Université du Sud Toulon-Var

Thèse de Doctorat

Mathématiques

Non Linéarité Parfaite Généralisée au Sens des Actions de Groupe, Contribution aux Fondements de la Solidité Cryptographique

---

par

Laurent Poinsot

Soutenue publiquement le lundi 12 septembre 2005

Devant le jury composé de :

Mme	Anne Canteaut	Chargée de Recherche INRIA, INRIA Rocquencourt	Présidente
MM.	Jean-Michel Combes	Professeur des Universités, Université du Sud Toulon-Var	Examinateur
	James A. Davis	Richardson Professor of Mathematics, University of Richmond	Rapporteur
	Sami Harari	Professeur des Universités, Université du Sud Toulon-Var	Directeur
	Jean-François Maurras	Professeur des Universités, Université de la Méditerranée	Rapporteur
	François Rodier	Directeur de Recherche CNRS, CNRS - Institut de Mathématiques de Luminy	Rapporteur

Remerciements

La route vers le but fixé est longue
et périlleuse, souvent bordée de
tavernes aux enseignes lumineuses.
Et c'est dur de résister à
l'invitation, de rester posé sur le
rail comme un wagon.

IAM, *La Saga*

Le mot « thèse » possède plusieurs significations et autres connotations selon le contexte dans lequel on l'emploie.

Grammaticalement, « thèse » est un nom féminin de cinq lettres.

Etymologiquement « thèse », du grec ou du latin « thesis », signifie « action de poser, affirmation, proposition ».

En programmation, « thèse » est un objet de type `chaîne de caractères`.

Philosophiquement, la thèse est une idée qui forme le premier terme d'une antinomie ou d'une contradiction de type dialectique.

Au sein de l'enseignement supérieur, une thèse est un ensemble de travaux présentés, sous forme d'ouvrage, en vue de l'obtention du grade de docteur.

Le guide galactique vous apprendrait qu'il existe une célèbre thèse selon laquelle la véritable question correspondant à « 42 » qui est la réponse à la Question fondamentale de la Vie, de l'Univers et du Reste serait : « Combien font six multiplié par neuf ? ».

Sur le Disque Monde, les manuscrits de thèse de doctorat en Métaphysique Condensée sont entreposés et enchaînés dans les niveaux inférieurs de la bibliothèque de l'Université de l'Invisible, derrière des portes verrouillées, et précieusement gardés par un orang-outang.

Pour beaucoup d'étudiants, une thèse est un moyen de repousser d'au moins trois ans l'entrée dans la fameuse vie active (via, parfois, une étape transitoire communément appelée « chômage ») et de bénéficier des nombreuses réductions dues à la carte d'étudiant.

Enfin en ce qui me concerne, la thèse représente tout simplement trois années de plaisir et d'enthousiasme - et, très honnêtement, très peu de moment de doute - au cours desquelles j'ai pu apprécier le travail extrêmement enrichissant (certes plus intellectuellement que financièrement)

de recherche scientifique et d'enseignement.

Les mots (voir les phrases !) que vous lisez maintenant, bien que situés en préambule du manuscrit et du travail de thèse proprement dit, ont été écrits en dernier lieu. En somme (ou en produit, tout dépendant de la représentation utilisée), ils constituent la dernière brique du modeste édifice que représente cette thèse, l'ultime coup de pinceau de l'artiste, la trente-sixième chambre des moines de Shaolin. C'est donc à ce moment-là qu'il convient de penser aux nombreuses personnes qui ont, de près ou de loin (voir de très loin, en distance plus qu'en intensité), contribué à l'aboutissement de mon projet de thèse.

En tout premier lieu, cela va de soi, ma reconnaissance et mon estime vont à mon directeur, le Professeur Sami Harari, de l'Université du Sud Toulon-Var, pour m'avoir accordé sa confiance, guidé (le terme ici n'est nullement galvaudé), supporté et constamment encouragé pendant ces trois années de thèse. Il m'a initié aux différents aspects de la cryptographie et a su orienter mes recherches. Avec lui, l'entropie inhérente à l'aboutissement du travail de thèse a été très largement réduite. Si, comme le soutient la fameuse loi populaire de l'économie, le temps, c'est de l'argent, vu le temps qu'il a « dépensé » en ma compagnie afin que je puisse mener à bien mes travaux et les longues discussions que nous avons eues, et bien, j'en ai peur, Monsieur Harari aujourd'hui serait ruiné[1] ! J'espère avoir répondu, au moins en partie, aux attentes qu'il avait initialement placées en moi.

Je tiens à exprimer ma profonde gratitude à James Davis, Professeur de Mathématiques de l'Université de Richmond (Etats-Unis d'Amérique), d'avoir accepté d'être l'un des rapporteurs de cette thèse. A ce jour, je reste encore stupéfait de la vitesse à laquelle il a lu et interprété le manuscrit pourtant écrit en langue française (à ϵ près ... tant j'ai fait du mieux que je pouvais pour rédiger dans un semblant de français correct !) ainsi que pour les remarques, toujours claires, précises et constructives, qu'il m'a transmises. Je le remercie au moins autant pour l'enthousiasme qu'il a manifesté au sujet de mes travaux ainsi que pour l'aide, les idées et les nombreuses constructions de G-ensembles à différences qu'il m'a permis d'utiliser dans ce manuscrit. Sans lui, il faut bien l'avouer, cette thèse ne proposerait que peu de constructions concrètes.

Dear Jim, that was a great pleasure to work with you.

Je remercie très vivement Jean-François Maurras, Professeur d'Informatique de l'Université de la Méditerranée, d'avoir aussi accepté d'être rapporteur. Il a su mettre en exergue les idées essentielles de mon travail en y portant le regard original, à la fois très enrichissant et profondément consciencieux, du chercheur en Informatique Fondamentale.

Un très grand merci à mon troisième rapporteur, Monsieur le Directeur de Recherche CNRS François Rodier, de l'Institut de Mathématiques de Luminy. Je lui suis reconnaissant de m'avoir invité au séminaire de l'équipe ATI afin que j'y présente mes travaux ainsi que pour les nombreuses remarques précises, circonstanciées et très constructives qu'il m'a alors adressées que ce soit aussi bien sur la forme - le manuscrit - que sur le fond. Je tiens par ailleurs à le remercier pour la très grande qualité pédagogique de ses enseignements de DEA que j'ai suivis.

Merci donc à mes deux rapporteurs Marseillais et Allez l'OM !

Je tiens à exprimer ma profonde reconnaissance à Jean-Michel Combes, Professeur de Mathématiques à l'Université du Sud Toulon-Var, d'avoir accepté d'être membre de mon jury de thèse.

[1] Et encore, je ne compte pas tous les cafés que je lui dois !

Sa participation à cette soutenance est un immense honneur pour moi tant je reste admiratif devant le grand chercheur qu'il est et, malgré sa renommée internationale, la modestie dont il fait preuve. J'en profite pour remercier le corps enseignant de l'Université du Sud Toulon-Var et de l'ISITV d'avoir, dans un premier temps, très largement contribué à ma formation scientifique et, dans un second temps, pour m'avoir chaleureusement accueilli le jour où était venu, à mon tour, le temps d'enseigner.

Je voudrais faire part de mon estime envers Madame Anne Canteaut, Chargée de Recherche en Informatique à l'INRIA, qui a accepté de participer au jury ainsi que pour les idées et les nombreux conseils qu'elle m'a prodigués lors de nos rencontres, plus souvent à l'étranger (en Inde et en Norvège) qu'en France. Je la remercie pour avoir suivi avec une grande attention l'évolution de mes travaux. Je salue au passage les membres du projet CODES que j'ai pu rencontrer.

Je ne sais comment remercier Claude Carlet, Professeur de Mathématiques à l'Université Paris VIII, tant ses travaux sur les fonctions courbes et parfaitement non linéaires, dans le cadre des groupes finis abéliens, ont très largement influencé les miens. Je regrette seulement qu'il n'ait pu assister à ma soutenance (à quand la téléportation de l'Australie vers la France ?).

Je remercie très sincèrement Pierre Liardet, Professeur de Mathématiques à l'Université de Provence ainsi que Lucas Vienne, Professeur de Mathématiques à l'Université d'Angers, pour leur patience, leur réactivité et pour les réponses aux questions non triviales sur les groupes finis soumises via l'Internet.

Merci à Omessaâd Hamdi, Cyril Prissette et Christian Tavernier pour avoir régulièrement assisté à mes exposés de recherche, parfois, sinon toujours, très éloignés de la cryptographie conventionnelle.

Que dire du bureau 166 (bis), le bureau caché des doctorants ? Avec Laurent Giulieri & Audrey (toutes mes félicitations !) et El Mostafa Fadaili (faut pas s'endormir, mon pote !), nous y avons passé des moments de rire (très souvent), de réflexion « philosophico-politique » sur la société (surtout le vendredi après-midi) et très rarement de frustration (seulement l'été en l'absence de clim !). J'en profite pour remercier les membres de l'aile « télécoms » de l'ISITV pour leur accueil et leur gentillesse.

Merci à Déborah, Karine, Solange, Sylvie et François - moniteurs CIES - pour *la thèse du petit Nicolas*. Un grand salut aussi à mon ami El-Hadi Khoumeri (Ulac smah ulac !).

Je remercie les dirigeants de la société Clearsy d'avoir accepté que j'effectue mon DEA conjointement à mes fonctions d'ingénieur et organisé mon temps et ma charge de travail en conséquence. En plus de l'expérience dont j'ai bénéficié, j'ai pris conscience d'une chose essentielle : manifestement, je suis davantage fait pour la Recherche théorique que pour la programmation ! Un petit clin d'œil au passage aux ex-grouillots avec qui j'ai effectué des parties endiablées de tennis de table et partagé de sympathiques soirées « jeudailles » à Aix-en-Provence : Anne-Lise, Marie, Hélène, Béa, François & Fanny, Pierrot & sa Nine, Pije et Jean-Pierre Jean.

Merci à Thierry Bec de m'avoir mis en relation avec Monsieur Harari. Je dois bien avouer que très probablement sans cela, je n'aurais jamais fait de thèse. Cela m'a en outre permis, dans une certaine mesure, de progresser en maths pures mais je ne m'appelle pas Thierry ! Puisque j'y suis, je salue ma garde rapprochée : Manu (Manolo : « Zizou ! Zizou ! »), David (comment qu'c'est ?)

& Carole, cela va de soi. Un petit coucou aussi à Sam & Emilie et Rico.

Je me dois de rendre hommage aux « ENAC All Stars » : Fabrizio (non, Fabrice, ce n'est pas l'orage que tu entends, c'est un moteur d'avion !), Séb l'ex-raptor (Séb, c'est du tout cuit !), Edu (l'indépendantiste Catalan qui vit partout sauf en Catalogne !), Pascalou (à quand la vie à la ferme ?), Alex (l'électron libre du FLNC canal ENAC) et mon binôme, qui m'a appris tout ce que je sais de l'Informatique, l'Hombre Jorge (¿ qué tal, Hombre ?) ainsi que sa dame, Eli (tu as toujours le permis ?). A la santé d'Alec, les gars !

Je remercie aussi ces particules quantiques d'inspiration parcourant le monde platonicien des Idées mathématiques et qui ont, par chance ou plus sûrement par mégarde, alimenté la partie de mon cerveau dédiée à l'intuition scientifique.

En dernier lieu, je souhaite naturellement remercier mes parents (je vous jure, cette fois c'est vrai, Tanguy a terminé ses études !), mes grands-parents, mes deux frères (mon grand frère, Frédéric, en particulier pour avoir relu ma thèse et Mathieu, alias Anthony, ça va, Duc ?), mes tantes et oncles, mes cousines et cousins, tous les membres de ma famille, mes ami(e)s, qui m'ont toujours soutenu et encouragé.

Bref, en un mot comme en mille six cent soixante-douze, MERCI !

Table des matières

Chapitre 1

Introduction

Un jour, une tortue va apprendre à voler.

TERRY PRATCHETT, *Les petits dieux*

Les techniques de chiffrement à clef secrète sont très exploitées afin d'assurer la confidentialité de certaines transactions. Leur succès en fait fatalement une cible de choix pour les cryptanalystes. Diverses attaques ont ainsi été développées contre ce type particulier d'algorithmes. Deux parmi les plus efficaces et célèbres sont les cryptanalyses *différentielle* [BS91] et *linéaire* [Mat94]. Les notions de *non linéarité parfaite* et de *fonction courbe* sont très pertinentes en cryptographie puisqu'elles ont pour dénominateur commun la formalisation des résistances optimales des systèmes de chiffrement à clef secrète face à ces deux fameuses attaques. Historiquement ces concepts, introduits par Dillon [Dil74] et Rothaus [Rot76], ont été exposés dans le cadre booléen c'est-à-dire pour des fonctions définies sur $\mathbb{F}_2^m$ et à valeurs dans $\mathbb{F}_2 = \{0, 1\}$.

Une fonction f est *parfaitement non linéaire* si pour tout vecteur non nul α de $\mathbb{F}_2^m$ et tout β de $\mathbb{F}_2$,

$$|\{x \in \mathbb{F}_2^m | f(x \oplus \alpha) \oplus f(x) = \beta\}| = 2^{m-1} \tag{1.1}$$

où le symbole « $\oplus$ » désigne à la fois l'addition modulo deux de $\mathbb{F}_2$ et celle composante par composante de $\mathbb{F}_2^m$.

Pour $f : \mathbb{F}_2^m \to \mathbb{F}_2$, appelons *signe* de f la fonction à valeurs réelles qui fait correspondre $(-1)^{f(x)}$ à un élément x de $\mathbb{F}_2^m$. Les fonctions *courbes* sont alors ces fonctions à un nombre pair de variables dont la valeur absolue de la transformée de Fourier (discrète) de leur signe est constante, égale à $2^{\frac{m}{2}}$.

Un résultat classique [Dil74] énonce l'équivalence entre ces deux notions, duales l'une de l'autre par la transformée de Fourier. Une propriété similaire a par ailleurs été développée dans le cadre des groupes finis commutatifs [CD04].

Plaçons-nous donc dans ce cadre abstrait. Soient alors G et H deux groupes finis commutatifs, tous deux notés additivement. Soit alors σ_α la translation $x \mapsto x + \alpha$ sur G. On peut ré-écrire la formule (1.1) comme suit :

$$|\{x \in G | f(\sigma_\alpha(x)) - f(x) = \beta\}| = \frac{|G|}{|H|}$$

où α est un élément de G, différent de l'élément neutre et $\beta \in H$.

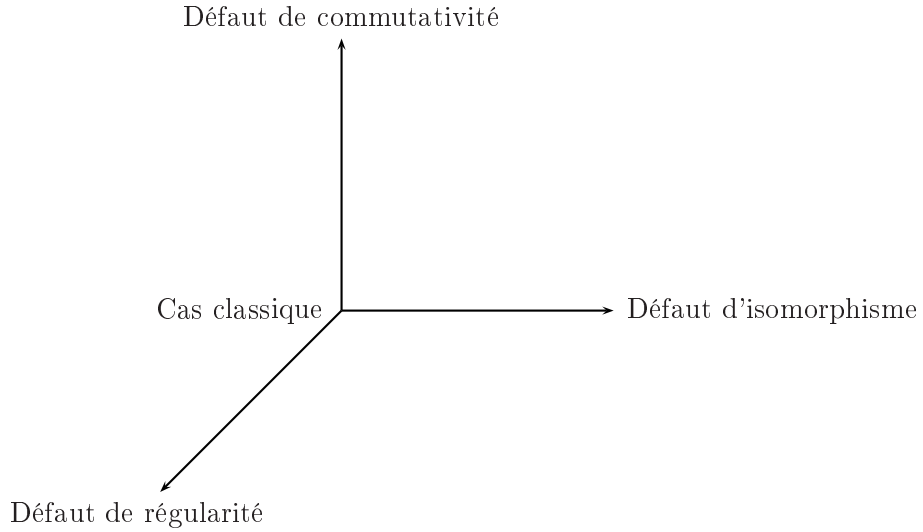
Manifestement la notion de non linéarité parfaite illustre le comportement d'une fonction soumise à des translations sur ses variables. L'action par addition ou translation d'un groupe sur lui-même est un cas particulier d'action de groupe *i.e.* un homomorphisme d'un groupe G dans le groupe symétrique $S(X)$ d'un ensemble non vide X. L'objectif de cette thèse consiste donc à ré-interpréter ce concept cryptographique en remplaçant les translations par une action de groupe abstrait [PH04, PH05]. Les travaux que nous présentons s'articulent donc principalement autour des thèmes de fonctions parfaitement non linéaire et courbe et de leur généralisation au sens des actions de groupe fini.

Lorsque G est un groupe fini agissant sur un ensemble non vide X et H est un groupe fini commutatif (noté additivement), une fonction $f : X \to H$ sera dite *G-parfaitement non linéaire* si pour tout élément $\mathbf{g}$ de G, différent de l'élément neutre, et tout $\beta \in H$,

$$|\{x \in X | f(\mathbf{g}.x) - f(x) = \beta\}| = \frac{|X|}{|H|}$$

où le symbole « . » désigne l'action de G sur X. On retrouve donc dans cette dernière formule la définition de la non linéarité parfaite dans laquelle les translations ont été substituées par une action de groupe quelconque.

Cette approche permet de généraliser la notion traditionnelle de non linéarité parfaite suivant trois axes selon que l'action de groupe considérée est régulière ou non, commutative ou non et suivant le type du groupe agissant lui-même (quelle est sa ressemblance avec les translations de X lorsque celui-ci est muni d'une structure de groupe ?). Ces propos sont illustrés par la figure suivante.



Action de groupe fini commutatif

Alors que l'action par translation d'un groupe sur lui-même est une action *régulière* (*i.e.* pour tout élément x de X, l'application qui envoie un élément $\mathbf{g}$ de G sur $\mathbf{g}.x$ est bijective), nous pouvons relaxer cette contrainte, dans le nouveau contexte, en considérant des actions *fidèles* (*i.e.* l'homomorphisme de groupe représentant l'action est injectif). En jouant ainsi sur le « défaut

de régularité » de l'action, nous pouvons espérer construire des fonctions G-parfaitement non linéaires notamment dans le cas où les fonctions parfaitement non linéaires classiques n'existent pas (par exemple pour un nombre impair de variables booléennes).

Par ailleurs, nous souhaitons caractériser la G-non linéarité parfaite en termes de transformée de Fourier, de manière identique au cas traditionnel, ce qui doit nous conduire naturellement à une notion appropriée de fonction courbe.

Cas non abélien

Dès lors qu'est exploitée la notion algébrique d'action de groupe, il est légitime de considérer le cas des groupes finis non abéliens. A première vue, cela n'a pas l'air foncièrement différent, mais à y regarder de plus près, le défaut de commutativité est plus sérieux qu'il n'y paraît. Ainsi nous ne disposons plus ni de la dualité classique des groupes finis commutatifs, ni de la transformée de Fourier, outils féconds dans l'étude des propriétés des fonctions. Il est donc indispensable d'utiliser d'autres notions très rarement envisagées dans le domaine de la cryptographie.

La théorie des représentations linéaires des groupes semble être l'outil idéal à exploiter afin de formuler la G-non linéarité parfaite dans le contexte non abélien via une caractérisation « à la Fourier » conduisant à une formule du type conservation de l'énergie similaire à la notion de fonction courbe. Toutefois, ainsi que nous le constaterons, la perte de commutativité a de sérieuses répercussions sur l'aspect de la formule finalement obtenue. En effet l'utilisation des représentations linéaires nous contraint à considérer des espaces vectoriels, certes de dimension finie, mais de dimension supérieure à 1. Ainsi dans ce cadre non abélien, la définition correspondante de la notion de fonction courbe sera de type matriciel plutôt que scalaire.

G-ensembles à différences

Un (v, k, λ)-*ensemble à différences* D (avec $|D| = k$) dans un groupe G (avec $|G| = v$) est un objet combinatoire défini par le fait que pour tout α de G, distinct du neutre, l'équation $x - y = \alpha$ admet exactement λ solutions dans D^2.

Classiquement, les fonctions courbes ou parfaitement non linéaires, à valeurs dans $\mathbb{F}_2$, sont les indicatrices[1] des ensembles à différences dits de *Hadamard*.

Observons que l'équation $x - y = \alpha$ peut simplement être ré-écrite $x = \alpha + y$. Une nouvelle fois nous voyons apparaître les translations. Il est donc clair que l'on peut naturellement généraliser cette notion via des actions de groupe commutatif ou non, de même que ce que l'on souhaite effectuer concernant la non linéarité parfaite. Nous définissons ainsi les *G-ensembles à différences*. Pour G un groupe fini agissant sur X (avec $|X| = v$), un tel ensemble D (avec $|D| = k$) de X de paramètres (v, k, λ) est défini par le fait que l'équation $x = \mathbf{g}.y$, pour tout $\mathbf{g}$ de G, différent du neutre de G, admet exactement λ solutions dans D^2. On se propose alors d'étudier les liens éventuels entre ces objets et la notion de fonction G-parfaitement non linéaire et notamment d'examiner si de telles fonctions à valeurs dans $\mathbb{F}_2$ sont les indicatrices de ces ensembles comme dans le cas classique. Si tel est le cas, puisque dans ce cadre combinatoire l'utilisation d'une

[1] L'indicatrice d'un ensemble A est la fonction $\mathbf{1}_A$ définie par :

$$\mathbf{1}_A(x) = \begin{cases} 1 & \text{si } x \in A\ , \\ 0 & \text{sinon}\ . \end{cases}$$

action fidèle plutôt que régulière représente explicitement un relâchement des contraintes, cela doit logiquement aboutir à des résultats cryptographiquement significatifs. Nous ambitionnons ainsi de converger vers des constructions explicites de fonctions G-parfaitement non linéaires définies sur $\mathbb{F}_2^m$ et à valeurs dans $\mathbb{F}_2$ dans le cas où les fonctions courbes classiques n'existent pas (l'entier m est impair).

Organisation du manuscrit

Le chapitre 2 est une introduction pédagogique au contexte dans lequel sont développées les notions de base sur lesquelles nos travaux s'appuient, à savoir, la cryptologie.

Ce chapitre introductif mis à part, le manuscrit est divisé en deux parties. Logiquement dans la première est exposée une partie des connaissances concernant les thèmes de la non linéarité parfaite et des fonctions courbes. La seconde partie, quant à elle, est spécifiquement dévolue à la présentation des développements originaux.

Première partie

Ce fragment du manuscrit est lui-même architecturé en quatre chapitres reprenant dans une large mesure le savoir actuel concernant le domaine de la non linéarité parfaite.

- Le chapitre 3 récapitule les notations et autres conventions valables pour le manuscrit dans son intégralité ;
- Dans le chapitre 4 sont, d'une part, recensés les définitions et outils classiques - comme la transformée de Fourier - notablement exploités dans un contexte booléen et, d'autre part, certaines des principales propriétés devant être satisfaites par des fonctions pour leur exploitation cryptographique ;
- Les notions de non linéarité parfaite et fonction courbe, toujours dans un cadre booléen, sont exposées au chapitre 5 ;
- Le chapitre 6, le dernier de cette partie, est entièrement réservé à certaines généralisations connues des concepts précédents dans des cadres non booléens. Il constitue le fondement théorique sur lequel nos travaux reposent en partie, notamment en ce qui concerne la théorie de Carlet et Ding.

Seconde partie

Nos contributions originales basées sur l'utilisation d'actions de groupe sont exposées dans cette seconde partie au sein de deux chapitres.

- Le thème de la non linéarité parfaite généralisée à l'aide d'une action fidèle ou régulière de groupe fini **commutatif** est intégralement développé dans le chapitre 7. On y trouve notamment les caractérisations en termes de transformée de Fourier ainsi que les formulations correspondantes via ces nouveaux objets combinatoires appelés G-ensembles à différences. Plusieurs constructions explicites de fonctions G-parfaitement non linéaires y sont aussi exposées ;
- Enfin au chapitre 8 est abordé le cas **non abélien**. Nous y introduisons la théorie des représentations linéaires et la théorie de Fourier adéquat, jouant un rôle comparable à celui de la dualité classique des groupes finis commutatifs dans ce nouveau contexte. Ces outils sont exploités afin de caractériser l'analogue dans le cadre non abélien de la théorie de la non linéarité de Carlet et Ding que nous développons et généralisons ensuite au sens des actions de groupe fini non commutatif. Pour finir, les G-ensembles à différences sont une

nouvelle fois utilisés afin d'exhiber des constructions de fonctions satisfaisant les critères généralisés.

Convention : Dans ce manuscrit, une référence[2] de chaque théorème et autre proposition est rappelée avant son énoncé hormis lorsqu'il s'agit de nos propres contributions. Après le chapitre 2, la plupart du temps les résultats exposés, orginaux ou non, sont suivis de leur preuve (parfois légèrement modifiée par nos soins lorsqu'il s'agit de la démonstration d'un autre auteur).

Conseils de lecture : Le chapitre 2 très informel n'a que peu d'influence sur la suite du contenu du manuscrit. Il s'agit simplement d'une introduction didactique au domaine de la cryptologie et non à notre travail proprement dit. Il peut donc être éventuellement survolé sans que la compréhension des développements ultérieurs soit compromise. La première partie de ce manuscrit, introduisant par étape les idées sur lesquelles s'appuient nos travaux, correspond à un corpus des principaux concepts connus concernant de près ou de loin la notion de non linéarité parfaite sous divers aspects. Elle ne contient ainsi que peu de nos contributions originales si ce n'est la relecture critique et l'étude croisée de certains concepts. Seule la lecture du chapitre 6 est absolument indispensable et nécessite réellement de s'y attarder. La seconde partie doit bien évidemment être consultée dans son intégralité puisqu'elle contient nos propres contributions à la problématique de la non linéarité parfaite. Bref, une première lecture du manuscrit[3] peut se représenter symboliquement par la suite exacte[4] :

$$0 \to \text{Introduction} \to \text{Chapitre 6} \to \text{Seconde Partie} \to \text{Conclusion et perspectives} \to 0$$

[2] Il ne s'agit pas forcément de *la* référence originale.

[3] Il s'agit d'un itinéraire bis, sous la forme d'un raccourci, s'adressant à un lecteur spécialiste du domaine de la non linéarité parfaite ou souhaitant directement connaître les nouveaux résultats sans s'éterniser sur des notions certes importantes mais non fondamentales.

[4] Dans la catégorie des « fragments de manuscrit ».

Chapitre 2

Préambule : introduction à la cryptologie

Va à Rome porter un message à César. Tu lui diras : « Toute la Gaule est occupée », il te demandera : « Toute ? », tu lui répondras : « Toute ! » il comprendra.

Uderzo & Goscinny, *Astérix*

Sommaire

2.1 Aux origines de la cryptographie

Au XVI^{e} avant notre ère fut gravé dans une tablette d'argile, retrouvée en Irak, le premier document crypté connu. Il avait pour auteur un potier souhaitant conserver secrète une certaine recette artisanale personnelle. Ce témoignage original d'acte de chiffrement fut composé en omettant les consonnes et en travestissant l'orthographe des mots. Ce qui aurait pu ne rester qu'une anecdote marque en réalité la naissance de la *cryptographie* et dévoile son but originel : rendre le contenu d'un message inintelligible pour la plupart des personnes hormis son (ses) auteur(s) ainsi que son (ses) destinataires. Présageant des avantages non négligeables à tirer d'une telle technique, très rapidement, politiciens et autres militaires s'approprièrent ces *procédés pour écrire des choses secrètes* afin de comploter ou de préparer quelques manœuvres martiales. Plusieurs siècles s'écoulèrent avant qu'apparaissent les méthodes de cryptographie proprement dites dont la première fut utilisée par un fameux romain du nom de Caius Julius Caesar. Craignant sans doute une fin « brutale » (il est bien connu que le décès pour cause naturelle était chose rare parmi les empereurs de l'époque - étant entendu qu'un régicide n'entre pas, cela va de soi, dans cette catégorie), cet illustre représentant de la République de Rome codait ses correspondances

les plus confidentielles en changeant le rang des lettres de l'alphabet, plus précisément en remplaçant chaque lettre par celle située trois places plus loin dans l'alphabet[1]. Ainsi à la veille de sa mort, César aurait pu écrire, s'il avait voulu garder la chose secrète et si on lui en avait laissé le temps,

wx txrtxh, ilol

représentant le cryptogramme de *tu quoque, fili*[2]. Au sein du bestiaire des antiques techniques d'écriture chiffrée cette méthode constitue le premier véritable système mathématique de cryptographie, marquant au passage la transition d'un artisanat vers un *art*[3] du secret. Peu ou prou la cryptographie était née. Nous aborderons au cours de la prochaine section la définition formelle de tels cryptosystèmes mais pour l'heure replongeons promptement dans l'Antiquité. Le subtil code de César appartient en fait à une classe plus générale de systèmes de chiffrement. On peut, en effet, légitimement considérer le même procédé dans un contexte élargi dans lequel on remplace la translation de trois lettres dans l'alphabet par une translation de k lettres, k étant un entier pris entre 0 et 25 appelé *clef* du code. Ainsi le code d'un certain message *clair* M est alors obtenu en substituant chaque lettre figurant dans M par son translaté par k dans l'alphabet *i.e.* par la lettre apparaissant k places plus loin. Bien que révolutionnaire pour l'époque, le code de César et ses semblables révélèrent rapidement leur limite en même temps que le revers de la cryptographie ou plutôt son corollaire : la *cryptanalyse* ou art de percer à jour les secrets. En effet ce type de systèmes de chiffrement possède un défaut rédhibitoire, à savoir, le petit nombre de clefs possibles puisque l'on ne peut translater les lettres que de 26 manières distinctes. Il en résulte une faiblesse intrinsèque ainsi qu'un moyen de « casser » le code, c'est-à-dire d'obtenir le message clair à partir du crypté correspondant sans connaître la clef utilisée ; l'essai de plusieurs clefs menant irrémédiablement à la découverte de la bonne. Depuis le monde se divise en deux catégories : ceux qui tentent de converser secrètement et ceux qui cassent. Cette vision manichéenne des choses constitue sans conteste une *course à l'armement cryptographique*. Afin de parer les attaques il est nécessaire de corriger les défauts des cryptosystèmes utilisés et de créer ainsi de nouveaux codes, lesquels seront à leur tour sensibles à de nouvelles attaques, et ainsi de suite. A la limite, il n'existe pas de remède universel en cryptographie mais seulement un long[4] processus itératif s'articulant autour de l'interaction entre de nouvelles parades défensives et des innovations offensives et se nourrissant de la mobilisation mutuelle de ces forces antagonistes. L'association des deux pôles opposés constituant alors le paradigme de la *cryptologie*.

2.2 Cryptologie moderne

2.2.1 Introduction

La cryptologie se partage entre la cryptographie, qui inclut l'étude des mécanismes destinés à assurer la confidentialité, et la cryptanalyse, dont le but est de déjouer les protections ainsi mises en place. Cette dernière constitue en outre un ensemble d'indicateurs de fiabilité des systèmes de chiffrement exploités. La sûreté cryptographique peut être étudiée de deux points de vue complètement différents. Historiquement la première approche, publiée en 1938, est dûe à Shannon [Sha49] et repose sur une mesure probabiliste de la sécurité du système. Cette démarche, succinctement présentée dans la sous-section 2.2.4, a abouti à la définition des cryptosystèmes à clef secrète (ou privée) que l'on développe de façon concise au cours de la sous-section suivante. Aussi on ne s'attardera pas dessus pour le moment. La seconde approche, appelée *sécurité calculatoire*,

[1] Ce qui est équivalent à l'application d'une translation sur chacune des lettres d'une phrase donnée.
[2] Signifie « toi aussi mon fils ». Exclamation de César apercevant son protégé Brutus parmi ses assassins.
[3] Lequel art laissera sa place, au cours du XX^{e} siècle, à une science.
[4] En réalité très long puisqu'il n'a sans doute pas de fin.

repose quant à elle sur une mesure de la quantité de calculs nécessaires pour casser un système et se base sur la théorie de la complexité des problèmes de décision permettant leur classification en termes de niveaux de difficulté. Elle a été introduite par Diffie et Hellman (cf. [DH76]) et a provoqué une scission avec la théorie héritée de Shannon en donnant naissance à la notion de cryptographie à clef publique dont l'article fondateur est [RSA78]. Dans ce cadre théorique, on dit qu'un procédé de chiffrement est un *obstacle combinatoire* si le meilleur algorithme pour le casser nécessite un trop grand nombre d'opérations ou, de manière équivalente, une quantité non raisonnable de temps ou de mémoire *i.e.* que son efficacité calculatoire est négligeable. C'est le cas, par exemple, si le temps de calcul de l'attaque est lié exponentiellement à la dimension de certaines données du système. L'augmentation de la taille des paramètres utilisés laisse alors sa sécurité hors de portée d'une attaque, et ce en dépit de la puissance toujours croissante des moyens informatiques. Dans la pratique ce type de propriété est inféré par *réduction* de la sécurité du cryptosystème à un problème connu pour être difficile. Cependant l'exclusion mutuelle entre problèmes simples et difficiles, parce que largement vérifiée et sans exemple du contraire, est une hypothèse non démontrée que l'on suppose être vraie soit, il faut le souligner, un *postulat*. Ainsi les preuves de sécurité dans le cadre calculatoire ne reposent que sur une présomption, certes hautement raisonnable, mais qui peut, à tout moment, être invalidée et condamner avec elle tout un pan de la cryptographie moderne[5]. Dans la suite nous n'évoquons plus l'approche calculatoire puisque nous évoluerons alors exclusivement dans le monde de la cryptographie à clef secrète.

Cette section est organisée comme suit. Nous introduisons tout d'abord la définition formelle des cryptosystèmes à clef secrète afin de disposer d'outils mathématiques pour étudier leurs propriétés. Puis nous dressons l'inventaire des modèles classiques d'attaques envers les systèmes de chiffrement. Ce classement en familles de cryptanalyses fournit à la fois un vocabulaire universel et aussi un cadre générique pour l'analyse de la fiabilité des algorithmes de cryptage. Parmi les critères de sécurité se rencontre la notion de sûreté inconditionnelle, inventée par Shannon et présentée dans l'avant-dernière sous-section, qui, modulo certaines exigences, garantit l'inviolabilité totale de tout système la vérifiant. Toutefois cette propriété ne se réalise que dans un environnement abstrait trop restrictif et se trouve ainsi être peu pertinente en pratique. Voilà pourquoi dans la dernière sous-section de cette introduction à la *cryptologie moderne* nous nous attachons à la description des instructions informelles pour la réalisation concrète des cryptosytèmes.

2.2.2 Définition des cryptosystèmes à clef secrète

Revenons sur-le-champ aux principes de la cryptographie. Son objectif fondamental est de permettre à deux personnes, traditionnellement appelées Alice et Bob, de communiquer via un canal public non sécurisé de telle sorte que les messages échangés soient incompréhensibles pour une tierce personne malveillante (ou bienveillante ... pour de mauvaises raisons) que l'on prénomme ici Xavier[6]. *A contrario* le but de la cryptanalyse est d'espionner et de décoder les conversations privées. Le canal public sur lequel transitent les informations est un médium parmi les services postaux, les lignes téléphoniques, les ondes hertziennes ou radios, l'atmosphère (pour les signaux de fumée) ou n'importe quel autre réseau de communication. Il est dit *public* car d'une part tout le monde peut y avoir accès et d'autre part il ne dispose d'aucun moyen de sécurisation des échanges entre les personnes. L'information communiquée entre Alice et Bob, constitue ce que l'on appelle un *message clair* (ou simplement un *message*), et peut être un texte dans une langue naturelle, un signal quelconque ou encore des données numériques. Une conversation cryptée s'élabore suivant une trame précise bien connue. Alice transforme, en utilisant un moyen de cryptage, le message

[5] Ce qui serait aussi directement fâcheux pour nos cartes bleues.
[6] Puisque l'on porte plainte contre X.

clair qu'elle entend transmettre à Bob en un *message chiffré* ou *cryptogramme* en utilisant une clef prédéterminée, connue du seul Bob, et le lui communique via le canal. Xavier, qui écoute le réseau de communication et donc intercepte le message crypté, ne peut en principe retrouver le message original, alors que Bob, qui connaît la clef, peut déchiffrer le texte reçu.

La présentation du principe de fonctionnement ainsi faite passons à sa formalisation mathématique (voir [Sti01]) qui nous intéresse au plus haut point.

Définition 2.1. Un *système cryptographique* ou *cryptosystème* correspond à la donnée d'un triplet d'ensembles finis $(\mathcal{M}, \mathcal{C}, \mathcal{K})$ ainsi que de deux familles de fonctions, indicées par l'ensemble $\mathcal{K}$, $\{e_K\}_{K\in\mathcal{K}}$ et $\{d_K\}_{K\in\mathcal{K}}$ où :

1. $\mathcal{M}$ est appelé *ensemble des messages clairs* ;
2. $\mathcal{C}$ est appelé *ensemble des messages chiffrés* ;
3. $\mathcal{K}$ est appelé *ensemble des clefs* ;
4. Pour tout $K \in \mathcal{K}$, $e_K : \mathcal{M} \to \mathcal{C}$ est appelé *règle de chiffrement* de clef K ;
5. Pour tout $K \in \mathcal{K}$, $d_K : \mathcal{C} \to \mathcal{M}$ est appelé *règle de déchiffrement* de clef K ;
6. Pour tout $K \in \mathcal{K}$ on a $d_K \circ e_K = Id_{\mathcal{M}}$ où le symbole « $\circ$ » représente la composition de fonctions et $Id_{\mathcal{M}}$ est la fonction identité de $\mathcal{M}$.

Si on observe attentivement la définition précédente on s'aperçoit que la caractéristique principale est la sixième. Elle spécifie le fait que si un texte clair M est chiffré en utilisant e_K, et si le crypté correspondant C est déchiffré en utilisant la règle d_K, on retrouve le texte clair M original. Dans le processus de chiffrement/déchiffrement il est nécessaire qu'à la fois Alice et Bob connaissent la clef K employée lors de la communication. Cette opération de choix de clef n'est pas décrite au sein du protocole de chiffrement tel que présenté dans ce manuscrit. En pratique Alice et Bob se rencontrent pour sélectionner la clef ou utilisent un canal de communication sécurisé auquel des espions comme Xavier n'ont pas accès.

Exemple 2.1. Le *chiffrement par décalage* (ou *par translation*), basé sur l'arithmétique modulaire, est défini par le cryptosystème suivant : $\mathcal{M} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_{26}$. Pour $K \in \mathbb{Z}_{26}$, on a

$$M \in \mathbb{Z}_{26} \mapsto e_K(M) = M + K \bmod 26 \in \mathbb{Z}_{26}$$

et

$$C \in \mathbb{Z}_{26} \mapsto d_K(C) = C - K \bmod 26 \in \mathbb{Z}_{26} \ .$$

La règle de chiffrement de clef K transforme un nombre modulo 26 en son translaté par K dans $\mathbb{Z}_{26}$. Inversement, la règle de déchiffrement convertit un certain nombre en son translaté par $-K$ modulo 26. Le choix de 26 pour la valeur du modulus permet à l'évidence de représenter chaque lettre de l'alphabet romain par un unique entier modulo 26 : $0 \leftrightarrow A$, $1 \leftrightarrow B$, etc. On peut donc crypter des textes écrits. Dans le cas particulier où la clef vaut 3, le système cryptographique est le code de César évoqué dans la section précédente.

Exemple 2.2. Dans le cas du chiffrement par décalage, dès lors qu'une clef est fixée, chaque caractère alphabétique est transformé en un unique caractère alphabétique. Pour cette raison, le procédé est dit *mono-alphabétique*. Au XVI^{e} siècle, Blaise Vigenère inventa le *chiffrement de Vigenère* qui est un cryptosystème *poly-alphabétique*. Soit m un entier strictement positif. On définit $\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_{26}^m$. Pour toute clef $K = (K_1, K_2, \ldots, K_m)$, on pose

$$e_K(M_1, M_2, \ldots, M_m) = (M_1 + K_1 \bmod 26, M_2 + K_2 \bmod 26, \ldots, M_m + K_m \bmod 26)$$

et

$$d_K(C_1, C_2, \ldots, C_m) = (C_1 - K_1 \bmod 26, C_2 - K_2 \bmod 26, \ldots, C_m - K_m \bmod 26) \ .$$

Les règles de chiffrement et de déchiffrement correspondent cette fois à des translations dans $\mathbb{Z}_{26}^m$. L'intérêt de ce cryptosystème est de traiter des blocs de m caractères alphabétiques à la fois. On remarque que le nombre de clefs possibles est 26^m, donc même pour de petites valeurs de m, une recherche exhaustive « à la main » de la clef demande beaucoup trop de temps. Cependant cela peut être dans les possibilités d'un ordinateur. Par exemple, si l'on prend $m = 5$, l'espace de clefs est de taille supérieure à $1,1 \times 10^7$, ce qui n'exclut pas une attaque exhaustive assistée par ordinateur.

Exemple 2.3. Nous avons déjà signalé l'impuissance du chiffrement par décalage face à une recherche exhaustive de la clef et nous venons de voir celle du cryptosystème de Vigenère. De manière à encore augmenter la cardinalité de l'ensemble des clefs possibles et rendre ainsi plus difficile une attaque par essai exhaustif de toutes les clefs, on peut introduire le *chiffrement par permutation*. Il est décrit comme suit : $\mathcal{M} = \mathcal{C} = \mathbb{Z}_{26}$ et $\mathcal{K}$ est le groupe symétrique $S(\mathbb{Z}_{26})$ de $\mathbb{Z}_{26}$. Pour chaque permutation $\pi \in \mathcal{K}$, on définit

$$e_\pi(M) = \pi(M)$$

et

$$d_\pi(C) = \pi^{-1}(C) \ .$$

Le nombre de clefs est 26!, nombre relativement grand même pour les standards actuels. Bien que protégeant le cryptosystème contre une recherche exhaustive des clefs, ce nombre ne permet pas d'éviter une attaque fréquentielle. En effet les lettres dans une langue naturelle donnée ne sont pas équi-réparties. Par exemple en français, la lettre « e » figure en moyenne deux fois plus souvent dans un texte que la lettre « a ». En se basant sur ces données statistiques, on peut partiellement casser le chiffrement par permutation en cherchant les lettres les plus fréquentes d'un message chiffré et en déduisant les lettres correspondantes du message clair.

2.2.3 La cryptanalyse des systèmes à clef secrète

Ainsi que nous l'avons préalablement signalé la cryptologie englobe à la fois les procédés de chiffrement et les techniques de cryptanalyse. La meilleure défense étant l'attaque, étudier les faiblesses d'un cryptosystème du point de vue d'un puissant ennemi permet de dégager des principes de solidité et par la même occasion d'améliorer sensiblement la sécurité des communications. L'hypothèse fondamentale toujours effectuée est que l'opposant, Xavier, connaît le système cryptographique qu'il tente d'attaquer. En effet il est généralement préférable de baser la sécurité sur le cryptosystème lui-même plutôt que sur la non divulgation de sa description. En résumé, aucun secret ne doit résider dans la connaissance du procédé, tout le secret devant être dans la clef. Cette prémisse est nommée *principe de Kerckhoffs* du nom d'Auguste Kerckhoffs qui l'a énoncée en 1883 dans « La cryptographie militaire » [Ker1883]. Cette hypothèse étant faite, on distingue cinq modèles d'attaques classiques que l'on inventorie ici dans l'ordre décroissant de pouvoir de l'espion (ou symétriquement dans l'ordre croissant de quantité d'information devant être connue afin de mener l'attaque).

L'attaque à texte chiffré seulement : l'opposant connaît un certain nombre de messages chiffrés correspondant à des textes clairs qui, eux, lui sont inconnus ;

L'attaque à texte clair connu : le cryptanalyste dispose de chiffrés d'un certain nombre de messages clairs que, cette fois, il connaît aussi ;

L'attaque à texte clair choisi : l'espion peut choisir arbitrairement des textes clairs et possède un moyen de connaître les cryptogrammes correspondants ;

L'attaque à texte clair choisi adaptative : l'ennemi choisit une suite de textes clairs M_1, ..., M_m et les chiffrés correspondants $C_1, \ldots, C_m$ de manière interactive. En d'autres termes l'assaillant choisit M_i, obtient C_i le texte chiffré correspondant, puis choisit M_{i+1} selon des critères qu'il a arbitrairement fixés ;

L'attaque à texte chiffré choisi : l'attaquant a temporairement accès à une machine à déchiffrer, simulant le comportement du cryptosystème utilisé. De cette manière il a la possibilité de choisir des textes chiffrés arbitrairement et d'obtenir les messages clairs correspondants.

Dans tous les cas, le but de l'ennemi est de déterminer la clef utilisée, ce qui est vraisemblablement plus délicat à effectuer que de décrypter un message donné.

2.2.4 Cryptosystèmes inconditionnellement sûrs

La sécurité inconditionnelle introduite par les travaux de Shannon mesure la solidité du système (à clef secrète) lorsqu'il est attaqué dans le cadre d'une cryptanalyse à texte chiffré seul par un ennemi disposant de moyens de calculs infinis. On utilise aussi très souvent le terme de *confidentialité parfaite*[7]. Ainsi un système de chiffrement assure une confidentialité parfaite s'il ne peut être cassé par un adversaire sans borne sur sa puissance de calcul. On s'abstrait ainsi du postulat concernant la difficulté des problèmes de décision. La sécurité du système ne reposant alors que sur ses qualités propres.

Du point de vue de Shannon les ensembles $\mathcal{M}$, $\mathcal{C}$ et $\mathcal{K}$ de messages clairs, de cryptogrammes et de clefs sont des espaces probabilisés qui représentent des sources d'information. Les mesures de probabilité correspondantes étant notées « $\Pr^{(\mathcal{V})}$ » pour $\mathcal{V} = \mathcal{M}$, $\mathcal{C}$ ou $\mathcal{K}$. Seuls les ensembles $\mathcal{M}$ et $\mathcal{K}$ disposent en réalité de lois de probabilité arbitraires. La loi sur $\mathcal{C}$ est induite par les lois $\Pr^{(\mathcal{M})}$, $\Pr^{(\mathcal{K})}$ et par le profil des règles de chiffrement. On suppose de plus qu'il existe des variables aléatoires $\mathbf{M}$ et $\mathbf{C}$ définies sur le même espace probabilisé de départ (muni d'une mesure de probabilité Pr), à valeurs respectivement dans $\mathcal{M}$ et $\mathcal{C}$ et suivant les distributions *a priori* de ces ensembles *i.e.* pour $(M, C) \in \mathcal{M} \times \mathcal{C}$, $\Pr_{\mathbf{M}}(M) = \Pr(\mathbf{M}^{-1}(\{M\}))$ (par définition) $= \Pr^{(\mathcal{M})}(M)$ et $\Pr_{\mathbf{C}}(C) = \Pr(\mathbf{C}^{-1}(\{C\})) = \Pr^{(\mathcal{C})}(C)$ avec « $\mathbf{M}^{-1}$ » désignant l'image réciproque ensembliste de $\mathbf{M}$ (et de même pour $\mathbf{C}$). Ces variables aléatoires permettent de représenter des tirages au sort suivant des lois de probabilité fixées de messages clairs ou chiffrés. Dans ce cadre, Shannon [Sha48] a introduit un mesure de l'information ou de l'incertitude d'une source, c'est-à-dire l'information inhérente à chacun des symboles produits par la source, appelée *entropie*. Elle est définie pour une variable aléatoire $\mathbf{X}$ à valeurs dans un ensemble fini X de loi de probabilité $\Pr_{\mathbf{X}}$ comme suit :

$$H(\mathbf{X}) = -\sum_{x \in X} \Pr_{\mathbf{X}}(x) \log_2(\Pr_{\mathbf{X}}(x))$$

où le terme « $\log_2$ » désigne le logarithme en base deux (avec par convention $\log_2(0) = 0$). Puisque pour définir la confidentialité parfaite on se place dans le cadre d'une attaque à texte chiffré seul, on souhaite mesurer l'information sur la source de messages clairs obtenue par l'attaquant lorsqu'il dispose d'un certain nombre de cryptogrammes. Il faut donc déterminer la perte d'incertitude sur une source induite par la connaissance d'information *a priori*. Entant donné $\mathbf{Y}$ une variable aléatoire définie sur le même espace probabilisé que $\mathbf{X}$ et à valeurs dans un ensemble fini Y, la perte d'incertitude de $\mathbf{X}$ sachant $\mathbf{Y}$, appelée *entropie conditionnelle*, est définie par :

$$H(\mathbf{X}|\mathbf{Y}) = -\sum_{x \in X} \sum_{y \in Y} \Pr_{\mathbf{Y}}(y) \Pr_{\mathbf{X}|\mathbf{Y}}(x|y) \log_2(\Pr_{\mathbf{X}|\mathbf{Y}}(x|y))$$

[7] Les termes *sûreté inconditionnelle* et *confidentialité parfaite* possèdent la même signification.

où $\Pr_{\mathbf{X}|\mathbf{Y}}(x|y)$ est la probabilité que $\mathbf{X}$ prenne comme valeur x sachant que $\mathbf{Y}$ a pris la valeur y. Finalement on dira qu'un cryptosystème assure une *confidentialité parfaite* si $H(\mathbf{M}|\mathbf{C}) = H(\mathbf{M})$ *i.e.* la connaissance de textes chiffrés n'apporte aucune information sur les messages clairs. On dispose par ailleurs de la caractérisation suivante de la sécurité inconditionnelle.

Théorème 2.1. [Sha49] *Soit* $(\mathcal{M}, \mathcal{C}, \mathcal{K}, \{e_k\}_{k\in\mathcal{K}}, \{d_k\}_{k\in\mathcal{K}})$ *un système cryptographique tel que* $|\mathcal{M}| = |\mathcal{C}| = |\mathcal{K}|$. *Pour que ce système assure une confidentialité parfaite il faut et il suffit que la clef soit utilisée de manière équiprobable et que pour chaque* $(M, C) \in \mathcal{M} \times \mathcal{C}$, *il existe une et une seule clef* $K \in \mathcal{K}$ *telle que* $e_k(M) = C$.

Exemple 2.4. Une célèbre réalisation de la sûreté inconditionnelle est le *chiffrement de Vernam*, encore appelé *masque jetable* ou *one-time pad* en anglais, inventé par Vernam [Ver26]. Il est défini comme une translation d'un vecteur de m bits (le texte clair) suivant un autre vecteur de m bits, jouant le rôle de clef, c'est-à-dire que l'on fait agir le groupe additif $\mathbb{Z}_2^m$ sur lui-même par translation[8]. La description formelle de ce cryptosystème est la suivante : soit $m \in \mathbb{N}^*$ et soient $\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_2^m$. Pour $K \in \mathcal{K}$ et $M \in \mathcal{M}$, on définit $e_K(M) = M \oplus K = (M_1 + K_1 \bmod 2, \ldots, M_m + K_m \bmod 2)$ où le symbole « $\oplus$ » représente donc la somme modulo deux composante par composante. L'addition modulo deux étant involutive[9] on en déduit que la règle de déchiffrement est identique à celle de chiffrement. En supposant que la loi de probabilité sur l'ensemble $\mathcal{K}$ des clefs soit l'équiprobabilité *i.e.* $\Pr^{(\mathcal{K})}(K) = \dfrac{1}{2^m}$ pour tout $K \in \mathcal{K}$ (ce qui revient au fait que chaque clef n'est utilisée qu'une unique fois, d'où notamment le nom de masque jetable) alors le chiffrement de Vernam est inconditionnellement sûr d'après le théorème précédent (l'unicité de la clef pour chacun des couples clairs-chiffrés est garantie *de facto* puisque l'action par addition de $\mathbb{Z}_2^m$ sur lui-même est régulière[10]).

Si la confidentialité parfaite est essentielle pour caractériser la sécurité, dans des termes probabilistes, des cryptosystèmes, elle ne constitue cependant pas la panacée. Les applications pratiques des cryptosystèmes parfaitement sûrs sont limitées car en général cela exige à la fois des clefs de même taille que celle des données à crypter et une utilisation unique de celles-ci dans un processus de chiffrement. Les problèmes de choix, de stockage et de transmission des clefs (puisque les deux personnes en communication doivent connaître la clef utilisée) deviennent trop complexes dans les faits pour être d'une quelconque utilité. Nous devons mettre un bémol à cette constatation. En effet le Professeur Harari de l'Université du Sud Toulon-Var a développé un algorithme de chiffrement inconditionnellement sûr dont la clef est plus courte que le message. Toutefois ce n'est ordinairement pas le cas. Aussi un autre critère de solidité doit être établi. Ainsi une version moins forte de la confidentialité parfaite est possible, définie elle aussi par Shannon, dans laquelle on ne se limite pas à l'utilisation d'une et une seule clef par cryptage. S'il est clair que l'exploitation d'une même clef dans le chiffrement de plusieurs messages affaiblit la sûreté du système, il est tout de même possible, dans une certaine mesure, de quantifier cette perte de fiabilité mais aussi de la limiter. Plaçons-nous, une nouvelle fois, dans le cadre d'une attaque à chiffré seul et supposons intercepté, par l'espion Xavier, un message crypté dont le texte clair correspondant est écrit dans une langue donnée. Dans son processus de cryptanalyse Xavier élimine un certain nombre de clefs, néanmoins il peut subsister plusieurs clefs possibles, parmi lesquelles se trouve la bonne clef, qui donnent, par déchiffrement à partir du cryptogramme, un texte sémantiquement correct dans la langue originale. Toutes les clefs qui ne sont pas la bonne sont appelées *clefs parasites* (on parle aussi de clefs *consistantes* avec le crypté). Xavier doit donc intercepter d'autres messages afin de distinguer la bonne clef parmi toutes les mauvaises. Ceci est dû à l'incertitude sur la clef utilisée lorsqu'on a connaissance d'un cryptogramme chiffré avec

[8] Nous verrons cette notion en détail au chapitre 7.

[9] Une involution d'un ensemble X est une application bijective $\boldsymbol{\sigma}$ de X dans lui-même telle que $\boldsymbol{\sigma}^2 = \boldsymbol{\sigma} \circ \boldsymbol{\sigma} = Id_X$.

[10] Se référer au chapitre 7 pour plus de précisions.

cette clef *i.e.* l'entropie $H(\mathbf{K}|\mathbf{C})$ où la lettre « $\mathbf{K}$ » désigne une variable aléatoire sur la source des clefs $\mathcal{K}$, suivant la distribution $\Pr_{\mathcal{K}}$. Motivé par ce fait, Shannon a défini la quantité suivante :

Définition 2.2. La *distance d'unicité*, notée « n_{du} », d'un système de chiffrement est le plus petit entier n telle qu'il n'y ait essentiellement qu'une valeur de clef possible pour $\mathbf{K}$ consistante avec les textes chiffrés $\mathbf{C}_1, \ldots, \mathbf{C}_n$.

De manière équivalente cela signifie que la distance d'unicité est le plus petit entier n tel que

$$H(\mathbf{K}|\mathbf{C}_1, \ldots, \mathbf{C}_n) \approx 0 \ .$$

Ce qui revient à dire qu'il s'agit du plus petit nombre de textes chiffrés devant être connus pour que l'ensemble des clefs parasites soit fondamentalement réduit à l'ensemble vide. La distance d'unicité permet d'utiliser la notion d'entropie dans un cadre moins contraignant que celui de la sûreté inconditionnelle en permettant l'utilisation d'une même clef un certain nombre de fois. Plus cette valeur est grande et plus l'attaque à texte chiffré seul est rendue difficile. Dans un cryptosystème pour lequel la distance d'unicité reste éloignée de 0 même pour un nombre n très grand de cryptogrammes interceptés, une attaque à texte chiffré seul ne réussira jamais. Remarquons au passage que cette quantité dépend de la redondance de la source des textes clairs. Par redondance on entend le fait que certains symboles ou lettres sont émis plus souvent que d'autres par la source d'information dans un langage donné. Autrement dit, certaines lettres apparaissent plus souvent que d'autres, en moyenne, dans un texte écrit dans une langue naturelle. Par exemple le contenu du présent chapitre, commandes LaTeX y compris, comporte plus de 100000 lettres. La lettre « e » (sans respecter la casse ni l'accentuation) y figure environ 20000 fois alors qu'il n'y a que 2000 occurrences de la lettre « z », soit dix fois moins. Pour un procédure de chiffrement cryptant des messages de m bits la redondance ρ est définie par

$$\rho = 1 - \frac{H(\mathbf{M})}{m} \ ,$$

$\frac{H(\mathbf{M})}{m}$ étant une estimation moyenne des bits d'information par bit de texte clair. Enfin on dispose du théorème suivant :

Théorème 2.2. [Sha49] *La distance d'unicité d'un cryptosystème est*

$$n_{du} = \frac{H(\mathbf{K})}{\rho}$$

où ρ est la redondance de la source des messages clairs.

Observons alors que pour disposer d'une distance d'unicité élevée, il faut une redondance tendant vers 0 *i.e.* que la fréquence d'occurrence des lettres soit proche de l'équiprobabilité, chose évidemment impossible pour un langage naturel. Néanmoins on peut toujours réduire la redondance d'un texte en utilisant une fonction de compression. C'est par exemple la cas si on retire les occurrences de la lettre « e » dans un texte écrit en français :

« Touts ls langus prsntnt des lmnts rdondants, c'st-à-dir porturs d'information faibl ou null, combinaisons d sons, d lttrs, d syllabs, d mots. Mais ils n sont pas ls mms dans chaqu langu. »

2.2.5 Critères pratiques de solidité

2.2.5.1 Introduction

La confidentialité parfaite (et son extension, la distance d'unicité) représente une sécurité idéale dans un univers utopique. Dans le monde réel, l'attaquant peut disposer d'autres informations

que la seule connaissance de textes chiffrés. Si, par exemple, nous faisons l'hypothèse raisonnable que les cryptogrammes proviennent du chiffrement de textes écrits dans une langue naturelle, un ennemi, s'il connaît la langue utilisée, peut faire usage de certaines statistiques de l'idiome telle que la fréquence d'occurrence des lettres et autres motifs plus compliqués afin de pratiquer une attaque. Il dispose ainsi d'un certain nombre d'informations complémentaires et la sécurité du système ne peut alors plus s'étudier dans le décor imaginaire de la confidentialité parfaite. Plus globalement, lorsqu'on change de modèle d'attaques, un cryptosystème réputé fiable par rapport à un type donné de cryptanalyses, peut parfaitement être très largement affaibli et même complètement impuissant face à une autre variété d'attaques. Ainsi, par exemple, le chiffrement de Vernam est-il vulnérable face à une attaque à texte clair connu. On retrouve en effet la clef K utilisée dans le chiffrement simplement en calculant $M \oplus e_K(M)$ lorsque l'on dispose à la fois du clair M et de son chiffré $e_K(M)$.

Shannon [Sha49] a déduit, de l'étude des qualités statistiques générales des cryptanalyses, deux recommandations pour la conception pratique des systèmes de chiffrement : la *diffusion* et la *confusion*. Ces indicateurs ont alors pour but d'empêcher les analyses basées sur les statistiques des sources de messages clairs et chiffrés. Attention cependant, ces principes sont à la fois génériques et informels et doivent être considérés comme des directives générales et pragmatiques pour la construction de mécanismes de chiffrement et non comme des lois absolues[11].

2.2.5.2 Diffusion

Le concept de diffusion est introduit par Shannon dans les termes subséquents :

«... the statistical structure [of the set of plaintexts] *which leads to its redundancy is " dissipated " into long range statistics - i.e. into statistical structure involving long combination of letters into the cryptogram. »*

Le principe de la diffusion est fondé sur la dissipation et dispersion de la structure statistique des messages clairs dans celle des messages chiffrés, de manière à l'uniformiser. Ainsi les motifs les plus fréquents de la source sont répandus et mélangés dans de longues séquences de messages chiffrés. Le but étant de rendre plus complexe l'utilisation des statistiques de la source de messages clairs. En effet, en distribuant les effets statistiques de chaque symbole de messages clairs sur de nombreuses lettres de messages chiffrés, il devient dès lors impossible de retrouver les régularités initiales, après chiffrement, sauf en considérant de très grandes quantités de textes chiffrés. En d'autres termes, on équilibre l'influence sur le cryptogramme de chacun des symboles du texte clair. Massey dans [Mas88] a ré-interprété la notion de diffusion dans le cadre de la cryptographie moderne en affirmant que chaque symbole de textes clairs doit influencer de nombreux symboles de textes chiffrés. Par exemple, si on suppose que les messages clairs et chiffrés sont constitués de caractères issus de l'alphabet latin et les clairs sont écrits dans la langue française, alors que la lettre « e » apparaît le plus souvent au sein des messages initiaux, l'effet de la diffusion induit qu'après chiffrement, la fréquence de cette lettre n'est plus distinguable des autres. Observons que pour mettre en œuvre une telle méthode il faut considérer les messages à chiffrer comme des blocs ou suites de symboles et non comme des éléments atomiques. C'est d'ailleurs ce qui a abouti aux approches de chiffrements par blocs et à flot présentées dans les deux sections suivantes. Ce dernier constat ne constitue pas une caractérisation suffisante de la diffusion mais seulement une propriété nécessaire. En effet si le chiffrement de Vernam repose sur la notion de bloc de bits constituant les messages clairs, chiffrés ainsi que les clefs, la transformation utilisée

[11] Par opposition par exemple aux lois de la gravité : on ne recommande pas à une pomme de tomber, elle chute nécessairement.

(translation suivant un vecteur) offre un très mauvais caractère diffuseur, et même, d'un certain point de vue, la plus faible diffusion possible, puisqu'un bit de message clair influence seulement un bit de message chiffré. La cause en étant que l'opération de chiffrement agit en parallèle sur chacun des bits de messages clairs/chiffrés et donc que l'utilisation d'un bloc dans la description du chiffrement de Vernam est tout à fait facultative. L'intrication de l'influence des symboles d'un texte clair sur ceux du cryptogramme correspondant, conseillée par la diffusion, doit, en particulier, rendre impossible une telle décomposition du système de chiffrement en parties plus petites et plus facilement attaquables. En définitive, selon l'interprétation de Massey, un léger changement parmi les symboles d'un texte clair doit provoquer de considérables variations dans le cryptogramme de manière la plus chaotique possible. La notion de diffusion est aujourd'hui unanimement acceptée par la communauté des cryptographes.

2.2.5.3 Confusion

La méthode de confusion a quant à elle pour objectif de rendre complexes les relations entre les statistiques simples des cryptogrammes et celles de la source des clefs. Si les connexions entre les symboles dans les messages chiffrés et dans les clefs sont trop imbriquées, un adversaire peut certes utiliser des statistiques permettant de limiter l'espace des clefs possibles mais cet espace possède alors une description trop compliquée pour être réellement exploitable. De même que dans le cas de la diffusion, le procédé de chiffrement de Vernam est très peu confus : les relations entre bits de cryptogramme et de clef sont très simples et trop peu mélangeantes. De manière analogue, il est conseillé d'éviter les relations qui ont une forme algébrique simple, telles que les transformations linéaires, ou dans lesquelles n'interviennent que peu de variables. La confusion est généralement réalisée à l'aide de substitutions. Cette approche a été validée par l'utilisation dans le DES des fameuses boîtes-S.

En général, un cryptosystème est construit comme une composition d'une transposition et d'une substitution afin de mettre en œuvre à la fois une phase de diffusion et une phase de confusion. Finalement comme conséquence directe des concepts de diffusion et de confusion on peut citer les notions de propagation, de résilience et de fonction courbe. Celles-ci seront étudiées, concernant les deux premières, au chapitre 4. La notion de fonction courbe constituant quant à elle la majeure partie du présent manuscrit.

2.3 Chiffrement par blocs

Au cours de cette section nous décrivons dans un premier temps les principes fondamentaux de la mise en œuvre du chiffrement par blocs. Puis nous présentons les progrès théoriques ayant conduit à la réalisation de certains algorithmes de chiffrement par blocs. Enfin nous abordons ce domaine par son versant cryptanalytique en exposant quelques-unes des attaques les plus éprouvées.

