ROYAUME DU MAROC
Université Mohammed V - RABAT -
جامعة محمد الخامس – الرباط –
Faculté des sciences
كلية العلوم

Université de Bretagne Occidentale

CENTRE D'ETUDES DOCTORALES - SCIENCES ET TECHNOLOGIES

N° d'ordre : CT 25

THÈSE DE DOCTORAT

Structure de recherche : Lab-MIA, LAB-STICC, CREC.

Discipline : Mathématiques et Applications.

Spécialité : Cryptographie.

Présentée et soutenue le 23/06/2016
par :

Soukayna QARBOUA

Approche quaternaire des fonctions cryptographiques, *fonctions booléennes et conjecture de Tu & Deng*

Devant le jury composé de :

Philippe LANGEVIN	PU, Université de Toulon et du Var, Toulon	Président
Saïd El HAJJI	PES, Faculté des Sciences, Université Mohammed V de Rabat	Directeur de Thèse
Caroline FONTAINE	CR CNRS HDR Télécom Bretagne, Brest	Co-directrice de Thèse
Patrice PARRAUD	*MCF Ecoles de Saint-Cyr Coëtquidan, Guer*	*Encadrant.*
Sihem MESNAGER	*MCF*, HDR Université Paris 8, Paris	Rapporteur
Patrick SOLÉ	DR CNRS, Télécom ParisTech, Paris	Rapporteur
El Mamoun SOUIDI	PES, Faculté des Sciences, Université Mohammed V de Rabat	Examinateur
François RECHER	MCF, Université de Lille 1, Lille	Examinateur

Année universitaire : **2015-2016**

. Faculté des Sciences, avenue Ibn Battouta, BP. 1014 RP, Rabat –Maroc
. 00212 (05) 37 77 18 76 00212(05) 37 77 42 61; http://www. fsr.um5.ac.ma

Remerciements

Les résultats présentés dans ce document sont le fruit de mes quatre années de thèse, de 2012 à 2016, au sein du Lab-STICC/CREC/LabMIA. Mes travaux de recherche s'inscrivent sous forme d'une co-tutelle de thèse Franco-Marocaine entre l' Université Mohammed V de Rabat, Faculté des Sciences, Télécom Bretagne , Site Technopôle de Brest-iroise (UBO), et les Écoles de Saint-Cyr Coëtquidan. Au cours de ma préparation de thèse j'ai bénéficié d'une bourse d'excellence octroyée par le Centre National de la Recherche Scientifique et Technique (CNRST) dans le cadre du programme des bourses de recherche initié par le Ministère de l'éducation Nationale, de l'enseignement Supérieur, de la Formation des Cadres et de la Recherche Scientifique et, une demi bourse de région octroyée par la région de Bretagne. Ce travail a à été réalisé au sein du laboratoire de recherche LabMIA sous la direction de M. Said EL HAJJI, professeur de l'enseignement supérieur à la faculté des Sciences de Rabat et, la co-direction de Mme. Caroline FONTAINE chargée de recherche au CNRS, Télécom Bretagne, Brest, France et, le co-encadrement de M. Patrice PARRAUD Maitre de conférence aux Écoles de Saint-Cyr Coëtquidan GUER.

Mes sincères remerciements s'adresse à Mme. Caroline FONTAINE, qui a accepté de codiriger ma thèse. Elle m'a présenté un soutien tout au long de mes quatre années de thèse et à su être présente aux moments les plus difficiles.

Je tiens également à exprimer toute ma gratitude à mon directeur de thèse M. Saïd EL HAJJI pour avoir accepter de diriger cette thèse. Non seulement, parce qu'il m'a donné la chance de travailler sur un sujet qui me passionne mais aussi pour toutes les heures qu'il a passé à écouter mes idée et à me conseiller.

Je remercie fortement M. Patrice PARRAUD, Maître de conférence aux Écoles de Saint-Cyr Coëtquidan, pour m'avoir encadré depuis mon projet de fin d'étude, sans son aide hors paire à , me relire, m'aider dans la rédaction des preuves et, des divers documents que j'ai été amenée à produire, je peux affirmer que mon travail ne serait certainement pas ce qu'il est aujourd'hui

sans cette précieuse aide.

Je remercie tout d'abord M. Philippe LANGEVIN, professeur des universités à l'université de Toulon, pour m'avoir fait l'honneur de présider le jury de cette thèse.

Je tiens à remercier Mme. Sihem MESNAGER, maître de conférence et habilité à dirigé une thèse à l'Université de Paris 8 pour avoir accepté de devenir rapporteur de cette thèse, et pour ses précieux conseils.

Je tiens à remercier M. Patrick SOLÉ Directeur de recherche au CNRS ParisTech, pour avoir accepté de devenir rapporteur de cette thèse ainsi que pour ses conseils avisés.

Je remercie M. El mamoum SOUIDI, PES à la Faculté des Sciences de Rabat, pour son déplacement afin d'examiner ma thèse ainsi que pour ses remarques constructives.

Un grand merci à M. François RECHER, MCF à l'Université de Lille 1 Pour avoir accepter de devenir examinateur de ma thèse.

Je tiens à remercier toutes les personnes qui ont rendu ces quatre années de thèse particulièrement enrichissantes. D'une part, ceux avec qui j'ai travaillé et qui ont directement contribué à mes travaux scientifiques et à l'élaboration de ce document, mais aussi tous les autres avec qui j'ai passé de bons moments et qui m'ont ainsi permis de réfléchir dans les meilleures conditions.

Je remercie tous les autres membres permanents de Macclia pour leurs disponibilités, leurs conseils avisés et toutes les discussions que nous avons pu avoir. Dans le désordre, Zoubida Jadda, Bertrand Galpin, Gregory Girault , Eric Jacopin, Jérémy Buisson, Stéphane Cardon.

Je remercie tous les membres permanents du Dépt. Image et Traitement Information pour leurs disponibilités, leur accueil chaleureux et toutes les discussions que nous avons pu avoir. Tout particulièrement , Basel Solaiman, Gwenaël Brunet, Didier Gueriot, Jean-Marc Le caillec, Christophe Sintes, Stéphane Cardon. Merci aussi à Corinne Le lann pour tout son travail administratif et sa compagnie de tous les jours au projet.

Je remercie Alex, Ramona, Pédro, Julien, Guillaume, Marisnel et Brahim qui, plus que des collègues de travail, sont devenus de véritables amis. Un grand merci à toutes ces personnes merveilleuses qui ont contribué à rendre la vie au laboratoire si animée.

Je tiens à remercier Sihem Mesnager et Patrick Solé pour avoir accepté d'être rapporteurs de ma thèse ainsi que Philippe Langevin, François Recher et El Mamoun Souidi de faire partie de mon jury.

Avant de finir je voudrais également exprimer ma profonde gratitude à toutes ces familles Françaises pour m'avoir accueilli à bras ouvert et fait

découvrir les multiples facettes de la culture française (Guilhon, Thiedey, Parraud, Jadda).

Je remercie également tous mes amis de leur présence. Merci donc à Bénédicte Parraud, Dounia, Nada, Foufina, Nora, Maha, Sylvain, Camille, Julie, Ben et Pierre François merci pour tous les moments de bonheurs que nous avons partagés (Haute- fenderie-family).

Les dernières lignes de ces remerciements vont à mon bien le plus precieux, ma famille. Votre soutien a été inconditionnel, merci donc à mes parents, mes grands parents et mes frères (Hicham, Anas, Simo et Adil).

Résumé

Cette thèse porte sur la conception et d'analyse d'objet mathématique utile en cryptographie, plus précisément, sur la conception de fonctions vérifiant un certain nombre de critères pour être utilisées dans un contexte de chiffrement symétrique. De toute évidence, les propriétés de ces fonctions sont essentielles pour les exigences de sécurité du système final qui les utilise. Et suite, à l'évolution permanente du domaine de la cryptanalyse et l'apparition de nouvelles attaques, la conception de fonctions cryptographiques reste en constante évolution. Naturellement, ceci implique de nouvelles restrictions sur les classes de fonctions adoptées et rend parfois obsolètes les familles de fonctions connues. Par ailleurs, ces critères présentent des incompatibilités, et des compromis doivent être considérés. Dans la première partie de cette thèse, nous donnons une description du contexte d'utilisation des fonctions booléennes dans le chiffrement à flot et définissons les propriétés cryptographiques retenues pour cette recherche, ainsi que les attaques correspondantes. En suite, nous nous intéressons aux fonctions booléennes courbes, aux fonctions quaternaires courbes, aux fonctions courbes généralisées, et exhibons les connexions entre les mondes quaternaire et binaire. Ceci nous permet de construire des fonctions booléennes courbes par projections de fonctions quaternaires particulières. Dans cette thèse nous construisons des classes infinies de fonctions booléennes répondent à la plupart des critères requis pour le chiffrement à flot, et étudions une conjecture combinatoire (Tu and deng) dont la validité conditionne l'immunité algébrique des classes infinies de fonctions étudiées dans ce manuscrit.

Mots-clefs : Fonctions Booléennes, Fonctions quaternaires, Propriétés cryptographiques, Conjecture de Tu & Deng, Anneau de Galois.

Abstract

The core of this thesis is the study of some mathematical objects or problems of interest in cryptology. The linear complexity of sequences is one of the important security measures for stream cipher systems. Recently, in the study of vectorized stream cipher systems, Bent functions have been generalized to the alphabet and also studied by several authors. This generalization maps the classical definition of binary bent functions to generalized bent functions. Among all known constructions of generalized bent functions not a lot matter about their binary projection. In the first part we present a state of the art around boolean functions, generalized functions, and associated combinational conjectures. The second part is devoted to our scientific contributions. We begin with a new construction of a family of m-variables quaternary bent functions over Galois ring and cyclotomic classes using an intern function defined on a particular splitting of the Teichmuller system. Using a particular binary projection map we obtain a family of 2m-variables Boolean bent functions and a family of -variables Boolean functions with maximal nonlinearity equal to . To design robust symmetric encryption schemes, we need to use Boolean functions with suitable properties. Among the security criteria these functions need to fulfill, we can mention algebraic immunity. A lot of papers study how to construct suitable functions, but some of them assume the validity of Tu- Deng's combinatorial conjecture to estimate the algebraic immunity of the Boolean functions they design. The last chapter of this part is devoted to the study of a combinatorial conjecture whose validity entails the existence of infinite classes of Boolean functions with good cryptographic properties. Although the conjecture seems quite innocuous, its validity remains an open question. We prove two new results about this conjecture and point out a new family of integers that satisfy it. However, we sincerely hope that the theoretical and experimental results presented here will give the reader a good insight into the conjecture.

Key Words : Quaternary functions , Boolean functions, security criteria, Galois ring, combinatorial conjecture,

Table des matières

Introduction

Le monde de la cryptologie est divisé en deux parties. D'une part, la cryptographie : l'art de concevoir des algorithmes, des protocoles et des systèmes aussi robustes et sécurisés que possible. D'autre part, la cryptanalyse : l'art de détecter des défauts de conception dans ces systèmes et le développement des attaques mettant en péril la sécurité présumée de ces systèmes. De manière générale, plus les attaques développées par les cryptanalystes sont puissantes, plus il est difficile pour les cryptographes de proposer des constructions appropriées. En particulier, la plupart des constructions cryptographiques reposent en quelque sorte sur la difficulté à résoudre des problèmes mathématiques, d'un point de vue théorique et/ou informatique. Le monde de la cryptologie est donc une source inépuisable de problèmes mathématiques. Aujourd'hui, il existe deux façons typiques pour assurer la sécurité des communications : la cryptographie symétrique où les deux parties légitimes partagent un secret commun, et la cryptographie asymétrique où seule une partie possède un tel secret. Dans ce dernier cas, certaines données publiques sont associées au secret, et rendent possible la transmission sécurisée d'informations dans une direction unique. Dans ce mémoire nous allons nous intéresser à la cryptogra-

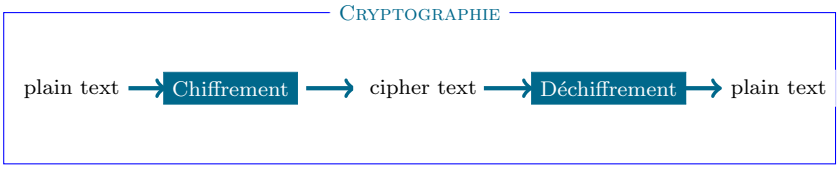

Figure 1 – <Chiffrement>

phie symétrique. La motivation de la recherche présentée dans ce manuscrit est d'étudier et construire des objets mathématiques vérifiant des propriétés appropriées pour être utilisées dans un contexte de chiffrement symétrique.

Les fonctions booléennes constituent des blocs de construction couramment utilisés dans la conception de systèmes cryptographiques symétriques, en particulier dans le chiffrement à flot. De toute évidence, les propriétés de

ces fonctions sont essentielles pour les exigences de sécurité du système final qui les utilise. En effet, si la fonction n'est pas soigneusement choisie, l'utilisation d'une fonction booléenne présentant des faiblesses peut mettre en péril l'ensemble du système. Par conséquent, plusieurs propriétés cryptographiques sur les fonctions booléennes ont été définies et étudiées pour assurer l'immunité du système face aux différents types d'attaques. Au départ, les fonctions booléennes ont été largement étudiées en raison de leur liaison avec la théorie des codes correcteurs. Leurs propriétés sont étroitement liées aux propriétés des codes cycliques. Suite à l'évolution permanente du domaine de la cryptanalyse et l'apparition de nouvelles attaques, la conception de fonctions booléennes reste en constante évolution. Naturellement, ceci implique de nouvelles restrictions sur les classes de fonctions booléennes adoptées et rend parfois obsolètes les familles de fonctions connues. Par ailleurs, ces critères présentent des incompatibilités, et des compromis doivent être considérés. Ainsi, il devient de plus en plus difficile de construire, ou même de caractériser des fonctions booléennes satisfaisant tous les critères.

Motivation et axes de recherche

Dans la première partie de cette thèse, nous donnons une description un peu plus formelle du contexte d'utilisation des fonctions booléennes dans le chiffrement à flot et définissons les propriétés cryptographiques suivantes : équilibre, degré algébrique, immunité algébrique, résistance aux attaques algébriques rapides, et haute non-linéarité. Les attaques correspondantes seront également mentionnées, mais pas décrites. Pour une présentation plus complète et plus approfondie, nous renvoyons le lecteur au chapitre de Carlet [Car10a] sur les fonctions booléennes pour la cryptographie et les codes correcteurs d'erreurs. Ensuite, nous nous intéressons tout particulièrement aux fonctions booléennes courbes, aux fonctions quaternaires courbes et aux fonctions courbes généralisées. La notion de fonctions booléennes courbes a été introduite par Rothaus, dans les années 70, [Rot76]. Les fonctions booléennes courbes sont les fonctions dont la distance de Hamming avec le code de Reed-Muller d'ordre 1 est maximale. Plus tard, cette notion a été généralisée par Kumar et al. dans [KSW85] à l'alphabet $\mathbb{Z}_q$ et étudiée par Nyberg [Nyb91]. Les définitions classiques des fonctions booléennes courbes mènent, à travers cette généralisation, aux notions des fonctions courbes généralisées. Les fonctions quaternaires courbes constituent un cas particulier des fonctions courbes généralisées. L'intérêt pour cette classe particulière de fonctions a pris de l'ampleur après l'apparition des travaux de Hammons et al. dans [HKC+94] sur la $\mathbb{Z}_4$-linéarité des codes de *Kerdock*, *Preparata*, *Goethals*

et codes associés. En 2009, Solé et Tokareva [ST09] ont étudié les liens directs entre les fonctions booléennes courbes, les fonctions booléennes courbes généralisées [Sch07] et les fonctions quaternaires courbes. Ils ont aussi étudié les images par la fonction de *Gray* des fonctions courbes. Nous allons nous intéresser dans un premier temps aux connexions entre les mondes quaternaire et binaire. Tout particulièrement, à la relation entre les fonctions quaternaires dites *courbes* et leurs homologues booléennes. Construire des fonctions booléennes satisfaisant les critères cryptographiques, voire prouver leur existence, est une tâche rude mais pas impossible. Aussi une des motivations de ce travail est de pouvoir construire des fonctions booléennes courbes par projections de fonctions quaternaires particulières.

Les incompatibilités entres les différents critères cryptographiques pourraient laisser croire que la construction de fonctions booléennes satisfaisant tous les critères cryptographiques est hors de portée. Heureusement, ce n'est pas le cas. Nous nous intéresserons dans cette thèse à des classes infinies de fonctions booléennes qui répondent à la plupart des critères requis pour le chiffrement à flot. Pour conclure, nous devons affirmer que notre intérêt pour ces familles de fonctions ne réside pas seulement dans le fait qu'elles donnent une réponse positive et concrète aux problèmes cryptographiques, mais aussi dans le fait que l'une de leurs propriétés : l'immunité algébrique dépend de la validité d'une conjecture combinatoire qui sera étudiée dans la deuxième partie de cette thèse.

Aperçu de la thèse

Les résultats présentés dans ce document sont le fruit de mes quatre années de thèse, de 2012 à 2016, au sein du Lab-STICC/CREC/LabMIA. Ces travaux, appartenant au domaine de la cryptographie ont fait l'objet de plusieurs publications :

[JPQ13] Zoubida Jadda, Patrice Parraud et Soukayna Qarboua. Quaternary cryptographic bent functions and their binary projection, Cryptography and Communications 5,1, 49–65,2013.

[SQF16] Soukayna Qarboua, Julien Schrek, Caroline Fontaine New results about Tu-Deng's conjecture, conference, IEEE International Symposium on Information Theory, ISIT, 2016.

Nous commençons ce manuscrit par une première partie état de l'art autour des fonctions booléennes, des fonctions généralisées et des conjectures

combinatoires associées. L'ordre des chapitres des états de l'art est choisi de manière à suivre l'ordre chronologique des contributions.

1. Dans le chapitre 1 on donne quelques notations et bases mathématiques sur les corps finis et les anneaux de Galois $GR(4, m)$.
2. Le chapitre 2 est consacré aux notions de fonctions courbes généralisées, les fonctions généralisées parfaitement non-linéaires et le cas particulier des fonctions quaternaires. Nous présentons aussi quelques constructions de fonctions quaternaires courbes et ou parfaitement non-linéaires.
3. Dans le chapitre 3 nous donnons une description du contexte d'utilisation des fonctions booléennes dans le chiffrement à flot et définissons un ensemble de propriétés cryptographiques. Les attaques correspondantes sont également mentionnées et des familles de fonctions booléennes dont l'immunité algébrique dépend de conjectures combinatoires.
4. Dans le chapitre 4 nous exposons brièvement les travaux effectués sur ces conjectures.

Dans la seconde partie de ce manuscrit nous présentons nos contributions de la façon suivante.

1. Dans le chapitre 5 nous exposons nos premiers résultats : la construction et modélisation d'une nouvelle famille de fonctions quaternaires courbes à m-variables définies sur un anneau de Galois $R = GR(4, m)$.
2. Puis, en utilisant une projection binaire, différente de l'usuelle fonction de Gray, et l'écriture 2-adique des éléments, et en exploitant le relèvement de Hensel nous obtenons deux nouvelles familles de fonctions booléennes. Une première famille de fonctions booléennes courbes à $2m$-variables et une seconde famille de fonctions booléennes à $(2m+1)$-variables de non-linéarité maximale ces résultats sont décrits dans le chapitre 6.
3. Enfin dans le (dernier) chapitre 7 nous étudions la conjecture de Tu et Deng et nous obtenons deux résultats généraux et une nouvelle famille d'entiers t vérifiant la conjecture. Le premier résultat est une formule pour calculer le cardinal de l'ensemble $S_t(i)$ qui se présente comme suit :

$$|S_t(i)| = \sum_{(x_0,\ldots,x_{w-1})\in E_t \text{ et } \sum_{i=0}^{w-1} x_i = i} 2^i \prod_{x_i=-1} 4 - 2\delta_{k-w}(i)$$

Comme deuxième résultat nous avons établi que : $P_t = P_{m(t)}$. Enfin, pour conclure nous en déduisons que la famille d'entiers construits

Première partie

État de l'art

Chapitre 1

Préliminaires

L'objet de ce chapitre est de présenter certains outils ou notions de base (les anneaux de Galois, les corps finis) qui seront utilisées dans les chapitres suivants. Il s'agit donc avant tout de donner, ou rappeler, quelques définitions et propriétés permettant une compréhension plus aisée de la thèse. Nous commençons ce manuscrit par rappeler quelques notions importantes sur les corps finis et anneaux de Galois dans le but de clarifier au maximum l'aspect technique de nos contributions. Toutes les notions et propriétés exposées dans cette section sont tirées des ouvrages de McEliece [McE87] et de Lidl et Niederreiter [LN83]. Nous commencerons ce chapitre par exposer quelques notions générales sur les corps finis à $q = p^n$ éléments, avec p un nombre premier et n un entier quelconque. Nous utiliserons la notation standard $\mathbb{F}_{p^n}$ et nous définirons les notions suivantes : polynôme irréductible, racine primitive, fonction trace. Pour les besoins des chapitres sur les fonctions booléennes nous travaillerons la plupart du temps en *caractéristique* $p = 2$. En suite, nous nous intéresserons à $\mathbb{Z}_4^m$ qui admet une structure d'anneaux de Galois. Cette structure va être largement utilisée dans les constructions des fonctions quaternaires.

1.1 Généralités et notations sur $\mathbb{F}_{p^n}$

Caractérisation d'un corps fini

Un corps fini $\mathbb{F}$ est un ensemble fini d'éléments muni de deux lois de composition internes, notées '$+$' et '$\cdot$' vérifiant : $\mathbb{F}$ est un groupe commutatif pour la loi '$+$' d'élément neutre 0, $\mathbb{F}^*$ est un groupe pour la loi '$\cdot$' et telles que la loi '$\cdot$' est associative et distributive par rapport à la loi '$+$'.
Un corps fini est entièrement déterminé, à isomorphisme près, par son *cardi-*

nal, qui est toujours une puissance d'un nombre premier, ce nombre premier étant sa *caractéristique*.
Pour tout nombre premier p et tout entier non nul n, il existe un corps de cardinal p^n, qui se présente comme l'unique extension de degré n du corps premier $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Le corps fini le plus petit est le corps $\mathbb{F}_2 = \{0, 1\}$. Ce corps fait partie des corps dits *premiers* définis pour un p premier par :

$$\mathbb{F}_p = \{0, 1, \ldots, p-1\}, \text{ avec une arithmétique modulo p.}$$

Tous les autres corps finis de la forme $\mathbb{F}_{p^n}$ vont être des extensions algébriques de ces corps. Pour tout nombre premier p et tout $n \in \mathbb{N}^*$, il y a donc existence et unicité, à isomorphisme près, d'un corps à p^n éléments. Ce corps est noté $\mathbb{F}_{p^n}$ ou $GF(p^n)$ (corps de Galois). Ce corps est le corps de décomposition sur $\mathbb{F}_p$ du polynôme $X^{p^n} - X$.

Représentation des éléments d'un corps fini Les corps finis de caractéristique p et de cardinal p^n peuvent être définis à l'aide de la notion des polynômes irréductibles.

Définition 1.1.1. *(Polynôme irréductible). Soit P un polynôme de degré n à coefficients dans un corps K. Le polynôme P est dit* irréductible *sur K si ses seuls diviseurs dans K sont 1 et P.*

Théorème 1.1.1. *Soient p premier et n un entier naturel, il existe un unique (à isomorphisme près) corps fini à $q = p^n$ éléments. Il est défini par*

$$\mathbb{F}_q = \mathbb{F}_p[X]/(P(X))$$

avec P(X) un polynôme irréductible de degré n dans $\mathbb{F}_p$.

Un corps premier de caractéristique p et de cardinal p^n peut aussi être vu comme une extension algébrique de son corps premier par adjonction d'une racine α du polynôme P, d'ordre $p^n - 1$ (où l'ordre est le plus petit entier d tel que $\alpha^d = 1$).

Un polynôme irréductible P de degré n à coefficients dans le sous corps premier $\mathbb{F}_p$ possède n racines dans $\mathbb{F}_{p^n}$. De plus, les fonctions $\sigma_i : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$, définies par $\sigma_i(x) = x^{p^i}$ sont des automorphismes de corps qui laissent le sous corps premier invariant (automorphisme de Frobenius).

Nous allons maintenant introduire la fonction trace sur le corps fini $\mathbb{F}_{p^n}$.

Définition 1.1.2 (Trace)**.** *Nous appelons* fonction trace *l'application de $\mathbb{F}_{p^n}$ dans $\mathbb{F}_p$ définie par*

$$tr(\alpha) = \sum_{i=0}^{n-1} \sigma_i(\alpha). \tag{1.1.1}$$

L'application trace est une application linéaire sur $\mathbb{F}_p$.

1.2 Généralités et notations sur $GR(4, m)$

Dans cette section nous donnons quelques notations, définitions et propriétés de l'anneau de Galois $GR(4, m)$ sans preuve. Pour plus de détails sur les anneaux de Galois le lecteur peut consulter [McD74a].

Nous nous intéressons tout particulièrement à l'ensemble $\mathbb{Z}_4 = \mathbb{Z}/4\mathbb{Z} = \{0, 1, 2, 3\}$ l'anneau des entiers modulo 4. L'anneau $\mathbb{Z}_4$ est isomorphe au groupe des racines 4-ième de l'unité dans $\mathbb{C}$, noté $\mathcal{U}_4 = \{\pm 1, \pm i\}$: soit i une racine primitive 4-ième de l'unité ($\mathcal{U}_4$ est engendré par i), alors $\mathbb{Z}_4$ est isomorphe à $\mathcal{U}_4$ par l'isomorphisme standard $x \to i^x$. L'anneau $\mathbb{Z}_4$ est un anneau local, son unique idéal maximal est $2\mathbb{Z}_4$ qui est l'ensemble des diviseurs de zéro.

Soit m un entier naturel, l'ensemble $\mathbb{Z}_4^m$ est l'ensemble de tous les m-uplets à coefficients dans $\mathbb{Z}_4$. L'addition dans $\mathbb{Z}_4$ (addition $\pmod 4$) sera notée $+$. L'ensemble $\mathbb{Z}_4^m$ peut aussi être vu comme un anneau de Galois à l'aide de la notion de *b-polynôme*. Considérons $P \in \mathbb{Z}_4[X]$, P est un *b-polynôme* sur $\mathbb{Z}_4$ s'il est unitaire et $\bar{P}$ est un polynôme irréductible sur $\mathbb{F}_2$, où $\bar{P}$ est le polynôme obtenu par la réduction modulo 2 des coefficients du polynôme P. Le passage entre les polynômes primitifs sur $\mathbb{F}_2$ est les b-polynômes sur $\mathbb{Z}_4$ est appelé "*relèvement de Hensel*".

Proposition 1.2.1. *Soit P un b-polynôme de degré m sur $\mathbb{Z}_4$. L'anneau de Galois $R = GR(4, m)$ est défini à isomorphisme près comme $\mathbb{Z}_4[x]/(P)$.*

Soit $P \in \mathbb{Z}_4[x]$ un b-polynôme de degré m. Le polynôme P est un facteur primitif de $X^{2^m-1} - 1$. Considérons maintenant β une racine primitive d'ordre $2^m - 1$ de P. Alors, l'anneau de Galois $GR(4, m)$ est isomorphe à l'extension d'ordre m, notée $\mathbb{Z}_4[\beta]$. L'anneau de Galois R est un anneau d'ordre 4^m. L'ensemble des diviseurs de zéro de R, noté D, est d'ordre 2^m. Son groupe multiplicatif $R^* = R \setminus D$ est un groupe d'ordre $(2^m - 1)2^m$. Le groupe multiplicatif R^* est le produit direct $\mathcal{H} \times \mathcal{U}$, avec $\mathcal{H}$ le groupe cyclique d'ordre $(2^m - 1)$ généré par β, et $\mathcal{U}$ le groupe abélien des unités d'ordre 2^m de R (les éléments de $\mathcal{U}$ sont de la forme $1 + 2z_0$ avec z_0 dans $\mathcal{T}$). Ainsi, $R^* = \{z_1(1 + 2z_0),\ z_0 \in \mathcal{T}, z_1 \in \mathcal{T} \setminus \{0\}\}$. Il existe deux représentations possibles des éléments de R : la représentation multiplicative et la représentation additive.

La première représentation des éléments de R est appelée représentation 2-adique,

$$\forall z \in R,\ \exists!\ x_1, x_2 \in \mathcal{T} \textbf{ tels que } z = x_1 + 2x_2. \tag{1.2.1}$$

Cette écriture est unique et découle directement du fait que $R = \mathcal{H} \times \mathcal{U}$. Les éléments de l'anneau R peuvent aussi s'écrire de manière additive en exploitant l'isomorphisme entre R et $\mathbb{Z}_4[\beta]$

$$\forall z \in R,\ z = \sum_{i=0}^{m-1} z_i \beta^i,\ z_i \in \mathbb{Z}_4. \tag{1.2.2}$$

De plus, R est une extension d'anneau d'ordre m de $\mathbb{Z}_4$ et son groupe cyclique de Galois d'ordre m est généré par l'automorphisme de Frobenius, noté ψ et donné par : $\psi(z) = z_1^2 + 2z_2^2$. Ainsi, l'application trace sur R et à valeur dans $\mathbb{Z}_4$, est définie par :

$$Tr(z) = \sum_{l=0}^{m-1} \psi^l(z) = \sum_{l=0}^{m-1} z_1^{2^l} + 2 \sum_{l=0}^{m-1} z_2^{2^l}. \tag{1.2.3}$$

Pour finir, le corps des classes résiduelles $K = R/D$ [Yam90] est isomorphe à $\mathbb{F}_{2^m}$ sous l'application canonique $\mu : z \mapsto \bar{z}$ de R dans K.

$$\begin{array}{ccc} R = GR(4,m)_{b-poly} & \xrightarrow{\mu} & GF(2^m)_{poly_irr} \\ \downarrow Tr & & \downarrow tr \\ \mathbb{Z}_4 & \xrightarrow{\mu} & \mathbb{F}_2 \end{array},$$

avec tr la trace relative au corps $K = GF(2^m)$ dans $\mathbb{F}_2$ et Tr la trace absolue de R vers $\mathbb{Z}_4$.

Chapitre 2

Fonctions quaternaires

Ce chapitre s'articule autour de l'existence de connexions entre les mondes quaternaire et binaire. Nous nous intéresserons tout particulièrement à la relation entre les fonctions quaternaires dites *courbes* et leurs homologues booléennes. Construire des fonctions booléennes satisfaisant les critères cryptographiques, voire prouver leur existence, est une tâche rude. De plus, ces critères présentent des incompatibilités comme nous le verrons dans le chapitre 3. Aussi, une des motivations de ce travail et de pouvoir construire des fonctions booléennes courbes par projections de fonctions quaternaires particulières.

La notion des fonctions booléennes courbes (*"bent"* en anglais) introduite par Rothaus [Rot76] dans les années 70, a reçu beaucoup d'attention. Les fonctions booléennes courbes sont les fonctions dont la distance de Hamming avec le code de Reed-Muller d'ordre 1 ($i.e$ l'ensemble de toutes les fonctions affines) est maximale. Nous disons qu'une fonction booléenne f est parfaitement non linéaire si la fonction booléenne $f(x)+f(x+s)$ est équilibrée pour tout s dans $\mathbb{F}_2^n$. Dans le monde des fonctions booléennes ces deux notions sont équivalentes.

Plus tard, la notion de fonction courbe a été généralisée par Kumar et al. dans [KSW85] à l'alphabet $\mathbb{Z}_q$ et étudiée par Nyberg [Nyb91]. Les définitions classiques des fonctions booléennes courbes mènent, à travers cette généralisation, aux notions des fonctions courbes généralisées et des fonctions q-aire de non-linéarité parfaite. Les deux notions de fonctions courbes et ou non-linéarité parfaite ont été généralisées sur les anneaux.

Nous commencerons ce chapitre par une section portant sur les fonctions courbes généralisées et les fonctions de non linéarité parfaite. Ensuite, nous décrirons le cas particulier des fonctions quaternaires et nous donnerons quelques notions supplémentaires sur la non linéarité sous les métriques de *Hamming* et de *Lee*. Nous finirons ce chapitre par la présentation quelques

liens déjà établis entre les transformées de *Walsh* des fonctions quaternaires à m variables et des fonctions booléennes à $2m$ variables.

2.1 Généralisation sur $\mathbb{Z}_q^m$

En 1970, les fonctions booléennes courbes eurent beaucoup de succès. Notamment pour la particularité de leur coefficients d'auto-corrélation hors-phase qui se trouvent être nuls. Les fonctions courbes possèdent une complexité linéaire maximale et des propriétés d'auto-corrélation quasi optimales. Elles étaient utilisées dans la construire des familles de séquences binaires possédant des propriétés adaptées pour des application dans les codes des communications à accès multiples. La motivation première de Kumar et al. dans [KSW85] est de prolonger les deux notions de non-linéarité parfaite et de fonctions courbes à un alphabet plus large, $\mathbb{Z}_q = \mathbb{Z}/(q\mathbb{Z})$, construisant ainsi des séquences sur $GF(p^n)$.

Fonctions cryptographiques généralisées

Soit q un entier, $\mathbb{Z}_q$ l'ensemble des entiers modulo q, et $u = \exp^{i\frac{2\pi}{q}}$ la q-ième racine de l'unité dans $\mathbb{C}$, avec $i = \sqrt{-1}$. Une *fonction q-aire à m variables* est toute application de $\mathbb{Z}_q^m$ dans $\mathbb{Z}_q$. Une fonction q-aire est *équilibrée* si elle prend toutes les valeurs de $\mathbb{Z}_q$ le même nombre de fois [CD01].

Transformée de *Walsh*

Introduisons maintenant la transformée de *Walsh*. Cette fonction va servir essentiellement à caractériser la notion de de fonctions q-aire à m variables courbes généralisées et de parfaite non linéarité généralisées. La transformée de *Walsh* d'une fonction $f : \mathbb{Z}_q^m \to \mathbb{Z}_q$ est la transformée de *Fourier* de χ_f ; la fonction à valeurs complexes définie par : $\forall x \in \mathbb{Z}_q^m,\ \chi_f(x) = (u)^{f(x)}$.

$$\hat{\chi_f}(w) = \sum_{x\in\mathbb{Z}_q^m} \chi_f(x)(u)^{-w\cdot x},\ w \in \mathbb{Z}_q^m, \tag{2.1.1}$$

$$= \sum_{x\in\mathbb{Z}_q^m} (u)^{f(x)-w\cdot x},\ w \in \mathbb{Z}_q^m, \tag{2.1.2}$$

où " $\cdot$ " désigne le produit scalaire usuel dans $\mathbb{Z}_q^m$.

Avant d'énoncer la deuxième propriété, rappelons ce qu'est le produit de convolution de deux fonctions complexes ϕ et ξ :

$$(\phi \otimes \xi)(w) = \sum_{x \in \mathbb{Z}_q^m} \phi(w-x)\xi(x) \ , \ \forall w \in \mathbb{Z}_q^m. \tag{2.1.3}$$

Considérons, ϕ et ξ deux fonctions complexes. La transformée de *Fourier* de la fonction de l'auto-corrélation de ϕ et ξ, notée $c(\phi, \xi)$ et définie comme suit :

$$c(\phi, \xi)(w) = \sum_{x \in \mathbb{Z}_q^m} \phi(x+w)\overline{\xi(w)} \ , \ \forall w \in \mathbb{Z}_q^m. \tag{2.1.4}$$

est égale à $\phi\hat{(w)} \otimes (-\xi\hat{(w)})$,

Nous pouvons à présent caractériser la généralisation de ces deux notions sur l'alphabet $\mathbb{Z}_q$.

