Autour de codes définis à l'aide de polynômes tordus

Delphine Boucher

UNIVERSITÉ DE RENNES 1

Mémoire d'habilitation à diriger des recherches

École doctorale MathSTIC
Mathématiques et leurs Interactions

préparé à l'IRMAR - Université de Rennes 1

présenté par

Delphine Boucher [1]

le 2 juin 2020

Autour de codes définis à l'aide de polynômes tordus

devant jury composé de

Mme Christine Bachoc	Professeure, Université de Bordeaux	Rapporteure
M. Thierry Berger	Professeur émérite, Université de Limoges	Rapporteur
M. Steven Dougherty	Professeur, Université de Scranton	Rapporteur
M. Daniel Augot	Directeur de recherche, INRIA Saclay	Examinateur
M. Bruno Salvy	Directeur de recherche, INRIA, Lyon	Examinateur
M. Felix Ulmer	Professeur, Université de Rennes 1	Examinateur

1. Univ Rennes, CNRS, IRMAR - UMR 6625, F-35000 Rennes, France

Table des matières

Introduction

Mes travaux se sont déroulés en deux étapes depuis que je suis maître de conférences à l'Université de Rennes 1. Tout d'abord, de 2001 à 2008, j'ai travaillé dans la continuité de ma thèse sur l'algorithmique des équations différentielles à paramètres et leur application aux systèmes hamiltoniens, avec la participation au projet ANR 'Intégrabilité réelle et complexe en Mécanique Hamiltonienne'(2005-2008). Puis, à partir de 2007, mes travaux se sont tournés vers la théorie des codes correcteurs et l'application des polynômes de Ore (ou tordus) aux codes. Même si ces deux axes de recherche peuvent paraître éloignés, ils partagent des points communs. Tout d'abord, d'un point de vue théorique, les équations différentielles sont des objets liés aux polynômes de Ore. Par ailleurs, le calcul formel et l'implantation d'algorithmes sont présents dans les deux axes (avec MAPLE pour le premier et avec MAGMA pour le second). Enfin, l'aspect expérimental du calcul formel est une source d'inspiration depuis le début de mes travaux de thèse et reste encore omniprésent à ce jour.

Les codes tordus ont été définis dans [BGU07] (codes cycliques tordus) puis [BU09b], [BU09a] (codes modules tordus) et font l'objet de plusieurs thèses : Lionel Chaussade en 2010 à l'Université de Rennes 1 ([Cha10]), Neville Fogarty en 2016 à l'université du Kentucky ([Fog16]) et Rayna D. Boulanouar à l'Université d'Alger (thèse en cours). Mes travaux sur ce sujet sont des collaborations principalement avec Felix Ulmer, qui est l'initiateur de l'étude des codes tordus ([BGU07]), mais aussi Willi Geiselmann ([BGU07], [BGG$^+$10]) puis Patrick Solé ([BSU08]), Philippe Gaborit et Olivier Ruatta ([BGG$^+$10]). Ils peuvent être regroupés en quatre parties :

— codes tordus et dualité ([BU11], [BU14b], [Bou15], [Bou16], [Bou18]) ;
— codes d'évaluation tordue et leur décodage ([BU14a], [Bou19]) ;
— codes tordus définis sur l'anneau GR(4,2) et applications ([BSU08]) ;
— un cryptosystème à base de polynômes tordus ([BGG$^+$10]).

Dans ce document, j'ai fait le choix de me focaliser plus particulièrement sur les codes cycliques tordus auto-duaux et sur les codes d'évaluation tordue puisque ces deux thématiques sont celles qui m'ont le plus particulièrement occupée ces cinq dernières années.

Dans la première partie, je rappellerai quelques généralités sur les codes linéaires et sur les polynômes tordus, puis je définirai les codes cycliques tordus et les codes modules tordus.

Dans la deuxième partie, je me focaliserai sur une équation, appelée équation auto-duale tordue, caractérisant les codes cycliques tordus auto-duaux. Quelques observations sur des résultats expérimentaux ont permis d'établir deux conjectures sur l'existence des codes cycliques tordus auto-duaux et sur leur énumération sur $\mathbb{F}_4$ en dimension 2^s. On peut démontrer ces deux conjectures en s'appuyant sur un peu d'arithmétique dans les corps finis, des résultats de Sloane et Thompson sur les codes cycliques auto-duaux et enfin des propriétés de factorisation des polynômes tordus de Giesbrecht et Odoni notamment. Les démonstrations de ces deux conjectures ont permis également de mettre en place les outils théoriques qui s'avèrent

utiles pour l'énumération et la construction des codes θ-cycliques auto-duaux sur $\mathbb{F}_{p^2}$.

La troisième partie est dédiée aux codes d'évaluation tordue. Un lien sera établi avec les codes de Gabidulin et un algorithme de décodage du type Berlekamp-Welch sera présenté pour la métrique de Hamming. Puis je m'intéresserai à la métrique tordue pour laquelle j'adapterai l'algorithme de décodage précédent. Enfin un début de décodage en liste sera proposé.

Chapitre 1

Une brève introduction aux codes modules tordus

1 Quelques généralités sur les codes.

Nous allons commencer par quelques généralités sur les codes linéaires. On pourra se référer à [Ple98] dans un premier temps puis à [MS77]. Soit $\mathbb{F}_q$ un corps fini à q éléments. Un code linéaire de longueur n sur $\mathbb{F}_q$ et de dimension k est un sous-espace vectoriel de $\mathbb{F}_q^n$ de dimension k. Un tel code C peut être vu comme l'image d'une application linéaire d'encodage injective :

$$\phi \left\{ \begin{array}{ccc} \mathbb{F}_q^k & \to & \mathbb{F}_q^n \\ m & \mapsto & mG \end{array} \right.$$

où G est une matrice $k \times n$ à coefficients dans $\mathbb{F}_q$ de rang k et m représente le message à coder. On dit que G est une *matrice génératrice* de C. La *distance minimale* de C est

$$d = \min_{x,y \in C, x \neq y} d_H(x,y) = \min_{x \in C, x \neq 0} w_H(x)$$

où pour x, y dans $\mathbb{F}_q^n$, $d_H(x,y) = w_H(x-y) = \#\{i \mid x_i - y_i \neq 0\}$ est la *distance de Hamming* de x à y. Un code linéaire sur $\mathbb{F}_q$ de longueur n, dimension k et distance minimale d est noté $[n,k,d]_q$.

Pour un code linéaire de distance minimale d, les boules centrées en les mots de code de rayon $t := \lfloor \frac{d-1}{2} \rfloor$ sont disjointes deux à deux. Ainsi, considérons $c = mG$ un mot de code, e dans $\mathbb{F}_q^n$ de poids de Hamming $w_H(e)$ inférieur ou égal à t et $r = c + e$ (mot reçu). Alors c est l'unique mot de code à une distance de Hamming inférieure ou égale à t de r et m est l'unique message associé. On dit que le code C est t-correcteur d'erreurs.

Pour un code $[n,k,d]_q$, on veut que le *taux d'information*, $\frac{k}{n}$ et la *distance relative*, $\frac{d}{n}$, soient les plus grands possibles. De plus on cherche à construire des algorithmes de décodage (permettant de retrouver m connaissant le mot reçu r) efficaces.

On a une contrainte sur la distance minimale du code, donnée par le théorème de la borne de Singleton ($d \leq n - k + 1$). Si cette borne est atteinte, on parle de code MDS (Maximum Distance Separable).

Un code linéaire peut aussi être caractérisé par le noyau d'une matrice, appelée *matrice de contrôle*.

Définition 1. *Soit C un code linéaire de longueur n sur $\mathbb{F}_q$. Le* dual $C^\perp$ *de C est*

$$C^\perp = \{x \in \mathbb{F}_q^n \mid \forall c \in C, < x, c >= 0\}$$

où pour $x = (x_1, \ldots, x_n)$ et $y = (y_1, \ldots, y_n)$ dans $\mathbb{F}_q^n$, $< x, y >:= \sum_{i=1}^n x_i y_i$ est le produit scalaire euclidien de x et y.

Le code C est dit auto-dual *si $C = C^\perp$.*

Une *matrice de contrôle* H de C est une matrice génératrice de $C^\perp$. On a donc :

$$C = \{mG \mid m \in \mathbb{F}_q^k\} = \{x \in \mathbb{F}_q^n \mid H \times {}^t x = 0\}.$$

2 Codes θ-cycliques ou cycliques tordus

Les codes θ-cycliques ont été introduits dans [BGU07] suivant une idée de Felix Ulmer :

Définition 2 ([BGU07])**.** *Soit C un code linéaire de longueur n sur $\mathbb{F}_q$ et soit θ un automorphisme de $\mathbb{F}_q$. C est un code* θ-cyclique *si*

$$\forall c = (c_0, \ldots, c_{n-1}) \in \mathbb{F}_q^n, c \in C \Rightarrow (\theta(c_{n-1}), \theta(c_0), \ldots, \theta(c_{n-2})) \in C.$$

Si θ est l'identité, le code est dit cyclique.

Si C est défini sur $\mathbb{F}_{q^n}$ (où n est la longueur de C) et θ est l'automorphisme de $\mathbb{F}_{q^n}$ défini par $a \mapsto a^q$, le code est dit q-cyclique de Gabidulin ([Gab85]).

Si θ est l'identité, on a une correspondance bijective entre $\mathbb{F}_q^n$ et $\mathbb{F}_q[X]/(X^n - 1)$ et un code cyclique peut être vu comme un idéal principal de l'anneau $\mathbb{F}_q[X]/(X^n - 1)$ engendré par g diviseur de $X^n - 1$.

On va donner une interprétation polynomiale aux codes θ-cycliques en se plaçant dans l'anneau des polynômes tordus. On définit l'anneau des polynômes tordus (ou de Ore, [Ore33]) $R = \mathbb{F}_q[X; \theta]$ par l'ensemble des $\sum a_i X^i, a_i \in \mathbb{F}_q$ où la somme est la somme habituelle des polynômes et où la multiplication est régie par la loi

$$\forall a \in \mathbb{F}_q, X \cdot a = \theta(a) X.$$

R est un anneau euclidien à droite et à gauche et on dispose d'un algorithme d'Euclide (voir [BP94]) pour le calcul des pgcd à droite (gcrd), pgcd à gauche (gcld), ppcm à gauche (lclm) et ppcm à droite (lcrm). Le centre $Z(R)$ de R est l'ensemble des $f \in \mathbb{F}_q^\theta[X^m]$ où $\mathbb{F}_q^\theta$ est le corps laissé fixe par θ et $m = |\theta|$ est l'ordre de θ. Par exemple, si $q = p^m$ et $\theta : x \mapsto x^p$ on a : $\forall a \in \mathbb{F}_q, X^m \cdot a = \theta^m(a) X^m = aX^m$.

Un code θ-cyclique est ainsi associé à un R-sous-module à gauche du R-module à gauche $R/R(X^n - 1)$ à savoir $Rg/R(X^n - 1)$ où g est un diviseur à droite de $X^n - 1$. On dit que g est un *polynôme générateur tordu* du code.

Une matrice génératrice G d'un code θ-cyclique $[n, k]$ engendré par $g = g_0 + g_1 X + \cdots + g_{n-k} X^{n-k}$ est

$$G = \begin{pmatrix} g_0 & \ldots & \ldots & g_{n-k} & 0 & \ldots & 0 \\ 0 & \theta(g_0) & \ldots & \ldots & \theta(g_{n-k}) & \ddots & \vdots \\ \vdots & \ddots & \ddots & & & \ddots & 0 \\ 0 & \ldots & 0 & \theta^{k-1}(g_0) & \ldots & \ldots & \theta^{k-1}(g_{n-k}) \end{pmatrix}.$$

Remarque 1. *Considérons un code C θ-cyclique de longueur n. Si θ est d'ordre m divisant n, alors C est m-quasi-cyclique. En effet, on a pour tout c dans C, $X^m \cdot c = c \cdot X^m$ (car les coefficients de c sont laissés fixes par θ^m) et $X^m \cdot c \in C$, donc $\forall c = (c_0, \ldots, c_{n-1}) \in C, (c_{n-m}, \ldots, c_{n-1}, c_0, \ldots, c_{n-m-1}) \in C$.*

Exemple 1. *Considérons les codes cycliques et les codes θ-cycliques $[2,1]_4$, $[4,2]_4$ et $[10,5]_4$ où $\theta : x \mapsto x^2$. On note $R = \mathbb{F}_4[X;\theta]$ où $\mathbb{F}_4 = \mathbb{F}_2(a)$ et $a^2 + a + 1 = 0$.*

— *Dans $\mathbb{F}_4[X]$, $X^2 - 1 = (X-1)^2$ donc il y a un code cyclique $[2,1]_4$. Dans R on a*

$$\begin{aligned} X^2 - 1 &= (X-1)\cdot(X-1) \\ &= (X+a)\cdot(X+a^2) \\ &= (X+a^2)\cdot(X+a) \end{aligned}$$

donc il y a 3 codes θ-cycliques $[2,1]_4$.

— *Dans $\mathbb{F}_4[X]$, $X^4 - 1 = (X+1)^4 = (X^2+1)(X^2+1)$, donc on a un code cyclique $[4,2]_4$. Dans R,*

$$\begin{aligned} X^4 - 1 &= (X^2+1)\cdot(X^2+1) \\ &= (X^2+aX+a^2)\cdot(X^2+aX+a) \\ &= (X^2+a^2X+a)\cdot(X^2+a^2X+a^2) \\ &= (X^2+X+a)\cdot(X^2+X+a^2) \\ &= (X^2+X+a^2)\cdot(X^2+X+a) \\ &= (X^2+a^2X+a^2)\cdot(X^2+a^2X+a) \\ &= (X^2+aX+a)\cdot(X^2+aX+a^2) \end{aligned}$$

donc il y a 7 codes θ-cycliques $[4,2]_4$.

— *Dans $\mathbb{F}_4[X]$, $X^{10} - 1$ possède trois facteurs de degré 5 :*

$$\begin{aligned} X^{10} - 1 &= (X^5-1)\cdot(X^5-1) \\ &= (X^5+X^4+a^2X^3+a^2X^2+X+1)(X^5+X^4+aX^3+aX^2+X+1) \\ &= (X^5+X^4+aX^3+aX^2+X+1)(X^5+X^4+a^2X^3+a^2X^2+X+1). \end{aligned}$$

Dans R, $X^{10} - 1$ possède 51 facteurs à droite de degré 5.
Il y a donc 3 codes $[10,5]_4$ cycliques et 51 codes $[10,5]_4$ θ-cycliques.

3 Quelques mots sur la factorisation des polynômes tordus

Comme l'illustre l'exemple précédent, les codes cycliques tordus sont intéressants du fait de la multiplicité des facteurs à droite de $X^n - 1$ (voir [ALS16]).

De nombreux travaux existent sur la factorisation des polynômes tordus : Ore ([Ore33]), Jacobson ([Jac43]) ; Giesbrecht ([Gie98]) ; Odoni ([Odo99]) ; Coulter, Havas, Henderson ([CHH04]) ; Caruso, Leborgne ([CLB17]).

Dans la suite du texte, on utilisera deux types de décompositions des polynômes tordus : une décomposition en produit de polynômes tordus irréductibles et une décomposition sous forme de ppcm à gauche de polynômes tordus.

Définition 3 ([Ore33] page 488, [Jac43] page 33)**.** *Deux polynômes g_1 et g_2 de R sont dits* similaires *($g_1 \sim g_2$) s'il existe u dans R tel que $u \cdot g_1 = \mathrm{lclm}(u, g_2)$ avec $\mathrm{gcrd}(u, g_2) = 1$.*

Cela est encore équivalent à dire que les modules à gauche (ou à droite) $R/(g_1)$ et $R/(g_2)$ sont isomorphes.

Théorème 1 ([Ore33], [Jac43]). *Soient $h = h_1 \cdots h_m = g_1 \cdots g_n$ deux décompositions en produits d'irréductibles de R. Alors $m = n$ et il existe une permutation σ de $\{1, \ldots, n\}$ telle que pour tout i dans $\{1, \ldots, n\}, g_{\sigma(i)} \sim h_i$.*

Définition 4. *([Jac43], chap3) Soit h dans R. h est* décomposable *si h est le ppcm à gauche de polynômes tordus de degrés strictement inférieurs à $\deg(h)$: $h = \mathrm{lclm}(h_1, h_2)$ où h_1 et h_2 sont dans R de degrés strictement inférieurs au degré de h. Le polynôme tordu h est* indécomposable *s'il n'est pas décomposable.*

Une décomposition de h dans R comme ppcm à gauche de polynômes tordus peut être calculée efficacement via le théorème 2 ci-dessous. On aura besoin tout d'abord de la notion de borne. D'après [Jac43], un élément h de R est *borné* si l'idéal à gauche Rh contient un idéal bilatère. Les idéaux bilatères sont engendrés par les polynômes $X^t \cdot f$ où t est un entier et f est dans $\mathbb{F}_q^\theta[X^m]$ avec $\mathbb{F}_q^\theta$ corps laissé fixe par θ et m ordre de θ. Le polynôme f unitaire de l'idéal maximal bilatère contenu dans Rh est la *borne* de h.

La borne f est irréductible si l'idéal bilatère $(f) \subset R$ est maximal.

Une borne f avec un terme constant non nul appartient à $Z(R)$ et est une borne irréductible si et seulement si $f \in \mathbb{F}_q^\theta[X^m]$ est irréductible.

La borne d'un polynôme tordu peut être calculée de manière efficace via de l'algèbre linéaire ([Jac43] ; Lemme 4.2 de [Gie98]).

Lemme 1 (Lemme 7 de [BU09b]). *Soit g, h dans R tels que $h \cdot g \in Z(R)$, alors $h \cdot g = g \cdot h$.*

Démonstration. On a $h \cdot (g \cdot h) = (h \cdot g) \cdot h = h \cdot (h \cdot g)$. Comme R n'a pas de diviseur de zéro non trivial, on peut simplifier à gauche par h l'égalité $h \cdot (g \cdot h) = h \cdot (h \cdot g)$. □

Ainsi, si g dans R divise à droite un polynôme central f, alors il le divise aussi à gauche et on dira que g divise f.

Théorème 2 (Theorème 4.1 de [Gie98]). *Soient h dans R et f dans $Z(R)$ tels que h divise f. Soit $f_1, \ldots, f_\ell$ dans $Z(R)$ premiers entre eux deux à deux tels que $f = f_1 \cdots f_\ell$. Alors*
$h = \mathrm{lclm}(h_1, \ldots, h_\ell)$ où pour i dans $\{1, \ldots, \ell\}$, $h_i = \mathrm{gcrd}(h, f_i)$;
$h = \mathrm{lcrm}(h_1, \ldots, h_\ell)$ où pour i dans $\{1, \ldots, \ell\}$, $h_i = \mathrm{gcld}(h, f_i)$.

Les polynômes h_i apparaissant dans la décomposition ci-dessus sont nécessairement premiers entre eux dans R.

Pour terminer voici un résultat liant décomposition en produit d'irréductibles et décomposition comme ppcm.

Théorème 3 ([Jac43]).
1. *Soit h dans R. h possède une décomposition unique en produit de facteurs irréductibles unitaires de R si et seulement si h est indécomposable.*
2. *Soient $h_1, \ldots, h_n$ dans R irréductibles unitaires ayant la même borne f dans $Z(R)$. Alors le produit $h = h_1 \cdots h_n$ est un polynôme tordu unitaire indécomposable si et seulement si la borne de h est f^n.*

Si h dans R divise f^n avec f dans $Z(R)$ irréductible alors h est un produit de polynômes tordus unitaires irréductibles divisant f.

4 Codes θ-négacycliques, θ-constacycliques et θ-modules

On peut étendre la définition des codes θ-cycliques :
— codes θ-négacycliques : $Rg/R(X^n+1)$ où g divise à droite X^n+1 ;
— pour a dans $\mathbb{F}_q$, codes (θ,a)-constacycliques : $Rg/R(X^n-a)$ où g divise à droite X^n-a ;
— pour f dans R de degré n, codes θ-modules : Rg/Rf où g divise à droite f.

Définition 5 ([BU09a]). *Soit f dans R de degré n. Un* code θ-module C *est un R-sous-module à gauche $Rg/Rf \subset R/Rf$ où g est un diviseur à droite de f dans R.*

Sa longueur est $n = \deg(f)$ et sa dimension est $k = \deg(f) - \deg(g)$.

On dit que g est un polynôme générateur (tordu) *de C. Si g est unitaire, g est le polynôme générateur tordu (unitaire) de C.*

Notation : $C = (g)_{n,\theta}$

Dit autrement, C est un code θ-module de longueur n s'il existe g dans $R = \mathbb{F}_q[X;\theta]$ tel que pour tout $c = (c_0,\dots,c_{n-1})$ dans $\mathbb{F}_q^n$, :

$$(c_0,\dots,c_{n-1}) \in C \Leftrightarrow \ g \text{ divise à droite } c_0 + c_1X + \cdots + c_{n-1}X^{n-1}.$$

Par ailleurs un code θ-module de longueur n et de polynôme générateur tordu $g = \sum_{i=0}^{n-k} g_iX^i$ de degré $n-k$ possède comme matrice génératrice la matrice G (qui ne dépend pas de f) :

$$G = \begin{pmatrix} g_0 & \dots & \dots & g_{n-k} & 0 & \dots & 0 \\ 0 & \theta(g_0) & \dots & \dots & \theta(g_{n-k}) & \ddots & \vdots \\ \vdots & \ddots & \ddots & & & \ddots & 0 \\ 0 & \dots & 0 & \theta^{k-1}(g_0) & \dots & \dots & \theta^{k-1}(g_{n-k}) \end{pmatrix}.$$

Si C est un code θ-module de générateur g et de longueur n, alors deux cas se produisent.
— Il existe a dans $\mathbb{F}_q^*$ tel que g divise à droite $X^n - a$; alors C est un code (θ,a)-constacyclique.
— Pour tout a dans $\mathbb{F}_q^*$, g ne divise pas $X^n - a$ à droite. Alors il existe $N > n$ tel que g divise à droite $X^N - 1$. En effet, g est borné : il existe f dans $Z(R)$ tel que g divise f à droite et on conclut dans l'anneau commutatif $Z(R)$. Dans ce cas C est le code raccourci d'un code θ-cyclique (de longueur N).

Remark 1. *Une définition des codes modules tordus apparaît dans le contexte plus général des anneaux de polynômes tordus avec dérivation dans [BL13] (définition 3) et [BU11] (définition 4).*

5 Codes tordus et dualité

On va maintenant chercher à caractériser le dual d'un code θ-constacyclique. Pour cela on utilisera le polynôme réciproque tordu d'un polynôme tordu. Dans la suite, on note

$$\Theta : \begin{cases} R & \to & R \\ \sum a_iX^i & \mapsto & \sum \theta(a_i)X^i. \end{cases}$$

Définition 6 (Définition 3 de [BU11] ou Définition 2 de [Bou16]). *Soit* $h = \sum_{i=0}^{k} h_i X^i \in R$ *de degré* k. *Le* polynôme réciproque (tordu) *de* h *est*

$$h^* = \sum_{i=0}^{k} X^{k-i} \cdot h_i.$$

Le polynôme réciproque (tordu) unitaire de h *est*

$$h^\natural = \frac{1}{\theta^{k-v}(h_v)} h^*$$

où $v = \min\{i \mid h_i \neq 0\}$ *est la* valuation *de* h.

