INRIA

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

Codes $\mathbb{Z}_{2^k}$-linéaires

Fabien Galand

N° 5073

Janvier 2004

THÈME 2

ISSN 0249-6399 ISRN INRIA/RR--5073--FR

INRIA
ROCQUENCOURT

Codes $\mathbb{Z}_{2^k}$-linéaires

Fabien Galand*

Thème 2 — Génie logiciel
et calcul symbolique
Projet CODES

Rapport de recherche n° 5073 — Janvier 2004 — 64 pages

Résumé : Après une présentation générale des codes $\mathbb{Z}_{2^k}$-linéaires, nous donnons la distance minimale des codes de Kerdock généralisés en petite longueur, obtenue par ordinateur. Une borne laissait espérer que cette famille de codes avait de bons paramètres, mais nos résultats infirment cette hypothèse. Nous donnons également les distances minimales de plusieurs codes construits par relèvement de Hensel et redescente par l'application de Gray généralisée, ce qui nous conduit à trois codes ayant les même paramètres que les meilleurs codes linéaires connus. Finalement, nous présentons une construction de codes binaires basée sur les codes $\mathbb{Z}_{2^k}$-linéaires et en dérivons une borne sur le cardinal des codes $\mathbb{Z}_{2^k}$-linéaires.

Mots-clés : anneaux de Galois, application de Gray, borne, construction, distance minimale, codes de Kerdock généralisés, codes de résidus quadratiques, relèvement de Hensel

* INRIA Roquencourt

Unité de recherche INRIA Rocquencourt
Domaine de Voluceau, Rocquencourt, BP 105, 78153 Le Chesnay Cedex (France)
Téléphone : +33 1 39 63 55 11 — Télécopie : +33 1 39 63 53 30

$\mathbb{Z}_{2^k}$-Linear Codes

Abstract: After presenting the general properties of $\mathbb{Z}_{2^k}$-linear codes, we give the minimum distance of generalized Kerdock codes of short length. A lower bound on their minimum distance let the possibility for those codes to have good minimum distances, but our results show this is not the case, at least for short lengths. We also compute the minimum distances of several binary codes constructed by Hensel lift and generalized Gray map. This leads to three codes with the same parameters as the best known linear codes. We conclude with a construction of binary codes using $\mathbb{Z}_{2^k}$-linear codes and with upper bounds on the cardinalities of $\mathbb{Z}_{2^k}$-linear codes induced by this construction.

Key-words: bound, construction, Galois ring, Gray map, generalized Kerdock codes, Hensel lift, minimum distance, quadratic residue codes

Table des matières

1 Introduction **5**

2 Préliminaires **6**
2.1 Relèvement de Hensel 6
2.2 Anneaux de Galois 9

3 Codes sur l'anneau $\mathbb{Z}_{2^k}$ **19**
3.1 Codes linéaires sur $\mathbb{Z}_{2^k}$ 19
3.2 Codes cycliques sur $\mathbb{Z}_{2^k}$ 21

4 Codes $\mathbb{Z}_{2^k}$-linéaires **26**
4.1 Application de Gray généralisée 26
4.2 Codes $\mathbb{Z}_{2^k}$-linéaires 29

5 Codes de Kerdock généralisés **32**
5.1 Structure $\mathbb{Z}_{2^k}$-linéaire 32
5.2 Structure $\mathbb{Z}_{2^k}$-cyclique 34
5.3 Distance minimale en petite longueur 40

6 Autres exemples de codes $\mathbb{Z}_{2^k}$-linéaires **46**
6.1 Code de Duursma et al. [DGLS01] 46
6.2 Code de Greferath et Schmidt [GS99] 48
6.3 Relevés des codes de résidus quadratiques 49

7 Construction de codes binaires à base de translatés de codes $\mathbb{Z}_{2^k}$-linéaires **50**
7.1 Principe de la construction 51
7.2 Quelques applications 53

8 Bornes sur le cardinal des codes $\mathbb{Z}_{2^k}$-linéaires **55**

9 Conclusions **59**

Bibliographie **62**

Liste des tableaux

1 Codes de Kerdock et Preparata généralisés. 42
2 Extrait de la table de Brouwer (binaire). 43
3 Extrait de la table de Litsyn. 44
4 Duaux des codes BCH. 44

5 Borne sur la distance minimale du code de Kerdock généralisé. 45
6 Distance minimale des codes $\Psi(\mathrm{QR}_n^{(k)+})$. 50
7 Deuxième extrait de la table de Brouwer (binaire). 50
8 Codes obtenus par la construction du Théorème 7.2 avec des codes $\mathbb{Z}_8$-linéaires. 53
9 Codes obtenus par la construction du Théorème 7.2 avec des codes $\mathbb{Z}_{16}$-linéaires. 54
10 Code de Kerdock généralisé, $p = 3$. 59
11 Extrait de la table de Brouwer (ternaire). 60

Table des figures

1 Application de Gray. 27
2 Exemples de bornes sur les codes $\mathbb{Z}_{2^k}$-linéaires 58

1 Introduction

Au début des années 90, dans leur article [HKC+94], Hammons et al. donnent une construction très simple de certains codes binaires non linéaires figurant parmi les meilleurs connus – notamment les codes de Kerdock et de Preparata – en les considérant comme des images de codes linéaires sur $\mathbb{Z}_4$, l'anneau des entiers modulo 4. 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, A.A. Nechaev, dans [Nec91], avait également donné une construction des codes de Kerdock utilisant l'anneau $\mathbb{Z}_4$.

L'approche utilisée consiste à construire des codes linéaires sur $\mathbb{Z}_4$ – c.a.d. 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 se fait 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 les codes binaires ainsi obtenus peuvent être "bons". Depuis son apparition, cette technique a très largement fait ses preuves comme peuvent en témoigner les travaux de Bonnecaze et al., Calderbank et al., et de Pless et Qian (voir respectivement [BSC95], [CMKH96], [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 C. Carlet dans [Car98], puis une seconde. Elle a ensuite été adaptée, par M. Greferath et S.E. Schmidt dans [GS99], aux anneaux $\mathbb{Z}_{p^k}$ (p premier) la généralisation de C. Carlet. 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 [DGLS01]).

Dans [Car98], C. 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 donne 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 fut un peu éloignée de la véritable distance minimale de ces codes. Nous donnons dans ce rapport 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, et de Duursma et al. 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 généralisée. C'est ainsi que nous avons considéré les codes de résidus quadratiques qui semblent bien se prêter à ce type de construction : en effet, ces codes nous ont permis d'obtenir trois nouveaux codes égalant les meilleurs codes linéaires de même longueur et cardinalité.

De plus dans [DGLS01], 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. Nous généralisons cette technique à tout code $\mathbb{Z}_{2^k}$-linéaire et nous en déduisons une borne sur les cardinaux de ces codes.

2 Préliminaires

2.1 Relèvement de Hensel

Lemme 2.1 (Lemme de Hensel, [Mac74, Chp. 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, i.e. 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 $P \in \mathbb{Z}_{p^k}[X]$:

$$P \equiv f_1^{e_1} \ldots, f_l^{e_l} \pmod{p} ,$$

où $f_1, \ldots, f_l$ sont des polynômes irréductibles de $\mathbb{Z}_p[X]$ et $e_1, \ldots, e_l$ des entiers strictement positifs. Le Lemme 2.1 donne donc par induction sur le nombre de facteurs :

Théorème 2.2 (Relèvement de Hensel, [Mac74, Chp. 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. Il existe un unique l-uplet $(g_1^{(k)}, \ldots, g_l^{(k)})$ de polynômes unitaires de $\mathbb{Z}_{p^k}[X]$, tel que*

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

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

Proposition 2.4 *Soit $Q \in \mathbb{Z}_p$ un facteur de $X^n - 1$. Son relevé de Hensel d'ordre k divise $X^n - 1$ dans $\mathbb{Z}_{p^k}[X]$.*

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. $p = 2$. On donne donc 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 [VG99].

Proposition 2.5 (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 degrés pairs et I ceux de degrés impairs. 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, choisi pour que Q^{k+1} soit unitaire.*

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

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

(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

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

avec $A(X)$, $B(X) \in \mathbb{Z}_{2^{k+1}}[X]$ et

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

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].

Alors

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

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

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

Il en résulte que le polynôme $f(X^2)$ 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 2.6 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 2.5 pour calculer son relevé d'ordre 3 (un B-polynôme avec notre définition). On a

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

donc

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

d'où,

$$\begin{aligned} Q^{(2)}\left(X^2\right) &= X^6 + 2X^4 + X^2 - 1 \mod 4 \ , \\ &= X^3 + 2X^2 + X - 1 \mod 4 \ . \end{aligned}$$

De même,

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

donne

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

On a donc

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

soit, finalement

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

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

$$Q^{(3)}(X)\left(X^4 + 2X^3 + 7X^2 + 5X + 1\right) = X^7 - 1 \mod 8 \ .$$

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

2.2 Anneaux de Galois

Proposition 2.7 *Soient p un nombre premier, k un entier strictement positif et $P \in \mathbb{Z}_{p^k}[X]$ un B-polynôme. L'anneau $\mathbf{A} = \mathbb{Z}_{p^k}[X]/(P)$ est de caractéristique p^k et de cardinal p^{km}. L'ensemble des éléments non inversibles forme un idéal engendré par p et cet idéal est le seul idéal maximal de A. De plus, l'anneau quotient $\mathbf{A}/(p)$ est un corps fini à p^m éléments.*

PREUVE. La caractéristique de l'anneau découle de l'inclusion $\mathbb{Z}_{p^k} \subset \mathbf{A}$ et son cardinal est une conséquence directe de la définiton 2.8.
On a (cf. [Hun80, Th. 2.12])

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

Or, $P \bmod p$ est irréductible (P est un B-polynôme) et de degré m, donc

$$\mathbf{A} \simeq \mathbb{F}_{p^m} \quad . \tag{*}$$

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 $\alpha \in \mathbf{A}$, on vérifie aisément qu'il est inversible si et seulement si $\alpha \bmod p$ est inversible. Ainsi, les éléments non inversibles de l'anneau $\mathbf{A}$ sont exactement ceux qui valent 0 modulo p, i.e. ce sont les éléments de l'idéal (p). D'autre part, soit $\mathcal{I} \subset \mathbf{A}$ un idéal. Si $\mathcal{I}$ contient un élément inversible alors $\mathcal{I} = \mathbf{A}$. Donc $\mathcal{I} \subset (p)$, ce qui termine la preuve. □

Définition 2.8 (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. Ceci motive la notation suivante :

Notation 2.9 (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 noté x, i.e. $x = X \bmod P(X)$. Le B-polynôme définissant $\mathrm{GR}(p^k, m)$ sera systématiquement noté P.*

Notation 2.10 *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 2.11 *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. *il engendre un groupe multiplicatif d'ordre $p^m - 1$,*

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

(par la propriété précédente, tout élément de $\mathcal{T}^*$ est donc inversible dans $\mathcal{T}^*$).

Les éléments d'un anneau de Galois peuvent être représentés de deux manières différentes.

Proposition 2.12 (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*

$$\alpha = \sum_{i=0}^{m-1} \lambda_i x^i \quad \textit{avec } (\lambda_i) \in {\mathbb{Z}_{p^k}}^m \ .$$

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

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

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 et l'unicité de la représentation multiplicative sont des conséquences directes de l'algorithme de conversion détaillé ci-dessous. □

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 représentation 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). 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'anneau. 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, on peut 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 d'après la Proposition 2.12 cette dernière est unique.

Exemple 2.13 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 :

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

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

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

Ce qui donne

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

$$\begin{aligned}\alpha+\beta &= \left(5+3x^2\right)+(x) &&= 5+x+3x^2\\ \alpha\beta &= \left(5+3x^2\right)(x) = 5x+3\left(-7-5x-6x^2\right) &&= 3+6x+6x^2\end{aligned}$$

- 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 calculs 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.

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

□

Lemme 2.14 *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 $\mathbb{F}_{p^m}$. Alors il existe un unique élément $\alpha \in \mathrm{GR}(p^k, m)$ vérifiant $Q(\alpha) = 0$ et $\chi(\alpha) = \overline{\beta}$.*

PREUVE. Pour prouver ce lemme, on utilise une généralisation du Lemme 2.1, 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 $\mathbb{F}_{p^m}$ (de même pour le Théorème 2.2, cf. [Mac74, Th. XIII.4 et Th. XIII.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 2.1 implique

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

pour $S(X), R(X) \in \mathrm{GR}(p^k, m)[X]$ unitaires, $\beta \in \mathrm{GR}(p^k, m)$ tels que $\chi(R) = \overline{R}$ et $\chi(\beta) = \overline{\beta}$. De plus, $X - \beta + pS(X)$ est unitaire et son degré doit être égal à $\deg((X - \overline{\beta})) = 1$. Donc nécessairement $pS(X) = p\beta' \in \mathrm{GR}(p^k, m)$. En posant $\alpha = \beta + p\beta'$, (*) donne

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

Donc, $Q(\alpha) = 0$ et comme $\chi(\alpha) = \overline{\beta}$, l'existence est prouvée.
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 2.15 *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 $\alpha \in \mathcal{T}^*$.*

PREUVE. Commençons par rappeler qu'un polynôme de degré n, irréductible sur $\mathbb{F}_p[X]$ est simplement scindé dans $\mathbb{F}_{p^n}[X]$ et que si on note $\overline{\alpha}$ l'une de ses racines, l'ensemble des racines du polynôme est simplement $\left\{\overline{\alpha}, \overline{\alpha}^p, \ldots, \overline{\alpha}^{p^{n-1}}\right\}$.
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 2.14, 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 2.11 implique que ces éléments sont des racines et le Lemme 2.14 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 preuve. □

Considérons l'application définie par

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

Cette application a des propriétés très proches de l'automorphisme de Frobenius des corps finis.

Théorème 2.16 (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, i.e.

