p^k-1})) = A - C\ ;$$

3. enfin, si $a \neq 0$ et $a \equiv 0 \pmod{p}$. Alors $\omega^{p^{k-1}\cdot a} = 1$ mais ω^a est toujours une p^k-ième de l'unité différente de 1. D'où

$$\mu_a(\Gamma(X_0), \ldots, \Gamma(X_{p^k-1})) = A + (p-1)C - pB \ .$$

Cela nous conduit à

$$\begin{aligned}
&HW_{\mathcal{C}_\perp}(X,Y) \\
&\qquad = CW_{\mathbf{C}_{p^k}^\perp}\left(\Gamma(X_0), \ldots, \Gamma\left(X_{p^k-1}\right)\right) \\
&\qquad = \frac{1}{|\mathbf{C}_{p^k}|} CW_{\mathbf{C}_{p^k}}\Big(\mu_0\left(\Gamma\left(X_0\right), \ldots, \Gamma\left(X_{p^k-1}\right)\right), \\
&\qquad\qquad\qquad \ldots, \mu_{p^k-1}\left(\Gamma\left(X_0\right), \ldots, \Gamma\left(X_{p^k-1}\right)\right)\Big) \\
&\qquad = \frac{1}{|\mathbf{C}_{p^k}|} SW_{\mathbf{C}_{p^k}}\Big(A + (p-1)C + \left(p^k - p\right)B, \\
&\qquad\qquad\qquad A - C, A + (p-1)C + pB\Big) \ .
\end{aligned}$$

□

Ce résultat généralise celui donné dans [Car98, §III, prop. 5] pour $p = 2$.

Le théorème ci-dessus permet d'exprimer le polynôme énumérateur des poids de Hamming du $\mathbb{Z}_{p^k}$-dual $\mathcal{C}_\perp$ à partir de l'énumérateur des poids symétrisés de $\mathbf{C}_{p^k}$. Pourtant, et bien que cela semble un peu paradoxal, il ne permet pas d'obtenir l'énumérateur des poids de Hamming du code $\mathcal{C}$ lui-même. En effet, les coordonnées divisibles par p^{k-2} sont simplement comptées comme étant divisibles par p, alors qu'elles ont un poids homogène supérieur aux autres éléments non nuls de $\mathbb{Z}_{p^k}$.

Dans le cas particulier $p = k = 2$, c'est-à-dire $\mathbb{Z}_4$, on prouve l'égalité

$$HW_{\mathcal{C}}(X+Y, X-Y) = SW_{\mathbf{C}_4}(X^2+Y^2+2XY, X^2-Y^2, X^2+Y^2-2XY) \ .$$

Autrement dit, l'égalité du théorème 3.15 se réécrit simplement $HW_{\mathcal{C}_\perp}(X,Y) = 1/|\mathcal{C}| \cdot HW_{\mathcal{C}}(X+Y, X-Y)$.

THÉORÈME 3.16 (DUALITÉ FORMELLE DES CODES $\mathbb{Z}_4$-DUAUX, [HKC+94, §II.E, TH. 3]) *Soient $\mathcal{C}$ un code $\mathbb{Z}_4$-linéaire et $\mathcal{C}_\perp$ son $\mathbb{Z}_4$-dual. Alors, $\mathcal{C}$ et $\mathcal{C}_\perp$ sont formellement duaux,* i.e. *on a*

$$HW_{\mathcal{C}_\perp}(X,Y) = \frac{1}{|\mathcal{C}|} HW_{\mathcal{C}}(X+Y, X-Y) \ .$$

Chapitre 4

Codes de Kerdock généralisés

Les codes de Kerdock sont des codes binaires de longueur 2^{m+1}, de cardinal 2^{2m+2} et de distance minimale $2^m - 2^{(m-1)/2}$, définis pour m impair. Ils ont été construits par Kerdock en 1972 (cf. [Ker72]).

Ces codes figurent parmi les meilleurs codes connus, *i.e.* à longueur et à distance minimale fixées, ils possèdent le cardinal le plus élevé. Bien qu'ayant une définition complexe en tant que simples codes binaires (cf. [MS96]), ils se définissent beaucoup plus facilement en tant que codes $\mathbb{Z}_4$-linéaires, construction qui fut obtenue dans [HKC$^+$94]. On trouve également une construction $\mathbb{Z}_4$-linéaire dans [Nec91] mais celle de [HKC$^+$94] a l'avantage d'expliquer algébriquement la dualité formelle des codes de Kerdock et des codes de Preparata et d'être plus générale.

La construction des codes sur $\mathbb{Z}_4$ ayant pour image les codes de Kerdock, se généralise naturellement aux anneaux $\mathbb{Z}_{2^k}$. Le problème sous-jacent est la transformation en code binaire, obtenue dans le cas de $\mathbb{Z}_4$ par l'application de Gray. L'introduction d'une généralisation de l'application de Gray résout ce problème et aboutit naturellement à une généralisation des codes de Kerdock donnant des codes $\mathbb{Z}_{2^k}$-linéaires (cf. [Car98]).

Hammons, Kumar, Calderbank, Sloane et Solé donnent deux constructions équivalentes des codes de Kerdock, l'une utilisant des codes cycliques sur $\mathbb{Z}_4$, l'autre des formes affines sur l'anneau $\mathrm{GR}(4, m)$. Nous adoptons cette dernière construction pour présenter la généralisation de ces codes, tout comme dans [Car98], à cela près que nous ne nous restreignons pas à $\mathbb{Z}_{2^k}$. Ensuite nous montrons le caractère cyclique de ces codes, ce qui revient à prouver que les deux constructions sur $\mathbb{Z}_4$ donne la même généralisation sur $\mathbb{Z}_{p^k}$. Nous terminons en étudiant leur distance minimale, ce qui est fait en deux temps. Tout d'abord, nous donnons une borne inférieure, généralisant celle présentée dans [Car98]. Ensuite, nous donnons les distances minimales des codes de Kerdock généralisés, obtenues par une légère variante de la recherche exhaustive. Cela nous permet de constater que, contrairement à ce que laissait supposer la borne inférieure, tout particulièrement pour $\mathbb{Z}_8$,

la distance minimale des codes de Kerdock généralisés est inférieure à celle des meilleurs codes linéaires pour toutes les valeurs des paramètres que nous avons pu tester, sauf dans un unique cas, $\mathcal{K}(2^3, 3)$.

4.1 Structure $\mathbb{Z}_{p^k}$-linéaire

Conceptuellement, la construction des codes de Kerdock sur $\mathbb{Z}_{p^k}$ est proche de celle des codes de Reed et Muller d'ordre 1 : elle utilise les fonctions affines.

Notation 4.1 *On notera $\mathcal{F}(p^k, m)$ l'ensemble des formes affines de l'anneau $\mathrm{GR}(p^k, m)$ dans $\mathbb{Z}_{p^k}$, restreintes à l'ensemble de Teichmuller $\mathcal{T} = \{0, 1, x, \ldots, x^{p^m-2}\} \subset \mathrm{GR}(p^k, m)$.*

Par le théorème 1.20, on a

$$\mathcal{F}\left(p^k, m\right) = \left\{ f : \beta \longmapsto \mathrm{Tr}(\alpha\beta) + b \;\middle|\; \alpha \in \mathrm{GR}(p^k, m) \text{ et } b \in \mathbb{Z}_{p^k} \right\} \quad .$$

On note π l'application d'évaluation des formes affines sur les éléments de $\mathcal{T}$ qui, à une forme affine f, associe le p^m-uplet

$$\pi(f) = \left(f(0), f(1), f(x), \ldots, f\left(x^{p^m-2}\right) \right) \quad .$$

Nous généralisons alors la définition [Car98, §IV, déf. 5] pour tout p premier par

Définition 4.2 (Code de Kerdock généralisé) *On appelle code de Kerdock généralisé de paramètres (p^k, m) et on note $\mathcal{K}(p^k, m)$ le code défini sur $\mathbb{Z}_p$ comme l'image par l'application de Gray généralisée de l'ensemble $\pi(\mathcal{F}(p^k, m))$*

$$\mathcal{K}\left(p^k, m\right) = \left\{ \Psi(\pi(f)) \;\middle|\; f \in \mathcal{F}\left(p^k, m\right) \right\} \quad .$$

Le relevé de $\mathcal{K}(p^k, m)$ est donc de longueur p^m sur $\mathbb{Z}_{p^k}$ et par conséquent $\mathcal{K}(p^k, m)$ est de longueur p^{m+k-1} sur $\mathbb{Z}_p$. D'autre part, l'ensemble des fonctions affines $\mathcal{F}$ de $\mathrm{GR}(p^k, m)$ sur $\mathbb{Z}_{p^k}$ forme un module libre de rang $m+1$. Une base de $\mathcal{F}$ est l'ensemble des formes coordonnées associées à la base $1, x, \ldots, x^{m-1}$ de $\mathrm{GR}(p^k, m)$ considéré comme un module sur $\mathbb{Z}_{p^k}$, *i.e.* les fonctions

$$x_j^* : \beta = \sum_{i=0}^{m-1} \lambda_i x^i \longmapsto \lambda_j \qquad j \in [0, m-1] \quad ,$$

plus la fonction constante égale à 1. Ainsi, une matrice génératrice du code relevé s'écrit

$$G = \begin{pmatrix} 1 & 1 & 1 & 1 & \dots & 1 \\ x_0^*(0) & x_0^*(1) & x_0^*(x) & x_0^*\left(x^2\right) & \dots & x_0^*\left(x^{p^m-2}\right) \\ x_1^*(0) & x_1^*(1) & x_1^*(x) & x_1^*\left(x^2\right) & \dots & x_1^*\left(x^{p^m-2}\right) \\ \dots & \dots & \dots & \dots & \dots & \dots \\ x_m^*(0) & x_m^*(1) & x_m^*(x) & x_m^*\left(x^2\right) & \dots & x_m^*\left(x^{p^m-2}\right) \end{pmatrix}.$$

Calculer cette matrice revient à construire la table des représentations additives des éléments du Teichmuller (cf. §1.2) : en effet, par définition des formes coordonnées, on a $x^j = \sum_{i=0}^{m-1} x_i^*(x^j)x^i$.

Le cardinal du relevé de $\mathcal{K}(p^k, m)$ est donc $(p^k)^{m+1} = p^{k(m+1)}$. Comme un code $\mathbb{Z}_{p^k}$-linéaire et son relevé ont même cardinal, ce cardinal est également celui de $\mathcal{K}(p^k, m)$.

PROPOSITION 4.3 *Le code de Kerdock généralisé $\mathcal{K}(p^k, m)$ est de longueur p^{m+k-1} sur $\mathbb{Z}_p$ et a $p^{k(m+1)}$ mots.*

EXEMPLE 4.4 Le relevé du code de Kerdock généralisé $\mathcal{K}(2^3, 3)$ est généré par la matrice

$$G = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 2 & 7 & 5 \\ 0 & 0 & 1 & 0 & 3 & 7 & 7 & 6 \\ 0 & 0 & 0 & 1 & 2 & 7 & 5 & 1 \end{pmatrix}$$

d'après l'exemple 1.14 page 23 (lorsque l'anneau $GR(2^3, 3)$ est représenté par $\mathbb{Z}_{2^3}[X]/(7 + 5X + 6X^2 + X^3)$). □

Lorsque $p = k = 2$ et pour $m \geq 3$ impair, les codes de Kerdock généralisés sont les codes introduits par Kerdock en 1972 (cf. [Ker72]). Ces codes sont actuellement les meilleurs connus pour de tels paramètres : la distance minimale de $\mathcal{K}(2^2, m)$ est $2^m - 2^{\frac{m-1}{2}}$ pour une longueur de 2^{m+1} et $2^{2(m+1)}$ mots. À titre de comparaison, les codes de Reed et Muller d'ordre 1 en $m+1$ variables, notés $RM(1, m+1)$, qui ont la même longueur, ont 2^{m+2} mots et une distance minimale de 2^m. En fait, les codes de Kerdock sont formés du code $RM(1, m+1)$ et de $2^m - 1$ de ses translatés. Ces translatés correspondent à des fonctions coubres, c'est-à-dire à des fonctions aussi éloignées que possible – pour la distance de Hamming – des fonctions affines, à savoir $2^m - 2^{\frac{m-1}{2}}$ lorsque m est impair.

Les codes de Kerdock ont donc 2^m fois plus d'éléments pour une distance minimale sensiblement identique. Or les codes de Reed et Muller d'ordre 1 sont optimaux, au sens où ils atteignent la borne de Griesmer ([MS96, chap. 17, §6, th. 24]) : pour toute longueur plus petite, il n'existe pas de code linéaire ayant la même distance minimale et le même cardinal que les codes de Reed et Muller d'ordre 1. La table 4.1 illustre la différence entre les deux

$\mathcal{K}(2^2, m)$			$\mathrm{RM}(1, m+1)$		
$\{16, 8, 6\}$	50%	0.333	$[16, 5, 8]$	31.52%	0.5
$\{64, 12, 28\}$	18.75%	0.438	$[64, 7, 32]$	10.94%	0.5
$\{256, 16, 120\}$	6.25%	0.469	$[256, 9, 128]$	3.52%	0.5
$\{1024, 20, 496\}$	1.95%	0.484	$[1024, 11, 512]$	1.07%	0.5

TAB. 4.1 – Paramètres, taux de transmission et distance relative des codes de Kerdock et de Reed et Muller en petite longueur.

familles de codes en donnant les valeurs des paramètres ainsi que le taux de transmission – rapport du logarithme en base 2 du cardinal à la longueur – et la distance relative – rapport de la distance minimale à la longueur. En fait, au-delà de la distance minimale, on connaît même la distribution des poids de Hamming des codes de Kerdock (voir [MS96] et [HKC+94]) :

i	A_i
0	1
$2^m - 2^{\frac{m-1}{2}}$	$2^{m+1}(2^m - 1)$
2^m	$2^{m+2} - 2$
$2^m + 2^{\frac{m-1}{2}}$	$2^{m+1}(2^m - 1)$
2^{m+1}	1

Ces codes sont fortement liés à des codes qui furent construits quatre ans plus tôt par Preparata ([Pre68]) : les codes de Preparata sont des duaux formels des codes de Kerdock. Autrement dit, les énumérateurs des poids des codes de Preparata et de Kerdock satisfont l'identité de MacWilliams s'appliquant pour les codes binaires. Une explication possible, suggérée par le théorème 3.16, serait que les codes de Preparata soient les $\mathbb{Z}_4$-duaux des codes de Kerdock, $\mathcal{K}(4, m)_\perp$. Toutefois, ce n'est pas le cas. Une différence importante est que les codes de Preparata sont contenus dans des codes de Hamming étendus, ce qui n'est pas le cas des codes $\mathcal{K}(4, m)_\perp$ (cf. [HKC+94]). Mais, les codes $\mathcal{K}(4, m)_\perp$ ont une distribution des poids identiques à celle des codes de Preparata, que l'on peut obtenir à partir de la distribution des codes de Kerdock et du théorème 3.16. Nous adopterons donc, suivant la terminologie de Hammons *et al.*, la définition suivante :

DÉFINITION 4.5 (CODE DE PREPARATA GÉNÉRALISÉ) *On appelle code de Preparata généralisé, et on note $\mathcal{P}(p^k, m)$, le $\mathbb{Z}_{p^k}$-dual du code de Kerdock généralisé $\mathcal{K}(p^k, m)$.*

PROPOSITION 4.6 *Le code $\mathcal{P}(p^k, m)$ est de longueur p^{m+k-1} et a $p^{k(p^m-m-1)}$ mots.*

4.2 Structure $\mathbb{Z}_{p^k}$-cyclique

Nous avons vu dans la section précédente une définition des codes de Kerdock généralisés à partir de codes linéaires sur $\mathbb{Z}_{p^k}$. Nous allons maintenant voir que ces codes peuvent être construits à partir de codes cycliques : dans le cas le plus simple, le code relevé est un code cyclique étendu sur $\mathbb{Z}_{p^k}$; de façon générale son dual est cyclique étendu. Cette construction est donnée dans le cas des codes de Kerdock – c'est-à-dire de $\mathbb{Z}_4$ – dans l'article de Hammons *et al.* [HKC+94], nous la généralisons ici à $\mathbb{Z}_{p^k}$.

Soit $P \in \mathbb{Z}_{p^k}[X]$, un B-polynôme de degré m et posons $n = p^m - 1$. Nous définissons le code cyclique $\mathbf{K}^-$ par son polynôme de contrôle : le polynôme réciproque de $(X-1)P(X)$. Pour appliquer la proposition 2.25 page 47, calculons les $\mathcal{Z}(i)$. Nous effectuons les calculs dans $\mathbb{Z}_{p^k}[X]/(P) = \mathrm{GR}(p^k, m)$ et par conséquent x désigne la classe de X modulo P. Nous avons

$$\begin{aligned}
&\mathcal{Z}(k) = \{x^{-1}, x^{-p}, \dots x^{-p^{m-1}}\} \cup \{x^0\} \ , \\
&\mathcal{Z}(1) = \cdots = \mathcal{Z}(k-1) = \{\} \ , \\
&\mathcal{Z}(0) = \{x^0, x, x^2, \dots, x^{p^m-2}\} \subset \mathcal{Z}(k) \ .
\end{aligned}$$

La proposition 2.25 permet alors de décrire le code $\mathbf{K}^-$ comme l'image par π^* de l'ensemble des formes affines

$$\beta \mapsto \mathrm{Tr}(\alpha\beta) + b$$

avec $\alpha \in \mathrm{GR}(p^k, m)$ et $b \in \mathbb{Z}_{p^k}$, autrement dit $\pi^*(\mathcal{F}(p^k, m))$. Remarquons que pour une fonction $f \in \mathcal{F}(p^k, m)$, la somme de ses valeurs sur $\mathcal{T}^*$ est égale à $n \cdot f(0)$:

$$\begin{aligned}
\sum_{i=0}^{n-1} f\left(x^i\right) &= \sum_{i=0}^{n-1} \mathrm{Tr}\left(\alpha x^i\right) + f(0) \\
&= \mathrm{Tr}\left(\alpha \sum_{i=0}^{n-1} x^i\right) + n \cdot f(0) \\
&= n \cdot f(0) \ ,
\end{aligned}$$

car

$$\sum_{i=0}^{n-1} x^i = \frac{x^n - 1}{x - 1} = 0 \ .$$

En effet, $x-1$ est inversible sinon on aurait $x = 1 + p\alpha$, $\alpha \in \mathrm{GR}(p^k, m)$ non nul, ce qui contredirait l'unicité de la forme multiplicative (cf. proposition 1.13).

Ainsi, si on note $\mathbf{K}$ le code étendu de $\mathbf{K}^-$ défini par

$$\mathbf{K} = \left\{ (v_0, v_1, \dots, v_n) \in \mathbb{Z}_{p^k}^{n+1} \;\middle|\; (v_1, \dots, v_n) \in \mathbf{K}^- \text{ et } v_0 + v_1 + \cdots + v_n = 0 \right\} \ ,$$

on a $\nu_0 = -(\nu_1 + \cdots + \nu_n) = \sum f(x^i)$ pour un certain $f \in \mathcal{F}(p^k, m)$, soit $\nu_0 = -n \cdot f(0)$. Lorsque $k \leq m$, alors $n = p^m - 1 \equiv -1 \pmod{p^k}$, d'où $\nu_0 = f(0)$. En d'autres termes, si $k \leq m$, le code $\mathbf{K}$ est l'ensemble des formes affines de $\mathrm{GR}(p^k, m)$ restreintes au Teichmuller, c'est donc le relevé du code de Kerdock généralisé $\mathcal{K}(p^k, m)$.