2.3.1 Structure générale

Le chiffrement par blocs constitue le type de cryptosystèmes le plus répandu mais aussi le plus exploité dans les transactions commerciales. Le principe de base consiste à diviser le message clair en un certain nombre de blocs de même taille et de crypter chacun d'entre eux à l'aide d'une méthode de chiffrement à clef secrète E qui, en vertu du principe de Kerckhoff, est connue du public. En règle générale, les blocs cryptés obtenus par application de l'algorithme de chiffrement ont la même taille que les blocs clairs dont ils sont issus. Dans la suite on supposera que les messages clairs, chiffrés et les clefs sont des séquences de bits. En résumé les blocs sont des

éléments de $\mathbb{F}_2^m$ pour un certain m ($\mathbb{F}_2$ étant le corps fini à deux éléments). La plupart des cryptosystèmes actuels se base sur l'utilisation d'algorithmes itératifs composés de k tours ou rondes dans lesquels s'exécute une même fonction « inversible » g paramétrée par une sous-clef K_i. Les sous-clefs $K_1, \ldots, K_k$ sont générées à partir d'une clef secrète K de manière, en particulier, à être toutes distinctes. Cette structuration en tours permet, hormis dans des cas pathologiques, d'assurer la diffusion et la confusion du cryptosystème. Après un certain nombre de rondes tous les bits en sortie dépendent d'un grand nombre de bits en entrée et ces corrélations sont par ailleurs généralement complexes.

Définition 2.3. Dans un *chiffrement par blocs itéré* à k tours le message crypté est calculé récursivement par application d'une *fonction de tour* g sur le texte clair, *i.e.*

$$C_i = g(C_{i-1}, K_i) \text{ pour } i = 1, \ldots, k$$

où C_0 est le texte clair, K_i est la sous-clef du $i^{ème}$ tour et C_k est le texte chiffré. Le déchiffrement est réalisé en inversant l'équation précédente. Ainsi est-il nécessaire que pour une sous-clef fixée K_i dans la $i^{ème}$ ronde, la fonction $g_{K_i} : C \mapsto g(C, K_i)$ soit inversible.

La fonction g est généralement la composition de deux transformations : une permutation linéaire assurant la diffusion et une substitution, en principe non linéaire, afin de brouiller les relations entre bits du texte clair, de la clef et du chiffré. Une grande partie de la sécurité des cryptosystèmes de ce type, dits *réseaux de substitution-permutation*, est basée sur les propriétés de la composante non linéaire de la fonction g.

2.3.2 Evolution des technologies

Dans cette sous-section sont décrits trois des plus célèbres cryptosystèmes à clef secrète par blocs en mettant en lumière les avancées techniques les caractérisant : le DES et son réseau de Feistel, IDEA et les lois de composition de groupes et l'AES et les transformations bijectives dans un corps fini. Ainsi plus que la description de ces systèmes de chiffrement, nous aborderons ici les outils fondamentaux utilisés par chacun d'eux.

2.3.2.1 Schéma de Feistel

A la fin des années 1970, le gouvernement américain adopta comme norme de chiffrement le DES (Data Encryption Standard) conçu par IBM [NBS80]. Cet algorithme utilise comme fonction de tour une *permutation de Feistel* du nom de son créateur H. Feistel (voir [Fei70, Fei73]). Le bloc de bits du message clair est découpé en deux. Une fonction f est appliquée sur l'une des deux moitiés et le résultat est combiné par une somme modulo deux composante par composante. Nous obtenons ainsi la définition suivante pour ce concept :

Définition 2.4. Soit $m \in \mathbb{N}^*$. Soit $f : \mathbb{F}_2^m \to \mathbb{F}_2^m$. On définit $\pi_f \in S(\mathbb{F}_2^{2m})$, appelé *permutation de Feistel*, par

$$\pi_f(G, D) = (D, G \oplus f(D)) \text{ avec } (G, D) \in \mathbb{F}_2^m \times \mathbb{F}_2^m.$$

Remarquons tout de suite que l'on a identifié les deux espaces vectoriels $\mathbb{F}_2^m \times \mathbb{F}_2^m$ et $\mathbb{F}_2^{2m}$. Ainsi que l'indique la définition, quelle que soit la fonction f choisie, π_f est, chose à la fois simple, admirable et remarquable, une permutation. Sa permutation inverse se calcule très facilement par

$$\pi_f^{-1}(G, D) = (D \oplus f(G), G) \textit{ i.e. } \pi_f^{-1} = \boldsymbol{\sigma} \circ \pi_f \circ \boldsymbol{\sigma}$$

où $\boldsymbol{\sigma} \in S(\mathbb{F}_2^m \times \mathbb{F}_2^m)$ est l'involution définie par $\boldsymbol{\sigma}(G, D) = (D, G)$. Comme nous allons le voir plus loin π_f joue le rôle de fonction de tour. Observons qu'en général la composition de deux

permutations de Feistel n'est pas une permutation de Feistel. Ceci est primordial pour leur utilisation dans un algorithme itératif de chiffrement par blocs.

Cette construction, introduite au début des années 1970, permit alors de combler partiellement les lacunes des chercheurs de l'époque sur les fonctions inversibles dans les espaces vectoriels sur $\mathbb{F}_2$. Cette notion fut par la suite généralisée (voir par exemple [AGH+92, Luc96, SK96]).

Définition 2.5. Soient $(m,k) \in (\mathbb{N}^*)^2$ et $(f^{(1)},\ldots,f^{(k)})$ un k-uplet de fonctions de $\mathbb{F}_2^m$ dans lui-même. On définit l'*échelle de Feistel* $\pi_{(f^{(1)},\ldots,f^{(k)})} \in S(\mathbb{F}_2^{2m})$ par

$$\pi_{(f^{(1)},\ldots,f^{(k)})} = \pi_{f^{(k)}} \circ \ldots \circ \pi_{f^{(1)}} \ .$$

Pour la donnée des k fonctions $f^{(i)} : \mathbb{F}_2^m \to \mathbb{F}_2^m$ pour $i = 1,\ldots,k$, $\pi_{(f^{(1)},\ldots,f^{(k)})} : \mathbb{F}_2^{2m} \to \mathbb{F}_2^{2m}$ est bien une permutation par composition des permutations de Feistel $\pi_{f^{(i)}}$.

La mise en œuvre pratique des échelles de Feistel dans un procédé de chiffrement s'effectue en paramétrant la fonction $f^{(i)}$ de la $i^{ème}$ permutation de Feistel par une clef K_i comme suit :

Définition 2.6. Soit m un entier strictement positif. Un *schéma de Feistel* à k tours est un cryptosystème itératif transformant un message $M = (G_0, D_0)$ où G_0 et D_0 sont des blocs de bits de taille m, en un chiffré $C = (G_k, D_k)$ tel que G_k et D_k sont eux aussi de taille m. Soit $f : \mathbb{F}_2^m \times \mathbb{F}_2^m \to \mathbb{F}_2^m$, appelée, par abus de langage, la fonction de tour, et $(K_1,\ldots,K_k)$ le k-uplet de (sous-)clefs de tour obtenu à partir de la clef principale de chiffrement K. Alors pour tout $i \in \mathbb{N}$ tel que $1 \leq i \leq k$ les blocs G_i et D_i de la $i^{ème}$ ronde sont obtenus grâce à la relation de récurrence suivante :

$$\begin{cases} G_i = D_{i-1} \ , \\ D_i = G_{i-1} \oplus f(D_{i-1}, K_i) \ . \end{cases}$$

On obtient donc en utilisant les notations précédentes pour la fonction de tour

$$g(G_{i-1}, D_{i-1}) = (D_{i-1}, G_{i-1} \oplus f(D_{i-1}, K_i)) \ .$$

En d'autres termes si on définit, pour $i = 1,\ldots,k$, $f^{(i)} : \mathbb{F}_2^m \to \mathbb{F}_2^m$ la fonction telle que $f^{(i)}(x) = f(x, K_i)$, un schéma de Feistel à k rondes correspond en fait à l'échelle de Feistel $\pi_{(f^{(1)},\ldots,f^{(k)})}$.

La justification théorique de cette approche pour le chiffrement itéré est établie par un profond résultat dû à Luby et Rackoff [LR88]. Ils ont en effet introduit la notion de permutations pseudo-aléatoires qui peuvent être interprétées comme des cryptostystèmes par blocs sûrs contre les attaques à texte clair choisi adaptatives. Informellement cela signifie qu'un adversaire, avec accès à une machine chiffrant les messages de son choix, ne peut distinguer ces chiffrements des valeurs d'une permutation réellement aléatoire ; le terme « aléatoire » étant pris ici au sens de la probabilité uniforme. Plus précisément les adversaires considérés sont des distingueurs. Un *distingueur* pour un cryptosystème donné est une machine de Turing, fonctionnant en temps probabiliste polynomial, tentant par un jeu de questions-réponses de distinguer un système de chiffrement E d'un autre système idéal, une permutation aléatoire, noté « E^* ». Le distingueur D a accès à un oracle qu'il peut interroger afin d'obtenir le résultat d'une des deux permutations pour une entrée de son choix, sans connaître la permutation choisie par l'oracle pour répondre. Une question type que peut poser le distingueur à l'oracle est, pour M un bloc de bits,

« Quelle est la valeur du chiffré du texte clair M ? »

L'oracle lui renvoie pour réponse la valeur du chiffrement de M soit par E soit par E^*. Le résultat énoncé par Luby et Rackoff signifie alors informellement qu'une échelle de Feistel (aléatoire)

$\pi_{(\mathbf{X}_1,\mathbf{X}_2,\mathbf{X}_3)}$, où les $\mathbf{X}_i$ sont des variables aléatoires à valeurs des fonctions de $\mathbb{F}_2^m$ dans lui-même, mutuellement indépendantes, n'est pas distinguable d'une permutation aléatoire *i.e.* une variable aléatoire E^* uniformément distribuée sur $S(\mathbb{F}_2^{2m})$. Notons « $\Pr(D^E = 1)$ » la probabilité que le distingueur, après que l'oracle lui ait fourni un certain nombre d'informations, produise le chiffre « 1 », *i.e.* que la suite de réponses données par l'oracle aux différentes requêtes permette au distingueur de deviner correctement que l'algorithme E est bien le chiffrement utilisé. De même $\Pr(D^{E^*} = 1)$ est la probabilité correspondante pour E^*. Il est alors possible de préciser le résultat de Luby et Rackoff en définissant l'*avantage* du distingueur comme suit

$$Adv_D(E, E^*) = |\Pr(D^E = 1) - \Pr(D^{E^*} = 1)| .$$

Ainsi dans le cas d'une échelle de Feistel, l'avantage du distingueur est une quantité négligeable par rapport au nombre de requêtes. De ce fait l'adversaire n'est pas capable, en moyenne, de distinguer l'utilisation de $E = \pi_{(\mathbf{X}_1,\mathbf{X}_2,\mathbf{X}_3)}$ plutôt que celle d'une permutation aléatoire E^*. Plus précisément encore, Luby et Rackoff ont montré qu'une attaque à clair choisi sur une échelle de Feistel d'au moins trois tours demande $\mathcal{O}(2^{\frac{m}{2}})$ clairs i.e. qu'il existe $c > 0$ telle que le nombre de messages clairs choisis soit dominé par $c2^{\frac{m}{2}}$. De ce fait, la complexité de l'attaque est exponentielle. Remarquons par ailleurs que 3 est le nombre minimum de tours à partir duquel une attaque à texte clair choisi nécessite ces $\mathcal{O}(2^{\frac{m}{2}})$ clairs. En effet si le nombre de tours est réduit cette propriété est prise en défaut puisque l'on peut alors exhiber des attaques à texte clair choisi de complexité indépendante de la taille des données. Sans prévaloir de la connaissance de ce résultat lors de la conception du DES, il offre un cadre théorique très confortable à la sécurité de ce cryptosystème. Ceci expliquant sans doute la très grande fiabilité de cet algorithme et son important succès. La description du DES est brièvement donnée ci-dessous.

Définition 2.7. Le DES est un schéma de Feistel comportant seize rondes. Les blocs de clairs et de chiffrés ont 64 bits et la clef principale 56 bits. Les clefs de tour K_i ont une taille de 48 bits. La fonction de tour f prend deux arguments, le premier étant un bloc de 32 bits, le second un bloc de 48 bits et son résultat est un bloc de 32 bits. Elle est définie à la $i^{ème}$ ronde par $f(D_{i-1}, K_i) = P(S(E(D_{i-1})) \oplus K_i)$ où E est une fonction d'expansion affine qui augmente la taille de D_{i-1} de 16 bits pour en faire un bloc de 48 bits, la fonction S fait appel en parallèle à huit boîtes-S différentes, chacune transformant un sous-bloc de 6 bits en un sous-bloc de 4 bits et enfin P est une simple permutation entre les bits du bloc, de longueur 32, final. Les boîtes-S du DES, que nous ne détaillons pas ici, sont des substitutions non linéaires.

2.3.2.2 Lois de composition internes de groupes

IDEA (acronyme de « International Data Encryption Algorithm ») est un algorithme de chiffrement par blocs proposé par Lai et Massey [LMM91]. Sa version préliminaire nommée PES (Proposed Encryption Standard) ayant quant à elle été publiée en 1991 dans [LM91]. Il est architecturé comme le DES, dont il convoitait le statut de standard américain de cryptage, suivant l'itération sur huit rondes d'une application inversible. Au contraire du DES cependant, l'application en question n'est pas construite à l'aide d'un moyen artificiel tel qu'une permutation de Feistel mais est réalisée directement par composition de plusieurs opérations inversibles. Ainsi le principe de base de ce cryptosystème est un mélange de trois lois de composition internes de différents groupes algébriques (non isomorphes). Ces opérations étant choisies de telle sorte que les exigences de confusion (éliminer les structures remarquables tant linéaires qu'algébriques du chiffrement) et de diffusion (chaque bit en sortie dépend d'un grand nombre de bits en sortie) soient entièrement satisfaites.

Décrivons donc brièvement ce cryptosystème. L'algorithme IDEA agit sur des blocs de bits, les blocs de messages clairs/chiffrés étant composés de 64 bits alors que la clef secrète est longue de

128 bits. Le bloc de message clair est divisé en 4 sous-blocs de 16 bits. Ces 4 sous-blocs de texte clair sont transformés en 4 sous-blocs de texte chiffré, en utilisant, au total à l'issue des huit tours, 52 sous-clefs de 16 bits. A chaque tour, le chiffrement (ainsi que le déchiffrement) est exécuté en sommant suivant les trois lois de groupes choisies, et ce dans un certain ordre, les 4 sous-blocs avec 6 sous-blocs de clefs. Toutefois nous ne nous intéressons pas ici au processus de chiffrement proprement dit aussi nous n'allons pas plus loin dans sa description et présentons les lois utilisées.

Pour $m \in \mathbb{N}^*$ tel que $2^m + 1$ soit premier, *i.e.* $2^m + 1$ est un nombre de Fermat[12], on définit :

- $(\mathbb{F}_2^m, \oplus)$ est le groupe des m-uplets sur $\mathbb{F}_2$ muni de l'addition modulo 2 composante par composante ;

- $(\mathbb{F}_2^m, \boxplus)$ est le groupe muni de la loi transportée sur $\mathbb{F}_2^m$ du groupe additif $(\mathbb{Z}_{2^m}, +)$ de l'anneau $\mathbb{Z}_{2^m}$ (les éléments de $\mathbb{F}_2^m$ étant alors identifiés à des représentations d'entiers modulo 2^m écrits en base deux) ;

- $(\mathbb{F}_2^m, \odot)$ est le groupe muni de la loi transportée sur $\mathbb{F}_2^m$ du groupe $(\mathbb{Z}_{2^m+1}^*, .)$, groupe multiplicatif des éléments non nul du corps premier $\mathbb{Z}_{2^m+1}$ (les éléments de $\mathbb{F}_2^m$ étant alors identifiés à des représentations d'entiers de $\mathbb{Z}_{2^m+1}$ écrits en base deux hormis le m-uplet constitué des bits tous à zéro qui est considéré comme représentant la valeur 2^m).

On a alors, par exemple pour $m = 16$,

$$(0, 0, \ldots, 0) \odot (1, 0, \ldots, 0) = (1, 0, \ldots, 1)$$

puisque $2^{16}2^{16} \pmod{2^{16} + 1} = 2^{15} + 1$.

Une partie considérable de la solidité du cryptosystème repose sur l'utilisation de ces trois lois de groupes algébriquement distincts mais de même cardinal. La confusion est achevée par l'algorithme de chiffrement à l'aide de propriétés d'incompatibilité des opérations de groupe dont par exemple les défauts de distributivité et d'associativité entre ces lois. Pour $m \in \{1, 2, 4, 8, 16\}$, et $(\top_1, \top_2) \in \{\oplus, \boxplus, \odot\}^2$ tel que $\top_1 \neq \top_2$, il existe $(x_1, y_1, z_1) \in (\mathbb{F}_2^m)^3$ et $(x_2, y_2, z_2) \in (\mathbb{F}_2^m)^3$ tels que l'on ait :

$$x_1 \top_1 (y_1 \top_2 z_1) \neq (x_1 \top_1 y_1) \top_2 (x_1 \top_1 z_1)$$

et

$$x_2 \top_1 (y_2 \top_2 z_2) \neq (x_2 \top_1 y_2) \top_2 z_2 \ .$$

Par ailleurs il est montré que la diffusion est satisfaite dès le premier tour, *i.e.* chaque bit en sortie du premier tour dépend de tous les bits en entrée et de tous les bits de clef utilisée pour ce tour.

2.3.2.3 Transformations bijectives dans un corps fini

Rijndael, vainqueur de l'appel d'offres organisé par le NIST (National Institute for Standards and Technology) pour le standard de chiffrement avancé (en anglais « Advanced Encryption Standard », soit en abrégé « AES ») pour les États-Unis d'Amérique, a été créé par deux chercheurs belges J. Daemen et V. Rijmen [DR02]. Il opère sur des blocs de 128 bits et utilise des clefs de longueur 128, 192 ou 256 bits. A l'instar de la majorité des algorithmes par blocs, l'AES consiste à itérer une permutation paramétrée par une valeur de sous-clef secrète changeant à chaque tour. Pour

[12] Par exemple $2^{16} + 1$ est premier.

fixer les idées, on suppose ici que la sous-clef de ronde est longue de 128 bits. Le nombre de rondes est alors 10. Chaque bloc, de clair, de chiffré et de clef, est considéré comme une matrice 4×4 d'octets (éléments de huit bits). La fonction itérée 10 fois est définie comme la composition de quatre transformations afin de satisfaire les principes fondamentaux de confusion et de diffusion. Ces transformations inversibles opèrent sur chacun des octets constituant les matrices à traiter. L'originalité de ce cryptosystème réside donc dans l'utilisation explicite de la structure du corps fini $\mathbb{F}_{2^8}$, plus riche que celles de groupes de m-uplets exploitées dans IDEA, à travers la mise en œuvre de permutations de $\mathbb{F}_{2^8}$ ayant chacune des particularités spécifiques. Les quatre transformations figurant donc dans une ronde sont les suivantes.

SubBytes est une substitution non linéaire (par rapport au corps fini $\mathbb{F}_{2^8}$) faisant appel sur chacun des octets de la matrice d'entrée à une boîte-S choisie pour garantir de bonnes propriétés de confusion. La substitution $S_{RD} : \mathbb{F}_{2^8} \to \mathbb{F}_{2^8}$ est définie par composition de l'involution non linéaire $\boldsymbol{\sigma}_{inv} : x \mapsto x^{-1}$ (avec $0^{-1}_{\mathbb{F}_{2^8}} = 0_{\mathbb{F}_{2^8}}$) et d'une transformation affine non singulière δ de $\mathbb{F}_2^8$. Ainsi la matrice d'octets $M_{i,j}$ $(i, j = 1, \ldots, 4)$ est transformée en une matrice d'éléments $C_{i,j} = S_{RD}(M_{i,j}) = \delta(M^{-1}_{i,j})$. A noter que nous reviendrons sur cette transformation S_{RD} au chapitre 7 afin d'exposer l'une de ses propriétés remarquables.

Shiftrows est une transposition des octets par décalages cycliques des lignes de la matrice, décalages de valeurs différentes suivant la ligne considérée (rotation de zéro pour la première ligne, d'une case pour la seconde, de deux cases pour la troisième et de trois pour la quatrième). Cette transformation a été choisie pour fournir une diffusion optimale au système.

MixColumn est une multiplication matricielle portant en parallèle sur chacune des colonnes de la matrice à chiffrer. Il s'agit d'une transformation linéaire inversible garantissant une bonne diffusion.

AddRoundKey est simplement l'addition modulo deux bit à bit de la matrice à chiffrer par la matrice de sous-clef de ronde.

Remarque 2.1. A chacune des deux premières transformations est dévolue un rôle particulier pour assurer une bonne diffusion globale au système. Ainsi *SubBytes* diffuse l'information à l'intérieur de chaque octet de la matrice. *Shiftrows* permet quant à elle de diffuser les octets à l'intérieur des colonnes. La troisième transformation, *MixColumn*, mélange tous les octets.

2.3.3 Cryptanalyses

Dans cette sous-section sont abordées quelques unes des attaques les plus connues sur les chiffrements par blocs. Nous présentons plus particulièrement les cryptanalyses différentielle et linéaire qui sont indubitablement le point de départ des notions que nous développons dans cette thèse.

2.3.3.1 Cryptanalyse différentielle

La plus célèbre et la plus efficace des attaques connues à ce jour est la cryptanalyse différentielle publiée dans [BS91] par E. Biham et A. Shamir. Cette méthode a prouvé à maintes reprises son efficacité puisqu'elle a été utilisée avec succès sur différents cryptosystèmes tels que le DES à 16 tours [BS93] ou Lucifer [B-AB96]. Cette attaque s'applique en fait à n'importe quel chiffrement itératif par blocs et utilise une faille potentielle de la fonction de ronde itérée g dans une dérivation d'ordre 1. En conséquence on étudie le comportement de la fonction g lorsqu'elle est soumise à une translation sur ses variables. Dans [LMM91] on trouve les conditions optimales pour la réussite de l'attaque différentielle. La clé de voûte de cette cryptanalyse est, ainsi que l'on peut le deviner

par connotation de « différentielle », l'emploi de la différence entre deux blocs de bits de même taille X et X', définie par

$$\Delta X = X \oplus X' \ .$$

Un bref aperçu de cette attaque dans son application à un chiffrement itéré, de fonction de ronde g, constitué de k tours et utilisant des blocs de m bits est exposé ci-contre. Soient (M, M') un couple de messages clairs et $C_1, \ldots, C_{k-1}, C_k$ les chiffrés de M en sortie de chacune des k rondes *i.e.* $C_1 = g(M, K_1)$ et pour $i = 2, \ldots, k$, $C_i = g(C_{i-1}, K_i)$, « K_i » désignant la sous-clef utilisée dans la $i^{ième}$ ronde. On note $C'_1, \ldots, C'_{k-1}, C'_k$ les chiffrés correspondants pour M'. Le principe est alors de déceler un lien statistique entre $\Delta M = M \oplus M'$ et $\Delta C_{k-1} = C_{k-1} \oplus C'_{k-1}$ assez discriminant pour découvrir la sous-clef K_k du $k^{ième}$ tour. Afin de réaliser cela, on introduit le concept de *différentielle* ainsi qu'il suit :

Définition 2.8. Une *différentielle* sur k tours est la donnée d'un couple (α, β) tel que $\alpha = \Delta M$ et $\beta = \Delta C_k$.
On définit la probabilité de la différentielle (α, β) par

$$\Pr(\Delta \mathbf{C}_k = \beta | \Delta \mathbf{M} = \alpha)$$

sous l'hypothèse que le texte clair $\mathbf{M}$ et les sous-clefs $\mathbf{K}_1, \ldots, \mathbf{K}_k$ soient des variables aléatoires indépendantes uniformément distribuées.

L'attaque différentielle s'effectue alors en quatre étapes décrites dans l'algorithme ci-dessous.

1. Trouver une différentielle (α, β) au $k-1^{ième}$ tour telle que la probabilité

   $$\Pr(\Delta \mathbf{C}_{k-1} = \beta | \Delta \mathbf{M} = \alpha)$$

   soit très largement supérieure à l'équiprobabilité quand $\mathbf{M}$ est une variable aléatoire uniformément distribuée ;

2. Choisir aléatoirement un texte chiffré M et soumettre M et $M \oplus \alpha$ au chiffrement. On obtient alors deux couples clairs-chiffrés (M, C_k) et $(M' = M \oplus \alpha, C'_k)$;

3. Déterminer toutes les valeurs possibles K'_k de la dernière sous-clef telles que $g^{-1}_{K'_k}(M) \oplus g^{-1}_{K'_k}(M') = \beta$;

4. Itérer les étapes 3. et 4. jusqu'à ce que l'une des valeurs de K'_k apparaisse plus souvent que les autres. On considérera alors cette valeur comme étant effectivement la sous-clef de la $k^{ième}$ ronde.

On peut remarquer que l'attaque décrite ci-dessus se trouve être inefficace lorsque toutes les différentielles au $k-1^{ième}$ tour ont une fréquence d'occurrence proche de $\frac{1}{2^m}$. Les fonctions résistant le plus à cette attaque sont conformes avec cette dernière observation. Elles sont appelées fonctions *parfaitement non linéaires* ou *presque parfaitement non linéaires*. Nous y reviendrons très largement dans la trame de ce texte (voir infra, chapitre 5).

Principales généralisations
La cryptanalyse différentielle a été extrapolée de plusieurs manières. On peut par exemple citer les attaques introduites par Knudsen [Knu95] utilisant des différentielles d'ordre supérieur ou tronquées. Le premier type d'attaques repose, comme dans le cas de la cryptanalyse différentielle classique, sur une éventuelle faiblesse de la dérivée de la fonction de tour mais ce coup-ci dans une

dérivation d'ordre supérieur à 1. Les différentielles tronquées, quant à elles, relaxent certaines contraintes et ajoutent de la souplesse : seuls certains bits dans une différence sont imposés. Cette attaque a en particulier permis de casser une version d'IDEA réduite à 3,5 rondes (voir [BKR97]).

2.3.3.2 Cryptanalyse linéaire

Publiée en 1993 par Matsui [Mat94], la cryptanalyse linéaire permit à son auteur d'exhiber des attaques sur le DES à huit tours et même à seize tours dans certaines situations favorables. Dans cette attaque l'adversaire tente d'approximer la fonction de chiffrement à l'aide de relations linéaires entre ses entrées et ses sorties déduites par projections sur le corps fini $\mathbb{F}_2$.

Explicitons séance tenante cette méthode. Plaçons-nous encore une fois dans le cadre d'une attaque appliquée à un chiffrement par blocs - de longueur m - itéré. L'essence même de cette cryptanalyse consiste à découvrir un grand nombre de couples clairs-chiffrés, au tour k, (M, C_k) ainsi que trois vecteurs (α, β, γ), appelés *masques*, tels que pour la plupart des clefs de chiffrement K on ait

$$\alpha.M \oplus \beta.C_k \oplus \gamma.K = 0$$

où le symbole « . » désigne le produit scalaire canonique de $\mathbb{F}_2^m$. Afin de mener à bien une telle cryptanalyse il est impératif que la relation précédente soit satisfaite avec une probabilité P la plus éloignée possible (en valeur absolue) de la valeur $\frac{1}{2}$ (puisque $\gamma.K$ ne peut prendre que l'une des deux valeurs 0 ou 1). Dans ce cas l'attaque révèle un bit d'information de la clef K. La description de l'algorithme est donnée ci-dessous.

Pour N couples clairs-chiffrés (M, C_k), on compte le nombre N' de textes chiffrés C_k vérifiant la relation précédente lorsque $\gamma.K = 0$.

Si $N' > \frac{N}{2}$ alors

$$\text{si } \mathsf{P} - \frac{1}{2} > 0 \text{ alors } \gamma.K = 0 \text{ sinon } \gamma.K = 1$$

sinon si $N' < \frac{N}{2}$ alors

$$\text{si } \mathsf{P} - \frac{1}{2} > 0 \text{ alors } \gamma.K = 1 \text{ sinon } \gamma.K = 0 \ .$$

La résistance des fonctions booléennes contre l'attaque linéaire est formalisée sous les termes de fonction *courbe* ou *presque courbe*. Ces applications assurent aussi une défense optimale contre la cryptanalyse différentielle. Nous y reviendrons ultérieurement dans la suite de ce manuscrit (voir le chapitre 5) comme pour le concept homologue de fonction parfaitement non linéaire.

Principales généralisations
Parmi les généralisations possibles de la cryptanalyse linéaire on peut évoquer le cas de l'attaque différentielle-linéaire, combinant les deux précédentes méthodes, développée par Hellman et Langford [LH94]. Très sommairement il s'agit d'une attaque à texte clair choisi au cours de laquelle sont considérées des paires de messages clairs-chiffrés dont les bits sont partiellement approximés à l'aide de relations linéaires.

Une autre extension envisagée, connue sous le nom de cryptanalyse *différentielle généralisée*, réside dans la substitution des relations linéaires par des relations non linéaires binaires entre des

bits d'entrée et de sortie (voir [HKM97]).

En dernier lieu la cryptanalyse bilinéaire introduite par Courtois [Cou04] permet d'attaquer les systèmes de chiffrement basés exclusivement sur une structure de Feistel tels que le DES à l'aide d'approximations bilinéaires des parties gauche et droite des blocs clairs-chiffrés.

2.3.3.3 Autres attaques

Nous survolons succinctement à présent des attaques n'appartenant pas à l'une ou l'autre des deux familles précédentes. Il ne faut pas y voir un quelconque objectif d'exhaustivité ou d'universalité mais seulement la volonté de porter à la connaissance d'autres types importants de cryptanalyses.

L'attaque par interpolation dûe à Jacobsen et Knudsen [JK97] se fonde sur la formule d'interpolation de Lagrange dont l'énoncé est donné en regard. Soient $\mathbb{K}$ un corps et $m \in \mathbb{N}^*$. Soit $(x_1, \ldots, x_m, y_1, \ldots, y_m) \in \mathbb{K}^{2m}$ tel que $x_i \neq x_j$ pour tout $(i, j) \in \{1, \ldots, m\}^2$ tel que $i \neq j$. Alors il existe un et un seul polynôme $P \in \mathbb{K}[\mathtt{X}]$ de degré au plus $m-1$ tel que $P(x_i) = y_i$ pour tout $i \in \{1, \ldots, m\}$ et défini par

$$P(\mathtt{X}) = \sum_{i=1}^{m} y_i \prod_{\substack{1 \leq j \leq m \\ j \neq i}} \frac{\mathtt{X} - x_j}{x_i - x_j} \ .$$

Si la fonction de tour utilisée possède un degré algébrique[13] bas, on peut facilement l'approximer à l'aide d'une interpolation de Lagrange et en déduire une attaque sur la sous-clef de la dernière ronde.

Dans l'attaque par partitionnement, développée par C. Harpes et J. Massey [HM97], est exploitée une faiblesse décrite à l'aide d'une paire de partitions *i.e.* une partition de l'ensemble des textes clairs et une partition de celui des messages chiffrés du dernier tour telles que, pour chaque clef, les chiffrés du dernier tour ne sont pas uniformément distribués dans la seconde partition lorsqu'on tire au hasard des messages dans la première partition. Cette cryptanalyse, bien que non cataloguée au sein des généralisations de l'attaque différentielle, a des traits communs avec cette dernière. En effet l'ensemble des blocs de clairs différant de α constitue une partition particulière en sous-ensembles de deux éléments M et son translaté $M \oplus \alpha$. Il en est de même relativement aux blocs de chiffrés de la ronde $k-1$. On dispose donc des deux partitions comme dans le cadre de l'attaque de Harpes et Massey.

Enfin en 2002, Courtois et Pieprzyk ont introduit un type inédit d'attaque [CP02] exploitant des propriétés algébriques de boîtes-S. L'idée consiste à représenter chaque boîte-S par un système d'équations (non linéaires) où les bits de la clef représentent les inconnues du système (dans le cadre de cette attaque un certain nombre de messages clairs et chiffrés sont connus). De cette manière on peut rapporter tout le processus de chiffrement à un tel système d'équations. Sa résolution éventuelle permet alors de retrouver la clef utilisée.

2.4 Chiffrement à flot

Dans cette section nous introduisons le mécanisme de chiffrement à flot en nous focalisant sur l'utilisation et les propriétés des registres à décalage à rétroaction linéaire. En particulier nous décrivons leur comportement face à certaines attaques bien connues.

[13] Voir le chapitre 4, sous-section 4.3.2.2, p. 50 pour plus de précisions.

2.4.1 Description

En dehors du chiffrement par blocs, l'autre catégorie notable de cryptosystèmes est celle des chiffrements à flot ou à la volée. Fondamentalement le chiffrement à flot consiste à considérer les ensembles de messages clairs, de messages chiffrés et de clefs comme des sources discrètes d'information *i.e.* à chaque unité de temps, ou top d'horloge, est produite une quantité élémentaire d'information[14], parfois appelée *lettre* ou *symbole* d'un certain alphabet, par chacune des sources correspondantes. On retrouve du reste le même archétype de représentation de la cryptographie que celui de Shannon. Dans ce contexte, le chiffrement à flot est alors interprété comme un canal de communication discret entre la source des messages clairs et celle des cryptogrammes, bruitée par la présence de clefs. En d'autres termes, le chiffrement est simulé par l'effet du bruit sur une source. Ainsi à un temps donné n, la source des textes clairs produit une lettre m_n et celle des clefs produit k_n. Le texte chiffré correspondant est alors $c_n = f(m_n, k_n)$ où f est une certaine fonction représentant le bruit, soit en fait la fonction de chiffrement. Au top suivant $n+1$ de l'horloge sont produits de manière analogue m_{n+1}, k_{n+1} et $c_{n+1} = f(m_{n+1}, k_{n+1})$ et ainsi de suite. Finalement la suite de clefs $K = k_1\ k_2\ \ldots$ permet de crypter le message clair $M = m_1\ m_2\ \ldots$ suivant la règle

$$C = c_1\ c_2\ \ldots = f(m_1, k_1)\ f(m_2, k_2)\ \ldots$$

Bref, chaque symbole est chiffré à la volée.

Remarque 2.2. Le chiffrement par blocs peut s'interpréter comme un cas singulier du chiffrement à flot dans lequel la séquence des clefs est constante.

On se rappelle que le cryptosystème de Vernam, certes parfaitement sûr, est péniblement exploitable en pratique puisqu'il conduit à une gestion de clefs qui devient rapidement un handicap. En effet, à chaque chiffrement, une nouvelle clef, de même longueur que le message à crypter, doit être tirée au hasard et doit en outre être portée à la connaissance à la fois de l'expéditeur et du destinataire du message. Bref ce cryptosystème n'est pas pratique. Mais faut-il pour autant jeter ce type de cryptosystèmes[15] ? Non bien évidemment. Il faut l'adapter. Pour ce faire, les générateurs aléatoires sont utilisés afin d'engendrer à partir d'une courte suite binaire[16], considérée comme étant la clef de chiffrement, une chaîne, plus longue, de bits dont on exige qu'elle ressemble le plus possible à une suite d'aléas purs *i.e.* à une séquence de tirages à pile-ou-face indépendants. On n'entre pas dans l'étude détaillée de tous les générateurs (le lecteur intéressé pourra néanmoins se référer, par exemple, à [Lub96]) afin de concentrer nos efforts sur ceux basés sur les registres à décalage à rétroaction linéaire ou LFSR (de l'anglais « Linear Feedback Shift Register ») majoritairement utilisés en cryptographie.

Les *registres à décalage* permettent de générer ces séquences pseudo-aléatoires. Le principe de fonctionnement est de débuter avec une série de « cases mémoires » (le registre) remplie avec une donnée initiale de bits (chaque case contenant un et un seul bit) puis, à chaque cycle de temps, sont translatés (ou décalés), dans un sens préalablement fixé (vers la gauche ou vers la droite), les contenus des cases d'un cran vers une position adjacente. Un LFSR est quant à lui la donnée d'un registre à décalage, composé d'une suite de N cellules (ou cases) mémoires, et d'une suite de N bits $(\alpha_1, \ldots, \alpha_N)$ que l'on nomme *paramètres de rétroaction*. Supposons arbitrairement fixé à droite le sens de décalage du registre[17] et soient $s_n, s_{n+1}, \ldots, s_{n+N-1}$ les bits contenus dans le registre au temps n. Au $n+1^{ième}$ top, lors de la translation d'un cran vers la droite des contenus

[14] En règle générale les « atomes » d'information sont des bits puisque les sources communément considérées sont binaires.

[15] Avec ses clefs, le bébé et l'eau du bain.

[16] Souvent appelée *germe*.

[17] Dans la suite on conserve ce sens de décalage.

des cellules, le bit le plus à droite, s_n, est *émis*, c'est-à-dire copié sur le terme suivant de la suite pseudo-aléatoire, alors que la case la plus à gauche, laissée vide après translation de son contenu, reçoit le bit

$$s_{n+N} = \sum_{i=1}^{N} \alpha_i s_{n+N-i} \bmod 2 \ . \tag{2.1}$$

La suite pseudo-aléatoire finalement produite par le LFSR est donc $\{s_n\}_{n\in\mathbb{N}}$. On remarque que celle-ci dépend évidemment des contenus des cases du registre avant le premier cycle de temps, ce que l'on appelle l'*état initial* du registre et qui joue le rôle de clef de chiffrement. La suite engendrée est appelée *séquence de chiffrement*. Elle est en outre entièrement déterminée par l'état initial.

Exemple 2.5. Supposons un LFSR à trois cases, initialisé par $(s_2, s_1, s_0) = (1, 0, 0)$ (« s_0 » représentant le bit contenu dans la cellule la plus à droite) et de paramètres de rétroaction $(\alpha_1, \alpha_2, \alpha_3) = (0, 1, 1)$. La relation permettant la mise à jour du bit de la cellule la plus à gauche est donc $s_{n+3} = s_{n+1} \oplus s_n$. Au temps $n = 1$, le bit $s_0 = 0$ est émis, on décale le contenu de toutes les cases d'un cran vers la droite et la case la plus à gauche reçoit $s_3 = s_0 \oplus s_1 = 0$. Le contenu du registre, de gauche à droite, est donc $(0, 1, 0)$. Au temps $n = 2$ est produit le bit libéré par la case la plus à droite, soit s_1 et la case la plus à gauche reçoit donc $s_4 = 1$. En laissant s'exécuter mentalement ce système on s'aperçoit que le LFSR correspondant génère la suite périodique, de période 7, suivante

$$0010111\ 0010111\ 0010111\ 0010111\ \ldots$$

L'équation (2.1) est une *équation linéaire de récurrence d'ordre N* (voir [LN97] pour une étude approfondie) et la suite définie par cette même équation est appelée *suite récurrente linéaire binaire*. Pour une telle suite, il existe un LFSR qui l'engendre. Les paramètres de rétroaction d'un LFSR, à N cases et tel que $\alpha_N = 1$ et $\alpha_0 = 1$, sont fréquemment représentés par un polynôme de $\mathbb{F}_2[\mathtt{X}]$ de degré N dit *polynôme de rétroaction* et défini par

$$P(\mathtt{X}) = \sum_{i=0}^{N} \alpha_i \mathtt{X}^i \bmod 2 \ .$$

On définit alors la *complexité linéaire* $\Lambda(S)$ d'une suite $S = \{s_n\}_{n\in\mathbb{N}}$ donnée par une relation (2.1), comme le degré k du plus petit[18] polynôme de rétroaction d'un LFSR générant S. Un tel polynôme est appelé *polynôme de rétroaction minimal*. On établit immédiatement que la complexité linéaire de S est égale au plus petit[19] LFSR l'engendrant. Elle peut donc être interprétée comme le degré de difficulté pour générer une suite donnée. On appelle *ordre* d'un polynôme $P \in \mathbb{F}_2[\mathtt{X}]$ le plus petit entier n tel que P divise le polynôme $\mathtt{X}^n \oplus 1$. Un polynôme P à coefficients dans $\mathbb{F}_2$ est dit *primitif* si son coefficient constant vaut 1 et son ordre est $2^k - 1$ où k est le degré de P. La *période* d'une suite S est le plus petit rang k tel que $s_{n+k} = s_n$ pour tout n. Un résultat classique énonce alors que la période d'une suite engendrée par un LFSR de longueur N est maximale (et vaut $2^N - 1$) quand le polynôme de rétroaction est primitif (en particulier son degré vaut N). De plus sa complexité linéaire est elle aussi maximale (et vaut ainsi N).

La complexité linéaire est un paramètre déterminant pour la solidité cryptographique d'un LFSR. En effet comme nous allons le voir maintenant l'observation d'un petit nombre de bits seulement d'une suite S permet de la reconstituer entièrement lorsque $\Lambda(S)$ est petit.

[18] Au sens de la relation d'ordre naturelle sur les degrés.
[19] Au sens du nombre de cases mémoire - appelé *longueur* - du registre à décalage sous-jacent.

2.4.2 Algorithme de Berlekamp-Massey

Supposons utilisé à la volée, comme présenté en préambule, un cryptosystème de Vernam dans lequel la suite binaire (pseudo-)aléatoire, ou clef de chiffrement, S est fournie via un LFSR dont le polynôme de rétroaction est primitif de degré N et pour lequel l'état initial et les paramètres de rétroaction sont gardés secrets. Un texte M composé d'un certain nombre de bits m_n est chiffré à l'aide de S. On obtient donc un cryptogramme $C = \{c_n\}_n = \{m_n \oplus s_n\}_n$, séquence obtenue à partir de M par translation suivant S. Mettons-nous maintenant dans la peau d'un cryptanalyste chanceux puisque disposant des k bits de message clair $m_{n_0}, m_{n_0+1}, \ldots, m_{n_0+k}$ et de message chiffré correspondants $c_{n_0}, c_{n_0+1}, \ldots, c_{n_0+k}$ (où n_0 est un certain rang dans la séquence de chiffrement). Comme nous l'avons déjà vu, les k bits de même rang de la séquence de chiffrement S sont facilement identifiés (en faisant la somme modulo 2 bit à bit des parties des suites que l'on connaît). Ainsi si on cherche, par une méthode identique, à retrouver la clef de chiffrement utilisée, il est nécessaire de découvrir une période entière de S c'est-à-dire $2^N - 1$ bits et donc connaître $2^N - 1$ bits du texte clair M. Cependant en adaptant un algorithme développé par E. R. Berlekamp [Ber68] dans le cadre du décodage des codes BCH, J. L. Massey [Mas69] a montré que l'on peut inférer le plus petit LFSR générant une suite $S = \{s_n\}_{n\in\mathbb{N}}$ à partir uniquement d'une relativement faible (largement inférieure à $2^N - 1$) quantité de bits consécutifs de S. L'algorithme utilisé porte le nom de *Berlekamp-Massey* et son principe de fonctionnement est le suivant.

`Entrée` : une suite $s_0, \ldots, s_{n-1}$ de longueur n.
`Sortie` : polynôme de rétroaction et état initial du plus petit LFSR engendrant $s_0, \ldots, s_{n-1}$.
`Algorithme` : Pour i variant de 1 à n, on calcule par récurrence la longueur N_i et le polynôme de rétroaction P_i du plus petit LFSR qui engendre les i premiers bits de la suite.

Ainsi l'algorithme de Berlekamp-Massey permet-il de construire, pour un certain nombre n de valeurs successives d'une suite S, le plus petit LFSR engendrant les n bits connus de S. Le résultat énoncé par Massey est alors le suivant.

Théorème 2.3. [Mas69] *Soit $S = \{s_n\}_{n\in\mathbb{N}}$ une suite récurrente linéaire binaire. A partir de $2\Lambda(S)$ bits consécutifs de la suite, l'algorithme de Berlekamp-Massey détermine le plus petit* LFSR *qui engendre la suite.*

Intuitivement ce théorème met à jour la redondance dans une suite récurrente qui peut être immédiatement utilisée en cryptanalyse. Il en découle que l'on peut retrouver tous les bits d'une séquence de chiffrement S à l'aide simplement de la connaissance de $2N$ bits consécutifs de texte clair M au lieu des $2^N - 1$ par la méthode « grossière » précédemment décrite. Ceci démontre clairement, on en convient, le rôle majeur de le complexité linéaire de la suite utilisée pour la sûreté cryptographique. C'est ainsi que l'on privilégie volontairement l'utilisation d'un LFSR dont la complexité linéaire de la suite engendrée est égale à sa longueur (ce qui est possible si le polynôme de rétroaction est irréductible). De la sorte on se prémunit alors contre le fait de construire un LFSR plus court permettant d'engendrer la suite de bits.

2.4.3 Combinaison de plusieurs LFSRs

Alors même que l'on emploie un LFSR optimal c'est-à-dire dont le polynôme de rétroaction est primitif, la complexité linéaire de la suite générée reste bien souvent trop faible en pratique pour résister à une attaque utilisant l'algorithme de Berlekamp-Massey. Une solution apportée à ce problème consiste à utiliser m LFSRs en parallèle, générant chacun une suite binaire de faible complexité linéaire, et de combiner les différentes sorties à l'aide d'une fonction booléenne à valeur binaire $f : \mathbb{F}_2^m \to \mathbb{F}_2$ appelée *fonction de combinaison*. Si on dispose de m LFSRs et

que $x_1, \ldots, x_m$ sont les sorties respectives, leur combinaison par f est $f(x_1, \ldots, x_m)$. On souhaite alors que la suite obtenue par ce stratagème soit de complexité linéaire élevée.

Cadre théorique de l'approche par combinaison
Nous décrivons maintenant le contexte théorique validant la combinaison de plusieurs LFSRs. Remarquons immédiatement que la fonction f ne doit pas être choisie au hasard. Il faut, par exemple, éviter des cas dégénérés tels que les projections. Dans ce paragraphe, nous abordons entre autres choses plusieurs critères devant être satisfaits par f pour assurer un niveau convenable de solidité cryptographique.

En premier lieu, on utilise en priorité une fonction de combinaison *équilibrée*, *i.e.* qui prenne un nombre égal de fois les valeurs 0 et 1, afin d'éviter une attaque utilisant un éventuel biais statistique.

Intéressons-nous maintenant à la complexité linéaire de la suite produite par combinaison ce qui, rappelons-le, est un indicateur fondamental de la sécurité du système. Pour cela on commence par introduire l'objet suivant. La *forme algébrique normale* d'une fonction $f : \mathbb{F}_2^m \to \mathbb{F}_2$ est l'unique polynôme P_f de $\mathbb{F}_2[\mathtt{X}_1, \mathtt{X}_2, \ldots, \mathtt{X}_m]/(\mathtt{X}_1^2 \oplus \mathtt{X}_1, \ldots, \mathtt{X}_m^2 \oplus \mathtt{X}_m)$ tel que pour tout m-uplet $(x_1, \ldots, x_m)$ d'éléments de $\mathbb{F}_2$, on ait $f(x_1, \ldots, x_m) = P_f(x_1, \ldots, x_m)$. Le *degré* de f est alors défini comme le degré du polynôme P_f. Ces deux notions sont reprises au chapitre 4. Comme on peut identifier f et P_f, la suite générée par combinaison à l'aide de f, est composée de sommes et de produits de bits des suites produites par les m LFSRs en parallèle. Sa complexité linéaire dépend ainsi de celles des sommes et produits des bits des séquences de départ. Il faut donc disposer d'un moyen pour quantifier cette dépendance. Un certain nombre de résultats ont été développés en ce sens (voir [ZM73, RS86, GN94]). En particulier en voici un qui valide l'approche de combinaison parallèle de plusieurs LFSRs.

Proposition 2.1. [ZM73, RS86, GN94] *Soient $S = \{s_n\}_{n\in\mathbb{N}}$ et $S' = \{s'_n\}_{n\in\mathbb{N}}$ deux suites récurrentes linéaires binaires de polynômes de rétroaction minimaux P et P'. On définit les suites somme et produit terme à terme de S et S' respectivement par $S \oplus S' = \{s_n \oplus s'_n\}_{n\in\mathbb{N}}$ et $SS' = \{s_n s'_n\}_{n\in\mathbb{N}}$. Soient P et P' les polynômes de rétroaction minimaux respectifs. On a alors les résultats suivants concernant leur complexité linéaire.*

1. *$\Lambda(S \oplus S') \leq \Lambda(S) + \Lambda(S')$ avec égalité si et seulement si les polynômes P et P' sont premiers entre eux i.e. $pgcd(P, P') = 1$. De plus dans le cas de l'égalité la période de la suite somme est égale au plus petit multiple commun des périodes des suites S et S' ;*

2. *$\Lambda(SS') \leq \Lambda(S)\Lambda(S')$ avec égalité si les polynômes P et P' sont primitifs et si les complexités $\Lambda(S)$ et $\Lambda(S')$ sont premières entre elles i.e. $pgcd(\Lambda(S), \Lambda(S')) = 1$. Dans ce cas la période de la suite produit est égale au produit des périodes des suites S et S'.*

Pour m LFSRs dont les polynômes de rétroaction sont primitifs et de degrés $k_1, \ldots, k_m$ deux à deux premiers entre eux, les résultats précédents impliquent que la complexité linéaire Λ de la suite obtenue en combinant ces LFSRs avec une fonction $f : \mathbb{F}_2^m \to \mathbb{F}_2$ vérifie

$$\Lambda = P_f(k_1, \ldots, k_n)$$

où P_f est considéré comme un élément de $\mathbb{F}_2[\mathtt{X}_1, \ldots, \mathtt{X}_n]$ et est évalué sur des entiers (*i.e.* on plonge $\mathbb{F}_2$ dans $\mathbb{N}$ et on remplace les sommes modulo 2 par des sommes d'entiers).

Exemple 2.6. Le générateur de Geffe [Gef73] est défini par trois LFSRs dont les polynômes de rétroaction sont primitifs et de degrés k_1, k_2, k_3 deux à deux premiers entre eux. Ces registres

sont combinés par la fonction booléenne f dont la forme algébrique normale est

$$P_f(\mathtt{X}_1, \mathtt{X}_2, \mathtt{X}_3) = \mathtt{X}_1 \oplus \mathtt{X}_1\mathtt{X}_2 \oplus \mathtt{X}_2\mathtt{X}_3 \ .$$

La complexité de la suite produite par ce générateur est donc $k_1 + k_1k_2 + k_2k_3$.

Attaque par corrélation

On déduit donc du calcul de la complexité linéaire d'une suite produite par combinaison par une fonction, supposée équilibrée, que celle-ci doit de surcroît avoir un degré le plus élevé possible. Bien qu'essentiel ce résultat n'apporte pas une solution définitive au problème de sécurité des systèmes de chiffrement à flot car il existe un autre type de cryptanalyses développé par Siegenthaler [Sie84] appelé *attaque par corrélation*. Il s'agit d'un attaque à texte chiffré connu qui repose sur l'existence d'une éventuelle corrélation entre la sortie de la fonction de combinaison f et l'une de ses entrées. Pour fixer le contexte de cette cryptanalyse on suppose que le message clair est produit par une source d'information binaire sans mémoire dont la sortie vaut 0 avec une probabilité P_0. Cette probabilité étant ordinairement déterminée par la langue naturelle utilisée. L'attaque est alors basée sur le résultat probabiliste qui suit.

Théorème 2.4. [Sie84] *Soit la donnée de m* LFSR*s. Soit $\mathbf{S}^i = \{\mathbf{s}_n^i\}_{n\in\mathbb{N}}$ la variable aléatoire représentant la sortie du $i^{ème}$* LFSR*. Soit $f : \mathbb{F}_2^m \to \mathbb{F}_2$ une fonction de combinaison. Pour $i \in \mathbb{N}$ tel que $1 \leq i \leq m$, on note « P'_i » la probabilité $\Pr(f(\mathbf{X}_1, \ldots, \mathbf{X}_m) = \mathbf{X}_i)$ où $(\mathbf{X}_1, \ldots, \mathbf{X}_m)$ est un m-uplet de variables aléatoires mutuellement indépendantes et uniformément distribuées sur $\mathbb{F}_2$ et* Pr *est la mesure d'équiprobabilité sur $\mathbb{F}_2$. Soient $c_1, \ldots, c_N$, N bits du texte chiffré. Alors la corrélation $\boldsymbol{\alpha}_i$ entre le chiffré et la sortie $\mathbf{S}^i$ du $i^{ème}$* LFSR *définie par*

$$\boldsymbol{\alpha}_i = \sum_{n=1}^{N} (-1)^{c_n + \mathbf{s}_n^i}$$

est une variable aléatoire gaussienne de moyenne $N(2\mathsf{P}_i - 1)$ et de variance $\sigma_i^2 = 4N\mathsf{P}_i(1 - \mathsf{P}_i)$ où $\mathsf{P}_i = 1 - \mathsf{P}_0 - \mathsf{P}'_i + 2\mathsf{P}_0\mathsf{P}'_i$.
De même la corrélation $\boldsymbol{\alpha}_0$ entre le chiffré et une suite aléatoire $\mathbf{S}^0$ indépendante de $\mathbf{S}^1, \ldots, \mathbf{S}^m$ est une variable aléatoire de moyenne 0 et de variance $\sigma_0^2 = N$.

Le biais statistique, représenté par la corrélation $\boldsymbol{\alpha}_i$, est utilisé afin de mener l'attaque comme suit. On parcourt toutes les initialisations possibles pour le $i^{ème}$ LFSR en calculant pour chacune d'elles la corrélation entre le chiffré supposé connu et la suite générée par ce LFSR afin de distinguer l'initialisation correcte. En effet si l'initialisation du LFSR en question est inexacte, la valeur calculée correspond à la corrélation entre le cryptogramme et une séquence aléatoire indépendante des entrées de f et vaut donc en moyenne 0 et, en revanche, si l'initialisation du LFSR est correcte la valeur de la corrélation est égale à $N(2\mathsf{P}_i - 1)$. La distinction entre les deux valeurs est alors possible dès que $\mathsf{P}_i \neq \frac{1}{2}$ soit encore $\mathsf{P}'_i \neq \frac{1}{2}$.

Résistance à l'attaque par corrélation

Afin de déduire des indications précédentes les fonctions booléennes offrant la résistance optimale face à ce type d'attaques, on introduit la notion suivante. Une fonction $f : \mathbb{F}_2^m \to \mathbb{F}_2$ est dite *sans corrélation d'ordre k* si pour tout ensemble $I \subset \{1, \ldots, m\}$ tel que $|I| = k$ et pour tout $(x_1, \ldots, x_k) \in \mathbb{F}_2^k$, $\Pr(f(\mathbf{X}_1, \ldots, \mathbf{X}_m) = 1 | \forall i \in I,\ \mathbf{X}_i = x_i) = \Pr(f(\mathbf{X}_1, \ldots, \mathbf{X}_m) = 1)$. Clairement une fonction f est sans corrélation d'ordre k si sa distribution de probabilité demeure inchangée lorsque l'on fixe k quelconques de ses entrées soit, en d'autres termes, le fait de ne faire varier que $m - k$ variables ne dévoile pas d'information sur la sortie. Finalement pour qu'une fonction de combinaison résiste à l'attaque par corrélation il faut qu'elle ait un ordre de non corrélation assez élevé. Cette notion est revue au chapitre 4.

2.5 Conclusion

Dans ce chapitre nous avons évoqué avec suffisamment de détails certaines notions d'ordre général de la cryptologie. Nous avons donc débuté ce manuscrit comme un exposé du corpus des idées fondatrices de la *science du secret*. Ainsi, en particulier, furent présentées les deux faces antagonistes de la cryptologie : son avers, la cryptographie et son revers, la cryptanalyse. On ne peut en effet concevoir la cryptographie sans son pendant la cryptanalyse. L'un permet de créer des systèmes de chiffrement quand l'autre en étudie la fiabilité. Bien que concurrentes, ces deux notions ne sont pas antinomiques mais bien complémentaires. Elles ne sont rien l'une sans l'autre. Seule leur alliance forme l'unité qu'est la cryptologie. C'est dans cette dualité que nous avons exposé conjointement les techniques mises en œuvre dans la réalisation des cryptosystèmes ainsi que les attaques, connues à ce jour, qu'ils peuvent subir. Dans la suite de ce manuscrit nous retrouvons cette dualité. Les notions abstraites introduites au fil de cette thèse peuvent en effet s'interpréter comme critères de résistance à certaines attaques.

Ce premier chapitre à première vue assez classique tant dans son contenu que dans la trame suivie, possède, à y regarder de plus près, une particularité au sein de cette thèse. Son style, dépouillé d'une grande part de la rigueur mathématique, est rapidement abandonné. En effet dès le prochain chapitre nous faisons le choix, autant que faire se peut, d'aborder les problèmes rencontrés, du point de vue du mathématicien qui ferait de la cryptographie et non l'inverse. Mais ne vous méprenez pas ! Nous ne négligeons pas l'aspect cryptographique des développements présentés, seulement nous évoluons dans un plan théorique où seule la Mathématique peut servir de conseiller. Cela est fait dans un souci d'exactitude et de complétude scientifique et n'a pas pour objectif de rebuter le lecteur. C'est en tout cas ce que nous espérons.

Le rôle de ce premier chapitre est donc de porter à la connaissance du lecteur le cadre général dans lequel les recherches théoriques, ultérieurement présentées, sont élaborées. Un premier chapitre de thèse, en général, se prête donc bien à l'utilisation d'une tournure verbeuse de l'écriture. Plonger directement le lecteur dans trop de détails peut être autant superflu que contre-productif. Le premier chapitre doit ainsi amener le lecteur dans le monde abstrait (et psychotique ?) des idées de l'auteur mais graduellement, sans à-coups. Il s'apparente donc à un train qui démarre doucement du quai de sa gare de départ et accélère progressivement pour ne pas indisposer le voyageur dans un si long trajet. Si vous voulez une autre image, un premier chapitre c'est comme un coureur de fond : pour aller loin, il doit commencer tranquillement. Par ailleurs cette approche s'avère très avantageuse pour l'auteur puisqu'elle l'autorise à introduire subtilement certains termes qui prendront toute leur importance au cours de ce manuscrit. Ainsi, par exemple, nous avons fait allusion à plusieurs reprises au mot « translation » qui, moralement, constitue l'essence même des travaux que vous allez découvrir avec intérêt, nous l'espérons, sinon avec plaisir.

Mais pour l'heure il est temps de conclure ... cette conclusion et de mettre un terme à ce premier chapitre par la même occasion.

Le train repart. Direction le second chapitre. Nous vous souhaitons un bon voyage en notre compagnie.

Première partie

Non linéarité parfaite et fonction courbe

Introduction

Une plus grande connaissance
pourrait éclairer notre chemin.

GEORGES LUCAS, *La Guerre des Etoiles - Episode III*

Les transactions commerciales, via un réseau informatique public, nécessitent, à l'évidence, un environnement hautement sécurisé. On conçoit aisément que certaines données bancaires personnelles, telles qu'un numéro de compte ou un code PIN de carte bleue, ne doivent en aucun cas être portées à la connaissance d'une tierce personne ; le risque de fraude étant alors trop grand et presque inéluctable. Aussi l'éclosion de nombreuses innovations cryptographiques a été favorisée par ce contexte très sensible. Mais le doute dans ce domaine financier n'est pas permis, seules comptent les certitudes. Ainsi des critères de solidité des algorithmes de chiffrement, universellement admis, ont été développés afin d'apporter la confiance nécessaire à une utilisation axée sur le commerce électronique. Les cryptosystèmes alors implémentés sur des plates-formes informatiques se fondent fréquemment sur l'exploitation de fonctions booléennes c'est-à-dire ces fonctions mathématiques à valeurs dans l'ensemble $\{0,1\}$. Les principes de sécurité se traduisent ainsi en termes de propriétés abstraites que doivent satisfaire ces applications.

La très grande quantité de données circulant sur les réseaux fait en sorte que les recommandations, concernant la sécurité des échanges, s'appuient systématiquement sur des critères statistiques. L'objectif étant de réduire au maximum les failles, dans la conception des fonctions booléennes, potentiellement exploitables par des cryptanalyses. Au nombre des attaques les plus efficaces, on compte les cryptanalyses différentielle et linéaire. Aussi les fonctions, manipulées au sein des systèmes de chiffrement à clef secrète, doivent exhiber la meilleure résistance possible envers ces deux catégories d'attaques. En conséquence, ce critère devient décisif pour la réalisation concrète de cryptosystèmes sûrs *a priori*, entraînant dans son sillage un certain nombre de développements théoriques fondamentaux telles que les notions de non linéarité parfaite et de fonction courbe qui garantissent la sécurité maximale face à une attaque respectivement différentielle et linéaire.

Intuitivement une fonction booléenne parfaitement non linéaire est une fonction qui ressemble le moins possible à une application affine. Plus exactement, la fonction booléenne f à m variables binaires est parfaitement non linéaire si pour chaque α vecteur non nul de m bits, la fonction

$$x \mapsto f(x) \oplus f(x \oplus \alpha)$$

prend un nombre de fois égal les valeurs 0 et 1. Les fonctions booléennes courbes sont ces fonctions à un nombre pair, m, de variables dont la transformée de Walsh est de valeur absolue constante égale à $2^{\frac{m}{2}}$. Elles représentent ainsi des signaux dont le spectre fréquentiel ne comporte que deux valeurs, à savoir $\pm 2^{\frac{m}{2}}$. Ces deux notions, bien que chacune de définition simple, sont tellement

fortes que les fonctions les vérifiant sont des êtres relativement rares. En outre, à l'aide d'une formule dite de *conservation de l'énergie* bien connue, la relation de Parseval, on peut lier ces deux propriétés et prouver qu'elles sont équivalentes.

Ces diverses constatations ont ainsi motivé l'intérêt que nous portons à ces fascinant objets, à la fois combinatoires et algébriques, dont la portée cryptographique est indéniable. Aussi l'intégralité de la première partie de ce manuscrit est-elle entièrement dévolue à leur étude précise et complète dans laquelle nous reprenons de nombreux travaux sur le sujet. De la sorte, cette fraction du document peut s'entendre comme un vaste état de l'art sur les fonctions parfaitement non linéaires et courbes alors que, dans la seconde partie, sont exposés nos résultats originaux fondés sur des généralisations de ces notions et justifiant ainsi amplement le contenu de cette première partie.

Cette première partie débute par un court chapitre dédié à l'ensemble des notations en rapport avec les concepts pré-requis pour la bonne compréhension du manuscrit. Suite à cela, les principales propriétés cryptographiques des fonctions booléennes, autres que la non linéarité parfaite et le fait d'être courbe, sont exposées au chapitre 4. Nous présentons aussi, dans ce même chapitre, la transformée de Fourier dans le contexte des espaces vectoriels sur $\mathbb{F}_2$ qui est un outil fondamental pour l'étude des fonctions booléennes. Puis les deux concepts qui sont au cœur de cette thèse, les fonctions parfaitement non linéaires et courbes, sont très largement dépeints, d'abord dans le monde booléen au chapitre 5 et dans des cadres plus abstraits au cours du chapitre 6. Nous présentons ainsi les généralisations de ces notions au cas des groupes finis commutatifs réalisées par Carlet, Ding, Logachev, Salnikov et Yashchenko, au cas de l'arithmétique modulaire suivant les travaux de Nyberg, Kumar, Scholtz et Welch et, finalement, dans le contexte des groupes finis par Ambrosimov. Notons que nous rappelons, dans ce dernier chapitre de cette première partie, la dualité des groupes finis commutatifs et la transformée de Fourier dans ce contexte ; ces concepts étant très amplement exploités dans la seconde partie du manuscrit.

Conseil de lecture : Un lecteur spécialiste de la question des fonctions booléennes en cryptographie et, plus sûrement, des concepts de fonction parfaitement non linéaire et courbe, peut éventuellement ne consacrer son attention qu'au chapitre 6 et principalement à ses sections 6.2, 6.3 et 6.4 dans lesquelles sont exposées des notions indispensables à l'intelligibilité de la seconde partie.

Chapitre 3

Notations

Tu t'appelles « Lebowski »,
Lebowski !

Joel & Ethan Coen, *The Big Lebowski*

Sommaire

3.1 Introduction

Avant d'entrer dans le vif du sujet, sont exposées, dans ce chapitre, les notations générales valables dans l'intégralité de ce manuscrit. Bien que fixées dès maintenant, elles sont, pour certaines d'entre elles, rappelées à plusieurs reprises dans le document.

Nous supposons préalablement connus les concepts dont nous arrêtons dès à présent les notations. Ainsi seules les notions classiques de base sont mentionnées ici. Par conséquent, ce chapitre ne contient pas toutes les notations établies dans ce manuscrit mais seulement le fragment le plus fondamental.