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

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, $P_\alpha(X), P_\beta(X), P_{\alpha\beta}(X) \in \mathbb{Z}_{p^k}[X]$ et $\alpha \equiv P_\alpha(X) \pmod{P(X)}$, avec P_α de degré strictement inférieur à m, 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 $Q(X) \in \mathbb{Z}_{p^k}[X]$ et $P(X)$ est le B-polynôme utilisé pour définir l'anneau de Galois. Donc,

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

Par la Proposition 2.15, on a $P(x^p) = 0$, et par conséquent la propriété 2 est vérifiée. Et on a donc que σ est un endomorphisme de $\mathrm{GR}(p^k, m)$.
Soit $\beta = x^j$ un élément de $\mathcal{T}^*$. Par la propriété 2, on a $\sigma(x^j) = \sigma(x)^j = x^{p\,j}$. Donc pour une forme multiplicative $\sum_{i=0}^{k-1} \mu_i p^i$, on a

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

Cette dernière expression de σ permet de prouver simplement que c'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. $\alpha = \beta$. Ayant déjà prouvé que σ est un endomorphisme, il en résulte que c'est un automorphisme.
Prouvons la dernière partie du théorème. Soit ψ un automorphisme de $\mathrm{GR}(p^k, m)$. Nécessairement, ψ est l'identité sur $\mathbb{Z}_{p^k}$, car $\psi(1) = 1$ et $\psi(\alpha + \beta) = \psi(\alpha) + \psi(\beta)$ par définition d'un automorphisme d'anneau. Donc $P(\psi(x)) = \psi(P(x)) = 0$ et par la Proposition 2.15,

$\psi(x)$ 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 2.17 (Indépendance linéaire de $\mathcal{A}(p^k, m)$) *Les automorphismes de l'anneau* $\mathrm{GR}(p^k, m)$ *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. Soit n minimal pour une relation du type

$$\alpha_1\psi_1 + \cdots + \alpha_n\psi_n = 0 \ . \tag{*}$$

Alors, pour tout y

$$\begin{aligned}\alpha_1\psi_1(xy) + \cdots + \alpha_n\psi_n(xy) &= \alpha_1\psi_1(x)\psi_1(y) + \cdots + \alpha_n\psi_n(x)\psi(y) \ , \\ &= 0 \ .\end{aligned} \tag{**}$$

L'élément x étant inversible, $\psi_i(x)$ l'est également et son inverse est simplement $\psi_i(x^{-1})$. Posons $x' = \psi_i(x^{-1})$, on a en multipliant (**) par x' et en soustrayant à (*)

$$\begin{aligned}&\alpha_1\left(1 - x'\psi_1(x)\right)\psi_1(y) + \alpha_2\left(1 - x'\psi_2(x)\right)\psi_2(y) + \cdots + \alpha_n\left(1 - x'\psi_n(x)\right)\psi_n(y) \\ &\qquad = \alpha_2\left(1 - x'\psi_2(x)\right)\psi_2(y) + \cdots + \alpha_n\left(1 - x'\psi_n(x)\right)\psi_n(y) \ , \\ &\qquad = 0 \ .\end{aligned}$$

Or clairement il existe $i \in [2, n]$ tel que $x'\psi_i(x) \neq 1$, ce qui contredit le caractère minimal de n et conclut la preuve. □

L'automorphisme de Frobenius permet, de manière similaire aux 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 2.18 *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 2.16 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 par 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 $\mathcal{T}^*$ qui est un groupe multiplicatif de cardinal p^m-1, p ne divisant pas p^m-1 la seule solution est $\mu_i = 1$. Donc $\mu_i \in \{0,1\}$ et par consequent $\alpha \in \mathbb{Z}_{p^k}$. □

L'importance de l'application Tr vient du théorème suivant :

Théorème 2.19 *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* $\alpha \mapsto \mathrm{Tr}(\beta\alpha)$ *pour un certain* $\beta \in \mathrm{GR}(p^k,m)$.

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 2.12, 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 (i.e. linéairement indépendante) de m éléments de la forme $\alpha \mapsto \mathrm{Tr}(\beta\alpha)$. Prouvons que la famille

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

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

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

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

$$\begin{aligned} b_0\mathrm{Tr}(x^0\alpha) + b_1\mathrm{Tr}(x^1\alpha) + \cdots + b_{m-1}\mathrm{Tr}(x^{m-1}\alpha) &= \mathrm{Tr}\left(\sum_{i=0}^{m-1} b_i x^i \alpha\right) \ , \\ &= \mathrm{Tr}(\beta\alpha) \ , \\ &= (b_0, \ldots, b_{m-1}) \cdot T \cdot {}^t(a_0, \ldots, a_{m-1}) \ . \end{aligned}$$

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 $T = S \cdot {}^tS$, en effet

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

(car σ^k est dans $\mathcal{A}(p^k, m)$ d'après le Théorème 2.16)

$$= \mathrm{Tr}(x^i x^j) \ .$$

Or il résulte du Lemme 2.17 que $\det(S)$ est inversible : dans le cas contraire, S serait non inversible, i.e. il existerait $(\alpha_1, \ldots, \alpha_m) \in \mathrm{GR}(p^k, m)^m$ non nul tel que

$$(\alpha_0, \ldots, \alpha_{m-1}) \cdot S = 0 \ ,$$

ce qui équivaut à

$$\alpha_0 x^i + \alpha_1 \sigma(x^i) + \cdots + \alpha_{m-1}\sigma^{m-1}(x^i) = 0$$

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

$$\alpha_0 Id + \alpha_1 \sigma + \cdots + \alpha_{m-1}\sigma^{m-1} = 0 \ ,$$

puisque tout élément de $\mathrm{GR}(p^k, m)$ s'écrit de façon unique comme combinaison linéaire sur $\mathbb{Z}_{2^k}$ de $1, x, \ldots, x^{m-1}$. D'après le Théorème 2.16, les σ^i, pour $i \in [0, m-1]$ sont des automorphismes 2 à 2 distincts, 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. □

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

3.1 Codes linéaires sur $\mathbb{Z}_{2^k}$

Définition 3.1 (Code linéaire sur $\mathbb{Z}_{2^k}$) *Un code $\mathbf{C}_{2^k}$ linéaire de longueur n sur $\mathbb{Z}_{2^k}$ est un sous-module de ${\mathbb{Z}_{2^k}}^n$.*

Contrairement aux espaces vectoriels, les $\mathbb{Z}_{2^k}$-modules n'admettent pas nécessairement une 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 3.2 (Matrice génératrice) *On appelle matrice génératrice du code $\mathbf{C}_{2^k}$ toute matrice de $\mathcal{M}(\mathbb{Z}_{2^k})$ 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 3.3 (Codes équivalents) *Soient $\mathbf{C}_{2^k}$ et $\mathbf{C}'_{2^k}$ deux codes linéaires sur $\mathbb{Z}_{2^k}$ de matrice génératrice G et G' respectivement. Les codes $\mathbf{C}_{2^k}$ et $\mathbf{C}'_{2^k}$ sont dit équivalents si il existe une matrice de permutation P telle que*

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

Théorème 3.4 ([CS95, §2]) *Soit $\mathbf{C}_{2^k}$, un code linéaire sur $\mathbb{Z}_{2^k}$. À une permutation des coordonnées près, $\mathbf{C}_{2^k}$ admet une matrice génératrice dite de forme normale*

$$G = \begin{pmatrix} I_{l_0} & A_{0,1} & \cdots\cdots\cdots\cdots & A_{0,k} \\ 0 & 2I_{l_1} & 2A_{1,2} & \cdots\cdots & 2A_{1,k} \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots. & 0 & 2^{k-1}I_{l_{k-1}} & 2^{k-1}A_{k-1,k} \end{pmatrix} ,$$

où les $A_{i,j}$ sont des matrices $l_i \times l_j$ à coefficients dans $\{0,1\}$ et I_{l_i} est la matrice identité de taille l_i.

Corollaire 3.5 *Avec les notations du théorème précédent, $\mathbf{C}_{2^k}$ a $\prod_{i=0}^{k-1} 2^{(k-i)\,l_i}$ éléments.*

On définit le produit scalaire sur ${\mathbb{Z}_{2^k}}^n$ par

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

les opérations étant effectuées dans $\mathbb{Z}_{2^k}$. Ce produit scalaire permet de définir une notion de dualité sur $\mathbb{Z}_{2^k}$.

Définition 3.6 (Code dual sur $\mathbb{Z}_{2^k}$) *Soit $\mathbf{C}_{2^k}$ un code linéaire sur $\mathbb{Z}_{2^k}$, on appelle code dual du code $\mathbf{C}_{2^k}$, et on note $\mathbf{C}_{2^k}^{\perp}$, le sous-module de ${\mathbb{Z}_{2^k}}^n$ défini par*

$$\mathbf{C}_{2^k}^{\perp} = \left\{ \mathbf{a} \;\middle|\; \forall \mathbf{b} \in \mathbf{C}_{2^k}, \quad \mathbf{a} \cdot \mathbf{b} = 0 \right\} \ .$$

Lorsque la matrice génératrice du code $\mathbf{C}_{2^k}$ est sous forme normale, la matrice génératrice du code dual se met sous la forme

$$G^\perp = \begin{pmatrix} B_{0,0} & B_{0,1} & B_{0,2} & \dots\dots\dots & I_{l_k} \\ 2B_{1,0} & 2B_{1,1} & 2B_{1,2} & \dots \; 2I_{l_{k-1}} & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 2^{k-1}B_{k-1,0} & 2^{k-1}I_{l_1} & 0 & \dots\dots\dots & 0 \end{pmatrix} ,$$

où les $B_{i,j}$ sont de dimensions $l_{k-i} \times l_j$ et à coefficients dans $\{0,1\}$. Cela a la conséquence suivante :

Proposition 3.7 ([CS95, §1]) *Avec les notations du Théorème 3.4, le code $\mathbf{C}_{2^k}^\perp$ a $\prod_{i=0}^{k-1} 2^{i\,l_i}$ éléments.*

La notion de dualité pour des codes linéaires sur $\mathbb{Z}_{2^k}$ est proche de celle définie pour les codes linéaires (sur un corps finis). Entre autres :

Proposition 3.8 ([CS95, §1]) *Soit $\mathbf{C}_{2^k}$ un code linéaire sur $\mathbb{Z}_{2^k}$. Le code dual de $\mathbf{C}_{2^k}^\perp$ est le code $\mathbf{C}_{2^k}$ lui-même.*

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

Théorème 3.9 (Identité de MacWilliams pour $\mathbb{Z}_{2^k}$) *Soit $\mathbf{C}_{2^k}$ un code linéaire sur $\mathbb{Z}_{2^k}$. On pose $\omega = e^{\frac{2i\pi}{2^k}}$. Les polynômes énumérateurs des poids complets de $\mathbf{C}_{2^k}$ et de $\mathbf{C}_{2^k}^\perp$ vérifient*

$$CW_{\mathbf{C}_{2^k}^\perp}(X_0, \dots, X_{2^k-1}) = \frac{1}{|\mathbf{C}_{2^k}|} CW_{\mathbf{C}_{2^k}} \left(\sum_{i=0}^{2^k-1} \omega^{0i} X_i, \sum_{i=0}^{2^k-1} \omega^{i} X_i, \dots, \sum_{i=0}^{2^k-1} \omega^{(2^k-1)i} X_i \right) .$$

3.2 Codes cycliques sur $\mathbb{Z}_{2^k}$

Dans toute cette section, on se restreint au cas où *la longueur n des codes est un entier impair.*

Définition 3.10 (Code cyclique sur $\mathbb{Z}_{2^k}$) *Un code $\mathbf{C}_{2^k}$ de longueur n sur l'anneau $\mathbb{Z}_{2^k}$ est dit cyclique si il est linéaire et si il est invariant par l'application shift définie par*

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

Un code cyclique sur $\mathbb{Z}_{2^k}$ est donc le pendant exact d'un code cyclique sur $\mathbb{Z}_2$. Ainsi, l'application

$$\begin{array}{cccc} \phi: & {\mathbb{Z}_{2^k}}^n & \longrightarrow & \mathbb{Z}_{2^k}[X]/(X^n - 1) \\ & \mathbf{v} = (v_0, \dots, v_{n-1}) & \longmapsto & \phi(\mathbf{v}) = \sum_{i=0}^{n-1} v_i X^i \end{array}$$

est un isomorphisme de $\mathbb{Z}_{2^k}$-module qui envoie les codes cycliques sur $\mathbb{Z}_{2^k}$ sur les idéaux de l'anneau quotient $\mathbb{Z}_{2^k}[X]/(X^n-1)$. On peut donc assimiler code cyclique sur $\mathbb{Z}_{2^k}$ et idéal de $\mathbb{Z}_{2^k}[X]/(X^n-1)$. Comme dans le cas des corps finis, l'anneau $\mathbb{Z}_{2^k}[X]/(X^n-1)$ est principale. Cependant, la structure de ses idéaux est plus complexe que celle de $\mathbb{F}_q[X]/(X^n-1)$:

Notation 3.11 *On note $\mathcal{R}$ l'anneau quotient $\mathbb{Z}_{2^k}[X]/(X^n-1)$.*

Théorème 3.12 (Idéaux de $\mathcal{R}$, [CS95, §3 Th. 6]) *Tout idéal de $\mathcal{R} = \mathbb{Z}_{2^k}[X]/(X^n-1)$ admet un générateur de la forme*

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

où les f_i sont unitaires et vérifient

$$f_{k-1} \mid f_{k-2} \mid \ \ldots \ \mid f_1 \mid f_0 \mid X^n - 1 \ .$$

De plus, un générateur de la forme ci-dessus est unique.

Corollaire 3.13 *L'anneau $\mathcal{R}$ a $(k+1)^r$ idéaux distincts, où r désigne le nombre de facteurs irréductibles de X^n-1 dans $\mathbb{Z}_{2^k}[X]$.*

Nous allons essentiellement nous intéresser aux idéaux pour lesquels

$$f_0 = f_1 = \cdots = f_{k-1} \ .$$

Cet intérêt provient du fait que ces idéaux s'obtiennent par relèvement de Hensel des codes cycliques sur $\mathbb{F}_2$. En effet, le générateur $g(X)$ de tout code cyclique binaire est un diviseur unitaire de X^n-1 dans $\mathbb{F}_2[X]$ (donc sans facteur multiple), on peut donc lui appliquer le relèvement de Hensel, on obtient ainsi un diviseur (unitaire) $g^{(k)}(X)$ de X^n-1 dans $\mathbb{Z}_{2^k}[X]$, donc (Théorème 3.12) un générateur d'un idéal pour lequel $f_0 = f_1 = \cdots = f_{k-1} = g^{(k)}$.

Définition 3.14 *Soient $g(X) \in \mathbb{F}_2[X]$ un diviseur de X^n-1 et $g^{(k)}(X) \in \mathbb{Z}_{2^k}(X)$ son relevé de Hensel d'ordre k. Le code $\mathbf{C}_{2^k} = \left(g^{(k)}(X)\right) \subset \mathcal{R}$ est appelé le code relevé du code cyclique binaire $\mathbf{C} = (g(X)) \subset \mathbb{F}_2[X]/(X^n-1)$. Le polynôme $g^{(k)}(X)$ est appelé* le *générateur du code $\mathbf{C}_{2^k}$.*

Soit m le plus petit entier tel que $g^{(k)}(X) \mid X^{2^m-1}-1$. Le polynôme $g^{(k)}(X)$ peut s'écrire comme produit de facteurs irréductibles de $X^{2^m-1}-1$, donc par la Proposition 2.15, $g^{(k)}$ a tous ses zéros dans l'anneau de Galois $\mathrm{GR}(2^k, m)$ et ces zéros sont au nombre de $\deg(g^{(k)})$.

Définition 3.15 (Zéros d'un code cyclique sur $\mathbb{Z}_{2^k}$) *Soient $g^{(k)}$ un diviseur unitaire de X^n-1 et $\mathbf{C}_{2^k}$ le code cyclique engendré par $g^{(k)}$. On appelle zéros du code $\mathbf{C}_{2^k}$ l'ensemble des zéros de $g^{(k)}$ dans* $\mathrm{GR}(2^k, m)$.