Exemple 2. *On considère ici* $\mathbb{F}_4 = \mathbb{F}_2(a), a^2+a+1 = 0$ *et* $\theta : x \mapsto x^2$. *Pour* $h = X^2 + aX + a$ *on a* $h^* = 1 + X \cdot a + X^2 \cdot a = 1 + a^2X + aX^2$ *donc* $h^\natural = X^2 + aX + a^2$.

Dans le lemme suivant, on exprime le polynôme réciproque d'un produit et le polynôme réciproque d'un polynôme réciproque. La partie 2 de ce lemme avait été initialement énoncée pour un polynôme tordu de coefficient constant non nul. Elle est complétée ici.

Lemme 2 (Lemme 1 de [BU11]). *Soient* f, g, h *dans* R *non nuls.*

1. $(h \cdot g)^* = \Theta^{\deg(h)}(g^*) \cdot h^*$.
2. *Soit* d *le degré de* f *et soit* v *la valuation de* f, *alors* $(f^*)^* \cdot X^v = \Theta^{d-v}(f)$.

Démonstration. (point 2.) Soit $f = \sum_{i=v}^{d} a_i X^i$ dans R de valuation v et de degré d. D'après la définition 6, $f^* = \sum_{i=v}^{d} \theta^{d-i}(a_i) X^{d-i} = \sum_{j=0}^{d-v} \theta^j(a_{d-j}) X^j$. Comme $\deg(f^*) = d - v$, on a $(f^*)^* = \sum_{i=0}^{d-v} X^{d-v-i} \cdot \theta^i(a_{d-i})$ et $(f^*)^* \cdot X^v = \sum_{j=0}^{d-v} \theta^{d-v}(a_{v+j}) X^{j+v} = \Theta^{d-v}(f)$.

□

Dans la proposition 1 qui suit, on établit que le dual d'un code (θ, a)-constacyclique est $(\theta, 1/a)$-constacyclique. Il se trouve que ce résultat découle d'un résultat plus général ([Huf98], lemme 1.3, page 1353) qui nous a été signalé par Thierry Berger. La démonstration de la proposition 1 permet néanmoins d'exprimer le polynôme générateur tordu du dual, ce qui sera utile pour la suite.

Proposition 1 (Théorème 1 et Lemme 2 de [BU11]). *Le dual d'un code* (θ, a)*-constacyclique* $C = (g)_{n,\theta}$ *est un code* $(\theta, 1/a)$*-constacyclique* $C^\perp = (h^\natural)_{n,\theta}$ *où* h *est défini par* $\Theta^n(h) \cdot g = X^n - a$.

Démonstration. Considérons le code (θ, a)-constacyclique C de longueur n, dimension k et polynôme générateur tordu (unitaire) g. Comme g divise $X^n - a$ à droite, il existe h dans R tel que

$$\Theta^n(h) \cdot g = X^n - a.$$

Multiplions cette égalité par h à droite, on obtient $\Theta^n(h) \cdot g \cdot h = (X^n - a) \cdot h$ donc $\Theta^n(h) \cdot (g \cdot h - X^n) = -a \cdot h$. En observant les degrés des membres de droite et de gauche, on obtient que $g \cdot h - X^n$ est une contante λ qui vérifie $\theta^k(\lambda) = -a$. On a donc

$$g \cdot h = X^n - \theta^{-k}(a).$$

De cette égalité, on déduit que le dual de C est engendré par le polynôme réciproque tordu $h^\natural$ de h. En effet on a, pour (i,j) dans $\{0,\dots,k-1\}\times\{0,\dots,n-k-1\}$ et $\ell = j-i+k \in \{1,\dots,n-1\}$:

$$< X^i\cdot g, X^j\cdot h^* >= \theta^i\left((g\cdot h)_\ell\right) = 0.$$

Par ailleurs, comme $\Theta^n(h)\cdot g = X^n - a$. On a $(\Theta^n(h)\cdot g)^* = 1-\theta^n(a)X^n$, donc $\Theta^k(g^*)\cdot\Theta^n(h^*) = 1-\theta^n(a)X^n$. On obtient :

$$\frac{-1}{a}\Theta^{k-n}(g^*)\cdot h^* = X^n - \frac{1}{a}.$$

Ainsi $h^\natural$ divise $X^n-\frac{1}{a}$ à droite et le code $C^\perp$ est un code $(\theta,\frac{1}{a})$-constacylique de polynôme générateur $h^\natural$.

□

On dit que h est le *polynôme de contrôle tordu* du code.

De la proposition 1, on déduit le corollaire suivant (voir corollaire 1 de [BU11] et la remarque qui suit).

Corollaire 1. *Soit C un code θ-module de polynôme générateur tordu g. On suppose que le coefficient contant de g est non nul. Si C est auto-dual alors C est θ-cyclique ou θ-négacyclique.*

Démonstration. Soit C un code θ-module auto-dual de longueur $n=2k$, dimension k et polynôme générateur tordu (unitaire) g ayant un coefficient constant non nul. Soit $h = \Theta^{-k}(g^*)$. On a $h^* = \Theta^{-k}(g^{**}) = \Theta^{-k}(\Theta^k(g)) = g$. De plus, comme C est auto-dual, on a, pour $i\in\{0,\dots,k-1\}$, $j\in\{0,\dots,k-1\}$ et $\ell = j-i+k$:

$$0 =< X^i\cdot g, X^j\cdot g >=< X^i\cdot g, X^j\cdot h^* >= \theta^i\left((g\cdot h)_\ell\right).$$

Le polynôme tordu $g\cdot h$ est donc un polynôme tordu de degré n dont tous les termes non dominants et non constants sont nuls. Notons u et v dans $\mathbb{F}_q^*$ tel que $g\cdot h = uX^n+v$. On a $\Theta^n(h)\cdot\frac{1}{u}\cdot g\cdot h = \Theta^n(h)\cdot X^n + \Theta^n(h)\cdot\frac{v}{u} = X^n\cdot h - \Theta^n(h)\cdot\frac{v}{u}$, donc $\Theta^n(h)\cdot\frac{1}{u}\cdot g - X^n$ est une constante, a. C est donc un code (θ,a)-constacyclique. D'après la proposition 1, $C^\perp$ est $(\theta,\frac{1}{a})$-constacyclique de longueur n, dimension $n-k$ et de polynôme générateur tordu (unitaire) $h^\natural$. Comme $C=C^\perp$, g divise à droite X^n-a et $X^n-\frac{1}{a}$ donc $a^2=1$. □

6 Le cas hermitien

On suppose ici que $q=r^2$ est une puissance paire d'un nombre premier. Pour a dans $\mathbb{F}_q$, on note $\overline{a} = a^r$. Le *dual Hermitien* d'un code linéaire C de longueur n sur $\mathbb{F}_q$ est défini par $C^{\perp_H} = \{x\in\mathbb{F}_q^n \mid \forall y\in C, < x,y >_H = 0\}$, où pour tout x,y dans $\mathbb{F}_q^n$, $< x,y >_H := \sum_{i=1}^n x_i\overline{y_i}$ est le produit scalaire hermitien de $x=(x_1,\dots,x_n)$ et $y=(y_1,\dots,y_n)$. Le code C est *auto-dual Hermitien* si $C=C^{\perp_H}$.

Dans la suite, on note, pour $f=\sum f_iX^i$ dans R, $\overline{f} = \sum\overline{f_i}X^i$.

Proposition 2. *Le dual hermitien d'un code (θ,a)-constacyclique $C=(g)_{n,\theta}$ est un code $(\theta,1/a^r)$-constacyclique $C^{\perp_H} = (\overline{h^\natural})_{n,\theta}$ où h dans R est défini par $\Theta^n(h)\cdot g = X^n-a$.*

Démonstration. Considérons le code (θ, a)-constacyclique C de longueur n, dimension k et polynôme générateur tordu (unitaire) g. Comme g divise $X^n - a$ à droite, il existe h dans R tel que

$$\Theta^n(h) \cdot g = X^n - a.$$

On a

$$g \cdot h = X^n - \theta^{-k}(a).$$

De cette égalité, on déduit que le dual hermitien $C^{\perp_H}$ de C est engendré par $\overline{h^\natural}$. En effet on a, pour (i, j) dans $\{0, \ldots, k-1\} \times \{0, \ldots, n-k-1\}$ et $\ell = j - i + k \in \{1, \ldots, n-1\}$:

$$< X^i \cdot g, X^j \cdot \overline{h^*} >_H = < X^i \cdot g, X^j \cdot h^* > = \theta^i \left((g \cdot h)_\ell \right).$$

Par ailleurs, $h^\natural$ divise $X^n - \frac{1}{a}$ à droite, donc $\overline{h^\natural}$ divise $X^n - 1/a^r$ à droite et le code $C^{\perp_H}$ est un code $(\theta, \frac{1}{a^r})$-constacylique de polynôme générateur $\overline{h^\natural}$.

□

Corollaire 2. *Un code θ-module auto-dual hermitien est (θ, a)-constacyclique avec $a^{r+1} = 1$.*

Démonstration. Soit C un code θ-module auto-dual hermitien de polynôme générateur tordu unitaire g. Nécessairement, il existe a dans $\mathbb{F}_q$ tel que g divise à droite $X^n - a$ dans R. C est (θ, a)-constacyclique et d'après la proposition 2, son dual hermitien $C^{\perp_H}$ est un code $(\theta, \frac{1}{a^r})$-constacyclique, ainsi g divise à droite $X^n - a$ et $X^n - 1/a^r$ donc $1/a^r = a$. □

Chapitre 2

Codes auto-duaux θ-cycliques et θ-cycliques étendus

C'est lors d'une visite à l'Xlim, à Limoges, que l'étude des codes θ-cycliques auto-duaux nous a été suggérée par Thierry Berger et Philippe Gaborit (voir [GO03] et [Gab04]).

Cette partie est une synthèse des papiers [BU11], [BU14b], [Bou15], [Bou16] et [Bou18].

Sans perte de généralité, on peut supposer que l'ordre m de θ divise la longueur du code n. En effet, tout diviseur à droite de $X^n - 1$ est à coefficients dans $\mathbb{F}_{p^\ell}$ où ℓ désigne le pgcd de m et n :

Lemme 3 (Lemme 2 de [Bou15])**.** *Soient $\mathbb{F}_q$ un corps fini, soit θ un automorphisme de $\mathbb{F}_q$, $R = \mathbb{F}_q[X;\theta]$, n un entier non nul, ℓ le pgcd de n et de l'ordre de θ et h un diviseur à droite unitaire de $X^n - 1$ dans R. Alors $X^\ell \cdot h = h \cdot X^\ell$ (ce qui signifie que les coefficients de h sont laissés fixes par θ^ℓ).*

Démonstration. Soient m l'ordre de θ, $u, v \in \mathbb{N}$ tels que $\ell = mu - nv$. On a $X^{mu} \cdot h \in Rh/R(X^n - 1)$, et $X^{mu} \cdot h = h \cdot X^{mu} = h \cdot X^\ell X^{nv} = h \cdot X^\ell \in R/R(X^n - 1)$, donc $h \cdot X^\ell \in Rh/R(X^n - 1)$ et il existe Q dans R unitaire de degré ℓ tel que $h \cdot X^\ell = Q \cdot h$. Le coefficient constant Q_0 de Q vérifie $Q_0 h_0 = 0$, or $h_0 \neq 0$, donc $Q_0 = 0$. De même on obtient que les termes de Q de degrés $\leq \ell - 1$ sont nuls ainsi $h \cdot X^\ell = X^\ell \cdot h$. □

Cette supposition implique en particulier que $X^n - 1$ est un polynôme central.

1 Equation auto-duale tordue

Rappelons qu'un code θ-cyclique de longueur n et de polynôme générateur tordu unitaire g est auto-dual si $g = h^\natural$ où h est le polynôme de contrôle tordu unitaire défini par $\Theta^n(h) \cdot g = X^n - 1$. Les polynômes de contrôle tordus unitaires des codes θ-cycliques auto-duaux de longueur n sont donc les h unitaires de R vérifiant $\Theta^n(h) \cdot h^\natural = X^n - 1$. Comme on suppose que l'ordre de θ divise n, $\Theta^n(h) = h$. Ainsi les codes auto-duaux θ-cycliques de longueur n sont caractérisés par l'« équation auto-duale tordue » :

$$h^\natural \cdot h = h \cdot h^\natural = X^n - 1.$$

Pour simplifier la présentation, on suppose que $q = p^m$ où p est premier et m est un entier non nul et que θ est l'automorphisme de Frobenius $x \mapsto x^p$ d'ordre m. On s'intéresse aux codes auto-duaux θ-cycliques de longueur n.

Exemple 3. *On considère ici les codes θ-cycliques auto-duaux de longueur 4 et 10 sur $\mathbb{F}_4 = \mathbb{F}_2(a)$ avec $a^2 + a + 1 = 0$ et $\theta : x \mapsto x^2$.*

Les factorisations de $X^4 - 1$ en produits de deux polynômes tordus de degré 2 sont au nombre de 7 (exemple 1). Il y a trois polynômes tordus unitaires vérifiant l'équation auto-duale tordue :

$$\begin{aligned} X^4 - 1 &= (X^2 + 1) \cdot (X^2 + 1) \\ &= (X^2 + aX + a^2) \cdot (X^2 + aX + a) \\ &= (X^2 + a^2X + a) \cdot (X^2 + a^2X + a^2). \end{aligned}$$

Les codes θ-cycliques auto-duaux de longueur 4 sont engendrés par $X^2 + 1$, $X^2 + aX + a$ et $X^2 + a^2X + a^2$. Par exemple, soit $h = X^2 + aX + a$, on a $h^* = 1 + X \cdot a + X^2 \cdot a = 1 + a^2X + aX^2$ donc $h^\natural = X^2 + aX + a^2$.

Le polynôme $X^{10} - 1$ possède 51 factorisations en produits de deux polynômes unitaires tordus de degrés 5. Parmi ces 51 facteurs à droite, 5 sont solutions de l'équation auto-duale tordue :

$$\begin{aligned} X^{10} - 1 &= (X^5 + 1) \cdot (X^5 + 1) \\ &= (X^5 + X^4 + a^2X^3 + a^2X^2 + X + 1) \cdot (X^5 + X^4 + a^2X^3 + aX^2 + X + 1) \\ &= (X^5 + X^4 + aX^3 + aX^2 + X + 1) \cdot (X^5 + X^4 + aX^3 + a^2X^2 + X + 1) \\ &= (X^5 + aX^4 + aX^3 + aX^2 + aX + 1) \cdot (X^5 + a^2X^4 + aX^3 + a^2X^2 + aX + 1) \\ &= (X^5 + a^2X^4 + a^2X^3 + a^2X^2 + a^2X + 1) \cdot (X^5 + aX^4 + a^2X^3 + aX^2 + a^2X + 1) \end{aligned}$$

On obtient cinq codes θ-cycliques auto-duaux $[10, 5]_4$.

Exemple 4. *Considérons les codes θ-cycliques auto-duaux de longueur 2 sur $\mathbb{F}_{p^2}$. L'équation auto-duale tordue s'écrit*

$$\underbrace{(X + 1/\theta(\alpha))}_{h^\natural} \cdot \underbrace{(X + \alpha)}_{h} = X^2 - 1 \Leftrightarrow \alpha^2 = -1 \text{ et } \alpha^{p-1} = -1.$$

On a quatre cas :

- *$p = 2$: une solution $X + 1$*
- *$p \equiv 3 \pmod 4$ et m pair : deux solutions $X + \alpha, \alpha^2 = -1$*
- *$p \equiv 3 \pmod 4$ et m impair : aucune solution*
- *$p \equiv 1 \pmod 4$: aucune solution.*

Pour construire les codes θ-cycliques auto-duaux de dimension k donnée, on résout le système polynomial vérifié par les coefficients inconnus de h solutions de $h^\natural \cdot h = X^n - 1$ ([BU09b]). Les calculs ont été effectués en MAGMA. Les résultats obtenus sur $\mathbb{F}_4$ en longueur inférieure ou égale à 50 et sur $\mathbb{F}_9$ en longueur inférieure ou égale à 30 sont résumés dans les deux tableaux 2.1 et 2.2. Il n'y a pas de code θ-cyclique auto-dual sur $\mathbb{F}_{25}$ de longueur inférieure ou égale à 30.

En observant ces résultats, on a pu émettre les conjectures suivantes :

- Sur $\mathbb{F}_{p^2}$, avec p impair, il existe un code auto-dual de dimension k si, et seulement si, $p^k \equiv 3 \pmod 4$.
- Sur $\mathbb{F}_4$ il y a 3 codes auto-duaux θ-cycliques de dimension 2^s.

longueur	nbr cyc.	meilleure dist. cyc.	nbr θ-cyc.	meilleure dist. θ-cyc.	meilleure dist. connue
4	1	2	3	3	3
6	3	3	3	3	3
8	**1**	**2**	**3**	**4**	4
10	1	2	5	4	4
12	5	4	21	6	6
14	3	4	11	6	6
16	**1**	**2**	**3**	**4**	6
18	9	4	27	6	6
20	1	2	63	8	8
22	3	6	33	8	8
24	9	4	93	7	8
26	1	2	65	8	8
28	5	4	279	9	9
30	27	6	285	10	10
32	**1**	**2**	**3**	**4**	10
34	1	2	289	10	10
36	25	6	1 533	11	11
38	3	8	513	11	11
40	1	2	1 023	12	12
42	81	10	2 211	12	12
44	5	6	3 171	14	14
46	3	8	2 051	14	14
48	17	4	1 533	12	14
50	1	2	5 125	14	14

TABLE 2.1 – Codes θ-cycliques auto-duaux sur $\mathbb{F}_4$ de longueur ≤ 50

longueur	nbr θ-cyc.	meilleure dist. θ-cyc.	meilleure dist. connue
4	0		3
6	**8**	**4**	4
8	0		5
10	20	5	6
12	0		6
14	56	6	6
16	0		8
18	**242**	**8**	8
20	0		10
22	492	9	9
24	0		10
26	1800	10	10
28	0		12
30	6560	11	12

TABLE 2.2 – Codes θ-cycliques auto-duaux sur $\mathbb{F}_9$ de longueur ≤ 30

2 CNS d'existence des solutions à l'équation auto-duale tordue

Les observations précédentes nous ont amené à conjecturer que sur $\mathbb{F}_{p^2}$ avec p premier impair, les codes θ-cycliques auto-duaux de longueur $2k$ existent si et seulement si $p \equiv 3 \pmod 4$ et $k \equiv 1 \pmod 2$. Remarquons qu'il existe un code θ-cyclique auto-dual en toute dimension k sur $\mathbb{F}_4$ puisque $h = X^k + 1$ vérifie l'équation $h^\natural \cdot h = X^{2k} + 1$ dans $\mathbb{F}_4[X;\theta]$. Dans ce qui suit, on se place sur $\mathbb{F}_{p^m}$ avec p premier impair et $m \geq 2$. Pour simplifier la présentation, on suppose que θ est l'automorphisme de Frobenius $x \mapsto x^p$ (voir tableau 2.4 pour θ puissance du Frobenius).

2.1 CNS d'existence de solutions binomiales tordues

La motivation pour commencer à étudier les solutions binomiales fut double. Tout d'abord, les binômes sont plus simples ! (un seul coefficient à gérer). Ensuite il n'existe pas de code cyclique auto-dual engendré par un binomial en caractéristique impaire ($(X^k+1/\alpha)(X^k+\alpha) \neq X^{2k}-1$). On peut se demander ce qu'il en est quand θ n'est pas trivial ($\theta \neq id$).

Proposition 3 (Proposition 1 de [Bou15])**.** *Soit p un nombre premier impair, soit $q = p^m$ et soit θ l'automorphisme de Frobenius sur $\mathbb{F}_q$. Il existe un code θ-cyclique de dimension k sur $\mathbb{F}_q$ engendré par un* binomial *tordu si, et seulement si,*

$$p \equiv 3 \pmod 4, k \equiv 1 \pmod 2, m \equiv 0 \pmod 2.$$

Démonstration. Considérons p impair et soit $h = X^k + \alpha$ dans R avec $\alpha \neq 0$. Alors $h^\natural = X^k + \frac{1}{\theta^k(\alpha)}$.

$$\begin{aligned}
h^\natural \cdot h &= \left(X^k + \frac{1}{\theta^k(\alpha)}\right) \cdot \left(X^k + \alpha\right) \\
&= X^{2k} + X^k \cdot \alpha + \frac{1}{\theta^k(\alpha)} X^k + \frac{\alpha}{\theta^k(\alpha)} \\
&= X^{2k} + \left(\theta^k(\alpha) + \frac{1}{\theta^k(\alpha)}\right) X^k + \frac{\alpha}{\theta^k(\alpha)} \\
h^\natural \cdot h = X^{2k} - 1 &\Leftrightarrow \theta^k(\alpha) + \frac{1}{\theta^k(\alpha)} = 0 \text{ et } \frac{\alpha}{\theta^k(\alpha)} = -1 \\
&\Leftrightarrow \alpha + \frac{1}{\alpha} = 0 \text{ et } 1 = -\theta^k(\alpha)/\alpha \\
&\Leftrightarrow \alpha^2 = -1 \text{ et } 1 = -\alpha^{p^k - 1} \\
&\Leftrightarrow \alpha^2 = -1 \text{ et } 1 = (-1)^{\frac{p^k+1}{2}} \\
&\Leftrightarrow \alpha^2 = -1, p^k \equiv 3 \pmod 4.
\end{aligned}$$

En conclusion, il existe un code θ-cyclique engendré par un binomial de degré k si et seulement si $p^k \equiv 3 \pmod 4$ et -1 est un carré dans $\mathbb{F}_{p^m}$, c'est à dire

$$p \equiv 3 \pmod 4, k \equiv 1 \pmod 2, m \equiv 0 \pmod 2.$$

□

2.2 CNS d'existence de solutions polynomiales tordues

Dans ce qui suit on s'intéresse à savoir si les conditions suffisantes d'existence de solutions à l'équation auto-duale tordue sont aussi nécessaires. Pour cela, on va fortement s'inspirer de travaux antérieurs :

— sur les codes cycliques auto-duaux : Sloane, Thompson, 1983 ([ST83]) ;

— sur la factorisation des polynômes tordus : Giesbrecht, 1998 ([Gie98]).

Tout d'abord, on rappelle le cas des codes cycliques auto-duaux (Théorème 4) en proposant une preuve que l'on adaptera ensuite rapidement au cas tordu.