Dans la mesure du possible, les notations choisies sont en accord avec l'usage traditionnel des mathématiques. Ceci ayant pour cause qu'un même symbole dénote parfois plusieurs objets distincts. Plutôt que de lever ces ambiguïtés en introduisant des signes supplémentaires, nous préférons prévenir le lecteur le cas échéant.

Nous divisons rationnellement ce chapitre en deux parties d'inégales longueurs. Dans la première, la plus courte, est établie une convention d'appelation des expressions linguistiques. Dans la seconde nous fixons un certain nombre de notations, des plus générales à celles un peu plus particulières, acquises pour la suite du texte.

A un lecteur au fait des notions classiques évoquées ici, nous ne pouvons que lui conseiller de se diriger directement vers le chapitre 4 concernant les propriétés cryptographiques des fonctions

booléennes. Toutefois, en cas de doute sur une notation, il lui suffira soit de brièvement revenir ici soit de consulter dans l'annexe A la table des notations.

3.2 Remarques préliminaires

Les règles de grammaire exigent qu'une phrase ne contienne jamais l'objet auquel des expressions se réfèrent, mais seulement son nom. Il est par exemple clair que lorsque nous parlons d'une ville, nous n'introduisons pas la ville elle-même dans notre phrase, mais son nom ; de même, si nous voulons dire quelque chose à propos d'un mot (ou d'un autre signe linguistique), ce n'est pas le mot lui-même (ou le signe) qui peut entrer dans notre phrase, mais seulement son nom. Cette distinction est subtile, mais bien fondée et riche de conséquences (la démonstration du fameux théorème de Gödel [GGN+89] en est une preuve flagrante).

Pour construire le nom d'une expression linguistique, la convention veut qu'on la place entre guillemets. Notre texte se plie à cette convention. Il est correct[1] d'écrire :

Marseille est la capitale du football.

Mais il est incorrect d'écrire :

Marseille s'écrit avec neuf lettres.

Il faut écrire dans ce cas :

« Marseille » s'écrit avec neuf lettres.

De même, il ne faut pas écrire :

□ est un symbole,

mais :

« □ » est un symbole.

Remarque 3.1. L'utilisation de la police de caractère *italique* ou un saut de ligne sont équivalents à la mise entre guillemets pour nommer un signe. Ainsi on peut écrire :

Marseille s'écrit avec neuf lettres.

mais aussi :

le nom propre
Marseille
s'écrit avec neuf lettres.

3.3 Notations générales

3.3.1 Notations métamathématiques

La convention grammaticale étant fixée, il nous faut aussi signaler que la logique (informelle) utilisée dans ce manuscrit est le calcul des prédicats au premier ordre standard (avec identité).

Introduisons deux premières notations : le symbole « □ » marque la *fin d'une preuve* alors que le symbole « $\stackrel{déf.}{=}$ » correspond à l'*égalité par définition*.

[1] C'est vrai aussi pour les gens du Midi.

Les signes « $\Leftrightarrow$ » et « $\Rightarrow$ » dénotent respectivement l'*équivalence* et l'*implication* logiques.

Les symboles logiques « $=$ » et « $\neq$ » possèdent quant à eux leur sémantique classique.

Les quantificateurs universel et existentiel sont notés respectivement « $\forall$ » et « $\exists$ ». Pour dénoter l'existence et l'unicité on utilise le symbole « $\exists\,!$ ».

Nous introduisons à présent la liste des variables méta-linguistiques, *i.e.* les lettres, utilisées pour dénoter des objets mathématiques quelconques. La convention voulant qu'à ces signes, normalement dénués de sens, soit attribué un rôle particulier dans la désignation d'un type donné d'entités. Ainsi, par exemple, on préfère l'usage de la lettre « m » à celui de la lettre « π », réservé préférentiellement aux permutations, pour la désignation d'un entier quelconque. Observons que toutes les lettres seront susceptibles d'être indicées, de posséder un exposant ou encore d'être accentuées par divers signes. Aussi nous ne listons que les lettres seules, dépourvues de leurs éventuels attributs supplémentaires. Notons enfin que la casse des lettres est évidemment respectée.

Les lettres de l'alphabet latin

Les lettres capitales de police penchée

- « A », « B », « I », « J », « X » et « Y » désignent des ensembles quelconques (« A » étant essentiellement utilisée pour nommer des sous-ensembles, « B » pour désigner une base quelconque d'un espace vectoriel et « I » et « J » pour des ensembles (finis) d'indices) ;
- « D » permet de désigner des ensembles à différences ;
- « G » et « H » représentent des groupes quelconques ;
- « M » désigne une matrice ;
- « P » parcourt les polynômes (et désigne, en deux occasions seulement dans ce manuscrit, un prédicat logique quelconque) ;
- « V » et « W » dénotent des espaces vectoriels.

La lettre majuscule « $\mathcal{K}$ » désigne une classe quelconque de fonctions courbes. Les lettres « $\mathcal{B}$ », « $\mathcal{C}$ », « $\mathcal{D}$ », « $\mathcal{E}$ », « $\mathcal{P}$ » et « $\mathcal{Q}$ » sont aussi utilisées pour désigner certains ensembles ou classes de fonctions courbes (et assimilées).

La lettre majuscule « $\boldsymbol{\mathcal{O}}$ » dénote une orbite suivant une action de groupe.

Les lettres capitales « L », « P » et « R » dénotent des bornes inférieures ou supérieures.

La lettre de graphie capitale, dans sa fonte grasse, « $\mathbf{X}$ » parcourt les variables aléatoires.

La lettre capitale de police `courier`, souvent indicée, « $\mathtt{X}$ » représente des indéterminées.

Les lettres majuscules « $\mathbb{K}$ » et « $\mathbb{F}$ » sont des noms pour les corps. Les lettres « $\mathbb{N}$ », « $\mathbb{Z}$ », « $\mathbb{Q}$ », « $\mathbb{R}$ » et « $\mathbb{C}$ » sont utilisées comme de coutume.

La lettre majuscule « $\Im$ » est réservée pour désigner les automorphismes intérieurs ou une opération de conjugaison ;

Les caractères minuscules de police penchée
- « e » désigne un élément quelconque d'une base d'un espace vectoriel ;
- « f », « g » et « h » dénotent des fonctions quelconques ;
- « i » et « j » représentent des indices entiers (ces lettres sont souvent employées comme variables muettes) ;
- « k », « m », « n » et « v » désignent des entiers naturels quelconques ;
- « l », toujours indicé, dénote une forme linéaire ;
- « p » représente un entier premier ;
- « x », « y » et « z » sont prioritairement utilisés afin de désigner des variables muettes apparaissant comme variables de fonctions, comme variables dans une somme ou encore comme inconnues d'une équation. Ils sont aussi utilisés pour nommer des éléments quelconques d'un ensemble donné.

Les lettres minuscules grasses « $\mathbf{g}$ », « $\mathbf{h}$ » et « $\mathbf{k}$ » dénotent des éléments d'un groupe utilisés en tant que variables d'une action de groupe ou d'une représentation linéaire.

Les lettres minuscules de fonte `courier` « `e` » et « `z` » désignent respectivement le nombre transcendant *exponentielle de* 1 et un nombre complexe quelconque.

La lettre « $\imath$ » désigne le nombre imaginaire pur tel que $i^2 = -1$.

Les lettres de l'alphabet grec

Les bijections sont dénotées par la lettre « Θ ». Les homomorphismes (entre certaines structures) sont désignés par « Ψ » alors que les isomorphismes le sont par « Φ ».

Les lettres minuscules du début de l'alphabet, « α », « β », « γ », etc. représentent des éléments d'un certain ensemble. Elles sont souvent employées comme variables de la transformée de Fourier d'une fonction ou encore en tant que paramètres (*i.e.* constantes indéterminées) d'une fonction.

Les lettres « λ » et « δ » désignent respectivement des applications linéaires et affines. A noter que la lettre « λ » représente aussi classiquement le troisième paramètre d'un ensemble à différences.

La lettre « χ » désigne un caractère quelconque.

Les caractères « φ » et « ψ » nomment des fonctions à valeurs dans $\mathbb{R}$ ou $\mathbb{C}$.

La lettre « ϕ » représente une action de groupe.

La lettre « ρ » désigne une représentation linéaire de groupe.

Les lettres « π », « σ » et « τ » dénotent des permutations quelconques. Les translations sont en particulier désignées par les deux dernières lettres. Remarquons que les involutions sont spécifiquement notées par les lettres grasses « $\boldsymbol{\sigma}$ » et « $\boldsymbol{\tau}$ ».

La lettre « κ » permet de désigner un automorphisme de corps.

La lettre « ω » permet de nommer des racines de l'unité dans $\mathbb{C}$.

Nous utilisons le symbole gras « $\boldsymbol{\pi}$ » afin de désigner le nombre irrationnel *pi* (rapport entre le périmètre d'un cercle et son diamètre en géométrie euclidienne).

3.3.2 Notations ensemblistes

Nous nous basons sur l'axiomatique ZMC[2] de la théorie des ensembles.

Les ensembles sont écrits soit en *intention* sous la forme « $\{P_1|P_2\}$ » où « P_1 » et « P_2 » désignent des prédicats, soit en *extension* sous la forme « $\{x_1, \ldots, x_m\}$ ».

Les symboles « $\in$ » et « $\notin$ », possèdent leur sémantique classique.

Les symboles « $\cup$ », « $\cap$ » et « $\setminus$ » désignent respectivement l'union, l'intersection et la soustraction ensemblistes. La réunion généralisée est dénotée par « $\bigcup$ ». Le symbole « $\times$ » dénote pour sa part le produit cartésien. Le symbole « $\subset$ » désigne l'inclusion ensembliste au sens *large*.

L'ensemble vide est noté « $\emptyset$ ».

L'infini est désigné par « ∞ ».

Pour X et Y deux ensembles non vides, on introduit les notations suivantes :

- Soit $m \in \mathbb{N}^*$. Soient $X_1, \ldots, X_m$ m ensembles (distincts ou non). Si $x \in X_1 \times \ldots \times X_m$ alors pour $i \in \{1, \ldots, m\}$, « x_i » désigne la $i^{éme}$ *coordonnée* (ou $i^{éme}$ *projection* de x) et, évidemment, $x = (x_1, \ldots, x_m)$;

- Y^X est l'ensemble des fonctions[3] de X dans Y. On utilise aussi pour $f \in Y^X$, la notation classique « $f : X \to Y$ ». La correspondance fonctionnelle entre $x \in X$ et $f(x) \in Y$ est notée « $x \mapsto f(x)$ ». La *composition* des applications est notée par le symbole « $\circ$ » ;

- Si $A \subset X$ et $f \in Y^X$ définie sur A tout entier alors $f(A)$ est l'*image* de A par f *i.e.* $\{f(x) \in Y | x \in A\}$ et la notation « $f|_A$ » désigne la restriction à l'ensemble A de f *i.e.* la

[2]La théorie axiomatique des ensembles « standard » comporte neuf axiomes. Ces axiomes ont été énoncés par Zermelo (1908) et complétés dans les années 1920 par Fraenkel et Skolem. Ils sont dits de Zermelo-Fraenkel et comprennent l'axiome du Choix, d'où le sigle « ZFC » souvent employé pour désigner cette théorie. L'œuvre de l'association Bourbaki a été développée dans ce cadre axiomatique.

[3]Dans ce manuscrit nous abusons du langage en considérant la plupart du temps les termes « fonction » et « application » comme étant synonymes. Les rares fois pour lesquelles ce n'est pas le cas nous indiquons l'ensemble de définition.

fonction définie sur A telle que $\forall x \in A$, $f|_A(x) = f(x)$. Si A' est un sous-ensemble de Y^X et $A \subset X$, on définit parfois $A'(A) \stackrel{déf.}{=} \{f(x) \in Y | f \in A',\ x \in A\} = \bigcup_{f \in A'} f(A)$;

- Soit $m \in \mathbb{N}^*$. Soient $(Y_1, \ldots, Y_m)$ un m-uplet d'ensembles et $f : X \to Y_1 \times \ldots Y_m$. Alors pour $i \in \{1, \ldots, m\}$, « f_i » désigne la $i^{éme}$ fonction coordonnée de f. En particulier $f_i : X \to Y_i$ et pour tout $x \in X$, $f(x) = (f_1(x), \ldots, f_m(x))$;

- $S(X)$ est le *groupe des permutations* (ou *groupe symétrique* si X est fini) de X *i.e.* l'ensemble des bijections de X dans lui-même. $Id_X \in S(X)$ est l'*application identité* de X. Si $\pi \in S(X)$, on définit pour $k \in \mathbb{N}$, $\pi^k \stackrel{déf.}{=} \underbrace{\pi \circ \ldots \circ \pi}_{k\ fois}$ avec par convention, $\pi^0 \stackrel{déf.}{=} Id_X$;

- Soit $A \subset X$, $A^c \stackrel{déf.}{=} X \setminus A$, $\mathbf{1}_A$ est la *fonction indicatrice* de A *i.e.* $\mathbf{1}_A : X \to \mathbb{R}$ définie par

$$x \mapsto \mathbf{1}_A(x) = \begin{cases} 1 & \text{si } x \in A\ , \\ 0 & \text{si } x \notin A\ , \end{cases}$$

  et si A est en outre fini, $|A|$ est son *cardinal*. Que A soit fini ou non, une suite d'éléments d'un certain ensemble indicée par A est notée sous la forme « $\{y_i\}_{i \in A}$ » ;

- Si $f \in Y^X$, f^{-1} est l'*image réciproque ensembliste* de f. Si f est en outre bijective, f^{-1} est aussi sa bijection réciproque. Si X est fini et « Pr » dénote une loi de probabilité sur X alors la *mesure de probabilité induit*e par f sur Y est désignée par « $\Pr_f$ » telle que pour tout $A \subset Y$ par $\Pr_f(A) \stackrel{déf.}{=} \Pr(f^{-1}(A))$;

- Si $A \subset \mathbb{R}$ est fini, $\min A$ (respectivement $\max A$) est la *borne inférieure* (respectivement la *borne supérieure*) de A. Si $\varphi : X \to \mathbb{R}$ et $A \subset X$, $\min_{x \in A} \varphi(x) \stackrel{déf.}{=} \min\{\varphi(x) \in \mathbb{R} | x \in A\}$ et $\max_{x \in A} \varphi(x) \stackrel{déf.}{=} \max\{\varphi(x) \in \mathbb{R} | x \in A\}$.

Lorsqu'un ensemble est muni d'une structure (de groupe, d'espace vectoriel, etc.), par abus de notation, on confond souvent celle-ci avec son ensemble sous-jacent.

Si l'ensemble X est muni d'une loi de composition interne, on note « $\sum$ » l'opération généralisée associée dans le cas d'une notation additive et « $\prod$ » dans le cas d'une notation multiplicative. Observons que l'on a deux exceptions à cette règle (voir la sous-section 3.3.5 et le chapitre 4 section 4.2 p. 46). Lorsque l'ensemble dispose de deux lois dont une multiplication, cette dernière est désignée à l'aide des symboles « $\times$ » ou « . » ou encore une absence de symbole lorsqu'elle ne dispose pas d'un nom particulier.

Enfin par convention de *bonne définition*, la notation « X^m », pour le produit cartésien, implique implicitement que $m \in \mathbb{N}^*$. De même dès que f est une fonction, on suppose que ses ensembles de départ et d'arrivée sont non vides.

3.3.3 Notations pour les ensembles de nombres

Avant tout, les symboles « $<$ », « $>$ », « $\leq$ » et « $\geq$ » possèdent leur sens classique comme relations d'ordre dans un $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ ou $\mathbb{R}$.

Dans les ensembles de nombres, $\mathbb{C}$ y compris, les symboles « $+$ », « $-$ » et « $\times$ » désignent les opérations de base sur les nombres et $\frac{x}{y}$ est évidemment une fraction. L'expression « $\pm x$ » pour

un nombre x est une abréviation commode pour l'expression « $+x$ ou $-x$ ».

Si $x \in \mathbb{R}$, $|x|$ est alors sa *valeur absolue*. Si $y \in \mathbb{R}$, « x^y » désigne l'expression « x *puissance* y » et, en particulier, « $\sqrt{x}$ » désigne l'expression « $x^{\frac{1}{2}}$ ». Si $\mathtt{z} \in \mathbb{C}$, « $|\mathtt{z}|$ » désigne son *module* et « $\overline{\mathtt{z}}$ » son *conjugué complexe*. La valeur de l'*exponentielle complexe* pour $\mathtt{z}$ est notée « $\mathtt{e}^{\mathtt{z}}$ ».

Par ailleurs on utilise les notations combinatoires classiques « $n!$ » et « C_n^k ».

3.3.4 Notations pour les groupes

Soit G un groupe.

- Nous désignons génériquement par « e_G » son *élément neutre* lorsque nous ne disposons pas de nom particulier pour celui-ci ;
- On a $G^* \stackrel{déf.}{=} G \setminus \{e_G\}$;
- Le symbole « $\top$ » désigne une loi de composition interne de groupe quelconque. Elle est toujours interprétée multiplicativement. Une loi additive quelconque est notée « $+$ » ;
- Soit $x \in G$. Les symboles « $-x$ » et « x^{-1} » désignent l'inverse de x dans G lorsqu'il est respectivement noté additivement ou multiplicativement ;
- Si H est un sous-groupe distingué de G, on note « G/H » le *groupe quotient* ;
- L'ensemble des automorphismes (de groupe) de G est désigné par « $Aut(G)$ ». C'est un groupe pour la loi $\circ$, sous-groupe de $S(G)$;
- Si H est un groupe, le *noyau* d'un homomorphisme Ψ de groupes de G dans H *i.e.* $\{x \in G | \Psi(x) = e_H\}$ est noté « $\ker(\Psi)$ » ;
- Le produit direct des groupes G et H est simplement noté « $G \times H$ » ;
- Si $x \in G$, on note « $\langle x \rangle$ » le sous-groupe *engendré* par x ;
- Si G est noté additivement, sa loi étant dénotée par le signe « $+$ », pour $(x, y) \in G^2$, « $x - y$ » est une abréviation pratique pour l'expression « $x + (-y)$ » ;
- Si en outre $(G, \top)$ est un groupe commutatif, on définit pour $\alpha \in G$, la *translation* par α :

$$\begin{array}{rccc} \sigma_\alpha : & G & \to & G \\ & x & \mapsto & x \top \alpha \ . \end{array}$$

  Le groupe (pour la loi $\circ$) des translations de G est noté « $T(G)$ ». C'est un sous-groupe de $S(G)$ isomorphe à G lui-même.

3.3.5 Notations pour les espaces vectoriels

Pour $\mathbb{K}$ un corps, V_1 et V_2 deux $\mathbb{K}$-espaces vectoriels de dimensions finies :

- Le vecteur nul de V_1 est noté « 0_{V_1} » ;

- La *dimension* de V_1 sur $\mathbb{K}$ est désignée par « $\dim_{\mathbb{K}}(V_1)$ » ;

- $\mathcal{L}(V_1, V_2) \subset V_2^{V_1}$ est le $\mathbb{K}$-espace vectoriel des applications $\mathbb{K}$-linéaires de V_1 dans V_2. On note « $End(V_1)$ » l'ensemble $\mathcal{L}(V_1, V_1)$ des *endomorphismes* (linéaires) de V_1. Enfin on note le *groupe linéaire* de V_1 (*i.e.* l'ensemble des applications linéaires bijectives de V_1 dans lui-même) par « $GL(V_1)$ » ;

- Si $\lambda \in \mathcal{L}(V_1, V_2)$, on note, comme dans le cas des groupes, « $\ker(\lambda)$ » son *noyau* et « λ^* » son application *adjointe* ;

- On dénote par « $V_1 \oplus V_2$ » la somme directe de V_1 et V_2 et on utilise le symbole « $\bigoplus$ » pour dénoter la somme généralisée ;

- Si V_1 est en outre muni d'un produit scalaire (dénoté par le symbole « . ») et $A \subset V_1$, on note « $A^{\perp}$ » l'*orthogonal* de A et pour $\alpha \in V_1$, on définit la *forme linéaire* $l_\alpha \in \mathcal{L}(V_1, \mathbb{K})$ par

$$\begin{array}{rccc} l_\alpha : & V_1 & \to & \mathbb{K} \\ & x & \mapsto & \alpha.x \ . \end{array}$$

3.3.6 Notations pour les anneaux d'entiers

Soit $m \in \mathbb{N}^*$. Les notations spécifiques aux anneaux d'entiers sont les suivantes.

- $\mathbb{Z}_m$ est l'anneau des entiers modulo m. Sa loi de composition interne additive est notée « $+$ » et à cette notation nous ajoutons parfois « $\bmod m$ » pour lever d'éventuelles ambiguïtés. On confond les classes modulo m avec leur représentant dans $\{0, \ldots, m-1\}$ et donc $\mathbb{Z}_m$ est assimilé à ce même ensemble. La relation d'ordre naturelle sur les entiers est transportée sur $\mathbb{Z}_m$. La *congruence* modulo m entre deux entiers x et y est notée « $x \equiv y \pmod m$ » et leur *plus grand commun diviseur* est désigné par « $pgcd(x, y)$ ». Enfin comme dans le cas des groupes, nous avons $\mathbb{Z}_m^* \stackrel{déf.}{=} \mathbb{Z}_m \backslash \{0\}$ et le *groupe des éléments inversibles* (pour la multiplication modulo m) est quant à lui noté « $\mathbb{Z}_m^\times$ ». On a donc $\mathbb{Z}_m^\times \stackrel{déf.}{=} \{x \in \mathbb{Z}_m | pgcd(x, m) = 1\}$;

- Le *module* $\mathbb{Z}_m^n$ est naturellement muni d'un produit scalaire défini pour $(x, y) \in (\mathbb{Z}_m^n)^2$ par

$$x.y = \sum_{i=1}^{m} x_i y_i$$

où « $x_i y_i$ » désigne le produit dans $\mathbb{Z}_m$ de x_i et y_i. Son élément neutre est noté « $0_{\mathbb{Z}_m^n}$ » (en particulier $0_{\mathbb{Z}_m^n} \stackrel{déf.}{=} (\underbrace{0, \ldots, 0}_{n \ fois})$ et $0 \stackrel{déf.}{=} 0_{\mathbb{Z}_m}$) et « $\mathbb{Z}_m^{n\,*}$ » désigne l'ensemble $\mathbb{Z}_m^n \setminus \{0_{\mathbb{Z}_m^n}\}$;

- Encore une fois, par *bonne définition*, l'occurrence de la lettre « m » dans la notation $\mathbb{Z}_m$ suppose implicitement l'hypothèse que $m \in \mathbb{N}^*$.

3.3.7 Notations pour les corps finis

Soit p un entier premier.

- La notation « $\mathbb{F}_p$ » désigne le corps fini à p éléments appelé *corps premier*. L'extension de degré k de $\mathbb{F}_p$ est quant à elle désignée par « $\mathbb{F}_{p^k}$ ». On note « $[\mathbb{F}_{p^k} : \mathbb{F}_p]$ » ce degré ;

- Si la lettre « $\mathbb{K}$ » désigne un corps fini, sa somme est notée « $+$ ». L'élément neutre du groupe additif de $\mathbb{K}$ est noté « $0_{\mathbb{K}}$ ». L'élément neutre pour la multiplication de $\mathbb{K}$ est noté « $1_{\mathbb{K}}$ ». « $\mathbb{K}^*$ » désigne naturellement le groupe multiplicatif de $\mathbb{K}$ d'ensemble sous-jacent $\mathbb{K} \setminus \{0_{\mathbb{K}}\}$;

- L'élément neutre pour la loi interne (la somme coordonnée par coordonnée), encore notée « $+$ », du $\mathbb{K}$-espace vectoriel $\mathbb{K}^m$ est noté « $0_{\mathbb{K}^m}$ » et donc $0_{\mathbb{K}^m} \stackrel{déf.}{=} (\underbrace{0_{\mathbb{K}}, \ldots, 0_{\mathbb{K}}}_{m\ fois})$. Les éventuelles ambiguïtés avec l'addition de $\mathbb{K}$ sont levées par le contexte. Evidemment la structure $(\mathbb{K}^m, +)$ est un groupe, sous-jacent à la structure de $\mathbb{K}$-espace vectoriel de $\mathbb{K}^m$. Encore un fois, on a $\mathbb{K}^{m\,*} \stackrel{déf.}{=} \mathbb{K}^m \setminus \{0_{\mathbb{K}^m}\}$;

- Le symbole « . » est une fois de plus utilisé afin de désigner le produit scalaire naturel du $\mathbb{K}$-espace vectoriel $\mathbb{K}^m$ défini pour $(x, y) \in (\mathbb{K}^m)^2$ par

$$x.y = \sum_{i=1}^{m} x_i y_i$$

  où « $x_i y_i$ » désigne le produit dans $\mathbb{K}$ de x_i et y_i.

Par *bonne définition*, la notation « $\mathbb{F}_{p^k}$ » seule implique toujours que p est un entier premier et $k \in \mathbb{N}^*$.

Enfin si X est un anneau $\mathbb{Z}_m$ ou un corps $\mathbb{K}$ alors pour $\alpha \in X^*$, on définit la *translation multiplicative* par α :

$$\begin{array}{rccc} \tau_\alpha : & X & \to & X \\ & x & \mapsto & \alpha x\ . \end{array}$$

Attention, le nom commun « translation » est employé de manière abusive (puisque l'application correspondante n'est pas forcément une permutation). Observons en outre que cette notation ne concerne pas les groupes notés multiplicativement (hormis bien évidemment $\mathbb{K}^*$) pour lesquels on utilise « σ_α ».

Si « $\mathbb{K}$ » désigne un corps quelconque (fini ou non), $Aut(\mathbb{K})$ est le groupe des automorphismes (de corps) du corps $\mathbb{K}$.

3.4 Conclusion

Les notations de base ont été rappelées au cours de ce bref chapitre. Elles correspondent aux notions *a priori* admises et se conforment à la tradition mathématique.

Le choix de réserver l'intégralité d'un chapitre afin d'exposer les représentations symboliques fondamentales n'est pas innocent et possède précisément deux avantages. En premier lieu, en fixant, dès maintenant, certains symboles, nous évitons une redondance arbitraire qui serait à la fois inutile et néfaste à la bonne compréhension de nos travaux. Par ailleurs cette approche offre une certaine cohérence sur la forme du manuscrit. Ceci n'étant pas négligeable puisque notre travail constitue une unité logique. Le fond et la forme sont donc en accord sur ce principe.

Signalons toutefois que ce chapitre ne contient pas la totalité des notations introduites dans ce document mais exclusivement celles qui, à notre discrétion, paraissent les plus courantes dans notre domaine scientifique. La grande majorité des notations est listée dans l'annexe A.

Enfin, bien que nous évitions l'utilisation de notations superflues, cela ne nous interdit pas, dans la suite du manuscrit, de répéter intentionnellement certains passages évoqués ici. Nous pensons que ce type précis de redondance ne nuit pas, bien au contraire, à la clarté de l'exposé.

Chapitre 4

Propriétés cryptographiques des fonctions booléennes

Tout est faux et vrai à la fois. Tel est le vrai caractère de la loi.

BOUDDHA, *Prajna Paramita Sutra*

Sommaire

4.1 Introduction

Qu'est-ce qu'une *fonction booléenne* ?
En 1854 Georges Boole décrivit les relations entre propositions logiques grâce à la notion d'*algèbre de Boole*. Ce nom recoupe en particulier les propriétés des lois classiques de conjonction, de disjonction et de négation logiques. L'algèbre de Boole dispose par ailleurs de deux éléments distingués conventionnellement désignés par « $\top$ » et « $\bot$ ». Ce sont les éléments neutres et absorbants des deux premières lois logiques. Ces constantes remarquables dénotent l'un, le *vrai* et l'autre, le *faux*. Imaginons maintenant un référentiel logique minimaliste réduit à ces deux constantes $\{\bot, \top\}$. Une fonction $f : \{\bot, \top\}^m \to \{\bot, \top\}$ est alors appelée *prédicat (logique) m-aire* ou encore *fonction booléenne* à m variables. Bien souvent le corps $\mathbb{F}_2$ est choisi comme réalisation concrète de l'algèbre booléenne à deux éléments. Il s'agit en particulier du choix qui est généralement effectué en cryptographie et que, bien entendu, nous reprenons à notre compte dans ce document.

Les fonctions booléennes ne sont pas, proprement dit, l'objet central du travail que nous présentons. Néanmoins les notions développées dans le manuscrit généralisent des concepts de type booléen. Comme par ailleurs les fonctions à valeurs dans $\mathbb{F}_2$ sont très largement exploitées dans le cadre de la cryptographie à clef secrète, il devient naturel d'en exposer les principales propriétés et particulièrement celles de nature cryptographique.

L'importance donc, des fonctions booléennes en cryptographie induit le fait que la majorité des critères de solidité se fonde sur leurs caractéristiques. Historiquement, la sûreté cryptographique ne dépendait que de la cardinalité des ensembles de départ et d'arrivée des applications booléennes. Cependant avec l'avènement des attaques telles que les cryptanalyses différentielle et linéaire, d'autres moyens d'estimer le degré de solidité garanti par une fonction donnée ont été établis. L'objectif est donc de trouver des fonctions satisfaisant simultanément plusieurs critères cryptographiques.

Au cours de ce chapitre nous exposons ainsi les principales propriétés cryptographiques des fonctions booléennes. Si nous n'évoquons pas les notions de non linéarité parfaite et de fonction courbe, ce n'est en aucun cas un oubli de notre part. Nous les avons volontairement omises puisque le chapitre 5 leur est entièrement dédié.

Ce chapitre est structuré de la façon suivante : nous nous attachons, dans un premier temps, à définir les notations propres à ce chapitre et les notions de base concernant le contexte booléen, puis une seconde section est assignée à la présentation de la transformée de Fourier, source de très nombreux résultats. Les propriétés cryptographiques des fonctions booléennes sont finalement développées dans l'avant-dernière section, la dernière étant consacrée à la conclusion du présent chapitre.

4.2 $\mathbb{F}_2^m$ et ses différentes représentations

4.2.1 Notations spécifiques à $\mathbb{F}_2^m$

Nous reprenons ici les notations définies pour les corps finis et présentées dans le chapitre 3 en les particularisant au cas de la caractéristique 2.

L'ensemble $\mathbb{F}_2 \stackrel{déf.}{=} \{0,1\}$ est le corps de Galois à deux éléments. En particulier $0 \stackrel{déf.}{=} 0_{\mathbb{F}_2}$ et $1 \stackrel{déf.}{=} 1_{\mathbb{F}_2}$. Il est naturellement plongé (c'est-à-dire vu comme un sous-ensemble) dans $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{R}$ ou $\mathbb{C}$. On utilise le symbole « $\oplus$ » pour désigner l'addition (modulo deux) *i.e.* la loi additive de $\mathbb{F}_2$.

$\mathbb{F}_2^m$ est le $\mathbb{F}_2$-espace vectoriel de dimension m des m-uplets d'éléments de $\mathbb{F}_2$. Le symbole « $\oplus$ » est aussi utilisé pour dénoter la somme de $\mathbb{F}_2^m$ *i.e.* la somme modulo deux coordonnée par coordonnée. Les éventuelles ambiguïtés avec l'addition de $\mathbb{F}_2$ sont levées par le contexte. On note « $\bigoplus$ » la somme généralisée associée. L'élément neutre du groupe additif $(\mathbb{F}_2^m, \oplus)$, sous-jacent à la structure d'espace vectoriel, est $0_{\mathbb{F}_2^m} \stackrel{déf.}{=} (\underbrace{0,\ldots,0}_{m\ fois})$.

On pose : $\mathbb{F}_2^{m*} \stackrel{déf.}{=} \mathbb{F}_2^m \setminus \{0_{\mathbb{F}_2^m}\}$, comme dans le cas des corps finis quelconques.
Soient $i \in \{1,\ldots,m\}$ et $e^{(i)} \in \mathbb{F}_2^m$ défini pour $j \in \{1,\ldots,m\}$ par

$$e_j^{(i)} = \begin{cases} 0 & \text{si } i \neq j\ , \\ 1 & \text{sinon}\ . \end{cases} \tag{4.1}$$

Alors $\{e^{(i)} \in \mathbb{F}_2^m | i \in \{1,\ldots,m\}\}$ est la *base canonique* de $\mathbb{F}_2^m$.
Comme dans le cas de la caractéristique quelconque, le symbole « . » est utilisé pour désigner le produit scalaire naturel de $\mathbb{F}_2^m$ défini pour $(x,y) \in (\mathbb{F}_2^m)^2$ par

$$x.y = \sum_{i=1}^{m} x_i y_i \bmod 2 = \bigoplus_{i=1}^{m} x_i y_i\ . \tag{4.2}$$

La *distance de Hamming* est notée « d_H » et le *poids* d'un vecteur $x \in \mathbb{F}_2^m$ est $w_H(x) \stackrel{déf.}{=} d_H(x, 0_{\mathbb{F}_2^m})$.

Enfin pour $x \in \mathbb{F}_2^m$, on désigne par « $\overline{x}$ » son *complémentaire* dans $\mathbb{F}_2^m$ *i.e.* $\overline{x} \stackrel{déf.}{=} x \oplus (\underbrace{1, \ldots, 1}_{m \text{ fois}})$.

$\mathbb{F}_{2^m}$ est le corps fini à 2^m éléments, extension finie de degré m de $\mathbb{F}_2$. Son addition est encore désignée par « $\oplus$ » et ses éléments neutres sont $0_{\mathbb{F}_{2^m}}$, neutre du groupe additif $(\mathbb{F}_{2^m}, \oplus)$, et $1_{\mathbb{F}_{2^m}}$, neutre du groupe multiplicatif $\mathbb{F}_{2^m}^*$.

4.2.2 Comment représenter les éléments de $\mathbb{F}_2^m$?

Il existe plusieurs manières de représenter $\mathbb{F}_2^m$ que l'on désigne parfois par le terme *identification*. Toutes celles présentées ici seront utilisées dans ce manuscrit.

$\mathbb{F}_2^m$ comme somme directe de produits cartésiens

Très naturellement, $\mathbb{F}_2^m$ peut être identifié, en tant que $\mathbb{F}_2$-espace vectoriel à certains produits directs d'espaces vectoriels. Soient en effet $k \in \mathbb{N}^*$ et $\{m_i\}_{i \in \{1,\ldots,k\}}$ une suite (finie) d'entiers strictement positifs tels que $m = \sum_{i=1}^{k} m_i$. Alors on confond les $\mathbb{F}_2$-espaces vectoriels $\mathbb{F}_2^m$ et $\mathbb{F}_2^{m_1} \times \ldots \times \mathbb{F}_2^{m_k}$. Cette identification a déjà été utilisée au chapitre 2 (sous-section 2.3.2.1). A plusieurs reprises de telles assimilations seront effectuées de manière *ad hoc* afin de simplifier les notations.

$\mathbb{F}_2^m$ plongé dans $\mathbb{F}_{2^m}$

Une autre possibilité d'identification entre $\mathbb{F}_2$-espaces vectoriels est la suivante. Le corps fini à 2^m éléments $\mathbb{F}_{2^m}$ possède une structure sous-jacente d'espace vectoriel sur $\mathbb{F}_2$. On peut donc confondre cette structure avec celle de $\mathbb{F}_2^m$. Afin d'effectuer cette opération, on se donne $B \stackrel{déf.}{=} \{e_1, \ldots, e_m\}$ une base quelconque de $\mathbb{F}_{2^m}$ sur $\mathbb{F}_2$. Alors pour tout $x \in \mathbb{F}_{2^m}$, on a :

$$x = x_1 e_1 \oplus \ldots \oplus x_m e_m \ ,$$

avec pour tout $i \in \{1, \ldots, m\}$, $x_i \in \mathbb{F}_2$. Soit donc la fonction

$$\begin{array}{rccc} \Phi_B : & \mathbb{F}_{2^m} & \to & \mathbb{F}_2^m \\ & x & \mapsto & (x_1, \ldots, x_m) \ . \end{array} \tag{4.3}$$

Il est facile de voir que Φ_B est un isomorphisme de $\mathbb{F}_2$-espaces vectoriels de $\mathbb{F}_{2^m}$ dans $\mathbb{F}_2^m$.

$\mathbb{F}_2^m$ comme représentation en base deux d'entiers

La dernière représentation que nous évoquons est établie entre $\mathbb{F}_2^m$ et l'anneau $\mathbb{Z}_{2^m}$. Nous l'avons déjà entrevue au chapitre 2 lorsqu'il a été fait mention du cryptosystème IDEA (sous-section 2.3.2.2). Elle est maintenant précisée.

Les applications

$$\begin{array}{rccc} \Theta_m^g : & \mathbb{F}_2^m & \to & \mathbb{Z}_{2^m} \\ & x & \mapsto & \Theta_m^g(x) \stackrel{déf.}{=} \sum_{i=1}^{m} x_i 2^{m-i} \end{array} \tag{4.4}$$

et

$$\begin{array}{rccc} \Theta_m^d : & \mathbb{F}_2^m & \to & \mathbb{Z}_{2^m} \\ & x & \mapsto & \Theta_m^d(x) \stackrel{déf.}{=} \sum_{i=1}^{m} x_i 2^{i-1} \end{array} \tag{4.5}$$

sont des bijections. Ainsi un m-uplet $x \in \mathbb{F}_2^m$ correspond à la représentation en base deux d'un entier de $\{0, \ldots, 2^m - 1\}$. Afin de différencier les deux représentations, dans le premier cas on dit que le *bit de poids fort* (*i.e.* le coefficient dans la somme de 2^{m-1}) est à gauche alors que dans le second, il est à droite.

Les notions de base étant fixées, dans la suite on pourra écrire que l'on utilise l'une quelconque de ses identifications sans autres précisions.

4.3 Fonctions booléennes

Nous nous attachons maintenant à dessiner les contours de la théorie des fonctions booléennes en mentionnant les définitions de base ainsi que les premiers résultats utilisés par la suite.

4.3.1 Définitions

Les différentes notations, concernant les fonctions booléennes, sont dévoilées maintenant.

Une fonction $f : \mathbb{F}_2^m \to \mathbb{F}_2$ est appelée *fonction booléenne binaire* (de m variables).

Une fonction $f : \mathbb{F}_2^m \to \mathbb{F}_2^n$ est appelée *fonction booléenne vectorielle*[1] (de m variables).

Par abus de langage, la plupart du temps seule l'expression *fonction booléenne* est employée. Les adjectifs « binaire » et « vectoriel » étant alors délibérément passés sous silence.

Pour un couple de fonctions booléennes $(f, g) \in (\mathbb{F}_2^{n\,\mathbb{F}_2^m})^2$, $f \oplus g$ est la somme terme à terme des fonctions f et g *i.e.* pour $x \in \mathbb{F}_2^m$, $(f \oplus g)(x) \stackrel{déf.}{=} f(x) \oplus g(x)$.

La *négation* de $f : \mathbb{F}_2^m \to \mathbb{F}_2$ est la fonction $f \oplus \mathbf{1}_{\mathbb{F}_{2^m}}$. Elle est notée « $\bar{f}$ » (attention de ne pas confondre cette notation avec la conjugaison dans $\mathbb{C}$). On a donc pour $x \in \mathbb{F}_2^m$, $\overline{f}(x) \stackrel{déf.}{=} f(x) \oplus 1 = \overline{f(x)}$.

Définition 4.1. Soit $f : \mathbb{F}_2^m \to \mathbb{F}_2$. Le *support* de f est l'ensemble des vecteurs $x \in \mathbb{F}_2^m$ tels que $f(x) \neq 0$. Il est noté « S_f ». On a donc

$$S_f \stackrel{déf.}{=} \{x \in \mathbb{F}_2^m | f(x) \neq 0\} .$$

Le cardinal de S_f, noté « $w_H(f)$ », est le *poids (de Hamming)* de la fonction f.
Enfin pour $(f, g) \in (\mathbb{F}_2^{\mathbb{F}_2^m})^2$, la *distance de Hamming* entre f et g, notée « $d_H(f, g)$ », est le nombre de vecteurs pour lesquels les deux fonctions diffèrent :

$$d_H(f, g) \stackrel{déf.}{=} |\{x \in \mathbb{F}_2^m | f(x) \neq g(x)\}| ,$$

soit, en d'autres termes, $d_H(f, g) = |S_{f \oplus g}| = w_H(f \oplus g)$.

Remarque 4.1.

1. d_H est bien une métrique sur $\mathbb{F}_2^{\mathbb{F}_2^m}$. En particulier l'inégalité triangulaire de d_H pour $(f, g, h) \in (\mathbb{F}_2^{\mathbb{F}_2^m})^3$ se vérifie comme suit : si pour $x \in \mathbb{F}_2^m$, $f(x) \neq h(x)$ alors soit $f(x) \neq g(x)$ soit $g(x) \neq h(x)$. Il provient de ce fait que $d_H(f, g) + d_H(g, h) = |\{x \in \mathbb{F}_2^m | f(x) \neq h(x)\}| + |\{x \in \mathbb{F}_2^m | g(x) \neq h(x)\}| \geq |\{x \in \mathbb{F}_2^m | f(x) \neq h(x)\}| = d_H(f, h)$.

[1] Parfois appelée « Boîte-S » en cryptographie.

2. Soit $(f,g) \in (\mathbb{F}_2^{\mathbb{F}_2^m})^2$. On a alors

$$d_H(f,\overline{g}) = 2^m - d_H(f,g) \ .$$

Enfin une notion apparaissant assez naturellement dès qu'une métrique est définie est celle de distance à un ensemble. Si $f : \mathbb{F}_2^m \to \mathbb{F}_2$ et $A \subset \mathbb{F}_2^{\mathbb{F}_2^m}$. On appelle *distance* (de Hamming) de f à l'ensemble A, le nombre

$$d_H(f,A) \stackrel{déf.}{=} \min_{g \in A} d_H(f,g) \ .$$

Code de Reed-Muller d'ordre 1
Soit $\mathcal{L}(\mathbb{F}_2^m, \mathbb{F}_2)$ l'ensemble des *formes linéaires* de $\mathbb{F}_2^m$ *i.e.* l'espace vectoriel - dual de $\mathbb{F}_2^m$ - des applications linéaires de $\mathbb{F}_2^m$ dans $\mathbb{F}_2$. L'identification de la forme linéaire, via le produit scalaire naturel de $\mathbb{F}_2^m$ (voir le chapitre 3),

$$\begin{array}{rccc} l_\alpha : & \mathbb{F}_2^m & \to & \mathbb{F}_2 \\ & x & \mapsto & \alpha.x \end{array}$$

avec le vecteur $\alpha \in \mathbb{F}_2^m$ fournit un isomorphisme de $\mathbb{F}_2$-espaces vectoriels (non canonique puisque dépendant du choix des bases) entre $\mathbb{F}_2^m$ et $\mathcal{L}(\mathbb{F}_2^m, \mathbb{F}_2)$. On désigne par « $R(1,m)$ » l'ensemble des fonctions affines de $\mathbb{F}_2^m$ dans $\mathbb{F}_2$. Cet ensemble est aussi appelé *code de Reed-Muller d'ordre* 1 de $\mathbb{F}_2^m$. Il contient 2^{m+1} fonctions (les formes linéaires et leur négation). Elles sont donc de la forme

$$x \mapsto \alpha.x \oplus \beta \ ,$$

où $(\alpha,\beta) \in \mathbb{F}_2^m \times \mathbb{F}_2$. On a donc encore

$$R(1,m) = \{\sigma_\beta \circ l_\alpha \in \mathbb{F}_2^{\mathbb{F}_2^m} | (\alpha,\beta) \in \mathbb{F}_2^m \times \mathbb{F}_2\}$$

avec, on le rappelle, $\sigma_\beta \in T(\mathbb{F}_2)$ la translation par β soit $x \mapsto \sigma_\beta(x) \stackrel{déf.}{=} x \oplus \beta$.

L'ensemble $R(1,m)$ peut être muni de la loi de groupe d'addition modulo 2 terme à terme puisque pour $(\sigma_\beta \circ l_\alpha, \sigma_{\beta'} \circ l_{\alpha'}) \in R(1,m)^2$, on a $\sigma_\beta \circ l_\alpha \oplus \sigma_{\beta'} \circ l_{\alpha'} = \sigma_{\beta \oplus \beta'} \circ l_{\alpha \oplus \alpha'}$. $R(1,m)$ est alors un groupe isomorphe au produit direct des groupes $\mathcal{L}(\mathbb{F}_2^m, \mathbb{F}_2)$ et $T(\mathbb{F}_2)$ et donc, en particulier, aussi isomorphe au groupe, produit direct, $\mathbb{F}_2^m \times \mathbb{F}_2$.

Dans la suite on s'intéresse en particulier à $d_H(f, R(1,m))$ pour $f : \mathbb{F}_2^m \to \mathbb{F}_2$.

4.3.2 Différentes représentations des fonctions booléennes

4.3.2.1 La table de vérité

Habituellement une fonction booléenne binaire est donnée via sa *table de vérité*[2] qui est son graphe. La table est canoniquement ordonnée par les arguments $x \in \mathbb{F}_2^m$ de f selon l'ordre lexicographique. Plus explicitement, par l'ordre naturel des entiers de $\mathbb{Z}_{2^m} = \{0, \ldots, 2^m - 1\}$, induit sur $\mathbb{F}_2^m$ par la bijection $\Theta_m^d : \mathbb{F}_2^m \to \mathbb{Z}_{2^m}$ précédemment définie.

[2] Le nom « vérité » est utilisé en référence à la logique propositionnelle.

Exemple 4.1. Considérons le cas où $m = 3$. Voici la définition d'une fonction $f : \mathbb{F}_2^3 \to \mathbb{F}_2$ par sa table de vérité :

élément de $\mathbb{F}_2^3$	valeur de f
$(0,0,0)$	1
$(1,0,0)$	1
$(0,1,0)$	0
$(1,1,0)$	0
$(0,0,1)$	0
$(1,0,1)$	1
$(0,1,1)$	1
$(1,1,1)$	0

On a ici $S_f = \{(0,0,0),(1,0,0),(0,1,1),(1,0,1)\}$ et $w_H(f) = 4$.

La table de vérité d'une fonction $f : \mathbb{F}_2^m \to \mathbb{F}_2$ peut aussi s'interpréter comme un 2^m-uplet d'éléments de $\mathbb{F}_2$, disons « x_f », appelé *vecteur des valeurs* de f et correspondant à sa seconde projection. On a donc $x_f \in \mathbb{F}_2^{2^m}$ et pour tout $i \in \{1,\ldots,2^m\}$, $(x_f)_i = f(\Theta_m^d(i-1))$. En particulier $w_H(f) = w_H(x_f)$.

4.3.2.2 La Forme Algébrique Normale

Cette représentation a auparavant été promptement décrite (voir le chapitre 2 p. 28). Nous y revenons maintenant afin de l'exposer avec plus de précisions. Il s'agit de l'analogue de la notion de *forme normale disjonctive* (voir [Gal87]) du calcul propositionnel : une proposition est écrite sous forme normale disjonctive si elle de la forme « $C_1 \vee \ldots \vee C_m$ » où chaque C_i est une conjonction de littéraux (un littéral étant un symbole propositionnel P ou sa négation) et « $\vee$ » désigne la disjonction logique.

Soient $\mathtt{X}_1 \ldots, \mathtt{X}_m$ m indéterminées (distinctes) de $\mathbb{F}_2$. On note « $\mathbb{F}_2[\mathtt{X}_1,\ldots,\mathtt{X}_m]$ » l'anneau des polynômes à m indéterminées et à coefficients dans $\mathbb{F}_2$ et on désigne par « $\mathbb{F}_2[\mathtt{X}_1,\ldots,\mathtt{X}_m]/(\mathtt{X}_1^2 \oplus \mathtt{X}_1,\ldots,\mathtt{X}_m^2 \oplus \mathtt{X}_m)$ » l'anneau quotienté par l'idéal principal $(\mathtt{X}_1^2 \oplus \mathtt{X}_1,\ldots,\mathtt{X}_m^2 \oplus \mathtt{X}_m)$.

Définition 4.2. La *forme algébrique normale* (FAN) de $f : \mathbb{F}_2^m \to \mathbb{F}_2$ est l'unique polynôme P_f de $\mathbb{F}_2[\mathtt{X}_1,\ldots,\mathtt{X}_m]/(\mathtt{X}_1^2 \oplus \mathtt{X}_1,\ldots,\mathtt{X}_m^2 \oplus \mathtt{X}_m)$ tel que

$$\forall (x_1,\ldots,x_m) \in \mathbb{F}_2^m,\ f(x_1,\ldots,x_m) = P_f(x_1,\ldots,x_m)\ .$$

Ce polynôme P_f vérifie en outre

$$P_f(\mathtt{X}_1,\ldots,\mathtt{X}_m) = \bigoplus_{x \in \mathbb{F}_2^m} \alpha_x \prod_{i=1}^{m} \mathtt{X}_i^{x_i}$$

où $\{\alpha_x\}_{x \in \mathbb{F}_2^m}$ est une suite (finie) d'éléments de $\mathbb{F}_2$.

Cette écriture, unique pour chaque fonction booléenne f, correspond à sa représentation sous forme de fonction polynomiale à m variables dont le degré relatif de chacune des variables est au plus 1.

Le calcul des coefficients α_x de la FAN d'une fonction $f : \mathbb{F}_2^m \to \mathbb{F}_2$ se fait via la *transformée de Möbius* :

$$\begin{array}{rccc} \mathring{f}: & \mathbb{F}_2^m & \to & \mathbb{F}_2 \\ & x & \mapsto & \displaystyle\bigoplus_{y \leq x} f(y) \end{array} \tag{4.6}$$

où l'on a

$$y \leq x \text{ si et seulement si } \forall i \in \{1,\ldots,m\},\ \text{si } y_i = 1 \text{ alors } x_i = 1\ .$$

Le lien entre FAN et la transformation de Möbius est obtenu par la proposition ci-dessous.

Proposition 4.1. [Pom03] *Soit* $f : \mathbb{F}_2^m \to \mathbb{F}_2$. *Alors* $\forall x \in \mathbb{F}_2^m$, $\alpha_x = \mathring{f}(x)$.

Preuve. Il suffit de montrer que pour tout $x \in \mathbb{F}_2^m$, $f(x) = \bigoplus_{y \in \mathbb{F}_2^m} \mathring{f}(y) \prod_{i=1}^{m} x_i^{y_i}$.

Pour ce faire nous effectuons une preuve par récurrence sur l'entier $m \in \mathbb{N}^*$.

1. Si $m = 1$ on a : $f(x_1) = f(0)(1 \oplus x_1) \oplus f(1)x_1$ et donc $f(x_1) = (f(0) \oplus f(1))x_1 \oplus f(0)$.
2. Soit $m > 1$ et supposons, par hypothèse de récurrence, que $\forall k \in \mathbb{N}^*$ tel que $1 \leq k < m$, $\forall g \in \mathbb{F}_2^{\mathbb{F}_2^k}$ et $\forall (x_1,\ldots,x_k) \in \mathbb{F}_2^k$, on ait

$$g(x_1,\ldots,x_k) = \bigoplus_{y \in \mathbb{F}_2^k} \bigoplus_{z \leq y} g(z) \prod_{i=1}^{k} x_i^{y_i}\ . \tag{4.7}$$

Soient $f : \mathbb{F}_2^m \to \mathbb{F}_2$ et $\alpha \in \mathbb{F}_2$ fixé. La fonction $f_\alpha : \mathbb{F}_2^{m-1} \to \mathbb{F}_2$ définie par $f_\alpha(x_1,\ldots,x_{m-1}) = f(x_1,\ldots,x_{m-1},\alpha)$ vérifie l'hypothèse de récurrence (4.7) *i.e.* pour tout $(x_1,\ldots,x_{m-1}) \in \mathbb{F}_2^{m-1}$:

$$f(x_1,\ldots,x_m,\alpha) = \bigoplus_{y \in \mathbb{F}_2^{m-1}} \bigoplus_{z \leq y} f(z_1,\ldots,z_{m-1},\alpha) x_1^{y_1} \ldots x_{m-1}^{y_{m-1}}\ .$$

Or $\forall (z_1,\ldots,z_{m-1}) \in \mathbb{F}_2^{m-1}$ et $\forall x \in \mathbb{F}_2$ on a :

$$\begin{aligned} f(z_1,\ldots,z_{m-1},x) &= f(z_1,\ldots,z_{m-1},0)(1 \oplus x) \oplus f(z_1,\ldots,z_{m-1},1)x \\ &= (f(z_1,\ldots,z_{m-1},0) \oplus f(z_1,\ldots,z_{m-1},1))x \oplus f(z_1,\ldots,z_{m-1},0)\ . \end{aligned}$$

On a donc bien pour tout $(x_1,\ldots,x_m) \in \mathbb{F}_2^m$:

$$f(x_1,\ldots,x_m) = \bigoplus_{y \in \mathbb{F}_2^m} \bigoplus_{z \leq y} f(z_1,\ldots,z_m) x_1^{y_1} \ldots x_m^{y_m}\ .$$

□

Le *degré algébrique* de $f : \mathbb{F}_2^m \to \mathbb{F}_2$, noté « $\deg(f)$ », est le degré de sa FAN, c'est-à-dire la plus grande valeur atteinte par le poids de Hamming des éléments $x \in F_2^m$ tels que $\alpha_x \neq 0$. L'ensemble des fonctions booléennes binaires définies sur $\mathbb{F}_2^m$ de degré algébrique inférieur ou égal à k est appelé le *code de Reed-Muller d'ordre k* et est noté « $R(k,m)$ ». En particulier les fonctions de degré algébrique 1 sont les fonctions affines évoquées précédemment.

Exemple 4.2. Soit $f : \mathbb{F}_2^3 \to \mathbb{F}_2$ définie par sa table de vérité

élément de $\mathbb{F}_2^3$	valeur de f
$(0,0,0)$	0
$(1,0,0)$	0
$(0,1,0)$	0
$(1,1,0)$	0
$(0,0,1)$	1
$(1,0,1)$	1
$(0,1,1)$	0
$(1,1,1)$	1

Sa FAN est alors $P_f(\mathtt{X}_1,\mathtt{X}_2,\mathtt{X}_3) = (1 \oplus \mathtt{X}_1)(1 \oplus \mathtt{X}_2)\mathtt{X}_3 \oplus \mathtt{X}_1(1 \oplus \mathtt{X}_2)\mathtt{X}_3 \oplus \mathtt{X}_1\mathtt{X}_2\mathtt{X}_3 = \mathtt{X}_1\mathtt{X}_2\mathtt{X}_3 \oplus \mathtt{X}_3$ et $\deg(f) = 3$.

La notion de FAN peut être généralisée au cas des fonctions booléennes vectorielles comme le résultat donné ci-dessous sans démonstration nous l'apprend.

Proposition 4.2. [Pom03] *Chaque fonction* $f : \mathbb{F}_2^m \to \mathbb{F}_2^n$ *possède une unique expression sous la forme*

$$f(x_1, \ldots, x_m) = \bigoplus_{I \subset \{1,\ldots,m\}} \alpha_I x^I$$

pour tout $(x_1, \ldots, x_m) \in \mathbb{F}_2^m$, *avec les coefficients* $\alpha_I \in F_2^n$ *et* $x^I \stackrel{déf.}{=} \prod_{i \in I} x_i \in \mathbb{F}_2$.

4.3.2.3 La représentation trace

Le dernier genre de représentations exposé ici n'est pas exploité dans le présent manuscrit. Simplement certaines notions connexes sont utilisées. Toutefois par souci de complétude, nous avons tout de même souhaité le présenter.

Définition 4.3. Soit $(m, k) \in (\mathbb{N}^*)^2$ tel que k divise m. On pose $n \stackrel{déf.}{=} 2^k$, $\mathbb{F} \stackrel{déf.}{=} \mathbb{F}_{2^m}$ et $\mathbb{K} \stackrel{déf.}{=} \mathbb{F}_{2^k}$. On définit la fonction *trace* de $\mathbb{F}$ sur $\mathbb{K}$ comme suit

$$\begin{array}{rccc} tr_{\mathbb{F}/\mathbb{K}} : & \mathbb{F} & \to & \mathbb{K} \\ & x & \mapsto & x \oplus x^n \oplus \ldots \oplus x^{n^{m-1}} \end{array} .$$

Les principales propriétés de cette application sont données ci-dessous. Les preuves des résultats peuvent être trouvées en consultant [LN97].

Théorème 4.1. [LN97] *Soit* $(m, k) \in (\mathbb{N}^*)^2$ *tel que* k *divise* m. *On pose* $n \stackrel{déf.}{=} 2^k$, $\mathbb{F} \stackrel{déf.}{=} \mathbb{F}_{2^m}$ *et* $\mathbb{K} \stackrel{déf.}{=} \mathbb{F}_{2^k}$. *La fonction trace* $tr_{\mathbb{F}/\mathbb{K}}$ *satisfait les propriétés suivantes :*

1. $\forall (x, y) \in \mathbb{F}^2$, $tr_{\mathbb{F}/\mathbb{K}}(x \oplus y) = tr_{\mathbb{F}/\mathbb{K}}(x) \oplus tr_{\mathbb{F}/\mathbb{K}}(y)$;
2. $\forall (\alpha, x) \in \mathbb{K} \times \mathbb{F}$, $tr_{\mathbb{F}/\mathbb{K}}(\alpha x) = \alpha tr_{\mathbb{F}/\mathbb{K}}(x)$;
3. $tr_{\mathbb{F}/\mathbb{K}}$ *est une application linéaire de* $\mathbb{F}$ *dans* $\mathbb{K}$, *où* $\mathbb{K}$ *et* $\mathbb{F}$ *sont identifiés à des* $\mathbb{K}$*-espaces vectoriels ;*
4. $\forall \alpha \in \mathbb{K}$, $tr_{\mathbb{F}/\mathbb{K}}(\alpha) = \underbrace{\alpha \oplus \ldots \oplus \alpha}_{m \text{ fois}}$;
5. $\forall x \in \mathbb{F}$, $tr_{\mathbb{F}/\mathbb{K}}(x^n) = tr_{\mathbb{F}/\mathbb{K}}(x)$.

Lorsque l'on considère le cas où $k = 1$ c'est-à-dire lorsque $\mathbb{K} = \mathbb{F}_2$, la trace de $\mathbb{F}_{2^m}$ sur son sous-corps premier $\mathbb{F}_2$, appelée *trace absolue*, est simplement dénotée par « *tr* » quand il n'y a pas d'ambiguïté et vérifie pour tout $x \in \mathbb{F}_{2^m}$,

$$tr(x) = x \oplus x^2 \oplus x^{2^2} \oplus \ldots \oplus x^{2^{m-1}} .$$

Un autre concept doit être introduit avant que la représentation trace ne soit dévoilée.

Définition 4.4. Une *classe cyclotomique* C_k modulo $2^m - 1$ est définie par

$$C_k = \{k, 2k, \ldots, 2^{m_k - 1}k\}$$

où m_k est le plus petit entier positif tel que $k \equiv 2^{m_k} k \pmod{2^m - 1}$. L'indice $k \in \mathbb{N}$ est choisi comme le plus petit entier dans C_k et est appelé *leader de classe*[3] de C_k. On note « $\Gamma(m)$ » l'ensemble contenant tous les leaders de classe modulo $2^m - 1$.

[3] Il s'agit évidemment d'un représentant particulier de la classe cyclotomique.

Exemple 4.3. Pour $m = 4$ les classes cyclotomiques modulo 15 sont :
$C_0 = \{0\}$, $C_1 = \{1, 2, 4, 8\}$, $C_3 = \{3, 6, 12, 9\}$, $C_5 = \{5, 10\}$ et $C_7 = \{7, 14, 13, 11\}$.
$\{0, 1, 3, 5, 7\}$ est l'ensemble $\Gamma(4)$ des leaders de classe modulo 15.
Pour une fonction $f \in \mathbb{F}_2^{\mathbb{F}_{2^m}}$ non identiquement nulle, pour tout $k \in \Gamma(m)$ il existe $\alpha_k \in \mathbb{F}_{2^{m_k}}$ où $m_k \stackrel{déf.}{=} |C_k|$ et $\alpha_{2^m-1} \in \mathbb{F}_2$ tels que pour tout $x \in \mathbb{F}_{2^m}$ on ait :

$$f(x) = \bigoplus_{k \in \Gamma(m)} tr_{\mathbb{F}_{2^{m_k}}/\mathbb{F}_2}(\alpha_k x^k) \oplus \alpha_{2^m-1} x^{2^m-1} .$$

Cette écriture est la *représentation trace* de la fonction f. Finalement en plongeant $\mathbb{F}_2^m$ dans la structure d'espace vectoriel du corps $\mathbb{F}_{2^m}$, on en déduit la représentation trace des fonctions booléennes de $\mathbb{F}_2^{\mathbb{F}_2^m}$.

4.4 Transformées de Fourier et de Walsh

La transformée de Fourier, d'une certaine fonction f, correspond intuitivement à une moyenne pondérée, un terme de la transformée dépendant en effet de toutes les valeurs de f. Des propriétés globales, souvent de type combinatoire, se trouvent ainsi réduites à des propriétés locales plus facilement exploitables. Il en résulte que la théorie de Fourier, via la transformée du même nom, est un outil extrêmement fécond dans le domaine des fonctions booléennes. Nombreuses sont leurs propriétés s'exprimant en effet par dualité à l'aide de cet instrument très élaboré. Cette même dualité est explicitement définie au chapitre 5 dans le cadre de l'étude des fonctions parfaitement non linéaires et courbes. Observons d'ailleurs que dans le chapitre 6 est évoquée la généralisation de la transformée de Fourier dans les groupes finis commutatifs alors qu'au chapitre 8, nous introduisons un outil encore plus raffiné dans le cas des groupes finis non abéliens. On comprend donc la forte influence de la théorie de Fourier sur notre travail et par là notre obstination à présenter celle-ci sous de nombreux angles au cours de ce manuscrit. Entamons donc cette étude par le cas de la transformée de Fourier des fonctions booléennes.

4.4.1 La transformée de Fourier

Les objets favoris de la théorie de Fourier - dans l'environnement booléen - sont les fonctions définies sur un espace vectoriel $\mathbb{F}_2^m$ et à valeurs dans le corps des réels. L'ensemble $\mathbb{R}^{\mathbb{F}_2^m}$ de ces fonctions est lui-même un $\mathbb{R}$-espace vectoriel. On le munit assez naturellement du produit scalaire euclidien suivant :

$$\begin{array}{rccl} \langle .\ ,\ . \rangle : & (\mathbb{R}^{\mathbb{F}_2^m})^2 & \to & \mathbb{R}^{\mathbb{F}_2^m} \\ & (\varphi, \psi) & \mapsto & \langle \varphi, \psi \rangle \stackrel{déf.}{=} \displaystyle\sum_{x \in \mathbb{F}_2^m} \varphi(x)\psi(x) . \end{array}$$

Dans ce contexte la transformée de Fourier se définit comme suit.

Définition 4.5. Soit $\varphi : \mathbb{F}_2^m \to \mathbb{R}$. La *transformée de Fourier* de φ, notée « $\widehat{\varphi}$ », est définie par

$$\begin{array}{rccl} \widehat{\varphi} : & \mathbb{F}_2^m & \to & \mathbb{R} \\ & \alpha & \mapsto & \displaystyle\sum_{x \in \mathbb{F}_2^m} \varphi(x)(-1)^{\alpha.x} . \end{array}$$

L'application *transformée de Fourier* Φ_F est donc

$$\begin{array}{rccl} \Phi_F : & \mathbb{R}^{\mathbb{F}_2^m} & \to & \mathbb{R}^{\mathbb{F}_2^m} \\ & \varphi & \mapsto & \widehat{\varphi} . \end{array}$$

Remarque 4.2.