Définition 2.1.1 (Kumar et al. [KSW85]). *Une fonction q-aire f est* courbe généralisée *si $\hat{\chi_f}(w) = 2^{\frac{m}{2}}$, pour tout $w \in \mathbb{Z}_q^m$.*

Cette définition ne dépend pas du produit scalaire utilisé sur $\mathbb{Z}_4^m$. Une autre généralisation de cette notion liée à la définition originale des fonctions booléennes courbes (*i.e* les fonctions à distance maximale du code de Reed-Muller d'ordre 1) est possible. Elle consiste à considérer les fonctions courbes comme les fonctions dont la distance de Hamming avec la généralisation du code de Reed-Muller d'ordre 1 est maximale. Cela conduit à un concept différent et ce sujet reste toujours ouvert [Lan93].
Une caractérisation de cette notion à l'aide de la fonction d'autocorrection à été donnée par Kumar et al. [KSW85].

Proposition 2.1.1 (Bentness). *Soit f une fonction q-aire à m variables. La fonction f est courbe si et seulement si $c(\chi_f, \chi_f)(w) = 0 \ , \ \forall w \neq 0$.*

Démonstration. En utilisant l'équation 2.1.4 [CD01]. □

La notion de non-linéarité parfaite est généralisée de la façon suivante :

Définition 2.1.2 (Nyberg [Nyb91]). *Une fonction q-aire f est* parfaitement non-linéaire*, si pour tout $w \in \mathbb{Z}_q^m$ non nul, la fonction q-aire $f(x+w)-f(x)$ est équilibrée.*

Ensemble à différence Soit G un groupe fini (Abélien) d'ordre m. Un sous-ensemble D de G de cardinal k est dit (m,k,s)-ensemble à différence si pour tout élément g de G différent de 1_G il existe exactement s couples $(d_1, d_2) \in D^2$ tel que de $g = d_1 {d_2}^{-1}$. Dans l'Algèbre d'un groupe fini (groupe ring), cela signifie que D obéit à la équation $DD^{-1} = k \cdot 1 + s(G-1)$.

Un (n, r, k, s) ensemble à différence relatif R d'ordre $n.r$ est un ensemble à différence relatif à un sous-groupe normal N de cardinal r de G obéissant à la même équation $RR^{-1} = k \cdot 1 + s(G - N)$. Cela signifie que la liste de tous les quotients $r_1 r_2^{-1}$ où $r_1, r_2 \in R^2$ contient exactement s occurrences des éléments de G/N.

Définitions 2.1.1. *Un (n, r, k, s)-ensemble à différence est dit semi régulier si $n = k = rs$.*

Proposition 2.1.2 (Feng [Fen09])**.** *Soient K,N deux groupes abéliens finis et $f : K \to N$ une fonction q-aire, alors f est parfaitement non linéaire si et seulement si $D = \{(a, f(a)) \ , \ a \in K\}$ est un $(|K|, |N|, |K|, |K|/|N|)$ ensemble à différence semi régulier dans $K \times N$ relatif à $\{0\} \times N$.*

Démonstration. [Yam90] □

Cette notion est intéressante d'un point de vue cryptographique parce qu'elle intervient dans la cryptanalyse différentielle [BS90].

Relation entre ces deux notions

Dans [Nyb91], Nyberg a démontré que chaque fonction q-aire parfaitement non linéaire est courbe généralisée. Plus tard, Carlet et Dubuc ont étudié dans [CD01] la relation entre la non-linéarité parfaite et les fonctions courbes.

Proposition 2.1.3. *Une fonction q-aire est parfaitement non linéaire, si et seulement si, pour tout $u \in \mathbb{Z}_q$, la fonction q-aire uf est courbe.*

Démonstration. Voir [CD01]. □

La proposition ci-dessus généralise le résultat de Nyberg dans [Nyb91] : si q est un nombre premier, alors les notions de fonctions courbes et de non linéarité parfaite sont équivalentes. De plus *Kumar et al.*[KSW85] ont démontré que pour tout entier q, pour tout $u \in \mathbb{Z}_q$ premier avec q et toute fonction q-aire parfaitement non linéaire, uf est courbe généralisée. Quand q n'est pas premier, il existe des fonctions courbes généralisées qui ne sont pas parfaitement non linéaires :[Nyb91, Th1 et 3], [CK89, Th1] et [Hou98, Th4.2].

Fonctions parfaitement non-linéaires sur $\mathbb{Z}_q$

Les résultats précédents suggèrent qu'il est difficile d'obtenir des fonctions parfaitement non linéaires. Toutefois, Carlet et Dubuc ont proposé dans

[CD01] une construction de fonctions parfaitement non-linéaires en utilisant les fonctions courbes généralisées proposées par Hou dans [Hou98]. Rappelons brièvement quelques notions sur les anneaux de Galois avant d'introduire cette construction.

Anneau de Galois et exemple de construction sur $\mathbb{Z}_q$

Nous rappelons dans un premier temps quelques définitions et propriétés de la théorie de Galois sur un anneau R. (Pour plus d'information nous envoyons le lecteur au livre [McD74b]). Dans toute la suite, R représente un anneau fini commutatif et unitaire.

Notons l'élément neutre multiplicatif 1. Un diviseur de zéro de R est un élément x "qui divise zéro", c'est à dire pour qui il existe $y \neq 0$ dans R tel que $x * y = 0$. Un inversible de R est un élément x de R "qui divise 1". En d'autres termes, on a $xy = 1$ pour un certain y dans R. L'élément y est alors ; noté x^{-1}.

Définition 2.1.3. *R est un anneau de Galois s'il est commutatif, unitaire, et si l'ensemble de tous les diviseurs de zéro est de la forme pR, p étant un entier premier.*

La *caractéristique* de R, notée $charR$, est l'ordre additif de l'élément neutre multiplicatif, 1. Ainsi $(\mathbb{Z}_k, +, *)$ est un anneau de caractéristique k, puisque 1 est d'ordre k dans $(\mathbb{Z}_k, +)$. Considérons maintenant l'exemple de $R = \mathbb{Z}_{p^k}$, l'anneau des entiers modulo p^k. La caractéristique de l'anneau R de Galois est égale à p^k.
Un anneau est *intègre* s'il est non nul et sans diviseur de zéro.

Définition 2.1.4. *Un idéal I d'un anneau A est un sous-groupe de son groupe additif tel que $xy \in A$ pour tous $x \in A$ et $y \in I$.*

Un idéal I de R est dit *maximal* si $I \neq R$ et s'il n'existe aucun idéal propre contenant I. Si R est un anneau et I un idéal maximal, alors $R \setminus I$ est un corps. Un anneau est dit *local* s'il admet un unique idéal maximal.

Ainsi les assertions suivantes sont équivalentes :

1. R est un anneau local.
2. R admet exactement un idéal maximal.
3. Les diviseurs de zéro de R sont contenus dans un idéal propre.
4. Les diviseurs de zéro de R forment un idéal.

5. Les diviseurs de zéro de R forment un groupe commutatif additif.
6. Pour tout x dans R , un des 2 éléments de l'ensemble $\{x, 1+x\}$ est un inversible.

A partir de maintenant et jusqu'à la fin du chapitre, R représente un anneau de Galois de caractéristique p^k et $D = pR$ l'ensemble des diviseurs de zéro de R. Puisque les diviseurs de zéro sont les seuls éléments non inversibles dans R. Les éléments de R^* sont donc les inversibles de R et D est l'unique idéal maximal de R.

Notons " \ " le symbole représentant la soustraction ensembliste, L'ensemble $R^* = R \setminus D$ est appelé groupe multiplicatif de R et $\bar{R} = R/D$ est le corps de Galois correspondant ($GF(q = p^r)$ de caractéristique p^k) il est appelé aussi corps de classe résiduelle de R. Nous avons alors que le nombre d'éléments de l'anneau R et du groupe multiplicatif R^* sont :

$$|R| = q^k \text{ et } |R^*| = q^{k-1}(q-1)$$

La caractéristique plus le cardinal d'un anneau suffisent à eux deux à la caractérisation complète, à isomorphisme près, d'un anneau de Galois R.

À présent, nous alors nous intéresser à la représentation de R sous forme d'un anneau quotient. Il existe un épimorphisme (un homomorphisme surjectif) d'anneau naturel défini de R dans $\bar{R}$ qui peut s'étendre en un épimorphisme d'anneau des polynômes défini de $R[X]$ (l'anneau des polynômes sur R) dans $\bar{R}[X] \simeq \bar{R}[X]/(pR[X])$. Soit $P(X) = \sum a_i X^i \in R[X]$ un polynôme. Son image par l'épimorphisme est :

$$\bar{P}(X) = \sum \bar{a}_i X^i \in \bar{R}[X].$$

On définit un *B-polynôme* sur R comme suit :

Définition 2.1.5. *Un* B-polynôme $P(X) \in R[X]$ *sur* R *est un polynôme unitaire tel que* $\bar{P}$ *est un polynôme irréductible sur le corps résiduel* $\bar{R}$.

La donnée d'un B-polynôme P de degré m sur R permet de construire une extension de R sous forme d'un anneau plus gros en adjoignant à R une racine ζ de P. Nous appelons cette extension une G-extension de R.

Théorème 2.1.1 (Extension et degré)**.** *Soit* R *un anneau de Galois de* q^r *éléments et de caractéristique* p^k. *Soit* $P(X)$ *un B-polynôme de degré* m. *Alors l'anneau*

$$S = R[X]/(P(X))$$

est un anneau de Galois de paramètres char $S = P^k$ *et de cardinal* $|S| = q^{mr}$ *On dit que l'anneau* S *est une G-extension de degré* m *de* R.

Démonstration. Voir [McD74b]. □

Il est clair qu'il existe un b-polynôme dans $R[X]$ pour n'importe quel degré m donné. Ainsi, par le résultat précédent, nous avons les deux propriétés suivantes concernant l'existence d'un anneau de Galois :

1. Pour tout anneau de Galois R et tout entier m, il existe une G-extension de degré m de R.

2. Pour tout p premier, $m, n \in \mathbb{N}$, il existe un anneau de Galois S de caractéristique p^n et de cardinal égal à p^{mn} .

Si l'on considère un élément α de l'extension S de R, le sous-anneau

$$R[\alpha] = \{P(\alpha) \ : \ P(X) \in R[X]\}$$

est une extension de l'anneau R par α. Il existe un lien entre les racines d'un polynôme dans $R[X]$ et les racines de son polynôme image par l'épimorphisme naturel étendu entre $R[X]$ et $\bar{R}[X]$ ce lien est le suivant :

Soient $P(X) \in R[X]$ et $\alpha \in S$ tels que $\bar{P}(\bar{\alpha}) = \bar{0}$ et $\bar{P}'(\bar{\alpha}) \neq \bar{0}$. Alors $\exists! \beta \in S$ tels que $P(\beta) = 0$ et $\bar{\beta} = \bar{\alpha}$ (voir [McD74b]).

Théorème 2.1.2. *Soit S une G-extension de degré m de R et $h(X)$ un b-polynôme sur R de degré r. Alors*
1. Le polynôme $h(X)$ a une racine dans S si et seulement si $r|m$.
2. Si $r|m$, $h(X)$ admet exactement r racines distinctes $\alpha_1, \ldots, \alpha_r$ dans S modulo l'idéal pS.
3. Pour tout élément $\alpha \in S$, on a $S = R[\alpha]$ si et seulement si α est une racine du b-polynôme de degré m sur R.

Démonstration. Voir [McD74b]. □

À présent, nous allons énoncer un corollaire important de ce théorème.

Corollaire 2.1.1. *Soit R un anneau de Galois de caractéristique p^k et de cardinal p^{km}. Alors*

$$R \simeq \mathbb{Z}_{p^k}[X]/(P(X))$$

où $P(X)$ est un B-polynôme de degré m sur $\mathbb{Z}_{p^k}$. Notons un tel anneau $GR(p^k, m)$.

Soient m, k deux entiers positifs non nuls et p un nombre premier. L'anneau de Galois $R = GR(p^k, m)$ est l'extension de degré m de l'anneau $\mathbb{Z}_{p^k}$ [McD74b]. Notons ζ une racine primitif d'ordre $p^m - 1$ du B-polynôme $P(X)$ sur $\mathbb{Z}_{p^k}$. Notons l'ensemble $\overline{\mathcal{T}} = \{0, 1, \zeta, \cdots, \zeta^{p^m-2}\}$ le système Teichmüller. Nous avons alors (voir [CD01]) :

1. Les éléments de $GR(p^k, m)$ peuvent s'écrire sous forme multiplicative ou additive. Pour tout $z \in GR(p^k, m)$,

$$z = \begin{cases} \sum_{i=1}^{k} p^{i-1}\zeta^i \\ \\ \sum_{i=0}^{m-1} a_i\zeta^i \quad a_i \in \mathbb{Z}_{p^k}. \end{cases} \tag{2.1.5}$$

2. L'automorphisme de *Frobenius* σ est l'automorphisme d'anneaux sur $GR(p^k, m)$ défini par :

$$\sigma(\sum_{i=1}^{k} p^{i-1}\zeta^i) = \sum_{i=1}^{k} p^{i-1}\zeta^{pi}. \tag{2.1.6}$$

3. La fonction trace sur $GR(p^k, m)$, notée Tr est définie comme suit :

$$Tr(x) = \sum_{i=0}^{m-1} \sigma^i(x). \tag{2.1.7}$$

Exemple de fonction q-aire parfaitement non-linaire. Replaçons-nous dans un anneau de Galois $R = GR(p^k, m)$. Il a été démontré dans [CD01] que les fonctions engendrées par la construction ci dessous ne sont pas que courbes généralisés mais qu'elles admettent aussi la propriété de non linéarité parfaire.

Construction 2.1.1 (Hou [Hou98])**.** *Soit $a \in \mathbb{Z}_{p^k}$, pour tout $i \in \{0 \dots k-1\}, \varphi_i : R/p^{k-i}R \to \mathbb{Z}_{p^k}$ une application tel que :*

$$\sum_{x \in \mathcal{T}} u^{\varphi_i(y+p^{k-i-1}x)} = 0 \ \ \forall y \in R/p^{k-i}R \tag{2.1.8}$$

et $f : R \times R \to \mathbb{Z}_{p^k}$ la fonction définie par :

$$f(x,y) = \begin{cases} a & si \quad y = 0 \\ \varphi_i(\left[\frac{x}{y'}\right]) & si \quad y = p^i y', \ y' \in R/pR, \end{cases} \tag{2.1.9}$$

avec $\left[\frac{x}{y'}\right]$ l'image de $\frac{x}{y'}$ dans $R/p^{k-i}R$. Alors f est une fonction courbe généralisée.

Carlet et Dubuc dans [CD01] ont étudié la parfaite non-linéarité de ces fonctions et ont démontré qu'elles étaient bel et bien parfaitement non linéaires. Il ont démontré aussi l'existence de fonctions courbes généralisées dans cas ou le nombre m de variables est impair (dans le cas binaire cela est impossible). Dans la suite de leur travail il ont prouvé l'existence de fonctions de non-linéarité parfaite pour un m quelconque et ont proposé une construction dans le cas particulier de $q = 4$.

2.2 Fonctions quaternaires

Cette section est consacrée aux définitions de base des fonctions quaternaires à m variables.

L'intérêt pour les fonctions quaternaires courbes et parfaitement non linéaires a pris de l'ampleur après l'apparition des travaux de *Hammons et al.* dans [HKC+94] sur la $\mathbb{Z}_4$-linéarité des codes de *Kerdock*, *Preparata*, *Goethals* et codes associés. Dans cet article, *Hammons et al.* ont montré que ces codes peuvent être construits d'une manière plus simple comme des images binaires d'une application spécifique, appelée fonction de *Gray* des codes linéaires sur $\mathbb{Z}_4$. La fonction de *Gray* est une isométrie de ${\mathbb{Z}_4}^m$ dans $\mathbb{F}^{2m}$ (elle sera décrite dans la prochaine section). Plus tard, plusieurs chercheurs se sont intéressés aux projections binaires des codes linéaires sur $\mathbb{Z}_4$.

En 2009, Solé et Tokareva [ST09] ont étudié les liens directs entre les fonctions booléennes courbes, les fonctions booléennes courbes généralisées (introduites par Schmidt, [Sch07]) et les fonctions quaternaires courbes. Ils ont aussi étudié les images par la fonction de *Gray* des fonctions courbes.

Récemment, Jadda et Parraud ont étudié dans [JP10] la $\mathbb{Z}_4$-non linéarité d'une classe de fonctions quaternaires cryptographiques et ont proposé une projection binaire à l'aide de la fonction de *Gray*.

Généralités

Soient $\mathbb{Z}_4 = \mathbb{Z}/4\mathbb{Z} = \{0, 1, 2, 3\}$ l'anneau des entiers modulo 4, m un entier strictement positif et $\mathbb{Z}_4^m$ l'ensemble des mots de longueurs m sur $\mathbb{Z}_4$. La métrique usuelle sur $\mathbb{Z}_4$ est *la métrique* de *Lee*. *Le poids* de *Lee* par définition sur $\mathbb{Z}_4$, est :

$$w_l(x) = min\{x, 4 - x\}, \ \forall x \in \mathbb{Z}_4. \tag{2.2.1}$$

Le poids de Lee d'un vecteur $v \in \mathbb{Z}_4^m$ est la somme des poids de ses composantes :

$$\forall u = (u_0, .., u_{m-1}) \in \mathbb{Z}_4^m, \ w_l(u) = \sum_{i=0}^{m-1} w_l(u_i).$$

La distance de Lee entre u et v dans Z_4^m, notée d_l est définie par :

$$d_l(u, v) = w_l(u + v). \tag{2.2.2}$$

Nous appellerons *fonction quaternaire à m variables* toute application de ${\mathbb{Z}_4}^m$ dans $\mathbb{Z}_4$ et noterons $\mathcal{F}(\mathbb{Z}_4^m, \mathbb{Z}_4)$ l'ensemble des fonctions quaternaires à m variables. Une fonction quaternaire est complètement caractérisée par sa *table de vérité* :

Définition 2.2.1. *Une fonction quaternaire à m variables F est une fonction définie de $\mathbb{Z}_4^m$ sur $\mathbb{Z}_4$:*

$$[F(0,0,\ldots,0),\ldots,F(3,3,\ldots,3)]$$

de longueur 4^m.

A présent, munissons $\mathcal{F}(\mathbb{Z}_4^m,\mathbb{Z}_4)$ de la métrique de Lee et définissons *le support* et *le poids de Lee* d'une fonction quaternaire F

Définition 2.2.2 (Support et poids)**.** *Soit $F \in \mathcal{F}(\mathbb{Z}_4^m,\mathbb{Z}_4)$. Le* support *de F, noté $supp(F)$ est l'ensemble $\{u \in \mathbb{Z}_4^m \mid F(u) \neq 0\}$. Pour tout $j \in \mathbb{Z}_4$, le* support relatif *noté $supp_j(F)$ de F est défini comme suit $\{u \in \mathbb{Z}_4^m \mid F(u) = j\}$, notons $\eta_i(F)$ le cardinal de $supp_j(F)$.*

Avec ces définitions nous avons :$|supp(F)| = \eta_1 + \eta_2 + \eta_3$. Le poids de Lee d'une fonction quaternaire est :

Définition 2.2.3. *Soit $F, G \in \mathcal{F}(\mathbb{Z}_4^m,\mathbb{Z}_4)$ alors,*

1. $w_l(F) = \eta_1(F) + 2\eta_2(F) + \eta_3(F)$.
2. $d_l(F,G) = w_l(F+G)$.

Walsh sur $\mathbb{Z}_4$

Nous avons introduit dans la section précédente la transformée de Walsh d'une fonction généralisée sur l'alphabet $\mathbb{Z}_q$. En considérant $q = 4$ et la fonction signe $\chi_F = (i)^F$, nous retrouvons les expressions de la transformée de Walsh d'une fonction quaternaire sur $\mathbb{Z}_4^m$ et $R = GR(4,m)$. Nous les rappelons ici. Considérons $x = (x_1, x_2, \ldots, x_n)$, $a = (a_1, a_2, \ldots, a_n)$ dans $\mathbb{Z}_4^m$ et " $\cdot$ " un produit scalaire sur $\mathbb{Z}_4^m$, défini par : $a \cdot u = \sum_{i=1}^{n} a_i \cdot u_i \mod 4$. Alors *la transformée de Walsh* d'une fonction F est définie par :

$$\hat{\chi}_F(u) = \sum_{a \in \mathbb{Z}_4^m} (i)^{F(a)+a\cdot u}. \tag{2.2.3}$$

La modification du produit scalaire change l'ordre des valeurs de la transformation de Walsh mais pas l'ensemble de ces valeurs, appelé le *spectre de Walsh*. Soit $x \in R$ la transformée de Walsh sur l'anneau de Galois R s'écrit de cette manière :

$$\hat{\chi}_F(u) = \sum_{\alpha \in R} (i)^{F(\alpha)+Tr(u\alpha)}, \tag{2.2.4}$$

avec $Tr : R \to \mathbb{Z}_4$ la trace absolue sur l'anneau de Galois R définie par : $\forall (a+2b) \in R$,

$$Tr(a+2b) = \sum_{i=0}^{m-1} \sigma^i(a+2b)$$

avec σ l'automorphisme de Frobenius et $\forall x \in \mathbb{Z}_4,\ \ Tr(x) \in \mathbb{Z}_4$.

Équilibre et non linéarité

Donnons maintenant une caractérisation de *l'équilibre* et de la *non linéarité* d'une fonction quaternaire à m variables.

Définition 2.2.4 (Équilibre)**.** *Soit* $F \in \mathcal{F}(\mathbb{Z}_4^m, \mathbb{Z}_4)$.

F *est dite* équilibrée *si et seulement si* $\forall i \in \{0,1,2,3\}\ ,\ \eta_i = 4^{m-1}$.

Proposition 2.2.1 ([JP10])**.** *Soit* $F \in \mathcal{F}(\mathbb{Z}_4^m, \mathbb{Z}_4)$.

F *est équilibrée, si et seulement si,* $\hat{\chi}_F(0) = \hat{\chi}_F^2(0) = 0$.

Démonstration. Le résultat découle directement de

$$\hat{\chi_F}^2(u) = \sum_{v \in R} (-1)^{F(v)+Tr(vu)}.$$

□

Poursuivons avec une caractérisation de la non-linéarité de la fonction quaternaire. Considérons $F \in \mathcal{F}(\mathbb{Z}_4^m, \mathbb{Z}_4)$. La *non-linéarité* de F est définie comme la distance minimale de l'ensemble des fonctions affines. Nous noterons la non-linéarité de F, $nl_4^d(F)$, avec d la métrique choisie (Hamming ou Lee).

Proposition 2.2.2 ([JP10])**.** *Soit* $F \in \mathcal{F}(\mathbb{Z}_4^m, \mathbb{Z}_4)$. *La non linéarité de* F *est caractérisée par*

$$\begin{aligned} nl_4^H(F) &= 3.4^{m-1} - \frac{1}{4} \underset{a \in \mathbb{Z}_4^m, b \in \mathbb{Z}_4}{Max} \{2Re(i^b \hat{\chi}_F(a)) + (-1)^b \hat{\chi^2}_F(2a)\} \\ &= 3.4^{m-1} - \frac{1}{4} \underset{a \in \mathbb{Z}_4^m}{Max} \{2|Re(\hat{\chi}_F(a))| + \hat{\chi^2}_F(2a), 2|Im(\hat{\chi}_F(a))| + \hat{\chi^2}_F(2a)\}, \end{aligned}$$

avec $Re(z)$ *et* $Im(z)$ *les parties réelle et la partie imaginaire du nombre complexe* z.

Proposition 2.2.3. *Soit* F *une fonction quaternaire à* m *variables. La non-linéarité de* F *sous la métrique de Lee est donnée par :*

$$nl_4^L = 4^m - max_{a \in \mathbb{Z}_4^m} |Re(\chi_F(a))|, |Im(\chi_F(a))|$$

Fonction quaternaire cryptographique

Continuons avec le cas particulier des fonctions quaternaires courbes et ou parfaitement non linéaires. Ces définitions et propriétés sont le cas quaternaire ($q = 4$) des caractérisations de ces notions pour les fonctions généralisées introduites dans la section 2.1.

Proposition 2.2.4. *Une fonction quaternaire F à m variables est* courbe *si et seulement si :*

$$\forall u \in \mathbb{Z}_4^m, \quad |\hat{\chi}_F(u)| = 2^m.$$

Proposition 2.2.5. *Soit F une fonction quaternaire à m variables.*
F est courbe si et seulement si $c(\chi_F, \chi_F)(w) = 0$, $\forall w \neq 0$.

Démonstration. [CD01]. □

En 2010, *Jadda et Parraud* [JP10] ont caractérisé la non linéarité des fonctions quaternaires courbes sous les deux métriques de Hamming et de Lee. Ces caractérisations sont données par les théorèmes ci-dessous.

Théorème 2.2.1 ([JP10])**.** *Soit F une fonction quaternaire courbe. Alors,*

1. $3.4^{m-1} - 2^{m-1} \leq nl_4^H(F) \leq 3.4^{m-1} - 2^{m-2}$

2. $nl_4^H(F) = 3.4^{m-1} - 2^{m-2}$*,si et seulement si,* $\hat{\chi^2}_F(2a) = \pm 2^m$

Démonstration. Nous avons d'après la proposition 2.2.2 que :

$$nl_4(F) = 3.4^{m-1} - \frac{1}{4} \underbrace{sup_{a \in \mathbb{Z}_4^m} \{2|Re(\hat{\chi}_F(a))| + \hat{\chi^2}_F(2a), 2|Im(\hat{\chi}_F(a))| + \hat{\chi^2}_F(2a)\}}_{y}$$

De plus, F est courbe, ainsi

$$|\hat{\chi}_F(a)| = 2^m \Rightarrow \begin{cases} |Re(\hat{\chi}_F(a))| = 2^m & et \quad |Im(\hat{\chi}_F(a))| = 0 \\ ou & \\ |Re(\hat{\chi}_F(a))| = 0 & et \quad |Im(\hat{\chi}_F(a))| = 2^m \end{cases}.$$

Enfin,

$$\hat{\chi^2}_F(2a) = \underbrace{\sum_{u \in \mathbb{Z}_4^m} (-1)^{a.u+F(u)}}_{x},$$

donc

$$y = \begin{cases} Max\{2^{m+1} + x, -x\} & si \quad \hat{\chi}_F(a) \text{ est réelle,} \\ Max\{x, 2^{m+1} - x\} & \text{sinon.} \end{cases}$$

On remarque après la représentation géométrique de y que :

$$2^m \leq y \leq 2^{m+1},$$

d'où l'inégalité (1).

(2) : si $\hat{\chi}_F(a)$ est réelle alors :

$$y = 2^m = sup\{2^{m+1} + \hat{\chi^2}_F(2a), -\hat{\chi^2}_F(2a)\} \Rightarrow \hat{\chi^2}_F(2a) = -2^m,$$

de même pour $\hat{\chi}_F(a)$ imaginaire. □

Théorème 2.2.2 ([JP10]). *Soit F une fonction quaternaire courbe à m variables alors*

$$nl_4^L(F) = 4^m - 2^m.$$

2.3 Fonctions booléennes et quaternaires courbes

Cette section est consacrée aux liens entre les fonctions quaternaires courbes et les fonctions booléennes courbes. Solé et Tokareva [ST09] ont étudié la connexion entre les fonctions quaternaires courbes, les fonctions booléennes généralisées courbes (toute application de ${\mathbb{F}_2}^m$ dans $\mathbb{Z}_4$) et les fonctions booléennes courbes. Dans cette section nous nous restreignons aux liens quaternaire-booléen. Nous commençons par introduire la fonction de Gray sur $\mathbb{Z}_4^m$.

La fonction de Gray

La fonction de Gray ϕ qui permet le passage de $\mathbb{Z}_4$ à $\mathbb{F}_2$ a été largement utilisée en théorie des codes pour construire les images binaires des codes cycliques sur $\mathbb{Z}_4$. Elle permet cette correspondance :

$$\begin{array}{ccc} \mathbb{Z}_4 & \rightarrow & \mathbb{F}_2^2 \\ 0 & \mapsto & 00 \\ 1 & \mapsto & 01 \\ 2 & \mapsto & 11 \\ 3 & \mapsto & 10 \end{array}$$

1. La fonction de Gray est donnée par

$$\begin{array}{rccc} \phi & : & \mathbb{Z}_4 & \rightarrow & \mathbb{F}_2 \times \mathbb{F}_2 \\ & & (2q + r) & \mapsto & (q, q \oplus r) \end{array} \tag{2.3.1}$$

2. Cette fonction est bijective et sa fonction inverse est définie comme suit :

$$\begin{array}{rccc} \phi^{-1} & : & \mathbb{F}_2 \times \mathbb{F}_2 & \to & \mathbb{Z}_4 \\ & & (q,r) & \mapsto & (2q + q \oplus r). \end{array} \tag{2.3.2}$$

Cette fonction est facilement étendue à $\mathbb{Z}_4^m$ et présente la particularité d'être une isométrie de $(\mathbb{Z}_4^m, d_l)$ sur $(\mathbb{F}_2^{2m}, d_H)$. La fonction de Gray est généralisée de la façon suivante :

$$\begin{array}{rccc} \phi_m & : & \mathbb{Z}_4^m & \to & \mathbb{F}_2^{2m} \\ & & (2q_0 + r_0, \ldots, 2q_{m-1} + r_{m-1}) & \mapsto & (q_0, \ldots, q_{m-1}, q_0 \oplus \cdots \oplus q_{m-1}). \end{array}$$

Soit F une fonction quaternaire à m variables et $f = \phi_m(F)$ sa projection booléenne à $2m$ variables.

Proposition 2.3.1. *Si F est équilibrée alors f est équilibrée.*

Démonstration. F est équilibrée, ainsi $\eta_0(F) = \eta_1(F) = \eta_2(F) = \eta_3(F)$. Nous savons que

$$\begin{cases} \phi(0) = (0,0) \\ \phi(1) = (0,1) \\ \phi(2) = (1,0) \\ \phi(3) = (1,1) \end{cases}$$

Comme

$$\begin{cases} \eta_0(f) = 2\eta_0(F) + \eta_1(F) + \eta_3(F) = 4\eta_0, \\ \eta_1(F) = \eta_1(F) + \eta_2(F) + 2\eta_3(F) = 4\eta_0, \end{cases}$$

alors f est équilibrée sur $\mathbb{F}_2^{2m}$. □

Image booléenne d'une fonction quaternaire courbe

Considérons $F \in \mathcal{F}(\mathbb{Z}_4^m, \mathbb{Z}_4)$ définie par : $F(x + 2y) = f(x,y) + 2g(x,y)$, avec f,g :$\mathbb{F}_2^m \times \mathbb{F}_2^m \to \mathbb{F}_2$ deux fonctions booléennes à $2m$ variables. Solé et Tokareva ont prouvé dans [ST09] les résultats suivants,

Lemme 2.3.1. *La relation entre les transformées de Walsh de $F, f+g$ et g est :*

$$\hat{\chi}_F(x + 2y) = \frac{1}{2}\left(W_g(x+y,x) + W_{f+g}(x,y)\right) + \frac{i}{2}\left(W_g(x,y) + W_{f+g}(x+y,x)\right).$$

Cette relation entre les transformées de Walsh des fonctions F, $f+g$ et f permet d'établir une connexion directe entre la notion de "Bentness" des fonctions quaternaires à m variables et les fonctions booléennes à $2m$ variables. Pour cela, Solé et Tokareva [ST09] ont introduit la notion de fonctions booléennes *courbes corrélées* suivante : deux fonctions booléennes f et g à $2m$ variables sont dites *courbes corrélées* si pour tout $x, y \in \mathbb{F}_2^m$ nous avons,

1. $W_f(x,y)^2 + W_f^2(x+y,y) + W_g^2(x,y) + W_g^2(x+y,y) = 4^{m+1}$,
2. $W_f(x,y) = W_g(x+y,y) = \pm 2^m \iff W_g(x,y) = W_f(x+y,y) = \pm 2^m$.

Avec cette notion ils établissent l'équivalence ci-dessous :

Théorème 2.3.1. *Ces deux assertions sont équivalentes :*

1. *La fonction quaternaire F à m variables est courbe.*
2. *Les deux fonctions booléennes f et $f+g$ à $2m$ variables sont courbes corrélées.*

Regardons maintenant "la fonction booléenne obtenue comme image par la fonction de Gray d'une fonction quaternaire courbe F. L'image de F par ϕ_m peut être définie comme la fonction booléenne à $2m+1$ variables suivante $\phi_m(F)(x,y,z) = f(x,y)z + g(x,y)$, avec $x, y \in \mathbb{F}_2^m$ et $z \in \mathbb{F}_2$.

Théorème 2.3.2. *Si F est courbe sur m variables, alors $\phi_m(F)$ est semi courbe sur $2m+1$ variables.*

Nous finirons ce chapitre en donnant quelques exemples de construction de fonctions quaternaires et de leur projections par la fonction de Gray.

Exemple de construction de fonctions quaternaires et projections

En 1985, Kumar et al. ont généralisé dans [KSW85] les deux notions de non-linéarité parfaite et de "bentness". Plus tard, plusieurs chercheurs ont proposé des constructions (avec q quelconque) de fonctions courbes généralisées comme : [Nyb91, Th1 et 3], [CK89, Th1] et [Hou98, Th4.2].

Construction 2.3.1 ([KSW85])**.** *Soit $f : \mathbb{Z}_q^m \times \mathbb{Z}_q^m \to \mathbb{Z}_q$ définie par :*

$$f(x,y) = x \cdot \pi(y) + g(y),\ x, y \in \mathbb{Z}_q^m$$

avec $g : \mathbb{Z}_q^m \times \mathbb{Z}_q^m \to \mathbb{Z}_q$ une fonction quelconque et π une permutation de $\mathbb{Z}_q^m$. La fonction f est courbe généralisée.

Cette classe de fonctions est la généralisation sur $\mathbb{Z}_q^m$ de la classe de fonctions booléennes courbes de Maiorana. Carlet a démontré dans [CD01] que ces fonctions ne sont par parfaitement non linéaires quand q n'est pas un nombre premier. Plus tard, Solé et Tokareva dans [ST09] ont démontré que les projections booléennes par ϕ_m des fonctions quaternaires décrites par cette construction sont semi courbes.

Carlet et Dubuc [CD01] ont proposé la construction de fonctions parfaitement non linéaires suivante :

Construction 2.3.2. *Soit fonction* $f : GR(4, m) \to \mathbb{Z}_4$ *définie par :*

$$\forall a, b \in \mathcal{T}, f(a + 2b) = h(ba^{2^m-2})$$

avec $h : \mathcal{T} \to \mathbb{Z}_4$*, une fonction équilibrée et*

$$\forall x \in \mathcal{T}, \ |\sum_{v\in\mathcal{T}} i^{h(v)-Tr(v(2x-1))}| = 2^{\frac{m}{2}}. \tag{2.3.3}$$

si $2h$ *vérifie l'équation2.3.3 alors la fonction* f *est parfaitement non linéaire.*

Dans ce chapitre, nous avons introduit les fonctions quaternaires courbes et parfaitement non linéaires. Ces fonctions sont un cas particulier des fonctions cryptographiques généralisées. Nous avons présenté aussi la fonction de Gray qui permet de construire des fonctions semi courbes à $2m+1$ variables à partir de fonctions quaternaires courbes. Dans la suite de ce manuscrit, nous allons proposer une construction de fonctions quaternaires courbes à m variables et deux projections booléennes à $2m$ et $2m+1$ variables. La première classe de projection binaire est composée de fonctions booléennes courbes et la deuxièmes classe est composée de fonctions booléennes semi-courbes.