THÉORÈME 4.7 *Soit* $P \in \mathbb{Z}_{p^k}[X]$ *un B-polynôme de degré* m. *Lorsque* $k \leq m$, *le relevé du code de Kerdock généralisé* $\mathcal{K}(p^k, m)$ *est l'étendu du code cyclique* $\mathbf{K}^-$ *dont le polynôme de contrôle est le polynôme réciproque de* $(X-1)P(X)$.

Lorsque $k > m$, l'égalité $\nu_0 = f(0)$ n'est plus vérifiée et en conséquence $\mathbf{K}$ n'est plus le relevé de $\mathcal{K}(p^k, m)$. Cependant, $-n$ est inversible dans $\mathbb{Z}_{p^k}$ et donc le relevé de $\mathcal{K}(p^k, m)$ est équivalent à $\mathbf{K}$, autrement dit, le relevé de $\mathcal{K}(p^k, m)$ est équivalent à un code cyclique étendu. Cela étant, on peut tout de même obtenir une information sur la structure du relevé de $\mathcal{K}(p^k, m)$: on peut le définir comme le dual d'un code cyclique étendu.

LEMME 4.8 *Soient* $\mathbf{C}_{p^k}$ *un code linéaire sur* $\mathbb{Z}_{p^k}$, $\mathbf{C}^+_{p^k}$ *son étendu, et* $G^\perp$ *une matrice génératrice du dual de* $\mathbf{C}_{p^k}$. *Alors la matrice*

$$\begin{pmatrix} 1 & \cdots & 1 \\ 0 & & G^\perp \end{pmatrix}$$

est génératrice du code dual de $\mathbf{C}^+_{p^k}$.

PREUVE. Nous commençons par prouver que tous les mots de la forme $(0, \nu_0, \ldots, \nu_{n-1})$, pour $(\nu_0, \ldots, \nu_{n-1}) \in \mathbf{C}^\perp_{p^k}$, sont dans $(\mathbf{C}^+_{p^k})^\perp$. Soit $\mathbf{u}^+ = (u_\infty, u_0, \ldots, u_{n-1}) \in \mathbf{C}^+_{p^k}$, alors

$$\mathbf{u}^+ \cdot (0, \nu_0, \ldots, \nu_{n-1}) = 0 \cdot u_\infty + \sum_{i=0}^{n-1} u_i \cdot \nu_i = 0 \ .$$

D'autre part,

$$\mathbf{u}^+ \cdot (1, \ldots, 1) = u_\infty + \sum_{i=0}^{n-1} u_i = 0 \ .$$

Donc, le code engendré par la matrice

$$M = \begin{pmatrix} 1 & \cdots & 1 \\ 0 & & G^\perp \end{pmatrix}$$

est inclus dans le dual de $(\mathbf{C}^+_{p^k})$. Or il est clair que les lignes de cette matrice sont linéairement indépendantes sur $\mathbb{Z}_{p^k}$. Le code engendré a donc $p^k \cdot |\mathbf{C}^\perp_{p^k}|$ éléments. Pour conclure ce lemme, prouvons que c'est également le cardinal du code $(\mathbf{C}^+_{p^k})^\perp$. L'opération consistant à étendre un code laisse invariant le

cardinal : $|\mathbf{C}_{p^k}| = |\mathbf{C}^+_{p^k}|$. D'après les résultats de la section 2.1 (théorème 2.4 et proposition 2.6), on a $|\mathbf{C}_{p^k}| \cdot |\mathbf{C}^\perp_{p^k}| = p^{kn}$ et $|\mathbf{C}^+_{p^k}| \cdot |(\mathbf{C}^+_{p^k})^\perp| = p^{k(n+1)}$. Donc

$$\begin{aligned}\left|(\mathbf{C}^+_{p^k})^\perp\right| &= \frac{p^{k(n+1)}}{\left|\mathbf{C}^+_{p^k}\right|} = \frac{p^{k(n+1)}}{|\mathbf{C}_{p^k}|} \\ &= \frac{p^{k(n+1)}}{p^{kn}} \cdot |\mathbf{C}^\perp_{p^k}| \\ &= p^k \cdot \left|\mathbf{C}^\perp_{p^k}\right| \quad .\end{aligned}$$

Il en découle que la matrice M engendre le code $(\mathbf{C}^+_{p^k})^\perp$, ce qui achève la démonstration. □

THÉORÈME 4.9 *Soit $P \in \mathbb{Z}_{p^k}[X]$ un B-polynôme de degré m. Le code relevé du code de Kerdock généralisé $\mathcal{K}(p^k, m)$ est le code dual de l'étendu du code cyclique $\mathbf{C}_{p^k}$ engendré par le polynôme réciproque de P, $\mathbf{C}_{p^k} = (\widetilde{P})$*

PREUVE. Appliquons le lemme précédent au code $\mathbf{C}_{p^k} = (\widetilde{P})$ Si l'on note G une matrice génératrice de $\mathbf{C}^\perp_{p^k}$, la matrice

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

est une matrice génératrice de $(\mathbf{C}^+_{p^k})^\perp$. Pour la matrice G, on peut prendre

$$G = \begin{pmatrix} x^*_0(1) & x^*_0(x) & \dots & x^*_0\left(x^{p^m-2}\right) \\ x^*_1(1) & x^*_1(x) & \dots & x^*_1\left(x^{p^m-2}\right) \\ \dots & \dots & \dots & \dots \\ x^*_m(1) & x^*_m(x) & \dots & x^*_m\left(x^{p^m-2}\right) \end{pmatrix} ,$$

où les x^*_i sont les formes coordonnées. En effet, $\mathbf{C}^\perp_{p^k}$ a pour polynôme de contrôle $\widetilde{P}$, donc on a $\mathcal{Z}(1) = \cdots = \mathcal{Z}(k-1) = \emptyset$ et $\mathcal{Z}(k) = \{x, x^p, \dots x^{p^{m-1}}\}$. Par application de la proposition 2.25, on a donc $\mathbf{C}^\perp_{p^k} = \pi^*(\mathcal{F}(p^k, m))$. De plus, les x^*_i formant une base des formes linéaires, G engendre bien $\mathbf{C}^\perp_{p^k}$. La matrice G' est alors exactement la matrice génératrice donnée dans la section 4.1. □

On peut remarquer que le théorème ci-dessus ne requiert aucune hypothèse particulière sur k et m. Autrement dit, le relevé d'un code de Kerdock généralisé possède toujours cette structure de dual d'un code cyclique étendu. Cela implique que dans le cas $k \leq m$ la structure de code cyclique étendu du code relevé coïncide avec la structure de dual de code cyclique étendu. Les théorèmes 4.7 et 4.9 permettent bien entendu de relier les codes de Preparata généralisés aux codes cycliques sur $\mathbb{Z}_{p^k}$:

THÉORÈME 4.10 *Le relevé du code de Preparata généralisé* $\mathcal{P}(p^k, m)$ *est l'étendu du code cyclique* $\left(\widetilde{P(X)}\right)$. *Lorsque* $k \leq m$, *ce code peut également être décrit comme le dual de l'étendu du code* $\mathbf{K}^-$.

EXEMPLE 4.11 Nous avons donné dans l'exemple 4.4 page 61 la matrice génératrice du code $\mathcal{K}(2^3, 3)$ obtenue par les formes affines lorsque $GR(2^3, 3)$ est représenté par $\mathbb{Z}_{2^3}[X]/(7 + 5X + 6X^2 + X^3)$:

$$G = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 2 & 7 & 5 \\ 0 & 0 & 1 & 0 & 3 & 7 & 7 & 6 \\ 0 & 0 & 0 & 1 & 2 & 7 & 5 & 1 \end{pmatrix} .$$

Posons $P(X) = X^3 + 6X^2 + 5X + 7$, alors le polynôme $h(\widetilde{X-1})P(X)$ est un polynôme de contrôle du code $\mathbf{K}^-$. Nous avons

$$(X-1)P(X) = X^4 + 5X^3 + 7X^2 + 2X + 1 \ ,$$

donc

$$h(X) = X^4 + 2X^3 + 7X^2 + 5X + 1 \ .$$

Le code $\mathbf{K}^-$ est donc engendré par

$$\begin{aligned} g(X) &= (X^7 - 1)/(h(X)) \\ &= X^3 + 6X^2 + 5X + 7 \ , \end{aligned}$$

et la matrice

$$G' = \begin{pmatrix} 5 & 7 & 5 & 6 & 1 & 0 & 0 & 0 \\ 5 & 0 & 7 & 5 & 6 & 1 & 0 & 0 \\ 5 & 0 & 0 & 7 & 5 & 6 & 1 & 0 \\ 5 & 0 & 0 & 0 & 7 & 5 & 6 & 1 \end{pmatrix}$$

est la matrice génératrice correspondante pour le relevé de $\mathcal{K}(2^3, 3)$. En posant

$$T = \begin{pmatrix} 7 & 2 & 3 & 1 \\ 7 & 3 & 1 & 5 \\ 0 & 7 & 3 & 6 \\ 0 & 0 & 7 & 1 \end{pmatrix}$$

on peut vérifier que l'on a

$$G = T \cdot G' \ .$$

Soit, en d'autres termes, puisque $\det(T) = 5$ est inversible, G et G' sont bien deux matrices génératrices d'un même code. □

4.3 Borne sur la distance minimale

On ne connaît la distance minimale des codes de Kerdock généralisés que dans le cas $p = k = 2$, autrement dit pour les codes de Kerdock eux-mêmes. Cependant, il existe une borne inférieure sur cette distance minimale dans le cas $p = 2$ (cf. [Car98, §IV, corollaire 1]). Suivant des techniques similaires, nous donnons une borne valable dans le cas général, celle dont on dispose pour $p = 2$ étant un raffinement. La preuve s'appuie sur l'écriture du poids homogène d'une fonction à valeur dans $\mathbb{Z}_{p^k}$ à l'aide de sommes exponentielles.

Lemme 4.12 *Soit une fonction* $f : E \mapsto \mathbb{Z}_{p^k}$. *En notant*

$$w_{hom}(f) = \sum_{e \in E} w_{hom}(f(e)) \ ,$$

on a

$$w_{hom}(f) = |E| \cdot p^{k-2}(p-1) - \frac{1}{p} \sum_{\lambda \in \mathbb{Z}_{p^k}{}^*} \sum_{e \in E} \omega^{\lambda \cdot f(e)} \ ,$$

où ω *désigne une racine primitive* p^k*-ième de l'unité et* $\mathbb{Z}_{p^k}{}^*$ *est l'ensemble des éléments inversibles de* $\mathbb{Z}_{p^k}$.

Preuve. Pour tout $a \in \mathbb{Z}_{p^k}$ on a

$$\sum_{\lambda \in \mathbb{Z}_{p^k}} \omega^{\lambda \cdot a} = \begin{cases} p^k & \text{si } a = 0 \ , \\ 0 & \text{sinon} \ , \end{cases}$$

et

$$\sum_{\lambda \in p \cdot \mathbb{Z}_{p^k}} \omega^{\lambda \cdot a} = \begin{cases} p^{k-1} & \text{si } p \cdot a = 0 \ , \\ 0 & \text{sinon} \ . \end{cases}$$

On peut donc écrire (cf. page 52)

$$\begin{aligned} w_{hom}(a) &= p^{k-2}(p-1) + \frac{1}{p} \sum_{\lambda \in p \cdot \mathbb{Z}_{p^k}} \omega^{\lambda \cdot a} - \frac{1}{p} \sum_{\lambda \in \mathbb{Z}_{p^k}} \omega^{\lambda \cdot a} \\ &= p^{k-2}(p-1) - \frac{1}{p} \sum_{\lambda \in \mathbb{Z}^*_{p^k}} \omega^{\lambda \cdot a} \ . \end{aligned}$$

En d'autres termes, le poids de a est le poids d'un élément non divisible par p^{k-1}, c'est-à-dire $p^{k-2}(p-1)$, plus le nombre p^{k-2} si a est divisible par p^{k-1}, moins p^{k-1} si a est nul. Compte tenu de notre définition de w_{hom} pour f, nous obtenons bien l'égalité annoncée :

$$w_{hom}(f) = |E| \cdot p^{k-2}(p-1) - \frac{1}{p} \sum_{e \in E} \sum_{\lambda \in \mathbb{Z}^*_{p^k}} \omega^{\lambda \cdot f(e)} \ .$$

□

Dans le cas du code de Kerdock généralisé, on a $f \in \mathcal{F}(p^k, m)$ et la somme exponentielle entre dans le cadre d'application de l'adaptation par Kumar *et al.* de la borne de Carlitz-Uchiyama aux anneaux de Galois [KHC95]. Dans notre cas, cette borne s'exprime de la manière suivante :

LEMME 4.13 ([KHC95, §I.C, TH. 1]) *Pour toute fonction* $f \in \mathcal{F}(p^k, m)$ *non constante et pour tout* $\lambda \in \mathbb{Z}_{p^k}{}^*$, *on a*

$$\left| \sum_{e \in \mathcal{T}} \omega^{\lambda \cdot f(e)} \right| \leq (p^{k-1} - 1) p^{\frac{m}{2}} \quad .$$

En combinant ces deux lemmes, nous obtenons la borne sur la distance minimale des codes $\mathcal{K}(p^k, m)$.

THÉORÈME 4.14 *La distance minimale du code de Kerdock généralisé* $\mathcal{K}(p^k, m)$ *est supérieure ou égale à*

$$(p-1) \cdot \left(p^{m+k-2} - p^{\frac{m}{2}+k-2} \cdot \left(p^{k-1} - 1 \right) \right) \quad .$$

PREUVE. Le poids minimal du code $\mathcal{K}(p^k, m)$ est le minimum des poids homogènes (non nuls) de $\mathcal{F}(p^k, m)$. En prenant $E = \mathcal{T}$, les lemmes 4.12 et 4.13 permettent d'obtenir la borne annoncée pour toutes les fonctions non constantes. Il reste alors à vérifier que le poids homogène d'une fonction constante, non nulle, est supérieur à cette borne inférieure, ce qui est clair puisqu'il vaut soit $p^m \cdot p^{k-1}$, soit $p^m \cdot p^{k-2}(p-1)$. □

Dans le cas où $p = 2$, il est possible de raffiner cette borne en utilisant une généralisation du théorème de McEliece aux codes cycliques sur les entiers 2-adiques (cf. [CLP97]).

THÉORÈME 4.15 ([CAR98, §IV, COR. 1]) *La distance minimale du code de Kerdock généralisé* $\mathcal{K}(2^k, m)$ *est supérieure ou égale à*

$$2^{m+k-2} - 2^{k+\left\lceil \frac{m}{2^{k-1}} \right\rceil - 4} \cdot \left\lfloor 2^{\frac{m}{2}+2-\left\lceil \frac{m}{2^{k-1}} \right\rceil} \left(2^{k-1} - 1 \right) \right\rfloor \quad .$$

Cette borne donne la distance minimale exacte lorsque $k = 2$ et $m \geq 3$ est impair, *i.e.* pour les codes de Kerdock. Nous verrons dans la section suivante que les résultats obtenus pour les distances minimales en petite longueur nous permettent d'affirmer que ce n'est plus le cas pour $k \geq 3$.

4.4 Distance minimale en petite longueur

Nous avons calculé la distance minimale des codes de Kerdock généralisés pour certaines longueurs, avec $p = 2$, 3 et 5. Les résultats obtenus figurent dans les tables 4.2, 4.7 et 4.9, respectivement pour $p = 2$, 3, et 5. Ils ont été obtenus par deux implémentations en langage C d'un parcours exhaustif des mots du code. La première implémentation est générique et s'applique à tout p premier. Elle calcule l'ensemble des combinaisons linéaires des lignes de la matrice génératrice sur $\mathbb{Z}_{p^k}$ à l'aide d'un code de Gray et calcule le poids homogène de chacune des combinaisons au fur et à mesure, afin de trouver le minimum non nul. Cela permet de passer d'un mot à un autre en n'effectuant qu'une seule addition vectorielle. Le nombre de mots étant $p^{k(m+1)}$ et ces derniers étant de longueur p^m, la complexité du calcul de la distance minimale de $\mathcal{K}(p^k, m)$ est donc en $p^m \cdot p^{k(m+1)}$. Une telle complexité ne permet pas de tester des paramètres très grands et nous avons donc dû nous restreindre à des valeurs relativement modestes.

La seconde implémentation est spécifique au cas $p = 2$. Elle reprend le principe général de la première, mais plus finement : elle représente la matrice génératrice sous une forme compacte – qui n'est possible que pour $p = 2$ – permettant de manipuler plusieurs coordonnées en même temps, aussi bien pour les additions que pour le calcul du poids. Enfin, elle ne parcourt pas exactement l'ensemble du code. En effet, soit $\mathbf{c} \in \mathbf{C}_{p^k}$ et considérons l'ensemble

$$\mathbf{c} + 2^i \mathbf{C}_{p^k} = \left\{ c + 2^i \cdot z \mid z \in \mathbf{C}_{p^k} \right\} \ ,$$

où i est un entier inférieur à k. Alors, $w_H(\mathbf{c} \mod 2^i)$ est un minorant du poids homogène minimal de cet ensemble. Donc, si le poids de Hamming de $\mathbf{c} \mod 2^i$ est supérieur au minimum du poids homogène déjà rencontré, il est inutile de parcourir les mots de $\mathbf{c} + 2^i \mathbf{C}_{p^k}$. Toutefois, bien que nettement plus efficace, cette dernière implémentation n'échappe pas à une croissance exponentielle du temps de calcul. Par exemple, pour obtenir le poids minimal de $\mathcal{K}(2^3, 10)$, il nous a fallu 6 heures et pour celui de $\mathcal{K}(2^3, 11)$, 96 heures [1]. Or les mots de $\mathcal{K}(2^3, 11)$ sont 2 fois plus longs et 8 fois plus nombreux que ceux de $\mathcal{K}(2^3, 10)$, ce qui donne bien un facteur 16. Nous avons également calculé la distance minimale du $\mathbb{Z}_{2^k}$-dual des codes de Kerdock généralisés, $\mathcal{P}(2^k, m)$, à l'aide du théorème 3.15 page 56 lorsque cela nous a été possible. Cela nécessite de connaître l'énumérateur des poids symétrisés de $\mathcal{K}(2^k, m)$. Nous ne pouvons donc plus éviter de parcourir tout le code. De plus, il faut gérer un polynôme multivarié, dans lequel nous devons faire une substitution de variables pour obtenir le poids minimal de $\mathcal{P}(2^k, m)$ – cette étape de la substitution a été faite avec le logiciel Maple. Cela fait que nous avons pu

[1] Pour être tout à fait précis, il convient d'ajouter que ces temps de calcul ont été obtenus avec des processeurs Pentium 4 cadencés à 2.60 GHz et disposant de 1 Go de RAM.

aller encore moins loin pour le code de Preparata généralisé, le calcul de la relation donnée du théorème 3.15 page 56 n'étant plus praticable.