1. Soit l'application[4]
$$\begin{array}{rccc} \chi^1_{\mathbb{F}_2} : & \mathbb{F}_2 & \to & \mathbb{R} \\ & x & \mapsto & (-1)^x \end{array}$$
où $\mathbb{F}_2$ a été plongé dans $\mathbb{R}$. Soit $(\varphi, \alpha) \in \mathbb{R}^{\mathbb{F}_2^m} \times \mathbb{F}_2^m$. Alors $\widehat{\varphi}(\alpha) = \langle \varphi, \chi^1_{\mathbb{F}_2} \circ l_\alpha \rangle$;

2. Trivialement Φ_F est une application $\mathbb{R}$-linéaire *i.e.* $\Phi_F \in \mathcal{L}(\mathbb{R}^{\mathbb{F}_2^m}, \mathbb{R}^{\mathbb{F}_2^m}) = End(\mathbb{R}^{\mathbb{F}_2^m})$;

3. Φ_F est un cas spécial de transformée de Fourier discrète sur un groupe abélien fini (cf. chapitre 6) ;

4. Si $f : \mathbb{F}_2^m \to \mathbb{F}_2$ ($\mathbb{F}_2$ étant plongé dans $\mathbb{R}$), alors $w_H(f) = \widehat{f}(0_{\mathbb{F}_2^m})$;

5. Clairement $\widehat{\overline{\mathbf{1}_{\mathbb{F}_2^m}}} = \overline{\widehat{\mathbf{1}_{\mathbb{F}_2^m}}} = \mathbf{1}_{\mathbb{F}_2^m} \oplus \mathbf{1}_{\mathbb{F}_2^m} = \mathbf{1}_\emptyset$ *i.e.* la transformée de Fourier de la fonction identiquement nulle est identiquement nulle. L'autre fonction constante $\mathbf{1}_{\mathbb{F}_2^m}$ est transformée en $2^m \mathbf{1}_{\{0_{\mathbb{F}_2^m}\}}$ *i.e.* à un coefficient 2^m près, $\widehat{\mathbf{1}_{\mathbb{F}_2^m}}$ est la fonction[5] qui vaut 0 partout mis à part en $0_{\mathbb{F}_2^m}$ où elle vaut 1.

La dernière remarque se déduit du lemme suivant :

Lemme 4.1. [Pom03] *Pour $\alpha \in \mathbb{F}_2^m$ on a :*
$$\sum_{x \in \mathbb{F}_2^m} (-1)^{\alpha.x} = 2^m \mathbf{1}_{\{0_{\mathbb{F}_2^m}\}}(\alpha) \ .$$

Preuve. Si $\alpha = 0_{\mathbb{F}_2^m}$ alors tous les exposants valent 0, tous les éléments de la somme sont égaux à 1 et on en a 2^m.
Pour $\alpha \neq 0_{\mathbb{F}_2^m}$ soit l'hyperplan $V \stackrel{déf.}{=} \{x \in \mathbb{F}_2^m | x.\alpha = 0\} = \{\alpha\}^\perp$. Alors on a $V^c = \{x \in \mathbb{F}_2^m | x.\alpha = 1\}$. On a donc $\mathbb{F}_2^m = V \cup V^c$, $V \cap V^c = \emptyset$ et $|V| = |V^c| = 2^{m-1}$. Puisque l'on a $(-1)^{\alpha.x} = 1$ si $x \in V$ et vaut -1 si $x \in V^c$, la somme vaut 0. □

Exemple 4.4. La transformée de Fourier de la fonction $f : \mathbb{F}_2^3 \to \mathbb{F}_2$ déjà considérée dans l'exemple 4.2 est (en plongeant $\mathbb{F}_2$ dans $\mathbb{R}$) :

élément de $\mathbb{F}_2^3$	valeur de f	valeur de $\widehat{f}$
$(0,0,0)$	0	3
$(1,0,0)$	0	-1
$(0,1,0)$	0	1
$(1,1,0)$	0	1
$(0,0,1)$	1	-3
$(1,0,1)$	1	1
$(0,1,1)$	0	-1
$(1,1,1)$	1	-1

[4] Cette application est appelée *caractère*. Cette dénomination ainsi que la notation utilisée sont explicitées au chapitre 6.
[5] Cette fonction est généralement appelée *masse de Dirac* en $0_{\mathbb{F}_2^m}$.

4.4.2 Propriétés de la transformée de Fourier

4.4.2.1 Bijectivité de la transformée

Appliquons deux fois successivement la transformée de Fourier sur une fonction $\varphi \in \mathbb{R}^{\mathbb{F}_2^m}$. Soit $x \in \mathbb{F}_2^m$. Nous avons :

$$\begin{aligned}
\widehat{\widehat{\varphi}}(x) &= \sum_{\alpha\in\mathbb{F}_2^m} \widehat{\varphi}(\alpha)(-1)^{\alpha.x} \\
&= \sum_{\alpha\in\mathbb{F}_2^m} \sum_{y\in\mathbb{F}_2^m} \varphi(y)(-1)^{\alpha.y}(-1)^{\alpha.x} \\
&= \sum_{y\in\mathbb{F}_2^m} \varphi(y) \left(\sum_{\alpha\in\mathbf{F}_2^m} (-1)^{\alpha.(x\oplus y)} \right) \\
&= 2^m\varphi(x) \text{ (car } \sum_{\alpha\in\mathbb{F}_2^m} (-1)^{\alpha.(x\oplus y)} = 2^m \mathbf{1}_{\{0_{\mathbf{F}_2^m}\}}(x\oplus y) \text{ d'après le lemme 4.1).}
\end{aligned}$$

Nous avons donc montré que $\Phi_F \circ \Phi_F(\varphi) = 2^m\varphi$ pour toute fonction φ définie sur $\mathbb{F}_2^m$ et à valeurs réelles, soit encore $\Phi_F^2 = 2^m Id_{\mathbb{R}^{\mathbb{F}_2^m}}$ et en particulier Φ_F est bijective. Comme Φ_F est $\mathbb{R}$-linéaire, sa bijectivité équivaut donc au fait que $\ker(\Phi_F) = \{Id_{\mathbb{R}^{\mathbb{F}_2^m}}\}$ et donc que $\Phi_F \in GL(\mathbb{R}^{\mathbb{F}_2^m})$. Cela nous permet d'énoncer la proposition suivante.

Proposition 4.3. [Pom03] *La transformée de Fourier Φ_F est un élément de $S(\mathbb{R}^{\mathbb{F}_2^m})$ et sa transformée inverse est donnée par $\Phi_F^{-1} = \frac{1}{2^m}\Phi_F$. Par linéarité on a en outre $\Phi_F \in GL(\mathbb{R}^{\mathbb{F}_2^m})$.*

Résultant de cette proposition nous avons les deux corollaires ci-dessous.

Corollaire 4.1 (Formule d'inversion). [Pom03] *Soit $\varphi : \mathbb{F}_2^m \to \mathbb{R}$. Pour tout $x \in \mathbb{F}_2^m$ on a*

$$\varphi(x) = \frac{1}{2^m} \sum_{\alpha\in\mathbb{F}_2^m} \widehat{\varphi}(\alpha)(-1)^{x.\alpha} \ .$$

Preuve. $\varphi(x) = \frac{1}{2^m}\widehat{\widehat{\varphi}}(x) = \frac{1}{2^m} \sum_{\alpha\in\mathbb{F}_2^m} \widehat{\varphi}(\alpha)(-1)^{x.\alpha}$. □

Corollaire 4.2. [Pom03] *Pour tout $\varphi \in \mathbb{R}^{\mathbb{F}_2^m}$, on a $\varphi(0_{\mathbb{F}_2^m}) = \frac{1}{2^m} \sum_{\alpha\in\mathbb{F}_2^m} \widehat{\varphi}(\alpha)$.*

Preuve. Il s'agit d'une simple réduction à un cas particulier de la formule d'inversion pour $x = 0_{\mathbb{F}_2^m}$. □

4.4.2.2 Isomorphisme d'algèbres

L'espace vectoriel $\mathbb{R}^{\mathbb{F}_2^m}$ est pourvu d'une structure naturelle de $\mathbb{R}$-algèbre via la *multiplication terme à terme* des fonctions définie de la façon suivante :

$$\forall(\varphi,\psi) \in (\mathbb{R}^{\mathbb{F}_2^m})^2,\ \forall x \in \mathbb{F}_2^m,\ (\varphi.\psi)(x) \stackrel{déf.}{=} \varphi(x)\psi(x) \ .$$

Cette structure d'algèbre est simplement notée « $(\mathbb{R}^{\mathbb{F}_2^m}, .)$ ». L'utilisation du symbole « . » pour désigner la multiplication peut conduire à des non-sens par confusion éventuelle avec le produit scalaire de $\mathbb{F}_2^m$. Aussi le lecteur prendra garde de bien vérifier le contexte d'emploi de ce symbole. Une autre structure de $\mathbb{R}$-algèbre peut être définie sur $\mathbb{R}^{\mathbb{F}_2^m}$. Elle est décrite ci-dessous.

Définition 4.6. Pour $(\varphi,\psi)\in(\mathbb{R}^{\mathbb{F}_2^m})^2$ le *produit de convolution* de φ et ψ, noté « $\varphi*\psi$ », est défini par

$$\begin{array}{rccc}\varphi*\psi: & \mathbb{F}_2^m & \to & \mathbb{R}\\ & \alpha & \mapsto & \displaystyle\sum_{x\in\mathbb{F}_2^m}\varphi(x)\psi(x\oplus\alpha)\ .\end{array}$$

Remarque 4.3. Pour $(\varphi,\psi)\in(\mathbb{R}^{\mathbb{F}_2^m})^2$ et $\alpha\in\mathbb{F}_2^m$, on a $(\varphi*\psi)(\alpha)=\langle\varphi,\psi\circ\sigma_\alpha\rangle$ où l'on désigne, rappelons-le, par le symbole « σ_α » la translation dans $\mathbb{F}_2^m$ par α *i.e.*

$$\begin{array}{rccc}\sigma_\alpha: & \mathbb{F}_2^m & \to & \mathbb{F}_2^m\\ & x & \mapsto & x\oplus\alpha\ .\end{array}$$

Il est facile de voir que $*:(\mathbb{R}^{\mathbb{F}_2^m})^2\to\mathbb{R}^{\mathbb{F}_2^m}$ est une application bilinéaire (et symétrique). $*$ est en outre commutatif (puisque symétrique) et associatif. Aussi $\mathbb{R}^{\mathbb{F}_2^m}$ muni de ce produit est une $\mathbb{R}$-algèbre, notée « $(\mathbb{R}^{\mathbb{F}_2^m},*)$ ».

Calculons maintenant la transformée de Fourier du produit de convolution de $(\varphi,\psi)\in(\mathbb{R}^{\mathbb{F}_2^m})^2$ pour $\alpha\in\mathbb{F}_2^m$:

$$\begin{aligned}\widehat{\varphi*\psi}(\alpha) &= \sum_{y\in\mathbb{F}_2^m}(\varphi*\psi)(y)(-1)^{\alpha.y}\\ &= \sum_{y\in\mathbb{F}_2^m}\sum_{x\in\mathbb{F}_2^m}\varphi(x)\psi(y\oplus x)(-1)^{\alpha.y}\\ &= \sum_{x\in\mathbb{F}_2^m}\varphi(x)\sum_{y\in\mathbb{F}_2^m}\psi(y\oplus x)(-1)^{\alpha.y}\\ &= \sum_{x\in\mathbb{F}_2^m}\varphi(x)\sum_{z\in\mathbb{F}_2^m}\psi(z)(-1)^{\alpha.(z\oplus x)}\ \text{(par le changement de variables : } z\stackrel{déf.}{=}y\oplus x)\\ &= \sum_{x\in\mathbb{F}_2^m}\varphi(x)\left(\sum_{z\in\mathbb{F}_2^m}\psi(z)(-1)^{\alpha.z}\right)(-1)^{\alpha.x}\\ &= \sum_{x\in\mathbb{F}_2^m}\varphi(x)(-1)^{\alpha.x}\widehat{\psi}(\alpha)\\ &= \widehat{\varphi}(\alpha)\widehat{\psi}(\alpha)\ .\end{aligned}$$

Le résultat suivant vient donc d'être démontré.

Proposition 4.4 (Trivialisation du produit de convolution). [Pom03] *Quel que soit* $(\varphi,\psi)\in(\mathbb{R}^{\mathbb{F}_2^m})^2$*, on a :*

$$\widehat{\varphi*\psi}=\widehat{\varphi}.\widehat{\psi}\ .$$

Il découle trivialement de cette proposition la conclusion ci-dessous.

Corollaire 4.3. [Pom03] *La transformée de Fourier* $\Phi_F:(\mathbb{R}^{\mathbb{F}_2^m},*)\to(\mathbb{R}^{\mathbb{F}_2^m},.)$ *est un isomorphisme de* $\mathbb{R}$*-algèbres.*

Puisque par ailleurs $\Phi_F^{-1}=\dfrac{1}{2^m}\Phi_F$, à un facteur 2^m près, Φ_F est aussi un homomorphisme de $\mathbb{R}$-algèbres de $(\mathbb{R}^{\mathbb{F}_2^m},.)$ dans $(\mathbb{R}^{\mathbb{F}_2^m},*)$. Soit en d'autres termes :

Corollaire 4.4. [Pom03] *Quel que soit* $(\varphi,\psi)\in(\mathbb{R}^{\mathbb{F}_2^m})^2$*, on a :*

$$\widehat{\varphi.\psi}=\frac{1}{2^m}\widehat{\varphi}*\widehat{\psi}\ .$$

Relation de Parseval
Soit $(\varphi, \psi) \in (\mathbb{R}^{\mathbb{F}_2^m})^2$. Remarquons qu'il existe deux façons de calculer la valeur du produit de convolution pour $0_{\mathbb{F}_2^m}$ de φ par ψ. La première s'effectue par définition du produit :

$$(\varphi * \psi)(0_{\mathbb{F}_2^m}) = \sum_{x \in \mathbb{F}_2^m} \varphi(x)\psi(x) \ .$$

La seconde à l'aide de la formule d'inversion de la transformée de Fourier :

$$(\varphi * \psi)(0_{\mathbb{F}_2^m}) = \frac{1}{2^m} \sum_{\alpha \in \mathbb{F}_2^m} \widehat{\varphi * \psi}(\alpha) = \frac{1}{2^m} \sum_{\alpha \in \mathbb{F}_2^m} \widehat{\varphi}(\alpha)\widehat{\psi}(\alpha) \ .$$

Nous venons ainsi de montrer :

Proposition 4.5 (Relation de Parseval). [Pom03] *Pour tout* $(\varphi, \psi) \in (\mathbb{R}^{\mathbb{F}_2^m})^2$,

$$\sum_{\alpha \in \mathbb{F}_2^m} \widehat{\varphi}(\alpha)\widehat{\psi}(\alpha) = 2^m \sum_{x \in \mathbb{F}_2^m} \varphi(x)\psi(x) \ .$$

D'où le corollaire immédiat suivant.

Corollaire 4.5. [Pom03] *Soit* $\varphi \in \mathbb{R}^{\mathbb{F}_2^m}$. *On a*

$$\sum_{\alpha \in \mathbb{F}_2^m} \widehat{\varphi}^2(\alpha) = 2^m \sum_{x \in \mathbb{F}_2^m} \varphi^2(x) \ .$$

Si de plus φ *est à valeurs dans* $\{\pm 1\}$, *alors :*

$$\sum_{\alpha \in \mathbb{F}_2^m} \widehat{\varphi}^2(\alpha) = 2^{2m} \ .$$

Les deux égalités du corollaire ci-dessus sont de type *conservation de l'énergie*. Cela signifie que par dualité la quantité d' « énergie » totale est maintenue. La seconde égalité est particulièrement significative puisque l'on y observe la valeur de cette énergie globale.

4.4.3 La transformée de Walsh

La plupart des critères cryptographiques d'une fonction booléenne $f : \mathbb{F}_2^m \to \mathbb{F}_2$ peut s'interpréter par dualité à l'aide de sa transformée de Fourier $\widehat{f}$ (en effectuant l'assimilation désormais classique de $\mathbb{F}_2$ comme sous-ensemble de $\mathbb{R}$). Néanmoins parce que la relation de Parseval s'exprime simplement dans le cas de fonctions à valeurs dans $\{\pm 1\}$, il est plus naturel d'utiliser la transformée de Fourier de la fonction $\chi^1_{\mathbb{F}_2} \circ f : \mathbb{F}_2^m \to \{\pm 1\}$.

Définition 4.7. Pour une fonction $f : \mathbb{F}_2^m \to \mathbb{F}_2$ la transformée de Fourier de la fonction $\chi^1_{\mathbb{F}_2} \circ f : \mathbb{F}_2^m \to \mathbb{R}$ est appelée *transformée* (ou *spectre*) *de Walsh*, ou encore *transformée de Hadamard*, de f.

Soit alors $f : \mathbb{F}_2^m \to \mathbb{F}_2$ et observons les faits suivants. Tout d'abord, puisque $\chi^1_{\mathbb{F}_2} \circ f$ est à valeurs dans $\{\pm 1\}$, d'après le corollaire 4.5, $\sum_{\alpha \in \mathbb{F}_2^m} \widehat{\chi^1_{\mathbb{F}_2} \circ f}^{\,2}(\alpha) = 2^{2m}$.

Puis $\forall \alpha \in \mathbb{F}_2^m$,

$$\widehat{\chi^1_{\mathbb{F}_2} \circ f}(\alpha) = \sum_{x \in \mathbb{F}_2^m} (-1)^{f(x) \oplus \alpha.x} = |\{x \in \mathbb{F}_2^m | f(x) = \alpha.x\}| - |\{x \in \mathbb{F}_2^m | f(x) \neq \alpha.x\}| \ ,$$

alors on a

$$\widehat{\chi^1_{\mathbb{F}_2} \circ f}(\alpha) = 2|\{x \in \mathbb{F}_2^m | f(x) = \alpha.x\}| - 2^m = 2d_H(f, \overline{l_\alpha}) - 2^m \ . \tag{4.8}$$

En particulier pour tout $\alpha \in \mathbb{F}_2^m$, $\widehat{\chi^1_{\mathbb{F}_2^m} \circ f}(\alpha)$ est toujours pair et $-2^m \leq \widehat{\chi^1_{\mathbb{F}_2} \circ f}(\alpha) \leq 2^m$. La borne inférieure est atteinte pour $f = \overline{l_\alpha}$, la négation de la forme linéaire l_α, et la borne supérieure pour $f = l_\alpha$. On a en effet :

$$d_H(f, l_\alpha) = 2^m - d_H(f, \overline{l_\alpha}) = 2^{m-1} - \frac{1}{2}\widehat{\chi^1_{\mathbb{F}_2} \circ f}(\alpha) \ . \tag{4.9}$$

La transformée de Walsh reflète la coïncidence ou déviation entre f et toutes les fonctions affines. De plus comme il est aisé de voir que

$$\forall x \in \mathbb{F}_2, \ \chi^1_{\mathbb{F}_2}(x) = 1 - 2x \tag{4.10}$$

où l'on a implicitement plongé $\mathbb{F}_2$ dans $\mathbb{R}$. Il en résulte que $\chi^1_{\mathbb{F}_2} \circ f = \mathbf{1}_{\mathbb{F}_2^m} - 2f$. On en déduit, d'après le lemme 4.1, que les transformées de Fourier et de Walsh de la fonction f se trouvent reliées par la formule

$$\widehat{\chi^1_{\mathbb{F}_2} \circ f} = 2^m \mathbf{1}_{\{0_{F_2^m}\}} - 2\widehat{f} \ . \tag{4.11}$$

Soit encore par la remarque 4.2 :

$$\widehat{\chi^1_{\mathbb{F}_2} \circ f}(0_{\mathbb{F}_2^m}) = 2^m - 2w_H(f) \ . \tag{4.12}$$

4.5 Propriétés cryptographiques des fonctions booléennes

4.5.1 Introduction

Les définitions et autres outils introduits dans la première partie de ce chapitre permettent de formaliser certaines propriétés devant être assurées par les fonctions booléennes dans le cadre de leur utilisation cryptographique. Manifestement ces fonctions ne peuvent être choisies aléatoirement. Il a par exemple déjà été vu au chapitre 2 que la diffusion et la confusion doivent être garanties afin de limiter au maximum d'éventuelles attaques statistiques. Le terme « statistique » par sa trop grande généralité peut rendre perplexe le lecteur. C'est ainsi que dans cette section sont précisés les principaux critères de sécurité, abstraction faite des notions de fonction courbe et parfaitement non linéaire, lesquelles se voient attribuer la totalité des chapitres 5 et 6.

Cette section est organisée comme suit. Le premier critère présenté est celui de l'*équilibre* qui permet d'éviter l'occurrence d'un biais statistique trop manifeste. Le deuxième est la résilience qui immunise les fonctions contre les attaques par corrélation dans le cadre de combinaison de LFSRs (cf. chapitre 2). Est ensuite exposée la non linéarité qui quantifie le degré de différence d'une fonction donnée avec une fonction du code de Reed-Muller d'ordre 1. Métaphoriquement ces fonctions affines offrent autant d'opposition aux attaques cryptographiques qu'un blindage en papier résiste à un missile. Ainsi les fonctions utilisées dans un contexte sécurisé doivent être très largement différentes des fonctions affines. En dernier lieu, divers critères dits de *propagation* ou de *bonne diffusion*, sont successivement présentés. Intuitivement ils établissent l'absence de régularité au sein des fonctions et invalident ainsi toute une catégorie d'attaques fréquentielles. Ces critères mesurent aussi la « non affinité » des fonctions booléennes.

4.5.2 Les fonctions équilibrées

Lorsqu'une fonction est utilisée dans un contexte cryptographique rien ne doit différencier la distribution de ses valeurs d'une distribution uniforme. Autrement dit la fonction doit prendre chacune de ses valeurs un même nombre de fois. De cette manière un attaquant ne peut tirer aucun avantage de la connaissance d'une valeur particulière de la fonction, puisque toutes ses valeurs ont précisément la même fréquence d'occurrence.

Définition 4.8. Une fonction $f : \mathbb{F}_2^m \to \mathbb{F}_2^n$ est dite *équilibrée* si la fonction φ_f définie par

$$\begin{array}{rccl} \varphi_f : & \mathbb{F}_2^n & \to & \mathbb{N} \\ & y & \mapsto & \varphi_f(y) \stackrel{déf.}{=} |f^{-1}(\{y\})| \end{array}$$

est constante.
L'application φ_f est appelée le *compteur de pré-images* de f.

Exemple 4.5. Soit $f : \mathbb{F}_2^3 \to \mathbb{F}_2$ représentée sous sa forme algébrique normale par

$$P_f(\mathtt{X}_1, \mathtt{X}_2, \mathtt{X}_3) = \mathtt{X}_1\mathtt{X}_2 \oplus \mathtt{X}_1\mathtt{X}_3 \oplus \mathtt{X}_2\mathtt{X}_3 \ .$$

Alors f est équilibrée puisque $\varphi_f(0) = \varphi_f(1) = 4$.

Remarque 4.4.

1. Si $f : \mathbb{F}_2^m \to \mathbb{F}_2^n$ est équilibrée alors f est surjective, donc en particulier $m \geq n$, et la valeur constante de φ_f est 2^{m-n} ;

2. Une fonction $f : \mathbb{F}_2^m \to \mathbb{F}_2$ est équilibrée si elle prend les valeurs 0 et 1 exactement 2^{m-1} fois *i.e.* $w_H(f) = 2^{m-1}$. En particulier sa table de vérité contient autant d'occurrences du chiffre « 0 » que d'occurrences du chiffre « 1 ». D'après l'égalité (4.12) la fonction f est équilibrée si et seulement si $\widehat{\chi^1_{\mathbb{F}_2} \circ f}(0_{\mathbb{F}_2^m}) = 0$;

3. Soit $f : \mathbb{F}_2^m \to \mathbb{F}_2^n$. Puisque les ensembles $f^{-1}(\{y\})$, quand y varie dans $\mathbb{F}_2^n$, forment une partition de $\mathbb{F}_2^m$, on a :
$$\sum_{y \in \mathbb{F}_2^n} |f^{-1}(\{y\})| = 2^m \ ;$$

4. Soit $f : \mathbb{F}_2^m \to \mathbb{F}_2$. On désigne par « f^+ » la fonction
$$\begin{array}{rccl} f^+ : & \mathbb{F}_2^{m+1} & \to & \mathbb{F}_2 \\ & (x_1, \ldots, x_m, x_{m+1}) & \mapsto & f(x_1, \ldots, x_m) \oplus x_{m+1} \ . \end{array}$$
Alors f^+ est équilibrée. En effet :
$$\begin{array}{l} |\{(x_1, \ldots, x_m, x_{m+1}) \in \mathbb{F}_2^{m+1} | f^+(x_1, \ldots, x_m, x_{m+1}) = 0\}| = \\ |\{(x_1, \ldots, x_m, x_{m+1}) \in \mathbb{F}_2^{m+1} | f(x_1, \ldots, x_m) \oplus x_{m+1} = 0\}| = \\ |\{(x_1, \ldots, x_m) \in \mathbb{F}_2^m | f(x_1, \ldots, x_m) = 0\}| + |\{(x_1, \ldots, x_m) \in \mathbb{F}_2^m | f(x_1, \ldots, x_m) = 1\}| = 2^m \ . \end{array}$$

4.5.2.1 Fonction équilibrée et transformée de Fourier

La notion de fonction équilibrée peut se définir par dualité à l'aide de la transformée de Fourier (comme dans le point 2. de la remarque précédente).

Proposition 4.6. [CD04] *Soit $f : \mathbb{F}_2^m \to \mathbb{F}_2^n$. La fonction f est équilibrée si et seulement si pour tout $\beta \in \mathbb{F}_2^{n\,*}$,*

$$\widehat{(\chi^1_{\mathbb{F}_2} \circ l_\beta \circ f)}(0_{\mathbb{F}_2^m}) = 0 \ .$$

Preuve. En préambule, remarquons que l'on a

$$\begin{aligned}
\widehat{(\chi^1_{\mathbb{F}_2} \circ l_\beta \circ f)}(0_{\mathbb{F}_2^m}) &= \sum_{x \in \mathbb{F}_2^m} (\chi^1_{\mathbb{F}_2} \circ l_\beta \circ f)(x) \\
&= \sum_{x \in \mathbb{F}_2^m} (-1)^{\beta.f(x)} \\
&= \sum_{y \in \mathbb{F}_2^n} |f^{-1}(\{y\})|(-1)^{\beta.y} \\
&= \sum_{y \in \mathbb{F}_2^n} \varphi_f(y)(-1)^{\beta.y} \ .
\end{aligned}$$

Supposons que f soit équilibrée. Alors $\varphi_f(y) = 2^{m-n}$ quel que soit $y \in \mathbb{F}_2^n$. Donc d'après ce qui précède, $\widehat{(\chi^1_{\mathbb{F}_2} \circ l_\beta \circ f)}(0_{\mathbb{F}_2^m}) = 2^{m-n} \sum_{y \in \mathbb{F}_2^n} (-1)^{\beta.y} = 2^{m-n} 2^n \mathbf{1}_{\{0_{\mathbb{F}_2^n}\}}(\beta)$ (d'après le lemme 4.1) $= 0$ dès que $\beta \neq 0_{\mathbb{F}_2^n}$.

Supposons que $\widehat{(\chi^1_{\mathbb{F}_2} \circ l_\beta \circ f)}(0_{\mathbb{F}_2^m}) = 0 \ \forall \beta \in \mathbb{F}_2^{n\,*}$ et calculons la transformée de Fourier de φ_f :

$$\begin{aligned}
\widehat{\varphi_f}(\beta) &= \sum_{y \in \mathbb{F}_2^n} \varphi_f(y)(-1)^{\beta.y} \\
&= \sum_{y \in \mathbb{F}_2^n} |f^{-1}(\{y\})|(-1)^{\beta.y} \\
&= \widehat{(\chi \circ l_\beta \circ f)}(0_{\mathbb{F}_2^m}) \text{ (d'après ce que l'on a dit en préambule)} \\
&= 0 \text{ pour } \beta \in \mathbb{F}_2^{n\,*} \text{ par hypothèse.}
\end{aligned}$$

D'après la formule d'inversion 4.1 (p. 55) pour $\beta \in \mathbb{F}_2^n$ on a

$$\begin{aligned}
\varphi_f(\beta) &= \frac{1}{2^n} \sum_{y \in \mathbb{F}_2^n} \widehat{\varphi_f}(y)(-1)^{\beta.y} \\
&= \frac{1}{2^n} \widehat{\varphi_f}(0_{\mathbb{F}_2^n}) \\
&= \frac{1}{2^n} \sum_{y \in \mathbb{F}_2^n} \varphi_f(y) \\
&= \frac{1}{2^n} \sum_{y \in \mathbb{F}_2^n} |f^{-1}(\{y\})| \\
&= 2^{m-n} \text{ (par le point 3. de la remarque précédente).}
\end{aligned}$$

□

Une fonction booléenne, lorsqu'elle est équilibrée, impose à toutes ses fonctions coordonnées de l'être également. Mais cette propriété est encore plus forte ainsi que le précise le résultat ci-dessous.

Proposition 4.7. [SZZ95] *Une fonction $f : \mathbb{F}_2^m \to \mathbb{F}_2^n$ est équilibrée si et seulement si pour tout $\beta \in F_2^{n\,*}$, la fonction $l_\beta \circ f \in \mathbb{F}_2^{\mathbb{F}_2^m}$ est équilibrée.*

Preuve. D'après la proposition 4.6 précédente la fonction f est équilibrée si et seulement si $\forall \beta \in \mathbb{F}_2^{n\,*}$, $\widehat{(\chi^1_{\mathbb{F}_2} \circ l_\beta \circ f)}(0_{\mathbb{F}_2^m}) = 0$ ce qui est équivalent (d'après le point 2. de la remarque 4.4) à $\forall \beta \in \mathbb{F}_2^{n\,*}$, la fonction $l_\beta \circ f$ est équilibrée. □

4.5.2.2 Fonction équilibrée et produit de convolution

Nous disposons aussi d'une caractérisation de la notion d'équilibre à l'aide du carré - au sens du produit de convolution - de la fonction φ_f :

Proposition 4.8. [Pom03] *Soit $f : \mathbb{F}_2^m \to \mathbb{F}_2^n$. Alors les propositions suivantes sont équivalentes :*

1. *f est équilibrée ;*
2. *$\varphi_f * \varphi_f$ est constant, égale à 2^{2m-n} ;*
3. *$\varphi_f * \varphi_f(0_{F_2^n}) = 2^{2m-n}$.*

Preuve.
L'implication « *1.* $\Rightarrow$ *2.* » est presque triviale : soit $\beta \in \mathbb{F}_2^n$,

$$\begin{aligned} \varphi_f * \varphi_f(\beta) &= \sum_{y \in F_2^n} \varphi_f(y)\varphi_f(y \oplus \beta) \\ &= 2^n 2^{m-n} 2^{m-n} \\ &= 2^{2m-n} \ . \end{aligned}$$

L'implication « *2.* $\Rightarrow$ *3.* » n'est qu'une réduction à un cas particulier.

Enfin en ce qui concerne « *3.* $\Rightarrow$ *1.* », nous avons $2^{2m-n} = \varphi_f * \varphi_f(0_{\mathbb{F}_2^n}) = \sum_{y \in \mathbb{F}_2^n} \varphi_f^2(y)$ et d'après le point 3. de la remarque 4.4, $2^m = \sum_{y \in \mathbb{F}_2^n} \varphi_f(y)$.
L'inégalité de Cauchy-Schwarz [Sch91] donne

$$2^{2m} = \left(\sum_{y \in \mathbb{F}_2^n} \mathbf{1}_{\mathbb{F}_2^n}(y)\varphi_f(y) \right)^2 \leq \left(\sum_{y \in \mathbb{F}_2^n} 1^2 \right) \left(\sum_{y \in \mathbb{F}_2^n} \varphi_f^2(y) \right) = 2^n 2^{2m-n} \ .$$

Puisque nous avons une égalité, le compteur de pré-images φ_f est constant, multiple de $\mathbf{1}_{\mathbb{F}_2^n}$. □

4.5.2.3 Fonction équilibrée et probabilités

Supposons que $\mathbb{F}_2^m$ (respectivement $\mathbb{F}_2^n$) soit muni de la probabilité uniforme notée « $\Pr^{(m)}$ » (respectivement « $\Pr^{(n)}$ »). Le résultat suivant énonce formellement ce qu'intuitivement on entend par « fonction équilibrée » en termes de distribution de valeurs.

Lemme 4.2. *La fonction $f : \mathbb{F}_2^m \to \mathbb{F}_2^n$ est équilibrée si et seulement si $\Pr_f^{(m)} = \Pr^{(n)}$ i.e. la probabilité induite par f sur $\mathbb{F}_2^n$ est l'équiprobabilité.*

Preuve.
On a en premier lieu, $\Pr_f^{(m)}(\emptyset) = \Pr^{(m)}(f^{-1}(\emptyset)) = \Pr^{(m)}(\emptyset) = 0 = \Pr^{(n)}(\emptyset)$.
Soit maintenant $A \subset \mathbb{F}_2^n$ tel que $A \neq \emptyset$. On a :

$$\begin{aligned} \Pr_f^{(m)}(A) &= \Pr^{(m)}(f^{-1}(A)) \\ &= \frac{1}{2^m} |\{x \in \mathbb{F}_2^m | f(x) \in A\}| \\ &= \frac{1}{2^m} \sum_{y \in A} |\{x \in \mathbb{F}_2^m | f(x) = y\}| \\ &= \frac{1}{2^m} \sum_{y \in A} |f^{-1}(\{y\})| \ . \end{aligned}$$

Si f est équilibrée alors $\frac{1}{2^m}\sum_{y\in A}|f^{-1}(\{y\})| = \frac{1}{2^m}|A|2^{m-n} = \frac{|A|}{2^n} = \Pr^{(n)}(A)$ et donc la distribution des valeurs de f est uniforme sur $\mathbb{F}_2^n$.

Si inversement $\Pr_f^{(m)} = \Pr^{(n)}$ alors $\forall y \in \mathbb{F}_2^n$, $\Pr_f^{(m)}(\{y\}) = \Pr^{(n)}(\{y\}) = \frac{|\{y\}|}{2^n} = \frac{1}{2^n} = \frac{1}{2^m}2^{m-n}$. D'après la suite d'égalités précédente appliquée à $A = \{y\}$, on a $\frac{1}{2^m}\sum_{y'\in\{y\}}|f^{-1}(\{y'\})| = \frac{1}{2^m}|f^{-1}(\{y\})| = \Pr^{(m)}(\{y\})$ donc $\forall y \in \mathbb{F}_2^n, |f^{-1}(\{y\})| = 2^{m-n}$ *i.e.* la fonction f est équilibrée. □

4.5.3 La résilience

4.5.3.1 Définitions et caractérisations

Dans le cadre de la combinaison de plusieurs LFSRs, au chapitre 2, nous avons rappelé la nécessité de pouvoir mesurer la résistance des fonctions booléennes aux attaques par corrélation définies par Siegenthaler [Sie84]. La solidité en question est établie par le fait que fixer certaines variables de la fonction ne change pas sa distribution de valeurs. Ceci implique en particulier que l'on ne peut attaquer la combinaison de LFSRs en réduisant le nombre des registres « actifs ».

Nous nous employons maintenant à présenter la formalisation de ce concept dans le contexte théorique des fonctions booléennes.

Soit $m \in \mathbb{N}^*$. L'ensemble des parties de $I \stackrel{déf.}{=} \{1,\ldots,m\}$ de cardinal $k \in \mathbb{N}$ est défini par

$$I_k \stackrel{déf.}{=} \{J \subset I \mid |J| = k\} .$$

En particulier, $I_k = \emptyset$ si $k = 0$ ou $k > m$.

Soit $k \in \mathbb{N}^*$ tel que $k \leq m$. Soit $J_k \in I_k$. Remarquons que $I \setminus J_k \in I_{m-k}$. On introduit $\Phi : J_k \to \{1,\ldots,k\}$ et $\overline{\Phi} : I \setminus J_k \to \{1,\ldots,m-k\}$ les isomorphismes de treillis[6] *i.e.* Φ (respectivement $\overline{\Phi}$) est une bijection telle que pour tout $(i,j) \in J_k^2$ (respectivement $(i,j) \in (I \setminus J_k)^2$), $i < j \Leftrightarrow \Phi(i) < \Phi(j)$ (respectivement $i < j \Leftrightarrow \overline{\Phi}(i) < \overline{\Phi}(j)$).

Soient $f : \mathbb{F}_2^m \to \mathbb{F}_2$ et $(\alpha_1,\ldots,\alpha_k) \in \mathbb{F}_2^k$ fixés. On définit la fonction $f_{J_k,(\alpha_1,\ldots,\alpha_k)} : \mathbb{F}_2^{m-k} \to \mathbb{F}_2$ telle que pour $(x_1,\ldots,x_{m-k}) \in \mathbb{F}_2^{m-k}$ on ait $f_{J_k,(\alpha_1,\ldots,\alpha_k)}(x_1,\ldots,x_{m-k}) \stackrel{déf.}{=} f(y_1,\ldots,y_m)$, où pour $i \in I$ on a

$$y_i \stackrel{déf.}{=} \begin{cases} \alpha_{\Phi(i)} & \text{si } i \in J_k , \\ x_{\overline{\Phi}(i)} & \text{si } i \in I \setminus J_k . \end{cases}$$

En d'autres termes, $f_{J_k,(\alpha_1,\ldots,\alpha_k)}$ est la fonction obtenue à partir de f en fixant les k variables x_i (pour $i \in J_k$) à certaines valeurs α_j (pour $j = \Phi(i)$).

Exemple 4.6. Soient $I = \{1,2,3,4,5\}$, $J_3 = \{2,4,5\}$ et $(\alpha_1,\alpha_2,\alpha_3) = (0,1,1)$. On a alors $\Phi : \{2,4,5\} \to \{1,2,3\}$ définie par

$$\begin{cases} 2 \mapsto 1 , \\ 4 \mapsto 2 , \\ 5 \mapsto 3 \end{cases}$$

[6] Un treillis est aussi appelé *ensemble réticulé* (cf. [Bou70]).

et $\overline{\Phi} : \{1,3\} \to \{1,2\}$ définie par

$$\begin{cases} 1 \mapsto 1 \ , \\ 3 \mapsto 2 \ . \end{cases}$$

D'où

$$\begin{array}{rccl} f_{J_3,(0,1,1)} : & \mathbb{F}_2^2 & \to & \mathbb{F}_2 \\ & (x_1,x_2) & \mapsto & f_{J_3,(0,1,1)}(x_1,x_2) \stackrel{déf.}{=} f(x_1,0,x_2,1,1) \ . \end{array}$$

Ayant précisé les notations, on peut maintenant s'atteler à l'étude théorique de la résistance aux attaques par corrélation.

Une fonction $f : \mathbb{F}_2^m \to \mathbb{F}_2$ est *sans corrélation d'ordre k* si sa distribution de valeurs ne change pas lorsque l'on fixe au plus k parmi ses variables. Plus formellement, Siegenthaler [Sie84] a défini ces fonctions comme suit.

Définition 4.9. Soit $I \stackrel{déf.}{=} \{1,\ldots,m\}$. Une fonction $f : \mathbb{F}_2^m \to \mathbb{F}_2$ est dite *sans corrélation d'ordre k* si $\forall k' \in \mathbb{N}$ tel que $1 \leq k' \leq k$, $\forall (J_{k'},\alpha) \in I_{k'} \times \mathbb{F}_2^{k'}$, $\mathrm{Pr}_f^{(m)} = \mathrm{Pr}_{f_{J_{k'},\alpha}}^{(m-k')}$. Une fonction équilibrée et sans corrélation d'ordre k est dite *k-résiliente*. On dit aussi qu'elle est *résiliente d'ordre k*.

D'après le lemme 4.2 (p. 61), on déduit du fait que la fonction f est k-résiliente, que $\forall k' \in \mathbb{N}$ tel que $1 \leq k' \leq k$, $\forall (J_{k'},\alpha) \in I_{k'} \times \mathbb{F}_2^{k'}$, $\mathrm{Pr}_f^{(m)} = \mathrm{Pr}_{f_{J_{k'},\alpha}}^{(m-k')} = \mathrm{Pr}^{(2)}$ *i.e.* les distributions de valeurs de f et de toutes les restrictions de f quand on fixe au plus k variables parmi les m sont identiques à l'équiprobabilité sur $\mathbb{F}_2$.

En 1988, G.-Z. Xiao et J. L. Massey (cf. [XM88]) ont caractérisé ces notions à l'aide de la transformée de Fourier. Leur résultat est donné ici sans démonstration.

Théorème 4.2. [XM88] *Soit $f : \mathbb{F}_2^m \to \mathbb{F}_2$. La fonction f est sans corrélation d'ordre k si et seulement si*

$$\widehat{f}(\alpha) = 0 \ \forall \alpha \in \mathbb{F}_2^m \ \textit{tel que} \ 1 \leq w_H(\alpha) \leq k \ .$$

On en déduit la caractérisation en termes de spectre de Walsh suivante.

Corollaire 4.6. [XM88] *La fonction booléenne $f : \mathbb{F}_2^m \to \mathbb{F}_2$ est sans corrélation d'ordre k si et seulement si elle vérifie $\forall \alpha \in \mathbb{F}_2^n$ tel que $1 \leq w_H(\alpha) \leq k$,*

$$\widehat{\chi^1_{\mathbb{F}_2} \circ f}(\alpha) = 0 \ .$$

Si de plus $\widehat{\chi^1_{\mathbb{F}_2} \circ f}(0_{\mathbb{F}_2^m}) = 0$ (i.e. f est équilibrée) alors f est k-résiliente.

Preuve. Le premier point provient du théorème précédent et de la formule (4.11) p. 58. Le second de la définition même de la résilience. □

T. Siegenthaler [Sie84] a pour sa part établi une borne sur le degré des fonctions sans corrélation et les fonctions résilientes, borne rappelée dans la proposition suivante dont la preuve est admise.

Proposition 4.9. [Sie84] *Soit $f : \mathbb{F}_2^m \to \mathbb{F}_2$. On a les propriétés suivantes :*

- *Si f est sans corrélation d'ordre k alors* $\deg(f) \leq m-k$ *;*
- *Si f est résiliente d'ordre k alors :*
  - *si $k \leq m-2$, on a* $\deg(f) \leq m-k-1$,
  - *si $k = m-1$, on a* $\deg(f) = 1$.

4.5.3.2 Constructions classiques de fonctions résilientes

On peut maintenant exposer, sans les preuves, certaines des constructions les plus connues de fonctions résilientes. Nous avons tout d'abord deux constructions introduites par P. Camion, C. Carlet, P. Charpin et N. Sendrier [CCC+92].

La première se présente comme suit. Soient $f : \mathbb{F}_2^m \to \mathbb{F}_2$ supposée k-résiliente et $f^+ : \mathbb{F}_2^{m+1} \to \mathbb{F}_2$ définie comme dans le point 4. de la remarque 4.4 p. 59. Alors f^+ est $k+1$-résiliente.

En ce qui concerne la seconde conception de fonctions résilientes de [CCC+92], on effectue l'identification, rappelée au début de chapitre, entre les espaces vectoriels isomorphes $\mathbb{F}_2^m$ et $\mathbb{F}_2^n \times \mathbb{F}_2^{m-n}$ pour $n \in \mathbb{N}^*$ tel que $1 \leq n \leq m-1$. Soit alors $g : \mathbb{F}_2^{m-n} \to \mathbb{F}_2^n$ et $h : \mathbb{F}_2^{m-n} \to \mathbb{F}_2$. On définit pour $(x, y) \in \mathbb{F}_2^n \times \mathbb{F}_2^{m-n}$ la fonction $f : \mathbb{F}_2^m \to \mathbb{F}_2$ par

$$f(x, y) = x.g(y) \oplus h(y)$$

où on rappelle que le symbole « . » désigne le produit scalaire usuel de $\mathbb{F}_2^n$. Alors la fonction f est k-résiliente avec $k \stackrel{déf.}{=} \min_{y \in \mathbb{F}_2^{m-n}} w_H(g(y)) - 1$.

On peut citer une autre construction introduite par P. Camion et A. Canteaut dans [CC96]. Soient :

1. la donnée de m fonctions $g^{(i)} : \mathbb{F}_2^n \to \mathbb{F}_2$ pour $i \in \{1, \ldots, m\}$,
2. une fonction $h : \mathbb{F}_2^m \to \mathbb{F}_2$.

On construit une fonction résilliente $f : \mathbb{F}_2^{mn} \to \mathbb{F}_2$ comme suit. Soit $(x_1, \ldots, x_m) \in \underbrace{\mathbb{F}_2^n \times \ldots \times \mathbb{F}_2^n}_{m\ fois}$ alors $f(x_1, \ldots, x_m) \stackrel{déf.}{=} h(g^{(1)}(x_1), \ldots, g^{(m)}(x_m))$. Remarquons que l'on a identifié les deux espaces vectoriels $\mathbb{F}_2^{mn}$ et $\underbrace{\mathbb{F}_2^n \times \ldots \times \mathbb{F}_2^n}_{m\ fois}$. Si les fonctions $g^{(i)}$ sont k-résilientes et si h est sans corrélation (respectivement résiliente) d'ordre k' alors la fonction f est sans corrélation (respectivement résiliente) d'ordre $(k+1)(k'+1) - 1$.

4.5.4 La non linéarité

4.5.4.1 Définitions

Les fonctions affines, éléments de $R(1, m)$, possèdent de mauvaises propriétés cryptographiques. En guise d'illustration, il suffit par exemple de connaître leurs valeurs pour des éléments d'une base quelconque (et en zéro) pour les reconstruire entièrement. Par ailleurs ce type de fonctions est beaucoup trop régulier pour être convenablement exploité en cryptographie. La prévisibilité du comportement d'une fonction affine se trouve être ainsi un trop grand handicap et risque de causer des failles fatales dans la sécurité des systèmes de chiffrement. Ainsi la non coïncidence d'une fonction f donnée avec les fonctions affines devient donc un critère pertinent de sûreté cryptographique.

Hormis le degré algébrique, la seule autre façon que l'on connaisse pour différencier une fonction booléenne $f : \mathbb{F}_2^m \to \mathbb{F}_2$ donnée des fonctions affines est de calculer la distance de Hamming de la fonction f à l'ensemble $R(1, m)$. Comme le degré algébrique, plus cette distance est élevée est plus on considère que la fonction est différente des fonctions affines. Cette distance est appelée la *non linéarité* de f.

Définition 4.10. La *non linéarité* d'une fonction $f : \mathbb{F}_2^m \to \mathbb{F}_2$, notée « N_f », est définie par

$$\mathsf{N}_f \stackrel{déf.}{=} d_H(f, R(1,m)) \ .$$

Cette définition a été généralisée par Nyberg [Nyb92] au profit des fonctions vectorielles de la manière suivante.

Définition 4.11. Pour une fonction $f : \mathbb{F}_2^m \to \mathbb{F}_2^n$ la *non linéarité* de f est

$$\mathsf{N}_f \stackrel{déf.}{=} \min\{\mathsf{N}_{l_\beta \circ f} \in \mathbb{N} | \beta \in \mathbb{F}_2^{n\,*}\} \ .$$

4.5.4.2 Non linéarité et transformée de Fourier

La non linéarité d'une fonction $f \in \mathbb{F}_2^{\mathbb{F}_2^m}$ peut être reliée aux coefficients de sa transformée de Walsh.

Lemme 4.3. [XM88] *La non linéarité de $f : \mathbb{F}_2^m \to \mathbb{F}_2$ vérifie*

$$\mathsf{N}_f = 2^{m-1} - \frac{1}{2} \parallel \widehat{\chi^1_{\mathbb{F}_2} \circ f} \parallel_\infty$$

où pour $\varphi : \mathbb{F}_2^m \to \mathbb{R}$, $\parallel \varphi \parallel_\infty \stackrel{déf.}{=} \max_{x \in \mathbb{F}_2^m} |\varphi(x)|$.

Preuve. Soit l_α une forme linéaire. D'après la formule (4.9) p. 58 on a :

$$\begin{aligned} d_H(f, l_\alpha) &= 2^{m-1} - \frac{1}{2}\widehat{\chi^1_{\mathbb{F}_2} \circ f}(\alpha) \ , \\ d_H(f, \overline{l_\alpha}) &= 2^m - d(f, l_\alpha) = 2^{m-1} + \frac{1}{2}\widehat{\chi^1_{\mathbb{F}_2} \circ f}(\alpha) \ , \\ d_H(f, \{l_\alpha, \overline{l_\alpha}\}) &= 2^{m-1} - \frac{1}{2}|\widehat{\chi^1_{\mathbb{F}_2} \circ f}(\alpha)| \ . \end{aligned} \tag{4.13}$$

La conclusion en découle. □

Nous avons une propriété identique pour les fonctions booléennes vectorielles.

Proposition 4.10. [Nyb94] *La non linéarité de la fonction $f : \mathbb{F}_2^m \to \mathbb{F}_2^n$ vérifie :*

$$\mathsf{N}_f = 2^{m-1} - \frac{1}{2} \max_{\beta \in \mathbb{F}_2^{n\,*}} \parallel \widehat{(\chi^1_{\mathbb{F}_2} \circ l_\beta \circ f)} \parallel_\infty \ .$$

Preuve.

$$\begin{aligned} \mathsf{N}_f &\stackrel{déf.}{=} \min\{\mathsf{N}_{l_\beta \circ f} \in \mathbb{N} | \beta \in \mathbb{F}_2^{n\,*}\} \\ &= \min_{\beta \in \mathbb{F}_2^{n\,*}} (2^{m-1} - \frac{1}{2} \parallel \widehat{(\chi^1_{\mathbb{F}_2} \circ l_\beta \circ f)} \parallel_\infty) \text{ (d'après le lemme 4.3)} \\ &= 2^{m-1} - \frac{1}{2} \max_{\beta \in \mathbb{F}_2^{n\,*}} \parallel \widehat{(\chi^1_{\mathbb{F}_2} \circ l_\beta \circ f)} \parallel_\infty \ . \end{aligned}$$

□

4.5.4.3 Non linéarité et rayon de recouvrement

En appliquant l'égalité de Parseval (p. 57) ainsi que le lemme 4.3, Meier et Staffelbach [MS89] ont montré que la non linéarité d'une fonction $f : \mathbb{F}_2^m \to \mathbb{F}_2$ satisfait l'inégalité suivante :

$$\mathsf{N}_f \leq 2^{m-1} - 2^{\frac{m}{2}-1} \ . \tag{4.14}$$

En effet par la relation de Parseval on a : $\sum_{\alpha\in\mathbb{F}_2^m} (\widehat{\chi^1_{\mathbb{F}_2}\circ f(\alpha)})^2 = 2^{2m}$ donc $2^m \max_{\alpha\in\mathbb{F}_2^m} (\widehat{\chi^1_{\mathbb{F}_2}\circ f}(\alpha))^2 \geq 2^{2m}$ ce qui implique que $\max_{\alpha\in\mathbb{F}_2^m} |\widehat{\chi^1_{\mathbb{F}_2^m}\circ f}(\alpha)| \geq 2^{\frac{m}{2}}$.

Cette borne, généralement notée « $\rho(1,m)$ » et appelée *rayon de recouvrement* du code de Reed-Muller d'ordre 1, représente la valeur maximale que peut atteindre la non linéarité d'une fonction de $\mathbb{F}_2^{\mathbb{F}_2^m}$.

Remarquons au passage que lorsque cette borne est atteinte, on a

$$\| \widehat{\chi^1_{\mathbb{F}_2}\circ f} \|_\infty = 2^{\frac{m}{2}} \Leftrightarrow \max_{\alpha\in\mathbb{F}_2^m} |\widehat{\chi^1_{\mathbb{F}_2}\circ f}(\alpha)| = 2^{\frac{m}{2}} \Leftrightarrow \max_{\alpha\in\mathbb{F}_2^m} (\widehat{\chi^1_{\mathbb{F}_2}\circ f}(\alpha))^2 = 2^m \ .$$

Or pour que le maximum d'une variable aléatoire numérique (*i.e.* à valeurs dans $\mathbb{R}$) définie sur un espace probabilisé muni de la loi de probabilité uniforme et prenant un nombre fini de valeurs soit égale à son espérance mathématique il faut et il suffit que cette variable aléatoire soit constante. Dans le cas présent, si on suppose $\mathbb{F}_2^m$ muni de l'équiprobabilité $\Pr^{(m)}$, l'espérance de la variable aléatoire $\mathbf{X}$ définie pour $\alpha \in \mathbb{F}_2^m$ par $\mathbf{X}(\alpha) = (\widehat{\chi^1_{\mathbb{F}_2}\circ f}(\alpha))^2$ est $\sum_{\alpha\in\mathbb{F}_2^m} \Pr^{(m)}(\{\alpha\})\mathbf{X}(\alpha) = \frac{1}{2^m}\sum_{\alpha\in\mathbb{F}_2^m} (\widehat{\chi^1_{\mathbb{F}_2}\circ f}(\alpha))^2$ et vaut, d'après la relation de Parseval, la valeur 2^m qui est elle-même égale au maximum de cette variable aléatoire. On en déduit que

$$\begin{aligned} \| \widehat{\chi^1_{\mathbb{F}_2}\circ f} \|_\infty = 2^{\frac{m}{2}} &\Leftrightarrow \forall\alpha\in\mathbb{F}_2^m,\ (\widehat{\chi^1_{\mathbb{F}_2}\circ f}(\alpha))^2 = 2^m \\ &\Leftrightarrow \forall\alpha\in\mathbb{F}_2^m,\ \widehat{\chi^1_{\mathbb{F}_2}\circ f}(\alpha) = \pm 2^{\frac{m}{2}} \ . \end{aligned}$$

On a donc finalement :

$$\mathsf{N}_f = \rho(1,m) \Leftrightarrow \forall\alpha\in\mathbb{F}_2^m,\ \widehat{\chi^1_{\mathbb{F}_2}\circ f}(\alpha) = \pm 2^{\frac{m}{2}} \ .$$

Les fonctions satisfaisant cette relation sont dites *courbes*. Le chapitre 5 leur est en grande partie dédié.

4.5.5 La bonne diffusion

4.5.5.1 Introduction

Le vocable « bonne diffusion » embrasse plusieurs notions en rapport avec le niveau de discordance entre une fonction booléenne donnée et les fonctions affines. Il s'agit de mesures, distinctes de la non linéarité, qui œuvrent néanmoins dans le même objectif : l'établissement de caractéristiques discriminantes des fonctions hautement non affines. Mis à part la notion de distance de linéarité, les autres mesures présentées dans cette sous-section sont exposées d'un point de vue combinatoire via des calculs de cardinaux appropriés.

Mais qu'est-ce que la bonne diffusion ?
Cette notion a évidemment trait aux *guidelines* (ou recommandations) de conception de cryptosystèmes originellement stipulées par Shannon, et reprises ensuite en partie par Massey (cf. chapitre 2 sous-section 2.2.5). Il s'agit en fait d'une tentative d'abstraction de la notion informelle de diffusion. Le *principe actif* de la diffusion est constitué par l'influence des bits en entrée d'une fonction booléenne sur ceux de ses valeurs correspondantes. Cette influence est établie en

mesurant ce que produit en sortie la modification de la valeur de certains bits en entrée.

Illustrons ces propos dans le cas trivial d'un changement d'un unique bit en entrée pour une fonction $f : \mathbb{F}_2^m \to \mathbb{F}_2^n$. Soit donc $i \in \{1, \ldots, m\}$. Afin de quantifier le « poids » du $i^{ème}$ bit dans le comportement de f, il suffit d'étudier la fonction $f \oplus (f \circ \sigma_{e^{(i)}})$. On rappelle que $e^{(i)}$ est le $i^{ème}$ vecteur de la base canonique de $\mathbb{F}_2^m$ et « $\sigma_{e^{(i)}}$ » représente la translation, dans $\mathbb{F}_2^m$, par $e^{(i)}$. Cette différence permet donc d'évaluer l'impact du $i^{ème}$ bit de f sur ses sorties. Dans la situation la pire, un bit en entrée influence un et un seul bit en sortie, disons le $j^{ème}$, il s'agit par exemple du cas du masque jetable, ce qui se traduit par $\forall x \in \mathbb{F}_2^m$, $f(x) \oplus f(x \oplus e^{(i)}) = e^{(j)}$ (où cette fois $e^{(j)} \in \mathbb{F}_2^n$). Plus généralement, on dira que f possède une mauvaise diffusion s'il existe $(\alpha, \beta) \in \mathbb{F}_2^{m*} \times \mathbb{F}_2^n$ tel que $\forall x \in \mathbb{F}_2^m$, $f(x) \oplus f(x \oplus \alpha) = \beta$. On s'aperçoit que ce symptôme est présenté par les fonctions affines de $\mathbb{F}_2^m$ dans $\mathbb{F}_2^n$: $\sigma_\beta \circ \lambda$ avec $\beta \in \mathbb{F}_2^n$ et $\lambda \in \mathcal{L}(\mathbb{F}_2^m, \mathbb{F}_2^n)$. En effet pour tout $(x, \alpha) \in \mathbb{F}_2^m \times \mathbb{F}_2^{m*}$, $\sigma_\beta \circ \lambda(x \oplus \alpha) = (\lambda(x) \oplus \lambda(\alpha)) \oplus \beta = \lambda(x) \oplus \beta \oplus \lambda(\alpha) = \sigma_\beta \circ \lambda(x) \oplus \beta$. Encore une fois, comme cela a déjà été précisé en exorde de cette sous-section, il faut maximiser la dissemblance entre les fonctions cryptographiques et ces fonctions affines - épouvantails de la cryptographie - afin d'obtenir une *bonne diffusion*.

4.5.5.2 La dérivée

La dérivation des fonctions booléennes est l'un des outils principalement utilisés dans les travaux contenus dans ce manuscrit. On la rencontrera ainsi plusieurs fois et sous plusieurs formes.

Définition 4.12. Soit $f : \mathbb{F}_2^m \to \mathbb{F}_2^n$. La *dérivée* de f suivant la direction $\alpha \in \mathbb{F}_2^m$ est l'application

$$\begin{array}{rccl} d_\alpha f : & \mathbb{F}_2^m & \to & \mathbb{F}_2^n \\ & x & \mapsto & d_\alpha f(x) \stackrel{déf.}{=} f(x \oplus \alpha) \oplus f(x) \ . \end{array}$$

Remarque 4.5. Pour $f : \mathbb{F}_2^m \to \mathbb{F}_2^n$ et $\alpha \in \mathbb{F}_2^m$, on a $d_\alpha f = (f \circ \sigma_\alpha) \oplus f$. Le comportement de la dérivée de f dépend donc de celui de f lorsqu'on lui applique une translation sur ses entrées.

Voici deux lemmes faciles établissant les premières propriétés de la dérivée.

Lemme 4.4. [Pom03] *Soit $(f, g) \in (\mathbb{F}_2^{n\,\mathbb{F}_2^m})^2$ et $\alpha \in \mathbb{F}_2^m$. Alors :*

1. $d_\alpha(f \oplus g) = d_\alpha f \oplus d_\alpha g$,
2. $\deg(d_\alpha f) \leq \deg(f) - 1$.

Preuve.
Le point 1. est trivial.
Concernant le point 2., supposons sans perte de généralité que $n = 1$ et que la forme algébrique normale de f soit $\mathtt{X}_1 \ldots \mathtt{X}_k$ pour un certain $k \in \mathbb{N}^*$. Alors

$$d_\alpha f(x) = (x_1 \oplus \alpha_1) \ldots (x_k \oplus \alpha_k) \oplus x_1 \ldots x_k \ .$$

Bien évidemment son degré est inférieur ou égal à $k - 1$. □

Lemme 4.5. [Pom03]
Soit $f : \mathbb{F}_2^m \to \mathbb{F}_2^n$. Si la fonction f est constante alors $d_\alpha f$ vaut identiquement la valeur $0_{\mathbb{F}_2^n}$ quel que soit $\alpha \in F_2^m$.
Soit $f : \mathbb{F}_2^m \to \mathbb{F}_2$. Si la fonction f est affine alors $d_\alpha f$ est constante quel que soit $\alpha \in F_2^m$.

Preuve.
Le premier point est évident.
Pour le second point si f est affine alors il existe $(\alpha, \beta) \in \mathbb{F}_2^m \times \mathbb{F}_2$ tel que $f = \sigma_\beta \circ l_\alpha$. Soit $(\gamma, x) \in (\mathbb{F}_2^m)^2$. On a $d_\gamma f(x) = d_\gamma(\sigma_\beta \circ l_\alpha)(x) = \alpha.(x \oplus \gamma) \oplus \alpha.x \oplus \beta = \alpha.\gamma \oplus \beta$. □

L'un des défauts que l'on tente de supprimer pour les fonctions booléennes utilisées en cryptographie a été introduit par Evertse [Eve88] sous le nom de *structure linéaire* et s'exprime à l'aide de la dérivée.

Définition 4.13. Un vecteur $\alpha \in \mathbb{F}_2^m$ est appelé *structure linéaire* de $f : \mathbb{F}_2^m \to \mathbb{F}_2^n$ si $d_\alpha f$ est constante.

Remarque 4.6.

1. Soient $(\alpha, \beta, x) \in (\mathbb{F}_2^m)^3$ et $f : \mathbb{F}_2^m \to \mathbb{F}_2^n$. Alors $d_{\alpha\oplus\beta} f(x) = f(x \oplus \alpha \oplus \beta) \oplus f(x) = f(x\oplus\alpha\oplus\beta)\oplus f(x\oplus\beta)\oplus f(x\oplus\beta)\oplus f(x) = d_\alpha f(x\oplus\beta)\oplus d_\beta f(x)$ donc $d_{\alpha\oplus\beta} = d_\alpha(f\circ\sigma_\beta)\oplus d_\beta f$;

2. Si $\delta : \mathbb{F}_2^m \to \mathbb{F}_2^n$ est affine alors tout vecteur de $\mathbb{F}_2^m$ est une structure linéaire de δ ;

3. $0_{\mathbb{F}_2^m}$ est toujours une structure linéaire de toute fonction $f : \mathbb{F}_2^m \to \mathbb{F}_2^n$;

4. Si $\alpha \in \mathbb{F}_2^m$ et $\beta \in \mathbb{F}_2^m$ sont des structures linéaires d'une fonction f alors il en est de même de $\alpha \oplus \beta$ d'après le premier point ci-dessus de la remarque. Ainsi les structures linéaires de f forment un sous-espace vectoriel de $\mathbb{F}_2^m$. Sur ce sous-espace f est affine. On en conclut que la réciproque du second point de la remarque est tout aussi vrai. On note « V_f^{SL} » le sous-espace des structures linéaires d'une fonction f ;

5. Soient $f : \mathbb{F}_2^k \to \mathbb{F}_2^m$ et $\lambda \in \mathcal{L}(\mathbb{F}_2^m, \mathbb{F}_2^n)$ alors pour tout $\alpha \in \mathbb{F}_2^k$, $d_\alpha(\lambda \circ f) = \lambda \circ d_\alpha f$.

L'ensemble des fonctions affines

Nous ouvrons ici une courte parenthèse afin d'évoquer la structure algébrique de l'ensemble des fonctions affines de $\mathbb{F}_2^m$ dans $\mathbb{F}_2^n$.

En premier lieu, cet ensemble est noté « $A(\mathbb{F}_2^m, \mathbb{F}_2^n)$ » et, dans le cas particulier où $m = n$, simplement « $A(\mathbb{F}_2^m)$ ». Nous avons donc $R(1, m) = A(\mathbb{F}_2^m, \mathbb{F}_2)$. Le sous-ensemble de $A(\mathbb{F}_2^m)$ défini par $\{\sigma_\alpha \circ \lambda \in A(\mathbb{F}_2^m) | \alpha \in \mathbb{F}_2^m,\ \lambda \in GL(\mathbb{F}_2^m)\}$ est quant à lui désigné par « $GA(\mathbb{F}_2^m)$ ». Cet ensemble contient à la fois $GL(\mathbb{F}_2^m)$ et $T(\mathbb{F}_2^m)$.

L'ensemble $A(\mathbb{F}_2^m, \mathbb{F}_2^n)$ peut être muni de la loi d'addition modulo 2 terme à terme des applications. Il devient ainsi un groupe abélien. On peut par ailleurs pourvoir $GA(\mathbb{F}_2^m)$ d'une structure de groupe pour la loi de composition. Toutefois dans ce cas, le groupe obtenu est non commutatif.