Chapitre 3

Fonctions booléennes

Nous commencerons ce chapitre par l'introduction du contexte d'utilisation des fonctions booléennes en cryptographie. Ensuite, nous donnerons quelques unes des représentations basiques des fonctions booléennes ainsi qu'un ensemble de définition des critères cryptographiques comme : l'équilibre, le degré algébrique, la non-linéarité et l'immunité algébrique. Avant d'introduire un outil puissant appelé transformée de *Walsh* nous allons présenter les incompatibilités existantes entre ces critères. Cet outil va servir essentiellement à caractériser les critères cryptographiques. Enfin, nous allons décrire un ensemble de constructions de fonctions booléennes vérifiant quelques uns de ces critères avant de présenter celles dont l'immunité algébrique dépend de conjectures combinatoires.

3.1 Contexte d'utilisation

Dans cette première section, nous nous intéressons à l'utilisation des fonctions booléennes en cryptographie symétrique. Une fonction booléenne f est une fonction du $\mathbb{F}_2$-espace vectoriel $\mathbb{F}_2^n$ de dimension n vers le corps $\mathbb{F}_2$ à deux éléments. Les fonctions booléennes constituent une brique fondamentale des systèmes cryptographiques symétriques. Plus particulièrement, dans les systèmes de chiffrement à flot, une fonction booléenne peut être utilisée comme fonction de filtrage, ou de combinaison des registres à décalage à rétroaction linéaire (LFSR). Nous pouvons schématiser les utilisations d'une fonction booléenne dans un système de chiffrement à flot comme :

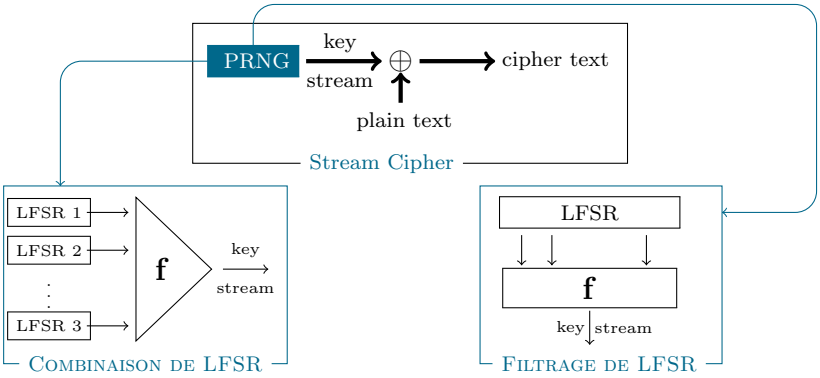

FIGURE 3.1 – chiffrement par flot

Pour résister aux attaques connues sur chaque modèle de chiffrement par flot, les fonctions booléennes doivent satisfaire divers critères simultanément [Car10b, DXS91] :

- *non-linéarité* (pour résister à l'attaque par la meilleure approximation affine [DXS91] et à l'attaque par corrélation rapide [MS89]),
- *équilibre* (pour éviter la dépendance statistique entre l'entrée et la sortie),
- *haute immunité algébrique* (pour résister à l'attaque algébrique [CM03a]) et un bon comportement face aux attaques algébriques rapides,
- *haut degré algébrique* (pour résister à l'attaque de Berlekamp-Massey [Mas69, RS87] et à l'attaque de Rønjom - Helleseth [RH07]).

D'autres propriétés des fonctions booléennes existent et elles peuvent être demandées. Par exemple : la $k-$résilience, c'est-à-dire que toute restriction de la fonction où m entrées ont été fixées doit rester équilibrée. Cette propriété permet de résister aux attaques par corrélation et n'est pas requise dans le modèle filtré.

Chiffrement par bloc : Ici, les fonctions booléennes sous une forme vectorielle sont utilisées pour construire des boîtes-S dans ces systèmes de chiffrement.

Construire des fonctions satisfaisant ces critères, voire prouver leur existence est une tâche rude. De plus, ces critères représentent des incompatibilités. Ainsi, le degré algébrique d'une fonction k-résiliente à n variables vérifie $k + deg(f) \leq n - 1$ (n pair). Ou encore, une fonction *courbe*, i.e. possédant une non-linéarité maximum, ne peut être équilibrée. Bien souvent, l'apparition d'un nouveau type d'attaque, et l'introduction d'un critère de résistance associé, rendent obsolètes toutes les familles de fonctions connues.

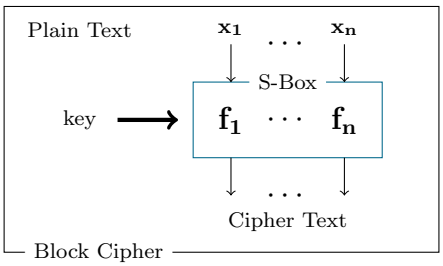

FIGURE 3.2 – Chiffrement par bloc

Par exemple, parmi les fonctions connues avant l'apparition des attaques algébriques, celles qui possédaient une immunité algébrique optimale avaient toutes une mauvaise non-linéarité.

Ce n'est qu'en 2008 que Carlet et Feng [CF08] mirent à jour une famille de fonctions booléennes et ses bonnes propriétés cryptographiques au sein de familles de fonctions booléennes précédemment étudiées par Feng, Liao et Yang [FLY09].

3.2 Définitions et propriétés cryptographiques

Cette section est consacrée aux définitions de base des fonctions booléennes à n variables. Nous appellerons *fonction booléenne* à n variables toute application de $\mathbb{F}_2^n$ dans $\mathbb{F}_2$ et noterons $\mathcal{B}_n$ l'ensemble de toutes les fonctions booléennes à n variables.

Représentation d'une fonction booléenne

Table de vérité

Une fonction booléenne est complètement caractérisée par sa *table de vérité* : le vecteur $[f(0,\cdots,0),\cdots,f(1,\cdots,1)]$ à 2^n éléments des images par f de tous les éléments de l'ensemble $\mathbb{F}_2^n$.

Définition 3.2.1. *Soit $f \in \mathcal{B}_n$. Le support de f, noté $supp(f)$ est l'ensemble des éléments u de $\mathbb{F}_2^n$ tels que $f(u) = 1$. Le cardinal du support de f est appelé poids de f et noté $w_H(f)$.*

Pour éviter la cryptanalyse à clair connu [And95], une fonction booléenne à n variables utilisée comme fonction de combinaison doit être *équilibrée*. En effet, une fonction de combinaison produisant plus de 0 que de 1 , induit dans

la majorité des cas une égalité entre les bits du chiffré et ceux du clair correspondant. Introduisons maintenant les premiers critères cryptographiques.

Définition 3.2.2 (équilibre[Car10b])**.** *Une fonction booléenne à n variables f est dite équilibrée si et seulement si $w_H(f) = |supp(f)| = 2^{n-1}$.*

Pour résister à l'attaque par corrélation introduite par Siegenthaler [MS] et ses dérivées, une fonction booléenne f à n variables utilisée comme fonction de combinaison doit avoir un bon ordre *d'immunité aux corrélations*. Une fonction permet une résistance optimale à l'attaque par corrélation si elle reste équilibrée quand on fixe les valeurs d'au plus k de ses variables.

Définition 3.2.3. *Une fonction booléenne $f \in \mathcal{B}_n$ est* sans corrélation d'ordre *k si sa distribution de valeurs ne change pas lorsque l'on fixe au plus k entrées*

Définition 3.2.4. *(k-résilience [Sie84] [XM88]) Une fonction booléenne $f \in \mathcal{B}_n$ est dite* k-résiliente *si elle est équilibrée et sans corrélation d'ordre k.*

Forme algébrique normale et transformée de Walsh

Nous allons introduire maintenant une autre représentation des fonctions booléennes : la *Forme Algébrique Normale* (FAN). Pour ce, nous munissons l'ensemble des fonctions booléennes des opérations induites par les opérations du corps $\mathbb{F}_2$. L'ensemble des fonctions booléennes sur $\mathbb{F}_2^n$ est alors un espace vectoriel de dimension 2^n sur $\mathbb{F}_2$.

Une base possible de cette espace vectoriel est constituée des fonctions caractéristiques :

$$\{x_i \ : \ \mathbb{F}_2^n \to \mathbb{F}_2, \text{ tel que } x_i(u) = u_i\}$$

- Les produits de fonctions caractéristiques sont aussi des fonctions booléennes sur $\mathbb{F}_2^n$, appelées monômes.
- Le degré d'un monôme $\prod_{i \in I \subset \{0,1,\ldots,m\}} x_i$ est le cardinal de I.
- A chaque monôme correspond un mot $u \in \mathbb{F}_2^n$ tel que le monôme x^u puisse s'écrire
$$x^u = \prod_{i=1}^{n} x_i^{u_i}.$$
- Le degré de ce monôme est le poids de Hamming du mot u (son nombre de coordonnées non nulles).

Ainsi l'ensemble des monômes constitue une base de l'espace vectoriel des fonctions booléennes sur $\mathbb{F}_2^n$. Cette écriture, unique, correspond à la représentation polynomiale à n-variables d'une fonction booléenne, avec le degré relatif de chacune des variables est égale au plus 1.

Définition 3.2.5 ((FAN) [Car10b]). *La* forme algébrique normale *d'une fonction booléenne f est l'écriture unique sous forme de combinaison linéaire à coefficients dans $\mathbb{F}_2$ de monômes*

$$f(x) = \sum_{u \in \mathbb{F}_2^n} a_u (\prod_{i=1}^{n} x^{u_i}) = \sum_{u \in \mathbb{F}_2^n} a_u x^u$$

avec, $a_u \in \mathbb{F}_2$ pour tout $u \in \mathbb{F}_2^n$.

Nous pouvons à présent définir un autre critère cryptographique :

Définition 3.2.6 ([Car10b]). *On appelle* degré algébrique *d'une fonction booléenne le degré global de sa forme algébrique normale.*

Le *degré algébrique* sera noté $deg(f)$ et correspond à la valeur maximale de $w_H(u)$ tel que $a_u \neq 0$. Une fonction booléenne est dite *affine* si son degré algébrique est au plus égal à 1. L'ensemble des fonctions affines est noté $\mathcal{A}_n$. Pour résister à l'attaque par meilleure approximation affine [DXS91] et à l'attaque par corrélation rapide [MS89], une fonction booléenne f utilisée dans le chiffrement à flot doit être la plus éloignée possible de l'ensemble des fonctions affines $\mathcal{A}_n$. Munissons l'ensemble des fonctions booléennes à n variables de la métrique de *Hamming*. La distance de *Hamming* entre f et g, notée $d_h(f, g)$ est alors le poids *Hamming* de $f \oplus g$, où $\oplus$ désigne le Xor.

Définition 3.2.7 ([Car10b]). *La non-linéarité d'une fonction booléenne à n variables, notée $nl_2(f)$ est :*

$$nl_2(f) = \min_{g \in \mathcal{A}_n} d_h(f, g).$$

Transformée de Walsh et FAN

Considérons maintenant l'ordre partiel sur $\mathbb{F}_2^n$ suivant : $u \leq v \Leftrightarrow \forall i = 1, \ldots, n$, $v_i = 1 \Rightarrow u_i = 1$, et définissons la *transformée de Möbius* de cette manière :

Définition 3.2.8. *La* transformée de Möbius *d'une fonction booléenne f à n variables est la fonction f° définie comme suit :*

$$\begin{array}{rccl} f^\circ & : & \mathbb{F}_2^n & \to & \mathbb{F}_2 \\ & & u & \mapsto & \sum\limits_{u \leq v} f(v) \ mod\ 2. \end{array}$$

En remarquant que f° correspond à la fonction qui à $u \to a_u$ dans la forme algébrique normale de f, alors toute fonction booléenne f sur $\mathbb{F}_2^n$ s'écrit :

$$f(x) = \sum_{u \in \mathbb{F}_2^n} f^\circ(u) x^u$$

Introduisons maintenant, *la transformée de Walsh.* cette fonction va servir essentiellement a analyser et caractériser les propriétés cryptographiques des fonctions booléennes.

Définition 3.2.9. *La transformée de Fourier d'une fonction numérique ϕ de $\mathbb{F}_2^n$ à valeurs dans $\mathbb{Z}$, $\mathbb{R}$ ou $\mathbb{C}$, est définie par :*

$$\widehat{\phi}(u) = \sum_{a \in \mathbb{F}_2^n} \phi(a)(-1)^{a \cdot u}.$$

avec "$\cdot$" désigne le produit scalaire usuel sur $\mathbb{F}_2^n$, défini par : $a \cdot u = \sum_{i=1}^{n} a_i \cdot u_i$ mod 2.

La transformée de Walsh d'une fonction booléenne est un cas particulier de la transformation générale de Fourier.

Soit $x = (x_1, x_2, \ldots, x_n)$ et $a = (a_1, a_2, \ldots, a_n)$ dans $\mathbb{F}_2^n$ on notera "$\cdot$" l'opération de produit scalaire sur $\mathbb{F}_2^n$, défini par : $a \cdot u = \sum_{i=1}^{n} a_i \cdot u_i \mod 2$. Alors la transformée de *Walsh* d'une fonction f est définie par :

$$W_f(x) = \sum_{a \in \mathbb{F}_2^n} (-1)^{f(a)+a \cdot x}. \tag{3.2.1}$$

La modification du produit scalaire change l'ordre des valeurs de la transformation de Walsh mais pas l'ensemble de ses valeurs. Appelons cet *ensemble le spectre de Walsh.* Soit $x \in \mathbb{F}_{2^n}$, la *transformée de Walsh* sur le corps fini $\mathbb{F}_{2^n}$ s'écrit :

$$W_f(x) = \sum_{\alpha \in \mathbb{F}_{2^n}} (-1)^{f(\alpha)+tr(x\alpha)}. \tag{3.2.2}$$

Proposition 3.2.1. *[MS78] Égalité de Parseval :*

$$\sum_{x \in \mathbb{F}_2^n} W_f(x)^2 = 2^{2n}.$$

Démonstration. Il suffit d'écrire ce que nous donne la somme des carrés. □

Critères cryptographiques

Afin d'assurer la sécurité des systèmes cryptographiques reposant sur des fonctions booléennes comme schématisé dans la figure 3.2, ces fonctions doivent vérifier un certain nombre de propriétés. Ainsi, elles doivent être équilibrées, avoir un haut degré algébrique, avoir une bonne non-linéarité, résister aux attaques algébrique rapide et avoir une haute immunité algébrique.

Malheureusement, tous les critères ci-dessus ne peuvent être maximisés ensemble, et des compromis doivent être considérés. Pour cette raison, il est plus important de construire des fonctions booléennes cryptographiques qui répondent simultanément à plusieurs critères (et si possible à tous) avec des compromis appropriés, plutôt que de satisfaire seulement quelques critères. Dans cette section nous allons définir et caractériser ces différentes propriétés.

Équilibre et résilience

Une caractérisation en terme de transormée de *Walsh* de ce critère a été introduite par Xiao et Massey [XM88] :

Proposition 3.2.2. *(k-résilience) Une fonction booléenne f à n variables est dites k-résiliente si $W_f(x) = 0$ pour tout $x \in \mathbb{F}_2,\ 0 \leq w_H(x) \leq k$.*

Proposition 3.2.3. *(équilibre) Une fonction booléenne f à n variables est dite équilibrée ssi : $W_f(0) = 0$*

Démonstration. D'après l'équation 3.2.1, nous avons $W_f(0) = \sum_{a \in \mathbb{F}_2^n} (-1)^{f(a)} = 0$ □

Degré algébrique, non linéarité et k-résilience :

Proposition 3.2.4. *Soit $f \in \mathcal{B}$*

- *si $k \leq n-1,\ deg(f) \leq n-(k+1)$ (Siegenthaler [Sie84])*
- $nl_2(f) \leq 2^{n-1} - 2^{k+1}\left\lceil \frac{2^{n-k-2}}{\sqrt{2^n - \sum_{i=0}^{k} \binom{i}{k}}} \right\rceil$ *[Car02]*

Degré algébrique

Les attaques algébriques sont des attaques à clair connu qui exploitent des relations algébriques entre les bits du clair, ceux du chiffré et ceux de la clef secrète. La connaissance de plusieurs couples clairs-chiffrés fournit donc un système d'équations dont les inconnues sont les bits de la clef secrète.

Ces derniers peuvent alors être retrouvés en résolvant le système, ce qui est possible s'il est de degré faible, de petite taille ou qu'il possède une structure particulière.

Il convient de noter que le degré algébrique maximal d'une fonction booléenne *équilibrée* à n variables est $n-1$. Une fonction booléenne f est de degré algébrique n si et seulement si, dans sa décomposition en une somme de fonctions atomiques, le nombre de ces fonctions atomiques est impair, qui est le cas si est seulement si le poids de f, $w_H(f)$ est impair.

Non-linéarité

La non-linéarité d'une fonction booléenne f peut aussi être exprimée à l'aide de sa transformée de Walsh. De l'équation 3.2.1, nous avons :

$W_f(0) = \sum_{a\in\mathbb{F}_2^n}(-1)^{f(a)} = 2^n - 2w_H(f)$, et $w_H(f) = 2^{n-1} - \frac{1}{2}W_f(0)$.

Ainsi, $d_h(f, ax) = 2^{n-1} - \frac{1}{2}W_f(a)$ et $d_h(f, ax+1) = 2^{n-1} + \frac{1}{2}W_f(a)$,

et on obtient :

$$nl_2(f) = 2^{n-1} - \frac{1}{2}\max_{a\in\mathbb{F}_2^n}|W_f(a)| \tag{3.2.3}$$

La relation de Parseval de la proposition 3.2.1 stipule que pour toute fonction booléenne à n variables, nous avons $\sum_{x\in\mathbb{F}_2^n} W_f(x)^2 = 2^{2n}$. Ceci implique que la moyenne des valeurs prises par W_f^2 est égale à 2^n. Ainsi nous avons $\max_{a\in\mathbb{F}_2^n}|W_f(a)| \geq 2^n$. Ce qui nous donne une borne sur la non-linéarité d'une fonction booléenne à n variables (Lobanov) :

$$nl_2(f) \leq 2^{n-1} - 2^{\frac{n}{2}-1}$$

La relation de Parseval implique qu'une fonction booléenne à n variables atteint la meilleure non-linéarité si pour tout $x \in \mathbb{F}_2^n$ $|W_f(x)| = 2^{\frac{n}{2}}$. Ceci n'est possible que dans le cas où le nombre de variables est pair. On appelle ces fonctions des fonctions *courbes* [Rot76].

Proposition 3.2.5. *(fonction courbe) Une fonction booléenne à n variable est dite* courbe *si et seulement si pour toutx* $\in \mathbb{F}_2^n$ $|W_f(x)| = 2^{\frac{n}{2}}$.

Proposition 3.2.6. *(fonction semi courbe à un nombre impair n de variables) Une fonction booléenne à n variables est dite semi courbe si et seulement si pour tout* $x \in \mathbb{F}_2^n$ $W_f(x) \in \{0, \pm 2^{\frac{n}{2}+1}\}$.

Immunité algébrique

Avant 2003, le haut degré algébrique d'une fonction booléenne à n variables suffisait à assurer la sécurité du système (3.1) contre les attaques algébriques connues. Toutefois, en 2003 Courtois et Meier ont montré en [CM03b] qu'il était parfois possible de mener une attaque algébrique même quand f est de degré élevé. Dès lors qu'il existe des relations de degré faible entre les entrées et la sortie de la fonction de filtrage. De telles relations correspondent à des multiples de petit degré de f, c'est-à-dire à des relations du type

$$g(x)f(x) = h(x), \forall x \in \mathbb{F}_2$$

où la fonction h est de plus petit degré.

Toute relation de ce type est équivalente à l'existence d'un annulateur de petit degré pour la fonction f ou pour la fonction $(1+f)$, au sens de la définition suivante [MPC04],[FA03]. En multipliant la relation précédente par $f(x)$, on obtient : $g(x)f^2(x) = h(x)f(x) = g(x)f(x) = h(x)$ ce qui implique

$$h(x) = h(x)[1 + f(x)] = 0$$

Ainsi, *l'immunité algébrique* d'une fonction booléenne f dépendra de l'ensemble des annulateurs de f et de $f+1$. Notons *l'ensemble des annulateurs* de f par $AN(f) = \{g \in \mathcal{B}_n \text{ tel que } g.h = 0,\ \forall x \in \mathbb{F}_2^n\}$.

Définition 3.2.10 ([MPC04])**.** L'immunité algébrique *d'une fonction booléenne f, notée AI(f), est le degré minimal atteint par une fonction non nulle de* $AN(f) \cup AN(1+f)$.

L'ensemble $AN(f)$ des annulateurs de f est un idéal de l'anneau des fonctions booléennes, et il est engendré par la fonction $(1+f)$. Cet idéal est composé des $2^{2^n} - w_H(f)$ fonctions à n variables qui s'annulent sur le support de f. Le nombre de fonctions de $AN(f)$ de degré au plus d est donc égal à 2^k où k est la dimension du noyau de la matrice obtenue par restriction au support de f de la matrice génératrice du code de *Reed-Muller* de longueur 2^n et d'ordre d. Dans [FA03] et dans [CM03b], les auteurs ont démontré que l'immunité algébrique d'une fonction à n variables est inférieure ou égale à $\lceil \frac{n}{2} \rceil$. Par ailleurs, quand le nombre de variables n est impair, seules les fonctions équilibrées peuvent atteindre l'immunité algébrique maximale. L'immunité algébrique d'une fonction booléenne est également liée à d'autres propriétés usuelles des fonctions booléennes, notamment à la non-linéarité [DGM]. Il est en effet clair que, pour toute fonction linéaire ax, l'immunité algébrique de $f + ax$ est au plus égale à $AI(f) + 1$.

La relation entre le poids d'une fonction et son immunité algébrique nous donne [Lob05] alors

$$nl_2(f) \geq \sum_{i=0}^{AI(f)-2} \binom{n}{i}$$

Dans la section qui va suivre nous présentons un petit échantillon des constructions présentes dans la littérature. Nous allons nous concentrer surtout sur les fonctions booléennes dont l'immunité algébrique dépend de conjectures combinatoires. Ce choix est justifié par notre travail sur la conjecture de *Tu-Deng* présenté dans les chapitres 4 et 7.

Dans ce qui suit, nous allons donner un aperçu des travaux antérieurs sur les fonctions booléennes utilisées dans le chiffrement à flot.

3.3 Constructions de fonctions cryptographiques

Avant l'apparition des attaques algébriques [CM03a] l'équilibre, immunité aux corrélations, un haut degré algébrique et une non linéarité élevée étaient les quatre principales exigences pour que les fonctions booléennes utilisées dans les chiffrements à flot soient considérées comme cryptographiques. Après l'apparition de ce critère en 2003 plusieurs fonctions d'immunité algébrique optimale ont été proposées [CDGM06, DMS06, LQ06, LQQ+08, CZLH09].

Fonction majorité

D. K. Dalai, S. Maitra et S. Sarkar ont proposé dans [DMS06] une sous-classe de fonctions booléennes symétriques qui admettent la même valeur pour le même poids de la variable. Cette classe de fonctions est définie comme suit : $Maj : \mathbb{F}_2^n \to \mathbb{F}_2$,

$$Maj(x) = \begin{cases} 0 & si \quad w_H(x) < \lceil \frac{n}{2} \rceil \\ 1 & \quad\quad w_H(x) \geq \lceil \frac{n}{2} \rceil \end{cases} \tag{3.3.1}$$

Ils ont prouvé que ces fonctions sont de degré égal à $2^{\lfloor \log_2 n \rfloor}$, d'immunité algébrique égale à $\lceil \frac{n}{2} \rceil$ et qu'elles sont de non-linéarité égale à $2^{n-1} - \binom{n-1}{\lfloor \frac{n}{2} \rfloor}$. Cette classe de fonctions a été utilisée par de nombreux chercheurs par la suite pour construire des fonctions booléennes dérivées avec une immunité algébrique optimale comme on peut le voir dans [BP05, QFLW09, CL11]. Malheureusement, la majorité de ces constructions donnent lieu à une non-linéarité qui s'approche de la borne de Lobanov [Lob05] qui se trouve être la plus mauvaise non-linéarité.

Fonctions de Carlet et Feng

En 2008, *Carlet et Feng* ont mis au point la première classe infinie de fonctions qui semble en mesure de satisfaire tous les critères présentés dans la section précédente [CF08] c'est à dire une classe infinie de fonctions booléennes équilibrées à n variables définies sur le corps fini F_{2^n}, d'immunité algébrique optimale, de degré algébrique maximal, et de non-linéarité élevée. Cette classe avait été antérieurement étudiée dans [BLW06] (pour le critère de non-linéarité). Ces fonctions constituent la version booléenne d'une classe de fonctions vectorielles étudiées dans [FLY09]. Dans [WPKX10], la même classe a été présentée par *Wang et al.* d'une autre façon (comme indiqué dans [Car11]) avec une très légère amélioration de la borne inférieure de la non-linéarité. D'autres études sur cette classe ont été introduites avec de légères modifications et les mêmes paramètres. Plus tard, dans [ZCSH11], *Zeng et al* ont proposé de nouvelles fonctions équilibrées ayant presque les mêmes propriétés cryptographiques que la fonction de *Carlet-Feng* en étendant la méthode d'analyse présentée dans [Riz10].

Construction 3.3.1 (Carlet et Feng)**.** *Soit $n \geq 2$ un entier positif et α une racine primitive de $\mathbb{F}_{2^n}$. La fonction f de Carlet et Feng est définie comme suit :*

$$Supp(f) = \{0, 1, \alpha \ldots, \alpha^{2^{n-1}-2}\}$$

Carlet-Feng ont prouvé que ces fonctions sont :

1. équilibrées
2. de degré algébrique : $n - 1$
3. d'immunité algébrique optimale $\lceil \frac{n}{2} \rceil$
4. de non-linéarité supérieure à : $2^{n-1} - \frac{2ln2}{\pi} n 2^{\frac{n}{2}}$

et qu'elles offrent une bonne résistance aux attaques algébriques rapides.

Fonction de Tu et Deng

En 2010, *Tu et Deng* [TD11] ont étudié l'immunité algébrique d'une sous classe de la famille des fonctions courbes introduite par *Dillon* [Dil74], connues sous le nom de *Partial Spread* (PS).

Pour $n = 2k$, le corps fini $\mathbb{F}_2^n$ peut être vu comme un espace à 2-dimensions vecteur $\mathbb{F}_{2^k} \times \mathbb{F}_{2^k}$ sur $\mathbb{F}_{2^k}$, qui est égal à l'union disjointe des $2^k + 1$ lignes à

travers l'origine. Ainsi, en choisissant arbitrairement 2^k-1 lignes à l'exception de l'origine comme support de ses fonctions, *Dillon* a formalisé la classe des fonctions PS-ap, définies sur $\mathbb{F}_{2^k} \times \mathbb{F}_{2^k}$ et à valeurs dans $\mathbb{F}_2$ comme :

$$f(x,y) = g(xy^{2^k-2})$$

où g est une fonction booléenne équilibrée sur $\mathbb{F}_2^k$ telle que $g(0) = 0$. Partant de là, *Tu et Deng* ont proposé deux classes de fonctions :

Construction 3.3.2 (Familles de fonctions de Tu et Deng [TD11])**.** *Soient $n = 2k$ un entier positif, α une racine primitif de $\mathbb{F}_{2^n}$, et $g : \mathbb{F}_{2^k} \to \mathbb{F}_2$ une fonction booléenne à k variables, avec*

$$Supp(g) = \{\alpha^s, \alpha^{s+1} \ldots, \alpha^{s+2^{n-1}-1}\},\ 0 \leq s \leq 2^k - 2$$

Les deux classes de fonctions booléennes à n variables proposées par Tu et Deng *et leur conjecture dans [TD11] sont définies comme suit :*

- *La fonction booléenne $f_s : \mathbb{F}_{2^k} \times \mathbb{F}_{2^k} \to \mathbb{F}_2$ est définie comme suit :*

$$f_s(x,y) = \begin{cases} g(xy^{2^k-2}) & si \quad x \neq 0 \\ 0 & sinon. \end{cases} \tag{3.3.2}$$

- *La fonction booléenne $h_s : F_{2^k} \times F_{2^k} \to \mathbb{F}_2$ de est définie comme suit :*

$$h_s(x,y) = \begin{cases} g(xy^{2^k-2}) & si \quad xy \neq 0 \\ 1 & si \quad x = 0 \ et \ y \in \alpha^{2^{k-1}-1} supp(g) \\ 0 & sinon. \end{cases} \tag{3.3.3}$$

Conjecture 1 (Tu-Deng)**.** *Soit $k \geq 2$ un entier, $t \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)^*$ et posons :*

$$S_{t,k} = \{(a,b) \in (\mathbb{Z}/(2^k-1)\mathbb{Z})^2 \mid a + b = t \ et \ w_H(a) + w_H(b) < k\},$$

où w_H est le poids de Hamming. Alors $|S_{t,k}| \leq 2^{k-1}$.

Tu et Deng ont prouvé que pour tout s tel que $0 \leq \forall s \leq 2^k - 2$,

1. les fonctions f_s définies par l'équation 3.3.2 sont :
   (a) de non-linéarité maximale : courbe,

(b) non équilibrée,

(c) de degré algébrique égal à $\frac{n}{2}$,

(d) d'immunité algébrique optimale $IA(f) = \frac{n}{2}$ sous l'hypothèse que $\forall k \geq 2$, $\forall t \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)^*$, $|S_{t,k}| \leq 2^{k-1}$.

2. la fonction h_s définie par l'équation 3.3.3 sont :

(a) de non linéarité supérieure à $2^{n-1} - (2^{\frac{n}{2}-1} + \frac{n}{2}2^{\frac{n}{4}} \ln 2 - 1)$,

(b) équilibrées,

(c) de degré algébrique égal à $n-1$,

(d) d'immunité algébrique optimale $IA(f) = \frac{n}{2}$ sous le même hypothèse.

Plus tard, *Tu et Deng* ont modifié leurs fonctions booléennes définies par 3.3.2 et ils ont réussi à obtenir une autre classe de fonctions.

Construction 3.3.3 ([TD10b, TD10a]). *Soient $n = 2k \geq 3$ un entier positif, α une racine primitif de F_{2^k} et l'ensemble $A = \{0, 1, \alpha, \alpha^2 \ldots, \alpha^{2^{n-1}-1}\}$. Pour $0 \leq s \leq 2^{k-1} - 1\}$ les fonctions booléennes $f_s : F_{2^k} \times F_{2^k} \to \mathbb{F}_2$ définies par*

$$supp(f_s) = \cup \begin{cases} \{(x, \alpha^i x),\ x \in \mathbb{F}_{2^k}^*\ et\ 1+s \leq i \leq 2^{k-1}-1+s\} \\ \{(x, x),\ x \in A\} \\ \{(x, 0),\ x \in A\} \\ \{(0, x),\ x \in \alpha^s A\} \end{cases} \tag{3.3.4}$$

admettent une haute non-linéarité, une haute immunité algébrique et sont 1 *résilientes (sans corrélations d'ordre* 1 *et équilibrées).*

plus précisément, ces fonctions sont :

1. équilibrées (car 1-résilientes)
2. de degré algébrique $deg(f) = n - 2$
3. d'immunité algébrique supérieure à $\frac{n}{2} - 1$ (si l' hypothèse est vraie)
4. de non linéarités supérieures à $2^{n-1} - (2^{k-1} + 3k2^{\frac{k}{2}} \ln 2 - 7))$

Inspirés par les travaux de *Dobbertin* [Dob95], *Tang et al* ont étudié dans [TTZH10] le degré algébrique des fonctions de *Dobbertin* et ont proposé une optimisation en terme de degré qu'il ont ensuite appliqué aux fonctions de *Tu et Deng* [TD11, TD10b, TD10a]. Ceci leur a permis d' obtenir deux classes de fonctions booléennes avec une meilleure non linéarité. La première classe est composée de fonctions booléennes équilibrées, de degré algébrique optimal, d'immunité algébrique optimale et de non-linéarité élevée. La deuxième classe est composée de fonctions 1-résilientes, de degré algébrique égal à $n-2$, d'immunité algébrique supérieure à $\frac{n}{2}-1$ et de non-linéarité élevée. Malheureusement, il a été observé et démontré par la suite que ces familles sont faibles face à l'attaque algébrique rapide. En dépit de cette découverte les constructions proposées par *Tu et Deng* et leur conjecture restent intéressantes et continuent à susciter de l'intérêt.

Plus tard, inspirés par les travaux précédents de *Tu et Deng* [TD11], *Tang, Carlet et Tang* [TCT13] ont construit une famille infinie de fonctions booléennes avec de nombreuses bonnes propriétés cryptographiques. L'idée principale de leur construction est d'utiliser la fonction $g(xy)$ à la place de $g(xy^{2^k-2})$ dans la construction de *Tu et Deng*. La conjecture combinatoire associée est alors modifiée à son tour et devient.

Conjecture 2 (*Tang–Carlet–Tang* [TCT13])**.** *Soient $k \geq 2$ un entier ; $t \in \mathbb{Z}/(2^k-1)\mathbb{Z}^*$; $u \in \mathbb{Z}/(2^k-1)\mathbb{Z}$; $\gcd(u, 2^k-1) = 1$ et $\epsilon \in \{-1, 1\}$. Posons :*

$$S_{t,k} = \{(a, b) \in \mathbb{Z}/(2^k-1)\mathbb{Z}^2, \text{ tel que } ua + \epsilon b = t \text{ et } w_H(a) + w_H(b) \leq k-1\},$$

avec $w_H(a)$ est le poids de Hamming de a. Alors $|S_{t,k}| \leq 2^{k-1}$.

Enfin, *Jin et al.* dans [QJ11] ont proposé une généralisation de ces constructions en remplaçant la fonction $g(xy)$ par $g(xy^{2^k-1-u})$, avec $u \in \mathbb{Z}/(2^k-1)\mathbb{Z}$. La conjecture combinatoire s'est retrouvée à son tour généralisée en

Conjecture 3 (*Jin et al* [QJ11])**.** *Soit $k \geq 2$ un entier, $t, u, v \in \mathbb{Z}/(2^k-1)\mathbb{Z}^*$, $\gcd(u, 2^k-1) = \gcd(v, 2^k-1) = 1$. Posons :*

$$S_{t,k} = \{(a, b) \in \mathbb{Z}/(2^k-1)\mathbb{Z}^2, \text{ tel que } ua + vb = t \text{ et } w_H(a) + w_H(b) \leq k-1\}.$$

Alors $|S_{t,k}| \leq 2^{k-1}$.