Proposition 3.16 *Soit $g^{(k)} \in \mathbb{Z}_{2^k}[X]$ 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 $\mathbf{C}_{2^k} = (g^{(k)}) \in \mathcal{R}$ et linéairement indépendante sur $\mathbb{Z}_{2^k}$, i.e. c'est une base de $\mathbf{C}_{2^k}$.

PREUVE. La famille considérée est clairement une famille génératrice de l'idéal $(g^{(k)})$. Montrons qu'elle est linéairement indépendante sur $\mathbb{Z}_{2^k}$. Posons $g^{(k)}(X)h^{(k)}(X) = X^n - 1$ et supposons l'existence d'un $(n-d)$-uplet $(a_i) \in \mathbb{Z}_{2^k}^{n-d}$ tel que $\sum_i a_i X^i g^{(k)}(X) = 0 \in \mathcal{R}$. 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 $A(X) = 0$, soit $(a_i) = 0$. D'où le résultat. □

Corollaire 3.17 *Posons $g^{(k)} = \sum_{i=0}^{d} g_i^{(k)} X^i$. La matrice*

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

est une matrice génératrice (de dimension $n \times (n-d)$) du code $\mathbf{C}_{2^k} = (g^{(k)}) \in \mathcal{R}$, et $\mathbf{C}_{2^k}$ a $2^{k(n-d)}$ 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 3.18 (Polynôme de contrôle) *Le polynôme $h^{(k)}$ est appelé polynôme de contrôle du code $\mathbf{C}_{2^k} = (g^{(k)})$.*

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

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

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

Proposition 3.19 *Soient $\mathbf{C}_{2^k} = (g^{(k)}) \subset \mathcal{R}$ un code cyclique et $h^{(k)}$ son polynôme de contrôle. Le code dual $\mathbf{C}_{2^k}^{\perp}$ est cyclique, engendré par le polynôme réciproque de $h^{(k)}$. Par*

conséquent, la matrice

$$G^{\perp} = \begin{pmatrix} h_{n-d}^{(k)} & h_{n-d-1}^{(k)} & \cdots\cdots & h_0^{(k)} & 0 & \cdots\cdots\cdots & 0 \\ 0 & h_{n-d}^{(k)} & h_{n-d-1}^{(k)} & \cdots & h_0^{(k)} & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots\cdots & 0 & h_{n-d}^{(k)} & h_{n-d-1}^{(k)} & \cdots\cdots & h_0^{(k)} & 0 \\ 0 & \cdots\cdots\cdots\cdots & 0 & h_{n-d}^{(k)} & h_{n-d-1}^{(k)} & \cdots & h_0^{(k)} \end{pmatrix}$$

est une matrice génératrice (de dimension $n \times d$) de $\mathbf{C}_{2^k}^{\perp}$ et $|\mathbf{C}_{2^k}^{\perp}| = 2^{kd}$.

PREUVE. La preuve de l'égalité $\mathbf{C}_{2^k}^{\perp} = (\widetilde{h^{(k)}})$ est semblable à celle pour les corps finis (cf. [MS96, Ch. 7 §4, Th. 4]). Il suffit ensuite d'appliquer le Corollaire 3.17. □

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 3.20 (Idempotent) *Soit $e(X) \in \mathbb{Z}_{2^k}[X]$. Le polynôme e est un idempotent de $\mathcal{R}$ si on a*

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

Théorème 3.21 (Idempotent générateur) *Soit $g^{(k)}$ un diviseur unitaire de $X^n - 1$. Le code cyclique $\mathbf{C}_{2^k} = (g^{(k)}) \subset \mathcal{R}$ admet un unique idempotent générateur $e(X)$. De plus, tout mot $c(X) \in \mathbf{C}_{2^k}$ 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 $\mathbf{C}_{2^k}$. Les polynômes $g^{(k)}$ et $h^{(k)}$ étant premiers entre eux, il existe un couple $(u(X), v(X)) \in (\mathbb{Z}_{2^k}[X])^2$ 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

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

D'où $\mathbf{C}_{2^k} = (g^{(k)}) = (e)$, i.e. e est un générateur du code $\mathbf{C}_{2^k}$. La relation (*) signifie que e est un élément neutre pour le groupe $(g^{(k)})$ munie de la multiplication, cette loi étant commutative, il est nécessairement unique. Terminons la preuve en demontrant la dernière assertion du théorème qui est une simple conséquence des résultats que nous venons d'obtenir : soit $c(X) \in \mathbb{Z}_{2^k}$ vérifiant $c(X) \equiv c(X)e(X) \pmod{X^n - 1}$, clairement $c(X) \in (e(X)) = \mathbf{C}_{2^k}$. Réciproquement, soit $c(X) \in \mathbf{C}_{2^k}$, alors $c(X) \equiv b(X)e(X) \pmod{X^n - 1}$ pour un certain $b(X) \in \mathbb{Z}_{2^k}[X]$. 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 3.22 Le polynôme $g^{(3)}(X) = 7 + 5X + 6X^2 + X^3$ divise $X^7 - 1$ dans $\mathbb{Z}_8[X]$ (voir l'exemple 2.6), 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 avec l'algorithme 15.10 de [VG99] à l'aide du logiciel MAGMA).
D'aprés 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 $\mathbf{C}_{2^k}$, i.e. non seulement $\mathbf{C}_{2^k}$ 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'apparenance 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 [VG99]). 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].

4 Codes $\mathbb{Z}_{2^k}$-linéaires

4.1 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 sequence 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 de permettre 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 $\mathrm{w_L}$, que l'on définit par

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

Proposition 4.1 ([HKC+94, §II.D Th. 1]) *L'application de Gray est une isométrie de* $(\mathbb{Z}_4, \mathrm{w_L})$ *dans* $(\mathbb{Z}_2^2, \mathrm{w_H})$*, i.e.*

1. *c'est une bijection,*

2. $\forall (a,b) \in \mathbb{Z}_4^2 \qquad \mathrm{d_L}(a,b) = \mathrm{d_H}(\Psi(a), \Psi(b))$.

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

FIG. 1: *Application de Gray.*

Cette isométrie est à l'origine de l'explication des bonnes propriétés de certains codes binaires non linéaires (cf. [HKC+94]). On a donc cherché à généraliser l'application de Gray à $\mathbb{Z}_{2^k}$. Malheureusement, quelque soit le poids w dont on munit $\mathbb{Z}_{2^k}$ il n'existe pas d'isométrie entre $(\mathbb{Z}_{2^k}, \mathrm{w})$ et $(\mathbb{Z}_2^k, \mathrm{w_H})$ pour $k \geq 3$ (cf. [SM99]). 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 $\mathbb{Z}_2^{2^{k-1}}$.

Afin de présenter cette généralisation, on identifie les fonctions de m variables à valeurs dans $\mathbb{Z}_2$ à leur table de vérité ($\in \mathbb{Z}_2^{2^m}$) : on numérote (de manière quelconque) les éléments $\mathbf{x}_0, \ldots \mathbf{x}_{2^m-1}$ de $\mathbb{Z}_2^m$ le 2^m-uplet associé à une fonction f définie sur $\mathbb{Z}_2^m$ est alors l'élément dont la ième coordonnée vaut $f(\mathbf{x}_i)$.

Exemple 4.2 On prend $m = 3$ et $f(y_1, y_2, y_3) = y_1 + y_3 \pmod 2$.

	$\mathbf{x}_0$	$\mathbf{x}_1$	$\mathbf{x}_2$	$\mathbf{x}_3$	$\mathbf{x}_4$	$\mathbf{x}_5$	$\mathbf{x}_6$	$\mathbf{x}_7$
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
f	0	1	0	1	1	0	1	0

La fonction f est donc représentée par $(0,1,0,1,1,0,1,0)$. □

On définit alors $\Psi(a)$ comme la fonction booléenne

$$\Psi(a) : (y_1, \ldots, y_{k-1}) \mapsto a_1 y_1 + \cdots + a_{k-1} y_{k-1} + a_k \ , \qquad (*)$$

pour $a \in \mathbb{Z}_{2^k}$ avec $a = \sum_{i=1}^{k} a_i 2^{i-1}$ l'écriture en base 2 de a. Ainsi, Ψ envoie a sur une fonction booléenne affine de $k-1$ variables que l'on identifiera à un élément de $\mathbb{Z}_2^{2^{k-1}}$. Le poids utilisé sur $\mathbb{Z}_2^{2^{k-1}}$ est le poids de Hamming, et sur $\mathbb{Z}_{2^k}$, c'est le poids homogène, que l'on définit pour tout $a \in \mathbb{Z}_{2^k}$ par

$$\mathrm{w_{hom}}(a) = \begin{cases} 0 & \text{si } a = 0, \\ 2^{k-2} & \text{si } a \neq 2^{k-1}, \\ 2^{k-1} & \text{si } a = 2^{k-1}. \end{cases}$$

Proposition 4.3 ([Car98, §II Prop. 1]) *L'application de Gray généralisée définie par* $(*)$ *conserve les distances entre* $(\mathbb{Z}_{2^k}, \mathrm{w_{hom}})$ *et* $(\mathbb{Z}_2^{2^{k-1}}, \mathrm{w_H})$*, i.e.*

$$\forall (a,b) \in \mathbb{Z}_{2^k}^2 \qquad \mathrm{d_{hom}}(a,b) = \mathrm{d_H}(\Psi(a), \Psi(b)) \ .$$

Remarque 4.4 Lorsque $k = 2$ cette généralisation redonne bien 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. □

Notation 4.5 *On notera également* Ψ *l'application de* $\mathbb{Z}_{2^k}^n$ *vers* $\left(\mathbb{Z}_2^{2^k-1}\right)^n = \mathbb{Z}_2^{n(2^k-1)}$ *étendant l'application de gray généralisée coordonnée par coordonnée.*

Exemple 4.6
• $k = 2$: $\Psi(a)$ est une fonction affine de $k-1 = 1$ variable identifiée à 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
$\Psi(a)$	0	y_1	1	$y_1 + 1$

(fonction de 1 variable)

L'ordre sur l'entrée y_1

	$\mathbf{x}_0$	$\mathbf{x}_1$
y_1	0	1

donne la correspondance

	00	01	11	10
$\mathrm{w_H}(\Psi(a))$	0	1	2	1

• $k = 3$: $\Psi(a)$ est une fonction affine de $k-1 = 2$ variables, identifiée à un mot binaire 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
$\Psi(a)$	0	y_1	y_2	y_1+y_2	1	y_1+1	y_2+1	y_1+y_2+1

L'ordre sur les entrées (y_1, y_2)

	$\mathbf{x}_0$	$\mathbf{x}_1$	$\mathbf{x}_2$	$\mathbf{x}_3$
y_1	0	0	1	1
y_2	0	1	0	1

donne la correspondance

	0000	0011	0101	0110	1111	1100	1010	1001
$\mathrm{w_H}(\Psi(a))$	0	2	2	2	4	2	2	2

□

Remarque 4.7 Il existe d'autres généralisations de l'application de Gray : celle de Greferath et Schmidt (cf. [GS99]) qui étend celle présentée dans cette section aux anneaux $\mathbb{Z}_{p^k}$ avec p premier (l'idée générale étant la même, un élément de l'anneau est décomposé en base p et les coefficients de cette décomposition servent à la définition d'un polynôme homogène de degré 1 en $k-1$ variable sur $\mathbb{F}_p$); et celle de Kuzmin et Nechaev (cf. [KN93, KN94]), qu'ils appellent Reed-Solomon map, qui définit une isométrie entre $\mathrm{GR}(p^2, m)$ et un code de longueur p^m sur $\mathbb{F}_{p^m}$, le code de Reed-Solomon de dimension 2.

4.2 Codes $\mathbb{Z}_{2^k}$-linéaires

L'application de Gray introduite à la section §4.1 permet de redescendre un code défini sur $\mathbb{Z}_{2^k}$ de longueur n en un code binaire (non nécessairement linéaire) de longueur $n+k-1$.

Définition 4.8 (Code $\mathbb{Z}_{2^k}$-linéaire) *Un code binaire $\mathcal{C}$ est dit $\mathbb{Z}_{2^k}$-linéaire si c'est l'image par l'application de Gray généralisée Ψ d'un code $\mathbf{C}_{2^k}$ linéaire sur $\mathbb{Z}_{2^k}$. Dans ce cas, le code $\mathbf{C}_{2^k}$ est appelé le code relevé de $\mathcal{C}$.*

Définition 4.9 (Code $\mathbb{Z}_{2^k}$-cyclique) *Un code binaire $\mathcal{C}$ est dit $\mathbb{Z}_{2^k}$-cyclique si il est $\mathbb{Z}_{2^k}$-linéaire et si son code relevé est cyclique sur $\mathbb{Z}_{2^k}$.*

Remarque 4.10 Avec nos définitions, un code relevé peut désigner deux types de codes : soit l'antécédent par l'application de Gray généralisée d'un code $\mathbb{Z}_{2^k}$-linéaire (cf. les deux définitions précédentes), soit un code cyclique sur $\mathbb{Z}_{2^k}$ obtenu en appliquant le relèvement de Hensel au générateur d'un code cyclique binaire (Définition 3.14). Le contexte rendra claire la définition pertinente. □

Les propriétés de Ψ rendent les codes $\mathcal{C} = \Psi(\mathbf{C}_{2^k})$ et $\mathbf{C}_{2^k}$ très proches.

Proposition 4.11 *Soit $\mathcal{C} = \Psi(\mathbf{C}_{2^k})$ un code $\mathbb{Z}_{2^k}$-linéaire. On a les propriétés suivantes :*

1. *le code $\mathcal{C}$ est distance-invariant (tout translaté du code selon un mot de code à la même distribution des poids que $\mathcal{C}$);*
2. *les codes $\mathcal{C}$ et $\mathbf{C}_{2^k}$ ont même distribution des poids ($\mathbb{F}_2$ étant muni du poids de Hamming et $\mathbb{Z}_{2^k}$ du poids homogène, cf. §4.1).*

Remarque 4.12 C'est la distance invariance des codes $\mathbb{Z}_{2^k}$-linéaires qui justifie que l'on s'interesse uniquement au poids minimal. En effet, un corollaire de cette propriété est que le poids minimale est égale à la distance minimale. □

L'application de Gray étant injective, le code $\mathcal{C}$ a le même cardinal que son relevé, en particulier son cardinal est une puissance de 2 (cf. Corollaire 3.5).

Définition 4.13 (Dimension d'un code $\mathbb{Z}_{2^k}$-linéaire) *Soit $\mathcal{C}$ un code $\mathbb{Z}_{2^k}$-linéaire (n, M). On appelle dimension de $\mathcal{C}$ le logarithme en base 2 du cardinal de $\mathcal{C}$, i.e. $\log_2(M)$.*

Il convient de remarquer qu'un code $\mathbb{Z}_{2^k}$-linéaire n'est pas, en général, linéaire sur $\mathbb{Z}_2$ (cf. [HKC+94, Car98]). Cependant, lorsque c'est le cas, les deux définitions se recoupent. Compte tenu de cette remarque sur la non-linéarité, en général, des codes $\mathbb{Z}_{2^k}$-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 $\mathbb{Z}_{2^k}$-dualité, qui utilise la dualité entre codes relevés, et donc au final, la dualité sur l'anneau $\mathbb{Z}_{2^k}$.