Etudions donc plus particulièrement cet ensemble. On peut observer que $GA(\mathbb{F}_2^m)$ est un sous-groupe de $S(\mathbb{F}_2^m)$. Précisément $GA(\mathbb{F}_2^m)$ est isomorphe au produit semi-direct $GL(\mathbb{F}_2^m) \ltimes_\Psi T(\mathbb{F}_2^m)$ où l'homomorphisme de groupes Ψ est ici défini par

$$\begin{array}{rccl} \Psi : & GL(\mathbb{F}_2^m) & \to & Aut(T(\mathbb{F}_2^m)) \\ & \lambda & \mapsto & (\Psi(\lambda) : \sigma_\alpha \mapsto \sigma_\alpha \circ \lambda)\ . \end{array}$$

On rappelle ci-dessous la notion de produit semi-direct.

Définition 4.14. Soient $(G, \top_G)$ et $(H, \top_H)$ deux groupes et $\Psi : (G, \top_G) \to Aut((H, \top_H))$ un homomorphisme de groupes. L'ensemble $G \times H$ muni de la loi de composition interne $\ltimes_\Psi$ définie par

$$\begin{array}{rccl} \ltimes_\Psi : & (G \times H)^2 & \to & G \times H \\ & ((x_1, y_1), (x_2, y_2)) & \mapsto & (x_1, y_1) \ltimes_\Psi (x_2, y_2) \overset{déf.}{=} (x_1 \top_G x_2, y_1 \top_H \Psi(x_1)(y_2)) \end{array}$$

est un groupe appelé *produit semi-direct* de G et H (par l'application Ψ) et noté « $G \ltimes_\Psi H$ ».

4.5.5.3 Critères de diffusion

La dérivée est utilisée comme instrument fondamental de l'étude pratique de la diffusion. Les critères les plus communément admis sont donnés ici. Historiquement le premier d'entre eux, mis en exergue par Feistel [Fei73], fut le *critère d'avalanche*. Le *critère d'avalanche strict* a ensuite été introduit par Webster et Tavares (cf. [WT86]). Puis Preenel et al. (cf. [PvLvL+91]) l'ont généralisé sous le terme de *critère de propagation*.

Définition 4.15. Une fonction $f : \mathbb{F}_2^m \to \mathbb{F}_2^n$ satisfait le *critère d'avalanche* si

$$\forall i \in \{1, \ldots, m\}, \ \sum_{x \in \mathbb{F}_2^m} d_H(f(x), f(x \oplus e^{(i)})) = n2^{m-1} \ .$$

Cela signifie qu'une moyenne statistique de la moitié du nombre des bits en sortie varie lorsque seulement un bit en entrée est complémenté. En effet, pour $x \in \mathbb{F}_2^m$ fixé, $d_H(f(x), f(x \oplus e^{(i)}))$ est le nombre de bits en sortie de f qui varient lorsque seul le $i^{ème}$ bit en entrée est complémenté. Ainsi la somme « $\sum_{x \in \mathbb{F}_2^m} d_H(f(x), f(x \oplus e^{(i)}))$ » est égale au nombre total de bits qui varient par complémentation du $i^{ème}$. Si f vérifie le critère d'avalanche alors $\frac{1}{2^m} \sum_{x \in \mathbb{F}_2^m} d_H(f(x), f(x \oplus e^{(i)})) = \frac{n}{2}$ et donc le nombre moyen de bits en sortie qui sont modifiés est $\frac{n}{2}$.

Les principaux autres critères sont listés ci-dessous.

Définition 4.16. Soit $I \stackrel{déf.}{=} \{1, \ldots, m\}$. Une fonction $f : \mathbb{F}_2^m \to \mathbb{F}_2$ satisfait

1. une *bonne diffusion* par rapport à $\alpha \in \mathbb{F}_2^m$ si $d_\alpha f$ est équilibrée ;

2. le *critère d'avalanche strict* noté « *CAS* » si elle possède une bonne diffusion par rapport à tous les vecteurs $\alpha \in \mathbb{F}_2^m$ tels que $w_H(\alpha) = 1$;

3. $CAS(k)$ pour $k \in \mathbb{N}^*$ si $\forall k' \in \mathbb{N}^*$ tel que $1 \leq k' \leq k$, on a $\forall (J_{k'}, \alpha) \in I_{k'} \times \mathbb{F}_2^{k'}$, $f_{J_{k'},\alpha}$ satisfait CAS ;

4. le *critère de propagation* noté « PC » par rapport à l'ensemble $A \subset \mathbb{F}_2^m$ si f possède une bonne diffusion par rapport à tous les éléments de A ;

5. PC de degré n, pour $n \in \mathbb{N}^*$, noté « $PC(n)$ », si elle possède une bonne diffusion pour tout $\alpha \in F_2^m$ tel que $1 \leq w_H(\alpha) \leq n$;

6. $PC(n)$ d'ordre k, pour $(k, n) \in (\mathbb{N}^*)^2$ tel que $k + n \leq m$, si $\forall k' \in \mathbb{N}^*$ tel que $1 \leq k' \leq k$, on a $\forall (J_{k'}, \alpha) \in I_{k'} \times \mathbb{F}_2^{k'}$, $f_{J_{k'},\alpha}$ vérifie $PC(n)$;

7. le *critère de propagation étendue* $EPC(n)$ d'ordre k (pour $(n, k) \in (\mathbb{N}^*)^2$) si pour tout $\alpha \in \mathbb{F}_2^m$ tel que $1 \leq w_H(\alpha) \leq n$, la dérivée $d_\alpha f$ est k-résiliente.

Remarque 4.7.

1. Les fonctions affines n'ont de bonne diffusion par rapport à aucun vecteur ;

2. Par rapport à $0_{F_2^m}$ aucune fonction n'a une bonne diffusion ;

3. *CAS* signifie qu'une modification d'un seul bit en entrée change exactement la moitié des valeurs de f ;

4. On a $CAS = PC(1)$ et $CAS(k)$ est égal à $PC(1)$ d'ordre k ;

Les fonctions booléennes offrant la meilleure diffusion possible sont les fonctions parfaitement non linéaires ou courbes décrites, dans le contexte booléen, au chapitre 5.

4.5.5.4 Distance de linéarité

Les structures linéaires permettent de distinguer les fonctions affines des autres fonctions. Ces objets sont donc susceptibles d'être utilisés dans une mesure de la diffusion.

Soit $SL_m \stackrel{déf.}{=} \{f : \mathbb{F}_2^m \to \mathbb{F}_2 | V_f^{SL} \setminus \{0_{\mathbb{F}_2^m}\} \neq \emptyset\}$ *i.e.* l'ensemble des fonctions qui ont au moins une structure linéaire non nulle. Il s'agit d'une union de sous-espaces vectoriels pour une structure linéaire fixée, cependant ce n'est en général pas lui-même un sous-espace vectoriel.

Définition 4.17. Soit $f : \mathbb{F}_2^m \to \mathbb{F}_2$. La distance de Hamming de f à l'ensemble SL_m

$$\mathsf{L}_f \stackrel{déf.}{=} d_H(f, SL_m) \tag{4.15}$$

est appelée la *distance de linéarité* de f.

Remarque 4.8.

1. $\mathsf{L}_f = 0 \Leftrightarrow f \in SL_m$.
2. Puisque $R(1, m) \subset SL_m$, on a en particulier $\mathsf{L}_f \leq \mathsf{N}_f$.

Intuitivement afin d'obtenir la meilleure diffusion, il faut maximiser la valeur de L_f. Quelle peut être sa valeur maximale ?

Soit donc $f : \mathbb{F}_2^m \to \mathbb{F}_2$. Soit $\alpha \in \mathbb{F}_2^{m*}$ fixé. On décompose $\mathbb{F}_2^m$ en deux sous-ensembles :

$$\begin{array}{l} \Delta_f(\alpha, 0) \stackrel{déf.}{=} \{x \in \mathbb{F}_2^m | d_\alpha f(x) = 0\} \ , \\ \Delta_f(\alpha, 1) \stackrel{déf.}{=} \{x \in \mathbb{F}_2^m | d_\alpha f(x) = 1\} \end{array} \tag{4.16}$$

de cardinaux $n_0(\alpha) \stackrel{déf.}{=} |\Delta_f(\alpha, 0)|$ et $n_1(\alpha) \stackrel{déf.}{=} |\Delta_1(\alpha, 1)| = 2^m - n_0(\alpha)$.

Supposons dans un premier temps que $n_0(\alpha) \geq n_1(\alpha)$. Pour transformer f en une fonction qui a α comme structure linéaire, on doit changer au moins $\dfrac{n_1(\alpha)}{2}$ de ses valeurs, ce qui est suffisant. Pour voir cela, soit $\Delta_f(\alpha, 1) = A' \cup A''$, décomposé en deux sous-ensembles quelconques de même taille, tels que $x \in A' \Leftrightarrow x \oplus \alpha \in A''$ et $|A'| = |A''| = \dfrac{n_1(\alpha)}{2}$. Alors la fonction $f' : \mathbb{F}_2^m \to \mathbb{F}_2$ définie par

$$x \mapsto \begin{cases} f(x) \oplus 1 & \text{pour } x \in A' \ , \\ f(x) & \text{sinon} \ , \end{cases}$$

a α comme structure linéaire. En effet soit $x \in \mathbb{F}_2^m$, on a :

$$d_\alpha f'(x) = f'(x \oplus \alpha) \oplus f'(x) = \begin{cases} f(x \oplus \alpha) \oplus f(x) & = 0 \text{ pour } x \in \Delta_f(\alpha, 0) \ , \\ f(x \oplus \alpha) \oplus f(x) \oplus 1 & = 0 \text{ pour } x \in A' \ , \\ f(x \oplus \alpha) \oplus 1 \oplus f(x) & = 0 \text{ pour } x \in A'' \ , \end{cases}$$

et ceci ne peut être fait avec moins de changements.

Si maintenant $n_0(\alpha) < n_1(\alpha)$, pour transformer f en une fonction g tel que $\alpha \in V_g^{SL}$, en raisonnant comme précédemment on trouve que l'on a besoin de $\frac{n_0(\alpha)}{2}$ changements. Donc la distance de f à n'importe quelle fonction g de SL_m ayant α comme structure linéaire est

$$d_H(f,g) \geq \min\{\frac{n_0(\alpha)}{2}, \frac{n_1(\alpha)}{2}\}$$

et cette valeur est atteinte par un g *ad hoc*. En définissant pour $\alpha \in \mathbb{F}_2^{m*}$

$$n_f(\alpha) \stackrel{déf.}{=} \min\{\frac{n_0(\alpha)}{2}, \frac{n_1(\alpha)}{2}\} , \tag{4.17}$$

on en déduit

$$\mathsf{L}_f = \min\{n_f(\alpha) \in \mathbb{N} | \alpha \in \mathbb{F}_2^{m*}\} . \tag{4.18}$$

Puisque par ailleurs on a toujours $n_0(\alpha) + n_1(\alpha) = 2^m$ on a

$$\mathsf{L}_f \leq 2^{m-2} . \tag{4.19}$$

On a donc démontré le résultat suivant.

Proposition 4.11. [MS89] *La distance de linéarité d'une fonction $f : \mathbb{F}_2^m \to \mathbb{F}_2$ vérifie :*

$$\mathsf{L}_f \leq 2^{m-2} .$$

Les fonctions booléennes exhibant l'aspect le moins régulier au sens de la distance de linéarité sont celles atteignant cette borne supérieure, évoquée à nouveau au chapitre 5.

4.5.6 Compromis

Les critères présentés ont chacun leur but et leur importance. Néanmoins il ne faut pas imaginer que des fonctions cryptographiques puissent satisfaire simultanément chacun d'entre eux ; ceci est impossible. En effet certaines notions sont antinomiques. Nous verrons par exemple au chapitre 5 que les fonctions possédant la meilleure non linéarité possible, les fonctions booléennes courbes, ne sauraient être équilibrées et donc encore moins résilientes. Aussi l'exploitation d'une fonction au sein d'un algorithme de chiffrement nécessite ainsi un savant dosage entre ces propriétés afin d'optimiser la sécurité du système.

4.5.6.1 Degré algébrique et fonction sans corrélation

La proposition 4.9 établie par Siegenthaler implique nécessairement qu'une fonction de $\mathbb{F}_2^{\mathbb{F}_2^m}$ n'a pas la possibilité de posséder conjointement un haut degré algébrique et un ordre de non corrélation k élevé puisque son degré est majoré par $m - k$. Ainsi ces deux critères cryptographiques sont fatalement incompatibles.

4.5.6.2 Non linéarité et fonction sans corrélation

Dans le paragraphe 4.5.4.3 nous avons observé que la non linéarité N_f d'une fonction $f : \mathbb{F}_2^m \to \mathbb{F}_2$ est maximale *i.e.* atteint la valeur du rayon de recouvrement du code de Reed-Muller d'ordre 1 si et seulement si $\forall \alpha \in \mathbb{F}_2^m$, $\widehat{\chi^1_{\mathbb{F}_2} \circ f}(\alpha) = \pm 2^{\frac{m}{2}}$. Par ailleurs la caractérisation de l'ordre d'immunité aux corrélations à l'aide de la transformée de Walsh, exposée dans le corollaire 4.6, indique que cette même fonction f est sans corrélation d'ordre k si et seulement si $\forall \alpha \in \mathbb{F}_2^m$ tel que $1 \leq w_H(\alpha) \leq k$, $\widehat{\chi^1_{\mathbb{F}_2} \circ f}(\alpha) = 0$. Il en résulte trivialement que dès que $k \geq 1$, f ne peut être de non linéarité maximale. Une fois encore nous disposons de deux critères résolument incompatibles.

4.6 Conclusion

L'outil essentiel de la cryptographie à clef secrète, les fonctions booléennes, fut le sujet du présent chapitre. Celui-ci était ainsi constitué d'une collection de résultats classiques. Outre les critères cryptographiques concernant le choix des fonctions, ont été rappelées les notions de base relevant des fonctions booléennes ainsi que de la théorie de Fourier dans le cadre des espaces vectoriels sur le corps $\mathbb{F}_2$.

Lors de la conception de cryptosystèmes utilisant une (voire plusieurs) fonction(s) booléenne(s), les propriétés cryptographiques de celle(s)-ci ne sont pas à négliger. Ainsi que nous l'avons remarqué les fonctions cryptographiques doivent, de préférence, être très différentes des fonctions affines.

Arrêtons-nous un instant sur l'adjectif *affine*. Il qualifie à la fois les éléments de $R(1,m)$, ceux de $A(\mathbb{F}_2^m, \mathbb{F}_2^n)$ et enfin ceux de $GA(\mathbb{F}_2^m)$. Puisque la confusion est possible, le lecteur prendra soin de ne pas considérer ces termes hors du contexte. Au chapitre 5 nous enrichissons d'autres signes ostentatoires de « non affinité » le recueil des critères de sécurité. Ils constituent le fondement théorique sur lequel les résultats développés dans ce manuscrit reposent.

Signalons enfin que l'incompatibilité observée entre certaines propriétés cryptographiques rend complexe sinon insoluble le problème d'obtention d'un système de chiffrement optimalement sûr au sens large du terme. La configuration idéale n'existant pas, il est nécessaire de maximiser mutuellement différents critères significatifs en tenant compte du contexte permettant éventuellement de favoriser certains d'entre eux.

A dire vrai, même pour les fonctions booléennes, rien n'est ni complètement vrai ni absolument faux, mais tout est un peu des deux à la fois.

Chapitre 5

Non linéarité parfaite et fonction courbe dans le cas booléen

La courbe ne peut inclure la ligne droite.

KOAN ZEN, *Proverbe zen*

Sommaire

5.1 Introduction

Nous sommes désormais en mesure de présenter le fondement théorique sur lequel se base notre travail. Comprendre les développements décrits dans ce manuscrit, c'est aussi appréhender les limites parfois subtiles des notions exposées maintenant. Un peu à l'instar de la gravité qui attire les masses, nous reviendrons toujours dans la suite à ces concepts comme poussés par une force invisible.

D'un côté nous avons les fonctions *parfaitement non linéaires*, de l'autre, les fonctions *courbes*. Ce chapitre, dans son intégralité, est consacré à ces notions dans un contexte booléen qui est le cadre classique pour leur présentation.

Les fonctions parfaitement non linéaires sont les fonctions les plus résistantes à l'attaque différentielle. Elles offrent le moins de régularités « affines » possibles. Figurativement, pour aller d'un point A à un point B elles préfèrent de sinueux détours à la ligne droite.

Les fonctions courbes sont ces fonctions booléennes maximalement non linéaires à un nombre pair de variables. Elles ont été introduites par Rothaus en 1976. Du fait de leur propre intérêt en tant qu'intriguants objets combinatoires mais aussi du fait de leurs applications à la cryptographie (résistance à la cryptanalyse linéaire) et leurs relations avec la théorie des codes (code

de Reed-Muller), elles ont provoqué de nombreuses et fécondes recherches.

Ces deux espèces de fonctions, bien que de définitions simples, sont rares. Leur densité dans l'ensemble des fonctions booléennes est si faible que l'on peut les comparer à des singularités.

Ces deux espèces de fonctions donc, d'apparences distinctes, représentent en fait les mêmes objets vus sous des angles différents. Les fonctions parfaitement non linéaires s'observent dans le monde de la combinatoire alors qu'on trouve les fonctions courbes dans le domaine de la théorie de Fourier. Ainsi étudier une des deux notions revient à analyser l'autre. C'est un peu comme une pièce de monnaie qui disposerait de deux côtés faces.

La transformée de Fourier est l'instrument qui permet de passer d'un monde à l'autre, le miroir déformant renvoyant la vision courbe d'une fonction parfaitement non linéaire et réciproquement. La *dualité* de Fourier sert ainsi de passeport entre les deux concepts.

Cependant cet *isomorphisme* conceptuel n'est essentiellement vrai que dans l'univers des fonctions booléennes ainsi que nous l'apprend le chapitre 6. Mais cela nous le gardons pour plus tard. Pour l'heure nous nous focalisons sur ces notions dans le cas booléen.

Avant de suivre le chemin menant à la non linéarité parfaite et autres fonctions courbes, examinons le contenu de ce chapitre ainsi que son agencement. La prochaine section est consacrée aux définitions et premiers résultats concernant les deux concepts essentiels du chapitre. On y trouve, entre autres, la description explicite de leur équivalence. Dans la section 5.3 on découvre certaines des nombreuses propriétés des fonctions parfaitement non linéaires et courbes ainsi que plusieurs de leurs caractérisations. La section 5.4 est quant à elle un recueil des constructions les plus connues de fonctions courbes. Nous débordons légèrement du sujet dans la section 5.5 en abordant les notions de fonctions presque parfaitement non linéaires et presque courbes *i.e.* les fonctions qui offrent, dans les cas où les fonctions parfaitement non linéaires et courbes n'existent pas, la résistance optimale face respectivement aux attaques différentielle et linéaire. Comme de coutume, ce chapitre est clos par une conclusion, sorte de pont vers le chapitre 6.

Il est grand temps maintenant de visiter cet espace des fonctions booléennes localement courbé par la présence d'un puissant champ de non linéarité parfaite.

5.2 Non linéarité parfaite et fonction courbe dans le cas booléen

5.2.1 Introduction

La redondance permet, dans les domaines de l'aéronautique ou du nucléaire par exemple, d'augmenter très sensiblement la sécurité ou la fiabilité des systèmes utilisés. Nous en usons ici pour souligner davantage - s'il fallait encore le faire - l'importance fondamentale des notions de fonctions parfaitement non linéaire et courbe dans les développements exposés dans ce manuscrit.

Ces fonctions, nous l'avons déjà précisé, constituent le matériau idéal pour bâtir des systèmes de chiffrement garantissant un haut niveau de résistance aux attaques différentielle et linéaire.

La non linéarité parfaite représente le degré maximum de non coïncidence avec l'ensemble des fonctions affines que peut atteindre une fonction booléenne.

Les fonctions courbes sont ces fonctions dont le spectre de Walsh ne peut prendre que deux valeurs.

Deux notions pour deux points de vue différents. Une question peut alors être posée : « qu'en est-il de leur(s) éventuel(s) point(s) d'intersection ? ». La réponse est à la fois simple et riche de conséquences dans le contexte booléen. En effet ces deux notions sont en réalité complètement identiques. La preuve de cela, apportée par Dillon et Nyberg, est présentée dans cette section.

Le présent exposé est construit comme suit : nous décrivons successivement la notion de non linéarité parfaite, puis celle de fonction courbe. Enfin les liens - évidemment très forts - entre ces deux concepts sont étudiés.

5.2.2 Non linéarité parfaite

5.2.2.1 Définitions et premières caractérisations

L'attaque différentielle (cf. chapitre 2 paragraphe 2.3.3.1) est un outil extrêmement fertile du domaine de la cryptanalyse des algorithmes de chiffrement à clef secrète. Ses performances ont donc entraîné l'élaboration d'un certain nombre de concepts, dans l'objectif de fiabiliser les algorithmes, que nous reprenons ici.

La plupart des notations utilisées dans ce paragraphe proviennent de [CD04].

Supposons que les espaces vectoriels $\mathbb{F}_2^k$ pour tout $k \in \mathbb{N}^*$ soient des espaces probabilisés munis de la loi de probabilité uniforme $\Pr^{(k)}$.

Une mesure robuste de la non linéarité[1] introduite par Nyberg [Nyb92], consiste à calculer le maximum atteint, pour une fonction booléenne f donnée, du nombre d'éléments pour lesquels sa dérivée (suivant une certaine direction) est constante. Bien entendu si f possède des structures linéaires non nulles, alors ce maximum est égal au cardinal de l'ensemble de départ de f. Aussi plus cette mesure sera petite et plus la non linéarité de f sera grande.

Examinons cette mesure d'un point de vue formel.

Définition 5.1. Soit $f : \mathbb{F}_2^m \to \mathbb{F}_2^n$. Pour $(\alpha, \beta) \in \mathbb{F}_2^m \times \mathbb{F}_2^n$, on définit :

$$\Delta_f(\alpha, \beta) \stackrel{déf.}{=} \{x \in \mathbb{F}_2^m | d_\alpha f(x) = \beta\} .$$

La *probabilité de non linéarité* de f est le nombre

$$\mathsf{P}_f \stackrel{déf.}{=} \max_{\alpha \in \mathbb{F}_2^{m\,*}} \max_{\beta \in \mathbb{F}_2^n} \Pr^{(m)}(\Delta_f(\alpha, \beta)) .$$

Remarque 5.1. Soit $f : \mathbb{F}_2^m \to \mathbb{F}_2^n$.

1. Puisque $0_{\mathbb{F}_2^n}$ est une structure linéaire pour toute fonction, il est naturel de ne prendre le maximum que sur $\mathbb{F}_2^{m\,*}$ (sinon la probabilité de non linéarité serait identiquement égale à 1 pour toutes les fonctions) ;

2. Par définition de la probabilité induite,

$$\mathsf{P}_f = \max_{\alpha \in \mathbb{F}_2^{m\,*}} \max_{\beta \in \mathbb{F}_2^n} \Pr^{(m)}_{d_\alpha f}(\{\beta\}) ;$$

[1] *A priori* distincte de celle donnée dans la définition 4.10 p. 65.

3. Par définition de l'équiprobabilité,

$$\mathsf{P}_f = \frac{1}{2^m} \max_{\alpha \in \mathbb{F}_2^{m*}} \max_{\beta \in \mathbb{F}_2^n} |\Delta_f(\alpha, \beta)| \ ;$$

4. Si $\delta \in A(\mathbb{F}_2^m, \mathbb{F}_2^n)$, *i.e.* $\delta : \mathbb{F}_2^m \to \mathbb{F}_2^n$ est affine, alors $\mathsf{P}_\delta = 1$.

Pour $k \in \mathbb{N}$, Nyberg [Nyb94] a appelé *k-différentiellement uniformes* les fonctions f telles que $\mathsf{P}_f = \frac{k}{2^m}$.

Pour $f : \mathbb{F}_2^m \to \mathbb{F}_2^n$, observons que pour tout $\alpha \in \mathbb{F}_2^m$, l'ensemble des parties $\Delta_f(\alpha, \beta)$ de $\mathbb{F}_2^m$, lorsque β parcourt $\mathbb{F}_2^n$, constitue une partition de $\mathbb{F}_2^m$. On en déduit alors le lemme suivant.

Lemme 5.1. [CV94] *Soit $f : \mathbb{F}_2^m \to \mathbb{F}_2^n$. Pour chaque $\alpha \in \mathbb{F}_2^m$,*

$$\sum_{\beta \in \mathbb{F}_2^n} |\Delta_f(\alpha, \beta)| = 2^m \ .$$

Notons par ailleurs que, le maximum d'une variable aléatoire numérique définie sur un espace probabilisé muni de la loi de probabilité uniforme et prenant un nombre fini de valeurs étant plus grand ou égal à son espérance mathématique, on a pour tout $\alpha \in \mathbb{F}_2^m$ et $f \in \mathbb{F}_2^{n\,\mathbb{F}_2^m}$

$$\max_{\beta \in \mathbb{F}_2^n} \mathrm{Pr}^{(m)}(\Delta_f(\alpha, \beta)) = \frac{1}{2^m} \max_{\beta \in \mathbb{F}_2^n} |\Delta_f(\alpha, \beta)| \geq \frac{1}{2^n}$$

et donc

$$\mathsf{P}_f \geq \frac{1}{2^n} \ . \tag{5.1}$$

Cette borne inférieure peut alors être considérée comme une borne supérieure de la non linéarité de f. Le concept de non linéarité parfaite est alors introduit comme suit.

Définition 5.2. Une fonction $f : \mathbb{F}_2^m \to \mathbb{F}_2^n$ est *parfaitement non linéaire* si $\mathsf{P}_f = \frac{1}{2^n}$.

5.2.2.2 Caractérisations

Puisque le maximum d'une variable aléatoire numérique définie sur un espace probabilisé muni de la loi de probabilité uniforme et prenant un nombre fini de valeurs est égal à son espérance mathématique si et seulement si la variable aléatoire est constante, l'inégalité (5.1) est une égalité si et seulement si, pour chaque $\beta \in \mathbb{F}_2^n$ et chaque $\alpha \in \mathbb{F}_2^{m*}$, $|\Delta_f(\alpha, \beta)| = 2^{m-n}$.

D'après ce que l'on vient d'observer, on dispose de la proposition suivante.

Proposition 5.1. [CD04] *Une fonction $f : \mathbb{F}_2^m \to \mathbb{F}_2^n$ est parfaitement non linéaire si et seulement si pour tout $\alpha \in \mathbb{F}_2^{m*}$, la dérivée de f suivant α, $d_\alpha f$, est équilibrée i.e. $\forall \alpha \in \mathbb{F}_2^{m*}$, $\forall \beta \in \mathbb{F}_2^n$,*

$$|\Delta_f(\alpha, \beta)| = |\{x \in \mathbb{F}_2^m | f(x \oplus \alpha) \oplus f(x) = \beta\}| = 2^{m-n} \ .$$

En particulier, on déduit de la proposition ci-dessus que $f : \mathbb{F}_2^m \to \mathbb{F}_2$ est parfaitement non linéaire si et seulement si $\forall \alpha \in \mathbb{F}_2^{m*}$, $|\Delta_f(\alpha, 0)| = |\Delta_f(\alpha, 1)| = 2^{m-1}$.

Corollaire 5.1. [CD04] *Une fonction $f : \mathbb{F}_2^m \to \mathbb{F}_2^n$ est parfaitement non linéaire si et seulement si $\forall \alpha \in \mathbb{F}_2^{m*}$, $\forall \beta \in \mathbb{F}_2^{n*}$, $(\chi^1_{\mathbb{F}_2} \circ \widehat{l_\beta \circ d_\alpha f})(0_{\mathbb{F}_2^m}) = 0$.*

Preuve. D'après la proposition 5.1, f est parfaitement non linéaire si et seulement si pour tout $\alpha \in \mathbb{F}_2^{m*}$, $d_\alpha f$ est équilibrée ce qui est équivalent, d'après la proposition 4.6 (p. 59), à $\forall \alpha \in \mathbb{F}_2^{m*}$, $\forall \beta \in \mathbb{F}_2^{n*}$, $(\chi^1_{\mathbb{F}_2} \widehat{\circ\, l_\beta \circ d_\alpha f})(0_{\mathbb{F}_2^m}) = 0$. □

5.2.3 Fonctions courbes

5.2.3.1 Définitions

On sait (cf. chapitre 4 paragraphe 4.5.4.3) que pour $f : \mathbb{F}_2^m \to \mathbb{F}_2$, N_f est majorée par la valeur $2^{m-1} - 2^{\frac{m}{2}-1}$ du rayon de recouvrement et que pour que cette borne soit atteinte il faut et il suffit que $\forall \alpha \in \mathbb{F}_2^m$, $\widehat{\chi^1_{\mathbb{F}_2} \circ f}(\alpha) = \pm 2^{\frac{m}{2}}$. Nous obtenons alors la définition des fonctions courbes telle qu'originellement introduite par Dillon dans sa thèse [Dil74] ainsi que par Rothaus [Rot76].

Définition 5.3. Soit m un entier pair. Une fonction $f : \mathbb{F}_2^m \to \mathbb{F}_2$ est dite *courbe* si $\forall \alpha \in \mathbb{F}_2^m$,

$$\widehat{\chi^1_{\mathbb{F}_2} \circ f}(\alpha) = \pm 2^{\frac{m}{2}} \ .$$

Cette notion a été généralisée par Nyberg [Nyb92] au cas des fonctions booléennes vectorielles :

Définition 5.4. Une fonction $f : \mathbb{F}_2^m \to \mathbb{F}_2^n$ est *courbe* si pour tout $\beta \in \mathbb{F}_2^{n\,*}$, la fonction $l_\beta \circ f : \mathbb{F}_2^m \to \mathbb{F}_2$, et définie, on le rappelle, par $x \mapsto \beta.f(x)$, est courbe au sens de la définition précédente. Autrement dit $\forall \beta \in \mathbb{F}_2^{n\,*}$, $\forall \alpha \in \mathbb{F}_2^m$,

$$\widehat{(\chi^1_{\mathbb{F}_2} \circ l_\beta \circ f)}(\alpha) = \pm 2^{\frac{m}{2}} \ .$$

Les fonctions courbes formalisent en pratique la solidité contre l'attaque linéaire.

Définition 5.5. La *résistance envers la cryptanalyse linéaire* d'une fonction $f : \mathbb{F}_2^m \to \mathbb{F}_2^n$ est mesurée par la quantité

$$\mathsf{R}_f \stackrel{déf.}{=} \max_{\alpha \in \mathbb{F}_2^m} \max_{\beta \in \mathbb{F}_2^{n\,*}} |k_f(\alpha, \beta)|$$

où pour $(\alpha, \beta) \in \mathbb{F}_2^m \times \mathbb{F}_2^{n\,*}$, $k_f(\alpha, \beta) \stackrel{déf.}{=} |\{x \in \mathbb{F}_2^m | \alpha.x \oplus \beta.f(x) = 0\}| - 2^{m-1}$.

Plus cette valeur est petite et plus la résistance à la cryptanalyse linéaire est élevée.

Remarque 5.2. Soit $f : \mathbb{F}_2^m \to \mathbb{F}_2^n$. Pour tout $(\alpha, \beta) \in \mathbb{F}_2^m \times \mathbb{F}_2^n$, on a

$$k_f(\alpha, \beta) = d_H(l_\beta \circ f, \overline{l_\alpha}) - 2^{m-1} = \frac{1}{2}\widehat{(\chi^1_{\mathbb{F}_2} \circ l_\beta \circ f)}(\alpha) \ .$$

La deuxième égalité provenant de la formule (4.8) p. 58 appliquée à la fonction $l_\beta \circ f$.

Cette résistance est intimement liée à la notion de fonction courbe.

Proposition 5.2. [CV94] *On a pour tout* $f \in \mathbb{F}_2^{n\,\mathbb{F}_2^m}$,

$$\mathsf{R}_f \geq 2^{\frac{m}{2}-1} \ .$$

Soit $f : \mathbb{F}_2^m \to \mathbb{F}_2^n$. *Alors on a*

$$f \text{ est courbe} \Leftrightarrow \mathsf{R}_f = 2^{\frac{m}{2}-1} \ . \tag{5.2}$$

Preuve.

Démontrons le premier point. Soit $f : \mathbb{F}_2^m \to \mathbb{F}_2^n$. D'une part on déduit de la remarque 5.2 que $\mathsf{R}_f = \frac{1}{2} \max_{\alpha \in \mathbb{F}_2^m} \max_{\beta \in \mathbb{F}_2^{n\,*}} |\widehat{(\chi^1_{\mathbb{F}_2} \circ l_\beta \circ f)}(\alpha)| = \frac{1}{2} \max_{\beta \in \mathbb{F}_2^{n\,*}} \| \widehat{(\chi^1_{\mathbb{F}_2} \circ l_\beta \circ f)} \|_\infty$. D'autre part la discussion effectuée au paragraphe 4.5.4.3 p. 65 du chapitre 4, nous permet d'affirmer que $\forall \beta \in \mathbb{F}_2^{n\,*}$, $\| \widehat{(\chi^1_{\mathbb{F}_2} \circ l_\beta \circ f)} \|_\infty \geq 2^{\frac{m}{2}}$. Cela nous conduit donc à inférer que $\mathsf{R}_f \geq 2^{\frac{m}{2}-1}$.

Prouvons maintenant le second point. D'après ce que l'on vient d'observer :

$$\begin{aligned} \mathsf{R}_f = 2^{\frac{m}{2}-1} &\Leftrightarrow \forall \beta \in \mathbb{F}_2^{n\,*},\ \| \widehat{(\chi^1_{\mathbb{F}_2} \circ l_\beta \circ f)} \|_\infty = 2^{\frac{m}{2}} \\ &\Leftrightarrow \forall \beta \in \mathbb{F}_2^{n\,*},\ \forall \alpha \in \mathbb{F}_2^m,\ \widehat{(\chi^1_{\mathbb{F}_2} \circ l_\beta \circ f)}(\alpha) = \pm 2^{\frac{m}{2}} \\ &\Leftrightarrow f \text{ est courbe.} \end{aligned}$$

La seconde équivalence étant une application d'un résultat du paragraphe 4.5.4.3 p. 65. □

Les fonctions qui résistent le mieux à l'attaque linéaire sont celles pour lesquelles R_f est le plus petit possible, on en déduit alors que ce sont les fonctions courbes.

5.2.3.2 Conditions d'existence

Soit $f : \mathbb{F}_2^m \to \mathbb{F}_2$. Pour que la fonction f soit courbe il est nécessaire que m soit pair. En effet, la remarque 5.2 nous indique que pour tout $\alpha \in \mathbb{F}_2^m$, $2k_f(\alpha, 1) = \widehat{\chi^1_{\mathbb{F}_2} \circ f}(\alpha)$ (puisque $l_1 \circ f = f$). La fonction f étant courbe, il en résulte que pour tout $\alpha \in \mathbb{F}_2^m$, $2k_f(\alpha, 1) = \pm 2^{\frac{m}{2}}$. *A priori* $\frac{m}{2} \in \mathbb{Q}$, mais comme $\forall \alpha \in \mathbb{F}_2^m$, $k_f(\alpha, 1) \in \mathbb{Z}$, il est donc nécessaire que m soit pair. Nous avions anticipé ce fait dans la définition 5.3.

De même que dans le cas des fonctions courbes à valeurs dans $\mathbb{F}_2$, l'existence de fonctions vectorielles courbes nécessite que m soit pair. Plus précisément nous disposons du résultat suivant dû à Nyberg [Nyb92].

Proposition 5.3. [Nyb92] *Les fonctions courbes de $\mathbb{F}_2^{n\,\mathbb{F}_2^m}$ n'existent que si m est pair et $m \geq 2n$.*

Preuve. Si f est courbe alors par la définition 5.4, $\forall \beta \in \mathbb{F}_2^{n*}$, $l_\beta \circ f$ est une fonction booléenne binaire courbe. Donc, d'après la discussion précédente, m doit être pair.
Soient $k \stackrel{déf.}{=} \frac{1}{2^{\frac{m}{2}}} \sum_{\beta \in \mathbb{F}_2^{n\,*}} (\widehat{\chi^1_{\mathbb{F}_2} \circ l_\beta \circ f})(0_{\mathbb{F}_2^m})$ et $k_{0_{\mathbb{F}_2^m}} \stackrel{déf.}{=} |\{\beta \in \mathbb{F}_2^{n*} | (\widehat{\chi^1_{\mathbb{F}_2} \circ l_\beta} \circ f)(0_{\mathbb{F}_2^m}) = +2^{\frac{m}{2}}\}|$.
Alors $k = k_{0_{\mathbb{F}_2^m}} - (2^n - 1 - k_{0_{\mathbb{F}_2^m}}) = 2k_{0_{\mathbb{F}_2^m}} - 2^n + 1$. Ainsi k est un entier impair. De plus on a :

$$\begin{aligned}
\sum_{\beta \in \mathbb{F}_2^{m\,*}} (\widehat{\chi^1_{\mathbb{F}_2} \circ l_\beta} \circ f)(0_{\mathbb{F}_2^m}) &= \sum_{\beta \in \mathbb{F}_2^n} (\widehat{\chi^1_{\mathbb{F}_2} \circ l_\beta} \circ f)(0_{\mathbb{F}_2^m}) - (\widehat{\chi^1_{\mathbb{F}_2} \circ l_{0_{\mathbb{F}_2^n}}} \circ f)(0_{\mathbb{F}_2^m}) \\
&= \sum_{\beta \in \mathbb{F}_2^n} \sum_{x \in \mathbb{F}_2^m} (-1)^{\beta \cdot f(x)} - 2^m \\
&= \sum_{x \in \mathbb{F}_2^m} \sum_{\beta \in \mathbb{F}_2^n} (-1)^{\beta \cdot f(x)} - 2^m \\
&= 2^n |\{x \in \mathbb{F}_2^m | f(x) = 0_{\mathbb{F}_2^m}\}| - 2^m \ .
\end{aligned}$$

Alors $k = \frac{1}{2^{\frac{m}{2}}}(2^n |\{x \in \mathbb{F}_2^m | f(x) = 0_{\mathbb{F}_2^m}\}| - 2^m)$ et donc $|\{x \in \mathbb{F}_2^m | f(x) = 0_{\mathbb{F}_2^m}\}| = 2^{\frac{m}{2}-n}(k + 2^{\frac{m}{2}})$.
Comme par ailleurs $|\{x \in \mathbb{F}_2^m | f(x) = 0_{\mathbb{F}_2^m}\}| \in \mathbb{N}$ et k est un entier pair, $2^{\frac{m}{2}-n}$ doit être un entier.
Alors $m \geq 2n$. □

Le lecteur intéressé par les divers développements sur la question des fonctions booléennes courbes pourra consulter les nombreuses références sur le sujet [Dob95, HL97, CG98, Car99a, Car99b, Wol99, CCC+00].

5.2.4 L'équivalence entre les deux notions

Nous disposons, d'un côté, d'un concept combinatoire - la non linéarité parfaite - et, d'un autre côté, d'une notion basée sur la transformée de Fourier. Bien que ne s'exprimant pas dans le même langage, ces deux idées représentent en fait le même objet abstrait, décrit différemment.

Cette équivalence, par dualité via la transformée de Fourier, est essentiellement vraie dans le cadre booléen. En dehors de celui-ci, ainsi que nous l'observons dans la suite au chapitre 6, la notion de non linéarité parfaite est souvent plus forte que celle de fonction courbe.

Dans cette sous-section, nous exposons deux théorèmes mettant en valeur le lien entre les deux concepts précédemment introduits.

Théorème 5.1. [Dil74] *La fonction $f : \mathbb{F}_2^m \to \mathbb{F}_2$ est parfaitement non linéaire si et seulement si elle est courbe.*

Preuve.

$$\begin{aligned} f \text{ est parfaitement non linéaire} &\Leftrightarrow \forall \alpha \in \mathbb{F}_2^{m*},\ d_\alpha f \text{ est équilibrée} \\ &\quad \text{(d'après la proposition 5.1)} \\ &\Leftrightarrow \forall \alpha \in \mathbb{F}_2^{m*},\ \widehat{(\chi^1_{\mathbb{F}_2} \circ d_\alpha f)}(0_{\mathbb{F}_2^m}) = 0 \\ &\quad \text{(d'après le point 2. de la remarque 4.4 p. 59).} \end{aligned}$$

Soit alors l'application

$$\begin{aligned} AC_f : \ \mathbb{F}_2^m &\to \mathbb{R} \\ \alpha &\mapsto \widehat{(\chi^1_{\mathbb{F}_2} \circ d_\alpha f)}(0_{\mathbb{F}_2^m}) \ . \end{aligned}$$

D'après les équivalences précédentes,

$$f \text{ est parfaitement non linéaire si et seulement si } \forall \alpha \in \mathbb{F}_2^{m*},\ AC_f(\alpha) = 0 \ . \tag{5.3}$$

Calculons la transformée de Fourier de AC_f pour $\alpha \in \mathbb{F}_2^m$.

$$\begin{aligned} \widehat{AC_f}(\alpha) &= \sum_{x \in \mathbb{F}_2^m} AC_f(x)(-1)^{x.\alpha} \\ &= \sum_{x \in \mathbb{F}_2^m} \sum_{y \in \mathbb{F}_2^m} (-1)^{f(x \oplus y)} (-1)^{f(y)} (-1)^{x.\alpha} \\ &= \sum_{x \in \mathbb{F}_2^m} (\chi^1_{\mathbb{F}_2} \circ f * \chi^1_{\mathbb{F}_2} \circ f)(x)(-1)^{x.\alpha} \\ &\quad \text{(par la définition 4.6 p. 56 du produit de convolution)} \\ &= \widehat{\left(\chi^1_{\mathbb{F}_2} \circ f * \chi^1_{\mathbb{F}_2} \circ f\right)}(\alpha) \\ &= (\widehat{(\chi^1_{\mathbb{F}_2} \circ f)}(\alpha))^2 \\ &\quad \text{(d'après la proposition 4.4 p. 56 sur la trivialisation du produit de convolution).} \end{aligned}$$

On a ainsi la formule ci-dessous, pour tout $\alpha \in \mathbb{F}_2^m$:

$$\widehat{AC_f}(\alpha) = (\widehat{(\chi^1_{\mathbb{F}_2} \circ f)}(\alpha))^2 \ . \tag{5.4}$$

Or on dispose de l'équivalence suivante, pour toute fonction $\varphi : \mathbb{F}_2^m \to \mathbb{R}$:

$$\forall x \in \mathbb{F}_2^{m*},\ \varphi(x) = 0 \Leftrightarrow \forall \alpha \in \mathbb{F}_2^m,\ \widehat{\varphi}(\alpha) = \varphi(0_{\mathbb{F}_2^m}) \ . \tag{5.5}$$

En effet

- L'implication directe se démontre comme suit.
  $\widehat{\varphi}(\alpha) = \sum_{x \in \mathbb{F}_2^m} \varphi(x)(-1)^{x.\alpha} = \varphi(0_{\mathbb{F}_2^m})$;
- L'implication réciproque se prouve quant à elle en utilisant la formule d'inversion de la transformée de Fourier (voir corollaire 4.1) :
  $\varphi(x) = \frac{1}{2^m} \sum_{\alpha \in \mathbb{F}_2^m} \widehat{\varphi}(x)(-1)^{x.\alpha} = \frac{1}{2^m} \varphi(0_{\mathbb{F}_2^m}) \sum_{\alpha \in \mathbb{F}_2^m} (-1)^{x.\alpha} = 0$ si $x \neq 0_{\mathbb{F}_2^m}$ (voir le lemme 4.1 p. 54).

Finalement on a

$$\begin{aligned}
f \text{ parfaitement non linéaire} &\Leftrightarrow \forall \alpha \in \mathbb{F}_2^{m\,*},\ AC_f(\alpha) = 0 \\
&\quad \text{(d'après l'équivalence (5.3))} \\
&\Leftrightarrow \forall \alpha \in \mathbb{F}_2^m,\ \widehat{AC_f}(\alpha) = AC_f(0_{\mathbb{F}_2^m}) = \sum_{x \in \mathbb{F}_2^m} \chi^1_{\mathbb{F}_2}(0) = 2^m \\
&\quad \text{(d'après l'équivalence (5.5) et la définition de } AC_f) \\
&\Leftrightarrow \forall \alpha \in \mathbb{F}_2^m,\ (\widehat{(\chi^1_{\mathbb{F}_2} \circ f)}(\alpha))^2 = 2^m \\
&\quad \text{(par l'égalité (5.4))} \\
&\Leftrightarrow \forall \alpha \in \mathbb{F}_2^m,\ \widehat{\chi^1_{\mathbb{F}_2} \circ f}(\alpha) = \pm 2^{\frac{m}{2}} \\
&\Leftrightarrow f \text{ est courbe par définition.}
\end{aligned}$$

□

Remarque 5.3. La fonction AC_f introduite dans la preuve est parfois appelée *fonction d'autocorrélation* de f.

Nous disposons d'un théorème analogue dans le cas des fonctions booléennes vectorielles.

Théorème 5.2. [Nyb92] *Soit $f : \mathbb{F}_2^m \to \mathbb{F}_2^n$. La fonction f est parfaitement non linéaire si et seulement si elle est courbe.*

Preuve. Remarquons d'une part que pour tout $(\alpha, \beta) \in \mathbb{F}_2^m \times \mathbb{F}_2^n$, on a $l_\beta \circ d_\alpha f = d_\alpha(l_\beta \circ f)$ (d'après le point 5. de la remarque 4.6 p. 68).
D'autre part on a la séquence d'équivalences suivante :

$$\begin{aligned}
f \text{ parfaitement non linéaire} &\Leftrightarrow \forall \alpha \in \mathbb{F}_2^{m\,*},\ d_\alpha f \text{ est équilibrée} \\
&\quad \text{(par la proposition 5.1 p. 76)} \\
&\Leftrightarrow \forall \beta \in \mathbb{F}_2^{n\,*},\ \forall \alpha \in \mathbb{F}_2^{m\,*},\ l_\beta \circ d_\alpha f \text{ est équilibrée} \\
&\quad \text{(par la proposition 4.7 p. 60)} \\
&\Leftrightarrow \forall \beta \in \mathbb{F}_2^{n\,*},\ \forall \alpha \in \mathbb{F}_2^{m\,*},\ d_\alpha(l_\beta \circ f) \text{ est équilibrée} \\
&\quad \text{(d'après la remarque initiale de cette démonstration)} \\
&\Leftrightarrow \forall \beta \in \mathbb{F}_2^{n\,*},\ l_\beta \circ f \text{ est courbe} \\
&\quad \text{(d'après le théorème 5.1)} \\
&\Leftrightarrow f \text{ est courbe (par définition).}
\end{aligned}$$

□

5.2.5 Conclusion

Ainsi donc, maintenant nous en sommes convaincus, les fonctions parfaitement non linéaires et les fonctions courbes sont les mêmes objets. Comme un *isomorphisme de Curry-Howard* entre preuves formelles et algorithmes, cette assertion ne paraît pas évidente au premier regard.

A cela deux raisons.
Le vocabulaire, au sens large du terme, en est la première. Comment voir que sous une caractérisation combinatoire se cache en réalité une propriété relevant de l'analyse de Fourier ? Comment percevoir la dualité sous-jacente à ces deux notions ?
La seconde raison réside dans la puissance de l'instrument qui permet de passer d'un concept à l'autre : la transformée de Fourier. Cet outil, simple dans sa conception, n'en demeure pas moins un formidable moyen d'analyse des propriétés des fonctions booléennes. On s'en convaincra encore davantage dans la suite du manuscrit.

Les propriétés, justement, constituent le sujet de la prochaine section. On y retrouvera donc aussi la fameuse transformée de Fourier.

5.3 Quelques propriétés

5.3.1 Introduction

Puisque les fonctions parfaitement non linéaires et courbes font exception parmi les fonctions booléennes, il est nécessaire de pouvoir les caractériser. Ainsi sont maintenant exposées les propriétés classiques qu'elles satisfont.

La dualité entre ces deux notions nous permet, chance inouïe, de choisir à tout moment la description idéale afin d'évoquer une propriété donnée. Nous abordons ainsi, dans cette section, la notion de fonction duale, le degré et la distance à $R(1,m)$ via le concept des fonctions courbes. Alors que le produit tensoriel et la caractérisation à l'aide des ensembles à différences sont décrits au travers de la notion de non linéarité parfaite.

5.3.2 Fonction courbe duale

Proposition 5.4. [Dil74] *Soit $f : \mathbb{F}_2^m \to \mathbb{F}_2$ une fonction courbe. Alors il existe $\tilde{f} : \mathbb{F}_2^m \to \mathbb{F}_2$ telle que pour tout $\alpha \in \mathbb{F}_2^m$, on ait*

$$\widehat{\chi^1_{\mathbb{F}_2} \circ f}(\alpha) = 2^{\frac{m}{2}}(-1)^{\tilde{f}(\alpha)}.$$

La fonction $\tilde{f}$, appelée duale *de f, est également courbe.*

Preuve. Remarquons tout d'abord que l'application $\chi^1_{\mathbb{F}_2}$ est bijective sur $\{\pm 1\}$. Son inverse est

$$\begin{array}{rccc} \Theta : & \{\pm 1\} & \to & \mathbb{F}_2 \\ & x & \mapsto & \dfrac{1}{2}(1-x) \end{array}$$

où l'on a plongé $\mathbb{F}_2$ dans $\mathbb{R}$ de manière naturelle.
Soit maintenant l'application suivante

$$\begin{array}{rccc} \varphi : & \mathbb{F}_2^m & \to & \mathbb{R} \\ & \alpha & \mapsto & \dfrac{1}{2^{\frac{m}{2}}}\widehat{\chi^1_{\mathbb{F}_2} \circ f}(\alpha)\ . \end{array}$$

Puisque, par hypothèse, la fonction f est courbe, on en déduit que la fonction φ est à valeurs dans $\{\pm 1\}$.

On définit ensuite $\tilde{f} : \mathbb{F}_2^m \to \mathbb{F}_2$ par $\tilde{f} \stackrel{déf.}{=} \Theta \circ \varphi$ *i.e.* d'après la remarque du début de la preuve :

$$\varphi = \chi^1_{\mathbb{F}_2} \circ \tilde{f}\ . \tag{5.6}$$

Alors on a pour $\alpha \in \mathbb{F}_2^m$:

$$\widehat{\chi^1_{\mathbb{F}_2} \circ f}(\alpha) = 2^{\frac{m}{2}}\varphi(\alpha) = 2^{\frac{m}{2}}\chi^1_{\mathbb{F}_2} \circ \tilde{f}(\alpha)\ .$$

On vient donc de démontrer la première partie de la proposition. Il ne reste qu'à prouver que $\tilde{f}$ est également courbe. Pour ce faire on calcule sa transformée de Walsh pour $\alpha \in \mathbb{F}_2^m$:

$$\begin{array}{rcl} \widehat{\chi^1_{\mathbb{F}_2} \circ \tilde{f}}(\alpha) & = & \widehat{\varphi}(\alpha) \text{ (d'après l'égalité (5.6))} \\ & = & \dfrac{1}{2^{\frac{m}{2}}}\widehat{\widehat{\chi^1_{\mathbb{F}_2} \circ f}}(\alpha) \\ & = & \dfrac{2^m}{2^{\frac{m}{2}}}\chi^1_{\mathbb{F}_2} \circ f(\alpha) \text{ (d'après la formule d'inversion 4.1 p. 55)} \\ & = & \pm 2^{\frac{m}{2}} \text{ (puisque } \chi^1_{\mathbb{F}_2} \text{ est à valeurs dans } \{\pm 1\}). \end{array}$$

□

Remarque 5.4. Notons « $\mathcal{B}_m$ » l'ensemble des fonctions de $\mathbb{F}_2^{\mathbb{F}_2^m}$ qui sont courbes. L'application $f \mapsto \tilde{f}$, qui associe à une fonction courbe sa duale, est une involution de $\mathcal{B}_m$.

5.3.3 Degré d'une fonction courbe

Proposition 5.5. [Rot76] *Soit m pair. Si $f : \mathbb{F}_2^m \to \mathbb{F}_2$ est courbe, on a :*
- *si $m \geq 4$ alors* $\deg(f) \leq \frac{m}{2}$.
- *si $m = 2$ alors* $\deg(f) = 1$.

Preuve. Rappelons d'une part la définition de la transformée de Möbius de f évaluée en $x \in \mathbb{F}_2^m$ (voir la formule (4.6) p. 50) :

$$\mathring{f}(x) = \bigoplus_{y \leq x} f(y) \ .$$

D'autre part, via la formule d'inversion 4.1 p. 55, la fonction f et sa transformée de Fourier sont reliées comme suit : soit $x \in \mathbb{F}_2^m$

$$f(x) = \frac{1}{2^m} \sum_{\alpha \in \mathbb{F}_2^m} \widehat{f}(\alpha)(-1)^{x.\alpha} \ .$$

En utilisant les deux égalités on obtient alors, pour $x \in \mathbb{F}_2^m$, la relation suivante entre les transformées de Möbius et de Fourier :

$$\begin{aligned}
\mathring{f}(x) &= \frac{1}{2^m} \bigoplus_{y \leq x} \sum_{\alpha \in \mathbb{F}_2^m} \widehat{f}(\alpha)(-1)^{y.\alpha} \\
&= \frac{1}{2^m} \sum_{y \leq x} \sum_{\alpha \in \mathbb{F}_2^m} \widehat{f}(\alpha)(-1)^{y.\alpha} \bmod 2 \\
&= \frac{1}{2^m} \sum_{\alpha \in \mathbb{F}_2^m} \widehat{f}(\alpha) \sum_{y \leq x} (-1)^{y.\alpha} \bmod 2 \ .
\end{aligned}$$

On pose $V_x \stackrel{déf.}{=} \{y \in \mathbb{F}_2^m | y \leq x\}$. Il s'agit d'un sous-espace vectoriel de $\mathbb{F}_2^m$ de dimension $w_H(x)$ et son orthogonal vérifie $V_x^\perp = V_{\overline{x}}$. On a ainsi

$$\mathring{f}(x) = \frac{2^{w_H(x)}}{2^m} \sum_{\alpha \in V_{\bar{x}}} \widehat{f}(\alpha) \bmod 2 \ .$$

D'après l'égalité (4.11) p. 58 on a :

$$\begin{aligned}
\mathring{f}(x) &= \frac{2^{w_H(x)}}{2^m} \left(2^{m-1} - \frac{1}{2} \sum_{\alpha \in V_{\bar{x}}} \widehat{\chi^1_{\mathbb{F}_2} \circ f}(\alpha) \right) \bmod 2 \\
&= 2^{w_H(x)-1} - \frac{2^{w_H(x)}}{2^{m+1}} \sum_{\alpha \in V_{\bar{x}}} \widehat{\chi^1_{\mathbb{F}_2} \circ f}(\alpha) \bmod 2 \ .
\end{aligned}$$

Puisque par hypothèse f est courbe, d'après la proposition 5.4, il existe une fonction $\tilde{f} : \mathbb{F}_2^m \to \mathbb{F}_2$, également courbe, telle que $\widehat{\chi^1_{\mathbb{F}_2} \circ f} = 2^{\frac{m}{2}} \chi^1_{\mathbb{F}_2} \circ \tilde{f}$. Ainsi $\mathring{f}(x)$ vérifie

$$\begin{aligned}
\mathring{f}(x) &= 2^{w_H(x)-1} - \frac{2^{w_H(x)}}{2^{\frac{m}{2}+1}} \sum_{\alpha \in V_{\bar{x}}} \chi^1_{\mathbb{F}_2^m} \circ \tilde{f}(\alpha) \bmod 2 \\
&= 2^{w_H(x)-1} - \frac{2^{w_H(x)}}{2^{\frac{m}{2}+1}} \sum_{\alpha \in V_{\bar{x}}} (1 - 2\tilde{f}(\alpha)) \bmod 2 \text{ (d'après (4.10) p. 58)} \\
&= 2^{w_H(x)-1} - \frac{2^{w_H(x)}}{2^{\frac{m}{2}+1}} \left(2^{w_H(\bar{x})} - 2 \sum_{\alpha \in V_{\bar{x}}} \tilde{f}(\alpha) \right) \bmod 2 \\
&= 2^{w_H(x)-1} - 2^{\frac{m}{2}-1} + \frac{2^{w_H(x)}}{2^{\frac{m}{2}}} \sum_{\alpha \in V_{\bar{x}}} \tilde{f}(\alpha) \bmod 2 \text{ (puisque } w_H(x) + w_H(\bar{x}) = m).
\end{aligned}$$

Il en résulte donc que si $m \geq 4$ et $w_H(x) > \dfrac{m}{2}$, alors $\mathring{f}(x) \equiv 0 \pmod 2$ et donc que le degré de f est au plus $\frac{m}{2}$. □

5.3.4 Produit tensoriel de fonctions

Définition 5.6. Soit (X, Y, G) un triplet pour lequel X et Y sont deux ensembles (non vides) et G est un groupe de loi de composition interne $\top$. Soit $(f, g) \in G^X \times G^Y$. On définit le *produit tensoriel* de f et g par :

$$\begin{array}{rccc} (f \otimes g): & X \times Y & \to & G \\ & (x, y) & \mapsto & f(x) \top g(y)\ . \end{array}$$

Proposition 5.6. *Soient $f : \mathbb{F}_2^m \to \mathbb{F}_2^n$ et $g : \mathbb{F}_2^k \to \mathbb{F}_2^n$ des fonctions parfaitement non linéaires. Alors la fonction $f \otimes g$ est parfaitement non linéaire (on identifie alors $\mathbb{F}_2^{m+k}$ avec $\mathbb{F}_2^m \times \mathbb{F}_2^k$).*

Preuve. Supposons dans un premier temps que $n = 1$.
Soit $(\alpha, \beta) \in (\mathbb{F}_2^m \times \mathbb{F}_2^k) \setminus \{(0_{\mathbb{F}_2^m}, 0_{\mathbb{F}_2^k})\}$ (ainsi α et β ne peuvent être simultanément nuls). Soit $(x, y) \in \mathbb{F}_2^m \times \mathbb{F}_2^k$, alors $d_{(\alpha,\beta)}(f \otimes g)(x, y) = d_\alpha f(x) \oplus d_\beta g(y)$. On a donc :

$$\begin{array}{rcl} |\{(x,y) \in \mathbb{F}_2^m \times \mathbb{F}_2^k | d_{(\alpha,\beta)}(f \otimes g)(x,y) = 0\}| & = & |\{(x,y) \in \mathbb{F}_2^m \times \mathbb{F}_2^k | d_\alpha f(x) \oplus d_\beta g(y) = 0\}| \\ & = & |\{(x,y) \in \mathbb{F}_2^m \times \mathbb{F}_2^k | d_\alpha f(x) = 0 \text{ et } d_\beta g(y) = 0\}| \\ & + & |\{(x,y) \in \mathbb{F}_2^m \times \mathbb{F}_2^k | d_\alpha f(x) = 1 \text{ et } d_\beta g(y) = 1\}|\ . \end{array}$$

Finalement on a

$$|\{(x,y) \in \mathbb{F}_2^m \times \mathbb{F}_2^k | d_{(\alpha,\beta)}(f \otimes g)(x,y) = 0\}| = \sum_{\gamma \in \mathbb{F}_2} |\{x \in \mathbb{F}_2^m | d_\alpha f(x) = \gamma\}||\{y \in \mathbb{F}_2^k | d_\beta g(y) = \gamma\}|\ .$$

On a trois cas possibles :

1. Si $\alpha = 0_{\mathbb{F}_2^m}$ alors par hypothèse, $\beta \neq 0_{\mathbb{F}_2^k}$. De plus $|\{x \in \mathbb{F}_2^m | d_\alpha f(x) = 1\}| = 0$ et $|\{x \in \mathbb{F}_2^m | d_\alpha f(x) = 0\}| = 2^m$. Par ailleurs puisque g est parfaitement non linéaire et que $\beta \neq 0_{\mathbb{F}_2^m}$, on en déduit par la proposition 5.1 que $\forall \gamma \in \mathbb{F}_2$, $|\{y \in \mathbb{F}_2^k | d_\beta g(y) = \gamma\}| = 2^{k-1}$. Finalement on a $\displaystyle\sum_{\gamma \in \mathbb{F}_2} |\{x \in \mathbb{F}_2^m | d_\alpha f(x) = \gamma\}||\{y \in \mathbb{F}_2^k | d_\beta g(y) = \gamma\}| = 2^m 2^{k-1} = 2^{m+k-1}$;
2. Si $\beta = 0_{\mathbb{F}_2^k}$ alors $\alpha \neq 0_{\mathbb{F}_2^m}$ et on raisonne comme au point 1. pour montrer que $\displaystyle\sum_{\gamma \in \mathbb{F}_2} |\{x \in \mathbb{F}_2^m | d_\alpha f(x) = \gamma\}||\{y \in \mathbb{F}_2^k | d_\beta g(y) = \gamma\}| = 2^{m-1} 2^k = 2^{m+k-1}$.
3. Si $\alpha \neq 0_{\mathbb{F}_2^m}$ et $\beta \neq 0_{\mathbb{F}_2^k}$. Alors pour tout $\gamma \in \mathbb{F}_2$, par non linéarité parfaite de f on a $|\{x \in \mathbb{F}_2^m | d_\alpha f(x) = \gamma\}| = 2^{m-1}$ et par celle de g on obtient $|\{y \in \mathbb{F}_2^k | d_\beta g(y) = \gamma\}| = 2^{k-1}$. Finalement on a $\displaystyle\sum_{\gamma \in \mathbb{F}_2} |\{x \in \mathbb{F}_2^m | d_\alpha f(x) = \gamma\}||\{y \in \mathbb{F}_2^k | d_\beta g(y) = \gamma\}| = 2\ 2^{m+k-2} = 2^{m+k-1}$.

Dans tous les cas on a $|\{(x,y) \in \mathbb{F}_2^m \times \mathbb{F}_2^k | d_{(\alpha,\beta)}(f \otimes g)(x,y) = 0\}| = 2^{m+k-1}$ ce qui nous permet de conclure que $f \otimes g$ est parfaitement non linéaire.

Supposons maintenant que $n > 1$.
Pour démontrer la proposition dans ce cas, il suffit de remarquer que pour tout $\gamma \in \mathbb{F}_2^n$ et pour tout $(x, y) \in \mathbb{F}_2^m \times \mathbb{F}_2^k$ on a $l_\gamma \circ (f \otimes g)(x, y) = \gamma.(f(x) \oplus g(y)) = l_\gamma \circ f(x) \oplus l_\gamma \circ g(y) = (l_\gamma \circ f \otimes l_\gamma \circ g)(x, y)$. Enfin on sait que pour que f soit parfaitement non linéaire il faut et il suffit que f soit courbe (d'après le théorème 5.2) et par définition f est courbe si et seulement si pour tout $\gamma \in \mathbb{F}_2^{n\,*}$, $l_\gamma \circ f$ est courbe (de même on a g parfaitement non linéaire si et seulement si pour tout $\gamma \in \mathbb{F}_2^{n\,*}$, $l_\gamma \circ g$ est courbe). Il suit de la remarque concernant $l_\gamma \circ (f \otimes g)$ et de la preuve de la présente proposition dans le cas où $n = 1$ que l'on a $\forall \gamma \in \mathbb{F}_2^{n\,*}$, $l_\gamma \circ (f \otimes g)$ est courbe. En remontant la chaîne d'équivalences on obtient le fait que $f \otimes g$ est parfaitement non linéaire. □

5.3.5 Distance aux fonctions affines

Il est possible de caractériser les fonctions courbes à l'aide de leur distance au code de Reed-Muller d'ordre 1.

Proposition 5.7. [Pom03] *Soit $f : \mathbb{F}_2^m \to \mathbb{F}_2$. Si la fonction f est courbe alors $\forall \delta \in R(1,m)$, $d_H(f,\delta) = 2^{m-1} \pm 2^{\frac{m}{2}-1}$.*
Soit $f : \mathbb{F}_2^m \to \mathbb{F}_2^n$. Si la fonction f est courbe alors $\forall \beta \in \mathbb{F}_2^{n\,*}$ et $\forall \delta \in R(1,m)$, $d_H(l_\beta \circ f, \delta) = 2^{m-1} \pm 2^{\frac{m}{2}-1}$.