Conclusion

Dans ce chapitre nous avons présenté un ensemble de constructions intéressantes du point de vue cryptographique ainsi qu'un ensemble de conjectures associées. La conjecture la plus générale est celle de *Jin et al* dans [QJ11]

Conjecture 3 (*Jin et al* [QJ11])**.** *Soient $k \geq 2$ un entier, $t, u, v \in \mathbb{Z}/(2^k - 1)\mathbb{Z}^*$, $\gcd(u, 2^k - 1) = \gcd(v, 2^k - 1) = 1$. Posons :*

$$S_{t,k} = \{(a, b) \in \mathbb{Z}/(2^k - 1)\mathbb{Z}^2, \text{ tel que } ua + vb = t \text{ et } w_H(a) + w_H(b) \leq k - 1\}.$$

Alors $|S_{t,k}| \leq 2^{k-1}$.

Elle recouvre les deux autres pour des valeurs particulières de u et v. Les valeurs de l'immunité algébrique de plusieurs classes d'entre elles dépendent exclusivement de ces conjectures. Dans la suite de cette thèse nous allons nous intéresser particulièrement à la conjecture originale de Tu et Deng.

Conjecture 1 (Tu-Deng)**.** *Soient $k \geq 2$ un entier, $t \in \mathbb{Z}/(2^k - 1)\mathbb{Z}^*$ et posons :*

$$S_{t,k} = \{(a, b) \in \mathbb{Z}/(2^k - 1)\mathbb{Z}^2, \text{ tel que } a + b = t \text{ et } w_H(a) + w_H(b) \leq k - 1\},$$

i.e w_H est le poids de Hamming. Alors $|S_{t,k}| \leq 2^{k-1}$.

Chapitre 4

Conjectures combinatoires

Ce chapitre est consacré aux conjectures combinatoires conditionnant l'optimalité de l'immunité algébrique d'un ensemble de fonctions booléennes introduites dans le chapitre 3. Plus précisément, les fonctions booléennes trouvées dans [TD10a, TD11, TD10b, TCT13, QJ11]. En 2009, une classe infinie de fonctions booléennes a été proposée par Tu et Deng [TD11] ayant de bonnes propriétés cryptographiques sous l'hypothèse que la conjecture combinatoire suivante sur les chaînes binaires soit vraie.

Conjecture 1 (Tu et Deng [TD11]). *Soit $k \geq 2$ un entier, $t \in \mathbb{Z}/(2^k-1)\mathbb{Z}^*$ et posons :*

$$S_{t,k} = \{(a,b) \in \mathbb{Z}/(2^k-1)\mathbb{Z}^2 | a+b=t \text{ et } w_H(a)+w_H(b) < k\},$$

où w_H est le poids de Hamming. Alors $|S_{t,k}| \leq 2^{k-1}$.

Plus tard, inspirés par les travaux précédents de Tu et Deng, [TD11]. Tang, Carlet et Tang [TCT13] ont construit une famille infinie de fonctions booléennes avec de nombreuses bonnes propriétés cryptographiques sous l'hypothèse que la conjecture combinatoire associée suivante soit vraie.

Conjecture 2 (Tang–Carlet–Tang [TCT13]). *Soit $k \geq 2$ un entier, $t \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)^*$, $u \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)$, $\gcd(u, 2^k-1) = 1$ et $\epsilon \in \{-1,1\}$. Posons :*

$$S_{t,k} = \{(a,b) \in (\mathbb{Z}/(2^k-1)\mathbb{Z})^2 | ua+\epsilon b = t \text{ et } w_H(a)+w_H(b) \leq k-1\},$$

où $w_H(a)$ est le poids de Hamming de a. Alors $|S_{t,k}| \leq 2^{k-1}$.

Enfin, Jin et al. dans [QJ11] ont proposé une généralisation qui a conduit à la conjecture combinatoire suivante.

Conjecture 3 (Jin et al.[QJ11]). *Soit $k \geq 2$ un entier, $t, u, v \in \mathbb{Z}/(2^k-1)\mathbb{Z}^*$, $\gcd(u, 2^k-1) = \gcd(v, 2^k-1) = 1$ et . Posons :*

$$S_{t,k} = \{(a,b) \in \mathbb{Z}/(2^k-1)\mathbb{Z}^2 | ua + vb = t \text{ et } w_H(a) + w_H(b) \leq k-1\},$$

w_H est le poids de Hamming. Alors $|S_{t,k}| \leq 2^{k-1}$.

On remarque que cette dernière conjecture recouvre les deux autres pour des valeurs particulières de u et v. En résumé, plusieurs conjectures ont été formulées et vérifiées exclusivement expérimentalement par leurs auteurs. Ainsi dans ce chapitre nous allons commencer par une section sur des généralités qui découlent directement de la définition permettant ainsi de conclure dans le cas de la conjecture de Tang, Carlet et tang [TCT13]. Ensuite, nous exposerons les différentes approches adoptées par les auteurs de [Car09a, CLS09, FRCM10, FR12, CF11] et qui ont permis de vérifier la validité de la conjecture de Tu et Deng pour des cas particuliers de t.

4.1 Généralités et conjecture de Tang, Carlet et Tang

La version la plus générale de ces conjectures combinatoires est celle introduite par Jim et al [QJ11]. Elle permet de couvrir la conjecture originale de Tu et Deng et celle de Tang, Carlet et Tang [TCT13].

Conjecture 3 (Jim et al [QJ11]). *Soient $k \geq 2$ un entier, $t, u, v \in \mathbb{Z}/(2^k-1)\mathbb{Z}$ tels que $gcd(u, 2^k-1) = pgcd(v, 2^k-1) = 1$. Alors*
$\#S_{t,v,u,k} = \#\{(a,b) \in \mathbb{Z}/(2^k-1)\mathbb{Z}^2 | ua + vb = t; w_H(a) + w_H(b) \leq k-1\} \leq 2^{k-1}$.

Ainsi, un certain nombre de propriétés que nous pouvons retrouver dans [FRCM10] ont été déduites de l'aspect cyclotomique induit par la relation d'équivalence suivante : $\forall i \in \mathbb{Z},\ 2^i a \sim a$. Pour $k \geq 2$ et $\forall t, u, v \in \mathbb{Z}/(2^k-1)\mathbb{Z}$:

- $\#S_{t,v,u,k} = \#S_{2t,u,v,k}$.
- $\#S_{t,v,u,k} = \#S_{t,u,v,k}$.
- $\#S_{t,v,u,k} = \#S_{ct,cv,cu,k}$ où, c est inversible.
- $\#S_{t,v,u,k} = \#S_{(uv)^{-1}t,v^{-1},u^{-1},k}$.

Par la suite, ces relations ont permis à G. Cohen et J.P Flori [CF11] de prouver le cas particulier de la conjecture requise par la famille de fonctions Tang, Carlet et Tang. Ces propriétés permettent de prouver la validité de la conjecture de Tang, Carlet et Tang [TCT13].

4.2 Conjecture de Tu et Deng

Plusieurs auteurs se sont intéressés à la conjecture originale de Tu et Deng. J.P. Flori. et al dans [FRCM10] ont été les premiers à s'intéresser à la conjecture de Tu et Deng pour une grande famille de t. Dans cet article les auteurs ont reformulé la conjecture en termes de retenues survenant dans une addition modulo $2^k - 1$. La **Conjecture** 1 en termes de retenues s'énonce de la façon suivante :

Reformulation 4.2.1.

$$\#S_{t,k} = \#\{a \in \mathbb{Z}/(2^k-1)\mathbb{Z} | r(a,t) > w_H(t)\} \leq 2^{k-1}$$

Où, $\forall a \in \mathbb{Z}/(2^k-1)\mathbb{Z}^*$ $r(a,t) = w_H(a) + w_H(t) - w_H(a+t)$ *et* $r(0,t) = k$.

Ceci leur a permis d'une part de trouver des expressions explicites pour certains cardinaux $S_{t,k}$ et d'autre part de montrer que la conjecture de Tu et Deng est asymptotiquement vraie. Ils ont également montré l'existence d'une famille d'entiers dont la représentation binaire contient beaucoup de "1" et des "0" isolés qui atteignent la borne de la conjecture. Pour poursuivre leur étude ils ont conjecturé que les éléments de cette famille étaient les seuls a atteindre cette limite.

Démarche et cas résolus

En utilisant un partitionnement selon le poids des éléments (a, b) qui produisent le même t par rapport à la somme modulaire, les propriétés de rotation et de négation des éléments dans $\mathbb{Z}/(2^k-1)\mathbb{Z}^2$, les auteurs de [FRCM10] observent le résultat suivant :

$$\#S_{t,k} + \#S_{-t,k} \leqslant \begin{cases} 2^k - 1 & si \quad 2t \neq -t \\ 2^k & sinon \end{cases} \tag{4.2.1}$$

Ce résultat leur permet de conclure dans le cas $t = 0$ et $t \simeq -t$. Pour continuer leur étude, ils considèrent la décomposition suivante de t :

$$t = \underbrace{\overbrace{1\ldots}^{\alpha_1}\overbrace{0\ldots0}^{\beta_1}}_{t_1}\ldots\underbrace{\overbrace{1\ldots}^{\alpha_i}\overbrace{0\ldots0}^{\beta_i}}_{t_i}\ldots\underbrace{\overbrace{1\ldots}^{\alpha_d}\overbrace{0\ldots0}^{\beta_d}}_{t_d}$$

où d est le nombre de blocs et α_i, β_i le nombre de 1 et de 0 dans le i-ième bloc, et ils cherchent à estimer le nombre de retenues produites entre t et un a lors de l'addition modulaire. Cette décomposition leur permet de calculer la valeur exacte de $\#S_{t,k}$ dans le cas ou t est composé d'un seul bloc (d=1). Ils poursuivent leur recherche en considérant les t composés de plusieurs blocs et en s'imposant comme condition que $\min_i(\alpha_i) \geq k - w_H(t) - 1$, en d'autres termes que tous les blocs de t se comportent de la même façon lors de l'addition, plus précisément une retenue se propage toujours d'un bloc à l'autre. Ainsi, la valeur exacte de $\#S_{t,k}$ ne dépend plus de l'ordre des blocs, ni de la valeur des α_i. Ce qui leur permet d'avoir une expression approximative de $P_{t,k} = 2^{-k}\#S_{t,k}$ sous une forme polynomiale qu'ils notent $f_d(\beta_1, \ldots, \beta_d)$.

Cette approximation leur permet de conclure dans le cas où t est de la forme $1^{\beta_1}0 \ldots 1^{\beta_d}0$. Une étude analytique des t composés de deux blocs leur permet de retrouver une expression explicite du cardinal. Ensuite une étude analytique plus poussée à l'aide de séries hypergéométriques de f_d permet d'exprimer la limite de f_d quand les β_i tendent vers l'infini (i.e $\lim_{\beta_i \to \infty} f_d(\beta_1, \ldots, \beta_d) = \frac{1}{2}(1 - P_d)$). Plus tard Flori a poursuivi ses investigations avec Randriam dans [FR12]. On y trouve une étude très poussée qui exhibe des propriétés supplémentaires de $P_{(t,k)}$. En généralisant l'approche dans [CF11] pour un nombre de blocs plus élevé ils expriment $f_d(\beta_1, \ldots, \beta_d)$ sous une forme close faisant intervenir des polynômes multivariés symétriques à n variables.

Pour conclure, ils ont fourni également des résultats expérimentaux établissant la validité de la conjecture de Tu et Deng jusqu'à 40 bits, prolongeant ainsi les résultats de Tu et Deng [TD11].

Les cas résolus

Plusieurs auteurs se sont intéressés à ce problème combinatoire, et ainsi on trouve dans [Car09a, CLS09] quelques cas résolus. Dans ce paragraphe on regroupe les résultats en fonction de la forme ou du poids de t.

Soit $k > 40$, et $t \in \mathbb{Z}/(2^k - 1)\mathbb{Z}^2$

1. Carlet [Car09a] prouve la conjecture pour t de la forme :
   - $w_H(t) = 0$ ou 1.
   - $t = 2^i - 2^j$.
2. Cusick et al.[CLS09] ont prouvé la conjecture dans les cas suivants :
   - t, $w_H(t) = 1$ ou 2,
   - $t = 2^k - t'$ avec $w(t') \leq 2$ pair,
   - $t = 2^k - t'$ avec $w(t') \leq 4$ impair,
3. Cheng et al.[CHZ15] ont prouvé la conjecture dans les cas suivants :

- Pour t, $w_H(t) = 1, 2$ ou 3, Ils ont trouvé une formule explicite du cardinal, ainsi qu'une borne dans le cas t, $w_H(t) = 4$.

Depuis, plusieurs auteurs ont attaqué le problème malheureusement un grand nombre de leur résultats restent à vérifier.

4.3 Conclusion

Jusqu'à ce jour, une preuve complète de la conjecture originale de Tu et Deng est toujours un problème ouvert malgré plusieurs tentatives et démonstrations non fructueuses, et des études inductives et analytiques très poussées réalisées notamment par les auteurs de [Car09a, FRCM10, FR12, CLS09]. Les résultats apportés par ces chercheurs ont contribué à une meilleure compréhension de ces conjectures combinatoires.
Pour conclure ce chapitre, notons qu'une approche inductive et naïve semble difficile à mettre en place ; de nombreuses données expérimentales soutiennent cette affirmation. Enfin, d'un point de vue calculatoire, la validité de leur conjecture est vérifiée jusqu'à $k = 40$ dans [FRCM10, FR12].

Dans la deuxième partie de cette thèse nous allons nous intéresser à la conjecture de Tu et Deng. Bien que nous ne donnons pas une preuve complète de sa validité, nous exhiberons dans cette partie une nouvelle famille de t appuyant la validité de cette conjecture ainsi qu'un ensemble de propriétés combinatoires sur la somme modulaire et le poids de Hamming des couples (a, b).

Deuxième partie

Contributions

Chapitre 5

Fonctions quaternaires courbes

Dans ce chapitre nous nous concentrons sur une propriété bien précise des fonctions quaternaires : la non-linéarité ; et plus particulièrement sur les fonctions quaternaires dites courbes (qui atteignent la $nl_4^L(F) = 4^m - 2^m$).

Nous allons décrire une méthode de construction algébrique permettant de générer un ensemble de fonctions quaternaires courbes : F_k à m variables avec $0 \leq k \leq 2^m - 2$. Cette méthode fait intervenir des notions de la théorie de *Galois* et d'algèbre linéaire : classes cyclotomiques, extension algébrique, corps résiduel, b-polynôme, espace vectoriel, dualité algébrique.

L'organisation de ce chapitre est la suivante. Nous commençons dans la section 5.1 par décrire une méthode de construction d'un ensemble de fonctions quaternaires à m variables $(F_k)_{k\in\{0\ldots 2^m-2\}}$ sur l'anneau de *Galois* $GR(4, m)$ faisant intervenir des fonctions intermédiaires $(h_k)_{k\in\{0\ldots 2^m-2\}}$ sur des ensembles plus petits que nous désignons par $\mathfrak{C}_k$. Enfin, nous allons exhiber des conditions nécessaires et suffisantes sur les fonctions intermédiaires $(h_k)_{k\in\{0\ldots 2^m-2\}}$ pour que les fonctions quaternaires associées soient courbes. De plus, nous verrons plus en détail comment générer efficacement des fonctions quaternaires courbes à partir de modèles prédéfinis en s'affranchissant ainsi du caractère assez technique des conditions sur les fonctions intermédiaires. Ce qui nous permet d'alléger considérablement la construction et nous terminerons ce chapitre par un exemple de construction de fonctions à 7 variables.

5.1 Notions de bases et définitions

Nous commençons cette section par rappeler des notions de bases tirées de la théorie de *Galois* que nous adaptons à notre situation dans le but de

décrire notre environnement de travail. Comme nous l'avons vu précédemment une fonction quaternaire F à m variables est une fonction définie sur $\mathbb{Z}_4^m$ à valeurs dans $\mathbb{Z}_4$. Intéressons-nous maintenant à l'ensemble de définition de cette fonction. Ici, nous allons considérer la structure d'anneau de Galois sur $\mathbb{Z}_4^m$. Comme décrit dans la section 1.2 du chapitre 1, nous avons :

$$R \simeq \mathbb{Z}_4^m \simeq GR(4,m) \simeq \mathbb{Z}_4[x]/(g(x)) \simeq \mathbb{Z}_4[\beta],$$

où $g(x)$ un b-polynôme de degré m et β une racine primitive d'ordre 2^m-1 de $g(x)$ (ou racine m-ième de l'unité d'ordre 2^m-1).

À présent nous rappelons les ensembles qui nous intéressent. Désignons par R l'anneau de Galois à 4^m éléments et notons :

- $\mathcal{T} = \{0, 1, \beta, \cdots, \beta^{2^m-2}\}$ le système Teichmüller.
- $D = 2R = 2\mathcal{T} = \{0, 2, 2\beta, \cdots, 2\beta^{2^m-2}\}$ l'ensemble des diviseurs de zero de R.
- $R^* = \{z_1(1+2z_0),\ z_0 \in \mathcal{T}, z_1 \in \mathcal{T} \setminus \{0\}\}$ le groupe multiplicatif de l'anneau R.

Avec ces notations nous avons :

$$R = GR(4,m) = R^*/\mathcal{T} \cup D \cup \mathcal{T}$$

Nous utiliserons dans notre construction un partitionnement bien particulier du groupe multiplicatif R^* de l'anneau R. Avant de parler de ce partitionnement à l'aide des classes cyclotomiques que nous définirons un peu plus loin, nous reformulons la représentation multiplicative des éléments de R, comme suit :

$$\forall z \in R, \qquad z = \begin{cases} \beta^j & si \quad z \in \mathcal{T}^* \\ 2\beta^j & si \quad z \in D^* \\ \beta^i + 2\beta^j & si \quad z \in R^*/\mathcal{T} \\ 0 & if \quad z = 0 \end{cases} \qquad \begin{array}{c} \text{(représentation multiplicative),} \\ 0 \leq j, i \leq 2^m - 2 \end{array}$$

cette représentation découle de la représentation 2-adique 5.1.1 que nous rappelons ici :

$$\forall z \in R, \exists!\ x_1, x_2 \in \mathcal{T} : z = x_1 + 2x_2. \tag{5.1.1}$$

Nous pouvons maintenant définir le partitionnement de R^* comme ci dessous :

Définition 5.1.1 (Classes cyclotomiques)**.** *Soit R l'anneau de Galois à 4^m éléments et R^* son groupe multiplicatif à $2^m(2^m-1)$ éléments. Les 2^m classes cyclotomiques $(C_j)_j$ d'ordre 2^m-1 de R^* sont définies par*

$$\forall j,\ 0 \le j \le 2^m-2, \qquad \begin{array}{l} C_j = \{\beta^l(1+2\beta^j),\ 0 \le l \le 2^m-2\} \\ C_{2^m-1} = \{\beta^l,\ 0 \le l \le 2^m-2\} = \mathcal{T}^*. \end{array}$$

On a ainsi le partitionnement suivant :

$$R^* = \cup_{j=0}^{2^m-1} C_j \text{ et } R = R^* \cup D = \cup_{j=0}^{2^m-1} C_j \cup D. \tag{5.1.2}$$

5.1.1 Définitions

Nous allons maintenant pouvoir définir nos fonctions quaternaires F_k sur R, en considérant conjointement l'écriture 2-adique des éléments de R équation 5.1.1 et le partitionnement de R équation 5.1.2.

Soit k un entier naturel compris entre 0 et 2^m-2, on définit l'ensemble $\mathfrak{C}_k$ par

$$\mathfrak{C}_k = \{\beta^k\} \cup \{\beta^k(1+2\beta^j),\ 0 \le j \le 2^m-2\}. \tag{5.1.3}$$

Cet ensemble est l'ensemble de définition de la fonction interne h_k qui nous permettra de construire F_k.

Définition 5.1.2. *Pour un $k \in \{0,1,..,2^m-2\}$, nous définissons la fonction quaternaire F_k à m-variables comme suit :*

$$\begin{array}{rccl} F_k & : & R & \to & \mathbb{Z}_4 \\ & & x_1+2x_2 & \to & F_k(x_1+2x_2) = h_k(\beta^k(1+2x_2{x_1}^{2^m-2})) \end{array} \tag{5.1.4}$$

avec la fonction interne $h_k : \mathfrak{C}_k \to \mathbb{Z}_4$.

De part la définition précédente on remarque que la fonction quaternaire $F_{k,\ 0\le k\le 2^m-2}$ reste constante sur les classes cyclotomiques $(C_j)_{0\le j\le 2^m-2}$. Nous pouvons alors redéfinir $F_{k,\ 0\le k\le 2^m-2}$.

Proposition 5.1.1 (Caractérisation de F_k)**.** *La fonction quaternaire F_k est constante sur le partitionnement défini dans 5.1.2 et peut être caractérisée par :*

$$\forall x \in R, \begin{cases} F_k(x) = h_k(\beta^k(1+2\beta^j)) & si \quad x \in C_j,\ 0 \le j \le 2^m-2. \\ F_k(x) = h_k(\beta^k) & si \quad x \in C_{2^m-1} \cup D. \end{cases} \tag{5.1.5}$$

Démonstration. Considérons le partitionnement de la proposition 5.1.2,

$$R = R^* \cup D = \cup_{j=0}^{2^m-1} C_j \cup D$$

$x \in R$ s'écrit comme $x = x_1 + 2x_2$ avec $x_1, x_2 \in \mathcal{T}$ (écriture 2-adique équation 5.1.1). Ainsi, pour $x \in C_{2^m-1} \cup D$ nous avons $F_k(x) = h_k(\beta^k)$ qui découle directement de la définition 5.1.4 car $x_1 = 0$ ou $x_2 = 0$.

Sinon pour tout j compris entre 0 et $2^m - 2$; nous avons $x \in C_j$ implique qu'il existe un unique l entre 0 et $2^m - 2$ tel que $x = \beta^l + 2\beta^{j+l}$.

De plus, nous avons pour tout $l_{0 \leq l \leq 2^m-2}$,

$$F_k(x) = h_k(\beta^k(1 + 2\beta^{j+l}\beta^{(2^m-2)l})) = h_k(\beta^k(1 + 2\beta^j)).$$

□

Ce regroupement nous permet de restreindre la recherche de l'ensemble image de 4^m éléments à un ensemble image à 2^m. Nous présenterons dans la section suivante des conditions qui nous permettent de garantir que les fonctions quaternaires générées sont courbes.

5.2 Conditions suffisantes sur h_k

L'idée ici est de faire une analyse spectrale d'une fonction quaternaire F_k définie par la définition 5.1.2 afin de déterminer les conditions suffisantes sur sa fonctions interne h_k pour que F_k soit courbe.

Pour cela, nous avons besoins d'un certain nombre de résultats techniques sur les sommes exponentielles des anneaux de Galois, ces résultats sont rappelés ici :

Lemme 5.2.1. *Soit $\mathcal{T}$ le système Teichmüller de l'anneau de Galois R.*

- $\sum_{x \in \mathcal{T}} i^{Tr(x)} = \pm 2^{\frac{m}{2}} e^{i\pi m/4} = \lambda.$
- $\forall a \in R : \sum_{x \in \mathcal{T}} i^{Tr(ax)} = \begin{cases} 2^m & si\ a = 0. \\ 0 & si\ a \in 2\mathcal{T}^*. \\ \bar{\lambda} i^{Tr((1+u)^2)} & si\ a \in (1+2u)\mathcal{T}^*, u \in \mathcal{T}. \end{cases}$ *avec* $\bar{\lambda}$ *le conjugué de* λ.

Démonstration. Voir [Car09b]. □

De plus, nous pouvons définir la loi interne sur le Teichmüller comme ci-dessous.

Définition 5.2.1. *On définit la loi interne $\oplus$ sur le Teichmüller par :*

$$\forall a, b \in \mathcal{T}, \quad a \oplus b = a + b + 2(ab)^{2^{m-1}}.$$

Nous pouvons à présent résumer les conditions suffisantes sur h_k pour que F_k soit courbe comme suit.

Proposition 5.2.1. *Si h_k est équilibrée sur $\mathfrak{C}_k$ et*

$$\forall x \in \mathcal{T}, \ |\sum_{v \in \mathcal{T}} i^{h_k(\beta^k(1+2v))-Tr(v\oplus x)}| = 2^{\frac{m}{2}},$$

alors la fonction quaternaire F_k est courbe.

Démonstration. Ici, nous allons étudier la transformée de Walsh de F_k.

Considérons $x, z \in R$ alors de la représentation 5.1.1 :

$$\exists! \ x_1, x_2, z_1, z_2 \in \mathcal{T} \text{ tel que, } \begin{cases} x = x_1 + 2x_2 \\ z = z_1 + 2z_2 \end{cases}$$

et

$$\begin{aligned} W_{F_k}(x) &= \sum_{z \in R} i^{F_k(z)+Tr(xz)} \\ &= \sum_{z_1+2z_2 \in R} i^{F_k(z_1+2z_2)+Tr((z_1+2z_2)(x_1+2x_2))} \\ &= \underbrace{\sum_{z_1+2z_2 \in R^*} i^{F_k(z_1+2z_2)+Tr((z_1+2z_2)(x_1+2x_2))}}_{(*)} \\ &\quad + \sum_{z_2 \in \mathcal{T}} i^{F_k(2z_2)+Tr(2z_2x_1)} \end{aligned} \tag{5.2.1}$$

Nous savons que $R^* = \cup_{j=0}^{2^m-1} C_j$ avec $C_j = \{\beta^l(1+2\beta^j), \ 0 \leq l \leq 2^m - 2\}$(voir représentation 5.1.1). Ainsi, nous pouvons déduire que les éléments d'une classe C_j peuvent être représentés comme des éléments de la forme $\beta^l(1+2v)$ avec l entre 0 et $2^m - 2$ et $v = 0$ si $j = 2^m - 1$ et $v = \beta^j$ sinon.

En appliquant cette remarque à la première partie (*) de l'équation (5.2.1) nous obtenons :

$$\begin{aligned}(*) &= \sum_{v\in\mathcal{T}}\sum_{l=0}^{2^m-2} i^{F_k(\beta^l(1+2v))+Tr(\beta^l(1+2v)(x_1+2x_2))} \\ &= \sum_{v\in\mathcal{T}}\sum_{l=0}^{2^m-2} i^{h_k(\beta^k(1+2v))+Tr(\beta^l(1+2v)(x_1+2x_2))} \qquad (5.2.2)\end{aligned}$$

Comme la fonction quaternaire F_k est constante sur les classes cyclotomiques alors 5.2.2 devient :

$$(*) = \sum_{v\in\mathcal{T}} i^{h_k(\beta^k(1+2v))} \sum_{l=0}^{2^m-2} i^{Tr(\beta^l(1+2v)(x_1+2x_2))} \qquad (5.2.3)$$

$$= \sum_{v\in\mathcal{T}} i^{h_k(\beta^k(1+2v))} \sum_{\omega\in\mathcal{T}^*} i^{Tr(\omega(1+2v)(x_1+2x_2))} \qquad (5.2.4)$$

Enfin l'équation 5.2.1 devient :

$$\begin{aligned}W_{F_k}(x_1+x_2) &= \sum_{v\in\mathcal{T}} i^{h_k(\beta^k(1+2v))} \sum_{\omega\in\mathcal{T}^*} i^{Tr(\omega(1+2v)(x_1+2x_2))} \\ &\quad + i^{h_k(\beta^k)} \sum_{z_2\in\mathcal{T}} i^{Tr(2z_2x_1)} \qquad (5.2.5)\end{aligned}$$

Nous allons maintenant procéder à un raisonnement par disjonction de cas selon les valeurs prises par x_1 et x_2.

Cas 1 : $\underline{x \in D}$ (c-à-d $x_1 = 0$) alors

$$W_{F_k}(2x_2) = \sum_{v\in\mathcal{T}} i^{h_k(\beta^k(1+2v))} \sum_{\omega\in\mathcal{T}^*} i^{Tr(2\omega x_2))} + 2^m i^{h_k(\beta^k)},$$

et comme h_k est équilibrée sur $\mathfrak{C}_k$ on obtient directement que $W_{F_k}(2x_2) = 2^m i^{h_k(\beta^k)}$. Et ainsi $\mid W_{F_k}(2x_2) \mid = 2^m$.

Cas 2 : $\underline{x \in R^*}$ (c-à-d $x_1 \neq 0$). De plus, nous savons du lemme 5.2.1 que :

$$\sum_{z_2\in\mathcal{T}} i^{Tr(2z_2x_1)} = 0$$

et ainsi, l'équation 5.2.5 devient :

$$\begin{aligned} W_{F_k}(x_1+2x_2) &= \sum_{v\in\mathcal{T}} i^{h_k(\beta^k(1+2v))} \sum_{\omega\in\mathcal{T}^*} i^{Tr(\omega(1+2v)(x_1+2x_2))} \\ &= \sum_{v\in\mathcal{T}} i^{h_k(\beta^k(1+2v))} \sum_{\omega\in\mathcal{T}} i^{Tr(\omega(1+2v)(x_1+2x_2))} \\ &\quad - \sum_{v\in\mathcal{T}} i^{h_k(\beta^k(1+2v))} \end{aligned} \tag{5.2.6}$$

et puisque la fonction h_k est équilibrée sur $\mathcal{T}$ alors,

$$W_{F_k}(x_1+2x_2) = \sum_{v\in\mathcal{T}} i^{h_k(\beta^k(1+2v))} \sum_{\omega\in\mathcal{T}} i^{Tr(\omega(1+2v)(x_1+2x_2))} \tag{5.2.7}$$

Nous allons maintenant nous intéresser à la deuxième somme de l'équation 5.2.7. Puisque $x_1 \neq 0$ alors

$$(1+2v)(x_1+2x_2) = x_1(1+2v)(1+2\frac{x_2}{x_1}) = x_1(1+2(v+\frac{x_2}{x_1})).$$

De plus, on remarque que $2(v+\frac{x_2}{x_1}) = 2(v\oplus\frac{x_2}{x_1})$ et ainsi l'élément $(1+2v)(x_1+2x_2)$ appartient à $(1+2y)\mathcal{T}^*$ avec $y=(v+\frac{x_2}{x_1})$.
En reprenant les notations du lemme 5.2.1 avec $a=(1+2v)(x_1+2x_2)$, on retrouve :

$$\sum_{\omega\in\mathcal{T}} i^{Tr(\omega x_1(1+2y))} = \bar{\lambda} i^{Tr((1+y)^2)} = \bar{\lambda} i^{Tr(1+3y)} = \bar{\lambda} i^m i^{-Tr(y)},$$

et ainsi

$$W_{F_k}(x_1+2x_2) = \bar{\lambda} i^m \sum_{v\in\mathcal{T}} i^{h_k(\beta^k(1+2v))-Tr(y)}.$$

Enfin puisque $|\sum_{v\in\mathcal{T}} i^{h_k(\beta^k(1+2v))-Tr(y)}| = 2^{\frac{m}{2}}$ (Proposition 5.2.1), alors

$$| W_{F_k}(x_1+2x_2) | = 2^m.$$

□

Dans la section suivante nous allons prouver qu'il n y a pas d'incohérence entre les deux conditions de la Proposition 5.2.1.

5.3 Existence de h_k

À présent, nous allons nous concentrer sur les fonctions internes h_k et proposer une méthode de construction efficace qui assure que les conditions citées dans la proposition 5.2.1 sont vérifiées. Tout d'abord, intéressons-nous à la première condition de la proposition 5.2.1 : l'équilibre de h_k sur $\mathcal{T}$. Nous remarquons que le système Teichmüller $(\mathcal{T}, \oplus)$ est un $\mathbb{F}_2$-espace vectoriel de dimension m. Ainsi nous pouvons ramener le problème de vérification de l'équilibre de h_k sur $\mathcal{T}$ à un problème de recherche de bon partitionnement de $\mathcal{T}$ en quatre parties distinctes de même cardinale. Pour cela, nous utiliserons la dualité algébrique en considérant la structure de $\mathbb{F}_2$ -espace vectoriel du système Teichmüller $\mathcal{T}$.

Ici, nous énonçons le théorème qui va nous permettre de partitionner l'ensemble de définition de la fonction interne h_k.

Théorème 5.3.1. *Soit $L(x, y)$ une fonction bilinéaire, symétrique et non-dégénérée de $(\mathcal{T}, \oplus)$ sur $2\mathbb{F}_2 = \{0, 2\}$ et*

$$\forall x \in \mathcal{T} \begin{cases} l_1(x) = L(b_1, x) \\ l_2(x) = L(b_2, x) \\ l_3(x) = L(b_3, x) \end{cases} \quad \begin{array}{c} \textit{trois fonctions équilibrées} \\ \textit{avec } b_1 \neq b_2 \neq 0 \textit{ et} \\ b_3 = b_1 \oplus b_2 \end{array}$$

Notons $\mathcal{T}^\star$ le dual de $\mathcal{T}$ et considérons $B^\star = \{l_1, l_2\}$ un sous ensemble de $\mathcal{T}^\star$. L' orthogonal de l'ensemble $B = \{0, b_1, b_2, b_3\} \subset \mathcal{T}$ est définit par $B^\perp = \{x \in \mathcal{T} \mid l_i(x) = 0,\ i = 1, 2\}$ et ainsi, si b_1, b_2 et b_3 ne sont pas dans $B^\perp$ alors $\sharp[B^\perp] = 2^{m-2}$ et $B^\perp \oplus B = \mathcal{T}$.

Démonstration. Pour tout k dans $\{0, 2\}$ et j dans $\{1, 2, 3\}$ nous définissons :

$$\begin{aligned} S_j^k &= \{x \in \mathcal{T},\ l_j(x) = k\} \\ \eta_k(l_j) &= \sharp[S_j^k] \end{aligned} \tag{5.3.1}$$

Comme l_1, l_2 et l_3 sont équilibrées sur $\mathcal{T}$, alors :

$$\forall j,\ 1 \leq j \leq 3 : \eta_0(l_j) = \eta_2(l_j) = 2^{m-1}.$$

De plus, comme $l_3(x) = L(b_3, x) = L(b_1, x) + L(b_2, x) = l_1(x) + l_2(x)$ on a

$$\sharp[S_3^0] = \sharp[\{x \in \mathcal{T},\ l_1(x) = l_2(x) = 2\} \cup \{x \in \mathcal{T},\ l_1(x) = l_2(x) = 0\}] = 2^{m-1}$$

et

$$\sharp[S_3^2] = \sharp[\{x \in \mathcal{T},\ l_1(x) \neq l_2(x)\}] = 2^{m-1}.$$

Par conséquent,

$$(*)\begin{cases} \sharp[S_1^2 \cap S_2^2 \cup S_1^0 \cap S_2^2] = \sharp[S_2^2 \cap (S_1^2 \cup S_1^0)] = \sharp[S_2^2 \cap \mathcal{T}] & = & 2^{m-1} \\ \sharp[S_1^2 \cap S_2^2 \cup S_1^2 \cap S_2^0] = \sharp[S_1^2 \cap (S_2^2 \cup S_2^0)] = \sharp[S_1^2 \cap \mathcal{T}] & = & 2^{m-1} \\ \sharp[S_1^2 \cap S_2^0 \cup S_1^0 \cap S_2^2] = 2^{m-1} & & . \end{cases}$$

En notant

$$\begin{cases} a = \sharp[S_1^2 \cap S_2^2] \\ b = \sharp[S_1^0 \cap S_2^2] \\ c = \sharp[S_1^2 \cap S_2^0], \end{cases}$$

le système $(*)$ devient :

$$\begin{cases} a + b = 2^{m-1} \\ a + c = 2^{m-1} \\ b + c = 2^{m-1} \end{cases}$$

par conséquent, $a = b = c = 2^{m-2}$ et ainsi

$$\sharp[B^\perp] = 2^{m-2}.$$

De plus, comme $B \cap B^\perp = \{0\}$ (car b_1, b_2 et b_3 n'appartiennent pas $B^\perp$) alors B est le supplémentaire de $B^\perp$ sur $\mathcal{T}$ et ainsi $B^\perp \oplus B = \mathcal{T}$.