Nous distinguons le cas binaire des autres pour essentiellement trois raisons. En premier lieu, nous avons réalisé une implémentation plus fine, ce qui est principalement lié au fait que le cas où $p = 2$ s'y prête le mieux. On peut utiliser efficacement les écritures en base 2. Ensuite, c'est dans ce cas que la complexité croît le moins rapidement et par conséquent c'est là que nous pouvons aller le plus loin. Enfin, nous disposons d'une borne inférieure sur la distance minimale (cf. théorème 4.15) plus précise que dans le cas général et qui pour $p^k = 8$ donne

$$2^{m+1} - 2^{\lceil \frac{m}{4} \rceil - 1} \cdot \left\lfloor 3 \cdot 2^{\frac{m}{2} - \lceil \frac{m}{4} \rceil + 2} \right\rfloor \quad .$$

Or il existe des codes binaires, les duaux des codes BCH 3-correcteurs, qui ont une longueur et un cardinal comparables à ceux des codes $\mathcal{K}(2^3, m)$, dont la distance minimale est proche de cette borne :

- pour m pair $\left[2^{m+2}, 3m + 6, 2^{m+1} - 2^{(m+4)/2}\right]$ (cf. [Ber68]) ;
- pour m impair $\left[2^{m+2} - 1, 3m + 7, 2^{m+1} - 2^{(m+3)/2}\right]$ (cf. [Kas69]).

D'autre part, ces codes figurent parmi les meilleurs codes linéaires connus pour les longueurs 31 et 127. Cette famille constitue donc une bonne référence pour juger de la qualité des codes de Kerdock généralisés $\mathcal{K}(2^3, m)$.

Cas binaire. La régularité de la distance minimale est ce qui ressort en premier lieu de la table 4.2 : pour m fixé, après le « saut » irrégulier entre $k = 2$ et $k = 3$, il suffit de doubler la distance minimale du code $\mathcal{K}(2^k, m)$ pour obtenir celle du code $\mathcal{K}(2^{k+1}, m)$. On peut remarquer que cela est vrai non seulement pour le Kerdock généralisé mais également pour son dual. On constate également que, pour $m = 3$, les codes de Kerdock généralisés et leurs $\mathbb{Z}_{2^k}$-duaux ont les mêmes paramètres, ce qui était prévisible puisque cela résulte simplement de la factorisation en trois facteurs de $X^7 - 1$ sur $\mathbb{Z}_2[X]$.

Pour juger de la qualité de ces codes, nous profitons de l'existence de sources détaillées pour les codes binaires et donnons différentes tables :

1. la table 4.3 donne les bornes connues sur les *codes binaires linéaires* de *longueurs* et de *cardinaux* égaux à ceux des codes $\mathcal{K}$ et $\mathcal{P}$. Cette table indique la distance minimale la plus grande possible, *i.e.* la borne supérieure, pour un code linéaire, ainsi que la distance minimale du meilleur code binaire linéaire connu lorsqu'elle est différente de la borne supérieure (extrait de la table de Brouwer, cf. [Bro98]).
2. la table 4.4 donne les paramètres du *code binaire* ayant le plus grand cardinal connu pour une *longueur* et une *distance minimale* égales à celles des codes $\mathcal{K}$ et $\mathcal{P}$ (ces données sont extraites de la table de Litsyn, cf. [Lit98]).

3. la table 4.5 donne des codes ayant même longueur (à une unité près lorsque m est pair) que les codes $\mathcal{K}(2^3, m)$ et un cardinal proche : il s'agit des duaux des codes BCH 3-correcteurs (voir [Kas69, Ber68] pour les paramètres de ces codes).

Les tables 4.3 et 4.4 montrent que pour les petites dimensions, les codes de Kerdock et de Preparata généralisés ne sont pas parmi les meilleurs, hormis dans le cas $k = 2$ avec m impair (cf. §4.1). On trouve même des codes linéaires plus performants dans plusieurs cas (par exemple $k = 3$ avec $m = 4, 5$ ou 6). D'autre part, la table 4.5 montre que pour $k = 3$, contrairement à ce que pouvait laisser supposer la borne inférieure sur la distance minimale rappelée plus haut, les codes de Kerdock généralisés sont moins bons que les duaux des codes BCH 3-correcteurs de même longueur : ils ont systématiquement un cardinal plus faible et une distance minimale moindre, sauf dans un cas, $\mathcal{K}(2^3, 3)$ qui a pour paramètres $\{32, 12, 10\}$. D'ailleurs, ce dernier code est intéressant car, bien que n'ayant pas une distance minimale strictement meilleure que celle des codes binaires linéaires de longueur 32 et de dimension 12, il les égale, ce qui est l'unique cas pour l'ensemble des paramètres que nous avons pu tester.

La table 4.6 indique la valeur de la borne sur la distance minimale (théorème 4.15) pour les cas pertinents [1]. Elle semble asymptotiquement assez bonne : l'erreur relative, $(\delta - b)/\delta$, avec δ distance minimale et b borne sur la distance minimale, décroît de façon monotone pour arriver à moins de 2% pour $\mathcal{K}(2^3, 10)$.

Cas général. Pour les cas où p est strictement supérieur à 2, nous donnons les distances minimales que nous avons obtenues et nous comparons le code de Kerdock généralisé $\mathcal{K}(p^k, m)$ avec le code BCH de longueur semblable, plus précisément de longueur $p^{m+k-1} - 1$, et de distance construite égale à la distance obtenue pour $\mathcal{K}(p^k, m)$. Ainsi, le code $\mathcal{K}(p^k, m)$ est comparé à un code de longueur inférieure et de distance minimale au moins aussi grande, puisque la distance construite constitue une borne inférieure sur la distance minimale d'un code BCH. On observe que systématiquement les codes BCH ont de meilleures distances et des cardinaux largement supérieurs – les paramètres de ces derniers ont été obtenus avec le logiciel MAGMA, pour la plupart par utilisation directe des primitives du logiciel. Nous ne donnons pas la valeur de la borne générale (cf. théorème 4.14) : pour les paramètres étudiés, elle n'est pas pertinente. Par exemple pour les codes $\mathcal{K}(3^2, m)$, $m \in [3, 7]$, l'erreur relative va de 52.6% à 42.6% (en décroissant strictement).

On constate encore la régularité de la croissance de la distance minimale

[1] Lorsque $k \geq 4$, la valeur de cette borne est négative pour les valeurs de nos paramètres. Pour $k = 2$, on sait qu'elle donne la distance minimale exacte (cf. §4.1).

lorsque k augmente : $\mathcal{K}(p^{k+1}, m)$ a une distance minimale p fois supérieure à celle de $\mathcal{K}(p^k, m)$. Ce phénomène a une traduction très simple lorsque l'on considère le code sur $\mathbb{Z}_{p^k}$. En normalisant le poids homogène w_{hom}, c'est-à-dire en prenant

$$w_{hn}(a) = \frac{1}{p^{k-2}} w_{hom}(a) \ ,$$

la distance (homogène normalisée) minimale du code $K(p^k, m)$, le code relevé de $\mathcal{K}(p^k, m)$, est indépendante de k pour tous les codes étudiés. On peut également remarquer que contrairement à $p = 2$, il n'y a pas de comportement particulier entre $k = 2$ et $k = 3$. Cela pourrait provenir de la bijectivité de Ψ lorsque $p^k = 4$, propriété que l'on perd dans tous les autres cas.

Distance minimale δ du Kerdock généralisé $\mathcal{K}(2^k, m)$.
Paramètres : $\left\{2^{(m+k-1)}, k(m+1), \delta\right\}$

m\k	2	3	4	5
3	{16, 8, 6}	{32, 12, 10}	{64, 16, 20}	{128, 20, 40}
4	{32, 10, 12}	{64, 15, 20}	{128, 20, 40}	{256, 25, 80}
5	{64, 12, 28}	{128, 18, 44}	{256, 24, 88}	{512, 30, 176}
6	{128, 14, 56}	{256, 21, 96}	{512, 28, 192}	{1024, 35, 384}
7	{256, 16, 120}	{512, 24, 212}	{1024, 32, 424}	
8	{512, 18, 240}	{1024, 27, 440}		
9	{1024, 20, 496}	{2048, 30, 928}		
10	{2048, 22, 992}	{4096, 33, 1888}		
11	{4096, 24, 2016}	{8192, 36, 3896}		

m\k	6	7	8
3	{256, 24, 80}	{512, 28, 160}	{1024, 32, 320}
4	{512, 30, 160}		

Distance minimale δ du Preparata généralisé $\mathcal{P}(2^k, m)$.
Paramètres : $\left\{2^{(m+k-1)}, k\left(2^m - (m+1)\right), \delta\right\}$

m\k	2	3	4	5
3	{16, 8, 6}	{32, 12, 10}	{64, 16, 20}	{128, 20, 40}
4	{32, 22, 4}	{64, 33, 8}	{128, 44, 16}	{256, 55, 32}
5	{64, 52, 6}	{128, 78, 10}	{256, 104, 20}	{512, 130, 40}
6	{128, 114, 4}	{256, 171, 8}	{512, 228, 16}	
7	{256, 240, 6}	{512, 360, 10}	{1024, 480, 20}	
8	{512, 494, 4}	{1024, 741, 8}		
9	{1024, 1004, 6}	{2048, 1506, 10}		
10	{2048, 2026, 4}			

m\k	6	7
3	{256, 24, 80}	{512, 28, 160}
4	{512, 66, 64}	

TAB. 4.2 – Distance minimale du code de Kerdock généralisé ainsi que de son dual en petite longueur. Rappelons que la notation $\{n, \ell, \delta\}$ signifie, pour un code $\mathbb{Z}_{2^k}$-linéaire, que ses paramètres sont $(n, 2^\ell, \delta)$, c'est-à dire qu'il est de longueur n sur $\mathbb{Z}_2$, de cardinal 2^ℓ et de distance minimale δ.

Borne sur la plus grande distance minimale possible pour un code binaire linéaire ayant mêmes longueur et dimension que le code $\mathcal{K}(2^k, m)$

$m\backslash k$	2	3	4	5	6
3	5	10	24	$48-53$	$100-114$
4	12	24	$48-53$	$100-114$	
5	$25-26$	$48-54$	$100-114$		
6	$56-57$	$112-116$			
7	$113-120$				

Borne sur la plus grande distance minimale possible pour un code binaire linéaire ayant mêmes longueur et dimension que le code $\mathcal{P}(2^k, m)$

$m\backslash k$	2	3	4	5	6
3	5	10	24	$48-53$	$100-114$
4	5	$12-114$	$28-38$	$68-96$	
5	5	$16-22$	$46-71$		
6	5	$24-34$			
7	5				

TAB. 4.3 – Extrait de la table de Brouwer (binaire) : morceaux choisis de la table des meilleurs codes binaires linéaires connus et des bornes sur leur distance minimale. La notation $b_{min}-b_{max}$ signifie que l'on connaît un code binaire linéaire de distance minimale b_{min} et que la borne supérieure la plus fine que l'on connaisse est b_{max}. Lorsque $b_{min} = b_{max} = b$, nous indiquons simplement b.

Meilleur code binaire connu de mêmes longueur et distance minimale que le code $\mathcal{K}(2^k, m)$

$m\backslash k$	2	3	4
3	$\{16, 8, 6\}$	$\{32, 13, 10\}$	$\{64, 19, 20\}$
4	$\{32, 11, 12\}$	$\{64, 19, 20\}$	
5	$\{64, 12, 28\}$		

Meilleur code binaire connu de mêmes longueur et distance minimale que le code $\mathcal{P}(2^k, m)$

$m\backslash k$	2	3	4
3	$\{16, 8, 6\}$	$\{32, 13, 10\}$	$\{64, 19, 20\}$
4	$\{32, 26, 4\}$	$\{64, 47, 8\}$	$\{128, 78, 16\}$
5	$\{64, 52, 6\}$	$\{128, 99, 10\}$	$\{256, 187, 20\}$
6	$\{128, 120, 4\}$	$\{256, 238, 8\}$	$\{512, 448, 16\}$
7	$\{256, 250, 6\}$	$\{512, 476, 10\}$	
8	$\{512, 502, 4\}$		

TAB. 4.4 – Extrait de la table de Litsyn : morceaux choisis de la table des meilleurs codes binaires connus. La notation $\{n, \ell, \delta\}$ a la même signification pour les codes $\mathbb{Z}_{2^k}$-linéaires : elle désigne une code de longueur n, de cardinal 2^ℓ et de distance minimale δ.

Dual du code BCH 3-correcteurs de longueur $2^{m+2} - 1$ (m impair)

m	$\left[2^{m+2} - 1, 3m + 6, 2^{m+1} - 2 \cdot 2^{\frac{m+1}{2}}\right]$	$\mathcal{K}(2^3, m)$
3	$[31, 15, 8]$	$\{32, 12, 10\}$
5	$[127, 21, 48]$	$\{128, 18, 44\}$
7	$[511, 27, 224]$	$\{512, 24, 212\}$
9	$[2047, 33, 960]$	$\{2048, 30, 928\}$

Dual du code BCH 3-correcteurs étendu de longueur 2^{m+2} (m pair)

m	$\left[2^{m+2}, 3m + 7, 2^{m+1} - 2 \cdot 2^{\frac{m+2}{2}}\right]$	$\mathcal{K}(2^3, m)$
4	$[64, 19, 16]$	$\{64, 15, 20\}$
6	$[256, 25, 96]$	$\{256, 21, 96\}$
8	$[1024, 31, 448]$	$\{1024, 27, 440\}$
10	$[4096, 37, 1920]$	$\{4096, 33, 1888\}$

TAB. 4.5 – Paramètres des duaux des codes BCH 3-correcteurs de longueur $2^{m+2} - 1$ pour m impair et des duaux des codes BCH 3-correcteurs étendus de longueur 2^{m+2} pour m pair.

m	3	4	5	6	7	8	9	10
δ	10	20	44	96	212	440	928	1888
borne (Th. 4.15)	0	8	32	80	190	416	892	1856
erreur (%)	–	60	27.3	16.7	10.4	5.5	3.9	1.7

TAB. 4.6 – Borne sur la distance minimale (cf. théorème 4.15) et distance minimale exacte δ pour le code $\mathcal{K}(2^3, m)$.

Distance minimale δ du code Kerdock généralisé $\mathcal{K}(3^k, m)$
Paramètres : $\left\{3^{(m+k-1)}, k(m+1), \delta\right\}$

m\k	2	3	4
3	{81, 8, 42}	{243, 12, 126}	{729, 16, 378}
4	{243, 10, 138}	{729, 15, 414}	
5	{729, 12, 450}		
6	{2187, 14, 1368}		
7	{6561, 16, 4248}		

TAB. 4.7 – Distance minimale du code de Kerdock généralisé en petite longueur.

Paramètres des codes BCH comparables aux codes de Kerdock généralisés $\mathcal{K}(3^k, m)$

m\k	2	3	4
3	[80, 11, 44]	[242, 21, 131]	[728, 39, 392]
4	[242, 11, 152]	[728, 18, 455]	
5	[728, 18, 455]		
6	[2186, 22, 1376]		
7	[6560, 21, $\geq$ 4292]		

TAB. 4.8 – Paramètres des codes BCH sur $\mathbb{Z}_3$ de longueur $3^{m+k-1} - 1$ et de distances construites égales aux distances minimales des codes $\mathcal{K}(3^k, m)$.

Distance minimale δ du code Kerdock généralisé $\mathcal{K}(5^k, m)$
Paramètres : $\left\{5^{(m+k-1)}, k(m+1), \delta\right\}$

$m\backslash k$	2	3
3	$\{625, 8, 460\}$	$\{3125, 12, 2300\}$
4	$\{3125, 10, 2380\}$	
5	$\{15625, 12, 12020\}$	

TAB. 4.9 – Distance minimale du code de Kerdock généralisé en petite longueur.

Paramètres des codes BCH comparables aux codes de Kerdock généralisés $\mathcal{K}(5^k, m)$

$m\backslash k$	2	3
3	$[624, 16, 468]$	$[3124, 32, 2343]$
4	$[3124, 11, 2474]$	
5	$[15624, 18, \geq 12369]$	

TAB. 4.10 – Paramètres des codes BCH sur $\mathbb{Z}_5$ de longueur $5^{m+k-1} - 1$ et de distances construites égales aux distances minimales des codes $\mathcal{K}(5^k, m)$.

Chapitre 5

Relevés des codes de résidus quadratiques

Les résultats du chapitre précédent ne sont pas ceux que l'on pouvait espérer et cela pose la question de la pertinence de la notion de $\mathbb{Z}_{p^k}$-linéarité. Certes, il existe de très bons codes $\mathbb{Z}_4$-linéaires, avec des constructions simples, et la $\mathbb{Z}_4$-linéarité permet d'expliquer algébriquement certaines de leurs propriétés qui jusque-là semblaintt étranges. Mais il est légitime de se demander ce qu'il en est lorsque p^k est différent de 4, d'autant plus après les résultats décevants que l'on a obtenus pour la distance minimale des codes de Kerdock généralisés.

Il existe des codes $\mathbb{Z}_8$ et $\mathbb{Z}_9$-linéaires, en fait $\mathbb{Z}_8$ et $\mathbb{Z}_9$-cycliques, dont les paramètres dépassent ceux des meilleurs codes précédemment connus, linéaires ou non. L'existence de ces deux codes, dus à Duursma *et al.* pour le $\mathbb{Z}_8$-cyclique (cf. [DGL$^+$01]), et à Greferath et Schmidt pour le $\mathbb{Z}_9$-cyclique (cf. [GS99]), justifie la poursuite de cette approche.

Les codes de Duursma *et al.*, et de Greferath et Schmidt sont obtenus par relèvement de Hensel des codes de Golay binaire et ternaire. Les codes de Golay étant des cas particuliers des codes de résidus quadratiques, il est naturel de procéder de même avec cette classe de codes. Nous commençons par présenter les relevés des codes de Golay puis nous donnons les résultats obtenus avec les codes de résidus quadratiques.

5.1 Code de Duursma *et al.* [DGL$^+$01]

Dans [DGL$^+$01], I.M. Duursma, M. Greferath, S.N. Litsyn et S.E. Schmidt construisent un code binaire $\mathcal{G}$ de paramètres $\{96, 37, 24\}$. Cette construction repose sur un code $\mathbb{Z}_8$-linéaire, que nous noterons $\mathcal{C}$, de paramètres $\{96, 36, 24\}$. Jusque-là, le meilleur code binaire connu de longueur 96 et de distance minimale 24 n'avait que 2^{33} éléments. Leur code $\mathcal{G}$ en a donc 16 fois plus, et le code G en a déjà 8 fois plus. Ce faisant, $\mathcal{C}$ est le premier exemple, et jusqu'à présent le seul, de code $\mathbb{Z}_8$-linéaire — de manière plus générale $\mathbb{Z}_{2^k}$-linéaire avec $k > 2$ — à être strictement meilleur que les codes linéaires.

Le code $\mathcal{G}$ est actuellement dans la table de Litsyn, table des meilleurs codes binaires connus.