Théorème 4 ([ST83], [JLX11])**.** *Soit p un nombre premier, soit s dans $\mathbb{N}$ tel que p^{s+1} divise exactement $n = 2k$ ($p^{s+2} \not| n$) et soit $T(n)$ le nombre de polynômes $f = g \times g^\natural$ tels que $g^\natural \neq g$ soit irréductible et divise $X^n - 1$ dans $\mathbb{F}_{p^m}[X]$. Le nombre de codes cycliques auto-duaux de longueur $n = 2k$ sur $\mathbb{F}_{p^m}$ est*

$$\begin{cases} (2^{s+1}+1)^{T(n)} & \text{si } p = 2 \\ 0 & \text{si } p \text{ impair.} \end{cases}$$

Démonstration. Soit s l'entier tel que p^{s+1} divise $2k$ et p^{s+2} ne divise pas $2k$. Comme $(X^{2k} - 1)^\natural = X^{2k} - 1$, le polynôme $X^{2k} - 1$ se factorise sur $\mathbb{F}_{p^m}[X]$ en un produit de polynômes

$f_i(X)^{p^{s+1}}$ premiers entre eux deux à deux avec $f_i = f_i^\natural$ irréductible ou produit de deux irréductibles distincts et réciproques :

$$X^{2k}-1 = \prod_{f_i=f_i^\natural,\ f_i\ irr} f_i(X)^{p^{s+1}} \prod_{f_i=g_ig_i^\natural, g_i\neq g_i^\natural\ irr} f_i(X)^{p^{s+1}} \in \mathbb{F}_{p^m}[X].$$

Les codes θ-cycliques auto-duaux de longueur $2k$ sont les codes cycliques de polynômes de contrôle h vérifiant

$$h^\natural h = X^{2k}-1 \quad \Leftrightarrow \quad \begin{array}{l} h = \prod h_i = \mathrm{ppcm}(h_i) \\ h_i^\natural \cdot h_i = f_i(X)^{p^{s+1}} \end{array}$$

donc le nombre de codes cycliques auto-duaux de longueur n est $\prod_{f_i} \#\mathcal{H}_i$ où $\mathcal{H}_i$ est l'ensemble des polynômes unitaires h_i de $\mathbb{F}_{p^m}[X]$ tels que $h_i^\natural h_i = f_i(X)^{p^{s+1}}$. Or

$$h_i^\natural h_i = f_i(X)^{p^{s+1}} \quad \Leftrightarrow \quad \begin{array}{lll} h_i = f_i(X)^{2^s} & \text{si} & f_i = f_i^\natural \text{ irréductible et } p=2 \\ h_i = g_i(X)^{\beta_i}(g_i^\natural(X))^{p^{s+1}-\beta_i} & \text{si} & f_i = g_ig_i^\natural \end{array}$$

donc

$$\#\mathcal{H}_i = \begin{cases} 1 & \text{si } p=2 \text{ et } f_i = f_i^\natural \text{ irréductible} \\ 0 & \text{si } p \text{ impair et } f_i = f_i^\natural \text{ irréductible} \\ 1+p^{s+1} & \text{si } f_i = f_i^\natural \text{ produit de deux irréductibles.} \end{cases}$$

De plus $f = X-1$ est un polynôme autoréciproque ($f = f^\natural$) irréductible divisant X^n-1, donc l'ensemble $\{f \in \mathbb{F}_{p^m}[X] \mid f = f^\natural, f \text{ irr}, f | X^{2k}-1\}$ est non vide, donc p est égal à 2. □

Exemple 5. *Considérons les codes $[10,5]_4$ auto-duaux. Le polynôme $X^{10}-1$ se factorise comme suit*

$$X^{10}-1 = (X^5-1)^2 = \underbrace{(X-1)^2}_{f=f^\natural, irr} \times \underbrace{(X^2+aX+1)^2}_{f=f^\natural, irr} \times \underbrace{(X^2+a^2X+1)^2}_{f=f^\natural, irr}$$

donc il y a un seul code cyclique auto-dual, il est engendré par X^5+1.

En s'inspirant du théorème 4 et de sa preuve et en utilisant la factorisation de X^n-1 sur $\mathbb{F}_p[X^m]$ (centre de R), on obtient le résultat suivant.

Proposition 4 (Proposition 28 de [BU14b], proposition 2 de [Bou15])**.** *Soit p un nombre premier, soit m un entier et soit $R = \mathbb{F}_{p^m}[X;\theta]$ avec $\theta : x \mapsto x^p$. On suppose $n = 2k = m \times p^s \times t$, $p \nmid t$ et on considère la factorisation suivante de $X^{2k}-1$ sur $\mathbb{F}_p[X^m]$:*

$$X^{2k}-1 = ((X^m)^t-1)^{p^s} = \prod_{f_i=f_i^\natural,\ f_i\ irr} f_i(X^m)^{p^s} \prod_{f_i=g_ig_i^\natural, g_i\neq g_i^\natural\ irr} f_i(X^m)^{p^s} \in \mathbb{F}_p[X^m].$$

On a

$$h^\natural \cdot h = X^{2k}-1 \in R \quad \Leftrightarrow \quad \begin{array}{l} h = \mathrm{lcrm}(h_i) \\ h_i^\natural \cdot h_i = f_i(X^m)^{p^s} \in R. \end{array}$$

Démonstration. On utilise la décomposition $h = \mathrm{lcrm}(h_i)$ avec $h_i = \mathrm{gcld}(h, f_i(X^m)^{p^s})$ (d'après Théorème 4.1 de [Gie98] ou théorème 2).

□

Dimension	$\mathbb{F}_2$	$\mathbb{F}_4$	$\mathbb{F}_8$	$\mathbb{F}_{16}$
2^s	1	1	1	1
$2^s \times 3$	1	$1 + 2^{s+1}$	1	$1 + 2^{s+1}$
$2^s \times 5$	1	1	1	$(1 + 2^{s+1})^2$
$2^s \times 7$	$1 + 2^{s+1}$	$1 + 2^{s+1}$	$(1 + 2^{s+1})^3$	$1 + 2^{s+1}$
$2^s \times 9$	1	$(1 + 2^{s+1})^2$	1	$(1 + 2^{s+1})^2$
$\dots$				

TABLE 2.3 – Nombres de codes cycliques auto-duaux sur $\mathbb{F}_2$, $\mathbb{F}_4$, $\mathbb{F}_8$ et $\mathbb{F}_{16}$.

Comme $X^m - 1$ divise $X^{2k} - 1$, s'il existe un code θ-cyclique auto-dual de dimension k alors, d'après la proposition 4, il existe H unitaire dans R tel que $H^\natural \cdot H = (X^m - 1)^{p^s}$. On note $H = X^K + \cdots + \alpha$ avec $\alpha \neq 0$ un tel polynôme.

Comme $m \times p^s = 2\deg(H) = 2K$, m est nécessairement pair.

De plus le coefficient constant de $H^\natural \cdot H$ est égal à $\frac{\alpha}{\theta^K(\alpha)} = -1$.

Utilisons maintenant des propriétés de factorisation des polynômes tordus. Comme $X^m - 1$ est un polynôme de degré 1 (irréductible) dans $\mathbb{F}_p[X^m]$ et comme H divise $(X^m - 1)^{p^s}$, H se factorise en produit de facteurs linéaires divisant $X^m - 1$:

$$H = (X + \alpha_1) \cdots (X + \alpha_K)$$

où $X + \alpha_i$ divise $X^{2K} - 1$ à droite pour tout i dans $\{1, \dots, K\}$.

Comme $X + \alpha_i$ divise $X^{2K} - 1$ pour tout i dans $\{1, \dots, K\}$, on a $N_{2K}(\alpha_i) = N_{2K}(-\alpha_i) = 1$ où

$$\forall j \in \mathbb{N}, N_j(x) := \theta^{j-1}(x) \cdots \theta(x)x$$

(voir le lemme 6 et la remarque 2 par ailleurs) donc

$$N_{2K}(\alpha) = \prod_{i=1}^{K} N_{2K}(\alpha_i) = 1.$$

Comme $\theta^K(\alpha) = -\alpha$ et $N_{2K}(\alpha) = 1$, on a
$N_K(\alpha)^2 = (-1)^K N_K(-\alpha) N_K(\alpha) = (-1)^K N_K(\theta^K(\alpha)) N_K(\alpha) = (-1)^K N_{2K}(\alpha) = (-1)^K$.
De plus $N_K(\alpha)^{p-1} = \frac{\theta(N_K(\alpha))}{N_K(\alpha)} = \frac{\theta^K(\alpha)}{\alpha} = -1$.
Ainsi $(-1)^{K\frac{p-1}{2}} = -1$ c'est à dire $(-1)^{\frac{m}{2}\frac{p-1}{2}p^s} = -1$ soit $(-1)^{p^{\frac{m}{2}}} = 1$.
On en déduit $p \equiv 3 \pmod 4$ et $\frac{m}{2} \equiv 1 \pmod 2$.

	θ-cyclique auto-dual	θ-negacyclique auto-dual
$q \equiv 1 \pmod 4$, $p \equiv 3 \pmod 4$	$r \times k \equiv 1 \pmod 2$	$r \times k \equiv 0 \pmod 2$
$q \equiv 1 \pmod 4$, $p \equiv 1 \pmod 4$	$\emptyset$	$k \in \mathbb{N}^*$
$q \equiv 3 \pmod 4$	$\emptyset$	$k \equiv 0 \pmod{2^{\mu-1}}$

TABLE 2.4 – Conditions nécessaires et suffisantes pour l'existence de codes θ-cycliques et θ-negacycliques auto-duaux de dimension k sur $\mathbb{F}_q$ où $\mathbb{F}_q$ est de caractéristique impaire p, $\mu \in \mathbb{N}$ est tel que 2^μ divise exactement $p+1$ et $\theta : x \mapsto x^{p^r}$.

Proposition 5 (Proposition 5 de [Bou15])**.** *Soit p un nombre premier impair, soient m et k des entiers. Il existe un code θ-cyclique de dimension k si, et seulement si,*

$$p \equiv 3 \pmod 4, k \equiv 1 \pmod 2, m \equiv 0 \pmod 2. \tag{2.1}$$

Démonstration. Si les conditions (2.1) sont réalisées, d'après la proposition 3, il existe une solution binomiale.
Réciproquement, s'il existe un code θ-cyclique auto-dual de dimension k alors, d'après la proposition 4, il existe H dans R tel que $H^\natural \cdot H = (X^m-1)^{p^s}$ (car X^m-1 divise $X^{2k}-1$). D'après ce qui précède on a nécessairement $p \equiv 3 \pmod 4$ et $\frac{m}{2} \equiv 1 \pmod 2$. De plus X^m+1 ne divise pas $X^{2k}-1$, sinon, d'après la proposition 4, l'équation $H^\natural \cdot H = (X^m+1)^{p^s}$ aurait aussi une solution et on aurait $(-1)^{p^{\frac{m}{2}}} = -1$. Ainsi, $\frac{2k}{m}$ est impair et comme $m/2$ est impair, k est impair. □

Pour terminer, en suivant les mêmes idées que précédemment, on obtient des conditions nécessaires et suffisantes d'existence de codes auto-duaux θ-cycliques et θ-négacycliques lorsque θ est un automorphisme quelconque de $\mathbb{F}_q$. Le tableau 2.4 résume les résultats.

3 Construction et énumération sur $\mathbb{F}_{p^2}$ en dimension p^s

La motivation initiale de la construction qui va suivre provient de la conjecture précédemment établie : il y a trois codes auto-duaux θ-cycliques de dimension 2^s sur $\mathbb{F}_4$ pour tout entier s non nul.

On se place ici sur $\mathbb{F}_{p^2}$ et on considère les codes auto-duaux θ-cycliques de dimension p^s. Rappelons que ceux-ci sont caractérisés par l'équation auto-duale tordue :

$$h^\natural \cdot h = (X^2-1)^{p^s}$$

où h est le polynôme de contrôle tordu unitaire.

Comme X^2-1 est central de degré 1 en X^2, le polynôme h est un produit de facteurs linéaires (divisant X^2-1).

Exemple 6. *Plaçons nous sur* $\mathbb{F}_4 = \mathbb{F}_2(a)$ *avec* $\theta : x \mapsto x^2$.
On a

$$\begin{aligned} X^4 - 1 &= \underbrace{(X^2 + aX + a^2)}_{h^\natural} \cdot \underbrace{(X^2 + aX + a)}_{h} \\ || & \\ (X^2+1)^2 &= \underbrace{(X + a^2) \cdot (X + 1)}_{\text{fact unique de } h^\natural} \cdot \underbrace{(X + 1) \cdot (X + a)}_{\text{fact unique de } h} \end{aligned}$$

Dans l'exemple précédent, on a pu remarquer que h possède une factorisation unique en produit de facteurs linéaires unitaires tordus. On établit ci-dessous un critère d'unicité d'une telle factorisation, que l'on utilisera ensuite pour la construction et l'énumération des solutions de $h^\natural \cdot h = (X^2 - 1)^{p^s}$.

Lemme 4 (Proposition 16 de [BU14b] ou corollaire 1 de [Bou16])**.** *Soit p un nombre premier, soit $\theta : x \mapsto x^p$ l'automorphisme de Frobenius sur $\mathbb{F}_{p^2}$ et soit $R = \mathbb{F}_{p^2}[X; \theta]$. Soit $h = (X+\alpha_1) \cdots (X+\alpha_k)$ dans R où pour tout i dans $\{1, \ldots, k\}$, α_i est dans $\mathbb{F}_q$ et vérifie $\alpha_i^{p+1} = 1$. Les assertions suivantes sont équivalentes :*

1. *La factorisation de h en produit de facteurs linéaires unitaires est unique.*
2. *$X^2 - 1$ ne divise pas h.*
3. *$\forall i \in \{1, \ldots, k-1\}, (X + \alpha_i) \cdot (X + \alpha_{i+1}) \neq X^2 - 1$.*

Démonstration. Démontrons (3) $\Rightarrow$ (1) pour $k = 2$. Soit $h = (X + \alpha_1) \cdot (X + \alpha_2)$ où $X + \alpha_1$ et $X + \alpha_2$ divisent à droite $X^2 - 1$. Supposons qu'il existe $\beta_2 \neq \alpha_2$ tel que $X + \beta_2$ divise h à droite. Considérons H le ppcm à gauche de $X + \alpha_2$ et $X + \beta_2$. Alors $\deg(H) = 2$ et H divise $X^2 - 1$, donc $H = X^2 - 1$, donc $h = X^2 - 1$. □

Le principe de la résolution de l'équation $h^\natural \cdot h = (X^2 - 1)^{p^s}$ va reposer sur un partitionnement de l'ensemble des solutions en solutions de la forme $(X^2 - 1)^i \cdot H$ où H n'est pas divisible par $X^2 - 1$, puis sur l'application du lemme 4 à H.

On va donc s'intéresser dans un premier temps à la résolution d'équation du type $h^\natural \cdot h = (X^2 - 1)^k$ où $X^2 - 1$ ne divise pas h. On va utiliser pour cela le lemme 4. Comme h divise $(X^2 - 1)^k$, h est un produit de facteurs linéaires divisant $X^2 - 1$. On a donc

$$h = (X + \alpha_1) \cdots (X + \alpha_k), \text{ avec } \forall i \in \{1, \ldots, k-1\}, \alpha_i^{p+1} = 1.$$

De plus, comme $X^2 - 1$ ne divise pas h, d'après le lemme 4, on a, pour tout i dans $\{1, \ldots, k-1\}, (X + \alpha_i) \cdot (X + \alpha_{i+1}) \neq X^2 - 1$ donc

$$\forall i \in \{1, \ldots, k-1\}, \alpha_i \alpha_{i+1} \neq -1.$$

Par un raisonnement par récurrence, on obtient

$$h^\natural = (X + \tilde{\alpha_k}) \cdots (X + \tilde{\alpha_1})$$

avec

$$\tilde{\alpha_i} = \begin{cases} \alpha_i(\alpha_1 \cdots \alpha_{i-1})^2 & \text{si} \quad i \equiv 1 \pmod 2 \\ \frac{1}{\alpha_i(\alpha_1 \cdots \alpha_{i-1})^2} & \text{si} \quad i \equiv 0 \pmod 2. \end{cases}$$

On a

$$\underbrace{(X+\tilde{\alpha_k})\cdots(X+\tilde{\alpha_1})}_{\text{fact unique}}\cdot\underbrace{(X+\alpha_1)\cdots(X+\alpha_k)}_{\text{fact unique}}=\underbrace{(X^2-1)^k}_{\text{fact non unique}}\quad.$$

D'après le lemme 4, on a nécessairement, $(X+\tilde{\alpha_1})\cdot(X+\alpha_1)=X^2-1$, c'est à dire $\alpha_1\tilde{\alpha_1}=-1$. Comme X^2-1 est dans le centre de R, on peut « simplifier » par X^2-1 et on en déduit :

$$\underbrace{(X+\tilde{\alpha_k})\cdots(X+\tilde{\alpha_2})}_{\text{fact unique}}\cdot\underbrace{(X+\alpha_2)\cdots(X+\alpha_k)}_{\text{fact unique}}=\underbrace{(X^2-1)^{k-1}}_{\text{fact non unique}}$$

puis on réitère le processus : $(X+\tilde{\alpha_2})\cdot(X+\alpha_2)=X^2-1$, ... On obtient, pour tout i dans $\{1,\ldots,k\}$, $\alpha_i\tilde{\alpha_i}=-1$. En combinant les k conditions ainsi obtenues, on a $\alpha_1^2=-1$ et $\alpha_i\alpha_{i+1}=1$ si i est pair. Ainsi,

$$\begin{array}{c} h^\natural\cdot h=(X^2-1)^k, X^2-1\not| h \\ \Updownarrow \\ h=(X+\alpha_1)\cdot(X+\alpha_2)\cdots(X+\alpha_k)\end{array}$$

avec

$$\begin{cases}\alpha_i^{p+1}=1\\ \alpha_i\alpha_{i+1}\neq -1\\ \alpha_1^2=-1\\ \alpha_i\alpha_{i+1}=1 \text{ si } i \text{ pair.}\end{cases}$$

Si $p=2$, on a les trois possibilités suivantes : si $k>2$, aucune solution ; si $k=2$, deux solutions, $(X+\alpha_1)\cdot(X+\alpha_2)$ avec $\alpha_1^3=\alpha_2^3=1$ et $\alpha_1\alpha_2\neq 1$; si $k=1$, une solution.

Si $p\equiv 3 \pmod 4$, on a $2p^{\lfloor (k-1)/2\rfloor}$ solutions et si $p\equiv 1 \pmod 4$, il n'y a pas de solution.

Proposition 6 (Proposition 4 de [Bou16])**.** *Soit p un nombre premier et soit s un entier non nul. Le nombre de codes θ-cycliques auto-duaux de dimension p^s sur $\mathbb{F}_{p^2}$ est :*

$$\begin{cases} 3 & si \quad p=2\\ 2\dfrac{p^{(p^s+1)/2}-1}{p-1} & si \quad p\equiv 3 \pmod 4\\ 0 & si \quad p\equiv 1 \pmod 4.\end{cases}$$

Démonstration. Soit h unitaire dans R. On a

$$h^\natural\cdot h=(X^2-1)^{p^s}\Leftrightarrow\exists i\in\{0,\ldots,\lfloor\frac{p^s}{2}\rfloor\}, h=(X^2-1)^i\cdot H, X^2-1\not| H, H^\natural\cdot H=(X^2-1)^{p^s-2i}.$$

Supposons $p=2$, alors l'équation

$$H^\natural\cdot H=(X^2-1)^{p^s-2i}, X^2-1\not| H \tag{2.2}$$

n'a pas de solution si $i<2^{s-1}-1$, deux solutions si $i=2^{s-1}-1$ et une solution si $i=2^{s-1}$.

Si $p \equiv 1 \pmod 4$, l'équation (2.2) n'a pas de solution. Si $p \equiv 3 \pmod 4$, l'équation (2.2) a $2p^{(p^s-1-2i)/2}$ solutions. On obtient donc

$$\sum_{i=0}^{(p^s-1)/2} 2p^{(p^s-1-2i)/2} = 2\frac{p^{(p^s+1)/2}-1}{p-1}$$

codes θ-cycliques auto-duaux de dimension p^s si $p \equiv 3 \pmod 4$. □

Bilan Dans le cas où $p = 2$ on obtient bien trois codes (voir tableau 2.1 par ailleurs). Dans le cas où $p = 3$, on en obtient $3^{(3^s+1)/2} - 1$. Pour $s = 1, 2$ on retrouve 8 et 242 codes sur $\mathbb{F}_9$ comme annoncé dans le tableau 2.2. Par ailleurs, l'énumération des codes auto-duaux θ-cycliques en dimension p^s est accompagnée d'une construction basée sur des multiplications de polynômes unitaires linéaires.

4 Construction et énumération sur $\mathbb{F}_{p^2}$ en dimension non divisible par p.

Arrivé à ce stade, on a démontré les deux conjectures annoncées (cns d'existence des codes auto-duaux θ-cycliques et comptage de ces codes en dimension p^s). Ces démonstrations ont permis de mettre en lumière une construction des codes auto-duaux tordus qui évite la résolution de systèmes polynomiaux d'une part et le calcul de tous les facteurs de degré k de $X^{2k}-1$ dans R d'autre part. Un nouveau double objectif se présenta alors, d'une part justifier tous les nombres de codes auto-duaux obtenus dans les tableaux 2.1 et 2.2 ; d'autre part fournir une nouvelle construction des codes auto-duaux en toute dimension. On s'intéresse ici au cas où p ne divise pas la dimension du code. D'après la proposition 4, les solutions h de l'équation auto-duale $h^\natural \cdot h = X^{2k} - 1$ sont obtenues comme ppcm à droite de polynômes tordus vérifiant des équations intermédiaires :

$$\begin{aligned} h^\natural \cdot h = X^{2k} - 1 \in R \quad \Leftrightarrow \quad & h = \mathrm{lcrm}(h_i) \\ & h_i^\natural \cdot h_i = f_i(X^2) \in R \end{aligned}$$

où les polynômes $f_i(X^2) \in \mathbb{F}_p[X^2]$ sont définis par :

$$X^{2k} - 1 = \prod_{f_i = f_i^\natural,\ f_i \ irr} f_i(X^2) \prod_{f_i = g_i g_i^\natural, g_i \neq g_i^\natural \ irr} f_i(X^2) \in \mathbb{F}_p[X^2].$$

Dans ce qui suit, on s'intéresse aux équations intermédiaires $h^\natural \cdot h = f(X^2)$ où $f(X^2)$ est un polynôme de $\mathbb{F}_p[X^2]$ auto-réciproque vérifiant l'une des conditions suivantes :

- irréductible de degré 1 :
- irréductible de degré $d > 1$ (nécessairement pair) ;
- produit de deux irréductibles distincts (qui sont réciproques l'un de l'autre).

• Si f est irréductible de degré 1 dans $\mathbb{F}_p[X^2]$ et autoréciproque alors $f = X^2 - \epsilon$ où $\epsilon^2 = 1$. On peut alors généraliser les calculs de l'exemple 4 :

$$\underbrace{(X+1/\theta(\alpha))}_{h^\natural}\cdot\underbrace{(X+\alpha)}_{h} = X^2-\epsilon \Leftrightarrow \alpha^2=-1 \text{ et } \alpha^{p-1}=-\epsilon.$$

On a trois cas :
— $p=2$: une solution $X+1$;
— $p\equiv -\epsilon \pmod 4$: deux solutions $X+\alpha, \alpha^2=-1$;
— $p\equiv \epsilon \pmod 4$: aucune solution.