Définition 4.14 ($\mathbb{Z}_{2^k}$-dual) *Soit $\mathcal{C} = \Psi(\mathbf{C}_{2^k})$ un code $\mathbb{Z}_{2^k}$-linéaire. On appelle code $\mathbb{Z}_{2^k}$-dual de $\mathcal{C}$, et on note $\mathcal{C}_\perp$, l'image par l'application de Gray du dual de $\mathbf{C}_{2^k}$, i.e.*

$$\mathcal{C}_\perp = \Psi\left(\mathbf{C}_{2^k}^\perp\right) \quad .$$

Toutefois cette notion ce comporte moins bien que la dualité dans le cas linéaire, e.g. elle ne donne pas lieu, en général, à une relation de "type MacWilliams" entre des codes $\mathbb{Z}_{2^k}$-duaux, et cela malgré le Théorème 3.9. La $\mathbb{Z}_{2^k}$-dualité est tout de même intéressante car elle permet d'obtenir la distribution des poids du $\mathbb{Z}_{2^k}$-dual grâce au polynôme des poids *symétrisés* du code *relevé* $\mathbf{C}_{2^k}$ (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 4.15 (Polynôme énumérateur des poids symétrisés) *Soit $\mathbf{C}_{2^k}$ un code de longueur n linéaire sur $\mathbb{Z}_{2^k}$. On appelle polynôme énumérateur des poids symétrisés le polynôme homogène de degré n en trois variables, défini par*

$$SW_{\mathbf{C}_{2^k}}(X,Y,Z) = \sum_{\mathbf{c}\in\mathbf{C}_{2^k}} X^{n_0(\mathbf{c})}Y^{n_i(\mathbf{c})}Z^{n_p(\mathbf{c})} \ ,$$

où $n_0(\mathbf{c}), n_i(\mathbf{c}), n_p(\mathbf{c})$ désignent le nombre de coordonnées de $\mathbf{c}$ respectivement, nulles, impaires, et paires non nulles. Le quadruplet $(n_0(\mathbf{c}), n_i(\mathbf{c}), n_p(\mathbf{c}))$ est appelé poids symétrisé du mot $\mathbf{c}$.

Remarque 4.16 Ce polynôme s'obtient à partir de $CW_{\mathbf{C}_{2^k}}(X_0,\ldots,X_{2^k-1})$, le polynôme énumérateur des poids complets du code $\mathbf{C}_{2^k}$, en remplaçant X_0 par X, X_i par Y pour i impair et par Z pour $i \neq 0$ pair. □

Théorème 4.17 (Distributions des poids de codes $\mathbb{Z}_{2^k}$-duaux, [Car98, §III Prop. 5]) *Soit $\mathcal{C} = \Psi(\mathbf{C}_{2^k})$ un code $\mathbb{Z}_{2^k}$-linéaire de longueur n. On a l'égalité suivante :*

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

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

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

Remarque 4.18 Étonnamment, l'énumérateur des poids symétrisés du code relevé, bien que permettant d'obtenir le polynôme énumérateur des poids de Hamming du $\mathbb{Z}_{2^k}$-dual $\mathcal{C}_\perp$, ne permet pas d'obtenir l'énumérateur des poids de Hamming du code $\mathcal{C}$ lui-même. En effet, les coordonnées égales à 2^{k-1} sont simplement comptées comme étant paires, alors que 2^{k-1} a un poids valant le double d'un autre élément non nul de $\mathbb{Z}_{2^k}$. En conséquence, pour obtenir le poids de Hamming de $\mathcal{C}$ il faut ajouter une variable T au polynôme $SW_{\mathbf{C}_{2^k}}$ avec comme exposant $n_{2^k}(\mathbf{c})$, le nombre de coordonnées du mot $\mathbf{c}$ égales à 2^k. Il faut également modifier la définition de $n_p(\mathbf{c})$ qui ne doit compter que les coordonnées paires, non nulles et différentes de 2^{k-1}. Nous noterons $SW^\#$ le polynôme ainsi obtenu et nous parlerons de poids symétrisé étendu. On a donc les égalités :

$$\begin{aligned} SW_{\mathbf{C}_{2^k}}(X,Y,Z) &= SW^\#_{\mathbf{C}_{2^k}}(X,Y,Z,Z) \ , \\ HW_{\mathcal{C}}(X,Y) &= SW^\#_{\mathbf{C}_{2^k}}\left(X^{2^{k-1}}, (XY)^{2^{k-2}}, (XY)^{2^{k-2}}, Y^{2^{k-1}}\right) \end{aligned}$$

et

$$HW_{\mathcal{C}_\perp} = \frac{1}{|\mathcal{C}|} SW^{\#}_{\mathbf{C}_{2^k}}\Big(X^{2^{k-1}} + Y^{2^{k-1}} + (2^k-2)(XY)^{2^{k-2}},\\ X^{2^{k-1}} - Y^{2^{k-1}},\\ X^{2^{k-1}} - Y^{2^{k-1}},\\ X^{2^{k-1}} + Y^{2^{k-1}} - 2(XY)^{2^{k-2}}\Big) \ .$$

□

Dans le cas particulier $k = 2$, on prouve l'égalité

$$HW_{\mathcal{C}}(X+Y, X-Y) = \frac{1}{|\mathcal{C}|} SW_{\mathbf{C}_4}(X^2+Y^2+2XY, X^2-Y^2, X^2+Y^2-2XY, X^2+Y^2-2XY) \ .$$

Autrement dit, l'égalité du Théorème 4.17 se récrit simplement $HW_{\mathcal{C}_\perp}(X,Y) = 1/|\mathcal{C}| \cdot HW_{\mathcal{C}}(X+Y, X-Y)$.

Théorème 4.19 (Distributions des poids de 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*

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

5 Codes de Kerdock généralisés

5.1 Structure $\mathbb{Z}_{2^k}$-linéaire

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. 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. Ces codes ont été généralisés dans [Car98] donnant des codes $\mathbb{Z}_{2^k}$-linéaires.

Conceptuellement, la construction de ces codes sur $\mathbb{Z}_{2^k}$ est proche de celle des codes de Reed et Muller d'ordre 1 : elle utilise les fonctions affines.

Définition 5.1 (Code de Kerdock généralisé, [Car98, §IV Déf. 5]) *On appelle code de Kerdock généralisé de paramètres (k,m) et on note $\mathcal{K}(k,m)$ le code binaire défini comme l'image par l'application de Gray généralisée de l'ensemble des fonctions*

$$\begin{array}{rccc} \mathbf{c}_{\alpha,\beta} : & \mathcal{T} & \longrightarrow & \mathbb{Z}_{2^k} \\ & \gamma & \longmapsto & \mathrm{Tr}(\alpha\gamma) + b \end{array}$$

où $\mathcal{T} = \{0, 1, x, \ldots, x^{2^m-2}\}$ *est le Teichmuller de l'anneau* $\mathrm{GR}(2^k, m)$, $\alpha \in \mathrm{GR}(2^k, m)$ *et* $b \in \mathbb{Z}_{2^k}$.

De même que pour les fonctions booléennes, (cf. §4.1) toute fonction $\mathbf{c} : \mathcal{T}^m \longrightarrow \mathbb{Z}_{2^k}$ est identifiée à sa table de valeurs qui est un 2^m-uplet de $\mathbb{Z}_{2^k}^{2^m}$: la coordonnée d'indice vaut $\mathbf{c}(x^{i-1})$ pour $i \geq 1$ et la coordonnée d'indice 0 vaut $\mathbf{c}(0)$,

$$\left(\mathbf{c}(0), \mathbf{c}(1), \mathbf{c}(x), \ldots, \mathbf{c}\left(x^{2^m-2}\right)\right) \quad .$$

Le relevé de $\mathcal{K}(k, m)$ est donc de longueur 2^m sur $\mathbb{Z}_{2^k}$ et par conséquent $\mathcal{K}(k, m)$ est de longueur 2^{m+k-1} sur $\mathbb{Z}_2$.

Par le Théorème 2.19 toute fonction affine de $\mathrm{GR}(2^k, m)$ sur $\mathbb{Z}_{2^k}$ s'exprime à partir de la trace plus une composante affine, ceci implique que le relevé de $\mathcal{K}(k, m)$ se compose de *toutes* les fonctions affines (restreintes à $\mathcal{T}$). Or, l'ensemble des fonctions affines $\mathcal{F}$ de $\mathrm{GR}(2^k, m)$ sur $\mathbb{Z}_{2^k}$ 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 $\mathrm{GR}(2^k, m)$ considéré comme un module sur $\mathbb{Z}_{2^k}$, i.e. les fonctions

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

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

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

Remarque 5.2 Calculer cette matrice revient à calculer la table des représentations additives des éléments du Teichmuller (cf. §2.2) : 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 $\mathcal{K}(k, m)$ est donc $(2^k)^{m+1} = 2^{k(m+1)}$, comme un code $\mathbb{Z}_{2^k}$-linéaire et son relevé ont même cardinal, c'est également celui de $\mathcal{K}(k, m)$.

Proposition 5.3 *Le code de Kerdock généralisé* $\mathcal{K}(k, m)$ *est de longueur* 2^{k+m-1} *et a* $2^{k(m+1)}$ *mots.*

Exemple 5.4 Le relevé du code de Kerdock généralisé $\mathcal{K}(3, 3)$ 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 2.13 (lorsque $\mathrm{GR}(2^3,3)$ est représenté par $\mathbb{Z}_{2^3}[X]/(7+5X+6X^2+X^3)$). □

Lorsque $k=2$ et pour $m \geq 3$ impair, les codes de Kerdock généralisés sont les codes introduits par A.M. Kerdock en 1972 (cf. [Ker72]). Ces codes sont actuellement les meilleurs connus pour de tels paramètres : la distance minimale de $\mathcal{K}(2,m)$ est $2^m - 2^{\frac{m-1}{2}}$. En fait, on connaît la distribution des poids (de Hamming) de ces codes (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 F.P. Preparata ([Pre68]) : les codes de Preparata sont des duaux formels des codes de Kerdock. Bien que les codes de Preparata ne soient pas exactement les $\mathbb{Z}_4$-duaux des codes de Kerdock, on a par le Théorème 4.19 que ces derniers ont la même distribution des poids que les codes de Preparata.

Définition 5.5 (Code de Preparata généralisé) *On appelle code de Preparata généralisé, et on note $\mathcal{P}(k,m)$, le $\mathbb{Z}_{2^k}$-dual du code de Kerdock généralisé $\mathcal{K}(k,m)$.*

Proposition 5.6 *Le code $\mathcal{P}(k,m)$ est de longueur 2^{k+m-1} et a $2^{k(2^m-m-1)}$ mots.*

Pour $k \geq 3$, on ne connaît pas la distance minimale des codes de Kerdock généralisés, cependant C. Carlet donne une borne sur cette distance minimale dans [Car98].

Théorème 5.7 ([Car98, §IV Cor. 1]) *La distance minimale du code de Kerdock généralisé $\mathcal{K}(k,m)$ est supérieure ou égale à*

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

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 §5.3 que ce n'est plus le cas pour $k \geq 3$.

5.2 Structure $\mathbb{Z}_{2^k}$-cyclique

Nous avons vu dans la section précédente une définition des codes de Kerdock généralisés à partir de codes linéaires sur $\mathbb{Z}_{2^k}$. 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 $\mathbb{Z}_{2^k}$; de façon générale son dual est cyclique étendu. Cette construction

est donnée dans le cas des codes de Kerdock – c.a.d. de $\mathbb{Z}_4$ – dans l'article de Hammons et al. [HKC+94], nous l'avons généralisée à $\mathbb{Z}_{2^k}$.

Soit $h^{(k)} \in \mathbb{Z}_{2^k}[X]$ un B-polynôme de degré m et posons $n = 2^m - 1$. Autrement dit, $h^{(k)}$ est un B-polynôme de degré m. Soit $\mathbf{SK}_{2^k}^-$ le code de longueur n cyclique sur $\mathbb{Z}_{2^k}$ et dont le polynôme de contrôle est le polynôme réciproque de $h^{(k)}(X)$, i.e. $\widetilde{h^{(k)}}(X)$. Posons $X^n - 1 = g^{(k)}(X)h^{(k)}(X)$, le polynôme $\widetilde{g^{(k)}}$ est donc le générateur de $\mathbf{SK}_{2^k}^-$. Ce code contient tous les mots de la forme

$$\left(\mathrm{Tr}(\alpha), \mathrm{Tr}(\alpha x), \ldots, \mathrm{Tr}\left(\alpha\left(x^{2^m-2}\right)\right)\right) \ , \qquad (*)$$

quelque soit $\alpha \in \mathrm{GR}(2^k, m)$. En effet, posons $\widetilde{h^{(k)}}(X) = \sum_{j=0}^{n-1} h_j X^j$, on a alors dans $\mathcal{R} = \mathbb{Z}_{2^k}[X]/(X^n - 1)$ (avec la convention $h_j = 0$ pour $j \geq n$)

$$\left(\sum_{j=0}^{n-1} h_j X^j\right) \cdot \left(\sum_{i=0}^{n-1} \mathrm{Tr}\left(\alpha x^i\right) \cdot X^i\right) = \sum_{j=0}^{n-1} h_j \left(\sum_{l=0}^{n-1} \mathrm{Tr}\left(\alpha x^{l-j \mod n}\right) \cdot X^l\right) \ ,$$

(car $X^n \equiv 1$ dans $\mathcal{R}$)

$$= \sum_{l=0}^{n-1} \mathrm{Tr}\left(\alpha \sum_{j=0}^{n-1} h_j x^{l-j \mod n}\right) \cdot X^l \ .$$

Mais

$$\sum_{j=0}^{n-1} x^{l-j \mod n} h_j = \sum_{j=0}^{n-1} x^{l-j} h_j \ ,$$

(car $x^n = 1$)

$$= x^l \sum_{j=0}^{n-1} h_j \left(x^{-1}\right)^j \ ,$$
$$= x^l \widetilde{h^{(k)}}(x^{-1}) \ .$$

Mais x est racine de $h^{(k)}$ dans $\mathrm{GR}(2^k, m)$, donc x^{-1} est racine de $\widetilde{h^{(k)}}$ (direct à partir de la définition du polynôme réciproque). Or il y a 2^{km} mots du type (*) (cf. §5.1) et c'est exactement le nombre de mots du code $\mathbf{SK}_{2^k}^-$ (Corollaire 3.17), d'où

$$\mathbf{SK}_{2^k}^- = \left\{ \left(\mathrm{Tr}(\alpha), \mathrm{Tr}(\alpha x), \ldots, \mathrm{Tr}\left(\alpha\left(x^{2^m-2}\right)\right)\right) \ \middle| \ \alpha \in \mathrm{GR}(2^k, m) \right\} \ .$$