Pour obtenir leur code, les auteurs relèvent à $\mathbb{Z}_8$ le polynôme générateur d'un code cyclique binaire connu sous le nom de code de Golay binaire de longueur 23 [MS96, chap. 16, §2]. Ce code est de dimension 12 et est bien connu pour avoir la meilleure distance minimale possible pour un code $[23, 12]$, à savoir 7, qui est la valeur de la borne de Hamming pour un code de longueur 23 et de cardinal 2^{12}. Après relèvement à $\mathbb{Z}_8$, ils obtiennent un code cyclique $\mathbf{C}_8$ de longueur 23 et de dimension 12 sur l'anneau $\mathbb{Z}_8$. Ils étendent ce code en rajoutant à chaque mot un symbole de parité qui est défini comme l'opposé de la somme des coordonnées du mot (cf. §4.2). Le code étendu $\mathbf{C}_8^+$ est alors de longueur 24 et de dimension 12 sur $\mathbb{Z}_8$. Pour trouver la distance minimale de $\mathbf{C}_8^+$, ils calculent le polynôme énumérateur des poids homogènes en passant en revue tous les mots de code à l'aide d'un ordinateur.

Le polynôme générateur du code de Golay binaire de longueur 23 est

$$g(X) = X^{11} + X^9 + X^7 + X^6 + X^5 + X + 1 \ ,$$

ce qui donne après relèvement à $\mathbb{Z}_8$

$$g^{(3)}(X) = X^{11}+2X^{10}+7X^9+4X^8+3X^7+3X^6+7X^5+2X^4+4X^3+4X^2+X+7 \ .$$

Le code $\mathbf{C}_8$ est donc $(g^{(3)}) \subset \mathbb{Z}_8[X]/(X^{23}-1)$, et le code étendu $\mathbf{C}_8^+$ est défini par

$$\mathbf{C}_8^+ = \left\{ (c_\infty, c_0, \ldots, c_{22}) \;\middle|\; (c_0, \ldots, c_{22}) \in \mathbf{C}_8 \text{ et } c_\infty + c_0 + \cdots + c_{22} = 0 \right\} \ .$$

Le polynôme énumérateur des poids homogènes de ce code est

$$\begin{aligned} hW_{\mathbf{C}_8^+}(X, Y) = {} & X^{96} + 255024X^{72}Y^{24} + 123648X^{70}Y^{26} \\ & + 5308032X^{68}Y^{28} + 10427648X^{66}Y^{30} + 63246711X^{64}Y^{32} \\ & + 218980608X^{62}Y^{34} + 429962368X^{60}Y^{36} + 1783127808X^{58}Y^{38} \\ & + 2047611984X^{56}Y^{40} + 6736260608X^{54}Y^{42} + 5912087808X^{52}Y^{44} \\ & + 12860133888X^{50}Y^{46} + 8584424464X^{48}Y^{48} + 128601338888X^{46}Y^{50} \\ & + 5912087808X^{44}Y^{52} + 6736260608X^{42}Y^{54} + 2047611984X^{40}Y^{56} \\ & + 1783127808X^{38}Y^{58} + 429962368X^{36}Y^{60} + 218980608X^{34}Y^{62} \\ & + 63246711X^{32}Y^{64} + 10427648X^{30}Y^{66} + 5308032X^{28}Y^{68} \\ & + 123648X^{26}Y^{70} + 255024X^{24}Y^{72} + Y^{96} \ . \end{aligned}$$

Le code $\mathcal{C} = \Psi(\mathbf{C}_8^+)$ est donc de longueur 96, de dimension 36 et de distance de Hamming minimale 24. Ce code est déjà supérieur aux codes binaires précédemment connus, mais on peut obtenir un code $\{96, 37, 24\}$, c'est-à-dire

doubler le cardinal sans réduire la distance minimale. Pour cela, Duursma *et al.* considèrent un translaté du code :

$$\mathbf{v} + \mathcal{C} = \{\mathbf{c} \mid \mathbf{c} - \mathbf{v} \in \mathcal{C}\} \ ,$$

où $\mathbf{v} = (1000\,1000\,1000 \cdots 1000) \in {\mathbb{F}_2}^{96}$. Le code $\mathcal{G}$ obtenu par réunion du code $\mathcal{C}$ et de son translaté $\mathbf{v} + \mathcal{C}$ est alors de cardinal $2^{36} + 2^{36} = 2^{37}$ et de distance minimale 24. En effet, si on considère deux mots $\mathbf{a}, \mathbf{b}$ de $\mathcal{G}$:

1. soit $\mathbf{a}$ et $\mathbf{b}$ sont tous les deux dans $\mathcal{C}$ ou dans $\mathbf{v} + \mathcal{C}$, auquel cas il est clair que $d_H(\mathbf{a}, \mathbf{b}) = w_H(\mathbf{a} - \mathbf{b}) \geq 24$ puisque le code $\mathcal{C}$ est de distance minimale δ ;
2. soit $\mathbf{a} \in \mathcal{C}$ et $\mathbf{b} \in \mathbf{v} + \mathcal{C}$ (quitte à permuter les rôles de $\mathbf{a}$ et $\mathbf{b}$). Dans ce cas, on peut écrire

$$\begin{aligned} \mathbf{a} &= (a_0, \ldots, a_{23}) \ , \\ \mathbf{b} &= (b_0 + 1000, \ldots, b_{23} + 1000) \ , \end{aligned}$$

avec $a_i, b_i \in \Psi(\mathbb{Z}_8) \subset \mathbb{Z}_2^4$. Les a_i et les b_i représentent des fonctions affines de 2 variables (cf. §3.1). Donc $a_i + b_i$ représente également une fonction affine de 2 variables. Par conséquent, $w_H(a_i + b_i)$ est pair. Il en résulte que $w_H(a_i + b_i + 1000)$ est non nul, et donc strictement positif. Finalement,

$$\begin{aligned} d_H(\mathbf{a}, \mathbf{b}) &= w_H((a_0 + b_0 + 1000, \ldots, a_{23} + b_{23} + 1000)) \\ &= \sum_{i=0}^{23} w_H(a_i + b_i + 1000) \\ &\geq 24 \ . \end{aligned}$$

Les auteurs ne donnent aucune raison particulière pour le choix du code de Golay binaire de longueur 23 et n'expliquent pas pourquoi le code obtenu après relèvement possède une bonne distance (homogène) minimale. Comme nous l'avons déjà mentionné, le code de Golay binaire de longueur 23 est connu pour être un code optimal – meilleure distance minimale pour un code $[23, 7]$ – mais surtout, il est *parfait*, c'est-à-dire que tout mot $\mathbf{v}$ de ${\mathbb{F}_2}^{23}$ peut être associé de manière unique à un mot de code $\mathbf{c}$ tel que $d_H(\mathbf{c}, \mathbf{v}) \leq e$ où e désigne la capacité de correction du code, dans le cas présent, $e = (7 - 1)/2 = 3$. Autrement dit, les boules fermées de rayon 3 centrées sur les mots de code forment une partition de ${\mathbb{F}_2}^{23}$. Il est possible que cette propriété soit à l'origine des bonnes propriétés du code relevé $\mathbf{C}_8$.

5.2 Code de Greferath et Schmidt [GS99]

Le code de Greferath et Schmidt, présenté dans [GS99] (en 1999), est également obtenu par relèvement d'un code cyclique. Mais, contrairement au cas précédent, le code cyclique en question n'est pas binaire : il est ternaire.

Greferath et Schmidt relèvent le polynôme générateur g du code de Golay ternaire $[11, 6, 5]$,

$$g(X) = X^5 + X^4 + 2X^3 + X^2 + 2 \ ,$$

à l'anneau $\mathbb{Z}_9$, obtenant

$$g^{(2)}(X) = X^5 + 7X^4 + 8X^3 + X^2 + 6X + 8 \ ,$$

qui engendre un code $\mathbf{C}_9$ cyclique sur $\mathbb{Z}_9$. Ils étendent $\mathbf{C}_9$ en ajoutant un symbole de parité, pour trouver le code

$$\mathbf{C}_9^+ = \left\{ (c_\infty, c_0, \ldots, c_{11}) \;\middle|\; (c_0, \ldots, c_{11}) \in \mathbf{C}_9 \text{ et } c_\infty + c_0 + \cdots + c_{11} = 0 \right\} \ .$$

Ils calculent alors le polynôme énumérateur des poids homogènes de ce code en utilisant un ordinateur et obtiennent :

$$\begin{aligned} hW_{\mathbf{C}_9^+}(X, Y) =& X^{36} + 4752X^{21}Y^{15} + 18800X^{15}Y^{21} \\ &+ 219456X^{12}Y^{24} + 16632X^6Y^{30} + 24Y^{36} \ . \end{aligned}$$

Le code $\Psi'(\mathbf{C}_9^+)$ est, à ce jour, le meilleur code ternaire connu de longueur 36 et de cardinal 3^{12}, sa distance de Hamming minimale étant 15 puisque Ψ' conserve les distances.

Là encore, les auteurs ne donnent aucune justification pour les bonnes propriétés de ce code, mais comme dans le cas binaire, le code de Golay ternaire de longueur 11 est parfait, *i.e.* les boules de rayon $2 = (5-1)/2$ centrées sur les mots de code forment une partition de $\mathbb{F}_3^{11}$.

5.3 Relevés des codes de résidus quadratiques

Les deux codes de Golay utilisés précédemment font en fait partie d'une famille de codes cycliques plus large, celle des codes de résidus quadratiques.

Ces codes ne sont définis que pour certaines longueurs : si p (premier) désigne le cardinal du corps fini servant d'alphabet, la longueur n doit être un nombre premier pour lequel p est un résidu quadratique modulo n, *i.e.* on doit avoir $p \equiv x^2 \pmod{n}$ pour un certain entier x. Le polynôme générateur g_n du code de résidus quadratiques de longueur n (noté QR_n) sur $\mathbb{F}_p$ est alors défini par

$$g_n(X) = \prod_{r \in Q} (X - \alpha^r) \ ,$$

où α désigne une racine primitive de l'unité d'ordre n sur $\mathbb{F}_p$ et où Q est l'ensemble des résidus quadratiques modulo n, *i.e.*

$$Q = \{r^2 \pmod{n},\ r \neq 0\} \ .$$

Dans ces conditions, le polynôme g_n est bien à coefficients dans $\mathbb{F}_p$. Le code QR_n est de dimension $(n+1)/2$ et sa distance (de Hamming) minimale est supérieure où égale à $\sqrt{n}$ (voir [MS96, Ch. 16 §6]).

Nous nous sommes essentiellement intéressé au cas binaire, *i.e.* $p = 2$. Les raisons de cet intérêt particulier sont identiques à celles données pour les codes de Kerdock généralisés. Nous avons effectué plusieurs simulations pour obtenir les distances minimales des codes obtenus par relèvement de Hensel des codes de résidus quadratiques. Ces simulations résultent d'une adaptation des logiciels développés pour l'étude des codes $\mathcal{K}(p^k, m)$ et sont donc dès l'origine plus rapides pour le cas binaire. Mais, ce qui encore plus restrictif, lorsque p est strictement supérieur à 2, les paramètres des codes rendent très rapidement impossibles toute énumération des mots. Ainsi, par exemple, le code QR_{23} sur $\mathbb{Z}_3$ donne un code relevé sur $\mathbb{Z}_9$ de cardinal 3^{24}, c'est-à-dire ayant approximativement 2^{38} éléments. En fait, hormis le code de Greferath et Schmidt présenté dans la précédente section, dont nous avons pu vérifier la distance minimale, nous n'avons pu obtenir la distance minimale que d'un seul code, défini sur $\mathbb{Z}_3$ et de paramètres $\{42, 14, 15\}$, construit en étendant le relevé à $\mathbb{Z}_9$ du code ternaire QR_{13}, de paramètres $[13, 6, 5]$. Précisons que le meilleur code ternaire linéaire de longueur 42 et de dimension 14 a une distance minimale de 16. Le code obtenu est donc très proche.

Pour la suite de cette section, on prend $p = 2$. Par conséquent, QR_n désigne désormais le code de résidus quadratiques *binaire* de longueur n. Dans ce cas, la condition sur la longueur équivaut à avoir pour n un nombre premier de la forme $8m \pm 1$. Nous noterons $\mathrm{QR}_n^{(k)}$ le code relevé à l'anneau $\mathbb{Z}_{2^k}$ du code QR_n, *i.e.* le code cyclique sur $\mathbb{Z}_{2^k}$ dont le polynôme générateur $g_n^{(k)}$ est obtenu par relèvement de Hensel du polynôme g_n. Nous pensons que cette famille est une source potentiellement intéressante pour construire de bons codes. Les codes $\mathrm{QR}_n^{(2)}$ ont été étudiés par Bonnecaze *et al.* [BSC95] ($n = 17, 23$), Pless et Qian [PQ96] ($n = 31, 47$) et Calderbank *et al.* [CMK+96] ($n = 31$). Le code $\mathrm{QR}_{23}^{(3)}$ est celui qui a été utilisé par Duursma *et al.* dans [DGL+01] (cf. §5.1) et, à notre connaissance, c'est actuellement le seul bon code $\mathbb{Z}_8$-linéaire connu. La table 5.1 donne la distance minimale de l'image par l'application de Gray généralisée du code étendu, noté $\mathrm{QR}_n^{(k)+}$, du code $\mathrm{QR}_n^{(k)}$ pour $n = 17, 23, 31, 47$ et $k = 2, 3, 4$. Ces codes $\mathbb{Z}_{2^k}$-linéaires sont de longueur $2^{k-1} \cdot (n+1)$ et de dimension $k(n+1)/2$. La table 5.2 donne la distance minimale des meilleurs codes linéaires binaires connus de mêmes longueur et dimension. Ajoutons que les codes QR_n pour $n = 17, 23, 31, 47$ sont des codes binaires linéaires optimaux (voir [Bro98]).

Finalement, les résultats de cette section sont mitigés : il existe au moins un code $\mathbb{Z}_{2^k}$-linéaire, avec $k \geq 2$, strictement meilleur que tout code linéaire de mêmes longueur et cardinalité, celui de Duursma *et alii*. Cependant nous

n'en avons pas trouvé d'autre, alors que la famille de codes explorés était, potentiellement, un choix prometteur si on considère [BSC95, PQ96] où sont obtenus de bons codes sur $\mathbb{Z}_4$ avec les codes de résidus quadratiques, et bien entendu [DGL$^+$01] et [GS99]. Toutefois, les codes que nous avons obtenus à défaut de dépasser les meilleurs codes linéaires, les égalent. Ils ne peuvent donc pas être considérés comme mauvais.

D'autre part, les résultats numériques de la table 5.1 présentent une régularité déjà rencontrée au chapitre précédent : la distance minimale double lorsque k augmente de 1. Cela reste vrai pour $k = 2$, ce qui n'était pas le cas des codes de Kerdock généralisés.

n	$\mathbb{Z}_4$	$\mathbb{Z}_8$	$\mathbb{Z}_{16}$
17	$\{36, 18, \mathit{8}\}$	$\{72, 27, 16\}$	$\{144, 36, 32\}$
23	$\{48, 24, \mathit{12}\}$	$\{96, 36, \mathbf{24}\}$	$\{192, 48, \mathit{48}\}$
31	$\{64, 32, \mathbf{14}\}$	$\{128, 48, \mathit{28}\}$	$\{256, 64, \leq 56\}$
47	$\{96, 48, \mathbf{18}\}$	$\{192, 72, \mathit{36}\}$	

TAB. 5.1 – Distance minimale des codes $\Psi\left(\mathrm{QR}_n^{(k)+}\right)$. La notation $\{l, d, \delta\}$ désigne un code de longueur l, de cardinal 2^d et de distance minimale δ. La distance minimale est en italique lorsque qu'elle égale celle du meilleur code linéaire de même longueur et même cardinal, et en gras lorsqu'elle la dépasse.

n	$\mathbb{Z}_4$	$\mathbb{Z}_8$	$\mathbb{Z}_{16}$
17	$[36, 18, \mathit{8}]$	$[72, 27, 19]$	$[144, 36, 38]$
23	$[48, 24, \mathit{12}]$	$[96, 36, \mathbf{20}]$	$[192, 48, \mathit{48}]$
31	$[64, 32, \mathbf{12}]$	$[128, 48, \mathit{28}]$	$[256, 64, 62]$
47	$[96, 48, \mathbf{16}]$	$[192, 72, \mathit{36}]$	

TAB. 5.2 – Distance minimale des meilleurs codes binaires linéaires connus de même longueur et même cardinal que $\Psi\left(\mathrm{QR}_n^{(k)+}\right)$. La distance minimale est en italique lorsque qu'il y a égalité, et en gras lorsqu'elle est inférieure.

Chapitre 6

Construction de codes sur $\mathbb{Z}_p$ fondée sur les translatés de codes $\mathbb{Z}_{p^k}$-linéaires

Les résultats du chapitre 4 montrent que les cardinaux des codes $\mathcal{P}(2^k, m)$ sont notablement plus faibles, lorsque $k \geq 3$, que ceux des meilleurs codes linéaires. Cependant, ces codes et de manière plus générale les codes $\mathbb{Z}_{p^k}$-linéaires peuvent être améliorés très fortement : en effet, il est possible de trouver des translatés de ces codes qui soient suffisamment loin du code d'origine ; en considérant la réunion du code et de ses translatés, on obtient donc un code de mêmes longueur et distance minimale mais possédant beaucoup plus de mots de code. Cette technique a été utilisée dans le cas de $\mathbb{Z}_8$ et avec un seul translaté, par Duursma, Greferath, Litsyn et Schmidt dans [DGL+01].

Cette construction nous conduit à une borne sur le cardinal des codes $\mathbb{Z}_{p^k}$-linéaires. La construction faisant intervenir plusieurs paramètres, il est assez difficile de comparer les différentes versions possibles entre elles, mais également aux autres bornes connues. Afin de pallier, autant que faire se peut, ce problème nous donnons quelques graphiques.

6.1 Principe de la construction

Considérons un code $\mathcal{C}$ défini sur $\mathbb{Z}_p$, de distance minimale δ et ayant la propriété d'être un sous-ensemble de $\mathrm{GRM}(r, m)^n$, où $\mathrm{GRM}(r, m)$ désigne le code de Reed et Muller généralisé d'ordre r en m variables défini sur $\mathbb{Z}_p$ (voir définition 3.3 page 51). Remarquons que les codes $\mathbb{Z}_{p^k}$-linéaires entrent dans cette catégorie puisque l'image par l'application de Gray généralisée de l'anneau $\mathbb{Z}_{p^k}$ est $\mathrm{GRM}(1, k-1)$.

Nous cherchons à construire des translatés du code $\mathcal{C}$ qui soient suffisamment éloignés les uns des autres pour pouvoir obtenir, par réunion de ces translatés, un code ayant plus de mots que $\mathcal{C}$ mais conservant la

même distance minimale. Formellement, on souhaite construire un ensemble $\mathcal{T} \subset \mathbb{Z}_p^{n \cdot p^m}$ de cardinal aussi grand que possible tel que

$$\bigcup_{t \in \mathcal{T}} t + \mathcal{C}$$

soit de distance minimale δ. Cela équivaut à chercher $\mathcal{T}$ tel que

$$w_H(t + t' + c + c') \geq \delta$$

pour tous $t, t' \in \mathcal{T}$ et $c, c' \in \mathcal{C}$.