Preuve. Prouvons le premier point. Soit $\delta \in R(1,m)$ alors il existe $\alpha \in \mathbb{F}_2^m$ tel que $\delta = l_\alpha$ ou $\overline{l_\alpha}$. On en déduit d'après les relations (4.13) p. 65 que l'on a :

$$\begin{aligned} d_H(f,\delta) &= 2^{m-1} \pm \frac{1}{2}\widehat{\chi^1_{\mathbb{F}_2} \circ f}(\alpha) \\ &= 2^{m-1} \pm 2^{\frac{m}{2}-1} \text{ (puisque } f \text{ est courbe).} \end{aligned}$$

En ce qui concerne la seconde partie de la proposition il suffit d'appliquer la preuve précédente aux fonctions $l_\beta \circ f$ pour $\beta \in \mathbb{F}_2^{n\,*}$ puisque par définition des fonctions courbes vectorielles, ces fonctions sont courbes dès que f l'est. □

On en déduit (en utilisant la proposition 4.3 p. 65 ainsi que la proposition précédente) par ailleurs qu'une fonction f courbe définie sur $\mathbb{F}_2^m$ et à valeurs dans $\mathbb{F}_2$ vérifie $\mathsf{N}_f = 2^{m-1} - 2^{\frac{m}{2}-1}$. Or d'après la borne (4.14) p. 65 cette valeur est maximale. Enfin puisque $\mathsf{N}_f \stackrel{déf.}{=} \min_{\delta \in R(1,m)} d_H(f,\delta)$ les fonctions courbes à valeurs dans $\mathbb{F}_2$ sont les fonctions les plus éloignées de l'ensemble des fonctions affines $R(1,m)$, c'est-à-dire qu'elles atteignent le rayon de recouvrement du code de Reed-Muller d'ordre 1.

Comme conséquence voici le résultat suivant montrant qu'une fonction booléenne ne peut posséder toutes les bonnes propriétés cryptographiques.

Corollaire 5.2. [Pom03] *Si $f : \mathbb{F}_2^m \to \mathbb{F}_2$ est courbe alors f a exactement $2^{m-1} \pm 2^{\frac{m}{2}-1}$ zéros. En particulier f n'est pas équilibrée. De manière identique si $f : \mathbb{F}_2^m \to \mathbb{F}_2^n$ est courbe alors elle n'est pas équilibrée.*

Preuve. Pour $f : \mathbb{F}_2^m \to \mathbb{F}_2$ courbe, on a (d'après la proposition 5.7) $d_H(f, l_{0_{\mathbb{F}_2^m}}) = 2^{m-1} \pm 2^{\frac{m}{2}-1} \neq 2^{m-1}$. Le deuxième point est obtenu par la définition des fonctions courbes vectorielles et grâce à la proposition 4.7 p. 60. □

5.3.6 Ensembles à différences

Il existe un autre moyen de caractériser les fonctions parfaitement non linéaires à valeurs dans $\mathbb{F}_2$. Pour ce faire on utilise la notion combinatoire d'ensembles à différences de Hadamard (voir [Dil74]).

On définit pour $A \subset \mathbb{F}_2^m$ et $\alpha \in \mathbb{F}_2^m$,

$$\sigma_\alpha(A) \stackrel{déf.}{=} \{x \oplus \alpha \in \mathbb{F}_2^m | x \in A\}$$

i.e. $\sigma_\alpha(A)$ est le *translaté* de A par α.

Proposition 5.8. [CD04] *Soit $f : \mathbb{F}_2^m \to \mathbb{F}_2$. Alors pour tout $\alpha \in \mathbb{F}_2^m$*

$$|\{x \in \mathbb{F}_2^m | d_\alpha f(x) = \beta\}| = \begin{cases} 2^m - 2(|S_f| - |\sigma_\alpha(S_f) \cap S_f|) & si\ \beta = 0\ , \\ 2(|S_f| - |\sigma_\alpha(S_f) \cap S_f|) & si\ \beta = 1\ . \end{cases}$$

Afin de démontrer cette proposition nous allons prouver tout d'abord les deux lemmes suivants inspirés de [GW99].

Lemme 5.2. *Soit X un ensemble fini non vide. Soit $A \subset X$ et $\pi \in S(X)$. On définit $\pi(A) \stackrel{déf.}{=} \{\pi(x) \in X | x \in A\}$ et $f_\pi(A) \stackrel{déf.}{=} \sum_{x \in X} \mathbf{1}_A(\pi(x)) \oplus \mathbf{1}_A(x)$ où la somme est évaluée sur les entiers.*

Alors $f_\pi(A) = |\pi(A^c) \cap A| + |\pi(A) \cap A^c|$ (où l'on rappelle que $A^c \stackrel{déf.}{=} X \setminus A$).

Preuve.

$$\begin{aligned} f_\pi(A) &= |\{x \in X | \pi(x) \in A,\ x \notin A\}| + |\{x \in X | \pi(x) \notin A,\ x \in A\}| \\ &= |\{x \notin A | \pi(x) \in A\}| + |\{x \in A | \pi(x) \notin A\}| \\ &= |\{\pi^{-1}(y) \in A^c | y \in A\}| + |\{\pi^{-1}(y) \in A | y \in A^c\}| \\ &\quad \text{(changement de variables } \pi(x) \stackrel{déf.}{=} y) \\ &= |\{y \in \pi(A^c) | y \in A\}| + |\{y \in \pi(A) | y \in A^c\}| \\ &= |\pi(A^c) \cap A| + |\pi(A) \cap A^c| \ . \end{aligned}$$

□

Lemme 5.3. *Sous les hypothèses du lemme 5.2, $f_\pi(A) = 2(|A| - |\pi(A) \cap A|)$.*

Preuve. Posons $k \stackrel{déf.}{=} |A|$ et $\lambda_\pi(A) \stackrel{déf.}{=} |\pi(A) \cap A|$.

$$\begin{aligned} |\pi(A) \cap A^c| &= |\{y \in \pi(A) | y \notin A\}| \\ &= |\pi(A) \setminus (\pi(A) \cap A)| \\ &= |\pi(A)| - |\pi(A) \cap A| \\ &= |A| - \lambda_\pi(A) \\ &= k - \lambda_\pi(A) \ . \end{aligned}$$

De plus

$$\begin{aligned} |\pi(A) \cup A^c| &= |(\pi(A) \cap A) \cup (\pi(A) \cap A^c) \cup A^c| \\ &= |(\pi(A) \cap A) \cup A^c| \\ &= |\pi(A) \cap A| + |A^c| \text{ (intersection vide)} \\ &= \lambda_\pi(A) + |X| - k \ . \end{aligned}$$

Ainsi $|(\pi(A) \cup A^c)^c| = |X| - |\pi(A) \cup A^c| = |X| - \lambda_\pi(A) - |X| + k = k - \lambda_\pi(A)$.
D'un autre côté $|(\pi(A) \cup A^c)^c| = |(\pi(A))^c \cap (A^c)^c| = |(\pi(A))^c \cap A| = |\pi(A^c) \cap A|$. La dernière égalité étant dûe au fait que $\pi(A)^c = \pi(A^c)$. En effet $\pi(A)^c = X \setminus \{\pi(x) \in X | x \in A\} = \{\pi(x) \in X | x \in X\} \setminus \{\pi(x) \in X | x \in A\}$ (car $\pi(X) = X$) $= \{\pi(x) \in X | \pi(x) \notin A\} = \pi(A^c)$.
D'où $|(\pi(A) \cup A^c)^c| = |\pi(A^c) \cap A| = k - \lambda_\pi(A)$ (d'après ce qu'on a déjà vu).
Il en résulte finalement que $f_\pi(A) = |\pi(A^c) \cap A| + |\pi(A) \cap A^c|$ (d'après le lemme 5.2) $= k - \lambda_\pi(A) + k - \lambda_\pi(A) = 2(k - \lambda_\pi(A)) = 2(|A| - |\pi(A) \cap A|)$. □

Preuve de la proposition 5.8. Il suffit de démontrer que $|S_{d_\alpha f}| = 2(|S_f| - |\sigma_\alpha(S_f) \cap S_f|)$. Or $|S_{d_\alpha f}| = f_{\sigma_\alpha}(S_f)$ et puisque $\mathbb{F}_2^m$ est un ensemble fini, $S_f \subset \mathbb{F}_2^m$ et $\sigma_\alpha \in S(\mathbb{F}_2^m)$ (puisque définie par $\sigma_\alpha : x \mapsto x \oplus \alpha$) on peut appliquer le lemme 5.3 :

$$|S_{d_\alpha f}| = 2(|S_f| - |\sigma_\alpha(S_f) \cap S_f|).$$

□

Rajoutons au passage un troisième lemme technique qui nous sert directement dans cette partie, mais sera aussi utilisé dans la suite du manuscrit.

Lemme 5.4. *Soit X un ensemble fini non vide. Soit $A \subset X$ et $\pi \in S(X)$. On a l'égalité suivante :*

$$A \cap \pi(A) = \{(x, y) \in A^2 | \pi(y) = x\} \ .$$

En particulier, $|A \cap \pi(A)|$ représente le nombre de solutions dans A^2 à l'équation à deux inconnues $x = \pi(y)$.

Preuve. Soit Θ l'application définie par

$$\begin{array}{rccl} \Theta : & A \cap \pi(A) & \to & \{(x,y) \in A^2 | \pi(y) = x\} \\ & x_0 & \mapsto & \Theta(x_0) \stackrel{déf.}{=} (x_0, \pi^{-1}(x_0)) \ . \end{array}$$

On montre tout d'abord que Θ est bien définie : c'est le cas puisque $\pi \in S(X)$.
On montre ensuite que Θ est une application bijective.
Elle est injective puisque si $(x_0, y_0) \in (A \cap \pi(A))^2$ tel que $x_0 \neq y_0$ alors $\Theta(x_0) = (x_0, \pi^{-1}(x_0)) \neq (y_0, \pi^{-1}(y_0)) = \Theta(y_0)$.
Elle est trivialement surjective puisqu'étant donné $(x_0, y_0) \in \{(x,y) \in A^2 | \pi(y) = x\}$ alors en particulier $x_0 \in A$ et $\pi^{-1}(x_0) = y_0 \in A$ donc $\Theta(x_0) = (x_0, \pi^{-1}(x_0)) = (x_0, y_0)$.
Le cardinal $|A \cap \pi(A)|$ est donc égal au cardinal $|\{(x,y) \in A^2 | \pi(y) = x\}|$ c'est-à-dire au nombre de solutions dans A^2 à l'équation à deux inconnues $x = \pi(y)$. □

Après cette courte mais utile digression reprenons le court normal de ce chapitre.

Un sous-ensemble D de $\mathbb{F}_2^m$ est un (v, k, λ)-ensemble à différences si $v = 2^m$, $|D| = k$ et l'équation à deux inconnues $x \oplus y = \alpha$ a exactement λ solutions distinctes $(x, y) \in D^2$ pour tout élément non nul α de $\mathbb{F}_2^m$.

Proposition 5.9. [CD04] *Soit D un (v, k, λ)-ensemble à différences de $\mathbb{F}_2^m$. Alors*

1. *pour chaque $\alpha \in \mathbb{F}_2^{m*}$,*

$$|\{x \in \mathbb{F}_{2^m} | d_\alpha \mathbf{1}_D(x) = \beta\}| = \begin{cases} v - 2(k-\lambda) & si\ \beta = 0 \ , \\ 2(k-\lambda) & si\ \beta = 1 \ . \end{cases}$$

2. $\max\limits_{\alpha \in \mathbb{F}_2^{m*}} \max\limits_{\beta \in \mathbb{F}_2} |\{x \in \mathbb{F}_{2^m} | d_\alpha \mathbf{1}_D(x) = \beta\}| = \max\{v - 2(k-\lambda), 2(k-\lambda)\}$.

Preuve. Le deuxième point n'étant qu'une application directe du premier, on se contente de simplement effectuer la preuve de ce dernier.
Remarquons que $S_{\mathbf{1}_D} = D$. Soit $\alpha \in \mathbb{F}_2^{m*}$. Il est facile de voir que $|\sigma_\alpha(D) \cap D| = \lambda$ (en utilisant le lemme 5.4). Maintenant il suffit d'appliquer la proposition 5.8 pour obtenir le résultat approprié. □

Théorème 5.3. [Dil74] *Soit $f : \mathbb{F}_2^m \to \mathbb{F}_2$. Alors f est parfaitement non linéaire si et seulement si S_f est un $(4n^2, 2n^2 \pm n, n(n \pm 1))$-ensemble à différences (de Hadamard) de $\mathbb{F}_2^m$ où $2^m = 4n^2$.*

Preuve. Nous commençons par l'implication directe. Le fait que la fonction f soit parfaitement non linéaire implique que $\forall (\alpha, \beta) \in \mathbb{F}_2^{m*} \times \mathbb{F}_2$, $|\{x \in \mathbb{F}_2^m | d_\alpha f(x) = \beta\}| = 2^{m-1} = 2(|S_f| - |\sigma_\alpha(S_f) \cap S_f|)$ (d'après la proposition 5.8) donc $2^m = 4(|S_f| - |\sigma_\alpha(S_f) \cap S_f|)$ d'où $2^m \equiv 0 \pmod 4$ et $\forall \alpha \in \mathbb{F}_2^{m*}$, $|\sigma_\alpha(S_f) \cap S_f|$ est constant. On désigne par la lettre grecque « λ » cette constante. Puisque pour tout $\alpha \in \mathbb{F}_2^{m*}$ il existe exactement $|\sigma_\alpha(S_f) \cap S_f| = \lambda$ solutions $(x, y) \in S_f^2$ à l'équation $x \oplus y = \alpha$ (par le lemme 5.4), S_f est un $(2^m, |S_f|, \lambda)$-ensemble à différences de $\mathbb{F}_2^m$. Comme $2^m \equiv 0 \pmod 4$, d'après [Jun92] un tel ensemble à différences n'existe que si $2^m = 4n^2$ (pour un certain n) et ses paramètres sont $(4n^2, 2n^2 \pm n, n(n \pm 1))$ (il s'agit d'un ensemble à différences de Hadamard).
Démontrons l'implication réciproque. Supposons donc que S_f soit un $(4n^2, 2n^2 \pm n, n(n \pm 1))$-ensemble à différences de $\mathbb{F}_2^m$ avec $2^m = 4n^2$. D'après la proposition 5.9 en remplaçant $\mathbf{1}_D$ par $f = \mathbf{1}_{S_f}$ et (v, k, λ) par les paramètres effectifs de S_f on conclut la preuve. □

5.3.7 Lien avec les critères de bonne diffusion

Théorème 5.4. [Pom03]
Soit $f : \mathbb{F}_2^m \to \mathbb{F}_2$. Si f est courbe alors
- *f n'a aucune structure linéaire non nulle ;*
- *f satisfait $PC(m)$. La réciproque est également vraie.*

Soit $f : \mathbb{F}_2^m \to \mathbb{F}_2^n$. Si f est courbe alors
- *f n'a aucune structure linéaire non nulle ;*
- *$\forall \beta \in {\mathbb{F}_2^n}^*$, $l_\beta \circ f$ satisfait $PC(m)$. La réciproque est également vraie.*

Preuve. Soit $f : \mathbb{F}_2^m \to \mathbb{F}_2$. Si f est courbe alors sa dérivée par rapport à tout vecteur non nul de $\mathbb{F}_2^m$ est équilibrée (théorème 5.1 et proposition 5.1). Cela implique donc que f n'a pas de structure linéaire non nulle et que f possède une bonne diffusion par rapport à tous les vecteurs de ${\mathbb{F}_2^m}^*$ *i.e.* f satisfait $PC(m)$. Supposons à l'inverse que f satisfasse $PC(m)$. Alors par définition $\forall \alpha \in \mathbb{F}_2^m$ tel que $1 \leq w_H(\alpha) \leq m$, $d_\alpha f$ est équilibrée. Ceci étant équivalent à $\forall \alpha \in {\mathbb{F}_2^m}^*$, $d_\alpha f$ est équilibrée, par applications du théorème 5.1 et de la proposition 5.1, on en déduit que f est courbe.

Soit $f : \mathbb{F}_2^m \to \mathbb{F}_2^n$. Si la fonction f est courbe, on en déduit (par le théorème 5.2) qu'elle est parfaitement non linéaire et par application de la proposition 5.1 que sa dérivée par rapport à tout vecteur non nul de $\mathbb{F}_2^m$ est équilibrée. La fonction f ne peut donc avoir de structure linéaire non nulle.
De plus par définition, f courbe $\Leftrightarrow \forall \beta \in {\mathbb{F}_2^n}^*$, $l_\beta \circ f : \mathbb{F}_2^m \to \mathbb{F}_2$ est courbe $\Leftrightarrow \forall \beta \in {\mathbb{F}_2^n}^*$, $l_\beta \circ f$ satisfait $PC(m)$ d'après la première partie de ce présent théorème. □

Proposition 5.10. *Soit $f : \mathbb{F}_2^m \to \mathbb{F}_2^n$. Si la fonction f est courbe alors elle satisfait le critère d'avalanche.*

Preuve. On sait que le fait que f soit courbe équivaut par définition à $\forall \beta \in {\mathbb{F}_2^n}^*$, $l_\beta \circ f : \mathbb{F}_2^m \to \mathbb{F}_2$ est courbe. En particulier $\forall j \in \{1, \ldots, n\}$ la fonction coordonnée $f_j : \mathbb{F}_2^m \to \mathbb{F}_2$ est courbe. Par le théorème 5.1 on en déduit que pour tout $j \in \{1, \ldots, n\}$, f_j est parfaitement non linéaire. La proposition 5.1 implique quant à elle que $\forall j \in \{1, \ldots, n\}$, $\forall \alpha \in {\mathbb{F}_2^m}^*$ et $\forall \beta \in \mathbb{F}_2$, $|\{x \in \mathbb{F}_2^m | f_j(x \oplus \alpha) \oplus f_j(x) = \beta\}| = 2^{m-1}$. En particulier pour tout $i \in \{1, \ldots, m\}$, on a $\forall j \in \{1, \ldots, n\}$ et $\forall \beta \in \mathbb{F}_2$, $|\{x \in \mathbb{F}_2^m | f_j(x \oplus e^{(i)}) \oplus f_j(x) = \beta\}| = 2^{m-1}$.
On a donc pour tout $i \in \{1, \ldots, m\}$:

$$\begin{aligned}
\sum_{x \in \mathbb{F}_2^m} d_H(f(x), f(x \oplus e^{(i)})) &= \sum_{x \in \mathbb{F}_2^m} \sum_{j=1}^{n} f_j(x \oplus e^{(i)}) \oplus f_j(x) \text{ (en plongeant } \mathbb{F}_2 \text{ dans } \mathbb{N}) \\
&= \sum_{j=1}^{n} \sum_{x \in \mathbb{F}_2^m} f_j(x \oplus e^{(i)}) \oplus f_j(x) \\
&= \sum_{j=1}^{n} |\{x \in \mathbb{F}_2^m | f_j(x \oplus e^{(i)}) \oplus f_j(x) = 1\}| \\
&= \sum_{j=1}^{n} 2^{m-1} \text{ (d'après les considérations précédentes)} \\
&= n 2^{m-1} .
\end{aligned}$$

Ainsi f satisfait le critère d'avalanche. □

Lien avec la distance de linéarité
Meier et Staffelbach [MS89] ont caractérisé la non linéarité parfaite à l'aide de la distance de linéarité L_f introduite au chapitre 4 (voir définition 4.17 p. 70).

Proposition 5.11. [MS89] *Soit* $f : \mathbb{F}_2^m \to \mathbb{F}_2$.

$$\mathsf{L}_f = 2^{m-2} \Leftrightarrow f \text{ est courbe.}$$

Preuve. Supposons que f soit parfaitement non linéaire. Alors en utilisant la proposition 5.1 et en reprenant les notations du chapitre 4 (voir p. 70), on a :
$\forall \alpha \in \mathbb{F}_2^{m*}$, $|\Delta_f(\alpha, 0)| = |\Delta_f(\alpha, 1)| = n_0(\alpha) = n_1(\alpha) = 2^{m-1}$. Donc $n_f(\alpha) = 2^{m-2}$ pour tout $\alpha \in \mathbb{F}_2^{m*}$ (voir la définition de n_f p. 71). Or comme $\mathsf{L}_f = \min\{n_f(\alpha) \in \mathbb{N} | \alpha \in \mathbb{F}_2^{m*}\}$, on a $\mathsf{L}_f = 2^{m-2}$.
Supposons maintenant que $\mathsf{L}_f = 2^{m-2}$. D'après le lien (4.18) entre L_f et n_f : $\mathsf{L}_f = \min\{n_f(\alpha) \in \mathbb{N} | \alpha \in \mathbb{F}_2^{m*}\}$, il existe $\alpha_0 \in \mathbb{F}_2^{m*}$ tel que $n_f(\alpha_0) = 2^{m-2}$. Or (d'après l'inégalité (4.19) p. 71) on a $\forall \alpha \in \mathbb{F}_2^{m*}$, $n_f(\alpha) \leq 2^{m-2}$. On déduit de ce qui précéde que $\forall \alpha \in \mathbb{F}_2^{m*}$, $n_f(\alpha) = 2^{m-2}$. Or comme par définition $n_f(\alpha) = \min\{\frac{1}{2}|\Delta_f(\alpha, 0)|, \frac{1}{2}|\Delta_f(\alpha, 1)|\}$ et que $|\Delta_f(\alpha, 0)| = 2^m - |\Delta_f(\alpha, 1)|$, on en déduit que $\forall \alpha \in \mathbb{F}_2^{m*}$, $|\Delta_f(\alpha, 0)| = |\Delta_f(\alpha, 1)| = 2^{m-1}$ et donc que f est parfaitement non linéaire par la proposition 5.1. □

On déduit de la proposition ci-dessus et de la borne sur L_f identifiée par Meier et Staffelbach et donnée dans la proposition 4.11 p. 71 que $f : \mathbb{F}_2^m \to \mathbb{F}_2$ est parfaitement non linéaire si et seulement si sa distance de linéarité est maximale parmi toutes les fonctions de $\mathbb{F}_2^{\mathbb{F}_2^m}$, soit encore si et seulement si f est la plus éloignée de l'ensemble SL_m des fonctions de $\mathbb{F}_2^{\mathbb{F}_2^m}$ ayant une structure linéaire non nulle (et cette distance est 2^{m-2}).

On a finalement une dernière relation entre distance de linéarité et résistance à la cryptanalyse différentielle.

Proposition 5.12. [MS89] *La distance linéaire* L_f *de* $f : \mathbb{F}_2^m \to \mathbb{F}_2$ *est liée à* P_f *par la formule :*

$$\mathsf{L}_f = 2^{m-1}(1 - \mathsf{P}_f) \ .$$

Preuve. On a $\mathsf{L}_f = \min\{n_f(\alpha) \in \mathbb{N} | \alpha \in \mathbb{F}_2^{m*}\} = \frac{1}{2}\min\{|\Delta_f(\alpha, \beta)| \in \mathbb{N} | (\alpha, \beta) \in \mathbb{F}_2^{m*} \times \mathbb{F}_2\}$. Supposons que le minimum soit atteint pour un certain $(\alpha_0, \beta_0) \in \mathbb{F}_2^{m*} \times \mathbb{F}_2$ *i.e.* $\mathsf{L}_f = \frac{1}{2}|\Delta_f(\alpha_0, \beta_0)|$. Alors $|\Delta_f(\alpha_0, \beta_0 \oplus 1)| = 2^m - |\Delta_f(\alpha_0, \beta_0)|$ est maximum et donc $|\Delta_f(\alpha_0, \beta_0)| = \max_{\alpha \in \mathbb{F}_2^{m*}} \max_{\beta \in \mathbb{F}_2} |\Delta_f(\alpha, \beta)| = 2^m \mathsf{P}_f$. Ce qui nous permet de conclure. □

5.3.8 Conclusion

Le bien-fondé de cette section est conséquence du fait que la suite du contenu du manuscrit est tributaire de la compréhension totale des notions de fonctions courbes et parfaitement non linéaires.

Les propriétés de ces fonctions, exposées ici, permettent d'une part de mieux appréhender leur « dynamique » et d'autre part de mettre en valeur leur caractère aberrant au sein des fonctions booléennes. De fait nous avons été amenés à considérer sous divers angles ces deux concepts équivalents. Plusieurs caractérisations, chacune d'entre elles illustrant un point de vue particulier, ont ainsi été formulées.

Certaines des propriétés évoquées *passent les généralisations* des chapitres suivants c'est-à-dire qu'elles restent vraies dans un cadre plus général. Cependant il faut prendre soin, autant que faire se peut, de ne pas raisonner par analogie en croyant, bien souvent à tord, que les caractérisations précédentes sont toutes conservées à l'identique dans des extensions des notions de non linéarité parfaite et de fonction courbe. Aussi, lorsque le moment sera venu, certaines de ces

propriétés seront explicitement et minutieusement établies de nouveau dans un scope plus général.

Au point où nous en sommes, aucune fonction courbe n'a encore été exhibée. Cette carence est comblée dans la section suivante.

5.4 Constructions de fonctions courbes

5.4.1 Introduction

Une classification complète des fonctions courbes semble à la fois hors de portée et sans espoir[2]. En dépit de leur simple et naturelle définition, elles s'avèrent posséder une structure fort complexe en général. Néanmoins de nombreuses instances de constructions explicites sont bien connues, les *primaires* donnant des fonctions courbes *from scratch* telle une génération spontanée c'est-à-dire les constructions *ex nihilo*, et les *secondaires* présupposant l'existence d'une ou de plusieurs fonctions courbes données *a priori* et en construisant de nouvelles à partir de celles-ci. Les ensembles de fonctions courbes regroupant des fonctions de même « forme » sont appelés *classes*. On s'intéresse ici essentiellement aux classes primaires de fonctions courbes à valeurs dans $\mathbb{F}_2$ c'est-à-dire que l'on déploie nos efforts sur les fonctions de $\mathcal{B}_m$.

La sous-section suivante expose un certain nombre de généralités concernant les classes de fonctions courbes. Par ailleurs la première preuve d'existence de telles fonctions, les plus simples d'entre elles, y est dépeinte. Puis nous nous focalisons sur des constructions primaires plus complexes en inventoriant celles qui sont les plus connues.

5.4.2 Etude générale

Rappelons que $GA(\mathbb{F}_2^m)$ est l'ensemble des applications affines bijectives de $\mathbb{F}_2^m$ dans lui-même (voir p. 68 le paragraphe : *L'ensemble des fonctions affines*).

Proposition 5.13. [CD04] *Soit $f : \mathbb{F}_2^m \to \mathbb{F}_2$. Soient $\delta \in GA(\mathbb{F}_2^m)$ et $\delta' \in R(1,m)$. Si f est courbe alors $(f \circ \delta) \oplus \delta'$ l'est également.*

Preuve. Dire que f est courbe revient à affirmer que f est parfaitement non linéaire (d'après le théorème 5.1). On a ainsi (d'après la proposition 5.1) pour tout $\alpha \in \mathbb{F}_2^{m\,*}$ et tout $\beta \in \mathbb{F}_2$,

$$|\{x \in \mathbb{F}_2^m \,|\, f(x \oplus \alpha) \oplus f(x) = \beta\}| = 2^{m-1} \,. \tag{5.7}$$

Par ailleurs puisque δ est une bijection affine de $\mathbb{F}_2^m$ dans lui-même, il existe $\lambda \in GL(\mathbb{F}_2^m)$ (en particulier son noyau vérifie $\ker(\lambda) = \{0_{\mathbb{F}_2^m}\}$) et $\mu \in \mathbb{F}_2^m$ tel que $\forall x \in \mathbb{F}_2^m$, $\delta(x) = \lambda(x) \oplus \mu$ *i.e.* $\delta = \sigma_\mu \circ \lambda$. Enfin comme $\delta' \in R(1,m)$, il existe $(\gamma, \epsilon) \in \mathbb{F}_2^m \times \mathbb{F}_2$ tel que $\forall x \in \mathbb{F}_2^m$, $\delta'(x) = \gamma.x \oplus \epsilon$. On a ainsi les égalités successives pour $(\alpha, \beta) \in \mathbb{F}_2^{m\,*} \times \mathbb{F}_2$:

$$\begin{aligned}
& |\{x \in \mathbb{F}_2^m \,|\, f(\delta(x \oplus \alpha) \oplus \delta'(x \oplus \alpha) \oplus f(\delta(x)) \oplus \delta'(x) = \beta\}| \\
= \; & |\{x \in \mathbb{F}_2^m \,|\, f(\lambda(x) \oplus \lambda(\alpha) \oplus \mu) \oplus \gamma.x \oplus \gamma.\alpha \oplus \epsilon \oplus f(\delta(x)) \oplus \gamma.x \oplus \epsilon = \beta\}| \\
= \; & |\{x \in \mathbb{F}_2^m \,|\, f(\delta(x) \oplus \lambda(\alpha)) \oplus f(\delta(x)) = \beta \oplus \gamma.\alpha\}| \\
= \; & |\{y \in \mathbb{F}_2^m \,|\, f(y \oplus \lambda(\alpha)) \oplus f(y) = \beta \oplus \gamma.\alpha\}| \text{ (par le changement de variables : } y \overset{déf.}{=} \delta(x)) \\
= \; & 2^{m-1} \,.
\end{aligned}$$

La dernière égalité étant obtenue à partir de la formule (5.7) dans laquelle on substitue les lettres « α » et « β » respectivement par les expressions « $\lambda(\alpha)$ » et « $\beta \oplus \gamma.\alpha$ ». Ceci est valide puisque $\lambda(\alpha) = 0_{\mathbb{F}_2^m} \Leftrightarrow \alpha = 0_{\mathbb{F}_2^m}$. □

[2] Mais rien n'empêche d'essayer !

Corollaire 5.3. *Soit $f : \mathbb{F}_2^m \to \mathbb{F}_2$ courbe. Alors sa négation $\overline{f} \stackrel{déf.}{=} f \oplus \mathbf{1}_{\mathbb{F}_2^m}$ est également courbe.*

Preuve. Il suffit d'utiliser le théorème précédent avec $\delta = Id_{\mathbb{F}_2^m}$ et $\delta' = \overline{l_{0_{\mathbb{F}_2^m}}} = \mathbf{1}_{\mathbb{F}_2^m}$. □

Pour $(\delta, \delta') \in GA(F_2^m) \times R(1,m)$, on définit

$$\begin{array}{rccc} \pi_{\delta,\delta'} : & {\mathbb{F}_2}^{\mathbb{F}_2^m} & \to & {\mathbb{F}_2}^{\mathbb{F}_2^m} \\ & f & \mapsto & (f \circ \delta) \oplus \delta' \ . \end{array}$$

Cette transformation est elle-même une application affine bijective[3] et donc en particulier l'ensemble de telles transformations est inclus dans $S({\mathbb{F}_2^{\mathbb{F}_2^m}})$. Il contient la transformation $\pi_{Id_{\mathbb{F}_2^m}, l_{0_{\mathbb{F}_2^m}}}$ qui est $Id_{\mathbb{F}_2^{\mathbb{F}_2^m}}$. Plus précisément, cet ensemble est un groupe non commutatif isomorphe au produit semi-direct (voir la définition 4.14 p. 68) $GA(\mathbb{F}_2^m) \ltimes_\Psi R(1,m)$ où l'homomorphisme de groupes Ψ est défini par

$$\begin{array}{rccc} \Psi : & GA(\mathbb{F}_2^m) & \to & Aut(R(1,m)) \\ & \delta & \mapsto & (\Psi(\delta) : \delta' \mapsto \delta' \circ \delta) \ . \end{array}$$

A partir de maintenant, nous confondons le groupe des transformations $\pi_{\delta,\delta'}$ avec $GA(\mathbb{F}_2^m) \ltimes_\Psi R(1,m)$.

D'après la proposition 5.13 et la discussion précédente, on en déduit par ailleurs que le groupe $GA(\mathbb{F}_2^m) \ltimes_\Psi R(1,m)$ agit sur $\mathcal{B}_m$. Nous évitons pour le moment d'entrer dans les détails tout en sachant que la notion d'actions de groupe est à la base des chapitres de la deuxième partie du manuscrit. Le lecteur pourra néanmoins se référer à la section 7.2 pour en savoir davantage au sujet des actions de groupe.

Comme signalé en introduction, les ensembles de fonctions courbes sont appelés *classes* de fonctions courbes. Par le biais de la proposition précédente on établit une notion de *complétude* pour une classe.

Définition 5.7. Une classe $\mathcal{K} \subset \mathcal{B}_m$ de fonctions courbes est dite *complète* si elle est stable par rapport à l'ensemble des transformations $GA(\mathbb{F}_2^m) \ltimes_\Psi R(1,m)$ *i.e.* $\forall (\delta, \delta') \in GA(F_2^m) \times R(1,m)$,

$$\text{si } f \in \mathcal{K} \text{ alors } \pi_{\delta,\delta'}(f) \in \mathcal{K} \ .$$

Si la classe $\mathcal{K}$ n'est pas complète, on appelle *complété* de $\mathcal{K}$, noté « $\overline{\mathcal{K}}$ », la classe obtenue en complétant $\mathcal{K}$ par l'ensemble des fonctions produites à partir de $\mathcal{K}$ à l'aide des transformations de $GA(\mathbb{F}_2^m) \ltimes_\Psi R(1,m)$:

$$\overline{\mathcal{K}} = \mathcal{K} \cup \{\pi(f) : \mathbb{F}_2^m \to \mathbb{F}_2 | \pi \in GA(\mathbb{F}_2^m) \ltimes_\Psi R(1,m),\ f \in \mathcal{K}\} \setminus \mathcal{K} \ .$$

Voici une caractérisation importante pour la classe des fonctions courbes les plus simples. Elle est donnée ici sans preuve.

Proposition 5.14. [Dil74] *Soit $m \in \mathbb{N}^*$ un entier pair. Soit $f : \mathbb{F}_2^m \to \mathbb{F}_2$ tel que* $\deg(f) = 2$. *Si f est courbe alors il existe $\pi \in GA(\mathbb{F}_2^m) \ltimes_\Psi R(1,m)$ tel que pour tout $(x_1, \ldots, x_m) \in \mathbb{F}_2^m$:*

$$\pi(f)(x_1, \ldots, x_m) = x_1x_2 \oplus x_3x_4 \oplus \ldots \oplus x_{m-1}x_m \ .$$

[3] En effet pour $(f, g) \in ({\mathbb{F}_2}^{\mathbb{F}_2^m})^2$:
- $\pi_{\delta,\delta'}$ est affine : $\pi_{\delta,\delta'}(f \oplus g) = (f \oplus g) \circ \delta \oplus \delta' = f \circ \delta \oplus g \circ \delta \oplus \delta'$
- $\pi_{\delta,\delta'}$ est bijective :
  - si $f \neq g$ alors par bijectivité de δ, $f \circ \delta \neq g \circ \delta$ et donc finalement $\pi_{\delta,\delta'}(f) \neq \pi_{\delta,\delta'}(g)$;
  - $\pi_{\delta,\delta'}((f \oplus \delta') \circ \delta^{-1}) = f$.

Etant donné $m \in \mathbb{N}^*$ pair, cette proposition indique ainsi que toute fonction quadratique courbe est en fait égale à la fonction

$$\begin{array}{rccl} q^{(m)}: & \mathbb{F}_2^m & \to & \mathbb{F}_2 \\ & x & \mapsto & x_1x_2 \oplus x_3x_4 \oplus \ldots \oplus x_{m-1}x_m \end{array}$$

modulo une transformation de $GA(\mathbb{F}_2^m) \ltimes_\Psi R(1,m)$ ou, en d'autres termes, que toute fonction quadratique courbe peut être mise sous la forme « canonique » $q^{(m)}$.

Pour m un entier pair, notons « $\mathcal{Q}_m$ » l'ensemble $\mathcal{B}_m \cap R(2,m)$ des fonctions courbes quadratiques définies sur $\mathbb{F}_2^m$ et à valeurs dans $\mathbb{F}_2$. On déduit de la proposition précédente que tout élément de $\mathcal{Q}_m$ est atteint à partir d'une certaine transformation de $q^{(m)}$, soit encore que $GA(\mathbb{F}_2^m) \ltimes_\Psi R(1,m)$ agit transitivement sur $\mathcal{Q}_m$ (voir la définition 7.6 p. 134). Attention cependant, ce résultat n'implique pas que $q^{(m)}$ est courbe puisqu'on ne sait pas, pour le moment, si des fonctions courbes quadratiques existent. Cette lacune est cependant tout de suite comblée.

Proposition 5.15. [Rot76] *Pour tout entier $m > 0$ pair, la fonction $q^{(m)} : \mathbb{F}_2^m \to \mathbb{F}_2$ comme précédemment définie est (quadratique) courbe.*

Preuve. Nous réalisons une preuve par récurrence sur $m \in \mathbb{N}^*$ pair.

Supposons que $m = 2$. Dans ce cas pour $(x_1, x_2) \in \mathbb{F}_2^2$, $q^{(2)}(x_1, x_2) = x_1x_2$. Soit $\alpha \in \mathbb{F}_2^2 \setminus \{(0,0)\}$. On a $|\{x \in \mathbb{F}_2^2 | q^{(2)}(x \oplus \alpha) \oplus q^{(2)}(x) = 0\}| = |\{x \in \mathbb{F}_2^2 | x_1\alpha_2 \oplus x_2\alpha_1 \oplus \alpha_1\alpha_2 = 0\}|$. Puisque $\alpha \in \mathbb{F}_2^2 \setminus \{(0,0)\}$, on a deux cas possibles : soit $w_H(\alpha) = 1$ soit $w_H(\alpha) = 2$.

1. Supposons que $w_H(\alpha) = 1$. Soit alors $j \in \{1,2\}$ tel que $\alpha_j = 1$. On a alors $x_1\alpha_2 \oplus x_2\alpha_1 \oplus \alpha_1\alpha_2 = x_i\alpha_j = x_i$ pour $i \in \{1,2\}$ tel que $i \neq j$. D'où $|\{x \in \mathbb{F}_2^2 | q^{(2)}(x \oplus \alpha) \oplus q^{(2)}(x) = 0\}| = 2$.
2. Supposons que $w_H(\alpha) = 2$ *i.e.* $\alpha = (1,1)$. On a alors $x_1\alpha_2 \oplus x_2\alpha_1 \oplus \alpha_1\alpha_2 = x_1 \oplus x_2 \oplus 1$ et donc $|\{x \in \mathbb{F}_2^2 | q^{(2)}(x \oplus \alpha) \oplus q^{(2)}(x) = 0\}| = |\{x \in \mathbb{F}_2^2 | x_1 \oplus x_2 = 1\}| = 2$.

On en déduit que la dérivée $d_\alpha q^{(2)}$ est équilibrée et donc que $q^{(2)}$ est parfaitement non linéaire, autrement dit $q^{(2)}$ est courbe.

Supposons $m > 2$ pair et par hypothèse de récurrence que $\forall k \in \mathbb{N}^*$ pair tel que $k < m$, $q^{(k)}$ soit courbe. On a pour $x \in \mathbb{F}_2^m$,

$$\begin{array}{rcl} q^{(m)}(x) & = & x_1x_2 \oplus x_3x_4 \oplus \ldots \oplus x_{m-1}x_m \\ & = & q^{(m-2)}(x_1, x_2, \ldots, x_{m-3}, x_{m-2}) \oplus q^{(2)}(x_{m-1}, x_m) \\ & = & (q^{(m-2)} \otimes q^{(2)})((x_1, x_2, \ldots, x_{m-3}, x_{m-2}), (x_{m-1}, x_m)) \ . \end{array}$$

Par hypothèse de récurrence on sait que $q^{(m-2)}$ et $q^{(2)}$ sont courbes et en utilisant la proposition 5.6 p. 83 on en déduit que $q^{(m)}$ est elle-même courbe. □

Remarquons que pour m pair et $(x_1, \ldots, x_m) \in \mathbb{F}_2^m$, on a

$$q^{(m)}(x_1, \ldots, x_m) = x_1x_2 \oplus \ldots \oplus x_{m-1}x_m = x^{(i)}.x^{(p)}$$

où $(x^{(i)}, x^{(p)}) \in (\mathbb{F}_2^{\frac{m}{2}})^2$ tel que $x_j^{(i)} \stackrel{déf.}{=} x_{2j-1}$ et $x_j^{(p)} \stackrel{déf.}{=} x_{2j}$ pour $j \in \{1, \ldots, \frac{m}{2}\}$ et « . » désigne le produit scalaire de $\mathbb{F}_2^{\frac{m}{2}}$. On en déduit en particulier que la fonction $(x,y) \in (\mathbb{F}_2^{\frac{m}{2}})^2 \mapsto x.y \in \mathbb{F}_2$ est courbe (quadratique).

Nous allons maintenant présenter les principales classes primaires de fonctions booléennes courbes. A plusieurs reprises sera effectuée, dans cette partie, l'identification suivante d'espaces vectoriels :

pour m un entier pair, on confond l'espace $\mathbb{F}_2^m$ avec $\mathbb{F}_2^{\frac{m}{2}} \times \mathbb{F}_2^{\frac{m}{2}}$. Dans cette configuration un vecteur de $\mathbb{F}_2^m$ est identifié à un couple $(x, y) \in (\mathbb{F}_2^{\frac{m}{2}})^2$.

La plupart des résultats énoncés jusqu'à la fin de cette section sont donnés sans preuve. Le lecteur pourra néanmoins consulter les références bibliographiques correspondantes.

5.4.3 Classe de Maiorana-MacFarland

Nous venons d'observer que la fonction $(x, y) \mapsto f(x, y) = x.y$ est courbe. Il s'agit certainement de la plus simple des constructions possibles de fonctions courbes. Rothaus [Rot76], ayant remarqué que si l'on somme la fonction précédente avec n'importe quelle autre fonction à valeurs dans $\mathbb{F}_2$ ne dépendant que d'une seule des deux variables x et y, cela ne modifie pas le caractère courbe, il a introduit une nouvelle classe de fonctions courbes :

Proposition 5.16. [Rot76] *Soit m un entier pair. Soit $g : \mathbb{F}_2^{\frac{m}{2}} \to \mathbb{F}_2$ une fonction. Alors la fonction $f : \mathbb{F}_2^m \to \mathbb{F}_2$ définie pour $(x, y) \in (\mathbb{F}_2^{\frac{m}{2}})^2$ par*

$$f(x, y) = x.y \oplus g(y)$$

est une fonction courbe.

Cette construction a été généralisée indépendamment par J.F. Dillon dans sa thèse [Dil74] ainsi que par Mac Farland [McF73].

Définition 5.8. Soit m un entier pair. La classe de *Maiorana-MacFarland*, notée « $\mathcal{M}_m$ », de fonctions courbes de $\mathbb{F}_2^{\mathbb{F}_2^m}$ est définie par :

$$\mathcal{M}_m = \{f \in \mathcal{B}_m | \exists (\pi, g) \in S(\mathbb{F}_2^{\frac{m}{2}}) \times (\mathbb{F}_2)^{\mathbb{F}_2^{\frac{m}{2}}} \text{ tel que } \forall (x, y) \in (\mathbb{F}_2^{\frac{m}{2}})^2,\ f(x, y) = x.\pi(y) \oplus g(y)\}$$

où comme d'habitude « . » désigne le produit scalaire naturel de $\mathbb{F}_2^{\frac{m}{2}}$.

Proposition 5.17. [Dil74] *Soit m un entier pair. Si $f \in \mathcal{M}_m$ alors sa duale $\tilde{f} : \mathbb{F}_2^m \to \mathbb{F}_2$ est définie pour $(x, y) \in (\mathbb{F}_2^{\frac{m}{2}})^2$ par*

$$\tilde{f}(x, y) = y.\pi^{-1}(x) \oplus g(\pi^{-1}(x)).$$

En particulier si on note $\boldsymbol{\sigma} \in S((\mathbb{F}_2^{\frac{m}{2}})^2)$ l'involution[4] définie par $(x, y) \mapsto \boldsymbol{\sigma}(x, y) \stackrel{déf.}{=} (y, x)$, pour tout $f \in \mathcal{M}_m$ on a $\tilde{f} \circ \boldsymbol{\sigma} \in \mathcal{M}_m$.

Proposition 5.18. [Dil74] *Soit m un entier pair. La classe complétée de $\mathcal{M}_m$ contient toutes les fonctions courbes quadratiques i.e.*

$$\mathcal{Q}_m \subset \overline{\mathcal{M}_m}\ .$$

5.4.4 Classe des « Partial Spreads »

Cette classe notée, pour m un entier pair, « $\mathcal{P}_m$ » a aussi été introduite par Dillon dans sa thèse.

Définition 5.9. Soit m un entier pair. La classe $\mathcal{P}_m$ de fonctions courbes de $\mathbb{F}_2^m \to \mathbb{F}_2$ est constituée de l'union de deux sous-classes $\mathcal{P}_m^-$ et $\mathcal{P}_m^+$ définies comme suit.
Soient $V_1, \ldots, V_{2^{\frac{m}{2}-1}}, V_{2^{\frac{m}{2}-1}+1}$ des sous-espaces vectoriels de $\mathbb{F}_2^m$ chacun de dimension $\frac{m}{2}$ tels que $V_i \cap V_j = \{0_{\mathbb{F}_2^m}\}$ pour $i \neq j$. Alors la fonction indicatrice $\mathbf{1}_{A_-}$ de

$$A_- = \bigcup_{i=1}^{2^{\frac{m}{2}-1}} V_i \setminus \{0_{\mathbb{F}_2^m}\}$$

[4] Cette involution a déjà été rencontrée au chapitre 2 p. 17. On rappelle en outre qu'une permutation $\boldsymbol{\sigma} \in S(X)$ est une *involution* si $\boldsymbol{\sigma} \circ \boldsymbol{\sigma} = \boldsymbol{\sigma}^2 = Id_X$ *i.e.* $\boldsymbol{\sigma}^{-1} = \boldsymbol{\sigma}$. Nous reparlons de cette notion dans l'annexe B.

est un élément de $\mathcal{P}_m^-$.
La fonction indicatrice $\mathbf{1}_{A_+}$ de

$$A_+ = \bigcup_{i=1}^{2^{\frac{m}{2}-1}+1} V_i$$

est un élément de $\mathcal{P}_m^+$.

La construction effective de fonctions de $\mathcal{P}_m$ s'avérant difficile, une certaine sous-classe, notée « $\mathcal{P}_{m,ap}$ », de $\mathcal{P}_m$ a également été définie :
$\mathcal{P}_{m,ap} \stackrel{déf.}{=} \{f : \mathbb{F}_2^m \to \mathbb{F}_2 | \exists g : \mathbb{F}_2^{\frac{m}{2}} \to \mathbb{F}_2$ équilibré et tel que $\forall (x,y) \in (\mathbb{F}_2^{\frac{m}{2}})^2,\ f(x,y) = g(\frac{x}{y})\}$ où le $\mathbb{F}_2$-espace vectoriel $\mathbb{F}_2^{\frac{m}{2}}$ est plongé dans le corps $\mathbb{F}_{2^{\frac{m}{2}}}$, $\frac{x}{y} \stackrel{déf.}{=} xy^{-1}$ pour tout $(x,y) \in \mathbb{F}_{2^{\frac{m}{2}}} \times \mathbb{F}^*_{2^{\frac{m}{2}}}$ (« y^{-1} » désignant quant à lui l'inverse de y dans le corps considéré) et conventionnellement prolongé aux points $(x, 0_{\mathbb{F}_2^{\frac{m}{2}}})$ par $\frac{x}{0_{\mathbb{F}_2^{\frac{m}{2}}}} \stackrel{déf.}{=} 0_{\mathbb{F}_2^{\frac{m}{2}}}$.

5.4.5 Classes introduites par C. Carlet

Les définitions de cette sous-section sont tirées de [Car94].

Définition 5.10. Soit m un entier pair. La classe $\mathcal{C}_m \subset \mathcal{B}_m$ est définie comme suit :
$f \in \mathcal{C}_m \Leftrightarrow \exists\, \pi \in S(\mathbb{F}_2^{\frac{m}{2}})$ et un sous-espace vectoriel V de $\mathbb{F}_2^{\frac{m}{2}}$ tel que pour tout $\alpha \in \mathbb{F}_2^m$ l'ensemble $\pi^{-1}(\alpha \oplus V^\perp)$ soit un espace affine (« $V^\perp$ » désignant, on le rappelle, l'orthogonal de V), tels que pour tout $(x,y) \in (\mathbb{F}_2^{\frac{m}{2}})^2$

$$f(x,y) = x.\pi(y) \oplus \mathbf{1}_V(y)\ .$$

La seconde classe introduite par Carlet dans [Car94] est la suivante :

Définition 5.11. Soit m un entier pair. La classe $\mathcal{D}_m \subset \mathcal{B}_m$ est définie comme suit :
$f \in \mathcal{D}_m \Leftrightarrow \exists \pi \in S(\mathbb{F}_2^{\frac{m}{2}})$ et deux sous-espaces vectoriels de $\mathbb{F}_2^{\frac{m}{2}}$ désignés par « V_1 » et « V_2 » tels que $\dim_{\mathbb{F}_2}(V_1) + \dim_{\mathbb{F}_2}(V_2) = \frac{m}{2}$, $\pi(V_2) = V_1^\perp$ et pour tout $(x,y) \in (\mathbb{F}_2^{\frac{m}{2}})^2$

$$f(x,y) = x.\pi(y) \oplus \mathbf{1}_{V_1}(x)\mathbf{1}_{V_2}(y)\ .$$

5.4.6 Classe des « Generalized Partial Spreads »

Claude Carlet dans [Car95] a défini une nouvelle et importante classe de fonctions courbes. Le résultat fondamental la concernant est que toute fonction courbe (binaire) appartient à cette classe, modulo une composition par une translation.

Théorème 5.5. [Car95] *Soit m un entier pair, $(V_1, \ldots, V_k)$ un k-uplet de sous-espaces vectoriels de $\mathbb{F}_2^m$ chacun de dimension $\frac{m}{2}$ et $(n_1, \ldots, n_k)$ un k-uplet d'entiers. Soit $f : \mathbb{F}_2^m \to \mathbb{F}_2$. Si $\forall x \in \mathbb{F}_2^m$, f satisfait*

$$f(x) = \sum_{i=1}^{k} n_i \mathbf{1}_{V_i}(x) - 2^{\frac{m}{2}-1}\mathbf{1}_{\{0_{\mathbb{F}_2^m}\}}(x) \tag{5.8}$$

alors f est courbe.
De plus sa duale $\tilde{f}$ satisfait alors pour tout $x \in \mathbb{F}_2^m$

$$\tilde{f}(x) = \sum_{i=1}^{k} n_i \mathbf{1}_{V_i^\perp}(x) - 2^{\frac{m}{2}-1}\mathbf{1}_{\{0_{\mathbb{F}_2^m}\}}(x)\ .$$

Définition 5.12. On appelle « $\mathcal{G}_m$ » la classe des fonctions courbes définies sur $\mathbb{F}_2^m$ et à valeurs dans $\mathbb{F}_2$ satisfaisant la formule (5.8).

Proposition 5.19. [Car95] *La classe complétée de $\mathcal{G}_m$ contient les classes $\mathcal{M}_m$, $\mathcal{P}_m$ et $\mathcal{D}_m$.*

Certaines des propriétés de cette classe sont listées ci-dessous.

Proposition 5.20. [Car95] *Soit $f \in \mathcal{G}_m$. Alors :*

- $\bar{f} \stackrel{déf.}{=} f \oplus \mathbf{1}_{\mathbb{F}_2^m} \in \mathcal{G}_m$;
- $\forall \lambda \in GL(\mathbb{F}_2^m)$, $f \circ \lambda \in \mathcal{G}_m$;
- $\tilde{f} \in \mathcal{G}_m$ *(la classe $\mathcal{G}_m$ est alors dite* auto-duale*)* ;
- $f(0_{\mathbb{F}_2^m}) = \tilde{f}(0_{\mathbb{F}_2^m})$.

Ainsi que cela fut remarqué par Carlet, une conséquence de la dernière propriété indique que $\mathcal{G}_m$ ne couvre pas toutes les fonctions courbes de $\mathcal{B}_m$. En effet si f est courbe et $\alpha \in \mathbb{F}_2^m$ tel que $f(\alpha) \neq f(0_{\mathbb{F}_2^m})$ alors la fonction $f_\alpha \stackrel{déf.}{=} f \circ \sigma_\alpha$, *i.e.* $f_\alpha : x \mapsto f(x \oplus \alpha)$, est courbe (d'après la proposition 5.13) et satisfait $f_\alpha(0_{\mathbb{F}_2^m}) = f(\alpha) \neq \tilde{f}(0_{\mathbb{F}_2^m}) = \tilde{f}_\alpha(0_{\mathbb{F}_2^m})$.

Dans [Gui01] Guillot a démontré le résultat fondamental suivant.

Théorème 5.6. [Gui01] *Soient m pair, $m \geq 4$ et $f \in \mathcal{B}_m$. Alors*

$$f \in \mathcal{G}_m \Leftrightarrow f(0_{\mathbb{F}_2^m}) = \tilde{f}(0_{\mathbb{F}_2^m}) \ .$$

De cela on en déduit que dans un certain sens la classe $\mathcal{G}_m$ contient toutes les fonctions booléennes courbes à valeurs dans $\mathbb{F}_2$.

Corollaire 5.4. [Gui01] *A une composition par une translation près, toute fonction de $\mathcal{B}_m$ est un élément de $\mathcal{G}_m$.*

Preuve. Soit $f \in \mathcal{B}_m$. Si $f(0_{\mathbb{F}_2^m}) \neq \tilde{f}(0_{\mathbb{F}_2^m})$, soit $\alpha \in \mathbb{F}_2^m$ tel que $f(0_{\mathbb{F}_2^m}) \neq f(\alpha)$. Alors la fonction $f_\alpha \stackrel{déf.}{=} f \circ \sigma_\alpha$ vérifie $f_\alpha(0_{\mathbb{F}_2^m}) = \tilde{f}_\alpha(0_{\mathbb{F}_2^m})$ (puisque $f_\alpha(0_{\mathbb{F}_2^m}) = f(\alpha) \neq f(0_{\mathbb{F}_2^m}) \neq \tilde{f}(0_{\mathbb{F}_2^m}) = \tilde{f}_\alpha(0_{\mathbb{F}_2^m})$) et donc appartient à $\mathcal{G}_m$ par le théorème précédent. □

Ce dernier résultat généralise donc celui énoncé par la proposition 5.13 de manière spectaculaire.

5.4.7 Conclusion

Comme pour la classification en branches et espèces du règne animal, les fonctions courbes se répartissent en certaines classes. Mais elles ne se laissent pas docilement cataloguer dans des catégories bien précises. Toutefois leur classification, sorte de quête du Saint-Graal, au sein de classes a été succinctement mais non exhaustivement exposée ici. Nous avons donc eu l'opportunité d'observer diverses approches pour la construction pratique de ces fonctions.

L'une des classes, celles des « Generalized Partial Spreads », est si générale qu'elle regroupe essentiellement toutes les fonctions courbes. Ainsi avec sa découverte, on aurait pu croire le problème d'élaboration concrète des fonctions courbes clos. Cependant il n'en est rien. Très récemment en effet, plusieurs travaux, dans ce domaine, ont été réalisés, donnant comme un second souffle aux recherches « constructives ».

Dans [Dob95] H. Dobbertin a introduit les notions de fonctions booléennes normales et faiblement normales. Soit m pair. Une fonction $f : \mathbb{F}_2^m \to \mathbb{F}_2$ est *faiblement normale* (respectivement

normale) si elle est affine (respectivement *constante*) sur un sous-espace affine de dimension $\frac{m}{2}$. Il a été montré dans [CDL+03] que la plupart des constructions primaires connues de fonctions courbes donnent des fonctions faiblement normales. Néanmoins une preuve d'existence de fonctions courbes non normales a été obtenue dans ce même papier, contredisant la conjecture faîte par plusieurs auteurs réfutant leur existence. La preuve est basée sur un algorithme très efficace déterminant pour une fonction donnée son caractère normal ou non (voir [DHL03]). Récemment dans [DH04] a aussi été exhibée une construction de fonction courbe non normale. Le résultat est rappelé ici (sans sa démonstration).

Théorème 5.7. [DH04] *Soit* $(m,k) \in (\mathbb{N}^*)^2$ *tel que* $pgcd(k,m) = 1$. *Soient* $n \stackrel{déf.}{=} 2^{2k} - 2^k + 1$ *et* $\alpha \in \mathbb{F}_{2^m}$. *Soit* B *une base de* $\mathbb{F}_{2^m}$. *La fonction*[5]

$$\begin{array}{rccl} f: & \mathbb{F}_2^m & \to & \mathbb{F}_2 \\ & x & \mapsto & tr(\alpha \Phi_B^{-1}(x^n)) \ . \end{array}$$

est courbe si et seulement si $\alpha \notin \{x^3 \in \mathbb{F}_{2^m} | x \in \mathbb{F}_{2^m}\}$.

Cette fonction courbe non normale est cependant assez énigmatique. D'une part elle n'appartient à aucune des classes connues à ce jour et d'autre part, on ne sait rien de sa duale. Gageons donc que de nouvelles avancées dans ce domaine vont rapidement être effectuées[6].

5.5 Fonctions presque parfaitement linéaires et presque courbes

5.5.1 Introduction

Nous ne sommes plus sans ignorer que les fonctions courbes ou parfaitement non linéaires de $\mathbb{F}_2^m$ $^{\mathbb{F}_2^n}$ n'existent que lorsque m est pair et $m \geq 2n$ (voir la proposition 5.3). Cependant dans toutes les configurations possibles des exposants $(m,n) \in (\mathbb{N}^*)^2$, nous devons être capables de mesurer les résistances optimales face aux attaques linéaire et différentielle. Puisque les bornes concernant les fonctions parfaitement linéaires et de manière équivalente, celles des fonctions courbes, ne sont plus atteignables lorsque m est impair ou $m < 2n$, il nous faut établir de nouveaux extrema.

Pour chaque fonction $f : \mathbb{F}_2^m \to \mathbb{F}_2^n$, il est facile de voir que $\max_{\alpha \in \mathbb{F}_2^{m*}} \max_{\beta \in \mathbb{F}_2^n} |\Delta_f(\alpha,\beta)| \geq 2$. Il en résulte que la probabilité de non linéarité de f satisfait toujours trivialement $\mathsf{P}_f \geq \frac{1}{2^{m-1}}$.

Dans [NK93] Nyberg et Knudsen se sont basés sur cette borne afin d'étudier les résistances idéales à l'attaque différentielle dans les cas où les fonctions parfaitement non linéaires n'existent pas.

5.5.2 Définitions et résultats

Définition 5.13. Une fonction $f : \mathbb{F}_2^m \to \mathbb{F}_2^n$ telle que $\mathsf{P}_f = \frac{1}{2^{m-1}}$ est dite *presque parfaitement non linéaire.*

Remarquons que si $f : \mathbb{F}_2^m \to \mathbb{F}_2^n$ est presque parfaitement non linéaire alors pour chaque $(\alpha,\beta) \in \mathbb{F}_2^{m*} \times \mathbb{F}_2^n$ la fonction $f_{\alpha,\beta} : \mathbb{F}_2^m \to \mathbb{F}_2^n$ telle que $f_{\alpha,\beta} \stackrel{déf.}{=} \sigma_\beta \circ (f \circ \sigma_\alpha \oplus f)$ *i.e.* $x \mapsto f(x \oplus \alpha) \oplus f(x) \oplus \beta$ prend au plus deux fois la valeurs $0_{\mathbb{F}_2^n}$.

[5] L'isomorphisme Φ_B est définie par la formule (4.3) p. 47.

[6] Il semblerait ainsi que de très récents travaux de Langevin et Leander permettent d'identifier la duale de cette fonction.

Puisque dans le cas général $\mathsf{P}_f \geq \frac{1}{2^n}$, les fonctions presque parfaitement non linéaires n'existent que si $\frac{1}{2^n} \leq \frac{1}{2^{m-1}} \Leftrightarrow \frac{2^m}{2^n} \leq \frac{2^m}{2^{m-1}} \Leftrightarrow 2^{m-n} \leq 2 \Leftrightarrow (m = n)$ ou $(m \leq n)$. Le cas où $(m, n) = (2, 1)$ étant trivial, ces fonctions n'existent que si $m \leq n$. Dans ce cas, les fonctions optimalement résistantes à la cryptanalyse différentielle sont donc les fonctions presque parfaitement non linéaires.

Par ailleurs Chabaud et Vaudenay, dans leur publication [CV94], ont formulé le résultat - que l'on expose ci-dessous en admettant sa démonstration - conduisant à la définition des fonctions presque courbes *i.e.* les fonctions optimalement résistantes à la cryptanalyse linéaire.

Théorème 5.8. [CV94] *Pour toute fonction $f : \mathbb{F}_2^m \to \mathbb{F}_2^n$, on a*

$$\mathsf{R}_f \geq \frac{1}{2}\left(3 \times 2^m - 2 - 2\frac{(2^m - 1)(2^{m-1} - 1)}{2^n - 1}\right)^{\frac{1}{2}} .$$

Lorsque cette borne est atteinte, on dit que la fonction f est presque courbe. *De plus, une fonction presque courbe est également presque parfaitement non linéaire.*

Ainsi une fonction presque courbe, offrant la plus grande résistance possible à l'attaque linéaire, assure par la même occasion une résistance optimale face à la cryptanalyse différentielle. Cependant la réciproque n'est pas vraie, contrairement au cas où $m \geq 2n$, m pair.

On peut remarquer que pour les fonctions presque courbes, la fonction k_f prend au plus trois différentes valeurs dans $\{0, \pm\mathsf{R}_f\}$. Ceci est comparable au cas des fonctions courbes pour lesquelles $\forall(\alpha, \beta) \in \mathbb{F}_2^m \times (\mathbb{F}_2^n)^*$, $k_f(\alpha, \beta) = \pm\mathsf{R}_f$ avec $\mathsf{R}_f = 2^{\frac{m}{2}-1}$.

La caractérisation des fonctions presque courbes dans le cas où les fonctions courbes n'existent pas est donnée par le théorème suivant, une nouvelle fois sans sa démonstration :

Théorème 5.9. [CV94] *Soit une fonction $f : \mathbb{F}_2^m \to \mathbb{F}_2^n$ telle que f soit presque courbe sans être courbe, alors $m = n$ et m est impair. Dans ce cas on a de plus :*

$$\mathsf{R}_f = \frac{1}{2}2^{\frac{m+1}{2}} .$$

Ainsi pour une fonction presque courbe $f : \mathbb{F}_2^m \to \mathbb{F}_2^m$, on a pour tout $(\alpha, \beta) \in \mathbb{F}_2^m \times \mathbb{F}_2^{m\,*}$, $(\widehat{\chi^1_{\mathbb{F}_2} \circ l_\beta \circ f})(\alpha) \in \{0, \pm 2^{\frac{m+1}{2}}\}$.

Exemple 5.1.