• Focalisons-nous maintenant sur l'équation $h^\natural \cdot h = f(X^2)$ d'inconnue h avec $f=f^\natural$ irréductible de degré $d>1$, nécessairement pair.

L'idée est de partir d'une paramétrisation des irréductibles divisant $f(X^2)$. D'après [Odo99], si f est irréductible de degré d dans $\mathbb{F}_p[X^2]$, on a un isomorphisme d'anneaux

$$\mathbb{F}_{p^2}[X;\theta]/(f) \sim \mathcal{M}_2(\mathbb{F}_{p^d}).$$

Les irréductibles unitaires $h(X)$ de $\mathbb{F}_{p^2}[X;\theta]$ divisant $f(X^2)$ sont en correspondance bijective avec les idéaux à gauche maximaux dans $\mathcal{M}_2(\mathbb{F}_{p^d})$ et il y en a $\frac{p^{2d}-1}{p^d-1}=p^d+1$.

On peut résumer la répartition des irréductibles de $\mathbb{F}_{p^2}[X;\theta]$ de degré d par la figure 2.1.

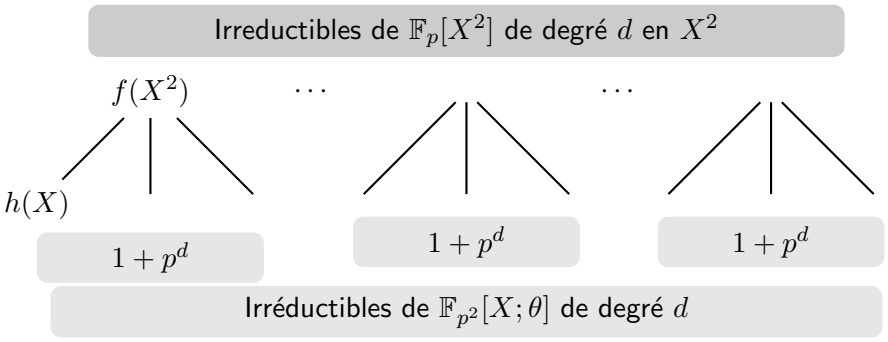

FIGURE 2.1 – Irréductibles unitaires de $\mathbb{F}_{p^2}[X;\theta]$ de degré d.

Dans ce qui suit, étant donné $f\in\mathbb{F}_p[X^2]$ irréductible de degré d en X^2, on construit tous ses diviseurs de degré d (nécessairement irréductibles) dans R. Pour simplifier on se placera dans le cas particulier où d est pair (ce qui est vérifié lorsque $f=f^\natural$). Le descriptif complet est donné en Annexe A de [Bou18].

Proposition 7 (Lemme 3.2 et lemme A1 de [Bou18])**.** *Soit p un nombre premier, soit θ l'automorphisme de Frobenius sur $\mathbb{F}_{p^2}$ et soit $R=\mathbb{F}_{p^2}[X;\theta]$. Soit $f(X^2)\in\mathbb{F}_p[X^2]$ irréductible unitaire de degré d pair en X^2 et soit $h=A(X^2)+X\cdot B(X^2)$ dans R de degré d en X et unitaire. Soit α dans $\mathbb{F}_{p^d}$ tel que $f(\alpha)=0$. Le polynôme tordu h est un facteur irréductible de $f(X^2)$ si et seulement si l'une des deux situations qui suivent se produit :*
— *$B=0$ et $A(X^2)$ diviseur de $f(X^2)$ dans $\mathbb{F}_{p^2}[X^2]$ de degré $d/2$ en X^2*
— *$B\neq 0$ et (A,B) solution du problème d'interpolation de Cauchy*

$$\frac{A}{B}\equiv P_u \pmod f \in \mathbb{F}_{p^2}(X)$$

où $P_u \in \mathbb{F}_{p^2}[X]$ est de degré $\leq d-1$ et défini par $P_u(\alpha) = u, P_u(\alpha^p) = \alpha^p/u^p$ et $u \in \mathbb{F}_{p^d} \setminus \{0\}$.

Démonstration. Le polynôme tordu $h = A(X^2) + X \cdot B(X^2)$ de degré d est un diviseur de $f(X^2)$ si et seulement si

$$A(\alpha)\Theta(A)(\alpha) - \alpha B(\alpha)\Theta(B)(\alpha) = 0$$

ce qui se traduit par $\frac{A}{B} \equiv P \pmod f$ où $P\Theta(P) \equiv X \pmod f$. Le polynôme P est déterminé par ses valeurs aux points α et α^p. Notons $u = P(\alpha) \in \mathbb{F}_{p^d}$. La relation $P\Theta(P) \equiv X \pmod f$ entraîne $P(\alpha^p) = \alpha^p/u^p$. De plus, comme $\alpha^{p^d} = \alpha$, on obtient $u^{p^d-1} = 1$. On vérifie que ces conditions nécessaires sont également suffisantes (voir le lemme 3.2 de [Bou18]).

□

La résolution se ramène à un problème d'interpolation de Cauchy dans $\mathbb{F}_{p^d}(X)$ (voir chapitre 5 de [vzGG13] ou chapitre 7 de [BCG+17]). En effet, on se donne ici 2δ points distincts $x_0, \ldots, x_{2\delta-1}$ dans $\mathbb{F}_{p^{2\delta}}$ et 2δ valeurs $y_0, \ldots, y_{2\delta-1}$ dans $\mathbb{F}_{p^{2\delta}}$ définis par

$$(x_i, y_i) = \begin{cases} (\theta^i(\alpha), \theta^i(u)) & \text{si} \quad i \equiv 0 \pmod 2 \\ (\theta^i(\alpha), \theta^i(\alpha/u)) & \text{si} \quad i \equiv 1 \pmod 2. \end{cases}$$

On recherche une fonction rationnelle A/B dans $\mathbb{F}_{p^{2\delta}}(X)$ telle que

$$B(x_i) \neq 0, \frac{A(x_i)}{B(x_i)} = y_i, i = 0, \ldots, 2\delta - 1, \deg(A) < \delta + 1, \deg(B) \leq \delta - 1$$

ce qui s'écrit encore

$$pgcd(B, f) = 1, A \equiv PB \pmod f, \deg(A) < \delta + 1, \deg(B) \leq \delta - 1$$

où $f = \prod_{i=0}^{2\delta-1}(X - x_i)$ et $P = P_u$ est le polynôme d'interpolation de degré $\leq 2\delta - 1$ aux points $(x_i, y_i), 1 \leq i < 2\delta - 1$.

L'avantage de cette construction est qu'elle permet de résoudre l'équation $h^\natural \cdot h = f(X^2)$ en restreignant l'espace des paramètres u :

Proposition 8 (Lemme 5 de [Bou16])**.** *Soit p un nombre premier, soit θ l'automorphisme de Frobenius sur $\mathbb{F}_{p^2}$ et soit $R = \mathbb{F}_{p^2}[X; \theta]$. Soit $f(X^2) = f^\natural(X^2) \in \mathbb{F}_p[X^2]$ irréductible unitaire de degré $d = 2\delta$ en X^2 et soit $h = A(X^2) + X \cdot B(X^2)$ unitaire dans R de degré d. Soit α dans $\mathbb{F}_{p^d}$ tel que $f(\alpha) = 0$.*

- *Si δ est impair, le polynôme tordu h vérifie $h^\natural \cdot h = f(X^2)$ si, et seulement si, l'une des deux situations se produit :*
  - *$B = 0$ et $A(X^2)$ diviseur de $f(X^2)$ dans $\mathbb{F}_{p^2}[X^2]$ de degré $d/2$ en X^2 ;*
  - *$B \neq 0$ et (A, B) solution du problème d'interpolation de Cauchy*

$$\frac{A}{B} \equiv P_u \pmod f \in \mathbb{F}_{p^2}(X)$$

où P_u est défini par $P_u(\alpha) = u, P_u(\alpha^p) = \alpha^p/u^p$ et $u \in \mathbb{F}_{p^d} \setminus \{0\}$ vérifie $u^{p^\delta - 1} = -\frac{1}{\alpha}$.

— *Si δ est pair, le polynôme tordu h vérifie $h^\natural \cdot h = f(X^2)$ si, et seulement si, $B \neq 0$ et (A, B) solution du problème d'interpolation de Cauchy*

$$\frac{A}{B} \equiv P_u \pmod{f} \in \mathbb{F}_{p^2}(X)$$

où P_u est défini par $P_u(\alpha) = u, P_u(\alpha^p) = \alpha^p/u^p$ et $u \in \mathbb{F}_{p^d} \setminus \{0\}$ vérifie $u^{p^\delta+1} = -1$.

Démonstration. On a ajouté la condition supplémentaire pour $P = P_u$ (quand $B \neq 0$) :

$$\alpha P(1/\alpha) + \Theta(P)(\alpha) = 0.$$

□

Corollaire 3 (Proposition 6 de [Bou16])**.** *Soit p un nombre premier, soit θ l'automorphisme de Frobenius sur $\mathbb{F}_{p^2}$ et soit $R = \mathbb{F}_{p^2}[X;\theta]$. Soit $f(X^2) = f^\natural(X^2) \in \mathbb{F}_p[X^2]$ irréductible unitaire de degré $d = 2\delta$ en X^2. Le nombre de polynômes tordus unitaires h vérifiant $h^\natural \cdot h = f(X^2)$ est égal à $1 + p^\delta$.*

Exemple 7. *Soit $f(X^2) = X^8+X^6+X^4+X^2+1 \in \mathbb{F}_2[X^2]$, soit $R = \mathbb{F}_4[X;\theta]$ avec $\mathbb{F}_4 = \mathbb{F}_2(a)$ et $\theta : x \mapsto x^2$. On a ici $d = 4$ et $\delta = 2$. Considérons $\mathbb{F}_{16} = \mathbb{F}_2(b)$ où $b^4+b+1 = 0$. Le polynôme tordu $h = A(X^2) + X \cdot B(X^2) \in R$ unitaire de degré 4 est un diviseur (nécessairement irréductilble) de $f(X^2)$ si et seulement si $B = 0$ et $A(X^2) \in \{X^4 + a^2\,X^2 + 1, X^4 + a\,X^2 + 1\}$ ou $B \neq 0$ et*

$$\frac{A(X)}{B(X)} \equiv P_u(X) \pmod{f(X)} \in \mathbb{F}_4(X) \text{ et } u \in \mathbb{F}_{16}^*.$$

De plus h vérifie $h^\natural \cdot h = f(X^2)$ si, et seulement si, $B \neq 0$ et $u^5 = 1$, soit $u \in \{1, b^3, b^6, b^9, b^{12}\}$ (en gras dans le tableau 2.5).

• Enfin il reste le cas où $f(X^2) = f^\natural(X^2) = f_{ir}(X^2)f_{ir}^\natural(X^2) \in \mathbb{F}_p[X^2]$ produit de deux irréductibles unitaires. La preuve du corollaire qui suit est une preuve un peu simplifiée de la preuve originale donnée dans [Bou16].

Corollaire 4 (Lemme 6 et proposition 7 de [Bou16])**.** *Soit p un nombre premier, soit θ l'automorphisme de Frobenius sur $\mathbb{F}_{p^2}$ et soit $R = \mathbb{F}_{p^2}[X;\theta]$. Soit $f(X^2) = f^\natural(X^2) = f_{ir}(X^2)f_{ir}^\natural(X^2) \in \mathbb{F}_p[X^2]$ produit de deux irréductibles unitaires de degré δ en X^2. Le nombre de polynômes tordus unitaires h dans R vérifiant $h^\natural \cdot h = f(X^2)$ est égal à $3 + p^\delta$.*

Démonstration. L'équation $h^\natural \cdot h = f(X^2)$ est équivalente à $h = \mathrm{lcrm}(h_1, h_2)$ où h_2 est déterminé de manière unique par $h_2^\natural \cdot h_1 = f_{ir}(X^2)$. Il s'agit donc de déterminer le nombre de diviseurs de $f_{ir}(X^2)$. Comme $f_{ir}(X^2)$ est irréductible dans $\mathbb{F}_p[X^2]$, il possède $1 + p^\delta$ facteurs unitaires de degré δ, deux diviseurs triviaux (1 et $f_ir(X^2)$), d'où le résultat. □

En conclusion, dans le cas où la dimension n'est pas divisible par p, on obtient donc le résultat suivant :

u	$P_u(X)$	$A(X)$	$B(X)$	$h = A(X^2) + X \cdot B(X^2)$
$\mathbf{1}$	$X^3 + a^2\,X + a$	$X^2 + a$	$a^2\,X + a^2$	$\mathbf{X^4 + a\,X^3 + a\,X + a}$
b	$a\,X^3 + a^2\,X^2 + X + 1$	$X^2 + 1$	$X + a^2$	$X^4 + X^3 + a\,X + 1$
b^2	$a^2\,X^3 + a\,X^2 + X + 1$	$X^2 + 1$	$X + a$	$X^4 + X^3 + a^2\,X + 1$
$\mathbf{b^3}$	$X^3 + a\,X + a^2$	$X^2 + a^2$	$a\,X + a$	$\mathbf{X^4 + a^2\,X^3 + a^2\,X + a^2}$
b^4	$a^2\,X^3$	$X^2 + X + 1$	$a\,X + a$	$X^4 + a^2\,X^3 + X^2 + a^2\,X + 1$
b^5	$a\,X^3 + X + a^2$	$X^2 + a$	$a\,X + a$	$X^4 + a^2\,X^3 + a^2\,X + a$
$\mathbf{b^6}$	$a^2\,X^3 + X^2 + a\,X + a$	$X^2 + 1$	$a^2\,X + a$	$\mathbf{X^4 + a\,X^3 + a^2\,X + 1}$
b^7	$X^3 + a^2\,X^2 + a\,X + a$	$X^2 + 1$	$a^2\,X + 1$	$X^4 + a\,X^3 + X + 1$
b^8	$a\,X^3 + a^2\,X + 1$	$X^2 + a^2$	$X + 1$	$X^4 + X^3 + X + a^2$
$\mathbf{b^9}$	X^3	$X^2 + X + 1$	$X + 1$	$\mathbf{X^4 + X^3 + X^2 + X + 1}$
b^{10}	$a^2\,X^3 + a\,X + 1$	$X^2 + a$	$X + 1$	$X^4 + X^3 + X + a$
b^{11}	$X^3 + a\,X^2 + a^2\,X + a^2$	$X^2 + 1$	$a\,X + 1$	$X^4 + a^2\,X^3 + X + 1$
$\mathbf{b^{12}}$	$a\,X^3 + X^2 + a^2\,X + a^2$	$X^2 + 1$	$a\,X + a^2$	$\mathbf{X^4 + a^2\,X^3 + a\,X + 1}$
b^{13}	$a^2\,X^3 + X + a$	$X^2 + a^2$	$a^2\,X + a^2$	$X^4 + a\,X^3 + a\,X + a^2$
b^{14}	$a\,X^3$	$X^2 + X + 1$	$a^2\,X + a^2$	$X^4 + a\,X^3 + X^2 + a\,X + 1$

TABLE 2.5 – Polynômes irréductibles de $\mathbb{F}_4[X;\theta]$ de degré 4 bornés par $X^8+X^6+X^4+X^2+1$ (exemple 7).

Proposition 9 (Proposition 8 de [Bou16]). *Soit p un nombre premier et soit k un entier tel que p ne divise pas k. On considère la factorisation suivante de $X^{2k}-1$ dans $\mathbb{F}_p[X^2]$*

$$X^{2k}-1 = \prod_{f_i=f_i^\natural,\ f_i\ irr} f_i(X^2) \prod_{f_i=g_ig_i^\natural, g_i\neq g_i^\natural\ irr} f_i(X^2) \in \mathbb{F}_p[X^2].$$

Le nombre de codes θ-cycliques auto-duaux sur $\mathbb{F}_{p^2}$ de dimension k est

$$N \times \prod_{f=f^\natural,\ irr, deg>1} (p^{d/2}+1) \times \prod_{f=gg^\natural} (p^{d/2}+3)$$

avec $d := \deg_{X^2}(f(X^2))$ et

$$N = \begin{cases} 1 & si \quad p=2 \\ 2 & si \quad p \equiv 3 \pmod 4 \text{ et } k \equiv 1 \pmod 2 \\ 0 & sinon. \end{cases}$$

Démonstration. On utilise la proposition 4 ainsi que les corollaires 3 et 4. □

Exemple 8. *Considérons les codes θ-cycliques auto-duaux de longueur 10 sur $\mathbb{F}_4$ (voir exemple 3 par ailleurs).*

On a

$$X^{10}-1 = (X^2+1)(X^8+X^6+X^4+X^2+1) \in \mathbb{F}_2[X^2]$$

$$h^\natural \cdot h = X^{10}-1 \Leftrightarrow h = \mathrm{lcrm}(h_1, h_2)$$

avec

$$\begin{cases} h_1^\natural \cdot h_1 = X^2-1 & : 1 \text{ solution} \\ h_2^\natural \cdot h_2 = X^8+X^6+X^4+X^2+1 & : 1+2^2 \text{ solutions (voir exemple 7).} \end{cases}$$

On obtient donc 5 codes θ-cycliques de longueur 10 auto-duaux sur $\mathbb{F}_4$ (voir exemple 3).

Bilan La proposition 9 permet de retrouver les nombres de codes auto-duaux θ-cycliques de dimension première avec p. Cette énumération est accompagnée d'une construction basée sur des paramétrisations de polynômes tordus via des interpolations de Cauchy dans $\mathbb{F}_{p^2}(X)$.

5 Construction et énumération sur $\mathbb{F}_{p^2}$ en dimension quelconque.

En utilisant des techniques de partitionnement similaires à celles utilisées en dimension p^s dans la proposition 6, on obtient une construction et un comptage des codes auto-duaux θ-cycliques en dimension quelconque. On utilisera encore le lemme 4, qui peut être formulé plus généralement :

Lemme 5 (Proposition 16 de [BU14b]). *Soit $\theta : x \mapsto x^p$ l'automorphisme de Frobenius sur $\mathbb{F}_{p^2}$ et soit $R = \mathbb{F}_{p^2}[X;\theta]$. Soit $f \in \mathbb{F}_p[x^2]$ irréducible dans $\mathbb{F}_p[x^2]$ et soit $h = h_m \cdots h_1$ un produit de polynômes tordus irréductibles unitaires divisant $f(X^2)$. Les assertions suivantes sont équivalentes :*

(i) h possède une factorisation en produit d'irréductibles unitaires unique ;
(ii) f ne divise pas h dans R ;
(iii) pour tout i dans $\{1,\dots,m-1\}$, $f \neq h_{i+1}\cdot h_i$.

Proposition 10 (Lemme 7 et proposition 9 de [Bou16])**.** *Soit p un nombre premier, soit θ l'automorphisme de Frobenius sur $\mathbb{F}_{p^2}$ et soit $k = p^s \times t$, $p \not| t$. Soit*

$$X^{2k}-1 = \prod_{f_i=f_i^\natural,\ f_i\ irr} f_i(X^2)^{p^s} \prod_{f_i=g_ig_i^\natural, g_i\neq g_i^\natural\ irr} f_i(X^2)^{p^s} \in \mathbb{F}_p[X^2].$$

Le nombre de codes θ-cycliques auto-duaux sur $\mathbb{F}_{p^2}$ de dimension k est

$$N \times \prod_{f=f^\natural,\ irr, deg>1} \frac{p^{\delta(p^s+1)}-1}{p^\delta-1} \times \prod_{f=gg^\natural} \frac{\left(p^{\delta(p^s+1)}-2p^s-3\right)\left(1+p^\delta\right)+4p^s+4}{\left(p^\delta-1\right)^2}$$

avec $\delta := \deg_{X^2}(f(X^2))/2$ et

$$N = \begin{cases} 1 & si \quad s=0, p=2 \\ 3 & si \quad s>0, p=2 \\ 2\dfrac{p^{(p^s+1)/2}-1}{p-1} & si \quad p\equiv 3 \pmod 4 \text{ et } k\equiv 1 \pmod 2 \\ 0 & sinon. \end{cases}$$

Exemple 9. *Les codes $[36,18]_4$ auto-duaux sont au nombre de 1533 d'après le tableau 2.1. On a $X^{36}-1 = (X^2+1)^2(X^4+X^2+1)^2(X^{12}+X^6+1)^2$. On a $p=2$, $s=1$, $t=9$. D'après la proposition 10, le nombre de codes θ-cycliques auto-duaux $[36,18]_4$ est $3\times\prod_{\delta\in\{1,3\}}\frac{2^{3\delta}-1}{2^\delta-1} = 3\times 7\times 73 = 1533$. Par exemple $g = X^{18}+X^{17}+aX^{16}+aX^{14}+X^{12}+aX^9+a^2X^6+aX^4+aX^2+a^2X+a^2$ engendre un code θ-cyclique $[36,18,11]_4$ auto-dual. On a $g = h^\natural$ où $h = \mathrm{lcrm}(h_0,h_1,h_2)$ avec $h_0 = X^2+1$, $h_1 = X^4+aX^3+aX^2+X+a^2 = (X^2+a^2)\cdot(X^2+aX+1)$, $h_2 = X^{12}+X^{10}+a^2X^9+a^2X^8+X^6+aX^4+aX^3+X^2+1 = (X^6+X^4+a^2X^3+a^2X^2+a^2)\cdot(X^6+a)$.*

6 Codes θ-cycliques étendus auto-duaux

Dans la continuité de la construction précédente, on construit ici des codes θ-cycliques C $[2k-2,k]_{p^2}$ tels que le dual $C^\perp$ de C soit inclus dans C. On étend ensuite ces codes pour obtenir des codes auto-duaux θ-cycliques étendus $[2k,k]_{p^2}$. On se repose ici sur [Bou18].

Définition 7 ([Bou18])**.** *Soit q une puissance d'un nombre premier, soit θ un automorphisme de $\mathbb{F}_q$ d'ordre m, soit $R = \mathbb{F}_q[X;\theta]$. Soit k un entier premier avec q tel que $mk-m$ est pair. Un code θ-*duadique (de multiplicateur -1) *de longueur $n = mk$ est un code θ-cyclique de polynôme générateur tordu unitaire $g \in \{(X^m-1)h^\natural, h^\natural\}$ où h vérifie*

$$(X^m-1)\cdot h^\natural \cdot h = X^n-1.$$

Un code θ-duadique de polynôme générateur tordu $g = (X^m-1)\cdot h^\natural$ est inclus dans son dual puisque g est multiple du polynôme générateur tordu $h^\natural$ du dual.

On se place dans le cas particulier de $\mathbb{F}_{p^2}$ dans ce qui suit et on décrit la famille des codes C θ-cycliques $[2k,k-1]_{p^2}$ tels que C est inclus dans son dual $C^\perp$.