Cependant, nous allons être plus restrictif et imposer que cette inégalité soit vérifiée pour tout mot c dans $\mathrm{GRM}(r, m)^n$, et pas seulement dans $\mathcal{C}$. Ainsi, l'ensemble $\mathcal{T}$ ne dépend plus du code $\mathcal{C}$ lui-même mais uniquement de sa propriété d'inclusion dans $\mathrm{GRM}(r, m)^n$. On peut donc réécrire la condition $w_H(t + t' + c + c') \geq \delta$ en $w_H(t + t' + c'') \geq \delta$ puisque $c + c'$ est dans $\mathrm{GRM}(r, m)^n$. Nous allons construire $\mathcal{T}$ comme un code concaténé : un code interne $S \subset \mathbb{Z}_p^{p^m}$ et un code externe T de longueur n défini sur un corps fini de cardinal égal à celui de S. Donc,

$$\begin{aligned} \mathcal{T} &= T(S) \ , \\ &= \left\{ (\varphi(x_1), \ldots, \varphi(x_n)) \ \middle| \ (x_1, \ldots, x_n) \in T \right\} \ , \end{aligned}$$

où $\varphi : \mathbb{F}_{|S|} \to S$ est une bijection quelconque. Clairement, une première condition apparaît sur S : son cardinal doit être une puissance d'un nombre premier. Pour assurer une distance minimale au moins égale à δ entre les translatés $t + \mathrm{GRM}(r, m)^n$, nous allons imposer une autre condition sur S :

LEMME 6.1 *Soit S un code de longueur p^m sur $\mathbb{F}_p$, de cardinal p^l tel que*

$$\forall z \in \mathrm{GRM}(r, m), \forall (x, y) \in S \times S, x \neq y, \qquad w_H(x + y + z) \geq d_S \qquad (*)$$

Soit T un code sur $\mathbb{F}_{p^l}$ de longueur n et de distance minimale d_T. On pose $\mathcal{T} = T(S)$. Alors la distance entre deux translatés $t + \mathrm{GRM}(r, m)^n$ et $t' + \mathrm{GRM}(r, m)^n$ pour $t, t' \in \mathcal{T}$, $t \neq t'$, est supérieure ou égale à $d_S \cdot d_T$.

PREUVE. L'hypothèse sur S signifie que les translatés de $\mathrm{GRM}(r, m)$ selon les mots de S sont au moins distants de d_S les uns des autres. Soient $\mathbf{a} = (a_1, \ldots, a_n), \mathbf{b} = (b_1, \ldots, b_n)$, avec les a_i, b_i dans $\mathrm{GRM}(r, m) \subset {\mathbb{F}_p}^{p^m}$. Par abus de notation, nous notons φ l'application de ${\mathbb{F}_{|S|}}^n \to S^n$ qui étend, coordonnée par coordonnée, la bijection de $\mathbb{F}_{|S|} \to S$. Soient $x, x' \in T$, $x \neq x'$, posons $t = \varphi(x), t' = \varphi(x')$. Nous avons,

$$w_H(\mathbf{a} + t + \mathbf{b} + t') = \sum_{i=0}^{n} w_H(a_i + \varphi(x_i) + b_i + \varphi(x'_i)) \ .$$

On peut écrire

$$w_H(\mathbf{a}+\mathbf{t}+\mathbf{b}+\mathbf{t}') \geq \sum_{x_i \neq x_i'} w_H(a_i + b_i + \varphi(x_i) + \varphi(x_i')) \ .$$

Par linéarité de $\mathrm{GRM}(r,m)$, la somme $a_i + b_i$ est dans $\mathrm{GRM}(r,m)$ et par hypothèse sur S, on déduit

$$w_H(\mathbf{a}+\mathbf{t}+\mathbf{b}+\mathbf{t}') \geq d_T \cdot d_S \ .$$

□

THÉORÈME 6.2 *Soit* $\mathcal{C} \subset \mathrm{GRM}(r,m)^n$ *de distance minimale* d. *Avec les notations et hypothèses du lemme 6.1, le code*

$$\mathcal{G} = \bigcup_{t \in \mathcal{T}} \mathbf{t} + \mathcal{C}$$

est de cardinal $|T| \cdot |\mathcal{C}|$ *et de distance minimale supérieure ou égale à* $\min(d, d_T \cdot d_S)$.

PREUVE. Le lemme précédent prouve que les translatés sont au moins distants de $d_T \cdot d_S$ et la distance entre deux mots d'un même translaté est supérieure ou égale à la distance minimale du code $\mathcal{C}$. □

Le code de Reed et Muller généralisé d'ordre $r+a$ en m variables défini sur $\mathbb{Z}_p$, $\mathrm{GRM}(r+a,m)$, peut être construit par réunion de p^ℓ translatés du code $\mathrm{GRM}(r,m)$ avec $\ell = \dim(r+a,m) - \dim(r,m)$ où

$$\dim(r,m) = \sum_{i=0}^{r} \sum_{j=0}^{m} (-1)^j \binom{m}{j} \binom{i - j\cdot p + m - 1}{i - j\cdot p}$$

qui est la dimension du code $\mathrm{GRM}(r,m)$. La construction dans le cas binaire est exposée dans [MS96, chap. 13, §3] ; le cas général, qui n'est qu'une simple transposition, peut être trouvé dans [AK98, §5.2]. Prenons pour S un système de représentants des p^ℓ translatés de $\mathrm{GRM}(r,m)$ dans $\mathrm{GRM}(r+a,m)$, autrement dit S contient exactement un mot de chacun des translatés. Cet ensemble S a la propriété $(*)$ requise par le lemme 6.1 pour $d_S = (p-f)p^{m-e}$, où e et f sont les entiers positifs tels que $r = e(p-1)+f$ avec $f < p-1$. En effet, les éléments de S sont des mots de $\mathrm{GRM}(r+a,m)$ qui est un code de distance minimale $(p-f)p^{m-e-1}$ (cf. [AK98, th. 5.25]).

Notons T un code sur $\mathbb{F}_{p^\ell}$, de longueur n et de distance de Hamming minimale $d_T \geq \delta/d_S$. Le théorème 6.2 nous permet alors de construire un code $\mathcal{G}$ ayant $|T|$ fois plus de mots que $\mathcal{C}$, à condition qu'il existe bien un code T de distance minimale au moins d_T – ce qui n'est plus le cas pour $n < d_S \cdot \delta$. D'autre part, il convient de remarquer que le code $\mathcal{G}$ obtenu est dans $\mathrm{GRM}(r+a,m)^n$ et que nous pouvons donc appliquer la même construction à ce code en utilisant d'autres codes S et T. On obtient ainsi une construction itérative.

EXEMPLE 6.3 Pour $\mathbb{Z}_8$, on a $r = 1$, $m = 2$ et $S = \{0000, 1000\}$. Si le code $\mathcal{C}$ a pour paramètres $\{96, 36, 24\}$, il n'y a qu'un seul code T de longueur 24 et de distance 24 sur $\mathbb{Z}_2$, le code trivial à deux éléments. Le code $\mathcal{G}$ obtenu a alors deux fois plus de mots que $\mathcal{C}$. C'est sous cette forme qu'a été utilisée cette construction dans [DGL+01]. □

Nous avons utilisé comme code S un ensemble de représentants des translatés de $\mathrm{GRM}(r, m)$ dans $\mathrm{GRM}(r + a, m)$. Toutefois, ce n'est pas la seule possibilité. Par exemple, pour $p = 2$, lorsque m est pair et $r = a = 1$, il est possible de considérer un ensemble de représentants de $\mathrm{RM}(1, m)$ dans le code de Kerdock. Cela revient à prendre pour S un ensemble de mots à distance maximale de $\mathrm{RM}(1, m)$ (fonctions courbes) tel que la somme de deux de ses éléments soit toujours à distance maximale. Cela réduit le cardinal de S, qui passe de $2^{m(m-1)/2}$ à 2^m, mais conduit à une valeur de d_S presque deux fois plus grande, passant à $2^{m-1} - 2^{(m-2)/2}$ au lieu de 2^{m-1}.

6.2 QUELQUES APPLICATIONS

CAS $\mathbb{Z}_8$. Tout code $\mathbb{Z}_8$-linéaire est une partie de $\mathrm{RM}(1,2)^n$ pour un certain entier n. Par conséquent, nous avons $r = 1$ et le choix de a est restreint à $a = 2$, auquel cas $|S| = 2$ et le code T est binaire, de mêmes longueur et distance minimale que le code $\mathbb{Z}_8$-linéaire. La table 6.1 donne les paramètres des codes que l'on peut obtenir avec notre construction lorsque l'on prend pour $\mathcal{C}$ le code de Preparata généralisé $\mathcal{P}(2^3, m)$ et pour T le meilleur code binaire connu de longueur 2^m et de même distance minimale que $\mathcal{P}(2^3, m)$ (cf. §4.4 Tab. 4.2 page 73 et [Lit98]). L'amélioration est très nette. Cependant, bien que très proches, ces codes ne sont toujours pas aussi bons que les meilleurs codes linéaires. Nous pensons que cette construction, avec d'autres codes que les Preparata généralisés, peut permettre d'obtenir des codes dépassant les capacités des codes actuellement connus. Rappelons que la construction de Duursma *et al.* (cf. §5.1 et [DGL+01]) est une version simplifiée de notre construction (cf. exemple 6.3).

$\mathcal{C}$	$\{64, 33, 8\}$	$\{128, 78, 10\}$	$\{256, 171, 8\}$	$\{512, 360, 10\}$	$\{1024, 741, 8\})$
T	$\{16, 7, 8\}$	$\{32, 13, 10\}$	$\{64, 47, 8\}$	$\{128, 99, 10\}$	$\{256, 233, 8\}$
$\mathcal{G}$	$\{64, 40, 8\}$	$\{128, 91, 10\}$	$\{256, 218, 8\}$	$\{512, 459, 10\}$	$\{1024, 974, 8\}$

TAB. 6.1 – Exemples de codes obtenus par la construction du théorème 6.2 avec des codes $\mathbb{Z}_8$-linéaires. La notation $\{\ell, d, \delta\}$ désigne un code de longueur ℓ, de cardinal 2^d et de distance minimale δ.

Cas $\mathbb{Z}_{16}$. Les codes $\mathbb{Z}_{16}$-linéaires sont des parties de $\mathrm{RM}(1,3)^n$. Il y a alors deux possibilités pour choisir a :

- soit $a = 1$, ce qui signifie qu'on cherche des translatés du code dans $\mathrm{RM}(2,3)^n$ pour obtenir un code $\mathcal{G}$ de plus grand cardinal. Le code T est alors défini sur $\mathbb{F}_{2^3}$ puisque $\mathrm{RM}(2,3)$ est la réunion de 2^3 translatés de $\mathrm{RM}(1,3)$, et doit avoir une distance minimale au moins égale à $\lceil \delta/2 \rceil$. On peut alors éventuellement itérer la construction, c'est-à-dire chercher des translatés de $\mathcal{G}$ dans $\mathrm{RM}(3,3)^n = \mathbb{Z}_2^{8n}$, conduisant à un code $\mathcal{G}'$ de cardinal encore plus élevé. Cette fois-ci le code T' utilisé pour construire les translatés est un code binaire ($\mathrm{RM}(3,3)$ est formé de deux translatés de $\mathrm{RM}(2,3)$) et doit avoir une distance minimale au moins égale à δ.
- soit $a = 2$, ce qui revient à chercher directement des translatés du code dans l'espace tout entier, $\mathbb{Z}_2^{8n}$. Le code $\mathrm{RM}(3,3)$ étant constitué de 2^4 translatés de $\mathrm{RM}(1,3)$, T est défini sur $\mathbb{F}_{2^4}$ et doit avoir une distance minimale au moins égale à δ.

Pour illustrer le caractère itératif de notre construction, nous avons choisi $a = 1$. La table 6.2 donne les paramètres des codes obtenus en prenant $\mathcal{C} = \mathcal{P}(2^4, m)$. Nous avons également indiqué les paramètres des codes intermédiaires $\mathcal{G} \subset \mathrm{RM}(2,3)^{8n}$. Donc formellement,

$$\mathcal{G}' = \bigcup_{t' \in T'(S')} \left(t' + \bigcup_{t \in T(S)} (t + \mathcal{C}) \right) ,$$

pour S et S' des systèmes de représentant de $\mathrm{RM}(1,3)$ dans $\mathrm{RM}(2,3)$ et de $\mathrm{RM}(2,3)$ dans $\mathrm{RM}(3,3)$, respectivement.

$\mathcal{C}$	$\{128,44,16\}$	$\{256,104,20\}$	$\{512,228,16\}$	$\{1024,480,20\}$
T	$[16,8,8]$	$[32,19,10]$	$[64,51,8]$	$[128,110,10]$
$\mathcal{G}$	$\{128,68,16\}$	$\{256,161,20\}$	$\{512,381,16\}$	$\{1024,810,20\}$

T'	$\{16,1,16\}$	$\{32,2,21\}$	$\{64,28,16\}$	$\{128,71,20\}$
$\mathcal{G}'$	$\{128,69,16\}$	$\{256,163,20\}$	$\{512,409,16\}$	$\{1024,881,20\}$

Tab. 6.2 – Exemples de codes obtenus par itération de la construction du théorème 6.2 avec des codes $\mathbb{Z}_{16}$-linéaires.

Utilisation de codes de Reed-Solomon. Il est délicat de calculer les paramètres des codes obtenus en choisissant $a = 2$ et en conservant $\mathcal{C} = \mathcal{P}(2^4, m)$. En effet, il n'existe pas de table des meilleurs codes connus pour des corps ayant strictement plus de 9 éléments. Or dans ce cas le code T

est défini sur $\mathbb{F}_{2^4}$. Cependant, pour certaines valeurs des paramètres, il est possible de prendre un code de Reed-Solomon pour T.

Considérons un code $\mathcal{C} \in \mathrm{RM}(r,m)^n$ de distance minimale d et cherchons des translatés dans $\mathrm{RM}(r+a,m)^n$ pour un certain $a \geq 1$. L'ensemble S des représentants de $\mathrm{RM}(r,m)$ dans $\mathrm{RM}(r+a,m)$ a 2^l éléments avec $l = \sum_{i=1}^{a} \binom{m}{r+i}$. Le code T est alors défini sur $\mathbb{F}_{2^l}$, doit être de longueur n et avoir une distance minimale supérieure à $\lceil d \cdot 2^{r+a-m} \rceil$. Pour que T puisse être un code de Reed-Solomon (éventuellement étendu), on doit avoir $n \leq 2^l$. Sa dimension est alors $n - \lceil d \cdot 2^{r+a-m} \rceil$.

EXEMPLE 6.4 Nous allons illustrer l'utilisation de codes de Reed-Solomon en appliquant notre construction, dans sa version itérée, au code $\mathcal{C} = \mathcal{P}(2^5, 4)$, qui est un sous-ensemble de $\mathrm{RM}(1,4)^{16}$ de cardinal 2^{55} et distance 32 d'après la table 4.2 page 73. Les cardinaux des espaces quotients sont

RM(4,4)/RM(3,4)	2
RM(3,4)/RM(2,4)	2^4
RM(2,4)/RM(1,4)	2^6

Examinons l'ensemble des constructions possibles. En premier lieu, il faut éliminer toutes les constructions faisant intervenir un ensemble S de représentants d'un code $\mathrm{RM}(r,4)$ dans $\mathrm{RM}(4,4)$, et cela pour tout $r \in \{1,2,3\}$. En effet, on aurait alors $d_S = 1$, ce qui imposerait de choisir un code T de distance minimale $d_T = 32$, de manière à satisfaire l'inégalité $d_T \cdot d_S \geq 32$ pour appliquer le théorème 6.2 page 89. Or le code T est de longueur 16, ce qui impose $d_T \leq 16$.

Il ne reste alors que deux possibilités :

1. $\mathrm{RM}(1,4)^{16} \to \mathrm{RM}(2,4)^{16} \to \mathrm{RM}(3,4)^{16}$: de $\mathrm{RM}(1,4)^{16} \to \mathrm{RM}(2,4)^{16}$, notons S un système de représentants de $\mathrm{RM}(2,4)/\mathrm{RM}(1,4)$. On peut utiliser un code T de longueur 16 sur $\mathbb{F}_{2^6}$, distance minimale

$$d_{\min}(\mathcal{C})/d_S = 32/4 = 8$$

et donc de dimension $16 - 8 + 1 = 9$ sur $\mathbb{F}_{2^6}$. On obtient ainsi un code $\mathcal{G} \subset \mathrm{RM}(2,4)^{16}$ constitué de $2^{9 \cdot 6}$ translatés de $\mathcal{C}$. Puis pour $\mathrm{RM}(2,4)^{16} \to \mathrm{RM}(3,4)^{16}$, notons S' un système de représentant de $\mathrm{RM}(3,4)/\mathrm{RM}(2,4)$. On peut utiliser un code T' de longueur 16 sur $\mathbb{F}_{2^4}$, distance minimale $d_{\min}(\mathcal{G})/d_{S'} = 32/2 = 1$ et dimension $16-16+1 = 1$. Finalement le code $\mathcal{G}'$ obtenu est un code de longueur 256, cardinal $2^{55} \cdot 2^{9 \cdot 6} \cdot 2^4 = 2^{113}$ et distance minimale 32 (ajoutons que le meilleur code binaire linéaire de longueur 256 et cardinal 2^{113} est de distance minimale 44).

2. $\mathrm{RM}(1,4)^{16} \to \mathrm{RM}(3,4)^{16}$: continuons à noter S un ensemble de représentants du quotient $\mathrm{RM}(3,4)/\mathrm{RM}(1,4)$, T est de longueur 16 sur $\mathbb{F}_{2^{10}}$ et doit être de distance $d_{\min}(\mathcal{C})/d_S = 16$, il est donc de dimension 1. Le code obtenu a alors un cardinal de 2^{65} éléments.

□

6.3 Bornes sur le cardinal des codes $\mathbb{Z}_{p^k}$-linéaires

L'existence de la construction qui est présentée au début de ce chapitre nous permet de déduire une borne supérieure sur le cardinal d'un code $\mathcal{C} \subset \mathrm{GRM}(r,m)^n$, donc entre autres d'un code $\mathbb{Z}_{p^{m+1}}$-linéaire.

Proposition 6.5 *Soit $\mathcal{C} \subset \mathrm{GRM}(r,m)^n$ de distance minimale δ. On note $\mathrm{dist}(r,m)$ la distance minimale du code $\mathrm{GRM}(r,m)$,*

$$\mathrm{dist}(r,m) = (p-f)p^{m-e-1} \ ,$$

avec $r = e(p-1)+f$ et $0 \le f < p-1$, et $\dim(r,m)$ sa dimension,

$$\dim(r,m) = \sum_{i=0}^{r}\sum_{j=0}^{m}(-1)^k\binom{m}{k}\binom{i-k\cdot p+m-1}{i-k\cdot p} \ .$$

Alors, pour tout entier $a \in [1, m(p-1)]$, on a la borne suivante sur le cardinal de $\mathcal{C}$:

$$|\mathcal{C}| \le \frac{A^{\delta}_{n\cdot p^m}(p)}{A_n^{\left\lceil \frac{\delta}{\mathrm{dist}(r+a,m)}\right\rceil}\left(p^{\ell}\right)} \ ,$$

où $A^d_n(q)$ désigne le cardinal maximal d'un code de longueur n et de distance de Hamming minimale supérieure ou égale à d sur $\mathbb{F}_q$ et $\ell = \dim(r+a,m) - \dim(r,m)$.