1. Soient m un entier impair et k un entier tel que $1 < k < m$, premier avec m. Soit

$$\begin{array}{rccc} \pi^{(2^k+1)} : & \mathbb{F}_{2^m} & \to & \mathbb{F}_{2^m} \\ & x & \mapsto & x^{2^k+1} . \end{array}$$

   Alors $\pi^{(2^k+1)}$ est une permutation presque courbe [Nyb94] ;

2. Soit $\boldsymbol{\sigma}_{inv}^{\mathbb{F}_{2^m}^*}$ l'involution de $\mathbb{F}_{2^m}^*$ définie par

$$\begin{array}{rccc} \boldsymbol{\sigma}_{inv}^{\mathbb{F}_{2^m}^*} : & \mathbb{F}_{2^m}^* & \to & \mathbb{F}_{2^m}^* \\ & x & \mapsto & x^{-1} . \end{array}$$

   Soit $\boldsymbol{\sigma}_{inv} : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ définie par $\boldsymbol{\sigma}_{inv}|_{\mathbb{F}_{2^m}^*} \overset{déf.}{=} \boldsymbol{\sigma}_{inv}^{\mathbb{F}_{2^m}^*}$ et $\boldsymbol{\sigma}_{inv}(0_{\mathbb{F}_{2^m}}) \overset{déf.}{=} 0_{\mathbb{F}_{2^m}}$, c'est-à-dire

$$x \mapsto \boldsymbol{\sigma}_{inv}(x) = \begin{cases} x^{-1} & \text{si } x \in \mathbb{F}_{2^m}^* , \\ 0_{\mathbb{F}_{2^m}} & \text{si } x = 0_{\mathbb{F}_{2^m}} . \end{cases}$$

TAB. 5.1 – Fonctions puissances presque parfaitement non linéaires $f^{(n)}$ sur $\mathbb{F}_{2^m}$, m impair

Nom	Puissance n	Condition(s)	Références
Inverse	-1		[LW87, LW90, BD94]
Gold	2^k+1	$pgcd(k,m)=1,\ 1\leq k\leq m-1$	[Nyb94]
Kasami	$2^{2k}-2^k+1$	$pgcd(k,m)=1,\ 2\leq k\leq m-1$	[Dob99b]
Welch	$2^{\frac{m-1}{2}}+3$		[Dob99a]
Niho	$2^{2k}+2^k-1$	$4k+1\equiv 0 \pmod m$	[Dob99a]
Dobbertin	$2^{\frac{4m}{5}}+2^{\frac{3m}{5}}+2^{\frac{2m}{5}}+2^{\frac{m}{5}}-1$	5 divise m	[Dob99b]

Alors $\boldsymbol{\sigma}_{inv}$ est une permutation (et même une involution). De plus si m est impair, $\boldsymbol{\sigma}_{inv}$ est presque parfaitement non linéaire [Nyb94]. Cependant elle n'est pas presque courbe (c'est une conséquence de [LW90]).

5.5.3 Les fonctions puissances

Une classe intéressante et très largement considérée de fonctions pour lesquelles ont étudie leur qualité d'être ou ne pas être[7] presque parfaitement non linéaire sont les fonctions puissances $f^{(n)} : x \mapsto x^n$ dans un corps fini $\mathbb{F}_{2^m}$ (où l'on identifie $\mathbb{F}_2^m$ avec la structure d'espace vectoriel sous-jacente au corps).

Il a été conjecturé par Dobbertin dans [Dob99b] que toutes les fonctions puissances presque parfaitement non linéaires d'un corps $\mathbb{F}_{2^m}$ pour m impair, sont listées dans le tableau 5.1. Observons que les résultats donnés dans le tableau restent vrais pour tout autre représentant de la classe cyclotomique modulo 2^m-1 de la puissance n et pour leurs inverses.

5.5.4 Conclusion

Lorsque l'on est dans l'impossibilité d'atteindre les bornes établies pour la définition des fonctions parfaitement non linéaires et courbes, il est opportun d'instaurer de plus faibles extrema sous peine de voir les tentatives de résistance aux attaques linéaire et différentielle échouées.

Ainsi dans le cas où $m = n$ et m est impair ont été introduites des notions de non linéarité presque parfaite et de fonction presque courbe. Elles supportent ainsi les définitions de solidité optimale envers les cryptanalyses différentielle et linéaire. Dans ce cadre imparfait, il est judicieux de relever que contrairement aux notions idéales, précédemment exposées dans ce chapitre, nous ne disposons plus de l'équivalence entre les deux critères de solidité.

Dans les cas différents de « $m \geq 2n$ et m pair » ou « $m = n$ et m impair » il faut trouver d'autres bornes pour définir les résistances optimales ainsi que d'éventuels liens entre ces notions.

Par la suite nous n'abordons plus ces cas approchés puisque l'on ne décrit que les situations idéales.

5.6 Conclusion

Dans le cadre booléen, les fonctions parfaitement non linéaires, objets combinatoires, et les fonctions courbes, issues de la théorie de Fourier, définissent *in fine* la même notion. Ces deux

[7] Telle est la question.

approches, duales l'une de l'autre par la transformée de Fourier, fournissent ainsi un ensemble complémentaire et cohérent de caractérisations de leur concept sous-jacent.

Ce type d'objets est d'une incroyable rareté dans l'ensemble des fonctions booléennes. Aussi afin de mieux les appréhender, il est nécessaire d'une part de disposer d'un certain nombre de descriptions additionnelles mais aussi d'autre part, d'apprécier leur comportement vis-à-vis des autres fonctions.

Un peu à la manière des extrêmophiles, ces formes de vie fréquentant les milieux particulièrement hostiles, les fonctions courbes « vivent » aux frontières du monde des fonctions booléennes moyennes. Elles sont par exemples les plus éloignées possibles des fonctions affines et n'ont aucune structure linéaire non nulle. Et, par définition, leurs résistances aux attaques différentielle et linéaire sont maximales.

Ces solidités optimales et simultanées envers deux des cryptanalyses les plus efficaces en font ainsi l'un des sujets de prédilection des recherches en cryptographie. Au cours de ce chapitre nous avons pu mesurer l'engouement provoqué par ces fonctions simplement par le nombre important de résultats exposés les concernant.

Au même titre que le chapitre 4 constituait un corpus de connaissance sur les fonctions booléennes dans leur plus grande généralité, ce présent chapitre est conçu comme un tutoriel sur les fonctions parfaitement non linéaires et courbes dans le cas booléen. En effet nous y trouvons les définitions de ces notions, leurs caractérisations ainsi que quelques constructions explicites.

Le spectre de ce chapitre est large et reprend ainsi la plupart du savoir concernant ces fonctions booléennes. Au prochain chapitre nous abandonnons l'environnement booléen mais pas les concepts exposés ici. Leurs généralisations essentielles y sont en effet rapportées. L'objectif étant d'enrichir la compréhension de ces notions avant d'aborder les concepts novateurs qui constituent la seconde partie du manuscrit.

Chapitre 6

Généralisations aux cas non booléens

Aucune généralisation n'est
totalement vraie, même pas celle-ci.

Olliver Windell Holmes Jr.,
Lettre à William James

Sommaire

6.1 Introduction

Les fonctions booléennes parfaitement non linéaires sont ces fonctions dont la dérivée, suivant n'importe quelle direction non nulle, suit une distribution de valeurs uniforme. Les fonctions booléennes courbes, pour leur part, sont ces fonctions de spectre de Walsh constant en valeur absolue. Leur légitimité en tant qu'objets cryptographiques tient au fait qu'elles exhibent la meilleure résistance possible aux attaques différentielle et linéaire.

A première vue, ces notions paraissent distinctes. Mais, à regarder les choses de plus près, on ne décèle en fait aucune différence. En effet, il apparaît à un œil exercé que, loin d'être disjoints, les deux concepts sont intrinsèquement liés. La non linéarité parfaite est une propriété décrite dans un cadre combinatoire alors que l'analyse de Fourier est l'outil adéquat pour formuler la notion de fonction courbe. Cependant il s'agit de deux modèles différents d'une même théorie sous-jacente. La première notion a simplement été déplacée dans un autre contexte.

L'idée de « modèle » d'une théorie abstraite est issue des formidables développements de la recherche mathématique du XIX^{e}. A cette époque de nombreux problèmes fondamentaux qui avaient résisté jusqu'alors à tous les efforts des chercheurs furent résolus. On créa de nouveaux secteurs d'étude mathématique et, dans diverses branches, on établit de nouveaux fondements ou

l'on remania des anciens à l'aide de techniques d'analyse plus précises. En bref d'anciens concepts furent généralisés au sein de théories abstraites, apportant ainsi, en se détachant de l'intuition pour ne manipuler que des objets formels, la réponse à un certain nombre de questions.

Dans la mesure où nous incombe la tâche proprement mathématique d'étudier les relations de dépendance purement logiques entre assertions concernant la non linéarité parfaite et les fonctions courbes, il nous faut faire abstraction des connotations courantes des termes primitifs du contexte booléen, pour ne retenir que la signification qui leur est attachée dans un cadre formel plus général.

Sont ainsi exposées dans ce chapitre plusieurs généralisations des notions booléennes présentées au chapitre 5. L'idée directrice est de s'abstraire de l'influence de la structure de $\mathbb{F}_2$-espace vectoriel sur les concepts centraux de nos travaux que sont la non linéarité parfaite et les fonctions courbes de telle sorte que chaque assertion se voit donner une valeur vrai ou faux par rapport à ces nouveaux modèles. De surcroît nous nous attachons à établir des relations entre ces diverses généralisations.

Il n'est certainement pas aisé de reconnaître son chemin dans ce pays de rigoureuse abstraction, dépourvu de tout repère familier de l'univers booléen. Toutefois on est dédommagé de sa peine par la liberté et les perspectives nouvelles qu'elle nous donne et dont nous usons largement dans la deuxième partie de ce document.

Ce chapitre est implicitement divisé en deux parties. Dans la première, elle-même découpée en deux sections, est introduite la notion de groupe dual d'un groupe fini abélien, utilisée à la fois dans ce chapitre mais aussi dans la suite du manuscrit. Puis la transformée de Fourier étendue au cadre des groupes finis commutatifs est présentée. Ainsi cette première « partie » est consacrée aux idées fondamentales sur lesquelles certains de nos travaux se fondent. Nous abordons ensuite quatre des principales généralisations élaborées dans un univers non booléen. Chacune d'elles se voyant attribuer l'intégralité d'une section. Une fois n'est pas coutume, nous exposons de manière « décroissante » les diverses théories *i.e.* de la plus générale à la plus particulière. Ainsi nous débutons par le concept de non linéarité parfaite établi par Carlet et Ding dans le cadre des groupes finis abéliens. Suite à cela nous exposons la théorie de Logachev, Salnikov et Yashchenko se rapportant aux fonctions définies sur un groupe fini commutatif et à valeurs dans l'ensemble des nombres complexes de module 1. Quasiment d'un même niveau théorique, nous décrivons les versions de la non linéarité parfaite et des fonctions courbes dans le cadre, d'une part, des fonctions k-aires c'est-à-dire ces fonctions à valeurs dans l'anneau d'entiers $\mathbb{Z}_k$ et, d'autre part, des fonctions dans des corps finis. Il est d'ailleurs amusant d'observer que nous bouclons la boucle, ouverte dans le chapitre 5, en retournant momentanément, au moyen de la dernière généralisation exposée, dans un monde booléen.

6.2 Dual d'un groupe fini abélien

6.2.1 Introduction

Historiquement, afin de mieux comprendre la structure intime des groupes abstraits, les mathématiciens représentèrent leurs éléments comme des fonctions à valeurs dans le corps des complexes. Cette manière d'agir permet d'exploiter pleinement les très riches outils d'analyse de $\mathbb{C}$ et donne naissance au concept de dualité des groupes.

Les résultats exposés dans cette section sont donnés sans preuve. Le lecteur pourra consulter par exemple [Pey04] afin d'obtenir ces démonstrations.

Dans cette section les groupes sont la plupart du temps notés multiplicativement et on rappelle d'une part que l'élément neutre d'un groupe G est désigné par « e_G » lorsqu'il ne dispose de dénomination *ad hoc* et d'autre part que $G^* \stackrel{déf.}{=} G \setminus \{e_G\}$.

6.2.2 Définitions et propriétés

Définition 6.1. Soit un G groupe fini. Un *caractère* χ de G est un homomorphisme de groupes de G dans le groupe multiplicatif $\mathbb{C}^*$. On note « $\widehat{G}$ » l'ensemble des caractères, que l'on appelle *dual* de G.

L'ensemble $\widehat{G}$ est en fait un groupe pour la multiplication terme à terme des applications définie, on le rappelle ici pour des caractères, comme suit :

$$\forall(\chi_1,\chi_2)\in\widehat{G}^2,\ \chi_1.\chi_2 : x\in G\mapsto \chi_1(x)\chi_2(x)\in\mathbb{C}^*\ .$$

Proposition 6.1. [Pey04] *Soit G un groupe fini, noté multiplicativement, de cardinal $m \stackrel{déf.}{=} |G|$. Les éléments de $\widehat{G}$ sont en fait les homomorphismes de groupes de G dans le groupe des racines $m^{ièmes}$ de l'unité dans $\mathbb{C}$:*

$$\mathbb{U}_m \stackrel{déf.}{=} \{\mathsf{e}^{\frac{2\imath k\pi}{m}}\in\mathbb{C}|0\leq k<m\}\ .$$

En particulier,

$$\forall\chi\in\widehat{G},\ \forall x\in G,\ |\chi(x)|=1,\ \chi(x^{-1})=\chi(x)^{-1}=\overline{\chi(x)}\ \textit{et}\ \chi(e_G)=1\ .$$

Remarque 6.1.

1. Il découle de la proposition précédente que $\widehat{G}$ est un groupe fini abélien (puisque la multiplication est commutative) ;

2. Le groupe $\mathbb{U}_m$ est un groupe cyclique d'ordre m. Un générateur de ce groupe s'appelle une *racine primitive $m^{ième}$* de l'unité dans $\mathbb{C}$;

3. On note « ω_m » la racine primitive $m^{ième}$ de l'unité dans $\mathbb{C}$ telle que

$$\omega_m \stackrel{déf.}{=} \mathsf{e}^{\frac{2\imath\pi}{m}}\ .$$

Intéressons-nous maintenant au dual d'un groupe cyclique.

Proposition 6.2. [Pey04] *Soit $G=\{e_G,x_0,x_0^2,\ldots,x_0^{m-1}\}$ un groupe cyclique (noté multiplicativement) d'ordre m et de générateur x_0. Soit ω une racine primitive $m^{ième}$ de l'unité dans $\mathbb{C}$. Les éléments de $\widehat{G}$ sont de la forme, pour $j\in\{0,\ldots,m-1\}$,*

$$\chi_j : \left\{\begin{array}{lcl} G & \to & \mathbb{C}^* \\ x=x_0^k & \mapsto & (\omega^j)^k. \end{array}\right.$$

En particulier, G et $\widehat{G}$ sont des groupes isomorphes.

On appelle *exposant* d'un groupe fini abélien G, que l'on note « $exp(G)$ », le maximum des ordres des éléments de G (c'est le cardinal de G s'il est cyclique).

En remarquant que si G et H sont deux groupes finis commutatifs alors $\widehat{G} \times \widehat{H}$ et $\widehat{G \times H}$ sont isomorphes via l'application[1]

$$\begin{array}{rccc} \Phi : & \widehat{G} \times \widehat{H} & \to & \widehat{G \times H} \\ & (\chi_1, \chi_2) & \mapsto & \chi_1 \otimes \chi_2 \ . \end{array}$$

On déduit de la décomposition classique d'un groupe fini commutatif en produit direct de groupes cycliques que, premièrement les caractères d'un tel groupe G sont à valeurs dans $\mathbb{U}_{exp\,(G)}$ et deuxièmement, le résultat important suivant.

Théorème 6.1 (Théorème d'isomorphisme). [Pey04] *Soit G un groupe fini commutatif. Alors $\widehat{G}$ est isomorphe à G. En particulier $|\widehat{G}| = |G|$.*

Soit G un groupe fini abélien, noté multiplicativement, et $\alpha \in G$. On note « χ_G^α » l'image de α par un isomorphisme (de groupes) de G dans $\widehat{G}$. En particulier $\chi_G^{e_G}$ est le *caractère trivial* de G *i.e.* il est égal à $\mathbf{1}_G$ la fonction constante égale à 1. De plus on a $\chi_G^{\alpha^{-1}} = (\chi_G^\alpha)^{-1} = \overline{\chi_G^\alpha}$.

Dans la suite et sans le préciser, dès que l'on introduit un groupe fini commutatif dans le contexte, on suppose systématiquement qu'un isomorphisme vers son groupe dual est fixé et on manipule toujours et sans exception les caractères via cet isomorphisme.

6.2.3 Exemples de caractères

Caractères des espaces vectoriels sur un corps fini

Les caractères de $\mathbb{F}_2$ sont donnés par $\chi_{\mathbb{F}_2}^0 = \mathbf{1}_{\mathbb{F}_2}$ et $\chi_{\mathbb{F}_2}^1$ que l'on connaît déjà.

Les caractères de $\mathbb{F}_2^m$ sont définis via le produit scalaire canonique de $\mathbb{F}_2^m$. Soit $\alpha \in \mathbb{F}_2^m$ alors :

$$\begin{array}{rccc} \chi_{\mathbb{F}_2^m}^\alpha : & \mathbb{F}_2^m & \to & \{\pm 1\} \\ & x & \mapsto & (-1)^{\alpha.x} \ . \end{array}$$

En particulier on a

$$\chi_{\mathbb{F}_2^m}^\alpha = \chi_{\mathbb{F}_2}^1 \circ l_\alpha \ .$$

Plus généralement pour p un entier premier, les caractères de $\mathbb{F}_p^m$ sont définis comme suit. Pour $\alpha \in \mathbb{F}_p^m$:

$$\begin{array}{rccc} \chi_{\mathbb{F}_p^m}^\alpha : & \mathbb{F}_p^m & \to & \mathbb{U}_p \\ & x & \mapsto & \omega_p^{\alpha.x} \ . \end{array}$$

où l'on sait que « . » désigne le produit scalaire naturel de $\mathbb{F}_p^m$.

Caractères additifs des corps finis

On rappelle la définition de la *trace*[2] *absolue* dans le cas d'un corps de caractéristique p :

$$\begin{array}{rccc} tr : & \mathbb{F}_{p^m} & \to & \mathbb{F}_p \\ & x & \mapsto & x + x^p + \ldots + x^{p^{m-1}} \ . \end{array}$$

Il s'agit d'une application linéaire de $\mathbb{F}_p$-espaces vectoriels. L'application

$$(x, y) \in \mathbb{F}_{p^m}^2 \mapsto tr(xy) \in \mathbb{F}_p$$

[1] Voir la définition 5.6 p. 83 du produit tensoriel $\otimes$.

[2] Nous l'avons déjà définie dans le cas de corps finis de caractéristique 2 au chapitre 4 p. 52

définit un produit scalaire. Le caractère du groupe additif de $\mathbb{F}_{p^m}$, extension finie de degré m du corps premier $\mathbb{F}_p$, correspondant à $\alpha \in \mathbb{F}_{p^m}$ est défini par

$$\begin{array}{rccc} \chi^{\alpha}_{\mathbb{F}_{p^m}} : & \mathbb{F}_{p^m} & \to & \mathbb{U}_p \\ & x & \mapsto & \omega_p^{tr(\alpha x)} \end{array} .$$

Les caractères de cette forme sont appelés les *caractères additifs* de $\mathbb{F}_{p^m}$.

Caractères d'un anneau d'entiers

Les caractères du groupe additif sous-jacent à l'anneau $\mathbb{Z}_k$ peuvent être représentés par

$$\begin{array}{rccc} \chi^{\alpha}_{\mathbb{Z}_k} : & \mathbb{Z}_k & \to & \mathbb{U}_k \\ & x & \mapsto & \omega_k^{\alpha x} \end{array}$$

quand α parcourt[3] $\mathbb{Z}_k$.

Les caractères du (groupe sous-jacent au) module $\mathbb{Z}_k^m$ peuvent quant à eux se représenter par

$$\begin{array}{rccc} \chi^{\alpha}_{\mathbb{Z}_k^m} : & \mathbb{Z}_k^m & \to & \mathbb{U}_k \\ & x & \mapsto & \omega_k^{\alpha.x} \end{array}$$

lorsque $\alpha \in \mathbb{Z}_k^m$ et où cette fois-ci « . » dénote le produit scalaire usuel du module $\mathbb{Z}_k^m$.

6.2.4 Propriétés d'orthogonalité des caractères

Voici quelques résultats importants pour la suite. Les preuves sont admises.

Lemme 6.1. [Pey04] *Soit G un groupe fini abélien. Pour tout $x \in G$ on a*

$$\sum_{\alpha \in G} \chi^{\alpha}_G(x) = \begin{cases} 0 & si\ x \in G^* \ , \\ |G| & si\ x = e_G \ . \end{cases} \tag{6.1}$$

Lemme 6.2. [Pey04] *Soit G un groupe fini abélien. Pour tout $\alpha \in G$, on a*

$$\sum_{x \in G} \chi^{\alpha}_G(x) = \begin{cases} 0 & si\ \alpha \in G^* \ , \\ |G| & si\ \alpha = e_G \ . \end{cases} \tag{6.2}$$

Pour G un groupe fini commutatif, munissons le $\mathbb{C}$-espace vectoriel $\mathbb{C}^G$ du produit scalaire (normalisé) hermitien :

$$\forall (\varphi, \psi) \in (\mathbb{C}^G)^2,\ \langle \varphi, \psi \rangle \stackrel{déf.}{=} \frac{1}{|G|} \sum_{x \in G} \varphi(x) \overline{\psi(x)} \ .$$

Proposition 6.3 (Orthogonalité des caractères). [Pey04] *Soit G un groupe fini abélien. Alors $\widehat{G}$ est une base orthonormale de $\mathbb{C}^G$. En particulier on a :*

$$\forall (\alpha_1, \alpha_2) \in G^2,\ \langle \chi^{\alpha_1}_G, \chi^{\alpha_2}_G \rangle = \begin{cases} 0 & si\ \alpha_1 \neq \alpha_2 \ , \\ 1 & si\ \alpha_1 = \alpha_2 \ . \end{cases}$$

Cette proposition indique en particulier que l'on peut décomposer toute fonction de $\mathbb{C}^G$ dans la base formée des caractères de G. Ceci nous amène à considérer la transformée de Fourier définie sur G.

[3] Ces caractères permettent d'établir une correspondance entre G et $\widehat{G}$ dans le cas général. En effet, soit G un groupe abélien fini. Alors on sait qu'il existe des entiers strictement positifs $n_1, \ldots, n_m$ tels que pour tout $k \in \{1, \ldots, m-1\}$, n_k divise n_{k+1} et tels que G soit isomorphe au produit direct $\mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_m}$. Soit $\Phi : G \to \mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_m}$ un tel isomorphisme de groupes. Il s'ensuit que les caractères de G peuvent être représentés pour $\alpha \in G$ par $\chi^{\alpha}_G : x \mapsto \prod_{k=1}^{m} \mathsf{e}^{\frac{2\imath\pi\Phi_k(\alpha)\Phi_k(x)}{n_k}}$. On remarque de plus que $\forall (\alpha, x) \in G^2$, $\chi^{\alpha}_G(x) = \chi^{x}_G(\alpha)$.

6.3 Transformée de Fourier sur un groupe fini abélien

Dans cette section, nous admettons les démonstrations des différents résultats énoncés.

Soit G un groupe fini abélien noté multiplicativement. Soit $\varphi : G \to \mathbb{C}$. Puisque l'on peut décomposer φ sur la base formée des caractères de G, on a :

$$\varphi = \sum_{\alpha \in G} n_\alpha \chi_G^\alpha \ .$$

Posons pour $\alpha \in G$, $\widehat{\varphi}(\alpha) \stackrel{déf.}{=} |G| \langle \varphi, \overline{\chi_G^\alpha} \rangle = \sum_{x \in G} \varphi(x) \chi_G^\alpha(x)$. On a alors

$$\widehat{\varphi}(\alpha) = |G| \sum_{\alpha' \in G} n_{\alpha'} \langle \chi_G^{\alpha'}, \overline{\chi_G^\alpha} \rangle = |G| n_{\alpha^{-1}}$$

et donc $\varphi = \dfrac{1}{|G|} \sum_{\alpha \in G} \widehat{\varphi}(\alpha^{-1}) \chi_G^\alpha$, soit encore

$$\varphi = \frac{1}{|G|} \sum_{\alpha \in G} \widehat{\varphi}(\alpha) \overline{\chi_G^\alpha} \ .$$

Définition 6.2. Soit G un groupe fini commutatif. La transformée de Fourier de la fonction $\varphi : G \to \mathbb{C}$ est la fonction $\widehat{\varphi} : G \to \mathbb{C}$ définie pour $\alpha \in G$ par :

$$\widehat{\varphi}(\alpha) = \sum_{x \in G} \varphi(x) \chi_G^\alpha(x) \ .$$

Remarque 6.2. On s'aperçoit facilement du fait que la transformée de Fourier définie au chapitre 4 n'est qu'une instance particulière de la transformée décrite ici.

Théorème 6.2. [Pey04] *Soit G un groupe fini commutatif. L'application $\Phi_F : \mathbb{C}^G \to \mathbb{C}^G$ qui associe à une fonction φ sa transformée de Fourier est un isomorphisme[4] d'espaces vectoriels.*

Remarquons que l'on a pour $\varphi \in \mathbb{C}^G$ et $\alpha \in G$,
$\widehat{\widehat{\varphi}}(\alpha) = |G| \langle \widehat{\varphi}, \overline{\chi_G^\alpha} \rangle = \dfrac{|G|}{|G|} \sum_{x \in G} \widehat{\varphi}(x) \chi_G^\alpha(x) = \sum_{x \in G} \widehat{\varphi}(x) \overline{\chi_G^{\alpha^{-1}}(x)} = |G| \varphi(\alpha^{-1})$ (G est ici noté multiplicativement[5]). L'isomorphisme inverse de la transformée de Fourier est donc donné par

$$\Phi_F^{-1}(\varphi) = \frac{1}{|G|} \Phi_F(\varphi \circ \boldsymbol{\sigma}_{inv}^G) \ , \tag{6.3}$$

où $\boldsymbol{\sigma}_{inv}^G : G \to G$ est l'involution telle que $\boldsymbol{\sigma}_{inv}^G(x) \stackrel{déf.}{=} x^{-1}$ pour tout $x \in G$ (nous l'avons déjà vue au chapitre 5 dans le deuxième point de l'exemple 5.1 dans le cas particulier où G est le groupe multiplicatif $\mathbb{F}_{2^m}^*$). Nous venons de (re-)démontrer le résultat suivant.

Proposition 6.4 (Formule d'inversion). [Pey04] *Soit G un groupe fini commutatif. Pour $\varphi \in \mathbb{C}^G$, on a la formule d'inversion*

$$\varphi = \frac{1}{|G|} \sum_{\alpha \in G} \widehat{\varphi}(\alpha) \overline{\chi_G^\alpha} \ .$$

[4] En toute rigueur, Φ_F est à valeur dans $\mathbb{C}^{\widehat{G}}$ mais puisque G est ici un groupe fini abélien, G et $\widehat{G}$ sont isomorphes.

[5] Nous avons ici implicitement utilisé le fait que $\forall (\alpha, x) \in G^2$, $\chi_G^\alpha(x) = \chi_G^x(\alpha)$.

Proposition 6.5. [Pey04] *Soit G un groupe fini commutatif. Pour $(\varphi, \psi) \in (\mathbb{C}^G)^2$ on a la formule suivante :*

$$\sum_{x\in G} \varphi(x)\overline{\psi(x)} = \frac{1}{|G|}\sum_{\alpha\in G} \widehat{\varphi}(\alpha)\overline{\widehat{\psi}(\alpha)} \text{ (formule de Plancherel).}$$

De plus en posant $\varphi = \psi$ on obtient la formule :

$$\sum_{x\in G} |\varphi(x)|^2 = \frac{1}{|G|}\sum_{\alpha\in G} |\widehat{\varphi}(\alpha)|^2 \text{ (relation de Parseval).} \tag{6.4}$$

En particulier si φ est à valeurs dans $\mathbb{U} \overset{déf.}{=} \{\mathtt{z} \in \mathbb{C} \mid |\mathtt{z}| = 1\}$, on a par application de la relation de Parseval :

$$\sum_{\alpha\in G} |\widehat{\varphi}(\alpha)|^2 = |G|^2 \ . \tag{6.5}$$

D'autres propriétés de la transformée de Fourier restent identiques au cas booléen. Elle trivialise par exemple le produit de convolution des fonctions de $\mathbb{C}^G$.

Définition 6.3. Soit G un groupe fini commutatif noté multiplicativement. Pour $(\varphi, \psi) \in (\mathbb{C}^G)^2$ le *produit de convolution* $\varphi * \psi$ est donné, pour $\alpha \in G$, par :

$$(\varphi * \psi)(\alpha) \overset{déf.}{=} \sum_{\substack{(x,y)\in G^2 \\ xy=\alpha}} \varphi(x)\psi(y) = \sum_{x\in G} \varphi(x)\psi(x^{-1}\alpha) \ .$$

Proposition 6.6. [Pey04] *Soit G un groupe fini commutatif. Le produit de convolution est commutatif, associatif et l'application $(\varphi, \psi) \mapsto \varphi * \psi$ est bilinéaire. On munit ainsi l'espace vectoriel $\mathbb{C}^G$ d'une structure d'algèbre notée « $(\mathbb{C}^G, *)$ ».*

Pour G un groupe fini commutatif, notons par le symbole « . » le produit terme à terme des éléments de $\mathbb{C}^G$ et « $(\mathbb{C}^G, .)$ » l'algèbre correspondante.

Théorème 6.3 (Trivialisation du produit de convolution). [Pey04] *Soit G un groupe fini commutatif. Pour $(\varphi, \psi) \in (\mathbb{C}^G)^2$ on a*

$$\widehat{\varphi * \psi} = \widehat{\varphi}.\widehat{\psi} \text{ et } \widehat{\varphi.\psi} = \frac{1}{|G|}\widehat{\varphi} * \widehat{\psi} \ .$$

La transformée de Fourier Φ_F est donc un isomorphisme d'algèbres de $(\mathbb{C}^G, *)$ dans $(\mathbb{C}^G, .)$.

Enfin on a un lemme important que nous démontrons puisqu'il est à la fois peu connu et très opportun.

Lemme 6.3. [CD04] *Soit G un groupe fini commutatif. Soit $\varphi \in \mathbb{C}^G$.*

1. *φ vérifie $\varphi(x) = 0$ pour chaque $x \in G^*$ si et seulement si $\widehat{\varphi}$ est constante.*
2. *$\widehat{\varphi}$ vérifie $\widehat{\varphi}(\alpha) = 0$ pour chaque $\alpha \in G^*$ si et seulement si φ est constante.*

Preuve.

1. – Supposons que φ vérifie $\varphi(x) = 0$ pour chaque $x \in G^*$. Par définition de la transformée de Fourier, on obtient $\forall \alpha \in G$, $\widehat{\varphi}(\alpha) = \varphi(e_G)$.
   – Supposons que $\widehat{\varphi}$ soit constante. Notons « k » cette constante. D'après la formule d'inversion, on a pour $x \in G$,

$$\varphi(x) = \frac{k}{|G|}\sum_{\alpha\in G} \overline{\chi_G^\alpha(x)} = 0 \text{ si } x \neq e_G \text{ (lemme 6.1).}$$

2. – Supposons que $\widehat{\varphi}$ vérifie $\widehat{\varphi}(\alpha) = 0$ pour chaque $\alpha \in G^*$. En utilisant la formule d'inversion, on obtient pour tout $x \in G$, $\varphi(x) = \frac{1}{|G|}\widehat{\varphi}(e_G)$.
   – Supposons que φ soit constante. Notons « k » cette constante. Par définition de la transformée de Fourier, on a $\widehat{\varphi}(\alpha) = k \sum_{x \in G} \chi_G^\alpha(x) = 0$ si $\alpha \neq e_G$ (lemme 6.2).

□

6.4 Fonctions parfaitement non linéaires au sens de Carlet et Ding

Dans [CD04] Carlet et Ding généralisent la notion classique de non linéarité parfaite au cas des groupes finis commutatifs. Nous exposons leurs travaux en respectant une trame conforme à celle suivie lors de la présentation de la non linéarité parfaite dans le cadre booléen effectuée au chapitre 5.

Certains résultats se trouvent transportés sans modification dans le nouveau contexte. Toutefois le passage des $\mathbb{F}_2$-espaces vectoriels aux groupes finis abéliens ne s'effectue pas sans perte. En effet, même si, de manière analogue au cas classique, on dispose toujours d'une caractérisation de la non linéarité parfaite au travers de la transformée de Fourier, il n'y a plus l'équivalence *stricto sensu* entre les notions de non linéarité parfaite et de fonction courbe.

Pour cette section dans son intégralité sont donnés deux groupes finis abéliens G_1 et G_2, tous deux notés additivement, les lois étant désignées par le même symbole « + » (l'ambiguïté étant levée par le contexte). On rappelle par ailleurs (voir chapitre 3) que pour $(y_1, y_2) \in G_2^2$, la notation « $y_1 - y_2$ » est une abréviation pour l'expression « $y_1 + (-y_2)$ », $-y_2$ étant bien entendu l'inverse dans G_2 de y_2. Les définitions et autres résultats restent évidemment valides si les lois + sont remplacées par n'importe quelle loi de composition interne de groupe fini commutatif.

On suppose par ailleurs que l'ensemble sous-jacent à la structure de groupe de G_1 est muni de la loi de probabilité uniforme notée « $\Pr^{(G_1)}$ ».

Débutons simplement par du vocabulaire.
Une fonction $\lambda : G_1 \to G_2$ est *linéaire* si λ est un homomorphisme de groupes de G_1 dans G_2.
Une fonction $\delta : G_1 \to G_2$ est *affine* s'il existe $\lambda : G_1 \to G_2$ linéaire et $\beta \in G_2$ tel que $\forall x \in G_1$, $\delta(x) = \lambda(x) + \beta$, en d'autre termes, $\delta = \sigma_\beta \circ \lambda$ où naturellement « σ_β » représente la translation par β sur G_2.

L'objectif est donc ici de définir une mesure de non coïncidence d'une fonction donnée avec les fonctions affines.

Définition 6.4. Soit $f : G_1 \to G_2$. La *dérivée*[6] de f suivant la direction $\alpha \in G_1$ est définie par

$$\begin{array}{rccc} d_\alpha f : & G_1 & \to & G_2 \\ & x & \mapsto & f(x+\alpha) - f(x) \ . \end{array}$$

Par analogie avec le cas classique des fonctions booléennes parfaitement non linéaires, est choisie, comme mesure de non linéarité d'une fonction $f \in G_2^{G_1}$, la grandeur

$$\mathsf{P}_f \stackrel{déf.}{=} \max_{\alpha \in G_1^*} \max_{\beta \in G_2} \Pr_{d_\alpha f}^{(G_1)}(\{\beta\}) = \frac{1}{|G_1|} \max_{\alpha \in G_1^*} \max_{\beta \in G_2} |\{x \in G_1 | d_\alpha f(x) = \beta\}| \ .$$

[6] Pour $f \in G_2^{G_1}$, l'application $\partial f : G_1 \to G_2^{G_1}$ qui a $\alpha \in G_1$ associe $d_\alpha f$ est un 1-cobord.

Plus petite est la valeur de la probabilité P_f, meilleure est la non linéarité de f. En particulier si f est linéaire ou affine, on a $\mathsf{P}_f = 1$.

Notons[7] que pour chacun des $\alpha \in G_1$, l'ensemble de parties $\{\{x \in G_1 | d_\alpha f(x) = \beta\} \subset G_1 |\ \beta \in G_2\}$ constitue une partition de G_1. Nous obtenons ainsi le lemme suivant.

Lemme 6.4. [CD04] *Pour chaque $\alpha \in G_1$, on a*

$$|G_1| = \sum_{\beta \in G_2} |\{x \in G_1 | d_\alpha f(x) = \beta\}| \ .$$

Le maximum d'une variable aléatoire numérique à un nombre fini de valeurs et définie sur un espace probabilisé muni de l'équiprobabilité est supérieur ou égal à son espérance mathématique. Il s'ensuit que pour chaque $\alpha \in G_1$,

$$\max_{\beta \in G_2} \frac{1}{|G_1|} |\{x \in G_1 | d_\alpha f(x) = \beta\}| \geq \frac{1}{|G_2|} \ .$$

Alors

$$\mathsf{P}_f \geq \frac{1}{|G_2|} \ . \tag{6.6}$$

Définition 6.5. Soit $f : G_1 \to G_2$. La fonction f est *parfaitement non linéaire (au sens de Carlet et Ding)*[8] si $\mathsf{P}_f = \dfrac{1}{|G_2|}$.

Puisque le maximum d'une variable aléatoire numérique prenant un nombre fini de valeurs et définie sur un espace probabilisé pourvu de la mesure de probabilité uniforme est égal à son espérance mathématique si et seulement si la variable aléatoire en question est constante, l'inégalité (6.6) est une égalité si et seulement si, pour tout $\beta \in G_2$ et tout $\alpha \in G_1^*$, la quantité $|\{x \in G_1 | d_\alpha f(x) = \beta\}|$ a la valeur $\dfrac{|G_1|}{|G_2|}$.

Définition 6.6. Soit (X, Y) un couple d'ensembles finis (non vides). Une fonction $f : X \to Y$ est *équilibrée* si la fonction

$$\begin{array}{rccc} \varphi_f : & Y & \to & \mathbb{N} \\ & y & \mapsto & |f^{-1}(\{y\})| \end{array}$$

est constante *i.e.* si pour tout $y \in Y$, $\varphi_f(y) = \dfrac{|X|}{|Y|}$.

On peut remarquer que la fontion φ_f a déjà été rencontrée au cours du chapitre 4 dans le contexte particulier des fonctions booléennes. La nouvelle définition des fonctions équilibrées remplace et annule celle exposée au chapitre 4.

Similairement au cas booléen, la notion de non linéarité parfaite dans le cadre des groupes finis abéliens s'exprime à l'aide de la notion d'équilibre appliquée aux dérivées d'une fonction.

Théorème 6.4. [CD04] *Une fonction $f : G_1 \to G_2$ est parfaitement non linéaire si et seulement si pour tout $\alpha \in G_1^*$, la dérivée $d_\alpha f$ est équilibrée.*

Preuve. D'après ce qui a été énoncé plus haut, le résultat est évident. □

[7] Nous reprenons ici un raisonnement déjà effectué dans le cas particulier de la définition de la non linéarité parfaite pour les fonctions booléennes.

[8] Connue sous le nom de *fonction planaire* en géométrie finie.

On s'intéresse maintenant à la caractérisation de la notion de non linéarité parfaite en termes de transformée de Fourier exposée par Carlet et Ding et qui généralise, d'un certain point de vue, l'équivalence entre la non linéarité parfaite et le concept de fonction courbe dans le cadre des fonctions booléennes.

Proposition 6.7. *Soit X un ensemble fini non vide et H un groupe fini commutatif. Soit $f : X \to H$. Alors f est équilibrée si et seulement si, pour chaque $\beta \in H^*$, nous avons*

$$\sum_{x \in X} (\chi_H^\beta \circ f)(x) = 0 \ .$$

Preuve. Pour $\beta \in H$ nous avons

$$\begin{aligned} \sum_{x \in X} (\chi_H^\beta \circ f)(x) &= \sum_{y \in H} |f^{-1}(\{y\})| \chi_H^\beta(y) \\ &= \sum_{y \in H} \varphi_f(y) \chi_H^\beta(y) \ . \end{aligned} \tag{6.7}$$

Ainsi si f est équilibrée et $\beta \neq e_H$ alors $\sum_{x \in X} (\chi_H^\beta \circ f)(x) = \frac{|X|}{|H|} \sum_{y \in H} \chi_H^\beta(y) = 0$ (d'après le lemme 6.2 p. 103).
Inversement si pour tout $\beta \in H^*$, $\sum_{x \in X} (\chi_H^\beta \circ f)(x) = 0$ alors d'après la relation (6.7), la fonction φ_f a la transformée de Fourier suivante

$$\beta \mapsto \begin{cases} 0 & \text{si } \beta \neq e_H \ , \\ |X| & \text{si } \beta = e_H \ . \end{cases}$$

D'après le lemme 6.3 p. 105, on en déduit que φ_f est constante. Cette constante ne peut être que $\frac{|X|}{|H|}$. □

Remarque 6.3. Si, dans la proposition précédente, on suppose que X est un groupe fini abélien G, alors $f : G \to H$ est équilibrée si et seulement si, pour chaque $\beta \in H^*$, nous avons

$$\widehat{\chi_H^\beta \circ f}(e_G) = 0 \ .$$

Lemme 6.5. [CD04] *Soit $f : G_1 \to G_2$. Pour $\beta \in G_2$ on définit*

$$\begin{aligned} AC_{f,\beta} : \ G_1 &\to \mathbb{C} \\ \alpha &\mapsto \widehat{\chi_{G_2}^\beta \circ d_\alpha f}(e_{G_1}) = \sum_{x \in G_1} \chi_{G_2}^\beta(d_\alpha f(x)) \ . \end{aligned}$$

Alors la transformée de Fourier de $AC_{f,\beta}$ vaut $|\widehat{\chi_{G_2}^\beta \circ f}|^2$.

Preuve. Soit $\alpha \in G_1$.

$$\begin{aligned}
\widehat{AC_{f,\beta}}(\alpha) &= \sum_{x\in G_1} AC_{f,\beta}(x)\chi^{\alpha}_{G_1}(x) \\
&= \sum_{x\in G_1} \widehat{\chi^{\beta}_{G_2} \circ d_x f(e_{G_1})}\chi^{\alpha}_{G_1}(x) \\
&= \sum_{x\in G_1}\sum_{y\in G_1} \chi^{\beta}_{G_2}(d_x f(y))\chi^{\alpha}_{G_1}(x) \\
&= \sum_{x\in G_1}\sum_{y\in G_1} \chi^{\beta}_{G_2}(f(x+y))\overline{\chi^{\beta}_{G_2}(f(y))}\chi^{\alpha}_{G_1}(x) \\
&= \sum_{x\in G_1}\sum_{y\in G_1} \chi^{\beta}_{G_2}(f(x+y))\overline{\chi^{\beta}_{G_2}(f(y))}\chi^{\alpha}_{G_1}(x+y)\overline{\chi^{\alpha}_{G_1}(y)} \\
&= (\widehat{\chi^{\beta}_{G_2} \circ f(\alpha)})\overline{(\widehat{\chi^{\beta}_{G_2} \circ f(\alpha)})} .
\end{aligned}$$

□

La caractérisation par la transformée de Fourier est finalement donnée par le théorème suivant.

Théorème 6.5. [CD04] *Soit une fonction $f : G_1 \to G_2$. Alors f est parfaitement non linéaire si et seulement si, pour chaque $\beta \in G_2^*$ et pour tout $\alpha \in G_1$,*

$$|\widehat{\chi^{\beta}_{G_2} \circ f(\alpha)}| = \sqrt{|G_1|} .$$

Preuve. D'après le théorème 6.4, f est parfaitement non linéaire si et seulement si pour tout $\alpha \in G_1^*$, $d_\alpha f$ est équilibrée. Ainsi d'après la proposition 6.7, f est parfaitement non linéaire si et seulement si pour tout $(\alpha,\beta) \in G_1^* \times G_2^*$, $\widehat{\chi^{\beta}_{G_2} \circ d_\alpha f(e_{G_1})} = AC_{f,\beta}(\alpha) = 0$. Par suite d'après le lemme 6.3 p. 105, f est parfaitement non linéaire si et seulement si pour tout $\beta \in G_2^*$, $AC_{f,\beta}$ a une transformée de Fourier constante. Cette constante est égale à $AC_{f,\beta}(e_{G_1})$ (voir la démonstration du lemme 6.3). Or $AC_{f,\beta}(e_{G_1}) = \widehat{\chi^{\beta}_{G_2} \circ d_{e_{G_1}} f(e_{G_1})} = \sum_{x\in G_1} \chi^{\beta}_{G_2}(e_{G_2}) = |G_1|$. En utilisant le lemme 6.5 on conclut cette preuve. □

En anticipant les résultats exposés dans la section 6.5, le théorème précédent indique que f est parfaitement non linéaire si et seulement si pour tout $\beta \in G_2^*$, $\chi^{\beta}_{G_2} \circ f$ est courbe au sens de Logachev, Salnikov et Yashchenko.

Une version moins forte du concept de fonction courbe peut être considérée. Soit $f : G_1 \to G_2$. La fonction f est dite *faiblement courbe* s'il existe $\beta \in G_2^*$ tel que pour tout $\alpha \in G_1$, $|\widehat{\chi^{\beta}_{G_2} \circ f(\alpha)}| = \sqrt{|G_1|}$. Dans ce cas l'équivalence entre non linéarité parfaite et la notion de fonction courbe n'est plus forcément assurée. Nous verrons par la suite des cas plus explicites pour cette perte d'équivalence.

6.5 Fonctions courbes au sens de Logachev, Salnikov et Yashchenko

Logachev, Salnikov et Yashchenko ont adapaté dans [LSY97] la notion de fonction courbe au cas général des fonctions définies sur un groupe fini abélien G quelconque et à valeurs dans l'ensemble $\mathbb{U}$ des nombres complexes de module 1. Le choix de $\mathbb{U}$, comme ensemble d'arrivée des fonctions étudiées, permet en l'occurrence de tirer partie de la formulation simplifiée de la relation de

Parseval dans ce cas particulier (voir l'égalité (6.5) p. 105).

Sont repris dans cette section un certain nombre de résultats de [LSY97].

Donnons-nous un groupe fini abélien G noté additivement et de loi de composition interne $+$.

Définition 6.7. Soit $\varphi : G \to \mathbb{U}$. La fonction φ est *courbe au sens de Logachev, Salnikov et Yashchenko* si pour tout $\alpha \in G$ on a

$$|\widehat{\varphi}(\alpha)| = \sqrt{|G|} \ .$$

Il s'agit donc d'une généralisation directe du concept de fonction courbe exposé au chapitre 5.

Notons, par analogie avec le cas classique, « $\mathcal{B}_G$ » l'ensemble des éléments de $\mathbb{U}^G$ qui sont courbes (au sens de Logachev, Salnikov et Yashchenko).

Certaines propriétés valables dans le cas des fonctions courbes booléennes le restent dans ce nouveau contexte.

Proposition 6.8. [LSY97] *Soit $\varphi : G \to \mathbb{U}$ une fonction courbe au sens de Logachev, Salnikov et Yashchenko. On définit*

$$\begin{array}{rccc} \tilde{\varphi}: & G & \to & \mathbb{U} \\ & \alpha & \mapsto & \dfrac{1}{\sqrt{|G|}}\widehat{\varphi}(\alpha) \ . \end{array}$$

Alors $\tilde{\varphi}$ est une fonction courbe (au sens de Logachev, Salnikov et Yashchenko) , appelée duale *de φ.*

Preuve. Puisque φ est courbe au sens de Logachev, Salnikov et Yashchenko, par définition, $\forall \alpha \in G$, $|\widehat{\varphi}(\alpha)| = \sqrt{|G|}$. Donc $\tilde{\varphi}$ est bien à valeurs dans $\mathbb{U}$.
Calculons sa transformée de Fourier pour $\alpha \in G$:

$$\begin{array}{rcl} \widehat{\tilde{\varphi}}(\alpha) & = & \dfrac{1}{\sqrt{|G|}}\widehat{\widehat{\varphi}}(\alpha) \\ & = & \dfrac{|G|}{\sqrt{|G|}}\varphi(-\alpha) \text{ (d'après l'égalité (6.3) p. 104)} \\ & = & \sqrt{|G|}\varphi(-\alpha) \end{array}$$

et donc $|\widehat{\tilde{\varphi}}(\alpha)| = \sqrt{|G|}$ (puisque φ est à valeurs dans $\mathbb{U}$). Ainsi $\tilde{\varphi}$ est courbe au sens de Logachev, Salnikov et Yashchenko. □

Il est possible de combiner, à l'aide du produit tensoriel (voir la définition 5.6 p. 83), des fonctions courbes pour en construire de nouvelles, exactement comme dans le cas traditionnel.

Proposition 6.9. *Soit (G_1, G_2) un couple de groupes finis commutatifs. Soit $(\varphi_1, \varphi_2) \in \mathcal{B}_{G_1} \times \mathcal{B}_{G_2}$. Alors la fonction $\varphi_1 \otimes \varphi_2 : G_1 \times G_2 \to \mathbb{U}$ appartient à $\mathcal{B}_{G_1 \times G_2}$.*

Preuve. La proposition est évidente sachant que les caractères de $G_1 \times G_2$ sont donnés par $\chi^{(\alpha,\beta)}_{G_1\times G_2} \stackrel{déf.}{=} \chi^{\alpha}_{G_1} \otimes \chi^{\beta}_{G_2}$ pour $(\alpha, \beta) \in G_1 \times G_2$. On a donc pour $(x, y) \in G_1 \times G_2$,

$$\begin{array}{rcl} \widehat{(\varphi_1 \otimes \varphi_2)}(\alpha,\beta) & = & \displaystyle\sum_{(x,y)\in G_1\times G_2} (\varphi_1 \otimes \varphi_2)(x,y)\chi^{(\alpha,\beta)}_{G_1\times G_2}(x,y) \\ & = & \displaystyle\sum_{(x,y)\in G_1\times G_2} \varphi_1(x)\chi^{\alpha}_{G_1}(x)\varphi_2(y)\chi^{\beta}_{G_2}(y) \\ & = & \displaystyle\sum_{x\in G_1} \varphi_1(x)\chi^{\alpha}_{G_1}(x) \sum_{y\in G_2} \varphi_2(y)\chi^{\beta}_{G_2}(y) \\ & = & \widehat{\varphi_1}(\alpha)\widehat{\varphi_2}(\beta) \ . \end{array}$$

La conclusion s'ensuit. □

Les auteurs de [LSY97] ont par ailleurs introduit une notion d'équilibre, nécessairement différente de celle présentée dans la section précédente puisque le groupe multiplicatif $\mathbb{U}$ n'est pas fini[9].

Définition 6.8. Soit $\varphi \in \mathbb{U}^G$. La fonction φ est dite *équilibrée au sens de Logachev, Salnikov et Yashchenko* si

$$\widehat{\varphi}(e_G) = \sum_{x \in G} \varphi(x) = 0 \ .$$

En d'autres termes une fonction de $\mathbb{U}^G$ est équilibrée au sens de Logachev, Salnikov et Yashchenko si sa décomposition dans la base des caractères de G ne contient pas le caractère trivial $\chi_G^{e_G}$.

Afin de caractériser le nouveau type de fonctions courbes à l'aide de ce concept de fonction équilibrée, comme dans le cas classique, on introduit aussi une notion convenable de dérivée. La *dérivée* de $\varphi : G \to \mathbb{U}$ dans la direction $\alpha \in G$ est naturellement définie comme la fonction

$$\begin{array}{rccc} d_\alpha\varphi : & G & \to & \mathbb{U} \\ & x & \mapsto & \varphi(\alpha + x)\overline{\varphi(x)} \ . \end{array}$$

Cette définition étend celle présentée dans la section 6.4 puisque, ainsi que cela a été signalé auparavant, $\mathbb{U}$ est un groupe infini (non dénombrable).
En utilisant les notions précédemment définies, on obtient la caractérisation des fonctions courbes suivante :

Théorème 6.6. [LSY97] *Soit $\varphi \in \mathbb{U}^G$. Alors*

$$\varphi \in \mathcal{B}_G \Leftrightarrow \forall \alpha \in G^*, \ d_\alpha\varphi \text{ est équilibrée au sens de Logachev, Salnikov et Yashchenko.}$$

Preuve. Définissons la version suivante de la fonction d'auto-corrélation

$$\begin{array}{rccc} AC_\varphi : & G & \to & \mathbb{C} \\ & \alpha & \mapsto & \widehat{d_\alpha\varphi}(e_G) \end{array}$$

et calculons sa transformée de Fourier pour $\alpha \in G$.

$$\begin{aligned} \widehat{AC_\varphi}(\alpha) &= \sum_{x \in G} AC_\varphi(x)\chi_G^\alpha(x) \\ &= \sum_{x \in G} \widehat{d_x\varphi}(e_G)\chi_G^\alpha(x) \\ &= \sum_{x \in G}\sum_{y \in G} d_x\varphi(y)\chi_G^\alpha(x) \\ &= \sum_{x \in G}\sum_{y \in G} \varphi(x+y)\overline{\varphi(y)}\chi_G^\alpha(x) \\ &= \sum_{x \in g}\sum_{y \in G} \varphi(x+y)\overline{\varphi(y)}\chi_G^\alpha(x+y)\overline{\chi_G^\alpha(y)} \\ &= \widehat{\varphi}(\alpha)\overline{\widehat{\varphi}(\alpha)} \\ &= |\widehat{\varphi}(\alpha)|^2 \ . \end{aligned}$$

On a donc

$$\begin{aligned} \varphi \in \mathcal{B}_G &\Leftrightarrow \forall \alpha \in G, \ |\widehat{\varphi}(\alpha)|^2 = |G| \text{ (par définition)} \\ &\Leftrightarrow \forall \alpha \in G, \ \widehat{AC_\varphi}(\alpha) = |G| \\ &\Leftrightarrow \forall \alpha \in G^*, \ AC_\varphi(\alpha) = 0 \text{ (lemme 6.3)} \\ &\Leftrightarrow \forall \alpha \in G^*, \ \widehat{d_\alpha\varphi}(e_G) = 0 \\ &\Leftrightarrow \forall \alpha \in G^*, \ d_\alpha\varphi \text{ est équilibrée au sens de Logachev, Salnikov et Yashchenko.} \end{aligned}$$

[9] L'ensemble $\mathbb{U}$ n'est même pas discret puisqu'il possède la puissance du continu.

C'est ce qu'il fallait démontrer. □

Observons au passage que si $\varphi \in \mathcal{B}_G$ alors pour tout $(\mathtt{z}, \chi) \in \mathbb{U} \times \widehat{G}$, la fonction $\mathtt{z}\chi.\varphi \in \mathbb{U}^G$ est courbe. En effet pour tout $(\alpha, x) \in G^2$, $d_\alpha(\mathtt{z}\chi.\varphi)(x) = d_\alpha(\mathtt{z}\chi(x)\varphi(x)) = \chi(\alpha)d_\alpha\varphi(x)$ et donc $\widehat{d_\alpha(\mathtt{z}\chi.\varphi)}(e_G) = \chi(\alpha)\sum_{x\in G} d_\alpha\varphi(x) = 0$ dès que $\alpha \neq e_G$ (en utilisant le théorème 6.6 puisque $\varphi \in \mathcal{B}_G$). Ce résultat est comparable au fait classique que si $f \in \mathcal{B}_m$ alors $\forall(\delta, \delta') \in GA(\mathbb{F}_2^m)\times R(1, m)$, $(f \circ \delta) \oplus \delta' \in \mathcal{B}_m$.

Cette notion de fonction courbe, au vue de sa définition et de certains des résultats exposés, semble relativement proche du concept classique. La différence, pouvant sembler légère mais riche de conséquences, est le fait de ne pas se limiter aux fonctions à valeurs dans un groupe particulier $\mathbb{U}_m$. Ce degré de liberté supplémentaire discrimine alors les deux notions de manière assez remarquable. Ainsi dans [Hou00] est démontré le résultat suivant (retranscrit ici sans sa preuve).

Théorème 6.7. [Hou00] *Quel que soit le groupe fini abélien G,*

$$\mathcal{B}_G \neq \emptyset \ .$$

Une conséquence immédiate de ce théorème est la constatation suivante. Alors que $\mathcal{B}_m = \emptyset$ dès que m est impair, il n'en est rien de $\mathcal{B}_{\mathbb{F}_2^m}$. Ainsi les deux notions bien que semblant similaires sont en réalité très largement différentes.

Le concept de fonction courbe au sens de Logachev, Salnikov et Yashchenko est moins fort que celui de fonction booléenne courbe. Moralement la nouvelle version est plus primitive et peut servir d'assise à la notion de non linéarité parfaite au sens de Carlet et de Ding au moyen du théorème 6.5.

6.6 Fonctions k-aires parfaitement non linéaires ou courbes

Une approche intermédiaire de la notion de non linéarité parfaite (ou fonction courbe) entre celle de Carlet et Ding (ou celle de Logachev, Salnikov et Yashchenko) dans le cadre des groupes finis commutatifs et celle du cas booléen consiste à considérer les fonctions définies et à valeurs dans certains modules $\mathbb{Z}_k^m$. Cette généralisation a été effectuée dans [KSW85] et [CK89]. Nous l'exposons dans l'actuel section. Dans un premier temps nous traitons le cas des fonctions à valeurs dans $\mathbb{Z}_k$ puis celui des fonctions « vectorielles » à valeurs dans $\mathbb{Z}_k^m$.

Rappelons avant toute chose quelques notations (voir le chapitre 3) et définitions très utiles ici.

Tout d'abord nous avons $\mathbb{Z}_k^* \overset{déf.}{=} \mathbb{Z}_k \setminus \{0\}$ et $\mathbb{Z}_k^{m*} \overset{déf.}{=} \mathbb{Z}_k^m \setminus \{0_{\mathbb{Z}_k^m}\}$ avec $0_{\mathbb{Z}_k^m} \overset{déf.}{=} (\underbrace{0, \ldots, 0}_{m\ fois})$.

En outre nous avons déjà observé (voir la sous-section 6.2.3) que les caractères du groupe additif sous-jacent à l'anneau $\mathbb{Z}_k$ sont donnés via un isomorphisme entre le groupe et son dual, pour $(\alpha, x) \in \mathbb{Z}_k^2$, par $\chi^\alpha_{\mathbb{Z}_k}(x) \overset{déf.}{=} \omega_k^{\alpha x}$ où ω_k est la racine primitive $k^{ième}$ de l'unité dans $\mathbb{C}$ telle que $\omega_k \overset{déf.}{=} \mathsf{e}^{\frac{2\imath\boldsymbol{\pi}}{k}}$ et l'expression « αx » désigne le produit de α et x dans $\mathbb{Z}_k$. Il en résulte que $\forall(\alpha, x) \in \mathbb{Z}_k^2$, $\chi^\alpha_{\mathbb{Z}_k}(x) = \chi^1_{\mathbb{Z}_k}(\alpha x)$ soit encore

$$\chi^\alpha_{\mathbb{Z}_k} = \chi^1_{\mathbb{Z}_k} \circ \tau_\alpha \tag{6.8}$$

où, comme indiqué au chapitre 3, τ_α est la translation multiplicative (modulo k) par α *i.e.*

$$\begin{array}{rccc} \tau_\alpha : & \mathbb{Z}_k & \to & \mathbb{Z}_k \\ & x & \mapsto & \alpha x \ . \end{array}$$

Les caractères du groupe additif sous-jacent au module $\mathbb{Z}_k^m$ sont quant à eux définis pour $\alpha \in \mathbb{Z}_k^m$:

$$\begin{array}{rccc} \chi^\alpha_{\mathbb{Z}_k^m} : & \mathbb{Z}_k^m & \to & \mathbb{Z}_k^m \\ & x & \mapsto & \omega_k^{\alpha.x} \ , \end{array}$$

le symbole « . » dénotant le produit scalaire usuel du module $\mathbb{Z}_k^m$. On a donc

$$\chi^\alpha_{\mathbb{Z}_k^m} = \chi^1_{\mathbb{Z}} \circ l_\alpha \tag{6.9}$$

avec $l_\alpha : \mathbb{Z}_k^m \to \mathbb{Z}_k$ la forme linéaire $x \mapsto \alpha.x$.

Dans ce contexte la transformée de Fourier d'une fonction $\varphi : \mathbb{Z}_k^m \to \mathbb{C}$ est ainsi définie pour $\alpha \in \mathbb{Z}_k^m$ par

$$\widehat{\varphi}(\alpha) = \sum_{x \in \mathbb{Z}_k^m} \varphi(x) \omega_k^{\alpha.x} \ .$$

De manière très analogue au cas booléen, on utilise une « transformée de Walsh » k-aire afin de définir les fonctions courbes.

Définition 6.9. Soit $f : \mathbb{Z}_k^m \to \mathbb{Z}_k$ (*i.e.* f est une fonction k-*aire*). La fonction f est k-*aire courbe*[10] si pour tout $\alpha \in \mathbb{Z}_k^m$, on a

$$|\widehat{\chi^1_{\mathbb{Z}_k} \circ f}(\alpha)| = k^{\frac{m}{2}} \ .$$

Une fonction f est donc k-aire courbe si et seulement si la fonction $\chi^1_{\mathbb{Z}_k} \circ f : \mathbb{Z}_k^m \to \mathbb{U}_k \subset \mathbb{U}$ est courbe au sens de Logachev, Salnikov et Yashchenko.

Une simple traduction dans le contexte k-aire permet de (re-)définir la notion de non linéarité parfaite étudiée par Nyberg dans [Nyb91]. En effet il s'agit d'une particularisation du concept de Carlet et Ding au sens où les groupes finis commutatifs G_1 et G_2 sont substitués par les groupes additifs sous-jacents respectivement au module $\mathbb{Z}_k^m$ et à l'anneau $\mathbb{Z}_k$.

Définition 6.10. Une fonction $f : \mathbb{Z}_k^m \to \mathbb{Z}_k$ est *parfaitement non linéaire* si pour tout $\alpha \in \mathbb{Z}_k^{m*}$ et pour tout $\beta \in \mathbb{Z}_k$,

$$|\{x \in \mathbb{Z}_k^m | d_\alpha f(x) = \beta\}| = k^{m-1} \ .$$

Comme dans le cas booléen les notions de non linéarité parfaite et de fonction courbe sont connexes, néanmoins nous ne disposons plus de l'équivalence.

Proposition 6.10. [Nyb91] *Soit $f : \mathbb{Z}_k^m \to \mathbb{Z}_k$. La fonction f est parfaitement non linéaire si et seulement si pour tout $\beta \in \mathbb{Z}_k^*$, la fonction*

$$\begin{array}{rccc} \tau_\beta \circ f : & \mathbb{Z}_k^m & \to & \mathbb{Z}_k \\ & x & \mapsto & \beta f(x) \end{array}$$

est k-aire courbe.

Preuve. Le résultat est évident par application du théorème 6.5. Il suffit en effet de substituer au groupe G_1 (respectivement G_2) le groupe additif sous-jacent au module $\mathbb{Z}_k^m$ (respectivement le groupe additif sous-jacent à l'anneau $\mathbb{Z}_k$) et de remarquer que $\chi^\beta_{\mathbb{Z}_k} = \chi^1_{\mathbb{Z}_k} \circ \tau_\beta$ (ainsi que nous l'avons auparavant observé avec l'égalité (6.8)). □

[10] Souvent dans la littérature ces fonctions sont dites *courbes généralisées*.

Il est temps d'étudier le cas des fonctions k-aires « vectorielles » comme cela a été fait dans le cas booléen.

Définition 6.11. Une fonction $f : \mathbb{Z}_k^m \to \mathbb{Z}_k^n$ est *parfaitement non linéaire* si, comme d'habitude, pour tout $\alpha \in \mathbb{Z}_k^{m*}$, la dérivée $d_\alpha f$ est équilibrée, ce qui revient à dire que $\forall(\alpha, \beta) \in \mathbb{Z}_k^{m*} \times \mathbb{Z}_k^n$,

$$|\{x \in \mathbb{Z}_k^m | f(x+\alpha) - f(x) = \beta\}| = k^{m-n} \ .$$

Dans [Nyb92] Nyberg a initialement énoncé le résultat suivant. Pour qu'une fonction $f : \mathbb{Z}_k^m \to \mathbb{Z}_k^n$ soit parfaitement non linéaire il faut et il suffit que pour chaque $\beta \in \mathbb{Z}_k^{n*}$, la fonction $l_\beta \circ f : \mathbb{Z}_k^m \to \mathbb{Z}_k$ soit parfaitement non linéaire. Ceci correspond peu ou prou au résultat connu dans le cas booléen. Toutefois ainsi que Carlet et Dubuc l'ont remarqué dans [CD00] la proposition de Nyberg est fausse. Elle fut alors remplacée par la suivante.

Proposition 6.11. [CD00] *Soit $f : \mathbb{Z}_k^m \to \mathbb{Z}_k^n$. La fonction f est parfaitement non linéaire si et seulement si pour tout $\beta \in \mathbb{Z}_k^{n*}$, la fonction*

$$\begin{array}{rccc} l_\beta \circ f : & \mathbb{Z}_k^m & \to & \mathbb{Z}_k \\ & x & \mapsto & \beta.f(x) \end{array}$$

est k-aire courbe.

Preuve. Cette fois encore la démonstration se réduit à l'application du théorème 6.5 où les rôles de G_1 et de G_2 sont joués par les groupes additifs sous-jacents à $\mathbb{Z}_k^m$ et $\mathbb{Z}_k^n$ et en remarquant que $\chi^\beta_{\mathbb{Z}_k^n} = \chi^1_{\mathbb{Z}_k} \circ l_\beta$ (voir l'égalité (6.9)). □

La relation entre les concepts de non linéarité parfaite et de fonction courbe a été exhibée par Nyberg dans [Nyb91].