Proposition 11 (Théorème 4.1 de [Bou18]). *Soit p un nombre premier, soit θ l'automorphisme de Frobenius sur $\mathbb{F}_{p^2}$. Soit k un nombre premier avec p. Soit C un code θ-cyclique $[2k, k-1]_{p^2}$ de polynôme générateur tordu unitaire g. Le code C est inclus dans son dual, si et seulement si l'une des trois situations suivantes est vérifiée :*

1. *$g = (X^2-1)\cdot h^\natural$ avec $h^\natural \cdot h = \frac{X^{2k}-1}{X^2-1}$. Dans ce cas on a $p = 2$ ou $p \equiv 1 \pmod 4$ et $k \equiv 0 \pmod 2$ ou $k \equiv 1 \pmod 2$. De plus C est un code θ-duadique.*
2. *$g = (X^2+1)\cdot h^\natural$ et $h^\natural \cdot h = \frac{X^{2k}-1}{X^2-1}$. Dans ce cas on a $k \equiv 0 \pmod 2$ et $p \equiv 3 \pmod 4$.*
3. *$g = (X-\lambda)\cdot(X+1/\lambda)\cdot h^\natural$ avec $\lambda^{(p+1)k} = 1$, $h = H\cdot(X+\lambda^p)$ ou $h = H\cdot(X-1/\lambda)$ et $H^\natural \cdot H = \frac{X^{2k}-1}{(X^2-\lambda^{p+1})\cdot(X^2-1/\lambda^{p+1})}$. Dans ce cas on a $k \equiv 1 \pmod 2$, $p \equiv 3 \pmod 4$ et $gcd(k, p-1) \neq 1$.*

Exemple 10. *D'après le point 1. de la proposition 11, les codes $[34,16]_4$ θ-cycliques C tels que $C \subset C^\perp$ sont les codes θ-duadiques de polynômes générateurs $(X^2-1)\cdot h^\natural$, où $h^\natural \cdot h = \frac{X^{34}-1}{X^2-1} = (X^{16}+X^{10}+X^8+X^6+1)(X^{16}+X^{14}+X^{12}+X^8+X^4+X^2+1)$. Comme les polynômes $X^{16}+X^{10}+X^8+X^6+1$ et $X^{16}+X^{14}+X^{12}+X^8+X^4+X^2+1$ sont irréductibles dans $\mathbb{F}_2[X^2]$, de degré 8 et autoréciproques, il y a $(1+2^4)^2 = 289$ tels codes. Par exemple $g = (X^2-1)\cdot h^\natural$ avec $h = X^{16}+X^{15}+aX^{12}+aX^{10}+X^9+X^8+X^7+a^2X^6+a^2X^4+X+1 = \mathrm{lcrm}(h_1, h_2)$ où $h_1 = X^8+aX^5+a^2X^3+1$ et $h_2 = X^8+X^7+a^2X^5+aX^3+X+1$ engendre un code θ-cyclique $[34,16]_4$ contenu dans son dual.*

Partant d'un code θ-cyclique $[2k-2, k]$ contenant son dual, on construit un code θ-cyclique étendu auto-dual $[2k, k]$ (voir Annexe B de [Bou18]) en suivant les trois étapes ci-après :

1. construire G matrice génératrice du code θ-cyclique $[2k-2, k]_{p^2}$ engendré par $g = h^\natural$ où $(X^2-1)\cdot h^\natural \cdot h = X^{2k-2}-1$:

$$G = \begin{pmatrix} g_0 & \dots & \dots & g_{k-2} & 0 & \dots & 0 \\ 0 & \theta(g_0) & \dots & \dots & \theta(g_{k-2}) & \ddots & \vdots \\ \vdots & \ddots & \ddots & & & \ddots & 0 \\ 0 & \dots & 0 & \theta^{k-1}(g_0) & \dots & \dots & \theta^{k-1}(g_{k-2}) \end{pmatrix}.$$

   On note $G_0, \dots, G_{k-1}$ les lignes de G.

2. construire $v_1, v_2, v_3, v_4 \in \mathbb{F}_{p^2}$ tels que

$$\begin{pmatrix} v_1^2+v_2^2 & v_1v_3+v_2v_4 \\ v_1v_3+v_2v_4 & v_3^2+v_4^2 \end{pmatrix} = -\begin{pmatrix} G_0 \times {}^tG_0 & G_0 \times {}^tG_1 \\ G_0 \times {}^tG_1 & G_1 \times {}^tG_1 \end{pmatrix}$$

   puis la matrice $k \times 2$ par blocs

$$M = \begin{pmatrix} v_1 & v_2 \\ v_3 & v_4 \\ \vdots & \vdots \\ v_1 & v_2 \\ v_3 & v_4 \end{pmatrix}.$$

   On note $M_0, \dots, M_{k-1}$ les lignes de M.

3. construire la matrice $k \times 2k$, $\tilde{G} = (G|M)$.
   On a $\tilde{G} \times {}^t\tilde{G} = 0$. En effet le code $C^\perp$ engendré par $(X^2-1)\cdot g$ est inclus dans son dual, engendré par g. On a donc $\forall i \in \{0, \ldots, k-3\}, \forall j \in \{0, \ldots, k-1\}, (G_{i+2}-G_i) \times {}^tG_j = 0$. On en déduit que pour i, j dans $\{0, \ldots, k-1\}$, $G_i \times {}^tG_j = G_{i \bmod 2}\, {}^tG_{j \bmod 2}$. De plus $M_i \times {}^tM_j = M_{i \bmod 2}\, {}^tM_{j \bmod 2} = -G_{i \bmod 2}\, {}^tG_{j \bmod 2}$ (par construction de M et v_1, v_2, v_3, v_4), donc $\tilde{G}_i \times {}^t\tilde{G}_j = 0$.
   Le code engendré par $\tilde{G}$ est donc auto-dual (mais n'est plus θ-cyclique).

Exemple 11. *(suite) On considère le code* $[34, 18]_4$ *qui est le dual du code* θ*-cyclique de l'exemple précédent. Il est engendré par* $h^\natural = X^{16} + X^{15} + a^2X^{12} + a^2X^{10} + X^9 + X^8 + X^7 + aX^6 + aX^4 + X + 1$. *On l'étend en un code* $[36, 18]_4$ *auto-dual en suivant le procédé précédent avec* $(v_1, v_2, v_3, v_4) = (0, 1, 1, 0)$.

7 Application à la construction de codes auto-duaux $[72, 36, 12]_2$

Cette partie est traitée dans [Bou18].

Les codes auto-duaux binaires $[72, 36]$ ont fait l'objet de nombreuses investigations. La principale question porte sur l'existence d'un code $[72, 36, 16]_2$ auto-dual et n'a pas de réponse à ce jour (voir [Dou11] pour une vue d'ensemble sur ce sujet). On s'intéresse ici aux codes auto-duaux binaires $[72, 36, 12]$ obtenus comme images binaires des codes θ-cycliques auto-duaux $[36, 18]_4$ et des codes θ-cycliques étendus auto-duaux $[36, 18]_4$. La distance minimale 12 est la meilleure distance que l'on a obtenue. Ces codes sont classés suivant leurs polynômes énumérateurs de poids, certains d'entre eux étant nouveaux.

On rappelle qu'un code binaire auto-dual est dit de Type II si tous ses mots ont un poids multiples de 4. Il est de Type I si au moins l'un de ses mots a un poids non multiple de 4. D'après [DGH97] et [KYS14], les énumérateurs de poids des codes $[72, 36, 12]_2$ auto-duaux de Type II sont

$$1 + (4398 + \alpha)y^{12} + (197073 - 12\,\alpha)y^{16} + (18396972 + 66\alpha)y^{20} + \cdots .$$

et ceux de Type I sont

$$W_{72,1} = 1 + 2\beta y^{12} + (8640 - 64\gamma)y^{14} + (124281 - 24\beta + 384\gamma)y^{16} + \cdots$$

et

$$W_{72,2} = 1 + 2\beta y^{12} + (7616 - 64\delta)y^{14} + (134521 - 24\beta + 384\delta)y^{16} + \cdots .$$

Les tableaux 2.6, 2.7, 2.8 et 2.9 résument les résultats obtenus. Les coeffcients $\alpha, \beta, \gamma, \delta$ des nouveaux énumérateurs de poids apparaissent en gras dans les tableaux.

8 Conclusion et perspectives

L'approche consistant à obtenir une écriture des solutions de l'équation auto-duale comme ppcm à gauche de polynômes tordus vérifiant des équations intermédiaires est résumée par le schéma 2.2 et a l'avantage d'éviter toute résolution de systèmes polynomiaux.

Cette approche a permis en particulier de construire des codes de grandes longueurs et de battre des records de distance minimale sur $\mathbb{F}_4$ en longueur 78 et sur $\mathbb{F}_9$ en longueur 52 ([BU14b]).

Coefficients de g	α
$[a^2, 0, a^2, a^2, 1, 1, a^2, 1, a^2, 0, 1, a^2, 1, a^2, a^2, 1, 1, 0, 1]$	**-2820**
$[1, a, a, a, a^2, a^2, a, 0, 0, 0, 0, 0, a^2, a, a, a^2, a^2, a^2, 1]$	**-3204**
$[1, a^2, a^2, 1, 1, a^2, 1, a, 0, 0, 0, a^2, 1, a, 1, 1, a, a, 1]$	**-3276**
$[a^2, 1, 1, 0, a, 1, 1, a^2, 0, 0, 0, 1, a^2, a^2, a, 0, a^2, a^2, 1]$	**-3312**
$[a^2, a^2, 1, a, a^2, 0, 0, 0, a, 0, a, 0, 0, 0, 1, a, a^2, 1, 1]$	**-3336**
$[a^2, a, a, 0, 1, a, a, a^2, a^2, 0, 1, 1, a, a, a^2, 0, a, a, 1]$	**-3372**
$[a^2, 0, 0, a^2, 0, a, a, a^2, a, a, a, 1, a, a, 0, 1, 0, 0, 1]$	**-3408**
$[1, 1, a, a^2, 1, 1, 1, a, 0, 1, 0, a^2, 1, 1, 1, a, a^2, 1, 1]$	**-3420**
$[a, a, 1, a, a^2, a^2, 1, a^2, a^2, a^2, a^2, a^2, a, a^2, a^2, 1, a, 1, 1]$	**-3456**
$[a, a^2, 1, a, 0, a, 0, a^2, a, a^2, 1, a^2, 0, 1, 0, 1, a, a^2, 1]$	**-3504**
$[1, a, a^2, a, a^2, 1, 1, a, a, 0, a^2, a^2, 1, 1, a, a^2, a, a^2, 1]$	**-3540**
$[a, 1, a^2, a^2, a, 0, a, 0, 0, 0, 0, 0, 1, 0, 1, a^2, a^2, a, 1]$	**-3564**
$[1, 0, 0, a, 1, 1, a^2, a, 0, 1, 0, a^2, a, 1, 1, a^2, 0, 0, 1]$	**-3576**
$[1, 1, a^2, a^2, 1, a^2, a, a^2, a, 0, a^2, a, a^2, a, 1, a, a, 1, 1]$	-3600
$[1, 0, 0, 0, 1, 1, 1, 0, a, 1, a^2, 0, 1, 1, 1, 0, 0, 0, 1]$	**-3612**
$[1, 0, 0, 0, 1, a^2, 0, 1, a^2, 0, a, 1, 0, a, 1, 0, 0, 0, 1]$	**-3636**
$[a, a^2, a^2, a^2, 1, 1, a^2, 0, a, 0, 1, 0, a^2, a, a, a^2, a^2, a^2, 1]$	-3660
$[1, 0, 0, a, 0, a, a, 1, 1, 1, 1, 1, a^2, a^2, 0, a^2, 0, 0, 1]$	-3696
$[a, 0, 0, a, a, 1, a^2, a^2, a, a^2, 1, a^2, a^2, a, 1, 1, 0, 0, 1]$	-3732
$[a, 0, a, a, 1, a^2, 0, a^2, 0, 0, 0, a^2, 0, a^2, a, 1, 1, 0, 1]$	-3744
$[a^2, a, 1, 1, a^2, a^2, 1, 0, a^2, a, 1, 0, a^2, 1, 1, a^2, a^2, a, 1]$	-3768
$[1, 1, a^2, 0, a, 0, a, 1, 0, 1, 0, 1, a^2, 0, a^2, 0, a, 1, 1]$	-3816
$[1, a^2, a^2, a, 0, a^2, a, a, a, 1, a^2, a^2, a^2, a, 0, a^2, a, a, 1]$	-3828
$[1, a, a, 1, 0, a^2, 0, a^2, 0, 0, 0, a, 0, a, 0, 1, a^2, a^2, 1]$	**-3924**

TABLE 2.6 – Enumérateurs de poids des auto-duaux binaires $[72, 36, 12]$ de Type II images binaires des codes θ-cycliques auto-duaux $[36, 18]_4$

Coefficients de g	β	γ
$[a^2, a, 1, 1, a^2, a^2, 1, 1, a, a, a, a^2, a^2, 1, 1, a^2, a^2, a, 1]$	**201**	**0**
$[1, 0, 0, a, 0, a^2, a, 0, a, 0, a^2, 0, a^2, a, 0, a^2, 0, 0, 1]$	237	0
$[1, a^2, a^2, a^2, a, 1, a^2, a, a, 1, a^2, a^2, a, 1, a^2, a, a, a, 1]$	249	0
$[1, 0, 1, a, a, 0, 1, 1, a^2, 1, a, 1, 1, 0, a^2, a^2, 1, 0, 1]$	273	0
$[a, 1, 1, 1, a^2, a, 1, a^2, 1, a^2, a, a^2, a, 1, a^2, a, a, a, 1]$	**273**	**36**
$[a^2, a^2, 1, 0, 1, 0, 0, a^2, 1, 0, a^2, 1, 0, 0, a^2, 0, a^2, 1, 1]$	309	0
$[1, 1, a, 1, a^2, a^2, a^2, 0, a, 1, a^2, 0, a, a, a, 1, a^2, 1, 1]$	**345**	**0**
$[a^2, a, 1, a^2, 0, 0, 1, 0, a^2, a, 1, 0, a^2, 0, 0, 1, a^2, a, 1]$	**381**	**0**
$[1, a, a, a^2, 0, a, a, 1, 1, 1, 1, 1, a^2, a^2, 0, a, a^2, a^2, 1]$	**393**	**36**
$[a, a, a^2, a, 1, a, 0, a, a^2, 0, a^2, 1, 0, 1, a, 1, a^2, 1, 1]$	**489**	**36**

TABLE 2.7 – Enumérateurs de poids des codes auto-duaux binaires $[72, 36, 12]$ de Type I images binaires des codes θ-cycliques auto-duaux $[36, 18]_4$.

Coefficients de g	v	α
$[a, a, 0, a, a^2, a, a, 0, 0, 0, 1, 1, a^2, 1, 0, 1, 1]$	$[1, a, 1, a^2]$	-3072
$[a, a^2, 0, a^2, a^2, a^2, 0, a^2, 0, a^2, 0, a^2, a^2, a^2, 0, a^2, 1]$	$[1, a, 1, a^2]$	-3276
$[a^2, 1, a^2, a^2, 1, a^2, 0, 1, 0, a^2, 0, 1, a^2, 1, 1, a^2, 1]$	$[1, a^2, 1, a]$	**-3480**
$[a, 1, a, 1, 0, 0, a, a^2, 0, a^2, 1, 0, 0, a, 1, a, 1]$	$[1, a, 1, a^2]$	-3582
$[a, 0, a^2, 0, 0, 1, 1, a^2, 0, a^2, a, a, 0, 0, a^2, 0, 1]$	$[1, a, 1, a^2]$	-3684
$[a^2, 1, 0, a, 0, 1, a^2, a, a, a, 1, a^2, 0, a, 0, a^2, 1]$	$[1, a^2, 1, a]$	-3990
$[a, a^2, a, 0, 0, 1, a, 1, 0, a, 1, a, 0, 0, 1, a^2, 1]$	$[1, a, 1, a^2]$	**-4092**

TABLE 2.8 – Enumérateurs de poids des codes auto-duaux $[72, 36, 12]$ de Type II images binaires des codes θ-cycliques étendus $[36, 18]_4$ auto-duaux

Coefficients de g	v	β	δ
$[1, 1, 0, 0, a, 0, a, 1, 1, 1, a^2, 0, a^2, 0, 0, 1, 1]$	$[0, 1, 1, 0]$	**221**	**0**
$[1, a^2, 1, 1, a, a^2, a^2, a^2, 0, a, a, a, a^2, 1, 1, a, 1]$	$[0, 1, 1, 0]$	**323**	**0**
$[a, 1, a, 1, 0, 0, a, a^2, 0, a^2, 1, 0, 0, a, 1, a, 1]$	$[0, a^2, a, 0]$	**238**	**0**
$[a, a, 0, a, a^2, a, a, 0, 0, 0, 1, 1, a^2, 1, 0, 1, 1]$	$[0, a^2, a, 0]$	**391**	**0**
$[a, a, 0, 1, 0, 0, a, 0, a^2, 0, 1, 0, 0, a, 0, 1, 1]$	$[0, a^2, a, 0]$	**289**	**0**
$[a^2, 1, 0, a, 0, 1, a^2, a, a, a, 1, a^2, 0, a, 0, a^2, 1]$	$[0, a, a^2, 0]$	**102**	**0**
$[a, 0, 1, a^2, 0, a, 0, a^2, 0, a^2, 0, 1, 0, a^2, a, 0, 1]$	$[0, a^2, a, 0]$	**255**	**0**
$[a, a^2, a, 0, 0, 1, a, 1, 0, a, 1, a, 0, 0, 1, a^2, 1]$	$[0, a^2, a, 0]$	**153**	**0**

TABLE 2.9 – Enumérateurs de poids des codes auto-duaux $[72, 36, 12]$ de Type I images binaires des codes θ-cycliques étendus $[36, 18]_4$ auto-duaux.

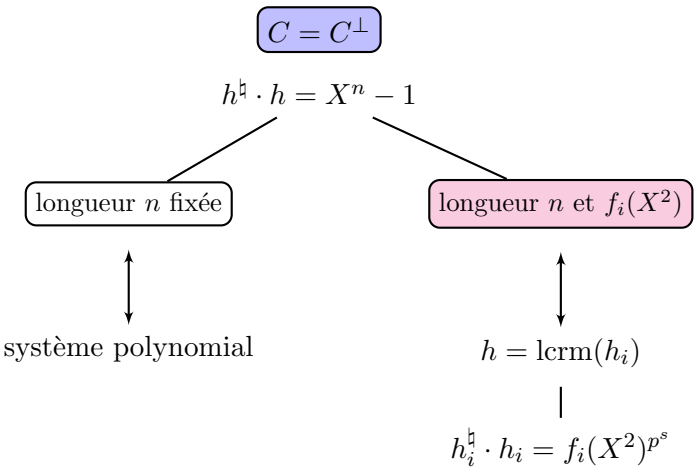

FIGURE 2.2 – Construction des codes θ-cycliques auto-duaux sur $\mathbb{F}_{p^2}$

En suivant le même procédé que précédemment, on peut aussi construire et énumérer les codes θ-négacycliques auto-duaux sur $\mathbb{F}_{p^2}$ (théorème 1 de [Bou16]).

Pour les codes auto-duaux hermitiens, l'étude n'a été que partiellement menée (théorème 3.7 de [Bou18] en dimension non multiple de p sur $\mathbb{F}_{p^2}$) et pourrait être complétée en longueur quelconque sur $\mathbb{F}_{p^2}$ en utilisant les mêmes techniques.

Par ailleurs, cette approche via les ppcm s'adapte bien pour une autre famille de codes, les codes LCD (tels que $C \cap C^{\perp} = \{0\}$ c'est à dire ici tels que $\mathrm{gcrd}(g, h^{\natural}) = 1$). On peut en effet remarquer que l'équation auto-duale se réécrit sous la forme $g \cdot h = X^n - 1$ avec $g = h^{\natural}$, ce qui est encore équivalent à $g = \mathrm{lclm}(g_i)$ où $g_i \cdot h_i = f_i(X^2)^{p^s}$ et $g_i = h_i^{\natural}$. Partant de cette nouvelle interprétation, il se déduit une interprétation des codes θ-cycliques LCD par l'équation $g \cdot h = X^n - 1$ avec $\mathrm{gcrd}(g, h^{\natural}) = 1$ et $\mathrm{gcrd}(g_i, h_i^{\natural}) = 1$. Un schéma récapitulatif est donné en figure 2.3. Ceci a donné lieu à un travail dans le cadre de la thèse de Rayna D. Boulanouar en co-direction avec Aicha Batoul ([BBB20b]).

Enfin les constructions ont été réalisées uniquement sur $\mathbb{F}_{p^2}$ et il serait intéressant d'étudier les constructions sur $\mathbb{F}_{p^m}$ avec $3 \leq m \leq n$ où n est la longueur du code. Le cas où $m = n$ correspond aux codes cycliques de Gabidulin et fait l'objet d'une prépublication avec Aicha Batoul et Rayna D. Boulanouar ([BBB20a]).

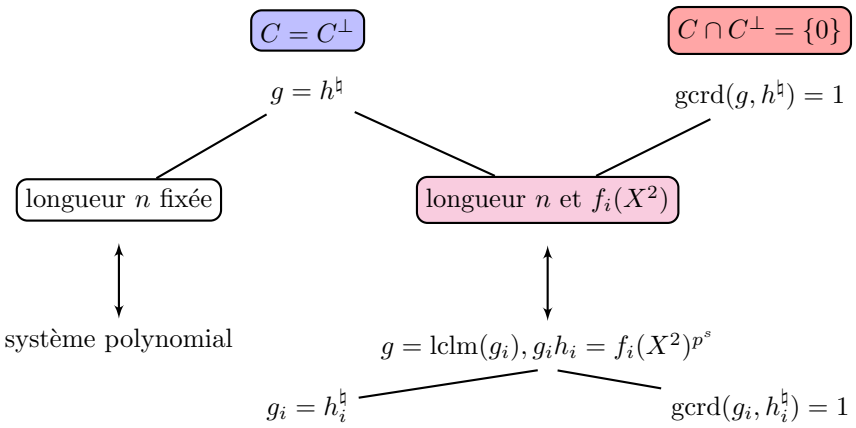

FIGURE 2.3 – Construction des codes θ-cycliques auto-duaux et LCD sur $\mathbb{F}_{p^2}$ de longueur n, polynômes générateur et de contrôle tordus g et h

Chapitre 3

Codes d'évaluation tordue

Le but de cette partie est de présenter une classe de codes d'évaluation définis à l'aide de polynômes tordus. Cette partie est une synthèse de [BU14a] puis de [Bou19].

1 Evaluation(s) des polynômes tordus

Les résultats qui suivent découlent des travaux de Lam et Leroy ([Lam86], [LL88]) et sont résumés dans la section 3 de [BU14a]. On s'intéresse ici à l'évaluation des polynômes tordus « par reste » puis « par opérateur ».