Preuve. Considérons un code T sur $\mathbb{F}_{p^\ell}$ de distance minimale $\lceil \delta/\mathrm{dist}(r+a,m)\rceil$ et de cardinal $A_n^{\lceil \delta/\mathrm{dist}(r+a,m)\rceil}\left(p^{\ell}\right)$. En appliquant le théorème 6.2 en prenant pour S un ensemble de représentants des translatés de $\mathrm{GRM}(r,m)$ dans $\mathrm{GRM}(r+a,m)$, on obtient un code $\mathcal{G}$ de distance minimale δ et de longueur np^m. Donc, $|\mathcal{G}| \le A^{\delta}_{n\cdot p^m}(p)$. Mais, $|\mathcal{G}| = |\mathcal{C}|\cdot|T|$ d'où $|\mathcal{C}|\cdot|T| \le A^{\delta}_{n\cdot p^m}(p)$, or $|T| = A_n^{\lceil \delta/\mathrm{dist}(r+a,m)\rceil}\left(p^{\ell}\right)$, ce qui donne

$$|\mathcal{C}| \le \frac{A^{\delta}_{n\cdot p^m}(p)}{A_n^{\left\lceil \frac{\delta}{\mathrm{dist}(r+a,m)}\right\rceil}\left(p^{\ell}\right)} \ .$$

□

La version itérée de la construction présentée donne une généralisation de la borne précédente :

PROPOSITION 6.6 *Soient* $\mathcal{C} \subset \mathrm{GRM}(r,m)^n$ *de distance minimale* d, *et* $s_0 = r < s_1 < \cdots < s_t \leq m(p-1)$. *Alors*

$$|\mathcal{C}| \leq \frac{A^d_{n\cdot p^m}(p)}{\prod_{j=1}^{t} A_n^{\left\lceil \frac{d}{\mathrm{dist}(s_j,m)} \right\rceil}\left(p^{\ell_j}\right)} \ ,$$

avec $\ell_j = \dim(s_j,m) - \dim(s_{j-1},m)$.

Nous avons déjà remarqué à la fin de la section 6 que notre construction n'imposait pas le code S. Nous avons choisi de prendre pour S un ensemble de représentants des translatés de $\mathrm{GRM}(r,m)$ dans $\mathrm{GRM}(r+a,m)$, mais d'autres choix sont possibles, chaque choix de S donnant bien entendu des bornes différentes.

COMPORTEMENT ASYMPTOTIQUE. Les performances asymptotiques des familles de codes sont usuellement mesurées à l'aide du taux de transmission défini par le rapport $R = \log_q(M)/n$ pour un code (n,M,d) sur $\mathbb{F}_q$. Notons $S(x)$ une borne supérieure sur le taux de transmission des codes de longueur n sur $\mathbb{Z}_p$ et de distance minimale $x \cdot n$, pour $n \to \infty$. De même, nous noterons $I_q(x)$ une borne inférieure sur R pour les codes de longueur n sur $\mathbb{F}_q$ de distance minimale $x \cdot n$. La proposition 6.6 donne alors

COROLLAIRE 6.7 *Soit* $R_m(x)$ *le taux de transmission maximal d'un code sur* $\mathbb{Z}_p$ *de longueur* $p^m \cdot n$, *distance minimale* $x \cdot p^m \cdot n$ *et inclus dans* $\mathrm{GRM}(1,m)^n$. *Avec les notations de la proposition 6.6, nous avons*

$$R_m(x) \leq S(x) - \frac{1}{2^m} \sum_{j=1}^{t} \ell_j \cdot I_{2^{\ell_j}}(x \cdot 2^{s_j}) \ .$$

PREUVE. En prenant le logarithme de la borne de la proposition 6.6 et en divisant par $p^m \cdot n$, on obtient

$$\frac{\log_p(|\mathcal{C}|)}{p^m \cdot n} \leq \frac{\log_p\left(A^d_{n\cdot p^m}(p)\right)}{p^m \cdot n} - \sum_{j=1}^{t} \frac{1}{p^m} \cdot \frac{\log_p\left(A_n^{\left\lceil \frac{d}{\mathrm{dist}(s_j,m)} \right\rceil}\left(p^{\ell_j}\right)\right)}{n} \ .$$

Soit, pour $x = d/(p^m \cdot n)$ fixé et n tendant vers l'infini,

$$R(x) \leq S(x) - \frac{1}{p^m} \sum_{j=1}^{t} \log_p\left(p^{\ell_j}\right) I_{p^{\ell_j}}\left(x \cdot p^{s_j}\right) \ ,$$

étant donné que $x \cdot p_j^s$ est la distance relative du code de longueur n sur $\mathbb{F}_{p^{l_j}}$ et de cardinal $A_n^{\lceil d/\mathrm{dist}(s_j,m)\rceil}(p^{\ell_j})$. □

Les bornes I_q peuvent être remplacées par la borne de Gilbert-Varshamov, ce qui donne

$$\lim_{n\to\infty} \frac{\log_q A_n^\delta(q)}{n} \geq 1 - h_q\left(\frac{\delta}{n}\right) \ ,$$

pour δ/n fixé et où h_q est l'entropie q-aire,

$$h_q(z) = z\log_q(q-1) - z\log_q(z) - (1-z)\log_q(1-z) \ ,$$

pour tout z de l'intervalle ouvert $]0,(q-1)/q[$ et 0 autrement. Pour la borne supérieure S nous utilisons la borne d'Elias, soit

$$\lim_{n\to\infty} \frac{\log_p A_n^\delta(p)}{n} \leq 1 - h_p\left(\theta - \sqrt{\theta\left(\theta - \frac{\delta}{n}\right)}\right) \ ,$$

où $\theta = 1 - 1/p$ et toujours pour δ/n fixé. En utilisant ces bornes et en prenant $s_j = j+1$, $j \in [1, m(p-1)-1]$ dans le corollaire précédent, on obtient

$$R_m(x) \leq 1 - h_p\left(\theta - \sqrt{\theta(\theta - x)}\right) - \frac{1}{p^m}\sum_{j=1}^{m(p-1)-1} \ell_j\left(1 - h_{p^{\ell_j}}\left(x \cdot p^{j+1}\right)\right) \ .$$

avec $l_j = \dim(j+1,m) - \dim(j,m)$.

Exemple 6.8 Nous allons calculer explicitement les différentes bornes que le corollaire précédent permet d'obtenir pour les codes $\mathbb{Z}_8$, $\mathbb{Z}_{16}$ et $\mathbb{Z}_{32}$-linéaires. Lorsque l'entropie h_q est binaire, nous notons simplement h en omettant l'indice.

Cas $\mathbb{Z}_8$. L'image de $\mathbb{Z}_8$ par l'application de Gray généralisée est le code $\mathrm{RM}(1,2) \subset \mathbb{F}_2^4$, ce qui ne laisse qu'une seule possibilité : $t = 1$, $s_0 = 1$ et $s_1 = 2$. Cela donne

$$\begin{aligned} l_1 &= \log_2(|\mathrm{RM}(s_1,2)/\mathrm{RM}(s_0,2)|) = 1 \ , \\ R_2(x) &\leq 1 - h\left(\frac{1}{2}\left(1 - \sqrt{1-2x}\right)\right) - \frac{1}{4}(1 - h(4x)) \\ &\leq \frac{3}{4} + \frac{1}{4}h(4x) - h\left(\frac{1}{2}\left(1 - \sqrt{1-2x}\right)\right) \ . \end{aligned} \qquad \text{(a)}$$

Cas $\mathbb{Z}_{16}$. On a $\Psi(\mathbb{Z}_{16}) = \mathrm{RM}(1,3) \subset \mathbb{F}_2^8$ et par conséquent deux possibilités sont ouvertes. Premièrement, nous pouvons rechercher des translatés de $\mathrm{RM}(1,3)$ dans $\mathrm{RM}(2,3)$, puis de $\mathrm{RM}(2,3)$ dans $\mathrm{RM}(3,3)$. Cela revient à choisir $t = 2$, $s_0 = 1$, $s_1 = 2$ et $s_2 = 3$. Dans ces conditions, nous avons

$$\begin{aligned} l_1 &= \log_2\left(|\mathrm{RM}(s_1,3)/\mathrm{RM}(s_0,3)|\right) = \binom{3}{2} = 3 \ , \\ l_2 &= \log_2\left(|\mathrm{RM}(s_2,3)/\mathrm{RM}(s_1,3)|\right) = \binom{3}{3} = 1 \ , \end{aligned}$$

qui donnent

$$\begin{aligned} R_3(x) &\leq 1 - h\left(\frac{1}{2}\left(1-\sqrt{1-2x}\right)\right) - \frac{1}{8}\left(3(1-h_8(4x)) + (1-h(8x))\right) \\ &\leq \frac{1}{2} + \frac{1}{8}\Big(3h_8(4x)) + h(8x)\Big) - h\left(\frac{1}{2}\left(1-\sqrt{1-2x}\right)\right) \ . \end{aligned} \tag{b}$$

La seconde possibilité consiste à rechercher directement des translatés de $\mathrm{RM}(1,3)$ dans $\mathrm{RM}(3,3)$, auquel cas $t = 1$ et $s_0 = 1$, $s_1 = 3$, donnant

$$\begin{aligned} l_1 &= \log_2\left(|\mathrm{RM}(s_1,3)/\mathrm{RM}(s_0,3)|\right) = \binom{3}{3} + \binom{3}{2} = 4 \ , \\ R_3(x) &\leq 1 - h\left(\frac{1}{2}\left(1-\sqrt{1-2x}\right)\right) - \frac{1}{2}(1-h_{16}(8x)) \\ &\leq \frac{1}{2} + \frac{1}{2}h_{16}(8x) - h\left(\frac{1}{2}\left(1-\sqrt{1-2x}\right)\right) \ . \end{aligned} \tag{c}$$

Cas $\mathbb{Z}_{32}$. Avec $\mathbb{Z}_{32}$, nous commençons à voir le nombre de possibilités exploser : on a $\Psi(\mathbb{Z}_{32}) = \mathrm{RM}(1,4)$ ce qui permet d'obtenir quatre bornes différentes. Une première borne est obtenue par la recherche successive des translatés de $\mathrm{RM}(1,4)$ dans $\mathrm{RM}(2,4)$, de $\mathrm{RM}(2,4)$ dans $\mathrm{RM}(3,4)$ et enfin de $\mathrm{RM}(3,4)$ dans $\mathrm{RM}(4,4)$. Autrement dit, $t = 3$, $s_0 = 1$, $s_1 = 2$, $s_2 = 3$ et $s_3 = 4$. Alors,

$$\begin{aligned} l_1 &= \log_2\left(|\mathrm{RM}(s_1,4)/\mathrm{RM}(s_0,4)|\right) = \binom{4}{2} = 6 \ , \\ l_2 &= \log_2\left(|\mathrm{RM}(s_2,4)/\mathrm{RM}(s_1,4)|\right) = \binom{4}{3} = 4 \ , \\ l_3 &= \log_2\left(|\mathrm{RM}(s_3,4)/\mathrm{RM}(s_2,4)|\right) = \binom{4}{4} = 1 \ , \end{aligned}$$

et finalement

$$\begin{aligned} R_4(x) &\leq 1 - h\left(\frac{1}{2}\left(1-\sqrt{1-2x}\right)\right) \\ &\quad - \frac{1}{16}\Big(6(1-h_{64}(4x)+4(1-h_{16}(8x)+(1-h(16x)\Big) \\ &\leq \frac{5}{16} + \frac{1}{16}\Big(6h_{64}(4x)+4h_{16}(8x)+h(16x)\Big) \\ &\quad - h\left(\frac{1}{2}\left(1-\sqrt{1-2x}\right)\right) \quad . \end{aligned} \tag{d}$$

Une deuxième borne est donnée quand on prend $t = 2$, $s_0 = 1$, $s_1 = 3$ et $s_2 = 4$, ce qui signifie qu'on translate RM$(1,4)$ directement dans RM$(3,4)$ et qu'on termine avec des translatés de RM$(3,4)$ dans RM$(4,4)$. Cela donne

$$\begin{aligned} l_1 &= \log_2\left(|\mathrm{RM}(s_1,4)/\mathrm{RM}(s_0,4)|\right) = \binom{4}{3} + \binom{4}{2} = 10 \ , \\ l_2 &= \log_2\left(|\mathrm{RM}(s_2,4)/\mathrm{RM}(s_1,4)|\right) = \binom{4}{4} = 1 \ , \\ R_4(x) &\leq 1 - h\left(\frac{1}{2}\left(1-\sqrt{1-2x}\right)\right) \\ &\quad - \frac{1}{16}\Big(10(1-h_{2^{10}}(8x)) + (1-h(16x))\Big) \\ &\leq \frac{5}{16} + \frac{1}{16}\Big(10h_{2^{10}}(8x)+h(16x)\Big) - h\left(\frac{1}{2}\left(1-\sqrt{1-2x}\right)\right) \quad . \end{aligned} \tag{e}$$

Lorsqu'on translate RM$(1,4)$ dans RM$(2,4)$ et qu'on passe ensuite directement de RM$(2,4)$ à RM$(4,4)$, on obtient

$$\begin{aligned} l_1 &= \log_2\left(|\mathrm{RM}(s_1,4)/\mathrm{RM}(s_0,4)|\right) = \binom{4}{2} = 6 \ , \\ l_2 &= \log_2\left(|\mathrm{RM}(s_2,4)/\mathrm{RM}(s_1,4)|\right) = \binom{4}{4} + \binom{4}{3} = 5 \ , \\ R_4(x) &\leq 1 - h\left(\frac{1}{2}\left(1-\sqrt{1-2x}\right)\right) \\ &\quad - \frac{1}{16}\Big(6(1-h_{64}(4x)) + 5(1-h_{32}(16x))\Big) \\ &\leq \frac{5}{16} + \frac{1}{16}\Big(6h_{64}(4x)+5h_{32}(16x)\Big) \\ &\quad - h\left(\frac{1}{2}\left(1-\sqrt{1-2x}\right)\right) \quad . \end{aligned} \tag{f}$$

Enfin, pour terminer la dernière borne est obtenue en translatant $\mathrm{RM}(1,4)$ dans $\mathrm{RM}(4,4)$ et donne

$$\begin{aligned} R_4(x) &\leq 1 - h\left(\frac{1}{2}\left(1-\sqrt{1-2x}\right)\right) - \frac{11}{16}(1 - h_{2^{11}}(16x)) \\ &\leq \frac{5}{16} + \frac{11}{16}h_{2^{11}}(16x) - h\left(\frac{1}{2}\left(1-\sqrt{1-2x}\right)\right) \quad . \end{aligned} \tag{g}$$

GRAPHIQUES. Afin de résumer les bornes (a-g) que nous venons de calculer, nous donnons les courbes de ces bornes, ainsi que celles de la borne de Gilbert-Varshamov et de celle d'Elias, dans les figures 6.1, 6.2 et 6.3, respectivement pour $\mathbb{Z}_8$, $\mathbb{Z}_{16}$ et $\mathbb{Z}_{32}$. Ces graphiques comportent également la borne triviale obtenue à partir de l'inclusion du code dans $\mathrm{RM}(1,m)^n$ qui a pour conséquence de borner supérieurement le taux de transmission du code par celui $\mathrm{RM}(1,m)$, à savoir $(m+1)/2^m$. L'interprétation de ces graphiques est simple : lorsque la courbe d'une borne est sous celle de Gilbert-Varshamov, il existe des codes linéaires strictement meilleurs que les $\mathbb{Z}_{2^k}$-linéaires. En revanche, nous n'avons pas de réciproque : lorsqu'elle est au-dessus, on ne peut pas conclure à l'existence de codes $\mathbb{Z}_{2^k}$-linéaires dépassant les codes linéaires. La borne d'Elias sert de référence pour le taux de transmission maximal d'un code binaire. Comme le montrent ces figures, le type de bornes asymptotiques que nous obtenons ne semble pas donner de grande amélioration : sur $\mathbb{Z}_8$, figure 6.1 page suivante, l'amélioration est faible ($x \in [0.06; 0.125]$), et pour $\mathbb{Z}_{16}$, figure 6.2, elle est presque imperceptible (x au voisinage de 0.21). □

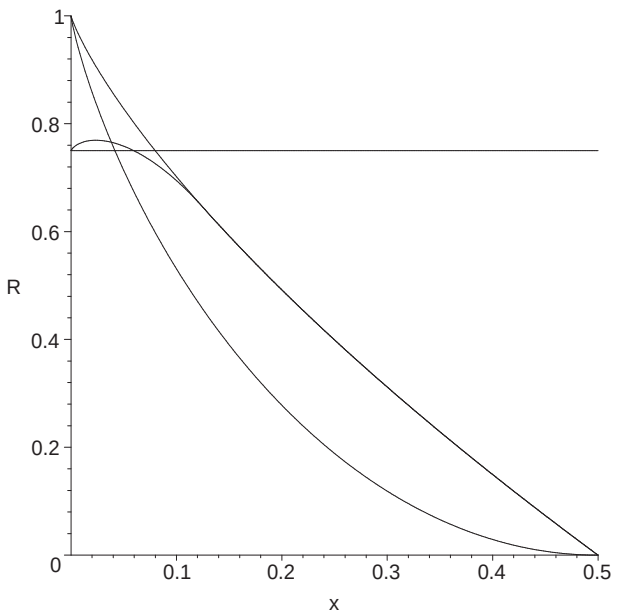

FIG. 6.1 – Bornes sur les codes $\mathbb{Z}_8$-linéaires : bornes d'Elias, de Gilbert-Varshamov et borne (a) de l'exemple 6.8, page 95.

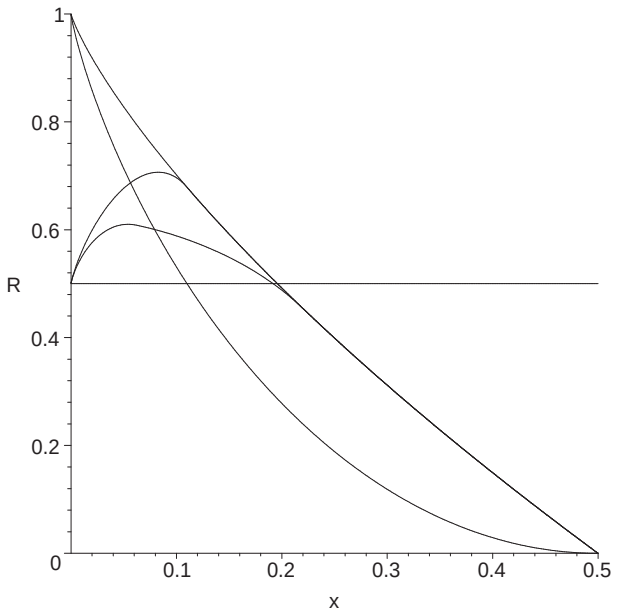

FIG. 6.2 – Bornes sur les codes $\mathbb{Z}_{16}$-linéaires : bornes d'Elias, de Gilbert-Varshamov, et bornes (b) et (c) de l'exemple 6.8, pages 96 et 96.