□

Proposition 5.3.1. *Considérons les notations du théorème 5.3.1. Soient $L(x, y) = 2Tr(xy)$, et b_1,$b_2 \in \mathcal{T}^*$ avec $b_1 \neq b_1$, $Tr(b_1)$ paire et $Tr(b_1 b_2)$ impaire. Alors B est un hyper plan défini par $B = \{b_0 = 0, b_1, b_2, b_3 = b_1 \oplus b_2\}$ et $\mathcal{T} = B^\perp \oplus B$.*

Démonstration. La fonction $2Tr(xy)$ est une fonction bilinéaire, symétrique et non-dégénérée de $(\mathcal{T}, \oplus)$ dans $2\mathbb{F}_2$. De plus, en utilisant le lemme 5.2.1 on obtient que $l_1(x) = 2Tr(b_1 x)$, $l_2(x) = 2Tr(b_2 x)$ et $l_3(x) = 2Tr(b_3 x)$ sont équilibrées. Il est facile de remarquer que b_1, b_2 et b_3 ne sont pas dans $B^\perp$ puisque $2Tr(b_1 b_2)$ et $2Tr(b_1 b_3)$ sont différents de zéro.

□

Maintenant, il est possible d'exploiter le partitionnement conditionné par la parité de b_1, b_2 et la fonction bilinéaire $2Tr(x_1 x_2)$ dans le but de vérifier qu'il n y a pas de contradiction entre les deux conditions de la proposition 5.2.1.

Proposition 5.3.2 (Construction de h_k)**.** *Soient b_1 et b_2 deux éléments différents de $\mathcal{T}^*$ tels que $Tr(b_1)$ est paire $Tr(b_1b_2)$ est impaire. Soit $\alpha_j \in \mathbb{Z}_4$, $0 \leq j \leq 3$ tel que :*

$$\begin{cases} |\, i^{\alpha_0} + i^{\alpha_1} + i^{\alpha_2} + i^{\alpha_3} \,| &= 2 \\ |\, i^{\alpha_0} + i^{\alpha_1} - i^{\alpha_2} - i^{\alpha_3} \,| &= 2 \\ |\, i^{\alpha_0} - i^{\alpha_1} + i^{\alpha_2} - i^{\alpha_3} \,| &= 2 \\ |\, i^{\alpha_0} - i^{\alpha_1} - i^{\alpha_2} + i^{\alpha_3} \,| &= 2 \end{cases} \tag{5.3.2}$$

avec

$$\alpha_i + Tr(b_i) \neq \alpha_j + Tr(b_j),\ \forall i \neq j. \tag{5.3.3}$$

Alors la fonction interne h_k définie par :

$$\forall j,\ 0 \leq j \leq 3,\ \forall x \in B^{\perp} \oplus b_j,\ h_k(\beta^k(1+2x)) = \alpha_j + Tr(b_j) \tag{5.3.4}$$

vérifie les conditions de la proposition 5.2.1.

Démonstration. La condition l'équation 5.3.3 suffit à prouver que la h_k définie par l'équation 5.3.4 est équilibrée sur $\mathcal{T}$.
Intéressons-nous maintenant à la deuxième condition de équation 5.2.1 :

$$\forall x \in \mathcal{T},\ |\sum_{v \in \mathcal{T}} i^{h_k(\beta^k(1+2v)) - Tr(v \oplus x)}| = 2^{\frac{m}{2}}.$$

Notons cette quantité $S(x)$ et démontrons que pour tout x dans $\mathcal{T}$, $S(x) = 2^{\frac{m}{2}}$. Considérons $E_i = \{v \in \mathcal{T},\ v = u \oplus b_i,\ u \in B^{\perp}\}$, $0 \leq i \leq 3$. Ainsi $\mathcal{T} = \biguplus_{i=0}^{3} E_i$, comme $Tr(v \oplus x) = Tr(x) + Tr(v(1+2x))$, on a

$$\begin{aligned} S(x) &= i^{-Tr(x)} \sum_{i=0}^{3} \sum_{v \in E_i} i^{h_k(\beta^k(1+2v)) - Tr(v(1+2x))} \\ &= i^{-Tr(x)} \sum_{i=0}^{3} \sum_{v \in E_i} i^{\alpha_i + Tr(b_i) - Tr(v(1+2x))}. \end{aligned} \tag{5.3.5}$$

De plus,

$$\begin{aligned} Tr(v(1+2x)) &= Tr((u \oplus b_i)(1+2x)) \\ &= Tr((u + b_i + 2(ub_i)^{2^{m-1}})(1+2x)) \end{aligned}$$

avec $Tr(2(ub_i)^{2^{m-1}}) = Tr(2(ub_i)$ et pour tout $u \in B^{\perp}$ $2Tr(ub_i) = 0$ alors :

$$Tr(v(1+2x)) = Tr(b_i) + 2Tr(xb_i) + Tr(u(1+2b_i)).$$

En remplaçant cette valeur dans l'équation 5.3.5 on obtient :

$$S(x) = i^{-Tr(x)}(\underbrace{\sum_{i=0}^{3} i^{\alpha_i} i^{2Tr(xb_i)}}_{S_1(x)})(\underbrace{\sum_{u\in B^\perp} i^{-Tr(u(1+2x))}}_{S_2(x)}).$$

Considérons $x \in \mathcal{T}$, nous savons que $\mathcal{T} = \biguplus_{i=0}^{3} E_i$ et donc il existe $0 \leq j \leq 3$ et $x_0 \in B^\perp$ tel que $x = x_0 \oplus b_j$ et ainsi

$$2Tr(xb_i) = 2Tr(b_ib_j) \quad (5.3.6)$$
$$Tr(u(1+2x)) = Tr(u(1+2x_0)) \quad (5.3.7)$$

en accordant la parité de $Tr(b_1)$, $Tr(b_1b_2)$ et la condition 5.3.2 nous obtenons que :

$$\mid S_1(x) \mid = \mid \sum_{i=0}^{3} i^{\alpha_i}(-1)^{Tr(b_ib_j)} \mid = 2$$

Intéressons-nous maintenant à $S_2(x)$. Nous savons du lemme 5.2.1 que :

$$\mid \sum_{v\in\mathcal{T}} i^{-Tr(v(1+2x_0))} \mid = \mid \sum_{v\in\mathcal{T}} i^{Tr(v(1+2(1\oplus x_0)))} \mid = 2^{\frac{m}{2}}$$

de plus comme,

$$\begin{aligned}\textstyle\sum_{v\in\mathcal{T}} i^{-Tr(v(1+2x_0))} &= \textstyle\sum_{i=0}^{3}\sum_{v\in E_i} i^{-Tr(v(1+2x_0))} \\ &= \textstyle\sum_{i=0}^{3} i^{-Tr(b_i)}\sum_{u\in B^\perp} i^{-Tr(u(1+2x_0)))} \\ &= \textstyle\sum_{i=0}^{3} i^{-Tr(b_i)} S_2(x)\end{aligned}$$

et

$$\mid \sum_{i=0}^{3} i^{-Tr(b_i)} \mid = \mid 1 + i^{-Tr(b_1)} + i^{-Tr(b_2)} + i^{-Tr(b_3)} \mid = 2$$

alors $\mid S_2(x) \mid = \frac{1}{2} \mid \sum_{v\in\mathcal{T}} i^{-Tr(v(1+2x_0))} \mid$.

Ce qui permet de conclure puisque : $\mid S(x) \mid = \mid S_1(x) \mid \times \mid S_2(x) \mid = 2^{\frac{m}{2}}$.

□

5.4 Modélisation

Dans cette section nous cherchons à identifier un certain nombre de modèles et un nombre de transformations nous permettant de couvrir toutes les fonctions quaternaires courbes qu'il nous est possible de construire grâce à notre méthode.

Dans la section précédente nous avons mis en place une dissociation de condition en rajoutant des paramètres $\alpha_j,\ \forall j,\ 0 \leq j \leq 3$ supplémentaires à la construction. Nous permettons ainsi de disposer d'un plus grand degré de liberté. En effet, les $\alpha_{j,\ 0\leq j\leq 3}$ démultiplient les méthodes de construction d'une même fonction interne et produisent ainsi une classe de fonctions quaternaires courbes, permettant ainsi d'explorer et d'extraire les classes de valeurs qui laissent la construction invariante.

Proposition 5.4.1 (modélisation de h_k)**.** *Pour toute fonction interne h_k définie par l'équation 5.3.4 et vérifiant la condition 5.3.3 il existe b_1, b_2 dans $\mathcal{T}$ vérifiant les conditions de la proposition 5.3.1 et $\alpha_j \in \mathbb{Z}_4,\ 0 \leq j \leq 3$ satisfaisant la condition du système 5.3.2.*

Démonstration. Soit le 4-uplet $(a_0, a_1, a_2, a_3) \in \mathbb{Z}_4$ et h_k une fonction définie par l'équation 5.3.4 avec :

$$a_j = \alpha_j + Tr(b_j),\ \forall j,\ 0 \leq j \leq 3 \tag{5.4.1}$$

Comme la fonction h_k vérifie la condition 5.3.3, alors les a_j sont tous différents, et donc il existe exactement 24 uplets possibles (soit 24 fonctions h_k équilibrées possibles). En remarquant que si la fonction construite h_k est équilibrée alors la fonction $h_k + l$ (pour l, $0 \leq l \leq 3$) l'est aussi. On gardera que les six fonctions génératrices.

Nous transcrivons dans la table ci-dessous ces six fonctions (4- uplet) :

Fonctions h_k				
n^o	a_0	a_1	a_2	a_3
1	0	1	3	2
2	0	1	2	3
3	0	2	1	3
4	0	2	3	1
5	0	3	1	2
6	0	3	2	1

TABLE 5.1 – Modèles génériques

D'autre part, les 64 valeurs des $(\alpha_0, \alpha_1, \alpha_2, \alpha_3)$ satisfaisant le système 5.3.2 sont :

$Valeurs\ (\alpha_0, \alpha_1, \alpha_2, \alpha_3)$															
α_0	α_1	α_2	α_3	α_0	α_1	α_2	α_3	α_0	α_1	α_2	α_3	α_0	α_1	α_2	α_3
0	**0**	**0**	**2**	1	0	0	3	2	0	0	0	3	0	0	1
0	**0**	**1**	**3**	1	0	1	2	2	0	1	1	3	0	1	0
0	**0**	**2**	**0**	1	0	2	1	2	0	2	2	3	0	2	3
0	**0**	**3**	**1**	1	0	3	0	2	0	3	3	3	0	3	2
0	**1**	**0**	**3**	1	1	0	2	2	1	0	1	3	1	0	0
0	**1**	**1**	**2**	1	1	1	3	2	1	1	0	3	1	1	1
0	**1**	**2**	**1**	1	1	2	0	2	1	2	3	3	1	2	2
0	**1**	**3**	**0**	1	1	3	1	2	1	3	2	3	1	3	3
0	**2**	**0**	**0**	1	2	0	1	2	2	0	2	3	2	0	3
0	**2**	**1**	**1**	1	2	1	0	2	2	1	3	3	2	1	2
0	**2**	**2**	**2**	1	2	2	3	2	2	2	0	3	2	2	1
0	**2**	**3**	**3**	1	2	3	2	2	2	3	1	3	2	3	0
0	**3**	**0**	**1**	1	3	0	0	2	3	0	3	3	3	0	2
0	**3**	**1**	**0**	1	3	1	1	2	3	1	2	3	3	1	3
0	**3**	**2**	**3**	1	3	2	2	2	3	2	1	3	3	2	0
0	**3**	**3**	**2**	1	3	3	3	2	3	3	0	3	3	3	1

TABLE 5.2 – Solutions du système

Ces valeurs peuvent être réduites aux 16 premières valeurs du tableau 5.2 en remarquant simplement que si $(\alpha_0, \alpha_1, \alpha_2, \alpha_3)$ vérifie le système 5.3.2 alors $(\alpha_0 + l, \alpha_1 + l, \alpha_2 + l, \alpha_3 + l)$ le vérifie aussi pour tout l, $0 \leq l \leq 3$.
Pour établir la correspondance, nous considérerons le système 5.3.2 et les 16 valeurs de $(\alpha_0, \alpha_1, \alpha_2, \alpha_3)$ transcrits dans le tableau 5.2 et nous distinguons l'association selon les différents cas de parité de $Tr(b_1)$ et $Tr(b_2)$.

$Valeurs\ (\alpha_0,\alpha_1,\alpha_2,\alpha_3)$	$Fonctions\ h_k$			
	$Tr(b_2)\ impaire$		$Tr(b_2)\ paire$	
	$Tr(b_1)=0$	$Tr(b_1)=2$	$Tr(b_1)=0$	$Tr(b_1)=2$
0002				34
0020				34
0200			34	
0222			34	
0013		34		
0031		34		
0211	34			
0233	34			
0103	**2**	**6**		
0121	2	6		
0301	6	2		
0323	6	2		
0112	1	5		
0130	1	5		
0310	5	1		
0332	5	1		

TABLE 5.3 – Correspondance solution/modèle

□

Exemple Les valeurs 0103 (tableau 5.3) produisent la fonctions génératrice (2) qui correspond au modèle générique (0,1,2,3) et la fonction génératrice (6) qui correspond au modèle (0,3,2,1) du tableau 7.1, pour $Tr(b_2)$ impair, et $Tr(b_1)=0$ et $Tr(b_1)=2$ respectivement.

En utilisant ces modèles nous pouvons construire directement des fonctions quaternaires courbes F_k. On peut remarquer que les 6 fonctions génératrices sont retrouvées.

Proposition 5.4.2. *Soit* $a=(a_0,a_1,a_2,a_3)$ *un modèle générateur de tableau 7.1 alors la fonction quaternaire courbe*

$$F_k\ :\ R=\cup_{i=0}^{2^m-1}C_i\cup D\ \rightarrow\ \mathbb{Z}_4$$

peut être construite comme suit :

$$\begin{cases} F_k(C_i) & = & a_j & if\ \beta^i\in B^{\perp}\oplus b_j,\ 0\le i\le 2^m-2,\ 0\le j\le 3 \\ F_k(\mathcal{T}\cup D) & = & a_0 & \end{cases}.$$

Démonstration. Voir proposition 5.1.1 et l'équation 5.3.4. □

5.5 Exemple complet de construction dans $GR(4,3)$

Considérons $(a_0, a_1, a_2, a_3) = (0, 2, 1, 3)$ la fonction $n^o = 3$, de la table 7.1. Pour la construction de l'anneau de Galois, on choisit $g(x) = x^3 + 2x^2 + x + 3$ comme b-polynôme et on note β une racine primitive de $g(x)$ d'ordre 7.
On commencera par la construction des classes cyclotomiques.

$$R = GR(4,3) \overset{\mathrm{d}}{\simeq} \mathbb{Z}_{\mathbf{4}}[\beta].$$

De plus, la proposition 5.1.1 nous permet d'avoir le bon partitionnement de $GR(4,3)$. On peut établir la correspondance suivante en considérant l'ensemble $\{1, \beta, \beta^2\}$ comme base de $\mathbb{Z}_4^3$ et $\beta^3 = 2\beta^2 + 3\beta + 1$.

$GR(4,3)$							
$\mathcal{T}^*$	1	β	β^2	β^3	β^4	β^5	β^6
$\mathbf{E}^*$	$\{1,0,0\}$	$\{0,1,0\}$	$\{0,0,1\}$	$\{1,3,2\}$	$\{2,3,3\}$	$\{3,3,1\}$	$\{1,2,1\}$
D^*	2	2β	$2\beta^2$	$2\beta^3$	$2\beta^4$	$2\beta^5$	$2\beta^6$
$\mathbf{W}^*$	$\{2,0,0\}$	$\{0,2,0\}$	$\{0,0,2\}$	$\{2,2,0\}$	$\{0,2,2\}$	$\{2,2,2\}$	$\{2,0,2\}$
C_0	3	3β	$3\beta^2$	$3\beta^3$	$3\beta^4$	$3\beta^5$	$3\beta^6$
$\mathbf{V}_0$	$\{3,0,0\}$	$\{0,3,0\}$	$\{0,0,3\}$	$\{3,1,2\}$	$\{2,1,1\}$	$\{1,1,3\}$	$\{3,2,3\}$
C_1	$1+2\beta$	$\beta+2\beta^2$	$\beta^2+2\beta^3$	$\beta^3+2\beta^4$	$\beta^4+2\beta^5$	$\beta^5+2\beta^6$	β^6+2
$\mathbf{V}_1$	$\{1,2,0\}$	$\{0,1,2\}$	$\{2,2,1\}$	$\{1,1,0\}$	$\{0,1,1\}$	$\{1,3,3\}$	$\{3,2,1\}$
C_2	$1+2\beta^2$	$\beta+2\beta^3$	$\beta^2+2\beta^4$	$\beta^3+2\beta^5$	$\beta^4+2\beta^6$	β^5+2	$\beta^6+2\beta$
$\mathbf{V}_2$	$\{1,0,2\}$	$\{2,3,0\}$	$\{0,2,3\}$	$\{3,1,0\}$	$\{0,3,1\}$	$\{1,3,1\}$	$\{1,0,1\}$
C_3	$1+2\beta^3$	$\beta+2\beta^4$	$\beta^2+2\beta^5$	$\beta^3+2\beta^6$	β^4+2	$\beta^5+2\beta$	$\beta^6+2\beta^2$
$\mathbf{V}_3$	$\{3,2,0\}$	$\{0,3,2\}$	$\{2,2,3\}$	$\{3,3,0\}$	$\{0,3,3\}$	$\{3,1,1\}$	$\{1,2,3\}$
C_4	$1+2\beta^4$	$\beta+2\beta^5$	$\beta^2+2\beta^6$	β^3+2	$\beta^4+2\beta$	$\beta^5+2\beta^2$	$\beta^6+2\beta^3$
$\mathbf{V}_4$	$\{1,2,2\}$	$\{2,3,2\}$	$\{2,0,3\}$	$\{3,3,2\}$	$\{2,1,3\}$	$\{3,3,3\}$	$\{3,0,1\}$
C_5	$1+2\beta^5$	$\beta+2\beta^6$	β^2+2	$\beta^3+2\beta$	$\beta^4+2\beta^2$	$\beta^5+2\beta^3$	$\beta^6+2\beta^4$
$\mathbf{V}_5$	$\{3,2,2\}$	$\{2,1,2\}$	$\{2,0,1\}$	$\{1,1,2\}$	$\{2,3,1\}$	$\{1,1,1\}$	$\{1,0,3\}$
C_6	$1+2\beta^6$	$\beta+2$	$\beta^2+2\beta$	$\beta^3+2\beta^2$	$\beta^4+2\beta^3$	$\beta^5+2\beta^4$	$\beta^6+2\beta^5$
$\mathbf{V}_6$	$\{3,0,2\}$	$\{2,1,0\}$	$\{0,2,1\}$	$\{1,3,0\}$	$\{0,1,3\}$	$\{3,1,3\}$	$\{3,0,3\}$

TABLE 5.4

Ensuite on choisira un couple $(b_1,b_2) \in \mathcal{T}^* \times \mathcal{T}^*$ vérifiant les conditions du lemme 5.2.1.

Pour cela nous allons calculer la trace des éléments de $\mathcal{T}$.

Nous savons que :

$$Tr(\beta^i) = \sum_{j=1}^{3} \beta^{2ij[7]}, i \in \{0, \dots 6\}$$

Par exemple pour $i = 3$:

$$Tr(\beta^3) = \beta^3 + \beta^6 + \beta^5 = (1 + 3\beta + 2\beta^2) + (1 + 2\beta + \beta^2)(+3 + 3\beta + \beta^2) = 1$$

Nous calculons de la même manière toutes les autres traces et nous les regroupons dans le tableau suivant :

$b_i \in \mathcal{T}$	1	β	β^2	β^3	β^4	β^5	β^6	0
$Tr(b_i)$	3	2	2	1	2	1	1	0

Comme, $Tr(b_1)$ doit être paire et $Tr(bb_1b_2)$ doit être impaire conformément à la proposition 5.3.1, nous pouvons choisir $b_1 = \beta^2$, $b_2 = \beta^3$.
Conformément aux notations de cette même proposition nous avons :

$$B = \{0, b_1, b_2, b_3\} \quad (5.5.1)$$
$$B^\perp = \{x \in \mathcal{T}\,,\ 2Tr(xb_1) = 2Tr(xb_2) = 0\} \quad (5.5.2)$$

avec $b_3 = b_1 \oplus b_2$ et $\mathcal{T} = B^\perp \oplus B = \cup_{i=0}^{3} B^\perp \oplus b_i$.

Pour aller plus loin et construire les ensembles $B^\perp \oplus b_i$ nous nous référons à la table ci-dessous :

$\oplus$	b_1	1	β	β^2	β^3	β^4	β^5	β^6	0
b_2									
1		0	β^3	β^6	β	β^5	β^4	β^2	1
β		β^3	0	β^4	1	β^2	β^6	β^5	β
β^2		β^6	β^4	0	β^5	β	β^3	1	β^2
β^3		β	1	β^5	0	β^6	β^2	β^4	β^3
β^4		β^5	β^2	β	β^6	0	1	β^3	β^4
β^5		β^4	β^6	β^3	β^2	1	0	β	β^5
β^6		β^2	β^5	1	β^4	β^3	β	0	β^6
0		1	β	β^2	β^3	β^4	β^5	β^6	0

on retrouve ainsi :

$$\begin{aligned} B^\perp \oplus b_0 &= \{0, \beta^6\} \\ B^\perp \oplus b_1 &= \{\beta^2, 1\} \\ B^\perp \oplus b_2 &= \{\beta^3, \beta^4\} \\ B^\perp \oplus b_3 &= \{\beta^5, \beta\} \end{aligned} .$$

On peut alors définir explicitement la fonction quaternaire courbe F par :

$$\forall x \in R,\ F(x) = \begin{cases} 0 & si\ x \in \cup C_6 \cup D \cup \mathcal{T}^* \\ 2 & si\ x \in \cup C_2 \cup C_0 \\ 1 & si\ x \in \cup C_3 \cup C_4 \\ 3 & si\ x \in \cup C_5 \cup C_1 \end{cases} \tag{5.5.3}$$

5.6 Conclusion

Nous avons décrit dans ce chapitre une méthode de construction de fonctions quaternaires à m variables courbes. Cette méthode peut se résumé de la façon suivante :

Soit m un entier non nul. On choisit un b-polynôme de degré m.

1. On construit l'anneau de Galois $GR(4, m)$.

2. On construit les classes cyclotomiques de la définition 5.1.1.

3. On choisit un couple d'éléments $(b_1,\ b_2)$ du système Teichmüller qui vérifient les conditions de la proposition 5.2.1.

4. En utilisant les modèles présentés dans le tableau 5.3 et l'équation 5.3.4, nous construisons un ensemble de fonctions quaternaires courbes.

Dans le chapitre suivant nous allons présenter des projections binaires qui conservent cette propriété cryptographique invariante.

Chapitre 6

Les projections binaires

Nous étudions dans ce chapitre les images binaires des fonctions quaternaires obtenues dans le chapitre précédent. Pour ce faite, nous allons définir une bijection de $\mathbb{Z}_4^m$ dans $\mathbb{F}_2^{2m}$ que l'on notera φ (l'équation (6.1.7)). A l'aide de cette application nous allons obtenir deux classes de fonctions booléennes, la première composée de fonctions booléennes courbes à $2m$-variables et la seconde composée de fonctions booléennes de non-linéarité maximale à $2m+1$-variables.

Nous exposerons dans un premier temps les notations et propriétés de base qui vont nous permettre d'avoir une représentation vectorielle des fonctions quaternaires construites sur $GR(4, m)$. En s'affranchissant ainsi du caractère primitif des classes cyclotomiques, de la dualité algébrique et des conditions sur les traces de b_1 et b_2 du théorème 5.3.1.

6.1 Définitions et notations

Reprenons les notations du chapitre précédent. Soit $R = GR(4, m)$ un anneau de Galois à 4^m éléments. Comme R est isomorphe à $\mathbb{Z}_4[\beta]$ avec β une racine primitive de l'unité d'ordre $2^m - 1$ et R est un $\mathbb{Z}_4$-espace vectoriel de dimension m, alors R est isomorphe à $\mathbb{Z}_4^m$. On note cet isomorphisme d.

L'idée ici est de donner une représentation vectorielle des éléments de R.

Notons :

- Pour tout j dans $\{0, 2^m - 2\}$ le vecteur $v_j = d(\beta^j)$ comme la représentation vectorielle de l'élément β^j.

- $E = d(\mathcal{T}) = \{\mathbf{0}, v_0, v_1, \cdots, v_{2^m-2}\}$ la représentation vectorielle de $\mathcal{T}$, avec $\mathbf{0} = d(0)$ le vecteur tout-à-zero de longueur m.

- Comme $D = 2\mathcal{T}$, la représentation de D est :

$$W = d(D) = 2E = \{\mathbf{0}, 2v_0, 2v_1, \cdots, 2v_{2^m-2}\}.$$

- La loi additive + sur $\mathcal{T}$ et E reste la même que celle sur dans $\mathbb{Z}_4^m$.
- La loi multiplicative sur $\mathcal{T}$ peut être redéfinie sur E comme suit :

$$\begin{aligned} \forall v_i, v_j \in E^*, \quad v_i \times v_j &= v_{(i+j) \pmod{2^m-1}} \\ \forall v_j \in E, \qquad \mathbf{0} \times v_j &= v_j \times \mathbf{0} = \mathbf{0}. \end{aligned} \tag{6.1.1}$$

Enfin, la représentation d'un élément $z \in R$ est naturellement déduite de la représentation 2-adique des éléments de R (équation 1.2.1 page 17). Avec les notations précédentes on à :

$$d(z) = u + 2v \in \mathbb{Z}_4^m \text{ avec } u, v \in E. \tag{6.1.2}$$

De la même manière, les classes cyclotomiques $C_{0 \le j \le 2^m-1}$ (proposition 5.1.1) peuvent être redéfinies comme suit :

$$V_j = d(C_j) = \{v_l(v_0 + 2v_j),\ 0 \le l \le 2^m - 2\} \tag{6.1.3}$$

$$V_{2^m-1} = d(C_{2^m-1}) = d(\mathcal{T}^*) = E^*. \tag{6.1.4}$$

Par conséquent,

$$\mathbb{Z}_4^m = d(\cup_{j=0}^{2^m-2} C_j \cup C_{2^m-1} \cup D) = \cup_{j=0}^{2^m-2} V_j \cup V_{2^m-1} \cup W.$$

La représentation vectorielle de $\mathfrak{C}_k$ Équation 5.1.3 est définie par :

$$\mathfrak{V}_k = d(\mathfrak{C}_k) = \{v_k\} \cup \{v_k(v_0 + 2v_j),\ 0 \le j \le 2^m - 2\}.$$

Définition 6.1.1. *Pour tout $k \in \{0, 1, .., 2^m - 2\}$ la représentation vectorielle $\bar{F}_k$ d'une fonction quaternaire F_k définie par la Définition 5.1.2 sera transposée comme suit :*

$$\bar{F}_k : \mathbb{Z}_4^m \to \mathbb{Z}_4,\ \bar{F}_k(x) = F_k(d^{-1}(x)) \tag{6.1.5}$$

avec la fonction interne :

$$\bar{h}_k : \mathfrak{V}_k \to \mathbb{Z}_4,\ \bar{h}_k(x) = h_k(d^{-1}(x)). \tag{6.1.6}$$

Dans le but d'étudier la non-linéarité de la fonction booléenne projetée à $2m$-variables, nous définissons ci-dessous une application directe entre $\mathbb{Z}_4^m$ et $\mathbb{F}_2^{2m}$.

Proposition 6.1.1. *L'application φ définie par :*

$$\begin{array}{rccc} \varphi & : & \mathbb{Z}_4^m & \to & \mathbb{F}_2^{2m} \\ & & u+2v & \mapsto & \tilde{u}||\tilde{v} \end{array} \tag{6.1.7}$$

avec˜ la réduction modulo 2 composante par composante et $||$ la concaténation vectorielle, est une bijection.

Démonstration. En utilisant le relèvement de *Hensel* du Chapitre 1 et la bijection entre E et $\mathbb{F}_2^m$, on peut généraliser cette bijection de $\mathbb{Z}_4^m$ dans $\mathbb{F}_2^{2m}$ avec le diagramme suivant :

$$\begin{array}{ccccccc} \mathbb{Z}_4^m & \to & E\times E & \to & F_2^m\times F_2^m & \to & \mathbb{F}_2^{2m} \\ u+2v & \mapsto & (u,v) & \mapsto & (\tilde{u},\tilde{v}) & \mapsto & \tilde{u}||\tilde{v} \end{array} \tag{6.1.8}$$

□

En utilisant l'application φ, on obtient :

$$\begin{aligned} \varphi(W) &= \{\mathbf{0}||\tilde{v}_l,\ 0\le l\le 2^m-2\}\cup\{\mathbf{0}||\mathbf{0}\} \\ \varphi(V_j) &= \{\tilde{v}_l||\tilde{v}_{l+j},\ 0\le l\le 2^m-2\}\ ,\ 0\le\forall j\le 2^m-2 \\ \varphi(V_{2^m-1}) &= \{\tilde{v}_l||\mathbf{0},\ 0\le l\le 2^m-2\}. \end{aligned}$$

Alors $\mathbb{F}_2^{2m}$ peut s'écrire :

$$\cup_{j=0}^{2^m-2}\varphi(V_j)\cup\varphi(V_{2^m-1})\cup\varphi(W).$$

Notons ψ toute application de $\mathbb{Z}_4$ dans $\mathbb{F}_2$ telle que :

$$\sum_{x\in\mathbb{Z}_4}(-1)^{\psi(x)}=0 \tag{6.1.9}$$

Exemple $\psi(2q+r)=q$ or $\psi(2q+r)=q+r\pmod 2$.

6.2 Les fonctions binaires projetées

Dans cette section nous allons présenter les deux familles de *fonctions booléennes projetées* à $2m$ variables et à $2m+1$ variables des fonctions quaternaires courbes construites dans le chapitre précèdent. Considérons F_k une fonction quaternaire courbe définie par la proposition 5.4.2 et $\bar{F}_k$ sa représentation vectorielle.

La fonction booléenne projetée à $2m$ variables est définie comme suit :

Définition 6.2.1. *La fonction booléenne f définie comme suit :*

$$\begin{array}{rccl} f & : & \mathbb{F}_2^{2m} & \to & \mathbb{F}_2 \\ & & x & \mapsto & \psi(\bar{F}_k(\varphi^{-1}(x))) \end{array} \tag{6.2.1}$$

est appelée fonction booléenne projetée.

Avant d'étudier la non-linéarité des fonctions booléennes projetées, nous pouvons caractériser ces fonctions en utilisant les propriétés héritées directement de la structure des fonctions quaternaires. Une fonction booléenne f à $2m$-variables projetée à partir d'une fonction quaternaire F_k peut être caractérisée comme suit :

$$\begin{array}{rcl} f(\tilde{u}||\tilde{v}) & = & \psi(\bar{F}_k(\varphi^{-1}(\tilde{u}||\tilde{v}))) \\ & = & \psi(\bar{F}_k(u+2v)) \\ & = & \left\{ \begin{array}{ll} \psi(\bar{h}_k(v_k(v_0+2v_j))) & if \quad \varphi^{-1}(\tilde{u}||\tilde{v}) \in V_j,\ 0 \le j \le 2^m-2 \\ \psi(\bar{h}_k(v_k)) & if \quad \varphi^{-1}(\tilde{u}||\tilde{v}) \in V_{2^m-1} \cup W \end{array} \right. \end{array}$$

En remarquant, que la fonction dérivée reste constante sur les images des classes cyclotomiques nous pouvons introduire une fonction interne pour les projections binaire de la façon suivante :

$$\begin{array}{rccl} \tilde{h}_k & : & \varphi(\mathfrak{V}_k) & \to & \mathbb{F}_2 \\ & & x & \mapsto & \psi(\bar{h}_k(\varphi^{-1}(x))) \end{array} \tag{6.2.2}$$

la fonction projetée devient alors :

$$\begin{array}{rcl} f(\tilde{u}||\tilde{v}) & = & \left\{ \begin{array}{ll} \tilde{h}_k(\varphi(v_k(v_0+2v_j))) & si \quad \varphi^{-1}(\tilde{u}||\tilde{v}) \in V_j,\ 0 \le j \le 2^m-2 \\ \tilde{h}_k(\varphi(v_k)) & si \quad \varphi^{-1}(\tilde{u}||\tilde{v}) \in V_{2^m-1} \cup W \end{array} \right. \\ & = & \left\{ \begin{array}{ll} \tilde{h}_k(\tilde{v}_k||\tilde{v}_{k+j}))) & si \quad \varphi^{-1}(\tilde{u}||\tilde{v}) \in V_j,\ 0 \le j \le 2^m-2 \\ \tilde{h}_k(\tilde{v}_k||\mathbf{0}) & si \quad \varphi^{-1}(\tilde{u}||\tilde{v}) \in V_{2^m-1} \cup W \end{array} \right. \end{array}$$

Maintenant, nous allons nous intéresser au partitionnement imposé par cette projection sur $\mathbb{F}_2^{2m}$ ainsi qu'aux propriétés du produit vectoriel et à la fonction introduite par l'équation . Notons la réduction modulo 2 de E comme :

$$\tilde{E} = \{\tilde{v}_i, 0 \le i \le 2^m-2\} \cup \{\mathbf{0}\} = \mathbb{F}_2^m.$$

Nous présentons ici des résultats facile à vérifier. Ces résultats vont nous être d'une grande utilité dans le calcul de la transformée de Walsh de f, $W_f(a),\ a \in \mathbb{F}_2^{2m}$.

Lemme 6.2.1. *(i) la fonction interne $\bar{h}_k$ est équilibrée sur E alors $\tilde{h}_k$ l'est aussi sur $\tilde{E}$ et donc $\sum_{\tilde{v}_j \in \tilde{E}} (-1)^{\tilde{h}_k(\tilde{v}_k||\tilde{v}_{k+j})} = 0$.*

(ii) $\forall \tilde{x}_1, \tilde{x}_2, \tilde{y}_1, \tilde{y}_2 \in \tilde{E}$ (respectivement $\forall x_1, x_2, y_1, y_2 \in E$) :

$$\begin{cases} < \tilde{x}_1||\tilde{x}_2, \tilde{y}_1||\tilde{y}_2 > & = & < x_1, y_1 > + < x_2, y_2 > \pmod 2 \\ \\ \mid \sum_{\tilde{x}_1 \in \tilde{E}} (-1)^{<\tilde{x}_1||\tilde{x}_2, \tilde{y}_1||\tilde{y}_2>} \mid & = & \mid \sum_{x_1 \in E} i^{2(<x_1,y_1>+<x_2,y_2>)} \mid \end{cases}$$

Le point (ii) nous permets de déduire que $\forall \tilde{u} \in \tilde{E}$(respect. $\forall u \in E$) nous avons :

$$\sum_{\tilde{v} \in \tilde{E}} (-1)^{<\tilde{v}||\tilde{v} \times \tilde{u}, \tilde{x}_1||\tilde{x}_2>} = \sum_{v \in E} i^{<v, 2(x_1 + u x_2)>}. \tag{6.2.3}$$

À présent, nous somme en mesure d'étudier la non-linéarité des fonctions booléennes projetées.