Considérons maintenant le code cyclique $\mathbf{K}_{2^k}^-$ de longueur n dont le polynôme de contrôle est $\widetilde{(X-1)h^{(k)}}(X)$. On a l'inclusion

$$\mathbf{SK}_{2^k}^- \subset \mathbf{K}_{2^k}^- \ ,$$

car le polynôme de contrôle de $\mathbf{K}_{2^k}^-$ est un multiple de celui de $\mathbf{SK}_{2^k}^-$, i.e. le polynôme générateur de $\mathbf{SK}_{2^k}^-$ est un multiple de celui de $\mathbf{K}_{2^k}^-$. D'autre part, $(1,\dots,1)$ est dans $\mathbf{K}_{2^k}^-$: le polynôme correspondant est $1+X+\cdots+X^{n-1}$, or

$$\begin{aligned}(1+X+\cdots+X^{n-1})\widetilde{(X-1)} &= (1+X+\cdots+X^{n-1})(1-X) \ , \\ &= (1+X+\cdots+X^{n-1}) - (X+X^2+\cdots+X^n) \ , \\ &= -(X^n-1) \ , \\ &= 0 \in \mathcal{R} \ .\end{aligned}$$

Le code $\mathbf{K}_{2^k}^-$ étant linéaire, on vient de prouver qu'il contient tous les mots correspondant aux formes affines, $\mathbf{c}(\mu) = \mathrm{Tr}(\alpha\mu)+b$, $\alpha \in \mathrm{GR}(2^k,m)$ et $b \in \mathbb{Z}_{2^k}$, restreintes au Teichmuller privé de 0. Comme $|\mathbf{K}_{2^k}^-| = 2^{k(m+1)}$ d'après le Corollaire 3.17, on a

$$\mathbf{K}_{2^k}^- = \left\{ \left(\mathbf{c}(1), \mathbf{c}(x), \dots, \mathbf{c}\left(x^{2^m-2}\right)\right) \ \middle| \ \mathbf{c}(\mu) = \mathrm{Tr}(\alpha\mu)+b, \quad \alpha \in \mathrm{GR}(2^k,m), b \in \mathbb{Z}_{2^k} \right\} \ .$$

Il en résulte que si G désigne une matrice génératrice de $\mathbf{SK}_{2^k}^-$, la matrice

$$\begin{pmatrix} 1 & \cdots & 1 \\ & G & \end{pmatrix}$$

est génératrice de $\mathbf{K}_{2^k}^-$. Remarquons que pour un mot $\mathbf{c} \in \mathbf{K}_{2^k}^-$, la somme des coordonnées, dans $\mathbb{Z}_{2^k}$, est égale à $n \cdot b$:

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

car

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

($x-1$ est inversible car autrement on aurait $x = 1 + p\alpha$, $\alpha \in \mathrm{GR}(2^k, m)$ non nul, ce qui contredirait l'unicité de la forme multiplicative, cf. Proposition 2.12).
Ainsi, si on note $\mathbf{K}_{2^k}$ le code étendu de $\mathbf{K}_{2^k}^-$ défini par

$$\mathbf{K}_{2^k} = \left\{ (v_0, v_1, \ldots, v_n) \in \mathbb{Z}_{2^k}^{n+1} \;\middle|\; (v_1, \ldots, v_n) \in \mathbf{K}_{2^k}^- \text{ et } v_0 + v_1 + \cdots + v_n = 0 \right\} \ ,$$

on a $v_0 = -(v_1 + \cdots + v_n) = \sum \mathbf{c}(x^i) = -n \cdot b$. Lorsque $k \leq m$, alors $n = 2^m - 1 \equiv -1 \pmod{2^k}$, d'où $v_0 = b = \mathbf{c}(0)$. En d'autre termes, si $k \leq m$, le code $\mathcal{K}_{2^k}$ est l'ensemble des formes affines de $\mathrm{GR}(2^k, m)$ restreintes au Teichmuller, c'est donc le relevé du code de Kerdock généralisé $\mathcal{K}(k, m)$.

Théorème 5.8 *Lorsque $k \leq m$, le relevé du code de Kerdock généralisé $\mathcal{K}(k, m)$ est l'étendu du code cyclique $\mathbf{K}_{2^k}^-$ dont le polynôme de contrôle est le polynôme réciproque de $(X-1)h^{(k)}(X)$.*

Lorsque $k > m$, on n'a plus l'égalité $v_0 = \mathbf{c}(0)$ et en conséquence $\mathbf{K}_{2^k}$ n'est plus le relevé de $\mathcal{K}(k, m)$. Cependant, $-n$ est inversible dans $\mathbb{Z}_{2^k}$ et donc le relevé de $\mathcal{K}(k, m)$ est équivalent à $\mathbf{K}_{2^k}$, autrement dit, le relevé de $\mathcal{K}(k, m)$ est équivalent à un code cyclique étendu. Ceci étant, on peut tout de même obtenir une information sur la structure du relevé de $\mathcal{K}(k, m)$, on peut le définir comme le dual d'un code cyclique étendu.

Lemme 5.9 *Soient $\mathbf{C}_{2^k}$ un code linéaire $\mathbb{Z}_{2^k}$, $\mathbf{C}_{2^k}^+$ son étendu, et $G^\perp$ une matrice génératrice du dual de $\mathbf{C}_{2^k}$. Alors la matrice*

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

est génératrice du code dual de $\mathbf{C}_{2^k}^+$.

Preuve. Nous commençons par prouver que les mots de la forme $(0, v_0, \ldots, v_{n-1})$, pour $(v_0, \ldots, v_{n-1}) \in \mathbf{C}_{2^k}^\perp$, sont dans $(\mathbf{C}_{2^k}^+)^\perp$. Soit $\mathbf{u}^+ = (u_\infty, u_0, \ldots, u_{n-1}) \in \mathbf{C}_{2^k}^+$, alors

$$\begin{aligned} \mathbf{u}^+ \cdot (0, v_0, \ldots, v_{n-1}) &= 0 \cdot u_\infty + \sum_{i=0}^{n-1} u_i \cdot v_i \ , \\ &= 0 \ . \end{aligned}$$

D'autre part,

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

Donc, si $\mathbf{v}_1, \ldots, \mathbf{v}_d$ sont les vecteurs lignes de $G^\perp$, la famille $\{\mathbf{v}'_1, \ldots, \mathbf{v}'_d, \mathbf{1}\}$ où $\mathbf{1} = (1, \ldots, 1)$, est dans $(\mathbf{C}^+_{2^k})^\perp$. Il est clair que cette famille est linéairement indépendante sur $\mathbb{Z}_{2^k}$. Le code engendré par cette famille a donc $2^k \cdot |\mathbf{C}^\perp_{2^k}|$ éléments. Or, l'opération consistant à étendre un code laisse invariant le cardinal : $|\mathbf{C}_{2^k}| = |\mathbf{C}^+_{2^k}|$. D'après les résultats de §3.1 (Corollaire 3.5 et Proposition 3.7), on a $|\mathbf{C}_{2^k}| \cdot |\mathbf{C}^\perp_{2^k}| = 2^{kn}$ et $|\mathbf{C}^+_{2^k}| \cdot |(\mathbf{C}^+_{2^k})^\perp| = 2^{k(n+1)}$. Donc

$$\begin{aligned}\left|(\mathbf{C}^+_{2^k})^\perp\right| &= \frac{2^{k(n+1)}}{\left|\mathbf{C}^+_{2^k}\right|} = \frac{2^{k(n+1)}}{|\mathbf{C}_{2^k}|} \ , \\ &= \frac{2^{k(n+1)}}{2^{kn}} \cdot |\mathbf{C}^\perp_{2^k}| \ , \\ &= 2^k \cdot \left|\mathbf{C}^\perp_{2^k}\right| \ .\end{aligned}$$

Il en découle que la famille $\{\mathbf{v}'_1, \ldots, \mathbf{v}'_d, \mathbf{1}\}$ engendre le code $(\mathbf{C}^+_{2^k})^\perp$ ce qui achève la démonstration. □

Théorème 5.10 *Le code relevé du code de Kerdock généralisé $\mathcal{K}(k,m)$ est le code dual de l'étendu du code* $(\mathbf{SK}^-_{2^k})^\perp = \left(\widetilde{h^{(k)}(X)}\right)$.

PREUVE. Appliquons le lemme précédent en prenant $\mathbf{C}_{2^k}$ égal au code dual de $\mathbf{SK}^-_{2^k}$, i.e. $\mathbf{C}_{2^k} = (\mathbf{SK}^-_{2^k})^\perp$. On a donc $\mathbf{C}^\perp_{2^k} = \mathbf{SK}^-_{2^k}$. Ainsi, en notant G une matrice génératrice de $\mathbf{SK}^-_{2^k}$, la matrice

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

est une matrice génératrice de $(\mathbf{C}^+_{2^k})^\perp$. Pour la matrice G, on peut peut prendre

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

où les x^*_i sont les formes coordonnées. En effet, les x^*_i forment une base des formes linéaires et d'après ce qui précède $\mathbf{SK}^-_{2^k}$ est l'ensemble des formes linéaires restreintes à $\mathcal{T}^*$, l'ensemble de Teichmuller privé de 0. La matrice G' est alors exactement la matrice génératrice donnée dans la section 5.1. □

On peut remarquer que le théorème ci-dessus ne requière 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. Ceci 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 5.8 et 5.10 permettent bien entendu de relier les codes de Preparata généralisés aux codes cycliques sur $\mathbb{Z}_{2^k}$:

Théorème 5.11 *Le relevé du code de Preparata généralisé $\mathcal{P}(k,m)$ est l'étendu du code cyclique $(\mathbf{SK}_{2^k}^-)^\perp = \left(\widetilde{h^{(k)}(X)}\right)$. Lorsque $k \leq m$, ce code peut également être décrit comme le dual de l'étendu du code $\mathbf{K}_{2^k}^-$.*

Remarque 5.12 Dans [HKC+94], Hammons et al. utilisent le Th. 5.8 comme définition pour le relevé du code de Kerdock classique $\mathcal{K}(2,m)$ et prouvent l'équivalence avec la définition sous forme de restriction au Teichmuller des formes affines de l'anneau $\mathrm{GR}(2^2,m)$ que nous avons adopté (Déf. 5.1) et c'est cette définition à partir des formes affines qu'ils utilisent pour redémontrer la distribution des poids de $\mathcal{K}(2,m)$. C'est également de cette définition dont se sert Carlet dans [Car98] pour obtenir la borne sur la distance minimale des codes de Kerdock généralisés du Th. 5.7. □

Exemple 5.13 Nous avons donné dans l'exemple 5.4 la matrice génératrice du code $\mathcal{K}(3,3)$ obtenue par les formes affines lorsque $\mathrm{GR}(2^3,3)$ est représenté par $\mathbb{Z}_{2^3}[X]/(7+5X+6X^2+X^3)$:

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

D'après ce que nous avons vu dans cette section, si on pose $h^{(3)}(X) = 7+5X+6X^2+X^3$, alors le polynôme

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

est le réciproque du générateur du code. Donc

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

est le générateur et

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

la matrice génératrice correspondante et 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 équivalentes. □

5.3 Distance minimale en petite longueur

La table 1 donne les résultats obtenus par l'implémentation en langage C d'une recherche exhaustive pour les valeurs des paramètres k et m donnant un code de cardinal raisonnable. En l'occurrence, nous avons considéré comme "raisonnable" des codes nécessitant moins de 7 jours de calculs pour obtenir le résultat [1]. De par la complexité exponentielle des calculs effectués, nous n'avons pu obtenir que quelques valeurs : par exemple pour $k = 3$, lorsque m augmente de 1, la taille du code est multipliée par 2^3 et la longueur du code est doublée, on peut donc s'attendre à un temps de calcul multiplié par 16 et pour l'implémentation réalisée c'est effectivement ce que l'on a constaté.

Ce qui ressort en premier lieu de ces résultats, c'est la régularité de la distance minimale : pour m fixé, après le "saut" irrégulier entre $k = 2$ et $k = 3$, il suffit de doubler la distance minimale du code $\mathcal{K}(k, m)$ pour obtenir celle du code $\mathcal{K}(k + 1, m)$. On peut remarquer que cela est vrai non seulement pour le Kerdock généralisé mais également pour son dual $\mathcal{P}$. On constate également que, pour $m = 3$, les codes de Kerdock généralisés et leurs $\mathbb{Z}_{2^k}$-duaux ont les même paramètres.

Pour juger de la qualité de ces codes, nous donnons différentes tables :

1. la table 2 donne les bornes connues sur les *codes binaires linéaires* de *longueur* et de *cardinal* égaux à ceux des codes $\mathcal{K}$ et $\mathcal{P}$. Cette table indique la distance minimale la plus grande possible, i.e. la borne sup, pour un code linéaire, ainsi que la distance minimale du meilleur code binaire linéaire connu lorsqu'elle est différente de la borne sup (extrait de la table de Brouwer, cf. [Bro98]).

2. la table 3 donne les paramètres du plus gros *code binaire* connu de *longueur* et de *distance minimale* égales à ceux des codes $\mathcal{K}$ et $\mathcal{P}$ (cette valeur est extraite de la table de Litsyn, cf. [Lit98]).

3. la table 4 donne des codes ayant même longueur (à une unité près lorsque m est pair) que les codes $\mathcal{K}(3, m)$ et un cardinal proche (voir [Aug93] pour les paramètres des codes utilisés).

Les tables 2 et 3 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. §5.1). On trouve même des codes linéaires plus performants dans plusieurs cas

1. Pour être tout à fait précis, il convient d'ajouter que les calculs ont été effectués sur deux processeurs DEC alpha 21264 (EV6) cadencés à 500Mhz.

(e.g. $k = 3$ avec $m = 4, 5$ ou 6). D'autre part, la table 4 montre que pour $k = 3$, on connaît des codes ayant (essentiellement) même longueur avec plus de mots et une distance minimale supérieure.

La table 5 indique la valeur de la borne de C. Carlet sur la distance minimale (Théorème 5.7) pour les cas pertinents[1]. Elle semble, asymptotiquement assez bonne : le pourcentage d'erreurs $(\delta - b)/\delta$, avec δ distance minimale et b borne sur la distance minimale, décroît de façon monotone pour arriver à moins de 2% pour $\mathcal{K}(3, 10)$.

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. §5.1).