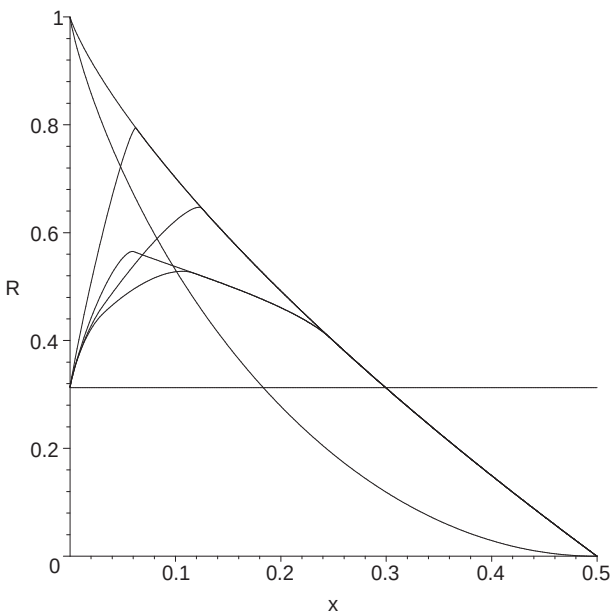

FIG. 6.3 – Bornes sur les codes $\mathbb{Z}_{32}$-linéaires : bornes d'Elias, de Gilbert-Varshamov, et bornes (d), (e), (f) et (g) de l'exemple 6.8, page 97.

Conclusion et perspectives

Nous avons étudié une technique pour construire des codes sur un corps premier. Elle consiste à appliquer le relèvement de Hensel au polynôme générateur d'un code cyclique sur un corps premier $\mathbb{Z}_p$ afin d'obtenir un code cyclique sur un anneau $\mathbb{Z}_{p^k}$. Le code ainsi obtenu est ensuite transformé en un nouveau code sur $\mathbb{Z}_p$, dont le cardinal et la distance minimale sont identiques à ceux du code sur l'anneau, lorsque $\mathbb{Z}_p$ est muni de la distance de Hamming et $\mathbb{Z}_{p^k}$ de la distance homogène.

Cette technique, déjà utilisée fructueusement avec les anneaux $\mathbb{Z}_4$, $\mathbb{Z}_8$ et $\mathbb{Z}_9$, nous a permis de construire plusieurs codes binaires égalant les meilleurs codes linéaires. Parmi ces codes, deux sont obtenus par relèvement de codes de résidus quadratiques de longueur 31 et 47 à $\mathbb{Z}_8$, et ont pour paramètres respectifs $\{128, 48, 28\}$ et $\{192, 72, 36\}$. Nous avons également obtenu un nouveau code par un relèvement à $\mathbb{Z}_{16}$ du code de résidus quadratiques de longueur 23. Ce code constitue le premier exemple de bon code construit en utilisant $\mathbb{Z}_{16}$. Enfin, nous avons trouvé un dernier code ayant une distance minimale élevée. Il s'agit du code $\mathcal{K}(2^3, 3)$ de paramètres $\{32, 12, 10\}$; il appartient à la famille des codes de Kerdock généralisés, qui peut être définie en utilisant le relèvement de Hensel, comme nous l'avons montré au chapitre 4. Mais c'est le seul exemple de bon code appartenant à cette famille, hormis bien entendu la classe des codes de Kerdock.

Dans une certaine mesure, ces résultats ne sont pas ceux auxquels nous pouvions nous attendre. Nous disposions d'une borne sur la distance minimale des codes de Kerdock généralisés qui laissait espérer, principalement pour les codes $\mathcal{K}(2^3, m)$, une distance minimale supérieure à celle des codes linéaires. La comparaison des résultats que nous avons obtenus avec les paramètres des codes BCH prouve que, pour tous les codes étudiés, sauf ceux cités ci-dessus, la généralisation des codes de Kerdock ne contient pas de bon code. Les codes de Kerdock généralisés sont même nettement moins bons que les codes BCH. Par ailleurs, la famille des codes de résidus quadratiques a été très largement utilisée pour construire des codes $\mathbb{Z}_4$-linéaires surpassant les meilleurs codes connus. Elle a même permis d'obtenir un code $\mathbb{Z}_8$-linéaire ayant cette propriété. Le fait que nous n'en ayons pas trouvé d'autres est donc inattendu.

Ce constat nous a conduit à nous interroger sur les causes de cette situation. Cela a débouché sur la construction fondée sur la réunion de translatés, dont nous avons déduit une famille de bornes supérieures s'appliquant au cardinal des codes $\mathbb{Z}_{p^k}$-linéaires. Cette construction étend celle donnée par Duursma *et al.* dans [DGL+01] pour obtenir un code binaire de paramètres $\{96, 37, 24\}$ à partir d'un code $\mathbb{Z}_8$-linéaire de paramètres $\{96, 36, 24\}$, ce code dépassant déjà les codes linéaires. Les exemples que nous avons donnés montrent l'efficacité de cette construction et l'ampleur des améliorations auxquelles elle conduit lorsqu'elle est appliquée aux codes $\mathbb{Z}_{p^k}$-linéaires. Cependant, elle ne nous a pas permis de construire des codes meilleurs que ceux déjà connus. Nous conjecturons toutefois que c'est possible : le code de résidus quadratiques ternaire de longueur 23 et dimension 12 semble donner, après relèvement à $\mathbb{Z}_9$, un code $\mathbb{Z}_9$-linéaire $\mathcal{C}$ de paramètres $\{72, 24, 24\}$. Nous ne sommes pas certain de la distance minimale de ce code : il comporte plus de 2^{38} éléments et nous n'avons donc qu'une borne supérieure sur la distance minimale, obtenue en calculant le poids d'environ 10% des mots de ce code. Si cette borne est la distance minimale exacte, alors notre construction permet d'obtenir un code $\{72, 25, 24\}$. En effet, le code $\mathrm{GRM}(1, 1)$ sur $\mathbb{Z}_3$ admet 3 translatés dans $\mathbb{Z}_3^3 = \Psi(\mathbb{Z}_9)$. Si on prend pour S un système de représentants des translatés, on a $d_S = 1$. D'autre part, il est possible de prendre pour T le code trivial de longueur 24 et de dimension 1 sur $\mathbb{Z}_3$ puisque sa distance minimale est bien égale à $24/d_S = 24$. Les mots du code concaténé $T(S)$ permettent alors d'obtenir 3 translatés du code $\mathbb{Z}_9$-linéaire, en assurant une distance minimale de 24 entre eux. Leur réunion donne le code ternaire de paramètres $\{72, 25, 24\}$ évoqué ci-dessus. Or la plus grande distance minimale connue pour un code linéaire sur $\mathbb{Z}_3$ de paramètres $\{72, 25\}$ est 23 – cette distance vaut 24 pour un code $\{72, 24\}$. Notre construction permettrait alors d'obtenir un code surpassant les codes linéaires connus, à partir d'un code les égalant. La vérification de la distance minimale du code $\mathcal{C}$ nécessite une réécriture de notre logiciel de calcul de poids minimal, mais ne semble pas hors de portée d'une implémentation optimisée.

Toutes les distances minimales obtenues l'ont été par un parcours quasi exhaustif des mots de codes. Nous avons mené ces calculs aussi loin qu'il nous semble possible à l'heure actuelle, compte tenu des capacités de calculs dont nous avons pu disposer, tout au moins dans le cas binaire. En effet, comme nous l'avons expliqué, des optimisations sur notre logiciel sont possibles dans le cas $p > 2$. Cependant, nous ne pouvons espérer explorer des codes aux cardinaux beaucoup plus importants avec de telles techniques. Fréquemment, la distance minimale des codes, avant relèvement, est connue. C'est par exemple le cas des codes de résidus quadratiques que nous avons utilisés. Un problème difficile est de réussir à utiliser cette information pour calculer le poids des codes après relèvement.

Si l'approche exhaustive montre ses limites sur les codes $\mathbb{Z}_{p^k}$-cycliques obtenus par relèvement de Hensel, il est encore possible de l'utiliser avec des

codes $\mathbb{Z}_{p^k}$-quasi cycliques. Aydin et Ray-Chaudhuri, dans [AR02], ont obtenu des codes dépassant les meilleurs codes connus en généralisant la technique du relèvement. Cela consiste à relever sur $\mathbb{Z}_4$ un code cyclique, à construire un code quasi cyclique sur cet anneau à partir du code précédent, et enfin à utiliser l'application de Gray pour obtenir un code binaire. Cette technique se généralise naturellement à $\mathbb{Z}_{p^k}$ mais, en dehors du cas où $p^k = 4$, ses potentialités n'ont pas encore été étudiées. Nous pensons qu'elle permet de construire de nouveaux codes performants.

Bibliographie

[An96a] R.J. Anderson (sld), *Proceedings of the workshop on information hiding,* Springer-Verlag, LNCS, vol. 1174, 1996, 306 p.

[An96b] R.J. Anderson, « Stretching the limits of steganography », dans [An96a], p. 39–48.

[AK98] E.F. Assmus et J.D. Key, « Polynomial codes and finite geometries », dans V.S. Pless et W.C. Huffman, *Handbook of coding theory,* North-Holland, 1998, p. 1269–1346.

[AP98] R.J. Anderson et F.A.P. Petitcolas, « On the limits of steganography », *IEEE Journal on Selected Areas in Communications*, vol. 16, n° 4, 1998, p. 474–481.

[AR02] N. Aydin et D.K. Ray-Chaudhuri, « Quasi-cyclic codes over $\mathbb{Z}_4$ and some new binary codes », *IEEE Transactions on Informations Theory*, vol. 48, n° 7, 2002, p. 2065–2069.

[Bar98] A. Barg, « Complexity issues in coding theory », dans V.S. Pless et W.C. Huffman, *Handbook of coding theory,* North-Holland, 1998, p. 649–754.

[Ber68] E. Berlekamp, *Algebraic coding theory,* McGraw-Hill, 1968.

[Bla72] I.F. Blake, « Codes over certain rings », *Information and Control*, vol. 20, 1972, p. 396–404.

[Bla75] I.F. Blake, « Codes over integer residue rings », *Information and Control*, vol. 29, n° 4, 1975, p. 295–300.

[Bli90] V.M. Blinovsky, « Asymptotically exact uniform bounds for spectra of cosets of linear codes », *Problems of Information Transmission*, vol. 26, n° 1, 1990, p. 83-86. (traduit du russe, *Problemy Peredachi Informatsii*, vol. 26, n° 1, 1990, p. 99–103).

[Bos] N. Boston, *A mathematical foundation for watermarking.* Preprint.
(`http://www.math.wisc.edu/~boston/bostonpreps.html`).

[Bro98] A.E. Brouwer, « Bounds on the size of linear codes », dans V.S. Pless et W.C. Huffman, *Handbook of coding theory,* North-Holland, 1998, p. 295–461.

[BGM+96] W. Bender, D. Gruhl, N. Morimoto et A. Lu, « Techniques for data hiding », *IBM System Journal*, vol. 35, n° 3–4, 1996, p. 313–336.

[BMT78] E. Berlekamp, R.J. McEliece et H.C.A. van Tilborg, « On the inherent intractability of certain coding problems », *IEEE Transactions on Informations Theory*, vol. 29, n° 3, 1978, p. 384–386.

[BP99] L.A. Bassalygo et M.S. Pinsker, « Centered error-correcting codes », *Problems of Information Transmission*, vol. 35, 1999, p. 25–31. (traduit du russe, *Problemy Peredachi Informatsii*, vol. 35, n° 1, 1999, p. 30–37).

[BR00] J.T. Blackford et D.K. Ray-Chaudhuri, « A transform approach to permutation groups of cyclic codes over galois rings », *IEEE Transactions on Informations Theory*, vol. 46, n° 7, 2000, p. 2350–2358.

[BSC95] A. Bonnecaze, P. Solé et A.R. Calderbank, « Quaternary quadratic residue codes and unimodular lattices », *IEEE Transactions on Informations Theory*, vol. 41, n° 2, 1995, p. 366–377.

[Cac04] C. Cachin, « An information-theoretic model for steganography », *Information and Computation*, vol. 192, n° 1, 2004, p. 41–56. (version préliminaire dans [An96a, p. 306–318]).

[Car95] C. Carlet, « On $\mathbb{Z}_4$-duality », *IEEE Transactions on Informations Theory*, vol. 41, n° 5, 1995, p. 1487–1494.

[Car98] C. Carlet, « $\mathbb{Z}_{2^k}$-linear codes », *IEEE Transactions on Informations Theory*, vol. 44, n° 4, 1998, p. 1543–1547.

[Car99] C. Carlet, « On Kerdock codes », *Contemporary Mathematics*, vol. 255, 1999, p. 155-163.

[Coh83] G.D. Cohen, « A nonconstructive upper bound on covering radius », *IEEE Transactions on Informations Theory*, vol. 29, n° 3, 1983, p. 352–353.

[Cra98] R. Crandall, *Some notes on steganography*, 1998. Envoyé à la Steganography Mailing List. (`http://os.inf.tu-dresden.de/~westfeld/crandall.pdf`).

[CGM86] G. Cohen, P. Godlewski et F. Merkx, « Linear binary codes for write-once memories », *IEEE Transactions on Informations Theory*, vol. 32, n° 5, 1986, p. 697–700.

[CH97] I. Constantinescu et W. Heise, « A metric for codes over residue class rings », *Problems of Information Transmission*, vol. 33, n° 3, 1997, p. 208–213. (traduit du russe, *Problemy Peredachi Informatsii*, vol. 33, n° 3, 1997, p. 22–28).

[CHL+97] G. Cohen, I. Honkala, S. Litsyn et A. Lobstein, *Covering codes,* North-Holland, 1997.

[CJL+03] K. Chang, C. Jung, K. Lee, S. Lee et H. Yoo, « High quality perceptual information hiding technique for color images », dans *Proceedings of the Pacific Rim Workshop on Digital Steganography (STEG)*, 2003.
(`http://www.know.comp.kyutech.ac.jp/STEG03/STEG03-PAPERS/`).

[CJL+04] K. Chang, C. Jung, S. Lee et W. Yang, « High quality perceptual steganographic techniques », dans *Proceedings of the 2003 International Workshop on Digital Watermarking*, éd. par T. Kalker, I.J. Cox et Y.M. Ro, Springer-Verlag, LNCS 2939, 2004, p. 518–531.

[CKL+96] I.J. Cox, J. Killian, T. Leighton et T. Shamoon, « A secure, robust watermark for multimedia », dans [An96a], p. 183–206.

[CLP97] A.R. Calderbank, W.-C.W. Li et B. Poonen, « A 2-adic approach to the analysis of cyclic codes », *IEEE Transactions on Informations Theory*, vol. 43, n° 3, 1997, p. 977–986.

[CM01] R. Chandramouli et N. Memon, « Analysis of lsb based image steganography techniques », dans *Proceedings of the IEEE International Conference on Image Processing*, vol. 3, 2001, p. 1019–1022.

[CMK+96] A.R. Calderbank, G. McGuire, P.V. Kumar et T. Helleseth, « Cyclic codes over $\mathbb{Z}_4$, locator polynomials and Newton's identities », *IEEE Transactions on Informations Theory*, vol. 42, n° 1, 1996, p. 217–226.

[CS95] A.R. Calderbank et N.J.A. Sloane., « Modular and $\mathfrak{p}$-adic cyclic codes », *Designs, Codes and Cryptography*, vol. 6, 1995, p. 21–35.

[DGL+01] I.M. Duursma, M. Greferath, S.N. Litsyn et S.E. Schmidt, « A $\mathbb{Z}_8$-linear lift of the binary Golay code and a non-linear binary $(96, 2^{37}, 24)$ code », *IEEE Transactions on Information Theory*, vol. 47, n° 4, 2001, p. 1596–1598.

[DP86] P. Delsarte et P. Piret, « Do most binary linear codes achieve the goblick bound on the covering radius ? », *IEEE Transactions on Informations Theory*, vol. 32, n° 6, 1986, p. 826–828.

[Fel85] M.R. Fellows, *encoding graphs in graphs,* Thèse de doctorat de l'université de californie, 1985.

[FGD01] J. Fridrich, M. Goljan et R. Du, « Detecting lsb steganography in color and gray-scale images », *Magazine of IEEE Multimedia*, vol. 8, n° 4, 2001, p. 22-28.

[FJM+96] E. Franz, A. Jerichow, S. Muller, A. Pfitzmann et I. Stierand, « Computer based steganography », dans [An96a], p. 7–21.

[Ga03a] F. Galand, *codes $\mathbb{Z}_{2^k}$-linéaires,* Rapport de recherche INRIA, janvier 2003.

[Ga03b] F. Galand, « On the minimum distance of some families of $\mathbb{Z}_{2^k}$-linear codes », dans *Proceedings of the 15th AAECC International Symposium*, éd. par M. Fossorier, T. Høholdt et A. Poli, Springer-Verlag, LNCS 2643, 2003, p. 235–243.

[Gal04] F. Galand, « Stéganographie », dans *Traité de sécurité des systèmes d'information*, Techniques de l'ingénieur, 2004.

[Gal68] R.G. Gallager, *Information theory and reliable communication,* Wiley, 1968, 608 p.

[GG99] J. von zur Gathen et J. Gerhard, *Modern computer algebra,* Cambridge University Press, 1999.

[GJ79] M.R. Garey et D.S. Johnson, *Computers and intractability : a guide to the theory of NP-completeness,* Freeman, 1979, 338 p.

[GK03a] F. Galand et G. Kabatiansky, « Information hiding by coverings », dans *Proceedings of the IEEE Information Theory Workshop*, 2003, p. 151–154.

[GK03b] F. Galand et G. Kabatiansky, « Steganography via covering codes », dans *Proceedings of the IEEE International Symposium on Information Theory*, 2003, p. 192.

[GS99] M. Greferath et S.E. Schmidt, « Gray isometries for finite chain rings and a nonlinear ternary $(36, 3^{12}, 15)$ code », *IEEE Transactions on Information Theory*, vol. 45, n° 7, 1999, p. 2522–2524.

[Hio03] H. Hioki, « A modified CPT scheme for embedding data into binary images », dans *Proceedings of the Pacific Rim Workshop on Digital Steganography (STEG)*, 2003.
(`http://www.know.comp.kyutech.ac.jp/STEG03/STEG03-PAPERS/`).

[Hun80] T.W. Hungerford, *Algebra,* Springer-Verlag, 1980.

[HKC+94] R. Hammons, P.V. Kumar, A.R. Calderbank, N.J.A. Sloane et P. Solé, « Kerdock, Preparata, Goethals and other codes are linear over $\mathbb{Z}_4$ », *IEEE Transactions on Information Theory*, vol. 40, n° 2, 1994, p. 301–319.

[HKM+96] T. Helleseth, P.V. Kumar, O. Moreno et A.G. Shanbhag, « Improved estimates via exponential sums for the minimum distance of $\mathbb{Z}_4$-linear trace codes », *IEEE Transactions on Informations Theory*, vol. 42, n° 4, 1996, p. 1212–1216.

[HL00] T. Honold et I. Landjev, « Linear codes over finite chain rings », *The Electronic Journal of Combinatorics*, vol. 7, n° 1, 2000.
(`http://www.combinatorics.org/Volume\_7/v7i1toc.html`).

[HN99] T. Honold et A.A. Nechaev, « Weighted modules and representations of codes », *Problems of Information Transmission*, vol. 35, n° 3, 1999, p. 205–223. (traduit du russe, *Problemy Peredachi Informatsii*, vol. 35, n° 3, 1999, p. 18–39).

[Kas69] T. Kasami, « Weight distribution of Bose-Chaudhuri-Hocquenghem codes », *Combinatorial Mathematics and its Applications*, 1969, p. 335–357.