Proposition 6.2.1. *La fonction booléenne projetée f définie dans la définition 6.2.1 est courbe.*

Démonstration. Considérons $x \in \mathbb{F}_2^{2m}$ alors $x = \tilde{x}_1||\tilde{x}_2$ avec $\tilde{x}_1, \tilde{x}_2 \in \tilde{E}$. Calculons maintenant la transformée de Walsh de f :

$$\begin{aligned} W_f(x) &= \sum_{b \in \mathbb{F}_2^{2m}} (-1)^{f(b)+<x,b>} \\ &= \sum_{b \in \cup_{j=0}^{2^m-1} \varphi(V_j)} (-1)^{f(b)+<x,b>} + \sum_{b \in \varphi(W)} (-1)^{f(b)+<x,b>} \\ &= \sum_{\tilde{v} \in \tilde{E}} \sum_{\tilde{v}_l \in \tilde{E}^*} (-1)^{f(\tilde{v}_l||\tilde{v}_l \times \tilde{v}) + <\tilde{v}_l||\tilde{v}_l \times \tilde{v}, \tilde{x}_1||\tilde{x}_2>} \\ &\quad + \sum_{\tilde{v} \in \tilde{E}} (-1)^{f(\mathbf{0}||\tilde{v}) + <\mathbf{0}||\tilde{v}, \tilde{x}_1||\tilde{x}_2>} \\ &= \sum_{\tilde{v} \in \tilde{E}} \sum_{\tilde{v}_l \in \tilde{E}^*} (-1)^{\tilde{h}_k(\tilde{v}_k||\tilde{v}_k \times \tilde{v}) + <\tilde{v}_l||\tilde{v}_l \times \tilde{v}, \tilde{x}_1||\tilde{x}_2>} \\ &\quad + \sum_{\tilde{v} \in \tilde{E}} (-1)^{\tilde{h}_k(\tilde{v}_k||\mathbf{0}) + <\mathbf{0}||\tilde{v}, \tilde{x}_1||\tilde{x}_2>} \\ &= \sum_{\tilde{v} \in \tilde{E}} (-1)^{\tilde{h}_k(\tilde{v}_k||\tilde{v}_k \times \tilde{v})} \sum_{\tilde{v}_l \in \tilde{E}^*} (-1)^{<\tilde{v}_l||\tilde{v}_l \times \tilde{v}, \tilde{x}_1||\tilde{x}_2>} \\ &\quad + (-1)^{\tilde{h}_k(\tilde{v}_k||\mathbf{0})} \sum_{\tilde{v} \in \tilde{E}} (-1)^{<\mathbf{0}||\tilde{v}, \tilde{x}_1||\tilde{x}_2>} \end{aligned}$$

Nous allons maintenant procéder à un raisonnement par disjonction de cas selon les valeurs prises par $\tilde{x}_1$ et $\tilde{x}_2$.

Cas 1 : $\underline{\tilde{x}_1 = \tilde{x}_2 = 0}$

$$\begin{aligned} W_f(\mathbf{0}||\mathbf{0}) &= \sum_{\tilde{v}\in\tilde{E}}(-1)^{\tilde{h}_k(\tilde{v}_k||\tilde{v}_k\times\tilde{v})}(2^m-1)+2^m(-1)^{\tilde{h}_k(\tilde{v}_k||\mathbf{0})} \\ &\overset{(i)}{=} 2^m(-1)^{\tilde{h}_k(\tilde{v}_k||\mathbf{0})} \end{aligned} \tag{6.2.4}$$

Cas 2 : $\underline{\tilde{x}_1 \neq 0,\ \tilde{x}_2 = 0}$

$$\begin{aligned} W_f(\tilde{x}_1||\mathbf{0}) &= \sum_{\tilde{v}\in\tilde{E}}(-1)^{\tilde{h}_k(\tilde{v}_k||\tilde{v}_k\times\tilde{v})}\underbrace{\sum_{\tilde{v}_l\in\tilde{E}^*}(-1)^{<\tilde{v}_l||\tilde{v}_l\times\tilde{v},\tilde{x}_1||\mathbf{0}>}}_{\overset{(ii)}{=}-1} \\ &\quad +(-1)^{\tilde{h}_k(\tilde{v}_k||\mathbf{0})}\sum_{\tilde{v}\in\tilde{E}}(-1)^{<\mathbf{0}||\tilde{v},\tilde{x}_1||\mathbf{0}>} \\ &= -\sum_{\tilde{v}\in\tilde{E}}(-1)^{\tilde{h}_k(\tilde{v}_k||\tilde{v}_k\times\tilde{v})}+2^m(-1)^{\tilde{h}_k(\tilde{v}_k||\mathbf{0})} \\ &\overset{(i)}{=} 2^m(-1)^{\tilde{h}_k(\tilde{v}_k||\mathbf{0})} \end{aligned} \tag{6.2.5}$$

Cas 3 : $\underline{\tilde{x}_1 = 0,\ \tilde{x}_2 \neq 0}$

$$\begin{aligned} W_f(\mathbf{0}||\tilde{x}_2) &= \sum_{\tilde{v}\in\tilde{E}}(-1)^{\tilde{h}_k(\tilde{v}_k||\tilde{v}_k\times\tilde{v})}\sum_{\tilde{v}_l\in\tilde{E}^*}(-1)^{<\tilde{v}_l||\tilde{v}_l\times v,\mathbf{0}||\tilde{x}_2>} \\ &\quad +(-1)^{\tilde{h}_k(\tilde{v}_k||\mathbf{0})}\sum_{\tilde{v}\in\tilde{E}}(-1)^{<\mathbf{0}||\tilde{v},\mathbf{0}||\tilde{x}_2>} \end{aligned} \tag{6.2.6}$$

Comme $\tilde{x}_2 \neq 0$ alors $\sum_{\tilde{v}\in\tilde{E}}(-1)^{<\mathbf{0}||\tilde{v},\mathbf{0}||\tilde{x}_2>} \overset{(ii)}{=} 0$ et ainsi l'équation 6.2.6 devient :

$$\begin{aligned} W_f(\mathbf{0}||\tilde{x}_2) &= \sum_{\tilde{v}_j\in\tilde{E}^*}(-1)^{\tilde{h}_k(\tilde{v}_k||\tilde{v}_{k+j})}\sum_{\tilde{v}_l\in\tilde{E}^*}(-1)^{<\tilde{v}_l||\tilde{v}_{l+j},\mathbf{0}||\tilde{x}_2>} \\ &\quad +(-1)^{\tilde{h}_k(\tilde{v}_k||\mathbf{0})}\sum_{\tilde{v}_l\in\tilde{E}^*}(-1)^{<\tilde{v}_l||\mathbf{0},\mathbf{0}||\tilde{x}_2>} \\ &= \sum_{\tilde{v}_j\in\tilde{E}^*}(-1)^{\tilde{h}_k(\tilde{v}_k||\tilde{v}_{k+j})}\sum_{\tilde{v}_l\in\tilde{E}^*}(-1)^{<\tilde{v}_l||\tilde{v}_{l+j},\mathbf{0}||\tilde{x}_2>} \\ &\quad +(2^m-1)(-1)^{\tilde{h}_k(\tilde{v}_k||\mathbf{0})} \\ &= \sum_{\tilde{v}_j\in\tilde{E}^*}(-1)^{\tilde{h}_k(\tilde{v}_k||\tilde{v}_{k+j})}\underbrace{\sum_{\tilde{v}_l\in\tilde{E}^*}(-1)^{<\tilde{v}_l||\tilde{v}_{l+j},\mathbf{0}||\tilde{x}_2>}}_{\overset{(ii)}{=}-1} \\ &\quad +(2^m-1)(-1)^{\tilde{h}_k(\tilde{v}_k||\mathbf{0})} \end{aligned}$$

$$
\begin{aligned}
&= -\sum_{\tilde{v}\in\tilde{E}}(-1)^{\tilde{h}_k(\tilde{v}_k||\tilde{v}_k\times\tilde{v})} + (2^m-1)(-1)^{\tilde{h}_k(\tilde{v}_k||\mathbf{0})} + (-1)^{\tilde{h}_k(\tilde{v}_k||\mathbf{0})} \\
&\overset{(i)}{=} 2^m(-1)^{\tilde{h}_k(\tilde{v}_k||\mathbf{0})} \qquad (6.2.7)
\end{aligned}
$$

Cas 4 : $\underline{\tilde{x}_1 \neq 0,\ \tilde{x}_2 \neq 0}$

$$
\begin{aligned}
W_f(\tilde{x}_1||\tilde{x}_2) &= \sum_{\tilde{v}\in\tilde{E}}(-1)^{\tilde{h}_k(\tilde{v}_k||\tilde{v}_k\times\tilde{v})} \sum_{\tilde{v}_l\in\tilde{E}^*}(-1)^{<\tilde{v}_l||\tilde{v}_l\times\tilde{v},\tilde{x}_1||\tilde{x}_2>} \qquad (6.2.8)\\
&\quad +(-1)^{\tilde{h}_k(\tilde{v}_k||\mathbf{0})} \underbrace{\sum_{\tilde{v}\in\tilde{E}}(-1)^{<\mathbf{0}||\tilde{v},\tilde{x}_1||\tilde{x}_2>}}_{\overset{(ii)}{=}0}
\end{aligned}
$$

Comme le produit scalaire est équilibré sur $\tilde{E}$ et $\tilde{x}_1$ et $\tilde{x}_2$ sont non nuls alors :

$$
\begin{aligned}
&(1)\ \textstyle\sum_{\tilde{v}_l\in\tilde{E}}(-1)^{<\tilde{v}_l||\tilde{v}_k\times\frac{\tilde{x}_1}{\tilde{x}_2},\tilde{x}_1||\tilde{x}_2>} &&= 2^m \quad si \qquad \tilde{v} = \tfrac{\tilde{x}_1}{\tilde{x}_2}\\
&(2)\ \textstyle\sum_{\tilde{v}_l\in\tilde{E}}(-1)^{<\tilde{v}_l||\tilde{v}_k\times\tilde{v},\tilde{x}_1||\tilde{x}_2>} &&= 0 \quad sinon
\end{aligned}
$$

alors l'équation 6.2.8 devient :

$$
\begin{aligned}
W_f(\tilde{x}_1||\tilde{x}_2) &= \sum_{\tilde{v}\in\tilde{E}\setminus\frac{\tilde{x}_1}{\tilde{x}_2}}(-1)^{\tilde{h}_k(\tilde{v}_k||\tilde{v}_k\times\tilde{v})} \underbrace{\sum_{\tilde{v}_l\in\tilde{E}^*}(-1)^{<\tilde{v}_l||\tilde{v}_k\times\tilde{v},\tilde{x}_1||\tilde{x}_2>}}_{\overset{(ii)}{=}-1}\\
&\quad +(2^m-1)(-1)^{\tilde{h}_k(\tilde{v}_l||\tilde{v}_l\times\frac{\tilde{x}_1}{\tilde{x}_2})}\\
&= -\sum_{\tilde{v}\in\tilde{E}\setminus\frac{\tilde{x}_1}{\tilde{x}_2}}(-1)^{\tilde{h}_k(\tilde{v}_k||\tilde{v}_k\times\tilde{v})} + (2^m-1)(-1)^{\tilde{h}_k(\tilde{v}_l||\tilde{v}_l\times\frac{\tilde{x}_1}{\tilde{x}_2})}\\
&= -\sum_{\tilde{v}\in\tilde{E}}(-1)^{\tilde{h}_k(\tilde{v}_l||\tilde{v}_l\times\tilde{v})} + (2^m-1)(-1)^{\tilde{h}_k(\tilde{v}_l||\tilde{v}_l\times\frac{\tilde{x}_1}{\tilde{x}_2})}\\
&\quad +(-1)^{\tilde{h}_k(\tilde{v}_l||\tilde{v}_l\times\frac{\tilde{x}_1}{\tilde{x}_2})}\\
&\overset{(i)}{=} 2^m(-1)^{\tilde{h}_k(\tilde{v}_l||\tilde{v}_l\times\frac{\tilde{x}_1}{\tilde{x}_2})} \qquad (6.2.9)
\end{aligned}
$$

Enfin, comme $\forall a \in \mathbb{F}_2^{2m}$, $\mid W_f(a) \mid = 2^m$ et que f est une fonction à $2m$ variables. Alors f est courbe.

□

On peut étendre naturellement la projection binaire exposée dans la section précédente à une projection à $2m+1$ variables. La projection de la fonction quaternaire F_k dans $\mathbb{F}_2^{2m+1}$ donne une fonction booléenne à $2m+1$ variables. La fonction projetée à $2m+1$ variables peut être vue soit comme l'adjonction d'une variable à la fonction booléenne projetée à $2m$ variables ou comme la concaténation de deux fonctions booléennes projetées à $2m$ variables .

Soit $\varepsilon \in \mathbb{F}_2$. En utilisant l'application φ définition 6.1.7 et en notant pour tout j, $0 \leq j \leq 2^m-2$, les ensembles qui nous intéressent comme suit :

$$\begin{array}{rcl} \varphi(V_j)_\varepsilon & = & \varphi(V_j)||\varepsilon = \{v_l||v_{l+j}||\varepsilon,\ 0 \leq l \leq 2^m-2\}, \\ \varphi(V_{2^m-1})_\varepsilon & = & \varphi(V_{2^m-1})||\varepsilon = \{v_l||\mathbf{0}||\varepsilon,\ 0 \leq l \leq 2^m-2\}, \\ \varphi(W)_\varepsilon & = & \varphi(W)||\varepsilon = \{\mathbf{0}||v_l||\varepsilon,\ 0 \leq l \leq 2^m-2\} \cup \{\mathbf{0}||\mathbf{0}||\varepsilon\}, \end{array} \tag{6.2.10}$$

on obtient :

$$\mathbb{F}_2^{2m+1} = \cup_{\varepsilon=0}^{1}[\cup_{j=0}^{2^m-1}\varphi(V_j)_\varepsilon \cup \varphi(W)_\varepsilon].$$

De la même manière on a :

$$\varphi(\mathfrak{V}_k)_\varepsilon = \varphi(\mathfrak{V}_k)||\varepsilon.$$

Ainsi nous pouvons déduire la proposition ci dessous des fonctions booléennes projetées à $2m+1$ variables.

Proposition 6.2.2. *Soit $\varepsilon \in \{0,1\}$ et ψ_ε une application définie par l'équation 6.1.9. La fonction booléenne f à $2m+1$ variables dite projetée de la fonction quaternaire F_k et définie comme suit :*

$$\begin{array}{rcccl} f & : & \mathbb{F}_2^{2m+1} & \to & \mathbb{F}_2 \\ & & x||\varepsilon & \mapsto & \psi_\varepsilon(\bar{F}_k(\varphi^{-1}(x))) \end{array} \tag{6.2.11}$$

admet une non-linéarité maximale égale à $4^m - 2^{m+1}$.

Démonstration. Soit $X = \tilde{x}_1||\tilde{x}_2||\varepsilon' \in \mathbb{F}_2^{2m+1}$ avec $\tilde{x}_1, \tilde{x}_2 \in \mathbb{F}_2^m$ et $\varepsilon' \in \mathbb{F}_2$.

D'après la caractérisation de la projection binaire à $2m$ variables, nous avons :

$$\begin{array}{rcl} f(\tilde{u}||\tilde{v}||\varepsilon) & = & \psi_\varepsilon(\bar{F}_k(\varphi^{-1}(\tilde{u}||\tilde{v}||\varepsilon))) \\ & = & \begin{cases} \psi_\varepsilon(\bar{h}_k(v_k(v_0+2v_j))) & si \quad \tilde{u}||\tilde{v}||\varepsilon \in \varphi(V_j)_\varepsilon,\ 0 \leq j \leq 2^m-2 \\ \psi_\varepsilon(\bar{h}_k(\varphi^{-1}(v_k))) & si \quad \tilde{u}||\tilde{v}||\varepsilon \in \varphi(V_{2^m-1})_\varepsilon \cup \varphi(W)_\varepsilon \end{cases} \end{array}$$

Posons $\tilde{H}_k : \varphi(\mathfrak{V}_k)_\varepsilon \to \mathbb{F}_2$ tel que $\tilde{H}_k(x||\varepsilon) = \psi_\varepsilon(\bar{h}_k(\varphi^{-1}(x))) = \tilde{h}_k^\varepsilon(x)$.

et calculons la transformée de Walsh de f.

$$
\begin{aligned}
W_f(X) &= \sum_{Y\in\mathbb{F}_2^{2m+1}}(-1)^{f(Y)+<X,Y>} \\
&= \sum_{\varepsilon\in\mathbb{F}_2}\Big[\\
&\quad \sum_{Y\in\cup_{j=0}^{2^m-1}\varphi(V_j)_\varepsilon}(-1)^{f(Y)+<X,Y>} + \sum_{Y\in\varphi(W)_\varepsilon}(-1)^{f(Y)+<X,Y>}\ \Big] \\
&= \sum_{\varepsilon\in\mathbb{F}_2}\Big[\\
&\quad \sum_{\tilde{v}_l||(\tilde{v}_l\times\tilde{v})||\varepsilon\ \in\ \cup_{j=0}^{2^m-1}\varphi(V_j)_\varepsilon}(-1)^{f(\tilde{v}_l||(\tilde{v}_l\times\tilde{v})||\varepsilon)+<\tilde{x}_1||\tilde{x}_2||\varepsilon',\tilde{v}_l||(\tilde{v}_l\times\tilde{v})||\varepsilon>} \\
&\quad + \sum_{\mathbf{0}||\tilde{v}||\varepsilon\ \in\ \varphi(W)_\varepsilon}(-1)^{f(\mathbf{0}||\tilde{v}||\varepsilon)+<\tilde{x}_1||\tilde{x}_2||\varepsilon',\mathbf{0}||\tilde{v}||\varepsilon>}\ \Big] \\
&= \sum_{\varepsilon\in\mathbb{F}_2}\Big[\\
&\quad \sum_{\tilde{v}\in\tilde{E}}\sum_{\tilde{v}_l\in\tilde{E}^*}(-1)^{\tilde{H}_k(\tilde{v}_k||(\tilde{v}_k\times\tilde{v})||\varepsilon)+<\tilde{x}_1||\tilde{x}_2||\varepsilon',\tilde{v}_l||(\tilde{v}_l\times\tilde{v})||\varepsilon>} \\
&\quad + \sum_{\tilde{v}\in\tilde{E}}(-1)^{\tilde{H}_k(\tilde{v}_k||\mathbf{0}||\varepsilon)+<\tilde{x}_1||\tilde{x}_2||\varepsilon',\mathbf{0}||\tilde{v}||\varepsilon>}\ \Big] \\
&= \sum_{\varepsilon\in\mathbb{F}_2}\Big[\\
&\quad \sum_{\tilde{v}\in\tilde{E}}(-1)^{\tilde{H}_k(\tilde{v}_k||(\tilde{v}_k\times\tilde{v})||\varepsilon)}\sum_{\tilde{v}_l\in\tilde{E}^*}(-1)^{<\tilde{x}_1||\tilde{x}_2||\varepsilon',\tilde{v}_l||(\tilde{v}_l\times\tilde{v})||\varepsilon>} \\
&\quad + (-1)^{\tilde{H}_k(\tilde{v}_k||\mathbf{0}||\varepsilon)}\sum_{\tilde{v}\in\tilde{E}}(-1)^{<\mathbf{0}||\tilde{v}||\varepsilon,\tilde{x}_1||\tilde{x}_2||\varepsilon'>}\ \Big] \\
&= \sum_{\varepsilon\in\mathbb{F}_2}(-1)^{\varepsilon\varepsilon'}\Big[\\
&\quad \sum_{\tilde{v}\in\tilde{E}}(-1)^{\psi_\varepsilon(\bar{h}_k(\varphi^{-1}(\tilde{v}_k||(\tilde{v}_k\times\tilde{v}))))}\sum_{\tilde{v}_l\in\tilde{E}^*}(-1)^{<\tilde{x}_1||\tilde{x}_2,\tilde{v}_l||(\tilde{v}_l\times\tilde{v})>} \\
&\quad + (-1)^{\psi_\varepsilon(\bar{h}_k(\varphi^{-1}(\tilde{v}_k||\mathbf{0})))}\sum_{\tilde{v}\in\tilde{E}}(-1)^{<\mathbf{0}||\tilde{v},\tilde{x}_1||\tilde{x}_2>}\ \Big]
\end{aligned}
$$

À cette étape, si on note

$$\tilde{h}_k^0(x) = \psi_0(\bar{h}_k(\varphi^{-1}(x))) \tag{6.2.12}$$
$$\tilde{h}_k^1(x) = \psi_1(\bar{h}_k(\varphi^{-1}(x))) \tag{6.2.13}$$

alors

$$W_f(X) = (-1)^{\varepsilon'}W_{f_1}(\tilde{x}_1||\tilde{x}_2) + W_{f_0}(\tilde{x}_1||\tilde{x}_2),$$

avec f_0 et f_1 sont deux fonctions courbes à $2m$ variables (proposition 6.2.1) et avec $\tilde{h}_k^0$ et $\tilde{h}_k^1$ leurs fonctions internes définies par l'équation 6.2.

Ainsi, comme $W_{f_0} = \pm 2^m$ et $W_{f_1} = \pm 2^m$ alors $W_f(X) = \pm 2^{m+1}$ or 0.

□

6.3 Exemples de projections

Reprenons l'exemple de la section 5.5. La représentation vectorielle $\bar{F}$ de la fonction quaternaire F construite par l'équation 5.5.3 est :

$$\forall x \in \mathbb{Z}_4^m,\ \bar{F}(x) = \begin{cases} 0 & if\ x \in \cup V_6 \cup W \cup E^* \\ 2 & if\ x \in \cup V_2 \cup V_0 \\ 1 & if\ x \in \cup V_3 \cup V_4 \\ 3 & if\ x \in \cup V_5 \cup V_1 \end{cases} \tag{6.3.1}$$

avec $(\mathbb{Z}_4^m = E^* \cup W \cup (\cup_{j=0}^{2^m-2} V_j))$ décrit dans le tableau 5.5.
Nous savons que :

$$\mathbb{F}_2^{2m} = \cup_{j=0}^{2^m-2} \varphi(V_j) \cup \varphi(V_{2^m-1}) \cup \varphi(W),$$

où φ est la bijection définie par l'équation 6.1.8.

Considérons l'ensemble :

$$\mathbf{E}^* = \{(1,0,0),(0,1,0),(0,0,1),(1,3,2),(2,3,3),(3,3,1),(1,2,1)\},$$

sa projection binaire est la suivante :

$\varphi(E)^* = \{(1,0,0,0,0,0),(0,1,0,0,0,0),(0,0,1,0,0,0),$
$(1,1,0,0,0,0),(0,1,1,0,0,0),(1,1,1,0,0,0),(1,0,1,0,0,0)\}$
De la même manière on peut retrouver tous les autres ensembles de $\mathbb{F}_2^{2m}$.

Exemple [Projection binaire à $2m$ variables] :
Considérons $\psi : \mathbb{Z}_4 \to \mathbb{F}_2$,$\psi(2q+r) = q$ alors la fonction f définie :

$$\forall x \in \mathbb{Z}_4^m,\ f(\varphi(x)) = \begin{cases} 0 & si\ \varphi(x) \in \cup\varphi(V_6) \cup \varphi(W) \cup \varphi(E^*) \\ 1 & si\ \varphi(x) \in \cup\varphi(V_2) \cup \varphi(V_0) \\ 0 & si\ \varphi(x) \in \cup\varphi(V_3) \cup \varphi(V_4) \\ 1 & si\ \varphi(x) \in \cup\varphi(V_5) \cup \varphi(V_1) \end{cases}$$

est courbe.

Dans le cas des projections à $2m+1$ variables nous savons que :

$$\begin{aligned} \mathbb{F}_2^{2m+1} &= \cup_{\varepsilon=0}^{1}[\cup_{j=0}^{2^m-1} \varphi(V_j)_\varepsilon \cup \varphi(W)_\varepsilon]. \\ \mathbb{F}_2^{2m+1} &= \mathbb{F}_2^{2m}||\varepsilon \end{aligned}$$

ainsi nous pouvons construire la fonction g à $2m+1$ variables comme suit :

Exemple [Projection binaire à $2m+1$ variables] :
Considérons $\psi_{\varepsilon\in\{0,1\}} : \mathbb{Z}_4 \to \mathbb{F}_2$, $\psi_\varepsilon(2q+r) = q * \varepsilon + \bar{\varepsilon} * r$

$$\forall x \in \mathbb{Z}_4^m,\ g(\varphi(x)||\varepsilon) = \begin{cases} 0 & si\ \varphi(x)||\varepsilon \in \cup\varphi(V_6)_\varepsilon \cup \varphi(W)_\varepsilon \cup \varphi(E^*)_\varepsilon \\ \varepsilon & si\ \varphi(x)||\varepsilon \in \cup\varphi(V_2)_\varepsilon \cup \varphi(V_0)_\varepsilon \\ \bar{\varepsilon} & si\ \varphi(x)||\varepsilon \in \cup\varphi(V_3)_\varepsilon \cup \varphi(V_4)_\varepsilon \\ \varepsilon+\bar{\varepsilon} & si\ \varphi(x)||\varepsilon \in \cup\varphi(V_5)_\varepsilon \cup \varphi(V_1)_\varepsilon \end{cases}$$

avec $\bar{\varepsilon} = \varepsilon + 1 \mod 2$. Cette fonction est de non-linéarité égale à $nl_4^L(F) = 4^m - 2^m$.

6.4 Conclusion

Nous avons vu dans ce chapitre comment générer des fonctions booléennes courbes à $2m$ variables et des fonctions booléennes de non-linéarité maximale à $2m+1$ variables.

Pour cela, nous avons utilisé une fonction quaternaire courbe F_k à m variable construite par la proposition 5.4.2, la bijection de la définition 6.1.7 de $\mathbb{Z}_4^m$ dans $\mathbb{F}_2^{2m}$ et les projections $\psi : \mathbb{Z}_4 \to \mathbb{F}_2$ équilibrées de l'équation (6.1.9).

Dans le cas de la projection à $2m$ variables :

$$\mathbb{F}_2^{2m} = \cup_{j=0}^{2^m-2} \varphi(V_j) \cup \varphi(V_{2^m-1}) \cup \varphi(W),$$

et la fonction booléenne projetée f est définie comme suit :

$$\begin{array}{rccl} f & : & \mathbb{F}_2^{2m} & \to & \mathbb{F}_2 \\ & & x & \mapsto & \psi(\bar{F}_k(\varphi^{-1}(x))) \end{array}$$

Dans le cas de la projection à $2m+1$ variables :

$$\mathbb{F}_2^{2m+1} = \cup_{\varepsilon=0}^{1} [\cup_{j=0}^{2^m-1} \varphi(V_j)_\varepsilon \cup \varphi(W)_\varepsilon].$$

et la fonction booléenne projetée g est définie comme suit :

$$\begin{array}{rccl} g & : & \mathbb{F}_2^{2m+1} & \to & \mathbb{F}_2 \\ & & x||\varepsilon & \mapsto & \psi_\varepsilon(\bar{F}_k(\varphi^{-1}(x))) \end{array}$$

Chapitre 7

La conjecture de Tu et Deng

Nous allons nous intéresser maintenant à la conjecture originale de *Tu et Deng*, introduite dans le chapitre 4. Il s'agit d'une conjecture combinatoire intimement liée à la notion d'immunité algébrique d'un nombre considérable de fonctions booléennes comme on a pu le voir précédemment. Plus précisément, l'optimalité de leur immunité algébrique dépend de la validité de cette conjecture combinatoire.

Conjecture 1 (Tu-Deng [TD11])**.** *Soit* $k \geq 2$ *un entier,* $t \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)^*$ *et posons :*

$$S_{t,k} = \{(a,b) \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)^2, \text{ tel que } \underbrace{a+b=t}_{\text{équation}(1)} \text{ et } \underbrace{w_H(a)+w_H(b) \leq k-1}_{\text{inéquation}(2)}\},$$

alors $|S_{t,k}| \leq 2^{k-1}$.

Ce chapitre est organisé de la façon suivante. Nous commençons par définir les notations et notions de base que nous allons utiliser tout au long de ce chapitre avant de donner un aperçu de l'approche utilisée. Dans la section 7.2 nous définissons une relation d'équivalence sur $(\mathbb{Z}/(2^k-1)\mathbb{Z})^2$. Dans la section 7.3 nous intégrons la première condition de la conjecture de Tu et Deng 1 ($a+b=t$) à la notion de classe d'équivalence puis nous présentons des applications qui manipulent les classes d'équivalence tout en gardant la somme modulaire invariante. Dans la section 7.4 nous définissons un partitionnement en blocs des classes d'équivalence et nous donnons une nouvelle présentation des classes, plus exploitable du point de vue pratique. Ensuite, pour un t fixé nous donnons dans la section 7.5 une formule du cardinal de l'ensemble des solutions $(a,b) \in (\mathbb{Z}/(2^k-1)\mathbb{Z})^2$ de même poids. Enfin, dans la section 7.6 nous introduisons un polynôme P_t qui présente un lien particulier avec l'ensemble des solutions $(a,b) \in (\mathbb{Z}/(2^k-1)\mathbb{Z})^2$ de même poids ce qui nous permet de trouver une famille de t vérifiant la conjecture.

7.1 Notations et aperçu

Avant de rentrer dans le vif du sujet, nous avons besoin de définir plusieurs notations autour des vecteurs de k bits que l'on va constamment manipuler tout au long de ce chapitre. Ainsi, sauf contre indication, nous utilisons les notations suivantes :

- $k \in \mathbb{N}$ désigne la longueur des chaînes binaires.
- $t \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)$ est un entier modulaire fixé.
- Pour un entier $a \in \mathbb{N}$ on note $(a_0, \ldots, a_{k-1})$ sa représentation binaire : $a = \sum_{i=0}^{k-1} a_i 2^i$, avec $a_i \in \mathbb{F}_2$.
- $u||v$ désigne la concaténation de u et v.
- Dans le cas ou J est un ensemble d'éléments, $|J|$ désignera le cardinal de J et , $J-1 = \{y-1, y \in J\}$ et $J+1 = \{y+1, y \in J\}$; dans le cas ou J est une valeur, il désignera la valeur absolue J,
- Pour $t \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)$ et $(t_0, \ldots, t_{k-1})$ sa représentation binaire, $w_H(t)$ désigne le poids de Hamming de t et on a $w_H(t) = \sum_{i=0}^{k-1} t_i$.
- Pour $t \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)$, $m(t)$ désigne l'image "miroir" de t : si $t = \sum_{i=0}^{k-1} t_i 2^i$, alors $m(t) = \sum_{i=0}^{k-1} t_{k-1-i} 2^i$.

Nous rappelons maintenant la conjecture de *Tu et Deng* [TD11] déjà mentionnée dans la partie précédente :

Conjecture 1 (Tu-Deng). *Soit $k \geq 2$ un entier, $t \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)^*$ et posons :*

$$S_{t,k} = \{(a,b) \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)^2, \text{ tel que } \underbrace{a+b=t}_{équation(1)} \text{ et } \underbrace{w_H(a)+w_H(b) \leq k-1}_{équation(2)}\},$$

alors $|S_{t,k}| \leq 2^{k-1}$.

Avant d'aller plus loin, nous allons résumer brièvement notre approche. La problématique de départ de ce travail est de pouvoir énumérer tous les éléments de $S_{t,k}$ de façon efficace. On essaie pour cela de passer d'un couple de $S_{t,k}$ à l'autre de façon assez simple. Nous utilisons ensuite ces nouveaux outils pour démontrer un nouveau résultat plus concret, $|S_{t,k}| = |S_{m(t),k}|$.

Donnons un exemple pour mieux comprendre la démarche :

$$a = 1000101010111101001010$$

$$b = 1101010110101000101010$$

Nous pouvons construire un autre couple (a', b') tel que $a' + b' = a + b$ et $w_H(a') + w_H(b') = w_H(a) + w_H(b) + 1$.

$$a' = 1010101010111101001010$$

$$b' = 1110010110101000101010$$

A partir de là nous pouvons nous poser plusieurs questions :

- Y a-t-il une autre transformation qui conserve la somme et qui ne change pas beaucoup la somme des poids ?
- Est ce que l'on peut atteindre tous les couples de $S_{t,k}$ en partant d'un seul ?
- En appliquant plusieurs fois les transformations, à partir de quand retombe-t-on sur les mêmes couples ?

Nous répondons à ces questions dans ce chapitre.

- Il y a deux transformations simples qui conservent la somme sans trop changer le poids : $01 + 01 = 11 + 01$ que nous appelons ϕ et $00 + 01 = 10 + 10$ que nous appelons ψ. Elles sont détaillées dans la section 7.3.
- Tous les couples de $S_{t,k}$ sont atteignables à partir de n'importe quel autre couple de $S_{t,k}$, on le démontre dans le lemme 7.3.3.
- On introduit une structure de blocs dans la section 7.4. On démontre que les applications ϕ et ψ ne retombent jamais sur les mêmes couples à l'intérieur des blocs et que l'on retombe systématiquement sur un couple déjà connu en sortant des blocs.

On peut aussi faire quelques remarques :

- Les couples $(0, t)$ et $(t, 0)$ appartiennent à $S_{t,k}$.
- Dans la somme $a + b$, lorsque $a_i + b_i = 1$, (a_i, b_i) peut être égal à $(0, 1)$ ou $(1, 0)$. Cela implique que des couples (a, b) peuvent être regroupés ensemble dans des classes dont le nombre d'élément est une puissance de deux, sauf dans le cas expliqué ci-dessous. On décrit ces classes dans les sections 7.2 et 7.3.
- Comme le mot tout à 1 '$11\ldots1$' est égal à 0 modulo $2^k - 1$, il y a deux couples de moins dans cette classe.

Nous commençons donc par regrouper les couples sous forme de classes dans les sections 7.2 et section 7.3 et nous expliquons comment passer d'une classe à une autre grâce aux applications ϕ et ψ. Ensuite nous décrivons une structure de blocs afin d'utiliser correctement ϕ et ψ dans 7.4. Cela nous amène à une formule pour calculer plus simplement $|S_{t,k}|$ dans 7.5. Dans la dernière section 7.6.2 nous démontrons que $|S_{t,k}| = |S_{m(t),k}|$ à l'aide des outils développés dans les sections précédentes. Enfin nous concluons en donnant une nouvelle famille d'entiers t qui vérifient la conjecture dans la proposition 7.6.3.

7.2 Relation d'équivalence sur $(\mathbb{Z}/(2^k-1)\mathbb{Z})^2$

Dans cette section nous nous intéressons de plus près aux éléments de l'ensemble $(\mathbb{Z}/(2^k-1)\mathbb{Z})^2$. L'objectif ici est de regrouper sous formes de *classes* les éléments qui ont un certain point commun. En effet, en permutant les bits de a et b sur le même indice nous obtenons d'autres couples qui ont la même somme modulaire (équation (1) de la conjecture) et la même somme des poids (équation (2) de la conjecture). Nous mettons en commun les éléments que l'on peut obtenir facilement en permutant les bits de a et b sur le même indice. Pour cela nous définissons la *relation d'équivalence* suivante sur l'ensemble $(\mathbb{Z}/(2^k-1)\mathbb{Z})^2$:

Définition 7.2.1 (relation d'equivalence)**.** *Soit* $k \in \mathbb{N}$.
Deux couples $(a,b),(a',b') \in (\mathbb{Z}/(2^k-1)\mathbb{Z})^2$ *sont* équivalents*, et on note* $(a,b) \sim (a',b')$ *si*

$$\forall i \in \{0,\dots,k-1\},\ a_i + b_i = a'_i + b'_i \text{ (dans } \mathbb{Z}),$$

avec a_i*,* b_i*,* a'_i *et* b'_i *les* i^{eme} *coefficients dans les représentations binaires de* a*,* b*,* a' *et* b'*. Notons* $\mathcal{C}$ *l'ensemble quotient de* $(\mathbb{Z}/(2^k-1)\mathbb{Z})^2$ *par la relation* $\sim$*.*

L'intérêt d'une telle approche est double. D'une part, elle permet de regrouper les couples (a,b) de mêmes caractéristiques dans la même classe d'équivalence. D'autre part, elle permet de faciliter la manipulation de ces éléments.