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

$m\backslash k$	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	$\{2048,22,992\}$	$\{4096,33,1888\}$		

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

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

$m\backslash k$	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	$\{2048,2026,4\}$			

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

TAB. 1: *Distance minimale du code de Kerdock généralisé ainsi que de son dual en petite longueur. La notation $\{l,d,\delta\}$ signifie que le code est de longueur l, de cardinal 2^d et de distance minimale δ.*

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

m\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 même longueur et dimension que le code $\mathcal{P}(k,m)$

m\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. 2: *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 $b_{min}=b_{max}=b$, on a simplement indiqué b.*

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

m\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 même longueur et distance minimale que le code $\mathcal{P}(m,k)$

m\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. 3: *Extrait de la table de Litsyn : Morceaux choisis de la table des meilleurs codes binaires connus. La notation $\{l,d,\delta\}$ désigne un code de longueur l, de cardinal 2^d et de distance minimale δ.*

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

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

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

m	$\left(2^{m+2}, 3m+7, 2^{m+1}-2\cdot 2^{\frac{m+2}{2}}\right)$	$\mathcal{K}(3,m)$
4	$(63,19,16)$	$\{64,15,20\}$
6	$(255,25,96)$	$\{256,21,96\}$
8	$(1023,31,448)$	$\{1024,27,440\}$
10	$(4095,37,1920)$	$\{4096,33,1888\}$

TAB. 4: *Paramètres des duaux des codes BCH 3 correcteur de longueur $2^{m+2}-1$ pour m impair et des duaux des codes BCH 3 correcteur étendus de longueur 2^{m+2} pour m pair. La notation (l,d,δ) désigne un code de longueur l, de cardinal 2^d et de distance minimale δ.*

m	3	4	5	6	7	8	9	10
δ	10	20	44	96	212	440	928	1888
borne (Th. 5.7)	0	8	32	80	190	416	892	1856
erreur (%)	–	60	27.3	16.7	10.4	5.5	3.9	1.7

TAB. 5: *Borne sur la distance minimale (cf. Théorème 5.7) et vraie distance minimale δ pour le code $\mathcal{K}(3, m)$.*

6 Exemples de codes $\mathbb{Z}_{2^k}$-linéaires dont les paramètres dépassent ceux des meilleurs codes précédemment connus

6.1 Code de Duursma et al. [DGLS01]

Dans [DGLS01] (mai 2001), I.M. Duursma, M. Greferath, S.N. Litsyn et S.E. Schmidt utilisent un code $\mathbb{Z}_8$-linéaire pour construire un code binaire de paramètres $(96, 2^{37}, 24)$. Jusque là, le meilleur code binaire connu de longueur 96 et de distance minimale 24 n'avait que 2^{33} éléments. Leur code en a donc 16 fois plus. 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 de longueur 96 et cardinal 2^{36}. De plus, le code $(96, 2^{37}, 24)$ obtenu à partir de ce code $\mathbb{Z}_8$-linéaire 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, Chp. 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. 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. §5.2). 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 connus avant [DGLS01], mais on peut obtenir un code $(96, 2^{37}, 24)$, 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 $\mathrm{d_H}(\mathbf{a}, \mathbf{b}) = \mathrm{w_H}(\mathbf{a} - \mathbf{b}) \geq 24$ 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. §4.1), donc $a_i + b_i$ représente également une fonction affine de 2 variables, par conséquent $\mathrm{w_H}(a_i + b_i)$ est pair. Il en résulte que $\mathrm{w_H}(a_i + b_i + 1000)$ est non nul, et donc strictement positif. Finalement,

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

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*, i.e. tout mot $\mathbf{v}$ de ${\mathbb{F}_2}^{23}$ peut être associé de manière unique à un mot de code $\mathbf{c}$ tel que $\mathrm{d_H}(\mathbf{c}, \mathbf{v}) \leq e$ où e désigne la capacité de correction du code, dans le cas présent, $e = (7-1)/2 = 3$. Autrement dit, les boules fermés 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 $\mathbf{C}_8$.

6.2 Code de Greferath et Schmidt [GS99]

Le code de Greferath et Schmidt, présenté dans [GS99] (novembre 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, i.e. c'est un code cyclique sur $\mathbb{F}_3$.

Nous n'avons pas présenté les codes $\mathbb{Z}_{3^k}$-linéaires dans ce document, mais leur définition est analogue à celle des codes $\mathbb{Z}_{2^k}$-linéaires : ces codes sont définis sur l'alphabet $\mathbb{F}_3$, comme étant des images, par une application Ψ' conservant les distances, de codes linéaires sur l'anneau $\mathbb{Z}_{3^k}$. Le corps $\mathbb{F}_3$ est muni de la distance de Hamming et l'anneau $\mathbb{Z}_{3^k}$, de la distance homogène que l'on définit par le poids

$$\mathrm{w_{hom}}(a) = \begin{cases} 0 & \text{si } a = 0, \\ (3-1)\cdot 3^{k-2} & \text{si } a \not\equiv 0 \pmod{3^{k-1}}, \\ 3^{k-1} & \text{si } a \equiv 0 \pmod{3^{k-1}}. \end{cases}$$

L'application Ψ' va de $\mathbb{Z}_{3^k}$ dans $\mathbb{F}_3^{3^{k-1}}$ et conserve les distances, i.e.

$$\mathrm{d_{hom}}(a, b) = \mathrm{d_H}\left(\Psi'(a), \Psi'(b)\right) \ ,$$

pour tout couple (a, b) d'éléments de $\mathbb{Z}_{3^k}$. Dans le cas qui va nous intéresser, c'est à dire pour $k = 3$, cette application peut être définie par

$$\begin{array}{rccll} \Psi' : & \mathbb{Z}_9 & \longrightarrow & \mathbb{F}_3^3 & \\ & x + 3y & \longmapsto & x(0,1,2) + y(1,1,1) & \text{avec } x, y \in \{0,1,2\} \end{array}$$

(cf. Rem. 4.7 et voir [GS99, §II] pour la définition générale de l'application Ψ'). Munis de cette application, 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

$$\mathbf{C}_9^+ = \left\{ (c_\infty, c_0, \ldots, c_{12}) \;\middle|\; (c_0, \ldots, c_{12}) \in \mathbf{C}_9 \text{ et } c_\infty + c_0 + \cdots + c_{12} = 0 \right\} \ .$$

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 $\mathbb{F}_3^{11}$).

6.3 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, appelé 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 Q est l'ensemble des résidus quadratiques modulo n, i.e. $Q = \{r^2 \pmod{n},\ r \neq 0\}$ et où α désigne une racine primitive de l'unité d'ordre n sur $\mathbb{F}_p$. 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, Chp. 16 §6]).

Dans le cas binaire, la condition sur la longueur équivaut à avoir pour n un nombre premier de la forme $8m \pm 1$. On se place dans la suite de cette section dans le cas binaire, i.e. $p = 2$ et par conséquent, QR_n désigne désormais le code de résidus quadratiques *binaire* de longueur n.

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 potentielle intéressante pour construire de

bons codes. Les codes $\mathrm{QR}_n^{(2)}$ ont été étudiés dans [BSC95] ($n = 17, 23$), [PQ96] ($n = 31, 47$) et [CMKH96] ($n = 31$). Le code $\mathrm{QR}_{23}^{(3)}$ est celui qui a été utilisé par Duursma et al. dans [DGLS01] (cf. §6.1) et à notre connaissance, c'est actuellement le seul bon code $\mathbb{Z}_8$-linéaire connu. La table 6 donne la distance minimale de l'image par l'application de Gray 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

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	$\{64, 32, \mathbf{14}\}$	$\{128, 48, \mathit{28}\}$	$\{256, 64, 56^*\}$
47	$\{96, 48, \mathbf{18}\}$	$\{192, 72, \mathit{36}\}$	

*: borne supérieure uniquement

TAB. 6: *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.

$n\backslash k$	2	3	4
17	*8*	19	38
23	*12*	**20**	*48*
31	**12**	*28*	62
47	**16**	*36*	

TAB. 7: *Distance minimale des meilleurs codes binaires linéaires connus de même longueur et même cardinal que* $\Psi\left(\mathrm{QR}_n^{(k)+}\right)$.

$\mathbb{Z}_{2^k}$-linéaires sont de longueur $2^{k-1} \cdot (n+1)$ et de dimension $k(n+1)/2$. La table 7 donne la distance minimale des meilleurs codes linéaires binaires connus de même longueur et dimension. Ajoutons que les codes QR_n pour $n = 17, 23, 31, 47$ sont des codes binaires linéaires optimaux (voir [Bro98]).

7 Construction de codes binaires à base de translatés de codes $\mathbb{Z}_{2^k}$-linéaires

Les tables 1, 2 et 3 montrent que les codes $\mathcal{P}(k, m)$ sont notablement moins bons, lorsque $k \geq 3$, que les codes linéaires. Cependant, ces codes et de manière plus générale les codes $\mathbb{Z}_{2^k}$-linéaires peuvent être améliorés très fortement : en effet, il est facile de trouver des translatés de ces codes qui sont suffisamment loin du code d'origine; en considérant la réunion du code et de ces translatés ont obtient donc un code de même 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 et al. dans [DGLS01].

7.1 Principe de la construction

Considérons un code binaire $\mathcal{C}$ de distance minimale δ ayant la propriété d'être un sous ensemble de $\mathrm{RM}(r,m)^n$, où $\mathrm{RM}(r,m)$ désigne le code de Reed et Muller d'ordre r en m variables. Les codes $\mathbb{Z}_{2^k}$-linéaires entrent dans cette catégorie puisque l'image par l'application de Gray généralisée de l'anneau $\mathbb{Z}_{2^k}$ est $\mathrm{RM}(1,k-1)$. 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 la même distance minimale.

Nous cherchons donc à construire un ensemble $\mathcal{T} \subset \mathbb{F}^{n\cdot 2^m}$ de cardinal aussi grand que possible tel que

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

soit de distance minimale δ. Ceci équivaut à chercher un ensemble $\mathcal{T}$ tel que $\mathrm{w_H}(t+t'+c+c') \geq \delta$ 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 $\mathrm{RM}(r,m)^n$, et pas seulement dans $\mathcal{C}$. Cela a pour conséquence de nous permettre de réécrire la condition $\mathrm{w_H}(t+t'+c+c') \geq \delta$ en $\mathrm{w_H}(t+t'+c'') \geq \delta$ puisque $c+c'$ est dans $RM(r,m)^n$. Nous allons construire $\mathcal{T}$ comme un code concaténé : un code interne $S \subset \mathbb{F}^{2^m}$ et un code externe T de longueur n définie 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 $\varphi : S \to \mathbb{F}_{|S|}$ 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 $t+\mathrm{RM}(r,m)^n$ nous allons imposer une autre condition sur S :

Lemme 7.1 *Soient un code $S \subset {\mathbb{F}_2}^{2^m}$ de cardinal 2^l tel que*

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

et une code T sur $\mathbb{F}_{2^l}$ de distance minimale d_T. On pose $\mathcal{T}=T(S)$. Alors la distance entre deux translatés $t+RM(r,m)^n$ et $t'+RM(r,m)^n$ pour $t,t'\in\mathcal{T}$, $t\neq t'$, est supérieure où égale à $d_S\cdot d_T$.

PREUVE. L'hypothèse sur S signifie que les translatés de $\mathrm{RM}(r,m)$ selon les mots de S sont au moins distant 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 $\mathrm{RM}(r,m) \subset \mathbb{F}_2{}^{2^m}$ et $\mathbf{t} = \varphi(x), \mathbf{t}' = \varphi(x')$ pour $x, x' \in T$, $x \neq x'$. Nous avons,

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

On peut écrire

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

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

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

□

Théorème 7.2 *Soit $\mathcal{C} \subset RM(r,m)^n$ de distance minimale d. Avec les notations et hypothèses du lemme 7.1, le code*

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

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 a la distance minimale du code $\mathcal{C}$. □

Le code de Reed et Muller d'ordre $r+a$ en m variables $\mathrm{RM}(r+a,m)$ peut être défini ([MS96, Chp. 13 §3]) comme la réunion de 2^l translatés du code $\mathrm{RM}(r,m)$ avec $l = \binom{m}{r+a} + \binom{m}{r+a-1} + \cdots + \binom{m}{r+1}$. Prenons pour S un système de représentants des 2^l translatés de $\mathrm{RM}(r,m)$ dans $\mathrm{RM}(r+a,m)$ — c.a.d. S contient exactement un mot de chacun des translatés. Cet ensemble S a la propriété $(*)$ requise par le lemme 7.1 pour $d_S = 2^{m-r-a}$: ces éléments sont dans $\mathrm{RM}(r+a,m)$ qui est un code de distance minimale 2^{m-r-a}.

Notons T un code sur $\mathbb{F}_{2^l}$, de longueur n et de distance (de Hamming) minimale $d_T \geq \delta/2^{m-r}$. Le théorème 7.2 nous permet alors de construire un code $\mathcal{G}$ ayant $|T|$ fois plus de mots que $\mathcal{C}$, à la condition qu'il existe bien un code T de distance minimale au moins d_T – ce qui n'est plus le cas pour $n < 2^{r-m}\delta$. D'autre part, il convient de remarquer que le code $\mathcal{G}$ obtenu est dans $\mathrm{RM}(r+a,m)^n$ et que nous pouvons donc appliquer la même construction a ce code en utilisant d'autres codes S et T. On obtient ainsi une construction itérative.

Exemple 7.3 Pour $\mathbb{Z}_8$, on a $r=1$, $m=2$ et $S = \{0000, 1000\}$. Si le code $\mathcal{C}$ est $\{96, 36, 24\}$, il n'y a qu'un seul code T de longueur 24 et de distance 24 sur $\mathbb{F}_2$, le code trivial à deux éléments, le code $\mathcal{G}$ obtenu à alors deux fois plus de mots que $\mathcal{C}$. C'est sous cette forme qu'à été utilisée cette construction dans [DGLS01]. □

Remarque 7.4 Nous avons utilisé comme code S un ensemble de représentant des translatés de $\mathrm{RM}(r,m)$ dans $\mathrm{RM}(r+a,m)$, toutefois, ce n'est pas la seule possibilité. Par exemple, lorsque m est pair et $r=a=1$, il est possible de considérer un ensemble de représentant 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}.

7.2 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, le choix de r est restreint à $r=2$, auquel cas $|S|=2$ et le code T est binaire, de même longueur et distance minimale que le code $\mathbb{Z}_8$-linéaire. La table 8 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 $\mathcal{P}(3,m)$ et pour T le meilleur code binaire connu de longueur 2^m et de même distance minimale que $\mathcal{P}(3,m)$ (cf. §5.3 Tab. 1 et [Lit98]). L'amélioration est

$\mathcal{C}$	$\{64,33,8\}$	$\{128,78,10\}$	$\{256,171,8\}$	$\{512,360,10\}$	$\{1024,741,8\})$
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. 8: *Exemples de codes obtenus par la construction du Théorème 7.2 avec des codes $\mathbb{Z}_8$-linéaires. La notation $\{l,d,\delta\}$ désigne un code de longueur l, de cardinal 2^d et de distance minimale δ.*

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. §6.1 et [DGLS01]) est une version simplifiée de notre construction (cf. exemple 7.3).