[Ker72] A.M. Kerdock, « A class of low-rate nonlinear codes », *Information and Control*, vol. 20, 1972.

[Ker83] A. Kerckhoffs, « La cryptographie militaire », *Journal des sciences militaires*, 1883, p. 5–38.

[KHC95] P.V. Kumar, T. Helleseth et A.R. Calderbank, « An upper bound for Weil exponential sums over Galois rings and applications », *IEEE Transactions on Informations Theory*, vol. 41, n° 2, 1995, p. 456–468.

[KL97] P. Kanwar et S.R. López-Permouth, « Cyclic codes over the integers modulo p^m », *Finite Fields and Their Applications*, vol. 3, 1997, p. 334–352.

[KN92] A.S. Kuzmin et A.A. Nechaev, « Construction of noise-stable codes using linear recurrent sequences over Galois rings », *Russian Mathematical Surveys*, vol. 47, n° 5, 1992, p. 189–190. (traduit du russe, *Uspehi Mat. Nauk.*, vol. 47, n°5, 1992, p. 183–184).

[KN94] A.S. Kuzmin et A.A. Nechaev, « Linearly presentable codes and Kerdock codes over arbitrary Galois fields of characteristic 2 », *Russian Mathematical Surveys*, vol. 49, n° 5, 1994, p. 183–184. (traduit du russe, *Uspehi Mat. Nauk.*, vol. 49, n°5, 1994, p. 165-166).

[KP02] S. Katzenbeisser et F. Petitcolas, « On defining security in steganographic systems », dans *Security and Watermarking of Multimedia Contents*, éd. par E.J. Delp et P.W. Wong, The International Society for Optical Engineering (SPIE), Proceedings of SPIE 4675, 2002, p. 50–56.

[KP99] S. Katzenbeisser et F.A.P. Petitcolas (sld), *Information hiding techniques for steganography and digital watermarking,* Artech House, 1999, 220 p.

[Lin99] J.H. van Lint, *Introduction to coding theory,* 3e édition, Springer-Verlag, 1999.

[Lit98] S.N. Litsyn, « An updated table of the best binary codes known », dans V.S. Pless et W.C. Huffman, *Handbook of coding theory,* North-Holland, 1998, p. 463–498.

[LN97] R. Lidl et H. Niederreiter, *Finite fields,* 2e édition, Cambridge University Press, Encyclopedia of Mathematics and its Applications, vol. 20, 1997.

[Mac74] B.R. MacDonald, *Finite rings with identity,* Dekker, 1974.

[Miz99] T. Mizzelholzer, « An information-theoretic approach to steganography and watermarking », dans *Proceedings of the Workshop on Information Hiding*, Springer-Verlag, LNCS 1768, 1999.

[MS96] F.J. MacWilliams et N.J.A. Sloane, *The theory of error-correcting codes,* 3e édition, North-Holland, 1996.

[Nec91] A.A. Nechaev, « Kerdock codes in a cyclic form », *Discrete Mathematics and Applications*, vol. 1, no 4, 1991, p. 365–384. (traduit du russe, *Diskretnaya Matematika*, vol. 1, no 4, 1989, p. 123–139).

[Pit96] I. Pitas, « A method for signature casting on digital images », dans *Proceedings of the IEEE International Conference on Image Processing*, vol. 3, 1996, p. 215–218.

[Pre68] F.P. Preparata, « A class of optimum nonlinear double-error correcting codes », *Information and Control*, vol. 16, no 4, 1968, p. 378–400.

[PCT00] H.-K. Pan, Y.-Y. Chen et Y.-C. Tseng, « A secure data hiding scheme for two-color images », dans *Proceedings of the IEEE Symposium on Computers and Communication*, 2000, p. 750–755.

[PQ96] V.S. Pless et Z. Qian, « Cyclic codes and quadratic residue codes over $\mathbb{Z}_4$ », *IEEE Transactions on Information Theory*, vol. 42, no 5, 1996, p. 1594–1600.

[PW95] O. Papini et J. Wolfmann , *Algèbre discrète et codes correcteurs,* Springer-Verlag, Mathématiques & Applications, vol. 20, 1995.

[PWW01] G. Pan, Y. Wu et Z. Wu, « A novel data hiding method for two-color images », dans *Proceedings of the International Conference on Information and Communications Security*, Springer-Verlag, LNCS 2229, 2001, p. 261–270.

[RS82] R.L. Rivest et A. Shamir, « How to reuse a "write-once" memory », *Information and Control*, vol. 55, no 1–3, 1982, p. 1–19.

[RS94a] B.S. Rajan et M.U. Siddiqi, « Transform domain characterization of cyclic codes over $\mathbb{Z}_m$ », *Applicable Algebra in Engineering, Communication and Computing*, vol. 5, no 5, 1994, p. 261–275.

[RS94b] B.S. Rajan et M.U. Siddiqi, « A generalized DFT for abelian codes over $\mathbb{Z}_m$ », *IEEE Transactions on Informations Theory*, vol. 6, n° 40, 1994, p. 2082–2090.

[Sha49] C.E. Shannon, « Communication theory of secrecy systems », *Bell System Technical Journal*, vol. 28, n° 4, 1949, p. 656–715.

[Sha79] P. Shankar, « On BCH codes over arbitrary integer rings », *IEEE Transactions on Informations Theory*, vol. 25, n° 4, 1979, p. 480–483.

[Sim84] G.J. Simmons, « The prisoners' problem and the subliminal channel », dans *Proceedings of Crypto'83 - Advances in Cryptology*, éd. par D. Chaum, Plenum Press, 1984, p. 51–67.

[Sim98] G.J. Simmons, « The history of subliminal channels », *IEEE Journal on Selected Areas in Communication*, vol. 16, n° 4, 1998, p. 452–462.

[Spi77] E. Spiegel, « Codes over $\mathbb{Z}_m$ », *Information and Control*, vol. 35, n° 1, 1977, p. 48–51.

[Spi78] E. Spiegel, « Codes over $\mathbb{Z}_m$, revisited », *Information and Control*, vol. 37, n° 1, 1978, p. 100–104.

[Săl99] A. Sălăgean-Mandache, « On the isometries between $\mathbb{Z}_{p^k}$ and $\mathbb{Z}_p^k$ », *IEEE Transactions on Information Theory*, vol. 45, n° 6, 1999, p. 2146–2148.

[SM95] D.R. Stinson et J.L. Massey, « An infinite class of counterexamples to a conjecture concerning nonlinear resilient functions », *Journal of Cryptology*, vol. 8, n° 3, 1995, p. 167–173.

[SSD+00] V.M. Sidelnikov, A.Yu. Serebriakov, A.G. Dyachkov et P.A. Vilenkin, *Methods of constructing steganographical channel*, 2000. Manuscript.

[STO94] R.G. van Schyndel, A.Z. Trikel et C.F. Osborne, « A digital watermark », dans *Proceedings of the IEEE International Conference on Image Processing*, vol. 2, 1994, p. 86–90.

[TP01] Y.-C. Tseng et H.-K. Pan, « Secure and invisible data hiding in 2-color images », dans *Proceedings of the IEEE Infocom*, vol. 2, 2001, p. 887-896.

[TP02] Y.-C. Tseng et H.-K. Pan, « Data hiding in 2-color images », *IEEE Transactions on Computers*, vol. 51, 2002, p. 873-880.

[TV91] M.A. Tsfasman et S.G Vlăduţ, *Algebraic-geometric codes,* Kluwer Academic Publishers, Mathematics and its Applications, 1991, 667 p.

[VT65] R.R. Varshamov et G.M. Tenengolts, « Codes which correct single asymmetric errors », *Automation and Remote Control*, vol.

26, n° 2, 1965, p. 286–290. (Translated from Russian, *Avtomatika i Telemekhanika*, vol. 26, n° 2, 1965, p. 288–292).

[Wal91] G. Wallace, « The JPEG still picture compression standard », *Communications of the ACM*, vol. 34, n° 4, 1991, p. 30-44.

[Wan97] Z.-X. Wan, *Quaternary codes,* World Scientific, Series on Applied Mathematics, vol. 8, 1997.

[Was82] S.K. Wasan, « On codes over $\mathbb{Z}_m$ », *IEEE Transactions on Informations Theory*, vol. 28, n° 1, 1982, p. 117–120.

[Wes01] A. Westfeld, « Capacity despite better steganalysis (F5 - A steganographic algorithm) », dans *Proceedings of the Workshop on Information Hiding*, Springer-Verlag, LNCS , 2001, p. 289–302.

[Wic98] S.B. Wicker, « Deep space applications », dans V.S. Pless et W.C. Huffman, *Handbook of coding theory,* North-Holland, 1998, p. 2119–2200.

[Wol99] J. Wolfmann, « Negacyclic and cyclic codes over $\mathbb{Z}_4$ », *IEEE Transactions on Informations Theory*, vol. 45, n° 7, 1999, p. 2527–2532.

[WL98] M.Y. Wu et J.H. Lee, « A novel data embedding method for two-color facsimile images », dans *Proceedings of the International Symposium on Multimedia Information Processing*, 1998.

[WTL00] M. Wu, E. Tang et B. Liu, « Data hiding in digital binary image », dans *Proceedings of the IEEE International Conference on Multimedia & Expo*, vol. 1, 2000, p. 393-396.

[ZC91] G. Zémor et G. Cohen, « Error-correcting wom-codes », *IEEE Transactions on Informations Theory*, vol. 37, n° 3, 1991, p. 730–734.

Index

A

Algorithme F5 136
Anneau
  de Galois 19-31
  factoriel 16
  local 19
Application
  d'extraction 111, 113, 115
  d'insertion 111, 113
  de Gray 50
    généralisée 52-55
  de Reed-Solomon 54
  trace 29
Automorphisme de Frobenius . . 26, 46

B

Borne
  code $\mathbb{Z}_{p^k}$-linéaire (cardinal) 93
  d'Elias 95, 98
  de Carlitz-Uchiyama 68
  de Gilbert-Varshamov 95, 98
  de Griesmer 61
  de Hamming 123

C

Carlitz . . . . . voir Borne
Code
  $\mathbb{Z}_{p^k}$-cyclique 54
  $\mathbb{Z}_{p^k}$-dual 55
  $\mathbb{Z}_{p^k}$-linéaire 54
  BCH 70, 71, 143
  concaténé 88
  correcteur d'erreurs centré 140
  cyclique sur $\mathbb{Z}_{p^k}$ 38
  de Golay
    binaire 80, 122
    ternaire 82
  de Gray 49, 69
  de Hamming 119, 121, 130, 135, 143, 144
    décodage 130
  de Kerdock 61
    distribution des poids 62
    généralisé 48, 60, 65
  de Preparata
    généralisé 62
  de résidus quadratiques 82
  de recouvrement 115
    paramètres 115
  de Reed et Muller 51, 60, 61
    généralisé 51, 87-89, 93
  de Reed-Solomon 54, 92, 145
  de Varshamov-Tenengolts . . 130, 133
    décodage 131
  distance-invariant 55
  dual 34, 41, 64
  en blocs 11
  linéaire sur $\mathbb{Z}_{p^k}$ 33
  paramètres d'un 55
  parfait 81, 122, 123
  quasi cyclique 103
  relevé 40, 54
  translaté 117
Copyright 108

D

Décodage de syndrome 118
  du code de Hamming 130
  problème de décision 119
Démarate 107
Distance
  de Hamming 115
  de Kullback-Leiber 120
  de Lee 50, 53
  minimale 55
    de $\mathcal{K}(2^k, m)$ 70
    de $\mathcal{K}(2^k, m)$ 68
    de $\mathcal{K}(p^k, m)$ 68
    de $\mathcal{P}(2^k, m)$ 70

Distorsion maximale... voir Schéma de dissimulation
Dualité formelle 58

E

Égalité de Poisson 36
Elias ..... voir Borne
Encodage
  matriciel 114, 127, 137, 138
  par translatés 127
Entropie
  q-aire 95
  binaire 123
  relative 120

F

Filigrane 108
Fonction
  courbe 61, 90
Forme
  affine 60
  linéaire 29
Fourier ..... voir Transformée
Frobenius ..... voir Automorphisme

G

Galois ..... voir Anneau
Gilbert ..... voir Borne
Golay ..... voir Code
Gray ..... voir Application et Code
Griesmer ..... voir Borne

H

Hérodote 107
Hadamard ..... voir Transformée
Hamming ..... voir Borne, Code et Polynôme
Hensel ..... voir Relèvement et Relevé
Histiée 107

I

Idéal
  de $\mathbb{Z}_{p^k}[X]/(X^n - 1)$ 38
Idempotent 42, 43
Identité de MacWilliams
  pour $\mathbb{Z}_{p^k}$ 35
Isométrie 50

J

JPEG 136

K

Kerckhoffs ..... voir Principe
Kerdock ..... voir Code et Distance
Kullback ..... voir Entropie relative

L

Lee ..... voir Distance et Poids
Leiber ..... voir Entropie relative

M

Mémoire
  à écriture
    contrainte 127, 140
    limitée 127, 140
  non effaçable 127, 143
MacWilliams ..... voir Identité
Matrice
  de parité 117
Matrice génératrice 34, 41
McEliece ..... voir Théorème
Modèle
  à adversaire actif 139
  à adversaire passif 115, 127
Muller ..... voir Code

N

NP-complétude 120
Numéro de série 108

P

Poids
  de Lee 50
  homogène 52, 67
Poisson ..... voir Égalité
Polynôme
  énumérateur des poids
    complets 35
    de Hamming 37, 56
    symétrisés 56
  B-polynôme 17, 64, 65
  de contrôle 41
  de Mattson-Solomon 44, 45
Preparata ..... voir Code et Distance
Principe de Kerckhoffs (second) ... 112
Problème
  de décision ..... voir Décodage de syndrome

des prisonniers 107

R

Résistance . . . . . voir Schéma de dissimulation
Rayon de recouvrement 115, 130
Reed . . . . . voir Application et Code
Relèvement de Hensel 16, 40, 54
Relevé de Hensel 16, 17
Représentation
  des éléments de $GR(p^k, m)$
    additive 21, 24
    changement de 22
    multiplicative 21, 24
  des codes par la trace 47
  des images
    fréquentielle 114, 137
    spatiale 114, 136
RVB 136

S

Schéma de dissimulation 113
  clef secrète d'un 111, 112
  construction 118
  distorsion maximale d'un 113
  paramètres d'un 113, 140
  résistance d'un 140
  sécurité d'un 120
Solomon . . . . . voir Application et Code
Somme direct de codes 125
Somme directe 143, 144
Stéganographie 107
Syndrome 117

T

Tatouage 108
Taux de transmission 62, 98
Teichmuller 21, 60
Tenengolts . . . . . voir Code
Théorème de McEliece 68
Théorie de la complexité 120
Trace . . . . . voir Application
Transformée
  de Fourier 43, 114
  de Hadamard 36
  en cosinus 137

U

Uchiyama . . . . . voir Borne

V

Varshamov . . . . . voir Borne et Code

Z

Zéro (d'un code cyclique sur $\mathbb{Z}_{p^k}$) . . 39

Table des figures

3.1 Application de Gray. 50

6.1 Bornes sur les codes $\mathbb{Z}_8$-linéaires 99
6.2 Bornes sur les codes $\mathbb{Z}_{16}$-linéaires 99
6.3 Bornes sur les codes $\mathbb{Z}_{32}$-linéaires 100

Liste des tableaux

4.1 Paramètres, taux de transmission et distance relative des codes de Kerdock et de Reed et Muller en petite longueur. 62
4.2 Codes de Kerdock et Preparata généralisés. 73
4.3 Extrait de la table de Brouwer (binaire). 74
4.4 Extrait de la table de Litsyn. 75
4.5 Duaux des codes BCH. 75
4.6 Borne sur la distance minimale du code de Kerdock généralisé. 76
4.7 Codes de Kerdock généralisés, $p = 3$ 77
4.8 Codes BCH sur $\mathbb{Z}_3$ 77
4.9 Codes de Kerdock généralisés, $p = 5$ 78
4.10 Codes BCH sur $\mathbb{Z}_5$ 78

5.1 Distance minimale des codes $\Psi\left(\mathrm{QR}_n^{(k)+}\right)$. 85
5.2 Deuxième extrait de la table de Brouwer (binaire). 85

6.1 Codes obtenus par la construction du théorème 6.2 avec des codes $\mathbb{Z}_8$-linéaires. 90
6.2 Codes obtenus par la construction du théorème 6.2 avec des codes $\mathbb{Z}_{16}$-linéaires. 91

Table des matières

Première partie : codes $\mathbb{Z}_{p^k}$-linéaires

Introduction 11

1 Préliminaires 15
- 1.1 Relèvement de Hensel . . . 15
- 1.2 Anneaux de Galois . . . 19

2 Codes sur l'anneau $\mathbb{Z}_{p^k}$ 33
- 2.1 Codes linéaires sur $\mathbb{Z}_{p^k}$ . . . 33
- 2.2 Codes cycliques sur $\mathbb{Z}_{p^k}$ . . . 38
- 2.3 Polynôme de Mattson-Solomon . . . 43

3 Codes $\mathbb{Z}_{p^k}$-linéaires 49
- 3.1 Application de Gray généralisée . . . 49
- 3.2 Codes $\mathbb{Z}_{p^k}$-linéaires . . . 54

4 Codes de Kerdock généralisés 59
- 4.1 Structure $\mathbb{Z}_{p^k}$-linéaire . . . 60
- 4.2 Structure $\mathbb{Z}_{p^k}$-cyclique . . . 63
- 4.3 Borne sur la distance minimale . . . 67
- 4.4 Distance minimale en petite longueur . . . 69

5 Relevés des codes de résidus quadratiques 79
- 5.1 Code de Duursma *et al.* [DGL+01] . . . 79
- 5.2 Code de Greferath et Schmidt [GS99] . . . 81
- 5.3 Relevés des codes de résidus quadratiques . . . 82

6 Construction fondée sur les translatés de codes $\mathbb{Z}_{p^k}$-linéaires 87
- 6.1 Principe de la construction . . . 87
- 6.2 Quelques applications . . . 90
- 6.3 Bornes sur le cardinal des codes $\mathbb{Z}_{p^k}$-linéaires . . . 93

Conclusion et perspectives 98

Seconde partie : schémas de dissimulation

Introduction 107

7 Position du problème 111
7.1 Cadre général . . . 111
7.2 Modèle adopté . . . 112
7.3 État de l'art . . . 113

8 Modèle avec adversaire passif 115
8.1 Problème équivalent . . . 115
8.2 Construction par des codes de recouvrement linéaires . . . 116
8.3 Sécurité de la construction . . . 120
8.4 Borne sur la capacité . . . 122
8.5 Schémas asymptotiquement optimaux . . . 124
8.6 Relation avec l'écriture sur les mémoires . . . 127

9 Réécriture de travaux précédents 129
9.1 Codes de Hamming et de Varshamov-Tenengolts . . . 129
9.2 Les schémas [WL98] et [PCT00] . . . 132
9.3 Les schémas [TP01, TP02] et [Hio03] . . . 133
9.4 Les schémas [CJL+03, CJL+04] et [Wes01] . . . 136

10 Modèle avec adversaire actif 139
10.1 Problème équivalent . . . 139
10.2 Borne sur le nombre de messages . . . 140
10.3 Schémas asymptotiquement proches de l'optimal . . . 142

Conclusion et perspectives 146

Bibliographie 148
Index 156