On considère l'anneau $R = A[X; \theta, \delta]$ où A est un corps non nécessairement commutatif, θ est un endomorphisme de A et δ est une θ-dérivation définie par

$$\forall a, b \in A, \begin{cases} \delta(a+b) = \delta(a) + \delta(b) \\ \delta(ab) = \delta(a)b + \theta(a)\delta(b). \end{cases}$$

La multiplication est alors régie par la loi

$$\forall a \in A, X \cdot a = \theta(a)X + \delta(a).$$

L'anneau R est un anneau Euclidien à droite. Si θ est un automorphisme il est aussi Euclidien à gauche.

Définition 8 (Evaluation, [LL88])**.** *Soit f dans R, soit α dans A. Il existe un unique q dans R et un unique a dans A tels que $f = Q \cdot (X - \alpha) + a$. L'application*

$$f : \begin{cases} A & \to & A \\ \alpha & \mapsto & a \end{cases}$$

est associée à cette division à droite et on note $a = f(\alpha)$ l'évaluation « par reste » de f en α.

Par ailleurs, l'expression de $f(\alpha)$ est donnée par le lemme :

Lemme 6 ([LL88])**.** *Soit α dans A et $f = \sum f_i X^i$ alors $f(\alpha) = \sum f_i N_i^{\theta,\delta}(\alpha)$ où $N_i^{\theta,\delta}(\alpha)$ est défini par*

$$\begin{array}{lcl} N_0^{\theta,\delta}(\alpha) & = & 1 \\ N_{i+1}^{\theta,\delta}(\alpha) & = & \theta(N_i^{\theta,\delta}(\alpha))\ \alpha + \delta(N_i^{\theta,\delta}(\alpha)). \end{array}$$

Remarque 2. *Si A est un corps fini ($A = \mathbb{F}_{p^m}$, avec p nombre premier), θ est l'automorphisme de Frobenius et δ est nulle, alors $N_m^{\theta,\delta}(\alpha) = \theta^{m-1}(\alpha)\cdots\theta(\alpha)\alpha = \alpha^{\frac{p^m-1}{p-1}}$ est la norme de α relative à l'extension $\mathbb{F}_{p^m}/\mathbb{F}_p$.*

Définition 9 ([LL88], page 321)**.** *Soit $n \in \mathbb{N}^*$. Soient $\alpha_1, \ldots, \alpha_n$ dans A et soit k dans $\mathbb{N}^*$. La* matrice (θ,δ)-Vandermonde $k \times n$ *de support $\underline{\alpha} = (\alpha_1, \ldots, \alpha_n)$ est définie par*

$$V_{k,n}^{\theta,\delta}(\underline{\alpha}) = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ N_1^{\theta,\delta}(\alpha_1) & N_1^{\theta,\delta}(\alpha_2) & \cdots & N_1^{\theta,\delta}(\alpha_n) \\ \vdots & \vdots & \cdots & \vdots \\ N_{k-1}^{\theta,\delta}(\alpha_1) & N_{k-1}^{\theta,\delta}(\alpha_2) & \cdots & N_{k-1}^{\theta,\delta}(\alpha_n) \end{pmatrix}.$$

Si $k = n$, la matrice est carrée et sera notée $V_n^{\theta,\delta}(\underline{\alpha})$. Si $\theta = id$ et $\delta = 0$, on obtient la matrice de Vandermonde classique.

Théorème 5 (Théorème 8, [LL88] page 326)**.** *Soient $n \in \mathbb{N}^*$, $\alpha_1, \ldots, \alpha_n \in A$ et $g = \mathrm{lclm}_{1\le i\le n}(X - \alpha_i) \in R$, alors* $\deg(g) = \mathrm{rang}\left(\mathrm{V_n^{\theta,\delta}}(\alpha_1, \ldots, \alpha_n)\right)$.

Si $\deg(g) = n$ *alors $\alpha_1, \ldots, \alpha_n$ sont dits* P-indépendants.

Considérons un sous-ensemble Ω de A. Le *rang* de Ω est $Rang(\Omega) := \deg \mathrm{lclm}_{u\in\Omega}(X - u)$.

Définition 10 (classes de conjugaison, [LL88])**.** *Soient $a, b \in A$. a et b sont* (θ,δ)-conjugués *s'il existe y dans A^* tel que $b = a^y$ où*

$$a^y := \theta(y)ay^{-1} + \delta(y)y^{-1}.$$

Ceci définit une relation d'équivalence sur A.

Remarque 3 (Remarque page 315 de [LL88])**.** *Les éléments a et b de A sont conjugués signifie que les polynômes $X - a$ et $X - b$ sont similaires dans R (voir définition 3). En effet $X-a \sim X-b$ si et seulement si il existe u et v non nuls dans A tels que $u\cdot(X-a) = (X-b)\cdot v$, soit $bv = ua + \delta(v)$ avec $u = \theta(v)$.*

Proposition 12 (Formule du produit, [LL88])**.** *Soient f, g dans R et soit α dans A.*

- *Si $g(\alpha) = 0$, alors $(f \cdot g)(\alpha) = 0$.*
- *Si $g(\alpha) \neq 0$, alors $(f \cdot g)(\alpha) = f(\alpha^{g(\alpha)})g(\alpha)$.*

Démonstration. ([LL88]) Soient $q_1(X)$ et $q_2(X)$ dans R tels que $g(X) = q_1(X)\cdot(X-\alpha)+g(\alpha)$ et $f(X) = q_2(X)\cdot(X - \alpha^{g(\alpha)}) + f(\alpha^{g(\alpha)})$. On a :

$$\begin{aligned} f(X)\cdot g(X) &= f(X)\cdot q_1(X)\cdot(X-\alpha) + q_2(X)\cdot \underbrace{(X-\alpha^{g(\alpha)})\cdot g(\alpha)}_{\theta(g(\alpha))\cdot(X-\alpha)} + f(\alpha^{g(\alpha)})g(\alpha) \\ &= (f(X)\cdot q_1(X) + q_2(X)\cdot\theta(g(\alpha)))\cdot(X-\alpha) + f(\alpha^{g(\alpha)})g(\alpha). \end{aligned}$$

□

A tout polynôme tordu on peut également associer un opérateur linéaire de la manière suivante (voir Lemme 2 de [BU14a] par ailleurs). Considérons l'opérateur $\mathcal{D}$ défini par :

$$\mathcal{D} = \begin{cases} \theta & \text{si} \quad \delta = 0 \\ \delta & \text{si} \quad \delta \neq 0. \end{cases}$$

A tout $f = \sum a_i X^i$ de R on associe l'opérateur $\mathcal{L}_f = \sum a_i \mathcal{D}^i$ dans $A[\mathcal{D}, +, \circ]$ où $\circ$ est la composition des opérateurs.

Définition 11 (Définition 3 de [BU14a]). *Soit f dans R et soit y dans A. L'évaluation tordue « par opérateur » de f en y est $\mathcal{L}_f(y)$.*

L'évaluation tordue « par opérateur » est liée à l'évaluation tordue « par reste » via la relation suivante :

$$\forall y \in A^*, \mathcal{L}_f(y) = f(\mathcal{D}(y)y^{-1}) \times y. \tag{3.1}$$

2 Codes d'évaluation tordue

On présente ici deux familles de codes de type Reed-Solomon basés sur l'évaluation tordue « par reste » et l'évaluation tordue « par opérateur » (section 4 de [BU14a]). Puis on propose un algorithme de décodage du type Berlekamp-Welch en métrique de Hamming (algorithme 1 de [BU14a]).

2.1 Codes d'évaluation tordue « par reste »

Définition 12 (Définition 7 de [BU14a]). *Soient $k \leq n$ dans $\mathbb{N}^*$, soient $\alpha_1, \ldots, \alpha_n$ P-indépendants dans A. Le* code d'évaluation tordue « par reste » de support $\underline{\alpha} = (\alpha_1, \ldots, \alpha_n)$ *et de dimension k est défini par*

$$\mathcal{C}_{k,n}^{\theta,\delta}(\underline{\alpha}) = \{(f(\alpha_1), \ldots, f(\alpha_n)) \mid f \in R, \deg(f) < k\}.$$

Une matrice génératrice de $\mathcal{C}_{k,n}^{\theta,\delta}(\underline{\alpha})$ est la matrice de Vandermonde rectangulaire $V_{k,n}^{\theta,\delta}(\underline{\alpha})$ (Lemme 1 de [BU14a]). Comme $\alpha_1, \ldots, \alpha_n$ sont P-indépendants, $V_{k,n}^{\theta,\delta}(\underline{\alpha})$ est de rang k.

Remarque 4 (Section 4.2 de [BU14a]). *Si $A = \mathbb{F}_q$, alors δ est nécessairement une dérivation interne : $\delta = \beta(\theta - id)$, avec $\beta \in \mathbb{F}_q$. On a alors pour tout i dans $\{1, \ldots, n\}$, $f(\alpha_i) = \psi(f)(\alpha_i + \beta)$ où ψ est l'isomorphisme d'anneaux défini par (cf. [Coh85], page 295)*

$$\psi : \begin{cases} \mathbb{F}_q[X; \theta, \delta] & \to & \mathbb{F}_q[Z; \theta] \\ \sum a_i X^i & \mapsto & \sum a_i \ (Z - \beta)^i . \end{cases} \tag{3.2}$$

On en déduit donc l'égalité $\mathcal{C}_{k,n}^{\theta,\delta}(\underline{\alpha}) = \mathcal{C}_{k,n}^{\theta}(\underline{\alpha} + \beta)$. Sur $\mathbb{F}_q$, la dérivation n'apporte donc rien pour les codes d'évaluation tordue « par reste ».

Exemple 12. *Si $A = \mathbb{F}_q$, $\theta = id$ et $\delta = 0$, alors $\alpha_1, \ldots, \alpha_n$ P-indépendants signifie que la matrice de Vandermonde (classique) $V_n^{id}(\underline{\alpha})$ est inversible c'est à dire que $\alpha_1, \ldots, \alpha_n$ sont distincts deux à deux. Ainsi, $\mathcal{C}_{k,n}^{id,0}(\underline{\alpha})$ est un code de Reed-Solomon de support $(\alpha_1, \ldots, \alpha_n)$.*

Proposition 13 (Proposition 2 de [BU14a]). *Soit $k \leq n$ dans $\mathbb{N}^*$. Soient $\alpha_1, \ldots, \alpha_n$ P-indépendants dans A. Le code $\mathcal{C}_{k,n}^{\theta}(\underline{\alpha})$ est un code MDS.*

Démonstration. On montre que le code ne possède pas de mot non nul de poids $< n-k+1$. Soit $c = (f(\alpha_1), \ldots, f(\alpha_n))$ avec $\deg(f) < k$ et $w_H(c) \leq n-k$. Soit $I = \{i \in \{1, \ldots, n\} \mid f(\alpha_i) = 0\}$ et soit $S(X) = \mathrm{lclm}_{i \in I}(X - \alpha_i)$. Alors $\#I \geq k$, $\deg(S) = \#I$ car $(\alpha_i)_{i \in I}$ sont P-indépendants et $S(X)$ divise $f(X)$ à droite donc $f = 0$ et $c = 0$.

□

2.2 Codes d'évaluation tordue « par opérateur »

L'évaluation tordue « par opérateur » permet de définir une nouvelle classe de codes, les codes d'évaluation tordue « par opérateur », qui ont un étroit lien avec les codes de Gabidulin et les codes d'évaluation tordue « par reste ». La définition qui suit est donnée dans un cadre plus général que celui des corps finis. On définit le corps K par :

$$K = \begin{cases} A^\theta = \{a \in A \mid \theta(a) = a\} & si \quad \delta = 0 \\ \{a \in A \mid \delta(a) = 0\} & si \quad \delta \neq 0. \end{cases}$$

Définition 13 (Définition 7 de [BU14a])**.** *Soient $k \leq n$ dans $\mathbb{N}^*$, soient $y_1, \ldots, y_n$ linéairement indépendants sur K. Le* code d'évaluation « par opérateur » de support $\underline{y} = (y_1, \ldots, y_n)$ *et de dimension k est défini par*

$$\mathcal{O}^{\theta,\delta}_{k,n}(\underline{y}) = \{(\mathcal{L}_f(y_1), \ldots, \mathcal{L}_f(y_n)) \mid f \in R, \deg(f) < k\}.$$

Une matrice génératrice de $\mathcal{O}^{\theta,\delta}_{k,n}(\underline{y})$ est le Wronskien

$$\mathrm{Wr}^{\theta,\delta}_{k,n}(y_1, \ldots, y_n) = \begin{pmatrix} y_1 & y_2 & \cdots & y_n \\ \mathcal{D}(y_1) & \mathcal{D}(y_2) & \cdots & \mathcal{D}(y_n) \\ \vdots & & & \\ \mathcal{D}^{k-1}(y_1) & \mathcal{D}^{k-1}(y_2) & \cdots & \mathcal{D}^{k-1}(y_n) \end{pmatrix}$$

(Lemme 1 page 11 de [BU14a]). Comme $y_1, \ldots, y_n$ sont linéairement indépendants sur K, le rang de $\mathrm{Wr}^{\theta,\delta}_n(y_1, \ldots, y_n)$ est égal à k.

Remarque 5. *Sur $\mathbb{F}_q$, si $\delta = 0$, alors $K = \mathbb{F}_q^\theta$ et $\mathcal{O}^{\theta,0}_{k,n}(\underline{y}) = \mathcal{O}^{\theta}_{k,n}(\underline{y})$ est un code de Gabidulin de support $(y_1, \ldots, y_n)$ ([Gab85]).*

2.3 Lien avec les codes de Gabidulin

On se place ici sur $A = \mathbb{F}_q$. Si $\delta \neq 0$, alors $\delta = \beta(\theta - id)$ où $\beta \in \mathbb{F}_q^*$. Le lemme 3 de [BU14a] montre que si β s'écrit sous la forme $\beta = \theta(u)/u$ avec $u \neq 0$, on a aussi $\mathcal{O}^{\theta,\delta}_{k,n}(\underline{y}) = \mathcal{O}^{\theta}_{k,n}(\underline{y})$. On généralise ici ce lemme avec β non nul quelconque dans $\mathbb{F}_q$:

Lemme 7 (Lemme 3 de [BU14a])**.** *Si A est un corps fini $\mathbb{F}_q$ alors $\mathcal{O}^{\theta,\delta}_{k,n}(\underline{y})$ est un code de Gabidulin.*

Démonstration. Comme $A = \mathbb{F}_q$, δ est une dérivation définie par $\delta = \beta(\theta - id)$ où $\beta \in \mathbb{F}_q$. Si $\beta = 0$, le résultat est immédiat. Supposons $\beta \neq 0$ et soient $\xi, u \in \mathbb{F}_q^*$ tels que $\beta = \xi \times \theta(u)/u$.

Soit y dans $\mathbb{F}_q^*$ et soit f dans R de degré $< k$. On a

$$\mathcal{L}_f(y) = f(\delta(y)/y) \times y = F\left(\xi \times \frac{\theta(uy)}{uy}\right) \times y \tag{3.3}$$

où $F = \psi(f) \in \mathbb{F}_q[Z;\theta]$ et ψ est défini en (3.2). Notons $\underline{\alpha} = (\frac{\theta(uy_1)}{uy_1}, \ldots, \frac{\theta(uy_n)}{uy_n})$ où $y_1, \ldots, y_n$ sont dans $\mathbb{F}_q$ et linéairement indépendants sur $\mathbb{F}_q^\theta$. On a, d'après (3.3),

$$(\mathcal{L}_f(y_1), \ldots, \mathcal{L}_f(y_n)) \quad = \quad (F(\xi\alpha_1), \ldots, F(\xi\alpha_n)) \times D_{\underline{y}}$$

où $D_{\underline{y}}$ est la matrice diagonale d'éléments diagonaux $y_1, \ldots, y_n$. Donc $\mathcal{O}_{k,n}^{\theta,\delta}(\underline{y})$ a pour matrice génératrice $V_{k,n}^\theta(\xi\underline{\alpha}) \times D_{\underline{y}}$. Or $V_{k,n}^\theta(\xi\underline{\alpha}) \times D_{\underline{y}} = P \times \mathrm{Wr}_{k,n}^\theta(u\underline{y})$ où P est la matrice diagonale inversible d'éléments diagonaux $(1/u, N_1^\theta(\xi)/u, \ldots, N_{k-1}^\theta(\xi)/u)$. Donc le code $\mathcal{O}_{k,n}^{\theta,\delta}(\underline{y})$ est égal au code de Gabidulin $\mathcal{O}_{k,n}^\theta(u\underline{y})$ de support $(uy_1, \ldots, uy_n)$. On conclut en utilisant le théorème 2 de [Ber03].

□

Si $A = \mathbb{F}_q$ et si $\alpha_1, \ldots, \alpha_n$ sont P-indépendants et conjugués à a ($\forall i, \alpha_i = a\theta(y_i)/y_i$), alors $y_1, \ldots, y_n$ sont linéairement indépendants sur $\mathbb{F}_q^\theta$ et $\mathcal{C}_{k,n}^\theta(\underline{\alpha})$ est un code équivalent à un code de Gabidulin de support $(y_1, \ldots, y_n)$. En effet

$$V_{k,n}^\theta(\underline{\alpha}) = \begin{pmatrix} N_0^\theta(a) & 0 & \cdots & 0 \\ 0 & N_1^\theta(a) & \cdots & 0 \\ \vdots & & \ddots & 0 \\ 0 & 0 & \cdots & N_{k-1}^\theta(a) \end{pmatrix} \times \mathrm{Wr}_{k,n}^\theta(\underline{y}) \times \begin{pmatrix} 1/y_1 & 0 & \cdots & 0 \\ 0 & 1/y_2 & \cdots & 0 \\ \vdots & & \ddots & 0 \\ 0 & 0 & \cdots & 1/y_n \end{pmatrix}.$$

Ainsi sur $\mathbb{F}_q$, les codes d'évaluation tordue « par opérateur » coincident avec les codes de Gabidulin et les codes d'évaluation tordue « par reste » sont équivalents aux codes de Gabidulin dans le cas particulier où les points du support du code tordu sont tous conjugués. Dans la suite on se focalisera uniquement sur les codes d'évaluation tordue « par reste » (avec des points du support non nécessairement conjugués).

Les codes de Gabidulin sont des codes optimaux pour la métrique rang. Ils ont fait l'objet de nombreux travaux dont deux thèses à l'Université de Rennes 1 ([WZ13] et [Rob15]). On rappelle ici rapidement la définition de la métrique rang sur un anneau A muni d'un automorphisme et d'une dérivation (voir Définition 8 de [BU14a] par ailleurs) :

Définition 14. *Soit $\underline{y} = (y_1, \ldots, y_n)$ dans A^n. Le* poids rang *de $\underline{y}$ est égal à* $\dim_K(y_1K + \cdots + y_nK) = \mathrm{rang}(Wr_n^{\theta,\delta}(\underline{y}))$.

Si $A = \mathbb{F}_q$ et θ est un automorphisme de $\mathbb{F}_q$, alors le *poids rang* de $\underline{y}$ sur $\mathbb{F}_q^\theta$, noté $\mathrm{rang}^\theta(\underline{y})$ est égal à la dimension du $\mathbb{F}_q^\theta$-sous-espace de $\mathbb{F}_q^n$ engendré par $y_1, \ldots, y_n$ ([Gab85], [Ber03]).

On a $\mathrm{rang}^\theta(\underline{y}) = \dim_{\mathbb{F}_q^\theta}(\underline{y}) = \mathrm{rang}(W_n^{\theta,\delta}(\underline{y}))$.

Les codes de Gabidulin sont des codes Maximum Rank Distance et il existe de nombreux travaux sur leur décodage en métrique rang ([WZ13], [Loi06], [Rob15]).

2.4 Un algorithme de décodage en métrique de Hamming

On s'inspire ici de l'algorithme de Welch-Berlekamp pour les codes de Reed-Solomon tel qu'il est présenté dans [Aug03] .

Soit C un code d'évaluation tordue $[n, k, n-k+1]_q$ de support $\underline{\alpha} = (\alpha_1, \ldots, \alpha_n)$ avec $\alpha_1, \ldots, \alpha_n$ P-indépendants.

Soient $c = (f(\alpha_1), \ldots, f(\alpha_n))$ dans C, e dans $\mathbb{F}_q^n$ et $r = c+e$ avec $w_H(e) \leq t := \lfloor (n-k)/2 \rfloor$.

Soit $E(X) = \mathrm{lclm}_{i|e_i \neq 0}(X - \alpha_i^{e_i})$ (qui correspond au polynôme tordu localisateur d'erreurs). Alors

$$\forall i \in \{1, \ldots, n\}, f(\alpha_i) = r_i \text{ ou } E(\alpha_i^{r_i - f(\alpha_i)}) = 0$$

donc $E \cdot (f - r_i) = E \cdot f - E \cdot r_i$ s'annule en α_i pour tout i dans $\{1, \ldots, n\}$:

$$\begin{cases} (E \cdot f)(\alpha_i) - E(\alpha_i^{r_i}) r_i = 0 & \text{si } r_i \neq 0 \\ (E \cdot f)(\alpha_i) = 0 & \text{si } r_i = 0. \end{cases}$$

Algorithme 1 Un algorithme de décodage des codes d'évaluation tordue pour la métrique de Hamming (Algorithme 1 de [BU14a])

Entrée : A corps non nécessairement commutatif, θ automorphisme de A, δ une θ-dérivation, $R = A[X; \theta, \delta]$, $\underline{\alpha} = (\alpha_1, \ldots, \alpha_n)$ P-indépendants sur A, $r \in A^n$ tel que $r = c + e$ avec $\mathrm{w}_H(e) \leq t := \lfloor (n-k)/2 \rfloor$, $c = (f(\alpha_1), \ldots, f(\alpha_n))$, $f \in R$ et $\deg(f) < k$.

Sortie : f

1: $d_0 \leftarrow n - 1 - t$

2: $d_1 \leftarrow d_0 - (k-1)$

3: Trouver une solution non nulle $q_{0,0}, \ldots, q_{0,d_0}, q_{1,0}, \ldots, q_{1,d_1}$ au système linéaire :

$$\begin{cases} \text{si } r_i = 0 : & \displaystyle\sum_{j=0}^{d_0} q_{0,j} \, N_j^{\theta,\delta}(\alpha_i) = 0 \\ \text{si } r_i \neq 0 : & \displaystyle\sum_{j=0}^{d_0} q_{0,j} \, N_j^{\theta,\delta}(\alpha_i) + \sum_{j=0}^{d_1} q_{1,j} \, N_j^{\theta,\delta}(\alpha_i^{r_i}) \, r_i = 0 \end{cases}$$

4: $Q_0 \leftarrow \displaystyle\sum_{j=0}^{d_0} q_{0,j} X^j$

5: $Q_1 \leftarrow \displaystyle\sum_{j=0}^{d_1} q_{1,j} X^j$

6: $f \leftarrow$ quotient dans la division euclidienne à gauche de Q_0 par $-Q_1$ dans R

7: **rendre** f

Proposition 14 (Proposition 5 de [BU14a])**.** *L'algorihme 1 est correct.*

Démonstration. Soient $Q_0(X)$ et $Q_1(X)$ dans R tels que pour tout i dans $\{1, \ldots, n\}$, $Q_0 + Q_1 \cdot r_i$ s'annule en α_i :

$$(*) \begin{cases} Q_0(\alpha_i) + Q_1(\alpha_i^{r_i}) r_i = 0 & \text{si } r_i \neq 0 \\ Q_0(\alpha_i) = 0 & \text{si } r_i = 0 \end{cases}$$

avec $\deg(Q_1) \leq t$ et $\deg(Q_0) \leq k - 1$, alors f est le reste de la division euclidienne à gauche de $-Q_0$ par Q_1.