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 r :

- soit $r=2$, 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 $\mathrm{RM}(3,3)^n = \mathbb{F}^{8n}$, conduisant à un code $\mathcal{G}'$ encore plus grand. Cette fois si le code T' utilisé pour construire les translatés est

binaires ($\mathrm{RM}(3,3)$ est formés de deux translatés de $\mathrm{RM}(2,3)$) et doit avoir une distance minimale au moins égale à δ.

- soit $r = 3$, donc chercher directement des translatés du code dans l'espace tout entier, $\mathbb{F}^{8n}$. 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 être de distance minimale au moins δ.

Pour illustrer le caractère itératif de notre construction, nous avons choisi $r = 2$. La table 9 donne les paramètres des codes obtenus en partant des codes $\mathcal{P}(4,m)$. 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. 9: *Exemples de codes obtenus par itération de la construction du Théorème 7.2 avec des codes $\mathbb{Z}_{16}$-linéaires.*

Utilisation de codes de Reed-Solomon. Donner un équivalent de la table 9 pour le cas $r = 3$, est délicat car il n'existe pas de table des meilleurs codes connus pour des corps ayant plus de 9 éléments. Or dans ce cas le code T est défini sur $\mathbb{F}_{2^4}$. Cependant, il existe une famille de cas où T peut être un code de Reed-Solomon.

Considérons un code $\mathcal{C} \in \mathrm{RM}(r,m)^n$ de distance 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 $\mathrm{RM}(r+a,m)$ à 2^l éléments avec $l = \sum_{i=1}^{a} \binom{m}{r+i}$. Le code T est alors défini sur $\mathbb{F}_{2^l}$ et doit avoir une longueur n et une distance minimale supérieure à $\lceil d \cdot 2^{r-m} \rceil$. Pour que T puisse

être un code de Reed-Solomon (éventuellement étendu), on doit avoir $n \leq 2^l$, sa dimension est alors $n - \lceil d \cdot 2^{r-m} \rceil$.

Exemple 7.5 Le code $\mathcal{C} = \mathcal{P}(5,4)$ est un sous ensemble de $\mathrm{RM}(1,4)^{16}$ de cardinal 2^{55} et distance 32. Les cardinaux des espaces quotients sont

$\mathrm{RM}(4,4)/\mathrm{RM}(3,4)$	2
$\mathrm{RM}(3,4)/\mathrm{RM}(2,4)$	2^4
$\mathrm{RM}(2,4)/\mathrm{RM}(1,4)$	2^6

Ne pouvant pas trouver de translatés de $\mathrm{RM}(r,4)^{16}$ dans $\mathrm{RM}(4,4)^{16}$ puisque cela conduirait à une distance minimale de 32 pour le code T, qui n'est que de longueur 16, nous avons uniquement 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 représentant 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 $\mathrm{d_{min}}(\mathcal{C})/\mathrm{d_{min}}(S) = 32/4 = 8$, 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*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 $\mathrm{d_{min}}(\mathcal{G})/\mathrm{d_{min}}(S') = 32/2 = 1$ 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 représentant 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 $\mathrm{d_{min}}(\mathcal{C})/\mathrm{d_{min}}(S) = 16$, il est donc de dimension 1. Le code obtenu a alors un cardinal de 2^{65} éléments.

□

8 Bornes sur le cardinal des codes $\mathbb{Z}_{2^k}$-linéaires

L'existence de la construction détaillées dans la section 7 permet de déduire une borne sur le cardinal d'un code $\mathcal{C} \subset \mathrm{RM}(r,m)^n$, donc entre autre d'un code $\mathbb{Z}_{2^{m+1}}$-linéaire.

Proposition 8.1 *Soit $\mathcal{C} \subset RM(r,m)^n$ de distance minimale δ. Alors on a la borne suivante sur le cardinal de $\mathcal{C}$:*

$$|\mathcal{C}| \leq \frac{A^{\delta}_{n \cdot 2^m}(2)}{A^{\lceil 2^{r+a-m} \cdot \delta \rceil}_n \left(2^l\right)} \quad ,$$

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 $l = \sum_{i=1}^{a} \binom{m}{r+i}$.

PREUVE. Considérons un code T sur $\mathbb{F}_{2^l}$ de distance minimale $\lceil 2^{r+a-m} \cdot \delta \rceil$ et de cardinal $A_n^{\lceil 2^{r+a-m} \cdot \delta \rceil}(2^l)$. En appliquant le Théorème 7.2 en prenant pour S un ensemble de représentants des translatés de $\mathrm{RM}(r,m)$ dans $\mathrm{RM}(r+a,m)$, on obtient un code $\mathcal{G}$ de distance minimale δ et de longueur $n2^m$. Donc, $|\mathcal{G}| \leq A^{\delta}_{n\cdot 2^m}(2)$. Mais, $|\mathcal{G}| = |\mathcal{C}| \cdot |T|$ d'où $|\mathcal{C}| \cdot |T| \leq A^{\delta}_{n\cdot 2^m}(2)$, or $|T| = A_n^{\lceil 2^{r+a-m} \cdot \delta \rceil}(2^l)$, ce qui donne

$$|\mathcal{C}| \leq \frac{A^{\delta}_{n\cdot 2^m}(2)}{A_n^{\lceil 2^{r+a-m} \cdot \delta \rceil}(2^l)} \ .$$

□

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

Proposition 8.2 *Soient $\mathcal{C} \subset \mathrm{RM}(r,m)^n$ de distance minimale d, et $s_0 = r < s_1 < \ldots < s_t \leq m$. Alors*

$$|\mathcal{C}| \leq \frac{A^{d}_{n\cdot 2^m}(2)}{\prod_{j=1}^{t} A_n^{\lceil 2^{s_j - m} \cdot d \rceil}(2^{l_j})} \ ,$$

avec $l_j = \sum_{i=s_{j-1}+1}^{s_j} \binom{m}{i}$.

La remarque 7.4 permet également d'obtenir d'autres bornes du même type.

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 $\mathrm{S(x)}$ une borne sup sur le taux de transmission des codes binaires de longueur n et de distance minimale $x \cdot n$, pour $n \to \infty$. De même nous noterons $\mathrm{I_q(x)}$ une borne inf sur R pour les codes de longueur n sur $\mathbb{F}_q$ de distance minimale $x \cdot n$. La proposition 8.2 donne alors

Corollaire 8.3 *Soit $R_m(x)$ le taux de transmission maximal d'un code binaire de longueur $2^m \cdot n$, distance minimale $x \cdot 2^m \cdot n$ et inclus dans $\mathrm{RM}(1,m)^n$. Avec les notation de la proposition 8.2 nous avons*

$$R_m(x) \leq \mathrm{S}(x) - \frac{1}{2^m} \sum_{j=1}^{t} l_j \cdot \mathrm{I}_{2^{l_j}}(x \cdot 2^{s_j}) \ .$$

PREUVE. En prenant le logarithme de la borne de la proposition 8.2 et en divisant par $2^m \cdot n$, on obtient

$$\frac{\log_2(|\mathcal{C}|)}{2^m \cdot n} \leq \frac{\log_2\left(A^d_{n\cdot 2^m}(2)\right)}{2^m \cdot n} - \sum_{j=1}^{t} \frac{1}{2^m} \cdot \frac{\log_2\left(A_n^{\lceil 2^{s_j-m}\cdot d\rceil}\left(2^{l_j}\right)\right)}{n} \quad .$$

Soit, pour $x = d/(2^m \cdot n)$ fixé et n tendant vers l'infini

$$R(x) \leq \mathrm{S}(x) - \frac{1}{2^m} \sum_{j=1}^{t} \log_2\left(2^{l_j}\right) \mathrm{I}_{2^{l_j}}\left(x \cdot 2^{s_j}\right) \quad ,$$

étant donné que $x \cdot 2^s_j$ est la distance relative du code de longueur n sur $\mathbb{F}_{2^{l_j}}$ et de cardinal $A_n^{\lceil 2^{s_j-m}\cdot d\rceil}(2^{l_j})$. □

Les bornes $\mathrm{I_q}$ peuvent être remplacée par la borne de Gilbert-Varshamov, ce qui donne

$$\lim_{n\to\infty} \frac{\log_q A^\delta_n(q)}{n} \geq 1 - H_q\left(\frac{\delta}{n}\right) \quad ,$$

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

$$H_q(x) = x\log_q(q-1) - x\log_q(x) - (1-x)\log_q(1-x)$$

pour $x \in [0,(q-1)/q]$ et 0 autrement. Pour la borne sup S nous utilisons la borne d'Elias, soit

$$\lim_{n\to\infty} \frac{\log_2 A^\delta_n(2)}{n} \leq 1 - H_2\left(\frac{1}{2}\left(1 - \sqrt{1-2\frac{\delta}{n}}\right)\right) \quad ,$$

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

$$R_m(x) \leq 1 - H_2\left(\frac{1}{2}\left(1-\sqrt{1-2x}\right)\right) - \frac{1}{2^m}\sum_{i=2}^{m} l_i\left(1 - H_{2^{l_i}}\left(x\cdot 2^i\right)\right)$$

avec $l_i = \binom{m}{i}$. La figure 2 donne une idée du comportement de ce type de bornes, et comporte également la borne triviale obtenue a 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 $(m+1)/2^m$. Comme le montre cette figure, le type de bornes asymptotiques que nous obtenons ne semble pas donnée de grande amélioration : sur $\mathbb{Z}_8$, l'amélioration est faible ($x \in [0.06; 0.125]$) et pour $\mathbb{Z}_{16}$, elle est presque imperceptible (x au voisinage de 0.21).

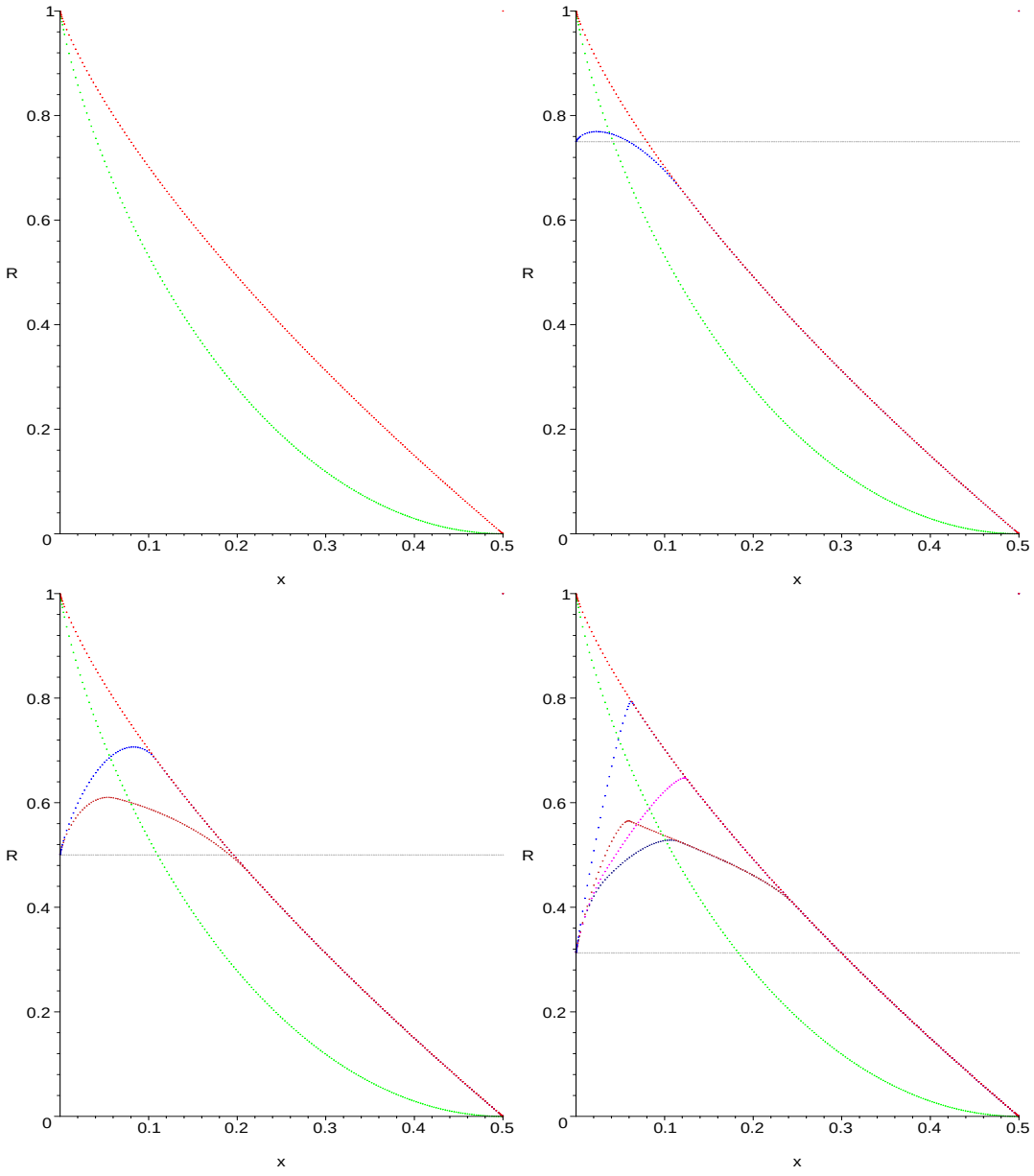

FIG. 2: *Bornes sur les codes $\mathbb{Z}_8$, $\mathbb{Z}_{16}$ et $\mathbb{Z}_{32}$-linéaires: en haut gauche, bornes d'Elias et de Gilbert-Varshamov; en haut à droite, bornes pour $\mathbb{Z}_8$; en bas à gauche, bornes pour $\mathbb{Z}_{16}$; en bas à droite, bornes pour $\mathbb{Z}_{32}$.*

9 Conclusions

Codes de Kerdock Généralisés

Les résultats de §5.3 montrent que, pour les valeurs de k et de m étudiées, les codes de Kerdock généralisés introduits dans [Car98] n'ont pas de bons paramètres. Il en est de même pour les codes de Preparata généralisés introduits dans ce document. Plus précisément, plus le nombre k augmente, plus les paramètres de ces codes se détériorent (e.g. $\mathcal{K}(3,8)$ et $\mathcal{K}(8,3)$ sont respectivement des codes $(1024, 2^{27}, 440)$ et $(1024, 2^{32}, 320)$ et sont à comparer au dual du code BCH 3 correcteur étendu qui est un code $[1023, 31, 448]$). Les sections 7 et 8 expliquent très bien cette observation, l'ensemble d'arrivée de l'application de Gray généralisée est trop petit relativement à la longueur des mots.

D'autre part, ces résultats numériques incitent à penser que les propriétés des codes $\mathbb{Z}_{2^k}$-linéaires dépendent essentiellement des propriétés de l'application de Gray : si on considère la structure cyclique des relevés des codes $\mathcal{K}(k,m)$ (cf. §5.2), on a qu'essentiellement ces derniers sont des codes obtenus par relèvement de Hensel d'un polynôme g divisant $X^{2^m}-1$. Les résultats obtenus signifient alors que le poids (homogène) minimal du code obtenu par relèvement de Hensel à $\mathbb{Z}_{2^{k+1}}$ du polynôme g est le double de celui du code obtenu par relèvement à $\mathbb{Z}_{2^k}$ du même polynôme pour $k \geq 3$. En d'autres termes, le poids homogène normalisé, défini comme le poids homogène divisé par le cardinal de l'anneau, ne dépend que de m. Ce phénomène semble assez général, nous l'avons observé pour tout les tests faits sur les codes construits par relèvement de Hensel.