Cependant, en raison du caractère invariant du poids de Hamming dans une même classe d'équivalence c de $\mathcal{C}$, une représentation plus simple en un k-uplet $(c_0,\dots,c_{k-1}) \in \{0,1,2\}^k$ des classes d'équivalences est possible et bienvenue. Cette représentation est définie comme suit : soit $(a,b) \in c$, alors

$$\forall i \in \{0,\dots,k-1\},\ c_i = \begin{cases} 0\ si & w_H((a_i,b_i)) = 0 \\ 1\ si & w_H((a_i,b_i)) = 2 \\ 2\ si & w_H((a_i,b_i)) = 1 \end{cases} \tag{7.2.1}$$

A partir de maintenant, nous désignerons les classes d'équivalences par leurs représentations en k-uplets. Nous allons à présent présenter quelques résultats relatifs à une classe d'équivalence $(c_0,\dots,c_{k-1})$ donnée mais quelconque.

Proposition 7.2.1. *Soient $c = (c_0,\dots,c_{k-1}) \in \{0,1,2\}^k$ et n_1 (resp. n_2) le nombre de composantes égales à 1 (resp. 2) dans cette représentation. Alors*

$$|c| = \{ \begin{array}{ll} 2^{n_2}-2 & si \quad c_i \neq 0,\ 0 \leq \forall i \leq k-1 \\ 2^{n_2} & sinon \end{array}$$

et $\forall (a,b) \in c\ ,\ w_H(a) + w_H(b) = 2n_1 + n_2$.

Démonstration. Nous savons par l'équation 7.2.1 que :

- $c_i = 2$ implique que $w_H(a_i,b_i) = 1$ et ainsi (a_i,b_i) est égal à $(0,1)$ ou $(1,0)$.
- $c_i = 0$ (resp. $c_i = 2$) implique $(a_i,b_i) = 0$ (resp. $(a_i,b_i) = (1,1)$)

Ainsi, tout i dans $\{0,\dots,k-1\}$ tel que $c_i = 2$ double le nombre de possibilités. Pour finir de démontrer le premier résultat il suffit de constater que les couples $(0, 2^k-1)$ et $(2^k-1, 0)$ ne sont pas des classes valides modulo 2^k-1. C'est pourquoi lorsqu'il n'apparaît aucune coordonnée nulle (dans la représentation en k-uplet), il faut retrancher 2 à la formule générale. D'où le premier résultat : $|c| = 2^{n_2}$, si il y a au moins une coordonnée non nulle et $|c| = 2^{n_2} - 2$ sinon.

Intéressons-nous maintenant au deuxième résultat : pour tout $(a,b) \in c$ nous avons

$$\begin{aligned} w_H(a) + w_H(b) &= \sum_{(a_i,b_i)=(0,0)} 0 + \sum_{(a_i,b_i)=(0,1)} 1 + \sum_{(a_i,b_i)=(1,0)} 1 + \sum_{(a_i,b_i)=(1,1)} 2 \\ &= \sum_{(a_i,b_i)=(0,1)ou(1,0)} 1 + \sum_{(a_i,b_i)=(1,1)} 2 \\ &= \sum_{c_i=2} 1 + 2\sum_{c_i=1} 1 = n_2 + 2n_1 \end{aligned}$$

avec les notations de la proposition.

□

7.3 Somme modulaire sur $(\mathbb{Z}/(2^k-1)\mathbb{Z})^2$ et classes d'équivalence

La conjecture de *Tu et Deng* porte sur deux conditions : $a+b=t$ et $w_H(a)+w_H(b) < k$. Ici nous nous intéressons aux classes qui vérifient la première condition. Nous désignerons par $\mathcal{C}_t$ l'ensemble de ces classes et nous le définissons comme suit :

Définition 7.3.1. *Soit* $t \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)$,

$$\mathcal{C}_t = \{c \in \mathcal{C} : \exists (a,b) \in c \text{ et } a+b=t\}$$

Le but ici est de trouver un moyen de passer d'une classe à une autre en jouant sur la variation du poids de Hamming tout en gardant la somme modulaire invariante. Pour ce, nous commencerons par définir un ensemble d'applications agissant sur un couple de composantes consécutives d'une classe c donnée, puis nous démontrerons que l'ensemble $\mathcal{C}_t$ reste invariant par ces applications.

Commençons par définir ces applications :

Définition 7.3.2. *Pour tout* i, $0 \leq i \leq k-1$, ϕ_i *et* ψ_i *sont des applications de* $\mathcal{C}$ *dans* $\mathcal{C}$ *définies comme suit :*

$$\forall c \in \mathcal{C},\ \phi_i(c) = \begin{cases} (c_0,\ldots,c_{i-1},0,1,\ldots,c_{k-1}) & \text{si } c_i = 1 \text{ et } c_{i+1}=2 \\ c & \text{sinon} \end{cases}$$

$$\forall c \in \mathcal{C},\ \psi_i(c) = \begin{cases} (c_0,\ldots,c_{i-1},0,2,\ldots,c_{k-1}) & \text{si } c_i = 1 \text{ et } c_{i+1}=0 \\ c & \text{sinon} \end{cases}$$

Nous allons maintenant démonter que ces applications conservent la somme modulaire.

Proposition 7.3.1. *Soient* $t \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)$ *et pour tout* i, $\forall\ 0 \leq i \leq k-1$ *les applications* ϕ_i *et* ψ_i *définies dans la Définition 7.3.2.*
Alors :

1. $\forall c \in \mathcal{C}_t, \phi_i^{-1}(c) \in \mathcal{C}_t$.
2. $\forall c \in \mathcal{C}_t, \psi_i^{-1}(c) \in \mathcal{C}_t$.

Démonstration. Considérons $c = (c_0,\ldots,c_i,c_{i+1},\ldots,c_{k-1})$ dans $\mathcal{C}_t$, avec $t = (t_0,\ldots,t_i,t_{i+1},t_{i+2}\ldots,t_{k-1})$.

Ces deux propriétés découlent directement de l'addition binaire modulo 2^k-1.

1. Le résultat de l'addition binaire : $11+01$ (représentée par $\ldots,1,2,\ldots$ dans la représentation en k-tuplet de c) est égal au résultat de l'addition $01+01$ (représentée par $\ldots,0,1,\ldots$ dans la représentation en k-uplet de c).
2. Nous pouvons utiliser le même argument $(10+10=00+01)$ pour prouver que $\psi_i^{-1}(c)\in\mathcal{C}_t$.

□

Pour continuer notre étude, nous démontrons l'existence d'une classe de poids maximal qu'on notera τ.

Proposition 7.3.2. *(Existence et unicité de τ) Il existe une seule classe dans $\mathcal{C}_t$, correspondant au k-uplet dont toutes les composantes sont non nulles. Nous notons cette classe τ et nous avons :*

$$\forall(a,b)\in\tau,\ w_H(a)+w_H(b)=k+w_H(t).$$

Démonstration. Soit $t\in\left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)^*$

- *Existence* : le couple $(a,b)=(t,2^k-1)$ est une solution de poids $k+w_H(t)$. On en déduit aisément que les coordonnées des composantes égales à 1 (resp. à 2) dans la représentation en k-upplet de τ sont exactement les mêmes que celles égales à 1 (resp. à 0) dans la représentation binaire de t.
- Unicité : soient $(a,b),(a',b')\in(\mathbb{Z}/(2^k-1)\mathbb{Z})^2$ appartenant à deux classes d'équivalence dont les représentations en k-uplets ne contiennent pas de coefficients à zero. Alors pour
  tout i tel que $0\leq i\leq k-1, a_i\neq 0$ ou $b_i\neq 0$. Nous avons
  $$a+b=\sum_{i=0}^{k-1}2^i(a_i+b_i)=\sum_{i=0}^{k-1}2^i+\sum_{i=0}^{k-1}2^i(a_i+b_i-1)$$
  avec $a_i+b_i-1\in\{0,1\}$ car $a_i+b_i\in\{1,2\}$.
  De même pour $a'+b'$. Alors, on obtient
  $$\sum_{i=0}^{k-1}2^i(a_i+b_i-1)=\sum_{i=0}^{k-1}2^i(a'_i+b'_i-1)\bmod 2^k-1.$$
  Comme la représentation binaire d'un nombre est unique, nous en déduisons que $a_i+b_i-1=a'_i+b'_i-1$, et que $a_i+b_i=a'_i+b'_i$, et ensuite que (a,b) et (a',b') appartiennent à τ.

□

Enfin, dans le lemme qui va suivre nous démontrerons qu'à partir d'une classe $c\in\mathcal{C}_t$ et d'un nombre de compostions fini des applications ϕ_i et ψ_i de la définition 7.3.2 nous pouvons retrouver la classe maximale τ.

Lemme 7.3.3. *Soit $c \in \mathcal{C}_t$ avec $1 \leq t \leq 2^k - 2$. Il existe un entier N et une sequence d'indices $i_1, \ldots, i_N$ tels que :*

$$\circ_{j=1}^{N} f_{i_j}(c) = \tau \text{ avec } f_{i_j} = \phi_{i_j}^{-1} \text{ ou } f_{i_j} = \psi_{i_j}^{-1}$$

avec $\circ$ l'application composition.

Démonstration. Soit $c \in \mathcal{C}_t$. Construisons récursivement la suite $(U_n)_{n\in\mathbb{N}}$ à valeurs dans $\mathcal{C}_t$ de la façon suivante :

$$U_0 = c \text{ et } U_n = \begin{cases} \psi_{j_0}^{-1}(U_{n-1}) & \text{si} \quad (U_{n-1})_{j_0} = 0 \text{ et } (U_{n-1})_{j_0+1} = 2 \\ U_{n-1} & \text{sinon} \end{cases}$$

où j_0 correspond à la première coordonnée de la classe U_{n-1} telle que $(U_{n-1})_{j_0} = 0$ et $(U_{n-1})_{j_0+1} = 2$. En notant I le nombre de composantes à 2 dans c, on remarque que pour tout $n \geq I$, (U_n) restera constante.

De la même manière nous définissons une deuxième suite $(V_n)_{n\in\mathbb{N}}$ comme :

$$V_0 = U_I \text{ et } V_n = \begin{cases} \phi_{j_1}^{-1}(V_{n-1}) & \text{si} \quad V_{n-1_{j_1}} = 0 \text{ et } V_{n-1_{j_1+1}} = 1 \\ V_{n-1} & \text{sinon} \end{cases}$$

où j_1 correspond à la première coordonnée de la classe V_{n-1} telle que $(V_{n-1})_{j_1} = 0$ et $(V_{n-1})_{j_1+1} = 1$.

La séquence devient constante après un nombre d'itérations au moins égal au nombre de 0 dans la classe c. Posons $c' = \lim_{n\to+\infty} V_n$. La classe c' ne contient pas de sequence à 01 ou à 02. Donc, c' ne comporte aucune coordonnée à zéro (car $t \neq 0$).

On déduit de la proposition 7.3.1 que $c' \in \mathcal{C}_t$ et de la proposition 7.3.2 que $c' = \tau$.

□

Ce lemme permet de déduire que pour un t fixé nous pouvons, à l'aide des transformations ϕ et ψ, recouvrir tout l'ensemble $\mathcal{C}_t$. Malheureusement, le nombre et le type des transformations pour atteindre la classe τ à partir d'une classe quelconque $c \in \mathcal{C}_t$ est difficile à appréhender et n'est pas unique. Dans le but de recouvrir exactement l'ensemble $\mathcal{C}_t$ nous allons dans la section suivante chercher une autre représentation plus facile à traiter.

7.4 Représentation en w-uplets

Dans la section précédente nous avons démontré qu'à partir de la classe maximale τ et des transformations ϕ et ψ définies dans la définition 7.3.2

nous pouvons retrouver toutes les classes appartenant à $\mathcal{C}_t$. On introduit maintenant une structure simple sur t afin de savoir comment utiliser ϕ et ψ pour énumérer tous les couples de $\mathcal{C}_t$ sans retomber sur les mêmes.

7.4.1 Blocs

Pour continuer notre étude, considérons t entre 1 et $2^k - 1$ et notons son poids w. Notons également les indices des coordonnées à 1 dans la représentation binaire de t comme $0 \leq p_0 \leq \cdots \leq p_{w-1} \leq k-1$.

Considérons d'abord la représentation binaire de t comme suit :

$$t = 0000\underset{\uparrow\, p_0}{1}0\ldots0\ \underset{\uparrow\, p_{j-1}}{1}\ \ \underset{\uparrow\, p_{j-1}+1}{0}\ \ \ldots0\underset{\uparrow\, p_j}{1}00\ldots000\ \underset{\uparrow\, p_{w-1}}{1}\ 000$$

Et décomposons les classes $c \in \mathcal{C}_t$ en w blocs $B_j, 0 \leq j \leq w-1$, de la façon suivante.

Définitions 7.4.1. *Soit $c = (c_0, \ldots, c_{p_j} \ldots, c_{k-1}), \in \mathcal{C}_t$. Pour $j \in \{0, \ldots, w-1\}$, nous désignerons par $B_j = c_{p_j \mod k} \ldots c_{p_{j+1}-1 \mod k}$ le j-éme bloc de c et nous noterons sa longueur $L_j = p_{j+1} - 1 - p_j \mod w$.*

Pour illustrer cette définition, considérons d'abord la représentation binaire de t et la représentation en k-uplets de τ :

$$t = 0000\underset{\uparrow\, p_0}{1}0\ldots0\ \underset{\uparrow\, p_{j-1}}{1}\ \ \underset{\uparrow\, p_{j-1}+1}{0}\ \ \ldots0\underset{\uparrow\, p_j}{1}00\ldots000\ \underset{\uparrow\, p_{w-1}}{1}\ 000$$

$$\tau = 2222\underset{\uparrow\, p_0}{1}2\ldots2\ \underset{\uparrow\, p_{j-1}}{1}\ \ \underset{\uparrow\, p_{j-1}+1}{2}\ \ \ldots2\underset{\uparrow\, p_j}{1}22\ldots222\ \underset{\uparrow\, p_{w-1}}{1}\ 222$$

Ceci définit les valeurs de $p_0, \ldots, p_{w-1}$ et ainsi toute classe $c \in \mathcal{C}_t$ sera découpée de la façon suivante :

$$c = (\underbrace{c_0, \ldots c_{p_0-1}}_{B_{w-1}}, \overbrace{c_{p_0} \ldots c_{p_1-1}}^{B_0}, \ldots, \overbrace{c_{p_j} \ldots c_{p_{j+1}-1}}^{B_j} \ldots,$$
$$\ldots, c_{p_{w-1}-1}, \underbrace{c_{p_{w-1}}, c_{k-1}}_{B_{w-1}})$$

Remarque : Le découpage est cyclique et le dernier bloc B_0 commence à partir de l'indice p_{w-1} du k-uplet.

L'intérêt de cette décomposition est qu'elle permet de déterminer les positions des séquences 12 dans τ et ainsi permettra de déterminer le nombre de transformations possibles.

7.4.2 Bijection

Dans cette sous-section, nous donnons une nouvelle représentation des éléments de $\mathcal{C}_t$ en introduisant une application qu'on notera $\Phi_t()$ et qui fera la correspondance entre $\mathcal{C}_t$ et un ensemble particulier qu'on notera E_t. L'intérêt ici est de trouver une expression plus exploitable qui intègre la décomposition en blocs expliquée dans la section précédente.

Pour $1 \leq t \leq 2^k - 1$, $0 \leq i \leq w-1$, et les longueurs L_i de la définition 7.4.1, nous définissons les ensembles qui nous intéressent de la façon suivante :

- $\mathcal{E} = \{-1, \ldots, L_0\} \times \cdots \times \{-1, ..., L_{w-1}\}$,
- $E_t = \{(x_0, \ldots, x_{w-1}) \in \mathcal{E}$ tel que si $x_j = -1$ alors $x_{j+1} \neq L_{j+1}\}$.

À présent, nous allons introduire une application qu'on notera $\Phi_t(.)$ et qui fera la correspondance entre l'ensemble des classes et l'ensemble E_t.

Définition 7.4.1. *Nous définissons l'application $\Phi_t(.)$ de E_t dans $\mathcal{C}$ par : $(x_0, \ldots, x_{w-1})$ correspond à $(B_0||\ldots||B_{w-1})$ avec :*

- *Si $x_j \neq -1$ et $x_{j-1} \neq -1$ alors $B_j = 0\ldots01\overbrace{2\ldots2}^{x_j}$.*
- *Si $x_j \neq -1$ et $x_{j-1} = -1$ alors $B_j = 20\ldots01\overbrace{2\ldots2}^{x_j}$.*
- *Si $x_j = -1$ et $x_{j-1} \neq -1$ alors $B_j = \overbrace{0\ldots0}^{L_j}$.*
- *Si $x_j = -1$ et $x_{j-1} = -1$ alors $B_j = \overbrace{20\ldots0}^{L_j}$.*

Remarque : Nous savons que les bits à 2 représentent à chaque fois les deux possibilités (0,1) ou (1,0) en termes de solutions possibles d'où l'apparition du x_j dans l'expression finale qui se trouve plus bas.

Dans ce qui va suivre, nous allons montrer comment associer un élément de E_t à un élément de $\mathcal{C}_t$. Pour ce faire, nous présentons quelques résultats techniques qui vont nous servir à démontrer que $\Phi_t()$ est une bijection.

Proposition 7.4.2. *Soit $0 \leq t \leq 2^k - 2$. Nous avons alors :*

1. $\forall\ 0 \leq i \leq k-1, \phi_i(\Phi_t(E_t)) \subset \Phi_t(E_t)$.
2. $\forall\ 0 \leq i \leq k-1, \psi_i(\Phi_t(E_t)) \subset \Phi_t(E_t)$.

Démonstration. Ici, nous voulons montrer que l'image d'une représentation en blocs par l'application ϕ est encore une représentation en blocs. Pour ce faire, nous énumérons les différentes possibilités.

1. Considérons $(x_0, \ldots, x_{w-1}) \in E_t$ et $\Phi_t((x_0, \ldots, x_{w-1})) = c$. Nous voulons démontrer que $\phi_i(c)$ admet une représentation par blocs pour toute valeur de i et x. Dans le cas $c_i \neq 1$ ou $c_{i+1} \neq 2$: ϕ_i est l'identité et donc le résultat est prouvé. Dans ce qui suit, considérons $c_i = 1$ et $c_{i+1} = 2$. Si i et $i+1$ sont deux coordonnées appartenant au même bloc B_i alors $B_i = 0 \ldots 012 \ldots 2$ ou $B_i = 20 \ldots 012 \ldots 2$. Sinon si i appartient au bloc B_j et $i+1$ appartient au bloc B_{j+1}, alors la dernière coordonnée de B_j est égale à 1 d'après la définition 7.4.1 ($x_j = 0$) et la première coordonnée de B_{j+1} est égale à 2 et donc d'après la définition 7.4.1 alors $x_j = -1$ (contradiction puisque $x_j = 0$) ce qui conclut la preuve.

2. Nous pouvons utiliser une argumentation similaire pour prouver ce deuxième point : dans le cas ou i et $i+1$ se trouvent dans le même bloc il y a une contradiction avec la définition 7.4.1. Dans le cas contraire l'application ψ_i transforme une représentation en blocs en une autre représentation en blocs.

□

Ici, nous montrons la proposition principale de cette section.

Proposition 7.4.3. *Soit $0 \leq t \leq 2^k - 2$. L'application $\Phi_t()$ définie de E_t dans $\mathcal{C}_t$ est une bijection.*

Démonstration. Nous montrerons que $\Phi_t(E_t) \subset \mathcal{C}_t$ et que $\mathcal{C}_t \subset \Phi_t(E_t)$.

- Soit $c \in \Phi_t(E_t)$. Conformément à la définition 7.4.1 nous pouvons voir c comme une concaténation de w blocs ($c = B_0||\ldots||B_{w-1}$) et que tout bloc de la forme $20 \ldots 012 \ldots 2$ ou $20 \ldots 0$ dans la représentation en blocs de c est précédé d'un bloc de la forme $0 \ldots 0$ ou $20 \ldots 0$. Cela implique que nous pouvons utiliser les applications ψ_i^{-1} avec i la dernière coordonnée des blocs de la forme $20 \ldots 0$ ou $0 \ldots 0$ et que nous obtenons une nouvelle classe c' dont les blocs ne commencent pas par la valeur 2. De plus, tous les blocs de la classe c' commencent avec une séquence de 0 suivie de la valeur 1. Pour chaque bloc, Nous utilisons récursivement l'application ϕ_i avec $i+1$ sa première coordonnée vallant 1. Nous obtenons une nouvelle classe c' dont la première coordonnée de chaque bloc vaut 1 alors que les autres valent 2. Pour chaque bloc, nous utilisons récursivement l'application ϕ_i avec $i+1$ sa première coordonnée valant 1. Nous obtenons une nouvelle classe c' dont la première coordonnée de chaque bloc vaut 1 alors que les autres valent 2. La classe obtenue par cette transformation est alors τ. De plus nous avons $\tau \in \mathcal{C}_t$, $\phi^{-1}(\mathcal{C}_t) \subset \mathcal{C}_t$ et $\psi_i^{-1}(\mathcal{C}_t) \subset \mathcal{C}_t$ de la

proposition 7.4.2. Ce qui suffit pour prouver le résultat.

- Considérons $c \in \mathcal{C}_t$ et montrons que $\Phi_t(c) \in \Phi_t(E_t)$. Du lemme 7.3.3 nous posons $f_{i_1}, \ldots, f_{i_N}$ la séquence de transformations telle que ; $f_{i_j} = \phi_j$ ou ψ_{i_j}, et $\circ_{j=1}^{N} f_{i_j}(c) = \tau$. Nous savons que τ est composée de w blocs de la forme $12\ldots2$, et donc que τ appartient $\Phi_t(E_t)$ ($\tau = \Phi_t((L_0, \ldots, L_{w-1}))$). Nous pouvons déduire également du lemme 7.3.3 que la sequence $g_{i_j} = f_{i_j}^{-1}$ de i_N jusqu'à i_1 appliquée à τ nous procure c. Et ainsi, le résultat provient directement du fait que $\tau \in \Phi_t(E_t)$, $\phi(\Phi_t(E_t)) \subset \Phi_t(E_t)$ et $\psi_i(\Phi_t(E_t)) \subset \Phi_t(E_t)$.

□

7.5 Représentation en w-uplets et contrainte sur le poids

Dans cette section, nous introduisons une décomposition de $\mathcal{C}_t$ en fonction du poids des solutions $(a, b) \in c$. Cela conduira à une formule pour calculer le nombre de solutions pour un poids $r + 2w$.

La proposition ci-dessous nous permet de traduire les conditions sur les classes de $\mathcal{C}_t$ dans leur nouvelle représentation en w-uplets.

Proposition 7.5.1. *L'ensemble* $\{c \in \mathcal{C}_t$ *tel que* $c \sim (a, b)$ *et* $w_H(a)+w_H(b) = r + 2w\}$ *et l'ensemble* $\{c \in \mathcal{C}_t$ *tels que* $c = \Phi_t((x_0, \ldots, x_{w-1}))$ *et* $\sum_{j=0}^{w-1} x_j = r\}$ *sont les mêmes.*

Démonstration. Pour prouver cette proposition, nous devons établir une relation entre une valeur x_i et le nombre de coordonnées égales à 2 et à 1 dans le bloc décrit par x_i. Si $x_i \neq -1$ alors le nombre de coordonnées à 2 (resp. le nombre de coordonnées à 1) dans ce bloc est égal à x_i (resp. est égal à 1) sinon il est égal à 1 (resp. est égal à 0).
Si on considère les w blocs de la représentation, alors le nombre de 2 est égal à

$$\sum_{x_i \geq 0} x_i + \sum_{x_i = (-1)} 1,$$

et le nombre de coordonnées à 1 est égal à $\sum_{x_i \geq 0} 1$.

Intéressons-nous maintenant au poids des éléments de ces ensembles. À partir des notations de la proposition 7.2.1 le poids d'une représentation par

blocs est défini par $2 \times n_1 + n_2$, où n_1 est le nombre de coordonnées égales à 1 et n_2 le nombre de coordonnées égales à 2. Dans ce cas nous avons

$$\begin{aligned} 2 \times n_1 + n_2 &= 2 \sum_{x_i \geq 0} 1 + \sum_{x_i \geq 0} x_i + \sum_{x_i = (-1)} 1 \\ &= 2 \sum_{x_i \geq 0} 1 + \sum_{x_i \geq 0} x_i + \sum_{x_i = (-1)} -1 + 2 \sum_{x_i = (-1)} 1 \\ &= 2w + \sum_{x_i \geq -1} x_i \\ &= 2w + r. \end{aligned}$$

D'où le résultat.

□

Ici, nous montrons la proposition principale de cette section.

Proposition 7.5.2. *Notons $S_t(r)$ l'ensemble :*

$$S_t(r) = \{(a, b) \mid a + b = t \text{ et } w_H(a) + w_H(b) = r + 2w\}.$$

Alors le cardinal de $S_t(r)$ est :

$$|S_t(r)| = \sum_{\substack{(x_0, \ldots, x_{w-1}) \in E_t \\ et \sum_{j=0}^{w-1} x_j = r}} 2^r \prod_{x_j = -1} 4 - 2\delta_{k-w}(r)$$

où $\delta_{k-w}(k-w) = 1$ et 0 sinon.

Démonstration. Par la proposition 7.2.1, le nombre d'éléments dans $c = (c_1, \ldots, c_k)$ est égal à 2^{n_2}, avec n_2 le nombre de coordonnées de c égales à 2 dans sa représentation en k-uplet.

Par ailleurs, nous avons $c = \Phi_t((x_0, \ldots, x_{w-1})) \in \mathcal{C}_t$ avec $\sum_{j=0}^{w-1} x_j = r$ (voir la proposition 7.5.1). De plus,

$$n_2 = \overbrace{\sum_{x_j \geq 0} x_j + \sum_{x_j = -1} |x_j|}^{\text{définition 7.4.1}} = \sum_{j=0}^{w-1} |x_j| = r + 2 \sum_{x_j = -1} |x_j|.$$

Alors le nombre de couples $(a, b) \in c$ est :

$$2^{r + 2 \sum_{xj=-1} |x_j|} - 2\delta_{w-k}(r) = 2^r \prod_{x_j = -1} 4 - 2\delta_{k-w}(r).$$

Par conséquent, considérons tous les w-uplets $(x_0, \ldots, x_{w-1}) \in E_t$ tels que $\sum_{j=0}^{w-1} x_j = r$. Alors le nombre d'éléments dans $S_t(r)$ se traduit comme suit :

$$|S_t(r)| = \sum_{\substack{(x_0,\ldots,x_{w-1})\in E_t \\ \text{and } \sum_{j=0}^{w-1} x_j = r}} 2^r \prod_{x_j=-1} 4 - 2\delta_{k-w}(r)$$

□

Remarque : Cette proposition permet de regrouper les solutions de même poids égal à $r + 2w$ dans le même ensemble et donne une expression du cardinal de ce dernier en traduisant les contraintes sur le poids sous une autre forme. Le lien avec la conjecture de *Tu et Deng* est le suivant :

$$S_{t,k} = \cup_{r<k-2w} S_t(r)$$

7.6 L'égalité entre l'expression polynomial de t et celle de $m(t)$

Dans cette section nous nous servons des résultats et des outils des sections précédentes pour démontrer que $|S_{t,k}| = |S_{m(t),k}|$ avec $m(t)$ le miroir de t. Nous en déduisons une nouvelle famille d'entiers t pour laquelle la conjecture est vraie.

7.6.1 Une deuxième énumération des w-uplets

Nous donnons dans cette sous-section une seconde énumération plus appropriée des w-uplets pour la démonstration finale. L'ensemble E_t est défini avec la condition (si $x_i = -1$ alors $x_{i+1} \neq L_{i+1}$) ce qui rend sa manipulation assez difficile. Dans la suite, nous allons utiliser les ensembles ci-dessous :

$$E_t(J) = \{(x_0, \ldots, x_{w-1}) \in \mathcal{E} \text{ t.q. } i \in J \Rightarrow x_i = -1 \text{ et } x_{i+1} = L_{i+1}\}$$

Ceci permet une énumération plus naturelle des w-uplets.

Le résultat de cette sous-section est que l'on peut décrire E_t à l'aide d'une combinaison linéaire des ensembles $E_t(J)$.

Notons $\gamma = \lfloor \frac{w}{2} \rfloor$ l'entier maximal tel que $E_t(J)$ est non vide et $|J| = \gamma$. Nous définissons $\gamma + 1$ coefficients $(v_\ell(x))_{0\leq\ell\leq\gamma}$ dépendant d'un w-uplet x, tels que $v_\ell(x)$ est le nombre d'ensembles J de cardinal ℓ tel que x appartient à $E_t(J)$. C'est exactement le nombre de fois où le w-uplet x apparaît dans les $E_t(J)$ avec $|J| = l$.

Présentons maintenant le résultat de cette sous section :

Proposition 7.6.1. *Il existe $\gamma+1$ coefficients $u_0,\dots,u_\gamma$ tels que*

$$\begin{cases} \sum_{\ell=0}^{\gamma} v_\ell(x)u_\ell = 1 & x \in E_t \\ \sum_{\ell=0}^{\gamma} v_\ell(x)u_\ell = 0 & sinon. \end{cases}$$

avec $\gamma = \lfloor \frac{w}{2} \rfloor$ et $v_\ell(x)$ le nombre d'ensembles J de cardinal ℓ tel que x appartient à $E_t(J)$.

Démonstration. La taille possible pour un ensemble J tel que $E_t(J)$ est non vide est entre 0 et γ car chaque indice dans J désigne une coordonnée égale à -1, et à chacune de ces coordonnées on fait correspondre une autre coordonnée à sa droite. Donc à chaque ensemble J on fait correspondre $2|J|$ coordonnées. Cela explique pourquoi un J de taille supérieure à γ donnerait un $E_t(J)$ vide. Cela nous servira pour la suite de la preuve.

Pour chaque $x \in \mathcal{E}$ il existe un ensemble J de taille maximale tel que $x \in E_t(J)$: on l'appelle J_x. Le nombre d'ensembles J de taille ℓ qui contiennent x est $\binom{|J_x|}{\ell}$. Donc les coefficients $u_0,\dots,u_\gamma$ vérifient les équations :

$$\begin{cases} \sum_{i=0}^{|J_x|} \binom{\ell}{i} u_i = 1 & x \in E_t \\ \sum_{i=0}^{|J_x|} \binom{\ell}{i} u_i = 0 & sinon \end{cases}$$

Car $x \in E_t$ pour $|J_x| = \emptyset$. Comme ces équations ne dépendent que de $|J_x|$, il y a au plus γ équations. Donc il existe au moins une solution pour $u_0,\dots,u_\gamma$. La forme des équations montre que la solution est unique. □

On peut alors exprimer d'une manière récursive la quantité $|S_t(r)|$ (relativement à $E_t(J)$) comme suit :

$$|S_t(r)| = \sum_{h=0}^{\gamma} u_h \sum_{\substack{J\subset\{0,\dots,w-1\} \\ |J|=h}} \sum_{\substack{(x_1,\dots,x_w)\in E_t(J) \\ \text{et } \sum_{j=0}^{w-1} x_j = r}} 2^r \prod_{x_j=-1} 4 - 2\delta_{k-w}(r)$$

7.6.2 L'expression polynomiale P_t

Le deuxième résultat de ce chapitre est de démontrer que pour tout entier r, $|S_t(r)| = |S_{m(t)}(r)|$. A cette étape de notre étude, nous voulons comparer tous les $|S_t(r)|$ et $|S_{m(t)}(r)|$ en même temps. Pour ce, nous introduisons l'expression polynomiale suivante ;

$$P_t(q) = \sum_{r=-w}^{k-w} \frac{|S_t(r)| + 2\delta_{k-w}(r)}{2^r} q^r.$$

Nous pouvons dès lors reformuler le résultat désiré comme : $P_t = P_{m(t)}$. Pour poursuivre notre approche, nous avons besoin de décrire le polynôme P_t à l'aide des ensembles $E_t(J)$ introduits précédemment :

$$P_t(q) = \sum_{r=-w}^{k-w} \sum_{\ell=0}^{\gamma} u_\ell \sum_{\substack{J\subset\{0,\ldots,w-1\} \\ |J|=\ell}} \sum_{\substack{(x_0,\ldots,x_{w-1})\in E_t(J) \\ \text{et } \sum_{j=0}^{w-1} x_j = r}} q^r \prod_{x_j=-1} 4$$

$$P_t(q) = \sum_{\ell=0}^{\gamma} u_\ell \sum_{\substack{J\subset\{0,\ldots,w-1\} \\ |J|=\ell}} \sum_{(x_0,\ldots,x_{w-1})\in E_t(J)} \prod_{x_i\geq 0} q^{x_i} \prod_{x_j=-1} \frac{4}{q}$$

Nous fixons l'ensemble $J \subset \{0,\ldots,w-1\}$ pour calculer

$$\sum_{x\in E_t(J)} \prod_{x_i\geq 0} q^{x_i} \prod_{x_j=-1} \frac{4}{q}$$

Nous pouvons voir cette somme comme un produit composé de tous les w-uplets. Cela veut dire que dans les w-uplets il y a $|J|$ couples de coordonnées de la forme $(-1, L_{j+1})$. Ce qui peut être traduit par $\prod_{j\in J} q^{L_{j+1}} \frac{4}{q}$. Il y a aussi toutes les autres valeurs possibles pour le reste des coordonnées, ce qui peut s'écrire comme une somme d'une progression géométrique :

$$\prod_{\substack{e\notin J \\ e\notin J+1}} \left(\frac{q^{L_e+1}-1}{q-1} + \frac{4}{q}\right)$$

Par conséquent, nous avons l'égalité :

$$\prod_{j\in J} q^{L_{j+1}} \frac{4}{q} \prod_{\substack{e\notin J \\ e\notin J+1}} \left(\frac{q^{L_e+1}}{q-1} + \left(\frac{-1}{q-1} + \frac{4}{q}\right)\right).$$

et nous distribuons le dernier produit pour obtenir :

$$\frac{4}{q}^w \prod_{j\in J} q^{L_{j+1}} \sum_{h=0}^{w-|J|} \left(\frac{-1}{q-1} + \frac{4}{q}\right)^{w-|J|-h} \left(\frac{q}{q-1}\right)^h \times$$

$$\sum_{\substack{L\subset\{0,\ldots,w-1\}\setminus(J\cup(J+1)) \\ |L|=h}} \prod_{e\in L} q^{L_e}$$

De là, nous pouvons constater que le résultat peut être exprimé sous la forme :

$$\sum_{h=0}^{w-|J|} \sum_{\substack{L\subset\{0,\ldots,w-1\}\setminus(J\cup(J+1)) \\ |L|=h}} C(w,|J|,h) \prod_{e\in L\cup(J+1)} q^{L_e}$$

Avec, $C(w,|J|,h)$ une quantité qui ne dépend que de $|J|$, w, hl et q. Dans la section suivante, nous allons prouver que le nombre de monômes $\prod_{e\in L\cup(J+1)} q^{L_e}$ est le même pour P_t and $P_{m(t)}$.