En effet, soit i dans $\{1, \ldots, n\}$ tel que $e_i = 0$, alors $r_i = f(\alpha_i)$ et d'après le point 3., $(Q_0 + Q_1 \cdot f)(\alpha_i) = 0$. Ainsi $\mathrm{lclm}_{i|e_i=0}(X - \alpha_i)$ divise $Q_0 + Q_1 \cdot f$ à droite. De plus $\deg \mathrm{lclm}_{i|e_i=0}(X - \alpha_i) \geq n - t$ car les α_i sont P-indépendants et $\deg(Q_0 + Q_1 f) \leq t + k - 1 \leq n - t - 1$ par hypothèse sur les degrés d_0 et d_1 (points 1. et 2.). On a donc $Q_0 + Q_1 \cdot f = 0$.

□

Exemple 13. *Considérons* $\underline{\alpha} = (a^2, a^{23}, 2, a^{13}, 0, 4, a^{19}, a^4, a^{21}) \in \mathbb{F}_{25}^9$ *où* $\mathbb{F}_{25} = \mathbb{F}_5(a)$ *avec* $a^2 + 4a + 2 = 0$. *Le polynôme* $P = \mathrm{lclm}_{1 \leq i \leq 9}(X - \alpha_i)$ *est égal à* $X^9 - X$ *donc* $\alpha_1, \ldots, \alpha_9$ *sont P-indépendants, donc le code d'évaluation tordue « par reste »* $[9, 2, 8]_{25}$ *de support* $\underline{\alpha}$ *est bien défini. Il est à noter que* $\alpha_1, \ldots, \alpha_9$ *ne sont pas linéairement indépendants sur* $\mathbb{F}_5$ *et on ne peut pas définir un code de Gabidulin de support* $\underline{\alpha}$.

La capacité de correction pour la métrique de Hamming est égale à 3.

Considérons $c = (f(\alpha_1), \ldots, f(\alpha_9))$ *où* $f = a^4X + a^{15}$ *et* $r = c + e$ *avec* $e = (a^2, 0, 0, a, 0, 0, 0, 1)$ *de poids de Hamming égal à* 3.

Les polynômes $Q_0 = a^{16}X^5 + a^{15}X^4 + a^7X^3 + X$ *et* $Q_1 = X^4 + a^{13}X^3 + a^2X^2 + a^9X$ *vérifient les conditions des points 3, 4 et 5 de l'algorithme 1. Le quotient de la division euclidienne à gauche de* $-Q_0$ *par* Q_1 *est bien égal à* $a^4X + a^{15}$.

Augmentons le poids de Hamming de e de telle façon à dépasser la capacité de correction du code : $e = (a^2, 0, 0, a^8, a, 0, 0, 0, 1)$. *On constate que l'algorithme fonctionne. En effet les polynômes tordus* $Q_0 = a^2X^5 + a^9X^4 + a^{10}X^3 + X^2$ *et* $Q_1 = a^{10}X^4 + a^{21}X^3 + a^{21}X^2$ *vérifient les conditions des points 3, 4 et 5 de l'algorithme 1. Le quotient de la division euclidienne à gauche de* $-Q_0$ *par* Q_1 *est bien égal à* $a^4X + a^{15}$. *Nous verrons une explication de ceci dans la section suivante et l'exemple 14.*

3 Codes d'évaluation tordue en métrique tordue

Cette section est une brève synthèse de [Bou19].

Dans la suite du document, un code d'évaluation tordue désignera un code d'évaluation tordue « par reste ».

On s'intéresse ici à une nouvelle métrique, appelée 'skew metric', ou métrique tordue introduite par Martinez-Penas dans [MPn18]. Après avoir donné une nouvelle interprétation à cette métrique, on démontre que les codes d'évaluation tordue sont MSD (Maximum Skew Distance). Enfin, après avoir adapté l'algorithme de décodage 1 à la métrique tordue (Algorithme 2), on donne quelques pistes pour l'adaptation de l'algorithme de décodage en liste de Sudan à la métrique tordue.

3.1 Une nouvelle interprétation de la métrique tordue

Définition 15 (Definition 9 de [MPn18])**.** *Soit n un entier non nul, soit* $\underline{\alpha} = (\alpha_1, \ldots, \alpha_n) \in A^n$, *P-indépendants sur A, soit* $P = \mathrm{lclm}_{1 \leq i \leq n}(X - \alpha_i)$, *soit* $y = (y_1, \ldots, y_n) \in A^n$ *et soit F le polynôme d'interpolation tordu en les points* $(\alpha_1, y_1), \ldots, (\alpha_n, y_n)$. *Le* poids tordu *de y (par rapport à* $\underline{\alpha}$*) est*

$$w_{\underline{\alpha}}(y) = n - Rank(\{u \in A \mid P(u) = F(u) = 0\}).$$

Dans les lemmes 8 et 9, on propose deux interprétations de la métrique tordue.

Lemme 8 (Lemme 1 de [Bou19])**.** *Soit n un entier non nul, soit* $\underline{\alpha} = (\alpha_1, \ldots, \alpha_n) \in A^n$, *P-indépendants sur A, soit* $P = \mathrm{lclm}_{1 \leq i \leq n}(X - \alpha_i)$, *soit* $y = (y_1, \ldots, y_n) \in A^n$ *et soit F le polynôme d'interpolation tordu de F en les points* $(\alpha_1, y_1), \ldots, (\alpha_n, y_n)$. *Le* poids tordu *de y (par rapport à* $\underline{\alpha}$*) est*

$$w_{\underline{\alpha}}(y) = n - \deg(\mathrm{gcrd}(P, F)).$$

Démonstration. Considérons l'ensemble $U = \{u \in A \mid P(u) = F(u) = 0\}$. D'après la définition 15, $w_{\underline{\alpha}}(y) = n - \deg(G)$ où $G = \mathrm{lclm}_{u \in U}(X - u)$. Pour tout u de U, $X - u$ divise P et F à droite, donc G divise P et F à droite.

Considérons une facteur à droite H commun à P et F. Comme P est un ppcm à gauche de facteurs linéaires, il existe un ensemble V d'éléments de A tel que $H = \mathrm{lclm}_{v\in V}(X - v)$. De plus pour tout v de V, $P(v) = F(v) = 0$ donc V est inclus dans U et H divise G.

□

Lemme 9 (Proposition 1 de [Bou19])**.** *Soit n un entier non nul, soit $\underline{\alpha} = (\alpha_1, \ldots, \alpha_n) \in A^n$, P-indépendants sur A, soit $y = (y_1, \ldots, y_n) \in A^n$. Le* poids tordu *de y (par rapport à $\underline{\alpha}$) est*

$$w_{\underline{\alpha}}(y) = \deg(\mathrm{lclm}_{y_i\neq 0}(X - \alpha_i^{y_i})).$$

Démonstration. Considérons $E = \mathrm{lclm}_{y_i\neq 0}(X - \alpha_i^{y_i})$. D'après le lemme précédent, $w_{\underline{\alpha}}(y) = n - \deg(\mathrm{gcrd}(P, F)) = \deg(P) - \deg(\mathrm{gcrd}(P, F)) = \deg(\mathrm{lclm}(P, F)) - \deg(F)$. Considérons $\tilde{E}$ dans R tel que $\tilde{E} \cdot F = \mathrm{lclm}(P, F)$, alors $w_{\underline{\alpha}}(y) = \deg(\tilde{E})$.

P divise $E\cdot F$ à droite. En effet $(E\cdot F)(\alpha_i) = 0$ par définition de E. Donc $\mathrm{lclm}(P, F) = \tilde{E}\cdot F$ divise $E \cdot F$ à droite donc $\tilde{E}$ divise E à droite.

$\tilde{E}$ s'annule en $\alpha_i^{y_i}$ si $y_i \neq 0$. En effet $\tilde{E} \cdot F$ s'annule en α_i, donc d'après la formule du produit, si $y_i \neq 0$, $\tilde{E}(\alpha_i^{y_i}) = 0$. Donc E divise $\tilde{E}$ à droite.

□

Exemple 14. *Considérons $\underline{\alpha} = (a^2, a^{23}, 2, a^{13}, 0, 4, a^{19}, a^4, a^{21}) \in \mathbb{F}_{25}^9$ (exemple 13). Considérons $e = (a^2, 0, 0, a^8, a, 0, 0, 0, 1) \in \mathbb{F}_{25}^9$. Le poids de Hamming de e est 4 et e poids tordu de e est $w_{\underline{\alpha}}(e) = 3$.*

De la deuxième interprétation donnée dans le lemme 9, on déduit une nouvelle preuve du théorème

Théorème 6 (Théorème 1 de [MPn18] ou Théorème 3 de [Bou19])**.** *Un code d'évaluation tordue est MSD (Maximum Skew Distance).*

Démonstration. Soit $c = (f(\alpha_1), \ldots, f(\alpha_n))$ un mot de code de poids $\leq n - k$ où $f \in R$ est de degré $< k$. Considérons $E = \mathrm{lclm}_{c_i\neq 0}(X - \alpha_i^{c_i})$. D'après la formule du produit, on a $(E \cdot f)(\alpha_i) = 0$ pour tout i dans $\{1, \ldots, n\}$, donc P divise $E \cdot f$ à droite. Enfin le degré de $E \cdot f$ est inférieur ou égal à $(n - k) + (k - 1) = n - 1 = \deg(P) - 1$, donc $E \cdot f = 0$ et $f = 0$.

□

3.2 Un algorithme de décodage unique pour la métrique tordue

Dans cette partie, on montre que l'algorithme de décodage 1 pour la métrique de Hamming s'adapte bien à la métrique tordue. Pour montrer ce résultat, on utilisera le lemme suivant.

Lemme 10. *Soient f et g dans R. Si g divise f à droite alors $w_{\underline{\alpha}}(f(\alpha_1), \ldots, f(\alpha_n)) \leq w_{\underline{\alpha}}(g(\alpha_1), \ldots, g(\alpha_n))$.*

Démonstration. Considérons F, G les polynômes d'interpolation tordue aux points $(\alpha_i, f(\alpha_i))$ et $(\alpha_i, g(\alpha_i))$. D'après le lemme 8, on a :

$$\begin{cases} w_{\underline{\alpha}}(g(\alpha_1), \ldots, g(\alpha_n)) = \deg(P) - \deg(\mathrm{gcrd}(P, G)) \\ w_{\underline{\alpha}}(f(\alpha_1), \ldots, f(\alpha_n)) = \deg(P) - \deg(\mathrm{gcrd}(P, F)). \end{cases}$$

Comme P divise à droite $G-g$ et $F-f$, on a $\gcrd(P,G)=\gcrd(P,g)$ et $\gcrd(P,F)=\gcrd(P,f)$. De plus $\gcrd(P,g)$ divise à droite $\gcrd(P,f)$ donc $\deg(\gcrd(P,F))-\deg(\gcrd(P,G))\geq 0$ et

$$\begin{aligned} w_{\underline{\alpha}}(f(\alpha_1),\ldots,f(\alpha_n)) &= w_{\underline{\alpha}}(g(\alpha_1),\ldots,g(\alpha_n))+\deg(\gcrd(P,F))-\deg(\gcrd(P,G)) \\ &\leq w_{\underline{\alpha}}(g(\alpha_1),\ldots,g(\alpha_n)). \end{aligned}$$

□

Algorithme 2 Un algorithme de décodage des codes d'évaluation tordue pour la métrique tordue

Entrée : A corps non nécessairement commutatif, θ automorphisme de A, δ une θ-dérivation, $R=A[X;\theta,\delta]$, $\underline{\alpha}=(\alpha_1,\ldots,\alpha_n)$ P-independants sur A, $r\in A^n$ tel que $r=c+e$ avec $\mathrm{w}_{\underline{\alpha}}(e)\leq t:=\lfloor (n-k)/2\rfloor$, $c=(f(\alpha_1),\ldots,f(\alpha_n))$, $f\in R$ et $\deg(f)<k$.

Sortie : f

1: $d_0\leftarrow n-1-t$

2: $d_1\leftarrow d_0-(k-1)$

3: Calculer $q_{0,0},\ldots,q_{0,d_0},q_{1,0},\ldots,q_{1,d_1}$ solution non nulle du système :

$$\begin{cases} \text{si } r_i=0: & \displaystyle\sum_{j=0}^{d_0} q_{0,j}\,N_j^{\theta,\delta}(\alpha_i)=0 \\ \text{si } r_i\neq 0: & \displaystyle\sum_{j=0}^{d_0} q_{0,j}\,N_j^{\theta,\delta}(\alpha_i)+\sum_{j=0}^{d_1} q_{1,j}\,N_j^{\theta,\delta}(\alpha_i^{r_i})\;r_i=0 \end{cases}$$

4: $Q_0\leftarrow \displaystyle\sum_{j=0}^{d_0} q_{0,j}X^j$

5: $Q_1\leftarrow \displaystyle\sum_{j=0}^{d_1} q_{1,j}X^j$

6: $f\leftarrow$ quotient dans la division euclidienne à gauche de Q_0 par $-Q_1$ dans R

7: **rendre** f

Proposition 15. *L'algorithme 2 est correct.*

Démonstration. Considérons $Z(X)=Q_0(X)+Q_1(X)\cdot f(X)$ et $g(X)$ le polynôme d'interpolation tordue en les points $(\alpha_1,r_1),\ldots,(\alpha_n,r_n)$.

Par construction de $Q_0(X)$ et $Q_1(X)$, le polynôme $Q_0(X)+Q_1(X)\cdot g(X)$ s'annule en les points $\alpha_1,\ldots,\alpha_n$.

On a donc, pour tout i de $\{1,\ldots,n\}$, $Z(\alpha_i)=(Q_1(X)\cdot(f(X)-g(X)))(\alpha_i)$. De plus $f(X)-g(X)$ divise à droite $(Q_1(X)\cdot(f(X)-g(X)))$, donc d'après le lemme 10, on a

$$w_{\underline{\alpha}}(Z(\alpha_1),\ldots,Z(\alpha_n))\leq w_{\underline{\alpha}}(e)\leq t$$

D'après le lemme 9, le polynôme $E(X)=\mathrm{lclm}_{Z(\alpha_i)\neq 0}(X-\alpha_i^{Z(\alpha_i)})$ est donc de degré $\leq t$. De plus, d'après la formule du produit (proposition 12), le polynôme tordu $E\cdot Z$ s'annule en α_i pour tout i de $\{1,\ldots,n\}$. Or son degré est $\leq n-t-1+t<n$, donc $E\cdot Z=0$ et $Z=0$.

□

Remarque 6. *Dans les algorithmes 1 et 2, si θ n'est pas un automorphisme, R n'est pas Euclidien à gauche, ainsi la division à gauche du point 6. ne peut pas être effectuée. Dans ce cas, on effectuera une division à droite de Q_0^* par Q_1^* (voir [Bou19]).*

Remarque 7. *Dans le cas où θ est le morphisme identité et δ est la dérivation nulle, l'algorithme 2 correspond à l'algorithme de Berlekamp-Welch pour les codes de Reed-Solomon et la métrique de Hamming.*

Exemple 15. *Considérons le code d'évaluation tordue $[9, 2, 8]_{25}$ de support*
$\underline{\alpha} = (a^2, a^{23}, 2, a^{13}, 0, 4, a^{19}, a^4, a^{21})$ *(voir exemples 13 et 14). Sa capacité de correction pour la métrique tordue associée à $\underline{\alpha}$ est égale à 3. Considérons $e = (a^2, 0, 0, a^8, a, 0, 0, 0, 1)$. Le poids tordu de e est $w_{\underline{\alpha}}(e) = 3$ c'est pourquoi l'algorithme 1 s'adapte bien (comme montré dans la fin de l'exemple 14).*

3.3 Décodage en liste en métrique tordue ?

Cette partie est extraite de la version longue de [Bou19] (soumission à DCC) et n'est pas encore complètement aboutie.

On propose ici un algorithme de décodage en liste pour les codes d'évaluation tordue. L'idée est d'obtenir l'algorithme de décodage de Sudan des codes de Reed-Solomon pour la métrique de Hamming (voir [Aug03]) quand $\theta = id$ et $\delta = 0$. A noter que l'étude du décodage en liste des codes de Gabidulin pour la métrique rang a fait l'objet de nombreuses investigations (voir [WZ13]).

On prend le parti ici de présenter l'algorithme sans utiliser le formalisme des polynômes bivariés, mais ce formalisme semble ensuite nécessaire pour ce qui est l'étude de la construction et de la taille de la liste (proposition 17).

Le point le plus délicat ici provient du fait que l'on va devoir imposer un peu plus sur le poids de l'erreur. On s'inspire de l'interprétation de la métrique tordue donnée dans le lemme 8 pour ajuster les conditions de départ sur le vecteur erreur.

Proposition 16. *L'algorithme 3 est correct.*

Démonstration. Les équations du point 5 de l'algorithme sont n équations linéaires en $\sum_{j=0}^{\ell} n - 1 - \tau - j(k-1) = (\ell+1)(n-1-\tau) - \ell(\ell+1)(k-1)/2 \geq n+1$ inconnues. Ainsi il existe $(q_{0,0}, \ldots, q_{0,d_0}, \ldots, q_{\ell,0}, \ldots, q_{\ell,d_\ell})$ non nul. Considérons $Q_s(X) = \sum_{j=0}^{d_s} q_{s,j} X^j$ pour $s = 0, \ldots, \ell$ et $Z(X) = \sum_{s=0}^{\ell} Q_s(X) \cdot f^s(X)$. Montrons que $Z(X) = 0$.

Considérons $E(X) = \mathrm{lclm}_{Z(\alpha_i) \neq 0}(X - \alpha_i^{Z(\alpha_i)})$. D'après la formule du produit (proposition 12), le polynôme tordu $E \cdot Z$ s'annule en $\alpha_1, \ldots, \alpha_n$ donc $E \cdot Z$ est divisible à droite par le polynôme $P = \mathrm{lclm}_{1 \leq i \leq n}(X - \alpha_i)$ de degré n. De plus $\deg(Z) \leq \max_{0 \leq s \leq \ell}(\deg(Q_s) + s(k-1)) \leq n - 1 - \tau$. Montrons que $\deg(E) \leq \tau$, ce qui signifie $w_{\underline{\alpha}}(Z(\alpha_1), \ldots, Z(\alpha_n)) \leq \tau$ (d'après le lemme 9).

Pour i dans $\{1, \ldots, n\}$, $Z(\alpha_i) = (\sum_{s=0}^{\ell} Q_s \cdot f^s)(\alpha_i)$. De plus, les polynômes tordus $Q_0(X)$, …, $Q_\ell(X)$ vérifient les relations du point 5. :

$$\forall i \in \{1, \ldots, n\}, \left(\sum_{s=0}^{\ell} Q_s \cdot g^s \right)(\alpha_i) = \left(\sum_{s=0}^{\ell} (\sum_{j=0}^{d_s} q_{s,j} X^j) \cdot g^s \right)(\alpha_i) = 0.$$

On obtient donc $Z(\alpha_i) = H(\alpha_i)$ où $H := \sum_{s=1}^{\ell} Q_s \cdot (f^s - g^s)$.

Algorithme 3 Algorithme de "décodage en liste" des codes de Reed-Solomon tordus

Entrée : A un corps non nécessairement commutatif, θ un endomorphisme de A, δ une θ-dérivation, $R = A[X;\theta,\delta]$, $\underline{\alpha} = (\alpha_1,\ldots,\alpha_n)$ P-independants sur A, $r \in A^n$ tel que $r = c+e$ avec $c = (f(\alpha_1),\ldots,f(\alpha_n))$, $f \in R$, $\deg(f) < k$ et

$$w_{\underline{\alpha}}(G(\alpha_1),\ldots,G(\alpha_n)) \leq \tau$$

où $\tau \leq \min\left(n\frac{\ell}{\ell+1} + (k-1)\frac{\ell}{2}, n-1-(k-1)\ell\right)$, $G = \mathrm{gcrd}(g-f,\ldots,g^\ell - f^\ell)$ et g est le polynôme d'interpolation tordue aux points $(\alpha_1,r_1),\ldots,(\alpha_n,r_n)$.

Sortie : L'ensemble $\mathcal{L}$ des polynômes tordus $\tilde{f}$ de R de degré $< k$ tels que $\deg(\tilde{f}) < k$ et $w_{\underline{\alpha}}(\tilde{G}(\alpha_1),\ldots,\tilde{G}(\alpha_n)) \leq \tau$ où $\tilde{G} = \mathrm{gcrd}(g-\tilde{f},\ldots,g^\ell-\tilde{f}^\ell)$

1: $g \leftarrow$ polynôme d'interpolation dans R aux points $(\alpha_1,r_1),\ldots,(\alpha_n,r_n)$
2: **pour** $s = 0,\ldots,\ell$ **faire**
3: $\quad d_s \leftarrow n-1-\tau-s(k-1)$
4: **fin pour**
5: Calcul d'une solution non nulle $(q_{0,0},\ldots,q_{0,d_0},q_{1,0},\ldots,q_{1,d_1},\ldots,q_{\ell,d_\ell})$ au système linéaire

$$\sum_{s=0}^{\ell}\sum_{j=0}^{d_s} q_{s,j} \times \left(\left(X^j \cdot g^s\right)(\alpha_i)\right) = 0, i = 1\ldots n$$

6: **pour** $s = 0,\ldots,\ell$ **faire**
7: $\quad Q_s(X) \leftarrow \sum_{j=0}^{d_s} q_{s,j}X^j$
8: **fin pour**
9: *Calcul* de l'ensemble $\mathcal{L}$ des $\tilde{f}$ dans R de degré $< k$ tels que

$$Q_0(X) + Q_1(X)\cdot\tilde{f}(X) + Q_2(X)\cdot\tilde{f}^2(X) + \cdots + Q_\ell(X)\cdot\tilde{f}^\ell(X) = 0$$

et $w_{\underline{\alpha}}((\tilde{G}(\alpha_1),\ldots,\tilde{G}(\alpha_n)) \leq \tau$ où $\tilde{G} = \mathrm{gcrd}(g-\tilde{f},\ldots,g^\ell-\tilde{f}^\ell)$
10: **rendre** $\mathcal{L}$

Considérons $G = \text{gcrd}(g - f, g^2 - f^2, \ldots, g^\ell - f^\ell)$. Alors G divise H à droite donc d'après le lemme 10, $w_{\underline{\alpha}}(H(\alpha_1), \ldots H(\alpha_n)) \leq w_{\underline{\alpha}}(G(\alpha_1), \ldots G(\alpha_n))$. De plus par hypothèse, $w_{\underline{\alpha}}(G(\alpha_1), \ldots G(\alpha_n)) \leq \tau$ donc $w_{\underline{\alpha}}(Z(\alpha_1), \ldots, Z(\alpha_n)) \leq \tau$.