Bien que dans le cas $\mathbb{Z}_{2^k}$-linéaire, les codes de Kerdock généralisés ne soient pas intéressants, il est possible que dans le cas plus général des codes $\mathbb{Z}_{p^k}$-linéaires, $p > 2$, leurs paramètres soient intéressants (la Définition 5.1 se généralise en l'état en utilisant l'application de Gray généralisée de [GS99], cf. 6.2 pour le cas particulier de $\mathbb{Z}_9$). Ceci dit, dans le cas $p = 3$ cela ne semble pas être le cas, cf. Tables 10 et 11. Et quoi qu'il en soit, le même

Distance minimale δ du Kerdock généralisé.
Paramètres: $(3^{(m+k-1)}, k(m+1), \delta)$

m \k	2	3	4
3	$(81, 8, 41)$	$(243, 12, 123)$	$(729, 16, 369)$
4	$(243, 10, 133)$	$(729, 15, 399)$	$(2187, 20, 1197)$
5	$(729, 12, 405)$	$(2187, 18, 1205)$	
6	$(2187, 14, 1215)$	$(6561, 21, 3645)$	
7	$(6561, 16, 3645)$		
8	$(19683, 18, 10935)$		

TAB. 10: *Distance minimale du code de Kerdock généralisé en petite dimension pour p=3. La notation (l, d, δ) signifie que le code est de longueur l, de pseudo-dimension d sur $\mathbb{Z}_3$ (i.e. a 3^d mots) et de distance minimale δ.*

genre de construction que celle donnée dans la section 7 s'appliquant, il ne faut pas espérer obtenir de bons codes pour des valeurs de k élevées.

Borne sur la plus grande distance minimale possible pour un code ternaire linéaire ayant même longueur et dimension que le Kg(m,k) pour $p = 3$

m\k	2	3
3	$48 - 50$	$144 - 153$
4	$153 - 155$	

TAB. 11: *Extrait de la table de Brouwer (ternaire): Morceaux choisis de la table des meilleurs codes ternaires linéaires connus et des bornes sur leur distance minimale. La notation* $b_{min} - b_{max}$ *signifie que l'on connaît un code ternaire linéaire de distance minimale* b_{min} *et que la borne supérieure la plus fine que l'on connaisse est* b_{max}.

Utilisation de Codes $\mathbb{Z}_{2^k}$-linéaires pour construire de bon codes binaires

Bien que n'ayant pas réussi à obtenir des codes dépassant les meilleurs codes connus en appliquant la construction du théorème 7.2, la table 9 donne une idée de l'augmentation du cardinal que l'on peut atteindre. Ainsi, il est fort probable que l'application de cette construction puisse conduire à de bons codes binaires. Rappelons également que le code de [DGLS01] est construit en premier lieu par le relèvement d'un code parfait, mais est ensuite amélioré par l'ajout d'un translaté, ce que nous avons généralisé avec notre construction – rappelons toutefois que dans ce cas précis, le code avant ajout du translaté est déjà meilleur que les précédents codes connus.

Application de Gray généralisée

Nous avons vu dans la section 6 que la notion de code $\mathbb{Z}_{2^k}$-linéaire permet de construire des codes dépassant les codes linéaires au moins dans le cas de $\mathbb{Z}_8$ et les égalant pour $\mathbb{Z}_{16}$ avec le relevé du code de résidus quadratiques (cf. section 6.3).

Une autre possibilité pour construire de bons codes est d'essayer de trouver une autre généralisation de l'application de Gray que celle de C. Carlet. Sa généralisation envoie $\mathbb{Z}_{2^k}$ dans l'ensemble des fonctions affines de $k-1$ variables. Or, cet ensemble est un code linéaire, le code de Reed-Muller d'ordre 1 en $k-1$ variables (noté $\mathrm{RM}(1, k-1)$), dont la distribution des poids est

i	A_i
0	1
2^{k-2}	$2^k - 2$
2^{k-1}	1

(voir [MS96, Chp. 13]).
Donc, une voie pour améliorer la généralisation de l'application de Gray est d'essayer de le faire arriver dans un "meilleur" code, e.g. un code $\mathbf{C}$ de longueur n ayant un meilleur rapport

$$\rho = \frac{\delta_{min}(\mathbf{C})}{n - \log_2(\mathbf{C})} \ .$$

Le nombre $n - \log_2(\mathbf{C})$ s'appelle la redondance du code $\mathbf{C}$, le rapport ρ mesure donc la capacité de correction du code par rapport à la redondance.
Le premier obstacle rencontré est que le code $\Psi(\mathbb{Z}_{2^k}) = \mathrm{RM}(1, k-1)$ est simple : il n'a, essentiellement, qu'un seul poids. Or, la propriété de conservation des distances est très restrictive. En effet, si on note w le poids défini sur $\mathbb{Z}_{2^k}$, on doit avoir

$$\begin{array}{ccccc} \mathrm{d}_w(a,b) & = & \mathrm{w}(a-b) & = & \mathrm{w_H}(\psi(a-b)) \\ \| & & & & \\ \mathrm{d_H}(\psi(a),\psi(b)) & = & & & \mathrm{w_H}(\psi(a)-\psi(b)) \end{array}$$

pour toute application $\psi : (\mathbb{Z}_{2^k}, \mathrm{w}) \leftarrow ({\mathbb{F}_2}^l, \mathrm{w_H})$ conservant les distances. Autrement dit, ψ conserve les distances si et seulement si les mots $\psi(a) - \psi(b)$ et $\psi(a-b)$, bien que n'étant pas nécessairement égaux, ont le même poids de Hamming. Le fait d'arriver dans un code linéaire simple est alors un avantage, cela facilite la construction d'une application conservant les distances (schématiquement pour Ψ, hormis quelques cas particuliers, $\Psi(a) - \Psi(b) \in \mathrm{RM}(1, k-1)$ a un poids de Hamming 2^{k-2} et $\Psi(a-b)$ est de poids 2^{k-2}, voir [Car98, §II Prop. 1] pour les détails). Ainsi, changer de code compliquerait nécessairement la construction d'une application ψ.

Un second obstacle provient de l'optimalité des codes de Reed-Muller d'ordre 1 : ils atteignent la borne de Griesmer, i.e. il n'existe pas de code linéaire de même dimension et de même distance minimale qui soit de longueur plus petite ([MS96, Chp. 17 §5]).

Compte tenu de cela, un candidat possible pour remplacer le code $\mathrm{RM}(1, k-1)$ est le code $\mathcal{K}(2, m)$, où $m = k/2 - 1$, au moins lorsque k est divisible par 4. Dans ce cas $m = k/2 - 1$ est un entier impair et $\mathcal{K}(2, k/2-1)$ est le code de Kerdock de longueur $2^{k/2}$. On sait alors que ce code a (essentiellement) 3 poids (cf. 5.1), donc, on peut espérer ne pas trop complexifier la construction d'une application ψ conservant les distances. D'autre part, ce code est bon puisqu'il est meilleur que les codes binaires (linéaires ou non) actuellement connus ayant une longueur et un cardinal comparable.

Références

[Aug93] AUGOT (D.). – *Étude Algébrique des Mots de Poids Minimum des Codes Cycliques, Méthodes d'Algèbre Linéaire sur les Corps Finis.* – Thèse de doctorat, Université de PARIS 6, 1993.

[Bro98] BROUWER (A.E.). – *Chapitre* "Bounds on the Size of Linear Codes" *dans Handbook of Coding Theory*, vol. 1, pp. 295–461. – North-Holland, 1998. (`http://www.win.tue.nl/~aeb/voorlincod.html`).

[BSC95] BONNECAZE (A.), SOLÉ (P.) et CALDERBANK (A.R.). – Quaternary quadratic residue codes and unimodular lattices. *IEEE Transactions on Information Theory*, vol. IT-41, n° 2, 1995, pp. 366–377.

[Car98] CARLET (C.). – $\mathbb{Z}_{2^k}$-linear codes. *IEEE Transactions on Information Theory*, vol. IT-44, n° 4, 1998, pp. 1543–1547.

[Car99] CARLET (C.). – On Kerdock codes. *Contemporary Mathematics*, vol. 255, 1999, pp. 155–163.

[CH97] CONSTANTINESCU (I.) et HEISE (W.). – A metric for codes over residue class rings. *Problems of Information Transmission*, vol. 33, n° 3, 1997, pp. 208–213. – (Traduit du Russe, *Problemy Peredachi Informatsii*, vol. 33, n° 3, 1997, pp. 22–28).

[CMKH96] CALDERBANK (A.R.), MCGUIRE (G.), KUMAR (P.V.) et HELLESETH (T.). – Cyclic codes over $\mathbb{Z}_4$, locator polynomials and Newton's identities. *IEEE Transactions on Information Theory*, vol. IT-42, n° 1, 1996, pp. 217–226.

[CS95] CALDERBANK (A.R.) et SLOANE. (N.J.A.). – Modular and p-adic cylic codes. *Designs, Codes and Cryptography*, vol. 6, 1995, pp. 21–35.

[DGLS01] DUURSMA (I.M.), GREFERATH (M.), LITSYN (S.N.) et SCHMIDT (S.E.). – 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. IT-47, n° 4, 2001, pp. 1596–1598.

[Gal03] GALAND (F.). – On the minimum distance of some families of $\mathbb{Z}_{2^k}$-linear codes. *In : 15th AAECC*, éd. par FOSSORIER (M.), HØHOLDT (T.) et POLI (A.), LNCS. pp. 235–243. – Springer, 2003.

[GS99] GREFERATH (M.) et SCHMIDT (S.E.). – Gray isometries for finite chain rings and a nonlinear ternary $(36, 3^{12}, 15)$ code. *IEEE Transactions on Information Theory*, vol. IT-45, n° 7, 1999, pp. 2522–2524.

[HKC+94] Hammons (R.), Kumar (P.V.), Calderbank (A.R.), Sloane (N.J.A.) et Solé (P.). – Kerdock, Preparata, Goethals and other codes are linear over $\mathbb{Z}_4$. *IEEE Transactions on Information Theory*, vol. IT-40, n° 2, 1994, pp. 301–319.

[HN99] Honold (T.) et Nechaev (A.A.). – Weighted modules and representations of codes. *Problems of Information Transmission*, vol. 35, n° 3, 1999, pp. 205–223. – (Traduit du Russe, *Problemy Peredachi Informatsii*, vol. 35, n° 3, 1999, pp. 18–39).

[Hun80] Hungerford (T.W.). – *Algebra.* – Springer-Verlag, 1980.

[Ker72] Kerdock (A.M.). – A class of low-rate nonlinear codes. *Information and Control*, vol. 20, 1972.

[KN93] Kuzmin (A.S.) et Nechaev (A.A.). – A construction of noise stable codes using linear recurring sequences over Galois ring. *Uspehi Mat. Nauk.*, vol. 48, n° 3, 1993, pp. 197–198. – (Russe).

[KN94] Kuzmin (A.S.) et Nechaev (A.A.). – Linearly presentable codes and Kerdock codes over arbitrary Galois fields of characteristic 2. *Uspehi Mat. Nauk.*, vol. 49, n° 5, 1994, pp. 165–166. – (Russe).

[Lit98] Litsyn (S.N.). – *Chapitre* "An Updated Table of the Best Binary Codes Known" *dans Handbook of Coding Theory*, vol. 1, pp. 463–498. – North-Holland, 1998. (`http://www.eng.tau.ac.il/~litsyn`).

[LN97] Lidl (R.) et Niederreiter (H.). – *Finite Fields.* – Cambridge Univerity Press, 1997, 2ème édition, *Encyclopedia of Mathematics and its Applications*, vol. 20.

[Mac74] MacDonald (B.R.). – *Finite Rings with Identity.* – Dekker, 1974.

[MS96] MacWilliams (F.J.) et Sloane (N.J.A.). – *The Theory of Error-Correcting Codes.* – North-Holland, 1996, 3ème édition.

[Nec91] Nechaev (A.A.). – Kerdock codes in a cyclic form. *Discrete Mathematics and Applications*, vol. 1, n° 4, 1991, pp. 365–384. – (Traduit du Russe, *Diskretnaya Matematika*, vol. 1, n° 4, 1989, pp. 123–139).

[PQ96] Pless (V.S.) et Qian (Z.). – Cyclic codes and quadratic residue codes over $\mathbb{Z}_4$. *IEEE Transactions on Information Theory*, vol. IT-42, n° 5, 1996, pp. 1594–1600.

[Pre68] Preparata (F.P.). – A class of optimum nonlinear double-error correcting codes. *Information and Control*, vol. 16, 1968.

[PW95] Papini (O.) et Wolfmann (J.). – *Algèbre Discrète et Codes Correcteurs.* – Springer-Verlag, 1995, *Mathématique & Applications*, vol. 20.

[SM99] SĂLĂGEAN-MANDACHE (A.). – On the isometries between $\mathbb{Z}_{p^k}$ and $\mathbb{Z}_p^k$. *IEEE Transactions on Information Theory*, vol. IT-45, n° 6, 1999, pp. 2146–2148.

[Van99] VAN LINT (J.H.). – *Introduction to Coding Theory.* – Springer-Verlag, 1999, 3ème édition.

[VG99] VON ZUR GATHEN (J.) et GERHARD (J.). – *Modern Computer Algebra.* – Cambridge University Press, 1999.

[Wan97] WAN (Z.-X.). – *Quaternary Codes.* – World Scientific, 1997, *Series on Applied Mathematics*, vol. 8.

[Wic98] WICKER (S.B.). – *Chapitre* "Deep Space Applications" *dans Handbook of Coding Theory*, vol. 2, pp. 2119–2200. – North-Holland, 1998.

Unité de recherche INRIA Rocquencourt
Domaine de Voluceau - Rocquencourt - BP 105 - 78153 Le Chesnay Cedex (France)

Unité de recherche INRIA Lorraine : LORIA, Technopôle de Nancy-Brabois - Campus scientifique
615, rue du Jardin Botanique - BP 101 - 54602 Villers-lès-Nancy Cedex (France)
Unité de recherche INRIA Rennes : IRISA, Campus universitaire de Beaulieu - 35042 Rennes Cedex (France)
Unité de recherche INRIA Rhône-Alpes : 655, avenue de l'Europe - 38330 Montbonnot-St-Martin (France)
Unité de recherche INRIA Sophia Antipolis : 2004, route des Lucioles - BP 93 - 06902 Sophia Antipolis Cedex (France)

Éditeur
INRIA - Domaine de Voluceau - Rocquencourt, BP 105 - 78153 Le Chesnay Cedex (France)
http://www.inria.fr
ISSN 0249-6399