7.6.3 P_t et $P_{m(t)}$

Dans cette section nous nous intéressons à $P_{m(t)}$. L'entier $m(t)$ peut être représenté par $(L_{w-1},\ldots,L_0)$. On voit que l'on peut exprimer $m(t)$ en fonction de la représentation $(L_{w-1},\ldots,L_0)$ grâce à l'ensemble :

$$E_{m(t)} = \{(x_0,\ldots,x_{w-1}) \in \mathcal{E} \text{ tel que si } x_j = -1 \text{ alors } x_{j-1} \neq L_{j-1}\}$$

Ensuite on peut exprimer $P_{m(t)}(q)$ par :

$$\sum_{\ell=0}^{\gamma} u_\ell \sum_{\substack{J\subset\{0,\ldots,w-1\} \\ |J|=\ell}} \sum_{\substack{L\subset\{0,\ldots,w-1\}\setminus(J\cup(J-1)) \\ |L|=h}} C(w,|J|,h) \prod_{e\in L\cup(J-1)} q^{L_e}$$

Le nombre de monômes $\prod_{e\in L\cup(J+1)} q^{L_e}$ in P_t dépend du nombre d'ensembles L et J que nous pouvons construire à partir de l'ensemble $T = L\cup(J+1)$ avec $L\cap(J+1)=\emptyset$ et $L\cap J=\emptyset$. Nous montrons dans le prochain lemme que cette quantité est égale au nombre d'ensembles L et J que nous pouvons construire à partir de l'ensemble $T = L\cup(J-1)$ avec $L\cap(J-1)=\emptyset$ et $L\cap J=\emptyset$.

Lemme 7.6.2. *Soit T un sous-ensemble de $\{0,\ldots,w-1\}$ et h un entier. La taille de l'ensemble*

$$\{(L,J)\ t.q.\ |L|=h\ et\ L\cup(J+1)=T\ et\ L\cap J=\emptyset\ et\ L\cap(J+1)=\emptyset\}$$

est égale à la taille de l'ensemble

$$\{(L,J)\ s.t.\ |L|=h\ et\ L\cup(J-1)=T\ et\ L\cap J=\emptyset\ et\ L\cap(J-1)=\emptyset\}.$$

Démonstration. Soit L et J des ensembles tels que $L\cup(J+1)=T$ et $L\cap J=\emptyset$ et $L\cap(J+1)=\emptyset$. L'ensemble T peut être décomposé de façon unique en

séquence de coordonnées consécutives de taille maximale. Par exemple T est la partie soulignée de l'ensemble $\{0, \ldots, 10\}$:

$$\{\underline{0,1,2},3,\underline{4},5,\underline{6,7,8,9},10\}.$$

Chaque séquence commence par une séquence (possiblement vide) d'éléments dans $J+1$ suivie d'une séquence (possiblement vide) d'éléments dans L car nous avons $L \cap J = \emptyset$. Par exemple, pour $J = \{10, 3, 5, 6, 7\}$ et $L = \{1, 2, 9\}$ dans l'exemple ci-dessous.

Pour tous les couples d'ensembles (L, J) nous procédons comme suit : pour toutes les séquences de coordonnées consécutives de T, $(s_1||s_2)$ avec $s_1 \subset (J+1)$ et $s_2 \subset L$, nous ajoutons les $|s_2|$ premiers éléments de $(s_1||s_2)$ à l'ensemble L' et le reste à l'ensemble J'. Dans notre exemple, cela donne : $L' = \{0, 1, 6\}$ et $J' = \{3, 8, 9, 10\}$.

Nous avons donc $L \cap (J' - 1) = \emptyset$ et $L' \cup (J' - 1) = T$. Cela décrit une bijection entre les deux ensembles et conclue la preuve. □

Nous déduisons que P_t et $P_{m(t)}$ ont les mêmes coefficients pour chaque monôme de même degré. Cela signifie que $P_t = P_{m(t)}$.

À partir du lemme 7.6.2 et de cette nouvelle expression on déduit que P_t et $P_{m(t)}$ ont les mêmes coefficients pour les monômes de même degré. Ce qui implique que $P_t = P_{m(t)}$. Donc, pour tout entier r on a l'égalité $|S_t| = |S_{m(t)}|$. Ce qui nous conduit au résultat phare de ce chapitre : $|S_t| = |S_{m(t)}|$.

Enfin, pour conclure ce chapitre nous présentons ci-dessous une nouvelle famille de t satisfaisant la conjecture de Tu et Deng.

Proposition 7.6.3 (Nouvelle famille de t)**.** *Soient $k \geq 2$ et $0 \leq t \leq 2^k - 2$: s'il existe j tel que $2^j m(t) = -t$, alors $|S_{t,k}| \leq 2^{k-1}$.*

Démonstration. Soit t un entier tel que $2^j m(t) = -t$. Dans ce chapitre nous avons prouvé que $|S_{t,k}| = |S_{m(t),k}|$. En utilisant le résultat $|S_{t,k}| = |S_{2^j t,k}|$ de [FRCM10, FR12] nous obtenons $|S_{t,k}| = |S_{2^j m(t),k}|$. Nous avons aussi en utilisant [FRCM10, FR12] : si t est tel que $|S_{t,k}| = |S_{-t,k}|$ alors $|S_{t,k}| \leq 2^{k-1}$. Ce qui permet de conclure.

□

Nous remarquons que la condition $2^j m(t) = -t$ n'est possible que si k est un nombre pair. On peut expliciter plus précisément les entiers qui forment cette nouvelle famille :

Pour chaque coordonnée t_i de t on a $t_i = -t_{k-1-i+j}$. Donc pour i entre 0 et $j-1$, on a $t_i = -t_{j-i}$, ce qui correspond à un palindrome inversé. Par exemple 00110101010011. Et pour i entre 0 et $k-1-j$, on a $t_{j+i} = -t_{j+k-1-j-i}$. Cela

correspond à un autre palindrome inversé, mais à l'indice j. Dont l'ensemble des entiers t qui vérifient $*2^j m(t) = -t$ est l'ensemble des mots binaires qui sont la concaténation de deux palindromes inversés (le premier de taille j). Par exemple 100110, 111000101010 ou 101100101111110011000000.

7.7 Conclusion

Dans ce chapitre, nous avons proposé deux nouveaux résultats sur la conjecture de Tu et Deng, et une nouvelle famille d'entiers qui vérifient la conjecture.

Nous avons décrit dans un premier temps, pour un $k \geq 2$, une relation d'équivalence sur l'ensemble $(\mathbb{Z}/(2^k-1)\mathbb{Z})^2$, qu'on a noté $\sim$. Puis nous avons proposé une première représentation des classes $c \in (\mathbb{Z}/(2^k-1)\mathbb{Z})^2/\sim$ sous forme de k-uplets dans $\{0,1,2\}^k$.

Cette première représentation n'est pas arbitraire. Elle nous permet d'avoir des informations sur le poids, la somme modulaire et les positions des retenues. Puis, en choisissant $t \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)$ et en lui associent

$$\mathcal{C}_t = \{c \in \mathcal{C} : \exists (a,b) \in c,\ a+b = t\}$$

nous avons prouvé l'existence d'une famille de fonctions $\phi_i, \psi_i, \mathcal{C}_t \to \mathcal{C}_t$. $0 \leq i \leq k-1$ qui permettent de couvrir toutes les classes de $\mathcal{C}_t$ en jouant sur la variation du poids. Dans la suite, nous avons cherché à exploiter cette famille d'applications et l'existence d'une classe de poids maximal τ. Ainsi, en partant de la classe maximale τ et en appliquant une suite de compositions finie on retrouve forcément une classe de $\mathcal{C}_t$ (réciproquement $\circ_{j=1}^{N} f_{i_j}(c) = \tau$ avec $f_{i_j} = \phi_j^{-1}$ ou $f_{i_j} = \psi_{i_j}^{-1}$). Cette propriété nous a permis de réaliser l'importance des positions à 1 dans la représentation binaire de t pour les classes $c \in \mathcal{C}_t$ et l'existence de quatre types de blocs B. Ceci nous a conduit à une deuxième représentation des classes d'équivalence sous forme de w-uplets $(x_0, \ldots, x_{w-1}) \in E_t$ ($E_t = \{(x_0, \ldots, x_{w-1}) \in \mathcal{E}$ tel que si $x_j = -1$ alors $x_{j+1} \neq L_{j+1}\}$.), avec $w = w_H(t)$. Cette nouvelle représentation tient compte des positions des 1 dans la représentation binaire de t, de la nature des blocs et de leurs longueurs. $k \geq 2$, $t \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)$

$$c = (c_0, \ldots, c_{k-1}) \in \mathcal{C}_t \approx (B_0 || \ldots || B_{w-1}) \approx (x_0, \ldots, x_{w-1}) \in E_t$$

Revenons maintenant sur les deux résultats qui nous semblent particulièrement intéressants. Le premier résultat est une formule pour calculer le cardinal de l'ensemble $S_t(i)$ qui se présente comme suit :

$$|S_t(i)| = \sum_{(x_0,\ldots,x_{w-1})\in E_t \text{ et } \sum_{i=0}^{w-1} x_i = i} 2^i \prod_{x_i=-1} 4 - 2\delta_{k-w}(i)$$

Comme deuxième résultat nous avons établi que : $P_t = P_{m(t)}$. Enfin, pour conclure nous en déduisons que la famille d'entiers construits par une concaténation de deux entiers vérifiant $m(t) = -t$ satisfait la conjecture de Tu et Deng.

Conclusion

Conclusion

Cette étude à mis en avant les liens existant entre les mondes quaternaire et binaire. Plus particulièrement, la relation entre les fonctions quaternaires courbes et des sous classes de fonctions booléennes. Notre approche avait pour but de transposer la problématique de la conception de fonctions booléennes avec de bons critères cryptographiques en une problématique quaternaire, ouvrant ainsi de nouvelles perspectives de résolution aux problèmes binaires. Nos premier résultats sur le lien quaternaire-binaire peuvent être schématisés de la façon suivante :

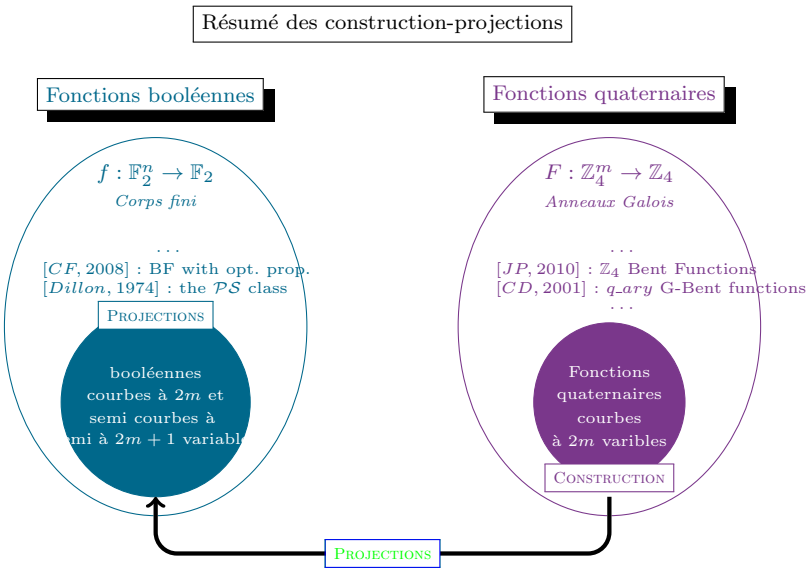

FIGURE 7.1 – Constructions-projections

Cette approche originale a permis d'établir le lien entre une construction de fonctions quaternaires courbes et deux classes de fonctions booléennes projetées : la première classes est composée de fonctions booléennes courbes à $2m$ variables, et la deuxième classe de fonctions booléennes de non-linéarité

maximale à $2m+1$ variables.
Construction quaternaire : nous avons réussi à modéliser les contraintes générées par le partitionnement de R^* sous forme de classes cyclotomiques en exhibant 6 modèles génériques qui permettent de caractériser toutes les fonctions quaternaires courbes qu'il nous est possible de générer pour un choix particulier d'un b-polynôme et de fonctions bilinéaires symétriques et non-dégénérées sur $\mathcal{T}$.

Fonctions h_k				
n^o	a_0	a_1	a_2	a_3
1	0	1	3	2
2	0	1	2	3
3	0	2	1	3
4	0	2	3	1
5	0	3	1	2
6	0	3	2	1

TABLE 7.1 – Modèles génériques

Projections binaires : en utilisant une projection binaire. différente de l'usuelle fonction de GRAY, et l'écriture 2-adique des éléments, puis en exploitant le relèvement de Hensel nous obtenons deux nouvelles familles de fonctions booléennes. Une première famille de fonctions booléennes courbes à $2m$-variables et une seconde famille de fonctions booléennes à $(2m+1)$-variables de non-linéarité maximale.

Conjecture de Tu et Deng : comme deuxième volet de cette thèse nous nous sommes intéressés à la conjecture de *Tu et Deng*.

Conjecture 1 (Tu-Deng [TD11]). *Soit $k \geq 2$ un entier, $t \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)^*$ et posons :*

$$S_{t,k} = \{(a,b) \in \left(\mathbb{Z}/(2^k-1)\mathbb{Z}\right)^2, \text{ tel que } \underbrace{a+b=t}_{équation(1)} \text{ et } \underbrace{w_H(a)+w_H(b) \leq k-1}_{équation(2)}\},$$

La problématique de départ de ce travail est de pouvoir énumérer tous les éléments de $S_{t,k}$ de façon efficace. On essaie pour cela de passer d'un couple de $S_{t,k}$ à l'autre de façon assez simple.
Nous commençons donc par regrouper les couples en classes d'équivalence. La

relation d'équivalence qu'on a choisie nous permet d'avoir des informations sur le poids, la somme modulaire et les positions des retenues. Ensuite nous définissons une famille de fonctions ϕ_i et ψ_i pour tout $0 \leq i \leq k-1$ qui permettent de retrouver toutes solutions de l'équation (1) de la conjecture en jouant sur la variation du poids. Le problème qu'on a rencontré par la suite est le suivant : comment peut-on exploiter ces informations pour parcourir une seule fois les solutions d'un t donné et ainsi calculer le cardinal de $S_{t,k}$? En remarquant l'existence d'une classe de poids maximal et l'importance des positions à 1 dans la représentation binaire d'un entier t, nous définissons un partitionnement en blocs sur les classes afin de pouvoir déterminer les positions sur lesquelles on applique nos transformations ϕ_i et ψ_i. Ceci nous amène à une deuxième représentation des classes d'équivalence en forme de w blocs :

$$c = (c_0, \ldots, c_{k-1}) \in \mathcal{C}_t \approx (B_0 || \ldots || B_{w-1}).$$

Dans la suite, nous cherchons à exploiter ces transformations et le partitionnement en w-blocs, et à intégrer la deuxième condition de la conjecture sur le poids de Hamming (équation (2)). Ceci nous amène a une représentation en w-uplets des classes d'équivalence

$$c = (c_0, \ldots, c_{k-1}) \in \mathcal{C}_t \approx (x_0, \ldots, x_{w-1}) \in E_t$$

Ceci nous conduit par la suite à une formule de calcul plus simple de $|S_{t,k}|$. Puis à l'aide des outils développés dans cette étude nous démontrons que $|S_{t,k}| = |S_{m(t),k}|$. Enfin nous concluons en donnant une nouvelle famille d'entiers t qui vérifient la conjecture.

Bien que nous ne donnions pas une preuve complète de la validité de cette conjecture, nous obtenons deux résultats généraux intéressants. Le premier résultat est une formule pour calculer le cardinal de l'ensemble $S_t(i)$ qui se présente comme suit :

$$|S_t(i)| = \sum_{(x_0,\ldots,x_{w-1}) \in E_t \text{ et } \sum_{i=0}^{w-1} x_i = i} 2^i \prod_{x_i=-1} 4 - 2\delta_{k-w}(i)$$

Comme deuxième résultat nous avons établi que : $P_t = P_{m(t)}$. Enfin, pour conclure, ce formalisme et les propriétés vérifiées par cette étude permettent de conclure : la famille de t construits par une concaténation de deux entiers vérifiant $m(t) = -t$ satisfait la conjecture de Tu et Deng. Il s'agit donc d'un pas de plus vers la démonstration de la conjecture. Et surtout, ce nouveau formalisme ouvre probablement la voie à d'autres nouveaux résultats qu'il reste encore à explorer.

Bibliographie

[And95] R. Anderson. *Searching for the optimum correlation attack*, pages 137–143. Springer Berlin Heidelberg, Berlin, Heidelberg, 1995. 36

[BLW06] N. Brandstätter, T. Lange, and A. Winterhof. On the Nonlinearity and Sparsity of Boolean Functions Related to the Discrete Logarithm in Finite Fields of Characteristic Two. In *Coding and Cryptography : International Workshop, WCC 2005, Bergen, Norway, March 14-18, 2005. Revised Selected Papers*, pages 135–143, Berlin, Heidelberg, 2006. Springer Berlin Heidelberg. 44

[BP05] A. Braeken and B. Preneel. On the Algebraic Immunity of Symmetric Boolean Functions. In *Progress in Cryptology - INDOCRYPT 2005, 6th International Conference on Cryptology in India, Bangalore, India, December 10-12, 2005, Proceedings*, pages 35–48, 2005. 43

[BS90] E. Biham and A. Shamir. Differential cryptanalysis of DES-like cryptosystems. In *Advances in Cryptology -CRYPTO '90, 10th Annual International Cryptology Conference, Santa Barbara, California, USA, August 11-15, 1990, Proceedings*, pages 2–21, 1990. 21

[Car02] C. Carlet. *A Larger Class of Cryptographic Boolean Functions via a Study of the Maiorana-McFarland Construction*, pages 549–564. Springer Berlin Heidelberg, Berlin, Heidelberg, 2002. 40

[Car09a] C. Carlet. *Private communication*, 2009. 50, 52, 53

[Car09b] C. Carlet. On a weakness of the Tu-Deng function and its repair. *IACR Cryptology ePrint Archive*, 2009 :606, 2009. 58

[Car10a] C. Carlet. Boolean functions for cryptography and error correcting codes. *Boolean models and methods in mathematics, computer science, and engineering*, 2 :257, 2010. 9

[Car10b] C. Carlet. Boolean functions for cryptography and error correcting codes. *Boolean Models and Methods in Mathematics Engineering, Computer Science*, 2010. 35, 37, 38

[Car11] C. Carlet. Comments on Constructions of Cryptographically Significant Boolean Functions Using Primitive Polynomials. *IEEE Transactions on Information Theory*, 57(7) :4852–4853, 2011. 44

[CD01] C. Carlet and S. Dubuc. *Finite Fields and Applications : Proceedings of The Fifth International Conference on Finite Fields and Applications Fq 5, held at the University of Augsburg, Germany, August 2–6, 1999*, chapter On Generalized Bent and q-ary Perfect Nonlinear Functions, pages 81–94. Springer Berlin Heidelberg, Berlin, Heidelberg, 2001. 19, 20, 21, 22, 24, 25, 29, 33

[CDGM06] C. Carlet, D.K. Dalai, K.C. Gupta, and S. Maitra. Algebraic Immunity for Cryptographically Significant Boolean Functions : Analysis and Construction. *IEEE Transactions on Information Theory*, 52(7) :3105–3121, 2006. 43

[CF08] C. Carlet and K. Feng. An Infinite Class of Balanced Functions with Optimal Algebraic Immunity, Good Immunity to Fast Algebraic Attacks and Good Nonlinearity. In *Advances in Cryptology - ASIACRYPT 2008, 14th International Conference on the Theory and Application of Cryptology and Information Security, Melbourne, Australia, December 7-11, 2008. Proceedings*, pages 425–440, 2008. 36, 44

[CF11] G.D. Cohen and J.P. Flori. On a generalized combinatorial conjecture involving addition mod $2^k - 1$. *IACR Cryptology ePrint Archive*, 2011 :400, 2011. 50, 51, 52

[CHZ15] K. Cheng, S. Hong, and Y. Zhong. A note on the Tu-Deng conjecture. *Journal of Systems Science and Complexity*, 28(3) :702–724, 2015. 52

[CK89] H. Chung and P. V. Kumar. A new general construction for generalized Bent functions. *IEEE Transactions on Information Theory*, 35(1) :206–209, Jan 1989. 21, 32

[CL11] Y. Chen and P. Lu. Two classes of symmetric Boolean functions with Optimum Algebraic Immunity : Construction and analysis. *IEEE Transactions on Information Theory*, 57(4) :2522–2538, April 2011. 43

[CLS09] T.W. Cusick, Y. Li, and P. Stanica. On a conjecture for balanced symmetric Boolean functions. *J. Mathematical Cryptology*, 3(4) :273–290, 2009. 50, 52, 53

[CM03a] N. Courtois and W. Meier. Algebraic Attacks on Stream Ciphers with Linear Feedback. In *Advances in Cryptology - EUROCRYPT 2003, International Conference on the Theory and Applications of Cryptographic Techniques, Warsaw, Poland, May 4-8, 2003, Proceedings*, pages 345–359, 2003. 35, 43

[CM03b] N.T. Courtois and W. Meier. *Algebraic Attacks on Stream Ciphers with Linear Feedback*, pages 345–359. Springer Berlin Heidelberg, Berlin, Heidelberg, 2003. 42

[CZLH09] C. Carlet, X. Zeng, C. Li, and L. Hu. Further properties of several classes of Boolean functions with optimum algebraic immunity. *Designs, Codes and Cryptography*, 52(3) :303–338, 2009. 43

[DGM] 42

[Dil74] J.F. Dillon. *Elementary Hadamard Difference Sets*. University of Maryland, 1974. 44

[DMS06] D.K. Dalai, S. Maitra, and S. Sarkar. Basic Theory in Construction of Boolean Functions with Maximum Possible Annihilator Immunity. *Designs, Codes and Cryptography*, 40(1) :41–58, 2006. 43

[Dob95] H. Dobbertin. *Fast Software Encryption : Second International Workshop Leuven, Belgium, December 14–16, 1994 Proceedings*, chapter Construction of Bent functions and balanced Boolean functions with high nonlinearity, pages 61–74. Springer Berlin Heidelberg, Berlin, Heidelberg, 1995. 47

[DXS91] C. Ding, G. Xiao, and W. Shan, editors. *The stability of linear complexity of sequences*. Springer Berlin Heidelberg, Berlin, Heidelberg, 1991. 35, 38

[FA03] JC. Faugère and G. Ars. An Algebraic Cryptanalysis of Nonlinear Filter Generators using Gröbner bases. Research Report RR-4739, INRIA, 2003. 42

[Fen09] T. Feng. A new construction of perfect nonlinear functions using galois rings. *Journal of Combinatorial Designs*, 17(3) :229–239, 2009. 21

[FLY09] K. Feng, Q. Liao, and J. Yang. Maximal values of generalized algebraic immunity. *Designs, Codes and Cryptography*, 50(2) :243–252, 2009. 36, 44

[FR12] J.P. Flori and H. Randriam. On the Number of Carries Occuring in an Addition mod 2^k-1. *Integers*, 12 :601–647, 2012. 50, 52, 53, 100

[FRCM10] J.P. Flori, H. Randriam, G.D. Cohen, and S. Mesnager. On a Conjecture about Binary Strings Distribution. In *Sequences and Their Applications - SETA 2010 - 6th International Conference, Paris, France, September 13-17, 2010. Proceedings*, pages 346–358, 2010. 50, 51, 53, 100

[HKC+94] A.R. Hammons, P.V. Kumar, A.R. Calderbank, N.J.A. Sloane, and P. Sole. The $\mathbb{Z}_4$-linearity of kerdock, preparata, goethals, and related codes. *IEEE Transactions on Information Theory*, 40(2) :301–319, Mar 1994. 9, 26

[Hou98] X.D. Hou. q-ary Bent functions constructed from chain rings. *Finite Fields and Their Applications*, 4(1) :55 – 61, 1998. 21, 22, 25, 32

[JP10] Z. Jadda and P. Parraud. *$\mathbb{Z}_4$-Nonlinearity of a Constructed Quaternary Cryptographic Functions Class*, pages 270–283. Springer Berlin Heidelberg, Berlin, Heidelberg, 2010. 26, 28, 29, 30

[JPQ13] Z. Jadda, P. Parraud, and S. Qarboua. Quaternary cryptographic Bent functions and their binary projection. *Cryptography and Communications*, 5(1) :49–65, 2013. 10

[KSW85] P.V Kumar, R.A Scholtz, and L.R Welch. Generalized Bent functions and their properties. *Journal of Combinatorial Theory, Series A*, 40(1) :90 – 107, 1985. 9, 18, 19, 20, 21, 32

[Lan93] P. Langevin. *On Generalized Bent Functions*, pages 147–152. Springer Vienna, Vienna, 1993. 20

[LN83] R. Lidl and H. Niederreiter. *Finite Fields*. Encyclopedia of mathematics and its applications. Addison-Wesley Publishing Company, 1983. 14

[Lob05] M. Lobanov. Tight bound between nonlinearity and algebraic immunity. *IACR Cryptology ePrint Archive*, 2005 :441, 2005. 43

[LQ06] N. Li and W.F. Qi. Construction and Analysis of Boolean Functions of $2t+1$ Variables with Maximum Algebraic Immunity. In *Advances in Cryptology - ASIACRYPT 2006, 12th International Conference on the Theory and Application of Cryptology and Information Security, Shanghai, China, December 3-7, 2006, Proceedings*, pages 84–98, 2006. 43

[LQQ+08] N. Li, L. Qu, W.F. Qi, G. Feng, C. Li, and D. Xie. On the Construction of Boolean Functions With Optimal Algebraic Immunity. *IEEE Trans. Information Theory*, 54(3) :1330–1334, 2008. 43

[Mas69] J.L. Massey. Shift-register synthesis and BCH decoding. *IEEE Transactions on Information Theory*, 15(1) :122–127, 1969. 35

[McD74a] B.R. McDonald. *Finite Rings With Identity*. Pure and Applied Mathematics Series. Marcel Dekker Incorporated, 1974. 16

[McD74b] B.R. McDonald. *Finite Rings With Identity*. Pure and Applied Mathematics Series. Marcel Dekker Incorporated, 1974. 22, 24

[McE87] R.J. McEliece. *Finite fields for computer scientists and engineers*. The Kluwer international series in engineering and computer science. Kluwer Academic Publishers, Boston, 1987. Réimpressions : 1995 (second printing), 2003 (Sixth Printing). 14

[MPC04] W. Meier, E. Pasalic, and C. Carlet. Algebraic Attacks and Decomposition of Boolean Functions. In *Advances in Cryptology - EUROCRYPT 2004, International Conference on the Theory and Applications of Cryptographic Techniques, Interlaken, Switzerland, May 2-6, 2004, Proceedings*, pages 474–491, 2004. 42

[MS] W. Meier and O. Staffelbach. Fast correlation attacks on certain stream ciphers. *Journal of Cryptology*, 1(3) :159–176. 37

[MS78] F.J. MacWilliams and N.J.A. Sloane. *The Theory of Error Correcting Codes*. Number vol. 2,ptie. 2 in Mathematical Studies. North-Holland Publishing Company, 1978. 39

[MS89] W. Meier and O. Staffelbach. Fast Correlation Attacks on Certain Stream Ciphers. *J. Cryptology*, 1(3) :159–176, 1989. 35, 38

[Nyb91] K. Nyberg. *Advances in Cryptology — EUROCRYPT '90 : Workshop on the Theory and Application of Cryptographic Techniques Aarhus, Denmark, May 21–24, 1990 Proceedings*, chapter Constructions of Bent functions and difference sets, pages 151–160. Springer Berlin Heidelberg, Berlin, Heidelberg, 1991. 9, 18, 20, 21, 32

[QFLW09] L. Qu, K. Feng, F. Liu, and L. Wang. Constructing symmetric Boolean functions with maximum algebraic immunity. *IEEE Transactions on Information Theory*, 55(5) :2406–2412, 2009. 43

[QJ11] B. Wu X. Zhang Q. Jin, Z. Liu. A general conjecture similar to T-D conjecture and its applications in constructing Boolean functions with optimal algebraic immunity. *IACR Cryptology ePrint Archive*, 2011 :515, 2011. 47, 48, 49, 50

[RH07] S. Rønjom and T. Helleseth. A New Attack on the Filter Generator. *IEEE Transactions on Information Theory*, 53(5) :1752–1758, 2007. 35

[Riz10] P. Rizomiliotis. On the resistance of Boolean functions against algebraic attacks using univariate polynomial representation. *IEEE Transactions on Information Theory*, 56(8) :4014–4024, 2010. 44

[Rot76] O.S Rothaus. On "Bent" functions. *Journal of Combinatorial Theory, Series A*, 20(3) :300–305, 1976. 9, 18, 41

[RS87] R.A. Rueppel and O. Staffelbach. Products of linear recurring sequences with maximum complexity. *IEEE Transactions on Information Theory*, 33(1) :124–131, 1987. 35

[Sch07] K. U. Schmidt. Quaternary Constant-Amplitude Codes for Multicode CDMA. pages 2781–2785, June 2007. 10, 26

[Sie84] T Siegenthaler. Correlation-immunity of nonlinear combining functions for cryptographic applications (Corresp.). *Information Theory, IEEE Transactions on*, 30(5) :776–780, 1984. 37, 40

[ST09] P. Solé and N. Tokareva. Connections between Quaternary and Binary Bent functions. *IACR Cryptology ePrint Archive*, 2009 :544, 2009. 10, 26, 30, 31, 32, 33

[TCT13] D. Tang, C. Carlet, and X. Tang. Highly nonlinear Boolean functions with optimal algebraic immunity and good behavior against fast algebraic attacks. *IEEE Transactions on Information Theory*, 59(1) :653–664, Jan 2013. 47, 49, 50, 51

[TD10a] Z. Tu and Y. Deng. Boolean functions with all main cryptographic properties. *IACR Cryptology ePrint Archive*, 2010 :518, 2010. 46, 47, 49

[TD10b] Z. Tu and Y. Deng. A class of 1-resilient function with high nonlinearity and algebraic immunity. *IACR Cryptology ePrint Archive*, 2010 :179, 2010. 46, 47, 49

[TD11] Z. Tu and Y. Deng. A conjecture about binary strings and its applications on constructing Boolean functions with optimal algebraic immunity. *Designs, Codes and Cryptography*, 60(1) :1–14, 2011. 44, 45, 47, 49, 52, 83, 84, 105

[TTZH10] X. Tang, D. Tang, X. Zeng, and L. Hu. Balanced Boolean Functions with (Almost) Optimal Algebraic Immunity and Very High Nonlinearity. *IACR Cryptology ePrint Archive*, 2010 :443, 2010. 47

[WPKX10] Q. Wang, J. Peng, H. Kan, and X. Xue. Constructions of cryptographically significant Boolean functions using primitive polynomials. *IEEE Transactions on Information Theory*, 56(6) :3048–3053, 2010. 44

[XM88] G. Z. Xiao and J. L. Massey. A spectral characterization of correlation-immune combining functions. *IEEE Transactions on Information Theory*, 34(3) :569–571, May 1988. 37, 40

[Yam90] M Yamada. Distance-regular digraphs of girth 4 over an extension ring of $\mathbb{Z}/4\mathbb{Z}$. *Graphs and Combinatorics*, 6(4) :381–394, 1990. 17, 21

[ZCSH11] X. Zeng, C. Carlet, J. Shan, and L. Hu. More Balanced Boolean Functions With Optimal Algebraic Immunity and Good Nonlinearity and Resistance to Fast Algebraic Attacks. *IEEE Transactions on Information Theory*, 57(9) :6310–6320, 2011. 44

ROYAUME DU MAROC
Université Mohammed V - RABAT -
جامعة محمد الخامس – الرباط –
Faculté des sciences
كلية العلوم

Université de Bretagne Occidentale

Résumé

Cette thèse porte sur la conception et d'analyse d'objet mathématique utile en cryptographie, plus précisément, sur la conception de fonctions vérifiant un certain nombre de critères pour être utilisées dans un contexte de chiffrement symétrique. De toute évidence, les propriétés de ces fonctions sont essentielles pour les exigences de sécurité du système final qui les utilise. Et suite, à l'évolution permanente du domaine de la cryptanalyse et l'apparition de nouvelles attaques, la conception de fonctions cryptographiques reste en constante évolution. Naturellement, ceci implique de nouvelles restrictions sur les classes de fonctions adoptées et rend parfois obsolètes les familles de fonctions connues. Par ailleurs, ces critères présentent des incompatibilités, et des compromis doivent être considérés. Dans la première partie de cette thèse, nous donnons une description du contexte d'utilisation des fonctions booléennes dans le chiffrement à flot et définissons les propriétés cryptographiques retenues pour cette recherche, ainsi que les attaques correspondantes. En suite, nous nous intéressons aux fonctions booléennes courbes, aux fonctions quaternaires courbes, aux fonctions courbes généralisées, et exhibons les connexions entre les mondes quaternaire et binaire. Ceci nous permet de construire des fonctions booléennes courbes par projections de fonctions quaternaires particulières. Dans cette thèse nous construisons des classes infinies de fonctions booléennes répondent à la plupart des critères requis pour le chiffrement à flot, et étudions une conjecture combinatoire (Tu et Deng) dont la validité conditionne l'immunité algébrique des classes infinies de fonctions étudiées dans ce manuscrit.

Mots-clefs (5) : Fonctions Booléennes, Fonctions quaternaires, Propriétés cryptographiques, Conjecture de Tu / Deng, Anneau de Galois.

Abstract

The core of this thesis is the study of some mathematical objects or problems of interest in cryptology. The linear complexity of sequences is one of the important security measures for stream cipher systems. Recently, in the study of vectorized stream cipher systems, Bent functions have been generalized to the alphabet $\mathrm{Z}_q = Z/qZ$ *. This generalization maps the classical definition of binary bent functions to generalized bent functions. In the first part we present a state of the art around boolean functions, generalized functions, and associated combinational conjectures. The second part is devoted to our scientific contributions. We begin with a new construction of a family of m-variables quaternary Bent functions over Galois ring. Using a particular binary projection map we obtain a family of 2m-variables Boolean bent functions and a family of (2m+1)-variables Boolean functions with maximal non-linearity. To design robust symmetric encryption schemes, we need to use Boolean functions with suitable properties. Among the security criteria these functions need to fulfill, we can mention algebraic immunity. A lot of papers study how to construct suitable functions, but some of them assume the validity of Tu and Deng's combinatorial conjecture to estimate the algebraic immunity of the Boolean functions they design. The last chapter of this part is devoted to the study of a combinatorial conjecture whose validity entails the existence of infinite classes of Boolean functions with good cryptographic properties. Although the conjecture seems quite innocuous, its validity remains an open question. We prove two new results about this conjecture and point out a new family of integers that satisfy it. However, we sincerely hope that the theoretical and experimental results presented here will give the reader a good insight into the conjecture.*

Key Words (5): Quaternary functions , Boolean functions, *security criteria*, Galois ring, combinatorial conjecture,