□

Remarque 8. *Si $\ell = 1$ et $\tau = t$, on retrouve l'algorithme 2. En effet la condition*

$$w_{\underline{\alpha}}(G(\alpha_1), \ldots, G(\alpha_n)) \leq \tau$$

s'écrit

$$w_{\underline{\alpha}}((g - f)(\alpha_1), \ldots, (g - f)(\alpha_n)) \leq \tau$$

c'est à dire $w_\alpha(e) \leq t$. De plus les équations

$$\sum_{s=0}^{\ell} \sum_{j=0}^{d_s} q_{s,j} \times \left(\left(X^j \cdot g^s\right)(\alpha_i)\right) = 0, i = 1 \ldots n$$

s'écrivent

$$\sum_{j=0}^{d_0} q_{0,j} \times \left(\left(X^j \cdot g^0\right)(\alpha_i)\right) + \sum_{j=0}^{d_1} q_{1,j} \times \left(\left(X^j \cdot g\right)(\alpha_i)\right) = 0, i = 1 \ldots n$$

soit

$$\begin{cases} \sum_{j=0}^{d_0} q_{0,j}\, N_j^{\theta,\delta}(\alpha_i) = 0 \text{ si } r_i (= (g(\alpha_i)) = 0 \\ \sum_{j=0}^{d_0} q_{0,j}\, N_j^{\theta,\delta}(\alpha_i) + \sum_{j=0}^{d_1} q_{1,j}\, N_j^{\theta,\delta}(\alpha_i^{r_i})\ r_i = 0 \text{ si } r_i \neq 0. \end{cases}$$

Arrivé à ce stade, deux questions se posent : quelle est la taille de la liste obtenue ? peut-on calculer cette liste de manière efficace ?

Dans ce qui suit, nous donnons des réponses partielles qui reposent essentiellement sur deux articles : [GM65] et [GS00].

Nous supposerons dans la suite que A est un corps $\mathbb{F}_q$, θ est un automorphisme de A et que la dérivation δ est nulle.

Nous allons associer aux $\ell + 1$ polynômes $Q_0(X), \ldots, Q_\ell(X) \in \mathbb{F}_q[X; \theta]$, le polynôme $Q(X, Y) \in \mathbb{F}_q(X; \theta)[Y]$ où $\mathbb{F}_q(X; \theta)$ est le corps des fractions à droite de $\mathbb{F}_q[X; \theta]$. Le polynôme $Q(X, Y)$ est alors un polynôme gauche, selon la terminologie de [GM65] que nous exposons en quelques lignes ci-dessous.

Considérons un corps non commutatif D. Un polynôme gauche à coefficients dans D est un expression de la forme $f = \sum a_i Y^i$ où $a_i \in D$. Pour c dans D, on définit $f(c) = \sum a_i c^i$. Si $f(c) = 0$, c est appelé zéro ou racine de f.

Les polynômes gauche peuvent être additionnés et multipliés en utilisant les règles usuelles : $\sum a_k Y^k + \sum b_k Y^k = \sum (a_k + b_k) Y^k$ et $(\sum a_k Y^k)(\sum b_k Y^k) = \sum (\sum_{i+j=k} a_i b_j) Y^k$.

Théorème 7 ([GM65])**.** *Un polynôme gauche de degré d à coefficients dans un corps non nécessairement commutatif D a ou bien au plus d racines, ou bien une infinité de racines.*

Exemple 16. *Le polynôme gauche $Y^2 + Y + X^2 + 1 \in \mathbb{F}_9(X; \theta)[Y]$ possède $4 > 2$ racines dans $\mathbb{F}_9[X; \theta]$: $a^5X + 1$, $a^7X + 1$, $aX + 1$ et $a^3X + 1$. Il possède un nombre infini de racines dans $\mathbb{F}_9(X; \theta)$.*

Ainsi le nombre de polynômes $f(X)$ de degré $< k$ vérifiant $Q_0(X) + Q_1(X) \cdot f(X) + \cdots + Q_\ell(X) f(X)^\ell = 0$ n'est pas nécessairement majoré par ℓ. La proposition suivante donne une condition suffisante pour que cette majoration soit vérifiée. Elle s'inspire directement du théorème 3 de [GS00].

Proposition 17. *Soit A un corps, soit θ un automorphisme de A et soit $R = A[X;\theta]$. Soit $Q(X,Y) = \sum_{s=0}^{\ell} Q_s(X) Y^s \in R[Y]$ and soit $H_0(Y) = \sum_{s=0}^{\ell} q_{s,0} Y^s \in A[Y]$. Si $H_0 \neq 0$ et si pour tout β dans A tel que $H_0(\beta) = 0$, on a*

$$\forall i \in \{1, \ldots, k-1\}, \Psi_0(\theta^i(\beta)) \neq 0$$

où $\Psi_0(Y) = H_0(Y)/(Y - \beta)$, alors $Q(X,Y)$ possède au plus ℓ racines dans R de degrés $< k$.

Démonstration. Soit $f(X) = \sum_{i=0}^{k-1} f_i X^i$ de degré $< k$ tel que $\sum_{s=0}^{\ell} Q_s(X) \cdot f(X)^s = 0$. D'après le théorème 1 de [GM65], il existe $B(X,Y)$ dans $A(X;\theta)[Y]$ tel que $Q(X,Y) = B(X,Y)(Y - f(X))$. De plus les coefficients de $B(X,Y)$ sont dans R car $Q_0, \ldots, Q_\ell, f$ sont dans R.

Les polynômes gauches $Q(X,Y)$, $B(X,Y)$ et $Y - f(X)$ peuvent être vus comme des polynômes de $A[Y][X;\sigma]$ où $\sigma : \sum a_i Y^i \mapsto \sum \theta(a_i) Y^i$:

$$Q(X,Y) = \sum_{i=0}^{d} H_i(Y) X^i = \underbrace{\left(\sum_{j=0}^{d-k+1} \Psi_j(Y) X^j \right)}_{B(X,Y)} \cdot \underbrace{\left(\sum_{j=0}^{k-1} \varphi_j X^j \right)}_{Y - f(X)}$$

où $\varphi_0 = Y - f_0$ et $\forall j \in \{1, \ldots, k-1\}, \varphi_j = -f_j$. De plus les polynômes H_j sont de degrés $\leq \ell$.

En développant et en regroupant les termes on obtient dans $A[Y]$: $\forall j \in \{0, \ldots, k-1\}$,

$$H_j(Y) = \Psi_0(Y)\varphi_j + \Psi_1(Y)\theta(\varphi_{j-1}) + \cdots + \Psi_j(Y)(Y - \theta^j(f_0)). \tag{3.4}$$

Pour $j = 0$, on a $H_0(Y) = \Psi_0(Y)\varphi_0(Y) = \Psi_0(Y)(Y - f_0)$. On en déduit que $H_0(f_0) = 0$ et qu'il y a au plus ℓ valeurs possibles pour f_0.

Fixons désormais f_0 tel que $H_0(f_0) = 0$ et considérons $\Psi_0(Y) = H_0(Y)/(Y - f_0)$. Supposons de plus que

$$\forall i \in \{1, \ldots, k-1\}, \Psi_0(\theta^i(f_0)) \neq 0$$

alors les coefficients f_j peuvent être déterminés de manière unique pour $j = 1, \ldots, k-1$. En effet, supposons $f_0, \ldots, f_{j-1}$ connus et $\Psi_0(Y), \ldots, \Psi_{j-1}(Y)$ connus. On a

$$H_j(\theta^j(f_0)) = \Psi_0(\theta^j(f_0))\varphi_j + \Psi_1(\theta^j(f_0))\theta(\varphi_{j-1}) + \cdots + \Psi_{j-1}(\theta^j(f_0))\theta^{j-1}(\varphi_1) + 0$$

donc

$$\varphi_j = \frac{H_j(\theta^j(f_0)) - \Psi_1(\theta^j(f_0))\theta(\varphi_{j-1}) - \cdots - \Psi_{j-1}(\theta^j(f_0))\theta^{j-1}(\varphi_1)}{\Psi_0(\theta^j(f_0))}. \tag{3.5}$$

De plus,

$$\Psi_j(Y) = \frac{H_j(Y) - (\Psi_0(Y)\varphi_j + \cdots + \Psi_{j-1}(Y)\theta^{j-1}(\varphi_1))}{Y - \theta^j(f_0)}.$$

donc $f_j = -\varphi_j$ et $\Psi_j(Y)$ sont déterminés de manière unique itérativement.

□

Exemple 17. *On considère le code d'évaluation tordue* $[9, 2, 8]_{25}$ *de support* $\underline{\alpha} = (a^2, a^{23}, 2, a^{13}, 0, 4, a^{19}, a^4, a^{21})$ *et de capacité de correction* $t = 3$ *(voir exemples 13, 14, 15). Supposons que* $\ell = 3$*, alors* $\tau = 5$.

Considérons $e = (a^{13}, 0, 0, a^5, 3, 0, a^8, 0, 0)$*. Le poids* $w_\alpha(e)$ *est égal à* 4.

Soient $f = a^4X + a^{15}$*,* $c = (f(\alpha_1), \ldots, f(\alpha_9)) = (a^{17}, 0, 1, a^8, a^{15}, a^{13}, a^{19}, a^{16}, a^4)$ *et* $r = c + e = (4, 0, 1, a^{15}, a, a^{13}, 1, a^{16}, a^4)$*. Le polynôme d'interpolation tordue* g *aux points* $(\alpha_i, r_i)_{1 \le i \le 9}$ *est* $g = 2X^8 + a^{14}X^7 + a^8X^6 + a^8X^5 + a^3X^4 + a^{11}X^3 + a^5X^2 + aX + 3$*. Le polynôme tordu* $G = \mathrm{gcrd}(g - f, g^2 - f^2, g^3 - f^3)$ *est égal à* $a^5X^4 + a^{21}X^3 + a^{15}X^2 + a^9X + 2$ *et on a* $w_\alpha(G(\alpha_1), \ldots, G(\alpha_9)) = 5 \le \tau$.

L'algorithme 3 fournit $Q_0(X) = a^{17}X^3 + a^8X^2 + a^7X + 1$*,* $Q_1(X) = a^2X^2 + 3X + 4$*,* $Q_2(X) = a^{14}X + a^{21}$ *et* $Q_3(X) = a^2$.

On considère le polynôme gauche $Q(X, Y) = Q_0(X) + Q_1(X)Y + Q_2(X)Y^2 + Q_3(X)Y^3 = a^{17}X^3 + a^8X^2 + a^7X + 1 + (a^2X^2 + 3X + 4)Y + (a^{14}X + a^{21})Y^2 + a^2Y^3 \in \mathbb{F}_{25}[X; \theta][Y]$.

On cherche les racines $f(X) = f_0 + f_1X$ *de* $Q(X, Y)$ *dans* $\mathbb{F}_{25}[X; \theta]$ *de degré strictement inférieur à* $k = 2$*. On a* $Q(X, Y) = H_0(Y) + H_1(Y)X + \cdots + H_3(Y)X^3 \in \mathbb{F}_{25}[Y][X; \sigma]$ *où* $\sigma : \sum a_iY^i \mapsto \sum a_i^5Y^i$*,* $H_0(Y) = a^2Y^3 + a^{21}Y^2 + 4Y + 1$ *et* $H_1(Y) = a^{14}Y^2 + 3Y + a^7$.

Pour chaque racine $\beta \in \{a, a^{15}, 3\}$ *de* $H_0(Y)$*, le polynôme* $\Psi_0(Y) = H_0(Y)/(Y - \beta)$ *ne s'annule pas en* $\theta(\beta) = \beta^5$*. Ainsi on a au plus trois solutions* $f(X)$.

D'après la relation (3.5), on obtient f_1 *de manière unique en fonction de* f_0 *en posant* $j = 1$ *:* $f_1 = -H_1(f_0^5)/\Psi_0(f_0^5)$*. Les solutions possibles sont donc* $a^{21}X + a$*,* $a^4X + a^{15}$ *et* $a^{13}X + 3$*. On vérifie que* $a^4X + a^{15}$ *est la seule racine du polynôme gauche* $Q(X, Y) \in \mathbb{F}_{25}[X; \theta]$ *de degré strictement inférieur à* 2.

4 Conclusion et perspectives

Nous avons vu dans cette partie que la métrique tordue s'adapte bien au décodage unique des codes d'évaluation tordue « par reste ». Par ailleurs elle ouvre des perspectives pour le décodage en liste qui demanderaient à être étudiées de plus près. La proposition 17 permet de calculer la liste des solutions $\mathcal{L}$ de l'algorithme 3 sous des hypothèses fortes. Il serait intéressant de chercher à généraliser cette construction en s'inspirant de [GS00] pour le calcul des séries solutions dans le cas commutatif. Une difficulté dans la généralisation de cet algorithme provient du fait que la structure des polynômes gauches n'est pas préservée lors de la recherche des séries solutions. Il serait alors probablement pertinent d'utiliser la représentation des polynômes 'généraux', tels qu'ils sont définis dans la section 3 de [GM65].

Bibliographie

[ALS16] Adel Alahmadi, André Leroy, and Patrick Solé. Long module skew codes are good. *Discrete Math.*, 339(5) :1624–1627, 2016.

[Aug03] Daniel Augot. Les travaux de Madhu Sudan sur les codes correcteurs d'erreurs. *Gaz. Math.*, (98) :5–13, 2003.

[BBB20a] Aicha Batoul, Delphine Boucher, and Rayna D. Boulanouar. A construction of self-dual skew cyclic and negacyclic codes of length n over $\mathbb{F}_{p^n}$. preprint, 2020.

[BBB20b] Rayna D. Boulanouar, Aicha Batoul, and Delphine Boucher. An overview on skew constacyclic codes and their subclass of lcd codes. accepted to Advances in Mathematics of Communications (AMC), 2020.

[BCG+17] Alin Bostan, Frédéric Chyzak, Marc Giusti, Romain Lebreton, Grégoire Lecerf, Bruno Salvy, and Éric Schost. *Algorithmes Efficaces en Calcul Formel*. Frédéric Chyzak (auto-édit.), Palaiseau, September 2017. 686 pages. Imprimé par CreateSpace. Aussi disponible en version électronique.

[Ber03] Thierry P. Berger. Isometries for rank distance and permutation group of Gabidulin codes. *IEEE Trans. Inform. Theory*, 49(11) :3016–3019, 2003.

[BGG+10] Delphine Boucher, Philippe Gaborit, Willi Geiselmann, Olivier Ruatta, and Felix Ulmer. Key exchange and encryption schemes based on non-commutative skew polynomials. In *Post-quantum cryptography*, volume 6061 of *Lecture Notes in Comput. Sci.*, pages 126–141. Springer, Berlin, 2010.

[BGU07] Delphine Boucher, Willi Geiselmann, and Felix Ulmer. Skew-cyclic codes. *Appl. Algebra Engrg. Comm. Comput.*, 18(4) :379–389, 2007.

[BL13] M'Hammed Boulagouaz and André Leroy. (σ, δ)-codes. *Adv. Math. Commun.*, 7(4) :463–474, 2013.

[Bou15] Delphine Boucher. A note on the existence of self-dual skew codes over finite fields. In *Codes, cryptology, and information security*, volume 9084 of *Lecture Notes in Comput. Sci.*, pages 228–239. Springer, Cham, 2015.

[Bou16] Delphine Boucher. Construction and number of self-dual skew codes over $\mathbb{F}_{p^2}$. *Adv. Math. Commun.*, 10(4) :765–795, 2016.

[Bou18] Delphine Boucher. A first step towards the skew duadic codes. *Adv. Math. Commun.*, 12(3) :553–577, 2018.

[Bou19] Delphine Boucher. An algorithm for decoding skew reed-solomon codes with respect to the skew metric. In *Workshop WCC19*, 2019. submitted to Design Codes and Cryptography.

[BP94] Manuel Bronshteĭn and Marko Petkovshek. Ore rings, linear operators and factorization. *Programmirovanie*, (1) :27–44, 1994.

[BSU08] Delphine Boucher, Patrick Solé, and Felix Ulmer. Skew constacyclic codes over Galois rings. *Adv. Math. Commun.*, 2(3) :273–292, 2008.

[BU09a] Delphine Boucher and Felix Ulmer. Codes as modules over skew polynomial rings. In *Cryptography and coding*, volume 5921 of *Lecture Notes in Comput. Sci.*, pages 38–55. Springer, Berlin, 2009.

[BU09b] Delphine Boucher and Felix Ulmer. Coding with skew polynomial rings. *J. Symbolic Comput.*, 44(12) :1644–1656, 2009.

[BU11] Delphine Boucher and Felix Ulmer. A note on the dual codes of module skew codes. In *Cryptography and coding*, volume 7089 of *Lecture Notes in Comput. Sci.*, pages 230–243. Springer, Heidelberg, 2011.

[BU14a] Delphine Boucher and Felix Ulmer. Linear codes using skew polynomials with automorphisms and derivations. *Des. Codes Cryptogr.*, 70(3) :405–431, 2014.

[BU14b] Delphine Boucher and Felix Ulmer. Self-dual skew codes and factorization of skew polynomials. *J. Symbolic Comput.*, 60 :47–61, 2014.

[Cha10] Lionel Chaussade. *Codes correcteurs avec les polynômes tordus.* PhD thesis, Université de Rennes 1, 2010. Thèse de doctorat dirigée par Ulmer, Felix Mathématiques et applications Rennes 1 2010.

[CHH04] Robert S. Coulter, George Havas, and Marie Henderson. On decomposition of sub-linearised polynomials. *J. Aust. Math. Soc.*, 76(3) :317–328, 2004.

[CLB17] Xavier Caruso and Jérémy Le Borgne. A new faster algorithm for factoring skew polynomials over finite fields. *J. Symbolic Comput.*, 79(part 2) :411–443, 2017.

[Coh85] Paul M. Cohn. *Free rings and their relations*, volume 19 of *London Mathematical Society Monographs.* Academic Press, Inc. [Harcourt Brace Jovanovich, Publishers], London, second edition, 1985.

[DGH97] Steven T. Dougherty, T. Aaron Gulliver, and Masaaki Harada. Extremal binary self-dual codes. *IEEE Trans. Inform. Theory*, 43(6) :2036–2047, 1997.

[Dou11] Steven T. Dougherty. The search for the [24k ; 12k ; 4k + 4] extremal type ii code. 2011. https ://sites.google.com/site/professorstevendougherty/files/survey.pdf.

[Fog16] Neville Lyons Fogarty. *On Skew-Constacyclic Codes.* ProQuest LLC, Ann Arbor, MI, 2016. Thesis (Ph.D.)–University of Kentucky.

[Gab85] È. M. Gabidulin. Theory of codes with maximum rank distance. *Problemy Peredachi Informatsii*, 21(1) :3–16, 1985.

[Gab04] Philippe Gaborit. *Codes auto-duaux et applications des codes.* Hdr, Université Limoges, 2004.

[Gie98] Mark Giesbrecht. Factoring in skew-polynomial rings over finite fields. *J. Symbolic Comput.*, 26(4) :463–486, 1998.

[GM65] Basil Gordon and Theodore S. Motzkin. On the zeros of polynomials over division rings. *Trans. Amer. Math. Soc.*, 116 :218–226, 1965.

[GO03] Philippe Gaborit and Ayoub Otmani. Experimental constructions of self-dual codes. *Finite Fields Appl.*, 9(3) :372–394, 2003.

[GS00] Shuhong Gao and M. Amin Shokrollahi. Computing roots of polynomials over function fields of curves. In *Coding theory and cryptography (Annapolis, MD, 1998)*, pages 214–228. Springer, Berlin, 2000.

[Huf98] W. Cary Huffman. Codes and groups. In *Handbook of coding theory, Vol. I, II*, pages 1345–1440. North-Holland, Amsterdam, 1998.

[Jac43] Nathan Jacobson. *The Theory of Rings*. American Mathematical Society Mathematical Surveys, vol. II. American Mathematical Society, New York, 1943.

[JLX11] Yan Jia, San Ling, and Chaoping Xing. On self-dual cyclic codes over finite fields. *IEEE Trans. Inform. Theory*, 57(4) :2243–2251, 2011.

[KYS14] Abidin Kaya, Bahattin Yildiz, and Irfan Siap. New extremal binary self-dual codes of length 68 from quadratic residue codes over $\mathbb{F}_2+u\mathbb{F}_2+u^2\mathbb{F}_2$. *Finite Fields Appl.*, 29 :160–177, 2014.

[Lam86] Tsit Y. Lam. A general theory of Vandermonde matrices. *Exposition. Math.*, 4(3) :193–215, 1986.

[LL88] Tsit Y. Lam and André Leroy. Vandermonde and Wronskian matrices over division rings. *Bull. Soc. Math. Belg. Sér. A*, 40(2) :281–286, 1988. Deuxième Contact Franco-Belge en Algèbre (Faulx-les-Tombes, 1987).

[Loi06] Pierre Loidreau. A Welch-Berlekamp like algorithm for decoding Gabidulin codes. In *Coding and cryptography*, volume 3969 of *Lecture Notes in Comput. Sci.*, pages 36–45. Springer, Berlin, 2006.

[MPn18] Umberto Martínez-Peñas. Skew and linearized Reed-Solomon codes and maximum sum rank distance codes over any division ring. *J. Algebra*, 504 :587–612, 2018.

[MS77] F. Jessie MacWilliams and Neil J. A. Sloane. *The theory of error-correcting codes*. North-Holland Publishing Co., Amsterdam-New York-Oxford, 1977. North-Holland Mathematical Library, Vol. 16.

[Odo99] Robert W. K. Odoni. On additive polynomials over a finite field. *Proc. Edinburgh Math. Soc. (2)*, 42(1) :1–16, 1999.

[Ore33] Oystein Ore. Theory of non-commutative polynomials. *Ann. of Math. (2)*, 34(3) :480–508, 1933.

[Ple98] Vera Pless. *Introduction to the theory of error-correcting codes*. Wiley-Interscience Series in Discrete Mathematics and Optimization. John Wiley & Sons, Inc., New York, third edition, 1998. A Wiley-Interscience Publication.

[Rob15] Gwezheneg Robert. *Gabidulin codes in characteristic 0 : applications to space-time coding*. Theses, Université Rennes 1, December 2015.

[ST83] N. J. A. Sloane and J. G. Thompson. Cyclic self-dual codes. *IEEE Trans. Inform. Theory*, 29(3) :364–366, 1983.

[vzGG13] Joachim von zur Gathen and Jürgen Gerhard. *Modern computer algebra*. Cambridge University Press, Cambridge, third edition, 2013.

[WZ13] Antonia Wachter-Zeh. *Decoding of block and convolutional codes in rank metric*. PhD thesis, 2013. Thèse de doctorat dirigée par Loidreau, Pierre et Bossert, Martin Mathématiques et applications Rennes 1 2013.