Théorème 6.8. [Nyb91] *Soit $f : \mathbb{Z}_k^m \to \mathbb{Z}_k$. Si la fonction f est parfaitement non linéaire alors elle est k-aire courbe. La réciproque n'est vraie que si k est un entier premier.*

Preuve. La première propriété s'obtient par application du théorème 6.10 puisque $\tau_1 \circ f = f$.
Supposons maintenant que k soit un entier premier et que f soit k-aire courbe.
On définit

$$\begin{array}{rccc} AC_f : & \mathbb{Z}_k^m & \to & \mathbb{C} \\ & \alpha & \mapsto & \widehat{\chi^1_{\mathbb{Z}_k} \circ d_\alpha f}(0_{\mathbb{Z}_k^m}) = \sum_{x \in \mathbb{Z}_k^m} \omega_k^{d_\alpha f(x)} \ . \end{array}$$

Cette application correspond à $AC_{f,\beta}$ définie dans le lemme 6.5 p. 108 où l'on a posé $G_1 = \mathbb{Z}_k^m$, $G_2 = \mathbb{Z}_k$, $\beta = 1$ et $e_{G_1} = 0_{\mathbb{Z}_k^m}$. Alors, d'après ce même lemme, on a pour tout $\alpha \in \mathbb{Z}_k^m$, $\widehat{AC_f}(\alpha) = |\widehat{\chi^1_{\mathbb{Z}_k} \circ f}(\alpha)|^2 = k^m$ (puisque la fonction f est supposée être k-aire courbe). D'après le lemme 6.3 p. 105, on en déduit que $\forall \alpha \in \mathbb{Z}_k^{m*}$, $AC_f(\alpha) = 0$ soit encore $\forall \alpha \in \mathbb{Z}_k^{m*}$, $\sum_{x \in \mathbb{Z}_k^m} \omega_k^{d_\alpha f(x)} = 0$. On a donc $\forall \alpha \in \mathbb{Z}_k^{m*}$, $\sum_{y \in \mathbb{Z}_k} \varphi_{d_\alpha f}(y) \omega_k^y = 0$ où pour $y \in \mathbb{Z}_k$, on a $\varphi_{d_\alpha f}(y) \stackrel{déf.}{=} |\{x \in \mathbb{Z}_k^m | d_\alpha f(x) = y\}|$.
Puisque $\{\omega_k, \omega_k^2, \ldots, \omega_k^{k-1}\}$ est une base du $k^{ième}$ corps cyclotomique sur le corps des rationnels $\mathbb{Q}$ (cf. [LN97]), il s'ensuit que tous les $\varphi_{d_\alpha f}(y)$ sont égaux, ce qui revient à dire que f est parfaitement non linéaire au sens de Carlet et Ding. □

Le résultat maintes fois annoncé concernant le défaut d'équivalence entre les notions de fonction parfaitement non linéaire et de fonction courbe a donc été explicité dans le cadre des fonctions k-aires. Cela prouve ainsi expressément que la non linéarité parfaite est, en général, une propriété plus forte que le fait pour une fonction d'être courbe.

Comme dans le cas booléen il existe un certain nombre de constructions de fonctions k-aires courbes (cf. [KSW85, Hou98]). On donne simplement l'exemple suivant des fonctions k-aires quadratiques ou plus précisément une généralisation de la classe de Maiorana-MacFarland (voir définition 5.8 p. 92).

Exemple 6.1. Soit m un entier pair. Soient $g : \mathbb{Z}_k^{\frac{m}{2}} \to \mathbb{Z}_k$ et $\pi \in S(\mathbb{Z}_k^{\frac{m}{2}})$. La fonction

$$\begin{array}{rccl} f: & \mathbb{Z}_k^m & \to & \mathbb{Z}_k \\ & (x,y) & \mapsto & x.\pi(y)+g(y) \end{array}$$

où $(x,y) \in (\mathbb{Z}_k^{\frac{m}{2}})^2$ (*i.e.* on identifie les deux modules $\mathbb{Z}_k^m$ et $(\mathbb{Z}_k^{\frac{m}{2}})^2$) est k-aire courbe. Cependant cette fonction n'est pas parfaitement non linéaire quand k n'est pas premier (cf. [CD00]).

Par ailleurs, dans [CD00] est exhibée une fonction k-aire parfaitement non linéaire pour $k = 4$.

Les fonctions k-aires courbes sont encore plus complexes à caractériser que dans le contexte booléen ou dans le cadre de la théorie de Logachev, Salnikov et Yashchenko. Par exemple l'existence d'une fonction duale n'est pas toujours satisfaite (si c'est le cas on parle alors de fonction courbe *régulière* [KSW85]). Il en est de même pour ce qui concerne une possible caractérisation en termes d'ensembles à différences de $\mathbb{Z}_k$.

Ces diverses difficultés sont essentiellement dûes à la contrainte déjà évoquée dans la section 6.5 : les fonctions $\chi^1_{\mathbb{Z}_k} \circ f$ sont à valeurs dans $\mathbb{U}_k$ contrairement aux fonctions courbes au sens de Logachev, Salnikov et Yashchenko, lesquelles peuvent prendre leurs valeurs dans $\mathbb{U}$ tout entier.

Néanmoins dans certains cas favorables (k premier et m pair) on peut, comme dans le cas booléen, déterminer la distance de « Hamming » à l'ensemble des fonctions affines définies sur $\mathbb{Z}_k^m$ et à valeurs dans $\mathbb{Z}_k$ (voir [Nyb91, Lan92]).

La plupart du temps cependant, ces fonctions restent difficiles à cerner. Leur classification en classes, par exemple, est très loin d'être achevée.

6.7 Fonctions courbes sur des corps finis

6.7.1 Introduction

Une structure très significative en théorie des codes et cryptographie est celle de groupe fini. Il est donc raisonnable de considérer la notion de non linéarité parfaite dans ce cadre conceptuel. Ce travail a été réalisé par Ambrosimov dans [Amb94]. Ainsi que nous allons nous en apercevoir, cette variante n'est véritablement qu'un cas particulier de la théorie générale de Carlet et Ding. Néanmoins il est intéressant d'étudier cette notion dans le cas de la caractéristique 2 et d'exhiber les liens éventuels avec les fonctions booléennes courbes.

Nous organisons cette section conformément au plan suivant :

- dans un premier temps est présentée la théorie générique d'Ambrosimov ;
- puis nous examinons spécifiquement le cas de la caractéristique 2 ;
- pour finir nous exposons la notion de fonction hyper-courbe étroitement liée aux idées d'Ambrosimov.

6.7.2 Caractéristique quelconque

Avant d'aborder les travaux d'Ambrosimov, nous effectuons un bref récapitulatif de certaines notations et définitions pratiques dans le contexte des corps finis.

Dans cette sous-section, on se donne un triplet $(p,k,m) \in \mathbb{N}^{*\,3}$ dans lequel p est un nombre premier. Examinons les caractères des différents groupes figurant dans ce cadre, à savoir les groupes additifs des corps finis $\mathbb{F}_p$ et $\mathbb{F}_{p^k}$ et le groupe additif sous-jacent au $\mathbb{F}_{p^k}$-espace vectoriel $\mathbb{F}_{p^k}^m$.

– *Caractères du groupe additif du corps premier* $\mathbb{F}_p$. Soit $\alpha \in \mathbb{F}_p$ alors

$$\begin{array}{rccc} \chi_{\mathbb{F}_p}^{\alpha} : & \mathbb{F}_p & \to & \mathbb{U}_p \\ & x & \mapsto & \omega_p^{\alpha x} \end{array}$$

où αx est naturellement interprété comme un produit dans le corps $\mathbb{F}_p$. On a donc

$$\chi_{\mathbb{F}_p}^{\alpha} = \chi_{\mathbb{F}_p}^{1_{\mathbb{F}_p}} \circ \tau_\alpha$$

où, on le rappelle,

$$\begin{array}{rccc} \tau_\alpha : & \mathbb{F}_p & \to & \mathbb{F}_p \\ & x & \mapsto & \alpha x \ . \end{array}$$

– *Caractères du groupe additif de* $\mathbb{F}_{p^k}$. Soit $\alpha \in \mathbb{F}_{p^k}$ alors

$$\begin{array}{rccc} \chi_{\mathbb{F}_{p^k}}^{\alpha} : & \mathbb{F}_{p^k} & \to & \mathbb{U}_p \\ & x & \mapsto & \omega_p^{tr(\alpha x)} \end{array}$$

où, cette fois, αx est interprété au sens de la multiplication dans le corps $\mathbb{F}_{p^k}$ et « *tr* » désigne la trace absolue de $\mathbb{F}_{p^k}$ (voir p. 102). Nous avons par ailleurs l'égalité suivante :

$$\chi_{\mathbb{F}_{p^k}}^{\alpha} = \chi_{\mathbb{F}_p}^{1_{\mathbb{F}_p}} \circ l_\alpha$$

où la forme linéaire l_α est définie via le produit scalaire associé à la trace :

$$\begin{array}{rccc} l_\alpha : & \mathbb{F}_{p^k} & \to & \mathbb{F}_p \\ & x & \mapsto & tr(\alpha x) \ . \end{array}$$

Comme en particulier $\chi_{\mathbb{F}_{p^k}}^{1_{\mathbb{F}_{p^k}}} : x \mapsto \omega_p^{tr(x)}$, on a aussi :

$$\chi_{\mathbb{F}_{p^k}}^{\alpha} = \chi_{\mathbb{F}_{p^k}}^{1_{\mathbb{F}_{p^k}}} \circ \tau_\alpha$$

où, comme toujours, τ_α est la translation multiplicative par α dans $\mathbb{F}_{p^k}$:

$$\begin{array}{rccc} \tau_\alpha : & \mathbb{F}_{p^k} & \to & \mathbb{F}_{p^k} \\ & x & \mapsto & \alpha x \ . \end{array}$$

– *Caractères du groupe additif sous-jacent au* $\mathbb{F}_{p^k}$*-espace vectoriel* $\mathbb{F}_{p^k}^m$. Soit $\alpha \in \mathbb{F}_{p^k}^m$ alors

$$\begin{array}{rccc} \chi_{\mathbb{F}_{p^k}^m}^{\alpha} : & \mathbb{F}_{p^k}^m & \to & \mathbb{U}_p \\ & x & \mapsto & \omega_p^{tr(\alpha.x)} \end{array}$$

où le symbole « . » désigne le produit scalaire naturel de $\mathbb{F}_{p^k}^m$ en tant qu'espace vectoriel sur $\mathbb{F}_{p^k}$ *i.e.* pour $(x,y) \in (\mathbb{F}_{p^k}^m)^2$, $x.y \stackrel{déf.}{=} \sum_{i=1}^{m} x_i y_i \in \mathbb{F}_{p^k}$. On a donc

$$\chi^{\alpha}_{\mathbb{F}_{p^k}^m} = \chi^{1_{\mathbb{F}_p}}_{\mathbb{F}_p} \circ l'_\alpha = \chi^{1_{\mathbb{F}_p^k}}_{\mathbb{F}_{p^k}} \circ l_\alpha$$

où

$$\begin{array}{rccc} l'_\alpha : & \mathbb{F}_{p^k}^m & \to & \mathbb{F}_p \\ & x & \mapsto & tr(\alpha.x) \end{array}$$

et

$$\begin{array}{rccc} l_\alpha : & \mathbb{F}_{p^k}^m & \to & \mathbb{F}_{p^k} \\ & x & \mapsto & \alpha.x \ . \end{array}$$

Les isomorphismes étant fixés, on obtient donc immédiatement la définition suivante.

Définition 6.12. Soit $\varphi : \mathbb{F}_{p^k}^m \to \mathbb{C}$. La *transformée de Fourier* de φ est définie par

$$\begin{array}{rccc} \widehat{\varphi} : & \mathbb{F}_{p^k}^m & \to & \mathbb{C} \\ & \alpha & \mapsto & \sum\limits_{x \in \mathbb{F}_{p^k}^m} \varphi(x) \omega_p^{tr(\alpha.x)} \ . \end{array}$$

Disposant de la transformée de Fourier, nous pouvons maintenant exposer la notion introduite par Ambrosimov.

Définition 6.13. Soit $f : \mathbb{F}_{p^k}^m \to \mathbb{F}_{p^k}$. La fonction f est *courbe au sens d'Ambrosimov* si pour tout $\beta \in \mathbb{F}_{p^k}^*$ et pour tout $\alpha \in \mathbb{F}_{p^k}^m$, $|\widehat{\chi^{\beta}_{\mathbb{F}_{p^k}} \circ f}(\alpha)| = p^{\frac{km}{2}}$.

Il est possible d'interpréter cette notion dans le cadre des travaux de Logachev, Salnikov et Yashchenko.

Proposition 6.12. [CD04] *Soit $f : \mathbb{F}_{p^k}^m \to \mathbb{F}_{p^k}$. La fonction f est courbe au sens d'Ambrosimov si et seulement si pour tout $\beta \in \mathbb{F}_{p^k}^*$, la fonction $\chi^{\beta}_{\mathbb{F}_{p^k}} \circ f : \mathbb{F}_{p^k}^m \to \mathbb{U}_p \subset \mathbb{U}$ est courbe au sens de Logachev, Salnikov et Yashchenko.*

Preuve. La fonction f est courbe au sens d'Ambrosimov si et seulement si $\forall \beta \in \mathbb{F}_{p^k}^*$, $\chi^{\beta}_{\mathbb{F}_{p^k}} \circ f : \mathbb{F}_{p^k}^m \to \mathbb{U}$ satisfait $|\widehat{\chi^{\beta}_{\mathbb{F}_{p^k}} \circ f}| = p^{k\frac{m}{2}} = \sqrt{|\mathbb{F}_{p^k}^m|}$. Cette dernière propriété est, par définition, équivalente au fait que $\forall \beta \in \mathbb{F}_{p^k}^*$, $\chi^{\beta}_{\mathbb{F}_{p^k}} \circ f$ est courbe au sens de Logachev, Salnikov et Yashchenko. □

On en déduit presque immédiatement la résultat suivant.

Corollaire 6.1. *Soit $f : \mathbb{F}_{p^k}^m \to \mathbb{F}_{p^k}$. La fonction f est courbe au sens d'Ambrosimov si et seulement si elle est parfaitement non linéaire au sens de Carlet et Ding.*

Preuve. Il s'agit d'une simple application du théorème 6.5. □

Dans le cas où $k = 1$, il est possible de lier la notion d'Ambrosimov à celle des fonctions p-aires courbes.

Proposition 6.13. [CD04] *Soit $f : \mathbb{F}_p^m \to \mathbb{F}_p$. La fonction f est courbe au sens d'Ambrosimov si et seulement si elle est p-aire courbe.*

Preuve. Puisque p est un entier premier, l'anneau $\mathbb{Z}_p$ est un corps. Sachant qu'il est de cardinal p, il s'agit en fait du corps premier $\mathbb{F}_p$. Il en résulte en particulier que le module $\mathbb{Z}_p^m$ est en fait le $\mathbb{F}_p$-espace vectoriel $\mathbb{F}_p^m$. La fonction f est donc une fonction de $\mathbb{Z}_p^{\mathbb{Z}_p^m}$. Les structures $\mathbb{Z}_p$ et $\mathbb{F}_p$ étant identiques, on peut donc appliquer à la fonction f à la fois les propositions concernant les fonctions p-aires courbes introduites dans la section 6.6 et celles exposées dans la présente section. En particulier, le théorème 6.8. En effet puisque p est premier, on a :

f est p-aire courbe $\Leftrightarrow$ f est parfaitement non linéaire au sens de Carlet et Ding.

Et d'après le corollaire 6.1 on a :

f parfaitement non linéaire au sens de Carlet et Ding $\Leftrightarrow$ f courbe au sens d'Ambrosimov.

On obtient donc la conclusion souhaitée. □

6.7.3 Caractéristique deux

Nous examinons de manière croisée la notion de fonction courbe d'Ambrosimov dans le cas de la caractéristique 2 et celle du cas booléen. Intuitivement ces deux concepts sont isomorphes puisqu'ils sont tous deux équivalents à la non linéarité parfaite. Nous démontrons formellement ce point.

Rappelons l'isomorphisme de $\mathbb{F}_2$-espaces vectoriels entre $\mathbb{F}_{2^m}$ et $\mathbb{F}_2^m$ entrevu au début du chapitre 4 (voir p. 47). Soit B une base de $\mathbb{F}_{2^m}$ vu comme un espace vectoriel sur $\mathbb{F}_2$. Alors Φ_B, qui associe à un élément $x \in \mathbb{F}_{2^m}$ ses coordonnées dans la base B, est un isomorphisme linéaire.

Démontrons maintenant l'équivalence entre la notion d'Ambrosimov et celle de fonction booléenne courbe.

Proposition 6.14. *Soit $f : \mathbb{F}_{2^m} \to \mathbb{F}_2$. Soit B une base de la structure de $\mathbb{F}_2$-espace vectoriel sous-jacente au corps $\mathbb{F}_{2^m}$. La fonction f est courbe au sens d'Ambrosimov si et seulement si $f \circ \Phi_B^{-1} : \mathbb{F}_2^m \to \mathbb{F}_2$ est courbe (au sens classique des fonctions booléennes).*

Preuve. Afin d'éviter des non-sens, nous rappelons que les lois additives de $\mathbb{F}_{2^m}$ et $\mathbb{F}_2^m$ sont toutes deux notées par le même symbole « $\oplus$ ». Le lecteur prendra donc soin d'observer le type des opérandes de $\oplus$.
Reprenons le cours normal de la preuve.
La fonction $f : \mathbb{F}_{2^m} \to \mathbb{F}_2$ est courbe au sens d'Ambrosimov
$\Leftrightarrow$ f est parfaitement non linéaire au sens de Carlet et Ding (corollaire 6.1)
$\Leftrightarrow \forall \alpha \in \mathbb{F}_{2^m}^*, \forall \beta \in \mathbb{F}_2, |\{x \in \mathbb{F}_{2^m} | f(x \oplus \alpha) \oplus f(x) = \beta\}| = 2^{m-1}$
$\Leftrightarrow \forall \alpha \in \mathbb{F}_{2^m}^*, \forall \beta \in \mathbb{F}_2, |\{x \in \mathbb{F}_{2^m} | f(\Phi_B^{-1}(\Phi_B(x \oplus \alpha))) \oplus f(\Phi_B^{-1}(\Phi_B(x))) = \beta\}| = 2^{m-1}$
$\Leftrightarrow \forall \alpha \in \mathbb{F}_{2^m}^*, \forall \beta \in \mathbb{F}_2, |\{x \in \mathbb{F}_{2^m} | f(\Phi_B^{-1}(\Phi_B(x) \oplus \Phi_B(\alpha))) \oplus f(\Phi_B^{-1}(\Phi_B(x))) = \beta\}| = 2^{m-1}$
(puisque Φ_B est un isomorphisme et donc en particulier un homomorphisme)
$\Leftrightarrow \forall \alpha' \in \mathbb{F}_2^{m*}, \forall \beta \in \mathbb{F}_2, |\{x \in \mathbb{F}_{2^m} | f \circ \Phi_B^{-1}(\Phi_B(x) \oplus \alpha') \oplus f \circ \Phi_B^{-1}(\Phi_B(x)) = \beta\}| = 2^{m-1}$ (car $\alpha \in \mathbb{F}_{2^m}^* \Leftrightarrow \alpha' \stackrel{déf.}{=} \Phi_B(\alpha) \in \mathbb{F}_2^{m*}$)
$\Leftrightarrow \forall \alpha' \in \mathbb{F}_2^{m*}, \forall \beta \in \mathbb{F}_2, |\{y \in \mathbb{F}_2^m | f \circ \Phi_B^{-1}(y \oplus \alpha') \oplus f \circ \Phi_B^{-1}(y) = \beta\}| = 2^{m-1}$ (par le changement de variables $y \stackrel{déf.}{=} \Phi_B(x)$)
$\Leftrightarrow$ $f \circ \Phi_B^{-1} : \mathbb{F}_2^m \to \mathbb{F}_2$ est parfaitement non linéaire (au sens classique)
$\Leftrightarrow$ $f \circ \Phi_B^{-1}$ est courbe au sens classique (par le théorème 5.1 p. 79). □

6.7.4 Fonctions hyper-courbes

On rappelle que les fonctions courbes (classiques) sont ces fonctions booléennes, à un nombre pair de variables, les plus éloignées du code de Reed-Muller d'ordre 1. Ces objets combinatoires sont relativement rares. Cependant l'ensemble des fonctions courbes contient un sous-ensemble de fonctions, dites *hyper-courbes*, dont les propriétés sont encore plus fortes et dont les éléments sont encore moins nombreux. Dans [YG01] Youssef et Gong ont étudié les fonctions $f : \mathbb{F}_{2^m} \to \mathbb{F}_2$ (pour un entier m pair) dont la distance de Hamming à chacune des fonctions $x \mapsto tr(\alpha x^n) \oplus \beta$ (avec $\alpha \in \mathbb{F}_{2^m}$, $\beta \in \mathbb{F}_2$ et n premier avec $2^m - 1$) est égale à $2^{m-1} \pm 2^{\frac{m}{2}-1}$.

On définit, comme dans la sous-section 5.5.3 p. 97, pour $n \in \{1, \ldots, 2^m - 1\}$, $f^{(n)} : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ la fonction $x \mapsto x^n$. Dans certains cas, cette fonction est une permutation de $\mathbb{F}_{2^m}$ On la note alors « $\pi^{(n)}$ » et on l'appelle *permutation puissance*.

Proposition 6.15. [Dob98] *Soit $n \in \{1, \ldots, 2^m - 1\}$. La fonction $f^{(n)}$ définie ci-dessus est une permutation de $\mathbb{F}_{2^m}$ si et seulement si $pgcd(n, 2^m - 1) = 1$ i.e. $n \in \mathbb{Z}_{2^m-1}^{\times}$ (soit encore, n est un élément inversible de $\mathbb{Z}_{2^m-1}$).*
Si $\pi^{(n)} \in S(\mathbb{F}_{2^m})$ alors ${\pi^{(n)}}^{-1} = \pi^{(k)}$ où k est l'inverse (multiplicatif) de n modulo $2^m - 1$ (en particulier $pgcd(k, 2^m - 1) = 1$ également).

Preuve. Supposons que $pgcd(n, 2^m - 1) = 1$ alors il existe $k \in \{1, \ldots, 2^m - 1\}$ tel que $kn \equiv 1 \pmod{2^m - 1}$. Alors pour tout $x \in \mathbb{F}_{2^m}$, on a $(x^n)^k = x$, puisque si $x \in \mathbb{F}_{2^m}^*$, on a $x^{2^m-1} = 1$ et si $x = 0_{\mathbb{F}_{2^m}}$, $0_{\mathbb{F}_{2^m}}^{k'} = 0_{\mathbb{F}_{2^m}}$ $\forall k' \in \mathbb{N}^*$.
Supposons que $\pi^{(n)} \in S(\mathbb{F}_{2^m})$. Utilisons la méthode de réduction à l'absurde en supposant que $pgcd(n, 2^m - 1) \neq 1$. Soit $\alpha \in \mathbb{F}_{2^m}$ une racine primitive du corps $\mathbb{F}_{2^m}$. Si $pgcd(n, 2^m - 1) = k \neq 1$ alors $\alpha^{\frac{2^m-1}{k}}$ et $\alpha^{2\frac{2^m-1}{k}}$ sont distincts et tous deux envoyés par $\pi^{(n)}$ sur $1_{\mathbb{F}_{2^m}}$.
Dans le cas où $\pi^{(n)} \in S(\mathbb{F}_{2^m})$ on a déjà vu (dans la première partie de cette preuve) qu'il existe $k \in \{1, \ldots, 2^m - 1\}$ tel que $kn \equiv 1 \pmod{2^m - 1}$ et ${\pi^{(n)}}^{-1} = \pi^{(k)}$. □

Remarque 6.4. L'ensemble des permutations puissances de $\mathbb{F}_{2^m}$ forme un sous-groupe commutatif de $S(\mathbb{F}_{2^m})$ noté « $G^{(puiss)}$ ».

Introduisons la notion de fonction hyper-courbe.

Définition 6.14. Soit m un entier pair. Une fonction $f : \mathbb{F}_{2^m} \to \mathbb{F}_2$ est dite *hyper-courbe* si pour tout $n \in \mathbb{Z}_{2^m-1}^{\times}$, $f \circ \pi^{(n)} : \mathbb{F}_{2^m} \to \mathbb{F}_2$ est courbe au sens d'Ambrosimov.

Il résulte directement de cette définition que dès que f est hyper-courbe, elle est également courbe au sens d'Ambrosimov (puisque $f \circ \pi^{(1)} = f \circ Id_{\mathbb{F}_{2^m}} = f$).

Cette notion peut se caractériser - comme dans le cas des fonctions booléennes courbes - à l'aide de la transformée de Fourier.

Proposition 6.16. [YG01] *La fonction $f : \mathbb{F}_{2^m} \to \mathbb{F}_2$ est hyper-courbe si et seulement si pour tout $n \in \mathbb{Z}_{2^m-1}^{\times}$ et pour tout $\alpha \in \mathbb{F}_{2^m}$,*

$$(\chi^1_{\mathbb{F}_2} \widehat{\circ f \circ \pi^{(n)}})(\alpha) = \sum_{x \in \mathbb{F}_{2^m}} (-1)^{f(x^n)}(-1)^{tr(\alpha x)} = \pm 2^{\frac{m}{2}} .$$

Preuve. Cela provient trivialement des définitions de fonctions hyper-courbe et courbe au sens d'Ambrosimov. □

Remarque 6.5. Puisque n est premier avec $2^m - 1$, $\pi^{(n)} \in S(\mathbb{F}_{2^m})$ et alors $(\chi^1_{\mathbb{F}_2} \widehat{\circ f \circ \pi^{(n)}})(\alpha) = \sum_{x \in \mathbb{F}_{2^m}} (-1)^{f(x)}(-1)^{tr(\alpha x^k)}$ où k est l'inverse de n modulo $2^m - 1$.

Définition 6.15. Soit $(n, \alpha, \beta) \in \mathbb{Z}_{2^m-1}^{\times} \times \mathbb{F}_{2^m} \times \mathbb{F}_2$. La fonction $\sigma_\beta \circ l_\alpha \circ \pi^{(n)}$ c'est-à-dire

$$\begin{array}{rccl} \sigma_\beta \circ l_\alpha \circ \pi^{(n)} : & \mathbb{F}_{2^m} & \to & \mathbb{F}_2 \\ & x & \mapsto & tr(\alpha x^n) \oplus \beta \end{array}$$

est appelée *fonction coordonnée du monôme inversible* $\mathtt{X}^n$ (où l'on rappelle que la forme linéaire l_α est ici définie par $x \mapsto tr(\alpha x)$).

Si on note, comme dans le cas des espaces vectoriels sur $\mathbb{F}_2$, « $R(1,m)$ » le code de Reed-Muller du corps $\mathbb{F}_{2^m}$ *i.e.* l'ensemble des fonctions de $\mathbb{F}_{2^m}$ dans $\mathbb{F}_2$ de la forme $x \mapsto tr(\alpha x) \oplus \beta$ soit encore les fonctions affines $\sigma_\beta \circ l_\alpha$, alors on observe que les fonctions coordonnées du monôme inversible $\mathtt{X}^n$ sont obtenues à partir des éléments de $R(1,m)$ de $\mathbb{F}_{2^m}$, par composition avec une permutation puissance. On note alors « $G^{(puiss)}(R(1,m))$ » l'ensemble de telles fonctions.

On peut aisément montrer, en utilisant la remarque 6.5 et en raisonnant comme dans le cas booléen classique, que l'on a pour toute fonction $f : \mathbb{F}_{2^m} \to \mathbb{F}_2$

$$d_H(f, G^{(puiss)}(R(1,m))) = 2^{m-1} - \frac{1}{2}\max\{|\chi_{\mathbb{F}_2}^1 \circ f \circ \pi^{(n)}(\alpha)| \in \mathbb{R} \mid \alpha \in \mathbb{F}_{2^m},\ n \in \mathbb{Z}_{2^m-1}^{\times}\}\ .$$

Aussi on en déduit que si f est hyper-courbe, $d_H(f, G^{(puiss)}(R(1,m)))$ est maximale et vérifie donc

$$d_H(f, G^{(puiss)}(R(1,m))) = 2^{m-1} - 2^{\frac{m}{2}-1}$$

ce qui constitue un résultat très similaire à la caractérisation des fonctions courbes par la distance au code de Reed-Muller d'ordre 1 (voir au chapitre 5 la sous-section 5.3.5).

Bien que la définition des fonctions hyper-courbes semble très contraignante, de telles fonctions existent bel et bien puisque Youssef et Gong en ont exhibé une construction (cf. [YG01]). Comme l'ont montré Carlet et Gaborit [CG04], les fonctions hyper-courbes élaborées par Youssef et Gong sont bien connues puisqu'il s'agit en fait des fonctions de la (sous-)classe $\mathcal{P}_{m,ap}$ (voir la sous-section 5.4.4 du chapitre 5) à une composition par une translation multiplicative de $\mathbb{F}_{2^m}$, $\tau_\alpha : x \mapsto \alpha x$ ($\alpha \in \mathbb{F}_{2^m}^*$), près.

6.8 Conclusion

Dans ce chapitre nous avons éliminé l'influence du monde booléen sur les concepts de non linéarité parfaite et de fonction courbe en les formalisant dans le cadre de théories plus générales. Cela nous permet de mieux cerner l'information réellement contenue dans ces propriétés et de dégager l'essence même de leur signification.

Certaines des généralisations exposées, il faut le reconnaître, ne se prête guère à des interprétations aussi immédiatement intuitives, c'est-à-dire en accord avec le sens commun, que ces notions dans le contexte booléen. Mais cela semble sans importance. En effet on ne saurait se servir de l'intuition dans la recherche scientifique ni comme critère de vérité, ni comme critère de fécondité.

L'abstraction accrue des notions de non linéarité parfaite et de fonction courbe dans des cadres plus généraux nous permet, au cours de la seconde partie de ce manuscrit, de développer de nouvelles approches se démarquant de manière significative des concepts traditionnels mais reposant néanmoins sur les idées évoquées ici.

De plus, dans ce chapitre, nous avons insisté sur deux termes très significatifs : *translation* et *forme linéaire* comme pour rappeler les liens qui unissent indéniablement les concepts généralisés avec leurs applications cryptographiques, les attaques différentielle et linéaire.

Nous arrivons désormais à un tournant crucial. La définition de la propriété de non linéarité parfaite décrit manifestement le comportement d'une fonction soumise à une translation sur ses variables. Nous nous posons maintenant la question suivante, dont la réponse est argumentée et développée dans la seconde partie,

que se passe-t-il si on substitue aux translations un autre type de permutations ?

Deuxième partie

Non linéarité parfaite au sens des actions de groupe

Introduction

Tu vois, le monde se divise en deux catégories.

SERGIO LEONE, *Le Bon, la Brute et le Truand*

Reprenons la définition de la non linéarité parfaite au sens de Carlet et Ding (voir le chapitre 6). Soient donc $(G,+)$ et $(H,+)$ deux groupes finis commutatifs et f une application de G dans H. Cette fonction est parfaitement non linéaire si et seulement si pour chaque $(\alpha,\beta) \in G^* \times H$,

$$|\{x \in G | f(x+\alpha) - f(x) = \beta\}| = \frac{|G|}{|H|} .$$

Que se passe-t-il maintenant si on remplace dans cette définition les translations $\sigma_\alpha : x \mapsto x+\alpha$ par un autre type de permutations ?

La question paraît simple parce que trop vague. Il nous faut donc préciser le sens de cette interrogation. Etant donné (G,X) un couple dans lequel G est un groupe et X est un ensemble non vide, une action de groupe de G sur X est simplement la donnée d'un homomorphisme de groupes $\phi : G \to S(X)$, autrement dit, G s'identifie à un groupe de permutations de X. Les translations en sont un cas très particulier. Puisqu'il en est ainsi la question peut s'interpréter comme la problématique de l'étude de la non linéarité parfaite généralisée par la prise en compte d'une action de groupe quelconque plutôt que des simples translations.

Le concept classique doit ainsi devenir de fait une concrétisation d'un genre spécifique d'une théorie à la fois plus abstraite et plus globale. Mais que signifie au juste « concept classique » ? Evidemment cette expression imprécise fait au minimum référence à la définition rappelée ci-dessus, mais pas seulement. D'un certain point de vue[11], la non linéarité parfaite se conçoit selon trois aspects différents, certes, mais complémentaires. Les deux premiers, fondamentaux, sont des représentations duales l'une de l'autre. Il s'agit d'une part de la caractérisation combinatoire de la non linéarité parfaite basée sur les notions de dérivée et de fonction équilibrée et d'autre part de sa formulation à l'aide de la transformée de Fourier relevant du concept de fonction courbe. Cette dernière représentation est souvent, si ce n'est toujours, caractérisée par une formule de *conservation de l'énergie i.e.* une formule traduisant le fait que la transformée de Fourier d'une certaine fonction soit de module constant telle que, par exemple, $\widehat{\chi^1_{\mathbb{F}_2} \circ f}(\alpha) = \pm 2^{\frac{m}{2}}$ dans le cas des fonctions booléennes courbes. A ces deux principales descriptions est juxtaposée la caractérisation combinatoire secondaire basée sur la notion d'ensemble à différences. Cette approche additionnelle bien que relativement restrictive, puisque ne concernant que les fonctions à valeurs dans $\mathbb{F}_2$, est en réalité particulièrement pratique quant à la construction explicite de fonctions

[11] Le nôtre en tous cas !

parfaitement non linéaires. En ce qui nous concerne la non linéarité parfaite est en définitive la donnée de ces trois types de formulations équivalentes (ou presque).

L'objectif de cette seconde partie consiste donc à élaborer une théorie générale de la non linéarité parfaite étendant simultanément ces trois caractérisations complémentaires. Informellement cela revient à étudier, selon les trois aspects, pour $(G,(H,+),X)$ un triplet dans lequel G est un groupe fini opérant (ou agissant) sur l'ensemble fini X via l'homomorphisme ϕ et H est un groupe fini commutatif, les fonctions $f : X \to H$ telles que pour chaque $(\mathbf{g},\beta) \in G^* \times H$,

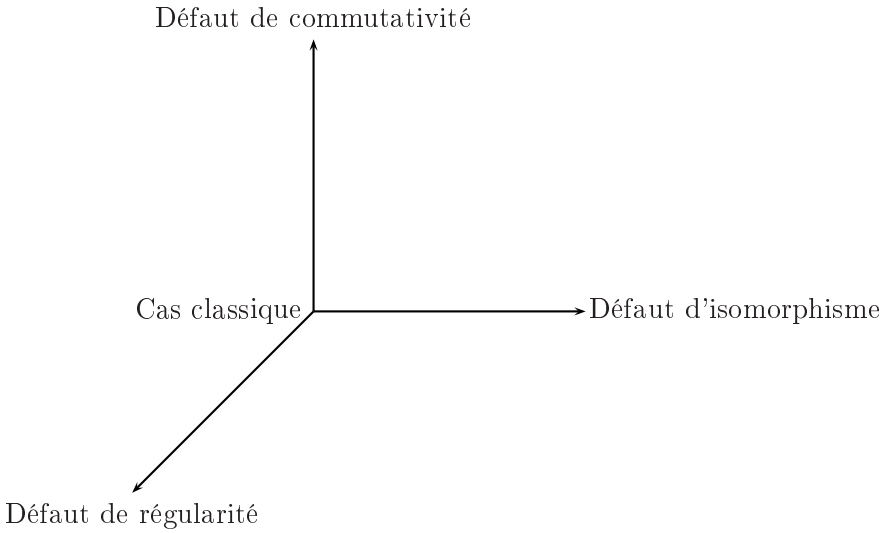
$$|\{x \in X | f(\phi(\mathbf{g}(x))) - f(x) = \beta\}| = \frac{|X|}{|H|} .$$

La définition traditionnelle de la non linéarité parfaite se reconnaît facilement dans la formule précédente, les translations ont simplement été substituées par une action de groupe quelconque.

Ce cadre beaucoup plus abstrait nous offre plusieurs directions dans lesquelles généraliser et caractériser cette approche. Celles-ci sont discriminées par les propriétés du groupe G dans son action sur l'ensemble X. Les trois principales étant les suivantes :

1. *Le défaut de régularité* : Le groupe fini G opère *fidèlement* sur X *i.e.* l'homomorphisme ϕ est injectif ;
2. *Le défaut d'isomorphisme* : L'action du groupe fini G sur X « imite » plus ou moins les translations de X (lorsque ce dernier est muni d'une structure de groupe) ;
3. *Le défaut de commutativité* : Le groupe fini G est soit abélien soit non abélien.

Ces trois paramètres indépendants et complémentaires sont symboliquement illustrés par le schéma suivant (déjà évoqué dans l'introduction du manuscrit).



Cette partie est constituée de deux chapitres - ainsi que de l'annexe B - reprenant chacun l'un des axes de généralisation du concept classique. Dans le chapitre 7 sont exposés les deux premiers points dans un contexte abélien (*i.e.* le groupe G est commutatif). Le dernier point est, quant à lui, développé au chapitre 8 dans lequel G est donc supposé non abélien. Observons que puisqu'il n'existe pas de théorie similaire à celle de Carlet et Ding dans un cadre non abélien, celle-ci est développée dans ce même chapitre avant l'étude d'une généralisation au sens des actions de

groupe non commutatif. Dans tous les cas une formule appropriée de conservation de l'énergie est présentée et de nouvelles fonctions satisfaisant les propriétés généralisées sous construites à l'aide des versions étendues des ensembles à différences. En définitive les trois aspects fondamentaux de la non linéarité parfaite énoncés plus haut se trouvent ainsi repris et généralisés selon les trois directions orthogonales dans cette partie.

Chapitre 7

Non linéarité parfaite basée sur des actions de groupe

Il n'y a point de forêt sans arbres tordus.

PROVERBE, *Bulgarie*

Sommaire

7.1 Introduction

La version la plus générale que nous ayons vue du concept de non linéarité parfaite est celle de Carlet et Ding (chapitre 6 section 6.4). Il s'agit du point de départ des travaux originaux présentés maintenant. Afin de fixer les idées, soient G et H deux groupes finis abéliens notés additivement. Une fonction $f : G \to H$ est *parfaitement non linéaire* (au sens de Carlet et Ding) si

$$\forall \alpha \in G^*,\ \forall \beta \in H,\ |\{x \in G | f(x+\alpha) - f(x) = \beta\}| = \frac{|G|}{|H|}\ .$$

Les translations et donc le groupe $T(G)$ lui-même jouent un rôle capital dans cette définition. Or celles-ci ne sont que des permutations particulières - car affines - de G. Il est donc légitime de les substituer par d'autres éléments de $S(G)$ et d'écrire

$$\forall \pi \in G'^*,\ \forall \beta \in H,\ |\{x \in G | f(\pi(x)) - f(x) = \beta\}| = \frac{|G|}{|H|}$$

où G' est un sous-groupe de $S(G)$. Plus généralement, si X est un ensemble fini non vide et G est maintenant un groupe fini abélien *opérant* sur X c'est-à-dire pour lequel il existe un

homomorphisme de groupes $\phi : G \to S(X)$, alors on peut encore affiner la notion de non linéarité comme suit.

$$\forall \mathbf{g} \in G^*,\ \forall \beta \in H,\ |\{x \in X | f(\phi(\mathbf{g})(x)) - f(x) = \beta\}| = \frac{|X|}{|H|}$$

où $f : X \to H$. La généralisation que nous développons dans cette partie est ainsi fortement liée à la notion d'*action de groupe*.

Immédiatement après avoir re-défini le concept de non linéarité parfaite, se pose alors le problème de l'existence d'une version duale sous l'allure d'une formule de conservation de l'énergie par la transformée de Fourier. Dans l'affirmative, quelle est alors sa forme explicite ? La réponse à cette question nous limite, en regard de ce que nous savons pour l'heure sur la transformée de Fourier, au cas où G est un groupe fini **abélien** de permutations ou, plus précisément, un groupe fini commutatif agissant sur X. Cette restriction, bien que sérieuse, ouvre néanmoins une petite lucarne par laquelle nous passons et que nous allons agrandir dans l'objectif de généraliser le concept traditionnel de non linéarité parfaite. La notion à laquelle nous aboutissons possède indéniablement des envies expansionnistes : elle déborde très largement du cadre primitivement établi qui, *a posteriori*, peut être jugé restrictif. Alors que la situation classique ne décrit qu'une configuration particulière très précise, la démarche exposée dans ce chapitre matérialise une idée polymorphe de la non linéarité parfaite : avec des données initiales identiques, à savoir un groupe commutatif fini H et un ensemble fini X, on décline cette notion en autant de variantes qu'il y a de groupes finis commutatifs G agissant sur X. Imaginez donc ce concept de non linéarité parfaite pour les applications de H^X comme une fonction d'un paramètre G décrivant l'ensemble des groupes commutatifs opérant sur X.

Ce paramètre G est en fait un indicateur synthétique de deux facteurs plus fondamentaux, que nous appelons ici les défauts de *régularité* et d'*isomorphisme* (par rapport à un groupe de translations) de G. Sans entrer dans des détails pour le moment superflus, le premier facteur mesure qualitativement la finesse de l'interaction géométrique entre les éléments de G et ceux de X : quelle est la trajectoire suivie par $\phi(\mathbf{g})(x)$ pour x fixé dans X lorsque $\mathbf{g}$ parcourt G ? Le second facteur est quant à lui en rapport avec le degré de ressemblance de G, dans son comportement avec les éléments de X, avec le groupe des translations $T(X)$ lorsque X est lui-même un groupe. Ces deux paramètres permettent ainsi de discriminer les multiples versions de la notion étendue de non linéarité parfaite.

Supposons maintenant que le groupe H sur lequel les fonctions étudiées prennent leurs valeurs soit le plus simple possible, c'est-à-dire $H = \mathbb{F}_2$ (la considération du groupe trivial réduit à un unique élément n'ayant, comme on peut aisément le concevoir, qu'un très faible intérêt). Dans le cas classique, les objets combinatoires appelés *ensembles à différences* de Hadamard (voir le chapitre 5 sous-section 5.3.6) fournissent sans exception toutes les fonctions parfaitement non linéaires à valeurs dans $\mathbb{F}_2$. Dans un groupe G, un tel ensemble est défini par le fait que lorsque α parcourt G^*, les équations $x - y = \alpha$ à deux inconnues (de G) possèdent exactement un nombre identique λ de solutions dans D^2. Le lecteur clairvoyant imagine sans aucun doute la généralisation qui peut être appliquée à ce type d'objets : le remplacement de la translation σ_α par l'action d'un groupe fini commutatif G sur un ensemble fini non vide X. Nous obtenons de la sorte le concept de G-ensemble à différences de X permettant de caractériser de manière combinatoire les nouvelles notions. Encore une fois la forme de l'action de G sur les éléments de X joue ici un rôle primordial.

Ce chapitre est essentiellement découpé en cinq parties distinctes. Dans la première est exposé

le concept classique d'action de groupe dont nous venons de signaler la présence dans nos travaux. Puis au cours des deux sections suivantes, nous explicitons les rôles des deux paramètres préalablement cités. Pour chacun d'eux, nous exposons une caractérisation via la transformée de Fourier de la notion correspondante de non linéarité parfaite ainsi que des constructions de nouvelles fonctions satisfaisant ces critères en mettant en valeur les différences fondamentales avec leurs homologues classiques. Dans la section suivante nous étendons davantage la notion de non linéarité parfaite au sens des actions de groupe en faisant agir régulièrement un groupe, non plus sur l'ensemble de départ des fonctions, mais bien sur leur ensemble d'arrivée. Toutefois le concept obtenu se trouve être très similaire à ceux décrits dans les deux sections précédentes. La dernière section enfin est quant à elle entièrement dévolue à l'étude combinatoire des ensembles à différences généralisés au sens des actions de groupe. Grâce à cette nouvelle notion, nous établissons un certain nombre de constructions explicites et pertinentes, mettant en outre très largement en lumière les distinctions avec les cas classiques.

Une partie seulement des résultats exposés ici proviennent de l'article [PH05]. Ces travaux sont très largement complétés dans ce chapitre.

7.2 Actions de groupe

7.2.1 Introduction

Les voies que nous désirons ouvrir dans la diversification de la notion monolithique de non linéarité parfaite classique reposent explicitement sur un pilier essentiel : les actions de groupe. Dans la mesure où celles-ci jouent un rôle majeur dans notre démarche, nous jugeons que la maîtrise de ce domaine est une condition *sine qua non* à la compréhension convenable de nos travaux. Nous assumons cela puisque dans cette section sont brièvement récapitulés un certain nombre de résultats fondamentaux et généraux concernant les actions de groupe, lesquels sont utilisés à la fois dans la deuxième partie de ce chapitre mais aussi dans le chapitre 8 et l'annexe B. Les notions évoquées ici sont tout aussi bien (et sans doute mieux) exposées dans les deux excellents livres [Wie64] et [Pas68].

Un lecteur pour lequel ces notions classiques sont particulièrement familières peut directement s'acheminer vers la section 7.3 du présent chapitre dans laquelle est exposée une partie de nos résultats originaux. Toutefois, eut égard à leur importance dans notre discours théorique, nous incitons à la lecture attentive au minimum des trois sous-sections suivantes et en définitive, s'il ne fallait ne retenir de cette section que deux notions seulement, ce seraient les points clefs d'actions de groupe *fidèle* et *régulière*.

Dans cette section, les éléments quelconques d'un groupe G sont souvent désignés par les lettres minuscules de police **grasse** « $\mathbf{g}$ », « $\mathbf{h}$ », etc. Cette convention étant nécessaire pour ne pas confondre les éléments d'un groupe avec ceux d'un ensemble sur lequel il agit. Observons néanmoins que parfois nous usons de la lettre grecque « α » afin de nommer un élément d'un groupe, essentiellement dans le cas d'une action d'un groupe sur lui-même.

7.2.2 Action d'un groupe sur un ensemble

Définition 7.1. Soit $(G, \top)$ un groupe et X un ensemble non vide. Un homomorphisme de groupes $\phi : G \to S(X)$ est appelé *action (à gauche)* de G sur l'ensemble X. En particulier pour tout $(\mathbf{g}_1, \mathbf{g}_2) \in G^2$ on a $\phi(\mathbf{g}_1 \top \mathbf{g}_2) = \phi(\mathbf{g}_1) \circ \phi(\mathbf{g}_2)$, $\phi(\mathbf{g}_1^{-1}) = (\phi(\mathbf{g}_1))^{-1}$ et $\phi(e_G) = Id_X$. On dit que G *agit* (ou *opère*) sur l'ensemble X.

On définirait de même la notion d'*action à droite* (ou *anti-action*) : c'est la donnée d'un anti-homomorphisme de groupes ϕ de G dans $S(X)$ *i.e.* pour tout $(\mathbf{g}_1, \mathbf{g}_2) \in G^2$, $\phi(\mathbf{g}_1 \top \mathbf{g}_2) = \phi(\mathbf{g}_2) \circ \phi(\mathbf{g}_1)$ et $\phi(e_G) = Id_X$. Cependant si l'on s'est donné une action à droite, on en déduit une action à gauche ϕ' de G sur X en posant $\phi'(\mathbf{g})(x) \stackrel{déf.}{=} \phi(\mathbf{g}^{-1})(x)$ pour tout $(\mathbf{g}, x) \in G \times X$; cela permet de ramener l'étude des actions à droite à celle des actions à gauche (et réciproquement). Donc, chaque définition que nous introduisons, chaque résultat que nous démontrons avec une action à gauche aura un analogue avec les actions à droite dont nous laisserons l'explicitation au lecteur. Bien entendu, en pratique, il ne faut pas hésiter à écrire les actions du côté où cela semble le plus naturel et en ce qui nous concerne ce sera toujours à gauche. Si le groupe G est abélien, c'est encore plus simple : dans ce cas, toute action à droite est aussi une action à gauche, sans qu'il soit nécessaire d'introduire d'inverses. Pour un groupe non abélien, les deux notions sont distinctes. Dans ce chapitre, on oublie, sauf à de rares exceptions près, le terme « gauche » pour ne retenir que la définition précédente.

Remarque 7.1. Dans la suite, on préfère souvent les notations dites *pointées* « $\mathbf{g}.x$ » et « $\mathbf{g}\top\mathbf{h}.x$ », pour $(\mathbf{g}, \mathbf{h}, x) \in G \times G \times X$ où G est un groupe agissant sur l'ensemble X, aux expressions « $\phi(\mathbf{g})(x)$ » et « $\phi(\mathbf{g}\top\mathbf{h})(x)$ ». Si en outre $G \subset S(X)$, ces mêmes expressions sont respectivement désignées par « $\pi(x)$ » et « $(\pi \circ \sigma)(x)$ » pour $(\pi, \sigma) \in G^2$.

Il existe une définition alternative suivante.

Définition 7.2. Soit $(G, \top)$ un groupe et X un ensemble non vide. On dit que G *agit* sur X lorsque l'on se donne une application $f : G \times X \to X$ vérifiant les deux propriétés suivantes :

1. $\forall (\mathbf{g}_1, \mathbf{g}_2) \in G^2$, $\forall x \in X$, $f(\mathbf{g}_1, f(\mathbf{g}_2, x)) = f(\mathbf{g}_1 \top \mathbf{g}_2, x)$;
2. $\forall x \in X$, $f(e_G, x) = x$.

En fait cette variante est équivalente à la première définition. Pour cela il suffit de remarquer qu'à toute action ϕ correspond une application f telle que $\forall (\mathbf{g}, x) \in G \times X$, $f(\mathbf{g}, x) \stackrel{déf.}{=} \phi(\mathbf{g})(x)$ et réciproquement.

Exemple 7.1.

1. Soit X un ensemble non vide. Alors $S(X)$ agit sur X via l'homomorphisme identité $Id_{S(X)}$;
2. Plus généralement tout sous-groupe G de $S(X)$ agit sur X (via l'injection canonique) ;
3. Soit $\mathbb{K}$ un corps. Le groupe linéaire $GL(\mathbb{K}^m)$ agit sur $\mathbb{K}^m$;
4. Soit V un $\mathbb{K}$-espace vectoriel. Alors le groupe multiplicatif $\mathbb{K}^*$ agit sur V ;
5. Le groupe additif $\mathbb{R}$ agit sur $\mathbb{C}$:
$$\forall x \in \mathbb{R},\ \forall \mathbf{z} \in \mathbb{C},\ x.\mathbf{z} \stackrel{déf.}{=} \mathrm{e}^{\imath x}\mathbf{z} \ .$$
Remarquons que dans ce cas précis l'élément x_0 de $\mathbb{R}$ tel que $x_0.\mathbf{z} = \mathbf{z}$ pour tout $\mathbf{z} \in \mathbb{C}$ n'est pas unique ;
6. Action sur les classes à droite. Soit H un sous-groupe d'un groupe $(G, \top)$. Pour $\mathbf{g} \in G$, on définit le *translaté de* H par $\mathbf{g}$ ou encore la *classe à gauche* de $\mathbf{g}$ *modulo* H par $\mathbf{g}\top H \stackrel{déf.}{=} \{\mathbf{g}\top\mathbf{h} \in G | \mathbf{h} \in G\}$. On considère l'ensemble des classes à gauche modulo H, noté « G/H » et défini par $G/H \stackrel{déf.}{=} \{\mathbf{g}\top H \subset G | \mathbf{g} \in G\}$. Alors G agit sur l'ensemble G/H via l'homomorphisme de groupes
$$\begin{array}{rccl} \phi : & G & \to & S(G/H) \\ & \mathbf{g} & \mapsto & (\phi(\mathbf{g}) : \mathbf{h}\top H \mapsto \mathbf{g}\top\mathbf{h}\top H) \ . \end{array}$$
Cette action est appelée *action sur les classes à gauche de* H (par translation à gauche de G). Remarquons que l'on peut définir de manière tout à fait similaire une action par translation à droite.

Il existe une notion d'équivalence entre actions de groupe permettant d'identifier les actions de *même forme*.

Définition 7.3. Soient $\phi_1 : G_1 \to S(X_1)$ et $\phi_2 : G_2 \to S(X_2)$ deux actions de groupes. Elles sont dites *équivalentes* ou encore *isomorphes* s'il existe un isomorphisme de groupes $\Phi : G_1 \to G_2$ ainsi qu'une bijection $\Theta : X_1 \to X_2$ tels que pour tout $(\mathbf{g}, x) \in G_1 \times X_1$, $\Theta(\phi_1(\mathbf{g})(x)) = \phi_2(\Phi(\mathbf{g}))(\Theta(x))$.

En d'autres termes, cela signifie que le diagramme suivant commute.

$$\begin{array}{ccc} G_1 & \stackrel{\Phi}{\to} & G_2 \\ {\scriptstyle\phi_1}\downarrow & & \downarrow{\scriptstyle\phi_2} \\ X_1 & \stackrel{\Theta}{\to} & X_2 \end{array}$$

Définition 7.4. Soient G un groupe et X un ensemble non vide. Soit $\phi : G \to S(X)$ une action. On dit que l'action ϕ est *fidèle* si elle est injective *i.e.* $\ker(\phi) = \{e_G\}$.

Remarque 7.2. Soit X un ensemble non vide. L'action de tout sous-groupe G de $S(X)$ sur X est fidèle, puisque G agit via l'injection canonique.

Etant donné une action $\phi : (G, \top) \to S(X)$ on peut toujours se ramener à une action fidèle. Il suffit pour cela de considérer l'action du groupe quotient[1] $G/\ker(\phi)$ sur X suivante

$$\begin{array}{rccc} \phi' : & G/\ker(\phi) & \to & S(X) \\ & \bar{\mathbf{g}} & \mapsto & \phi(\mathbf{g}) \end{array}$$

où l'expression « $\bar{\mathbf{g}}$ » désigne la classe à gauche $\mathbf{g}\top\ker(\phi)$ de $\mathbf{g}$. Remarquons que la relation ϕ' est bien définie en tant qu'application. En effet, soit $(\mathbf{g}_1, \mathbf{g}_2) \in G^2$ tel que $\bar{\mathbf{g}}_1 = \bar{\mathbf{g}}_2$ alors par définition de $G/\ker(\phi)$, $\mathbf{g}_2^{-1}\top\mathbf{g}_1 \in \ker(\phi)$. Pour $x \in X$ on obtient alors $\phi(\mathbf{g}_2^{-1}\top\mathbf{g}_1)(x) = x$ donc $\phi(\mathbf{g}_2)(x) = \phi(\mathbf{g}_1)(x)$ soit encore $\phi'(\bar{\mathbf{g}}_1) = \phi'(\bar{\mathbf{g}}_2)$.

7.2.3 Orbites sous une action de groupe

On considère une action du groupe $(G, \top)$ sur l'ensemble X. On définit alors la relation binaire sur X

$$x \equiv_G y \Leftrightarrow \exists \mathbf{g} \in G,\ \mathbf{g}.x = y\ .$$

Il s'agit d'une relation d'équivalence sur X.

- Réflexivité : $e_G.x = x$ d'où $x \equiv_G x$;
- Symétrie : si $x \equiv_G y$ alors il existe $\mathbf{g} \in G$ tel que $y = \mathbf{g}.x$ alors $x = \mathbf{g}^{-1}.y$ et donc $y \equiv_G x$;
- Transitivité : si $x \equiv_G y$ et $y \equiv_G z$, alors il existe $(\mathbf{g}_1, \mathbf{g}_2) \in G^2$ tel que $y = \mathbf{g}_1.x$ et $z = \mathbf{g}_2.y$. Donc $z = \mathbf{g}_2.\mathbf{g}_1.x = (\mathbf{g}_2\top\mathbf{g}_1).x$ d'où $x \equiv_G z$.

Définition 7.5. Soit G un groupe opérant sur un ensemble X. Soit $x \in X$. On appelle *G-orbite* de x (ou simplement *orbite* de x), notée « $\boldsymbol{\mathcal{O}}_G(x)$ », la classe d'équivalence de x suivant la relation $\equiv_G$:

$$\boldsymbol{\mathcal{O}}_G(x) \stackrel{déf.}{=} \{\mathbf{g}.x \in X | \mathbf{g} \in G\} = G.\{x\}\ .$$

L'application

$$\begin{array}{rccc} \phi_x : & G & \to & X \\ & \mathbf{g} & \mapsto & \mathbf{g}.x \end{array}$$

[1] Il s'agit bien d'un groupe puisque $\ker(\phi)$ est un sous-groupe distingué de G.

s'appelle l'*application orbitale* de x et on a $\boldsymbol{\mathcal{O}}_G(x) = \phi_x(G)$.
L'ensemble des orbites $X/G \stackrel{déf.}{=} \bigcup_{x \in G} \{\boldsymbol{\mathcal{O}}_G(x)\}$ constitue (évidemment) une partition de X.

Définition 7.6. On dit que l'action d'un groupe G sur un ensemble non vide X est *transitive* si elle ne possède qu'une seule orbite :

$$\forall (x, y) \in X^2,\ \exists \mathbf{g} \in G \text{ tel que } y = \mathbf{g}.x\ .$$

C'est-à-dire $\forall x \in X$, $\boldsymbol{\mathcal{O}}_G(x) = X$.

Remarquons qu'en règle générale, l'élément $\mathbf{g}$ tel que $y = \mathbf{g}.x$ n'est pas unique.

Exemple 7.2. Soit $m \in \mathbb{N}^*$ et $I \stackrel{déf.}{=} \{1, \ldots, m\}$. Soit $\pi \in S(I)$ une permutation circulaire. Alors le groupe engendré par π, $\langle \pi \rangle \stackrel{déf.}{=} \{\pi^k \in S(I) | k \in \mathbb{Z}\}$, agit transitivement sur I.

Proposition 7.1. [Wie64, Pas68] *Un groupe G agit transitivement sur un ensemble $X \Leftrightarrow \forall x \in X$, l'application orbitale ϕ_x de x est surjective.*

Preuve. Supposons que G agisse transitivement sur X. Soit $x \in X$. Montrons que ϕ_x est surjective. Soit alors $y \in X$. Par transitivité de l'action de G sur X, $y \in \boldsymbol{\mathcal{O}}_G(x) = X$ donc il existe $\mathbf{g} \in G$ tel que $y = \mathbf{g}.x = \phi_x(\mathbf{g})$.
Réciproquement, supposons, pour tout $x \in X$, ϕ_x surjective. Alors $\forall y \in X$, $\exists \mathbf{g} \in G$ tel que $\phi_x(\mathbf{g}) = \mathbf{g}.x = y$ et donc G opère transitivement sur X. □

Définition 7.7. L'action d'un groupe G sur un ensemble (non vide) X est dite *libre* si pour tout $x \in X$, l'application orbitale ϕ_x de x est injective.

Supposons que l'action de G sur X soit libre et fixons $x \in X$. Si $\mathbf{g}_1.x = \mathbf{g}_2.x$ alors $\mathbf{g}_1 = \mathbf{g}_2$ (par injectivité de l'application orbitale de x).

Lemme 7.1. [Wie64, Pas68] *Une action libre d'un groupe G sur un ensemble X est fidèle.*

Preuve. Soit ϕ l'action de G sur X. Soit $\mathbf{g} \in G^*$. Supposons par contradiction que $\mathbf{g} \in \ker(\phi)$. Alors $\forall x \in X$, $\phi(\mathbf{g})(x) = x$ donc $\forall x \in X$, $\phi_x(\mathbf{g}) = x = \phi_x(e_G)$ donc $\forall x \in X$, ϕ_x n'est pas injective ce qui est en contradiction avec le fait que l'action soit libre. □

Définition 7.8. On dit qu'une action d'un groupe G sur un ensemble (non vide) X est *régulière* lorsqu'elle est libre et transitive. Autrement dit pour tout $x \in X$, l'application orbitale ϕ_x de x est bijective, soit encore

$$\forall (x, y) \in X^2,\ \exists\ !\ \mathbf{g} \in G \text{ tel que } y = \mathbf{g}.x\ .$$

En particulier $|G| = |X|$.

Lorsque l'action est régulière on dit aussi que G agit *simplement transitivement* sur X.

Voici un petit lemme bien utile pour la suite de l'exposé.

Lemme 7.2. *Soit G un groupe agissant régulièrement sur un ensemble X. Soit $(x_0, \mathbf{g}_1, \mathbf{g}_2) \in X \times G \times G$. Alors on a*

$$\mathbf{g}_1 = \mathbf{g}_2 \Leftrightarrow \mathbf{g}_1.x_0 = \mathbf{g}_2.x_0\ .$$

Preuve. L'implication directe est évidente (que l'action soit régulière ou non).
Montrons l'implication réciproque. Le fait que $\mathbf{g}_1.x_0 = \mathbf{g}_2.x_0$ équivaut à $\phi_{x_0}(\mathbf{g}_1) = \phi_{x_0}(\mathbf{g}_2)$. Puisque l'action est régulière, l'application orbitale ϕ_{x_0} de x_0 est bijective et donc, en particulier injective, d'où $\mathbf{g}_1 = \mathbf{g}_2$. □

7.2.4 Action d'un groupe sur lui-même

Soit $(G, \top)$ un groupe abélien ou non. On peut définir trois actions de $(G, \top)$ sur l'ensemble sous-jacent à sa structure de groupe.

1. *Action par translation (ou par addition) à gauche.* Pour $\alpha \in G$ on note $\sigma_\alpha^g \in S(G)$ la *translation à gauche par* α définie par $x \mapsto \alpha \top x$. Alors
$$\begin{array}{rccc} \phi : & G & \to & S(G) \\ & \alpha & \mapsto & \sigma_\alpha^g \end{array}$$
est un action régulière ;
2. *Action par translation (ou par addition) à droite.* De manière analogue on peut définir l'action régulière suivante :
$$\begin{array}{rccc} \phi : & G & \to & S(G) \\ & \alpha & \mapsto & \sigma_\alpha^d \end{array}$$
où $\sigma_\alpha^d : x \mapsto x \top \alpha$.
Evidemment si le groupe G est commutatif les deux actions sont confondues. On rappelle que l'on note alors « σ_α » la translation par α et « $T(G)$ » le groupe $\{\sigma_\alpha \in S(G) | \alpha \in G\}$ des translations de G (qui est isomorphe au groupe G lui-même) ;
3. *Action par conjugaison (ou automorphisme intérieur).* On rappelle que $Aut(G)$ est l'ensemble des automorphismes (de groupe) de G *i.e.* l'ensemble des homomorphismes de groupe bijectifs de G dans lui-même. C'est un groupe pour la composition des applications et en particulier un sous-groupe de $S(G)$. Soit $\alpha \in G$. On définit l'*automorphisme intérieur* $\Im_\alpha \in Aut(G)$ (de conjugaison par α) par
$$\begin{array}{rccc} \Im_\alpha : & G & \to & G \\ & x & \mapsto & \alpha \top x \top \alpha^{-1} \ . \end{array}$$
Il s'ensuit alors que
$$\begin{array}{rccc} \phi : & G & \to & Aut(G) \\ & \alpha & \mapsto & \Im_\alpha \end{array}$$
est une action de G sur lui-même appelée *action par conjugaison.* Pour $x \in G$, l'orbite de x sous l'action par conjugaison $\boldsymbol{\mathcal{O}}_G(x) = \{\Im_\alpha(x) \in G | \alpha \in G\}$ est appelée *classe de conjugaison* de x.

Définition 7.9. Soit $(G, \top)$ un groupe. Si x et y sont deux éléments de G appartenant à la même classe de conjugaison, on dit qu'ils sont *conjugués*. Plus généralement deux sous-groupes G_1 et G_2 de G sont dit *conjugués* lorsqu'il existe $\mathbf{g} \in G$ tel que $G_2 = \mathbf{g} \top G_1 \top \mathbf{g}^{-1}$ *i.e.* pour chaque $y \in G_2$, il existe $x \in G_1$ tel que $y = \Im_{\mathbf{g}}(x) = \mathbf{g} \top x \top \mathbf{g}^{-1}$.

Remarquons que si G est commutatif alors l'action par conjugaison n'a que peu d'intérêt puisque quel que soit $\mathbf{g} \in G$, on a $\Im_{\mathbf{g}} = Id_G$ et pour tout $x \in G$, $\boldsymbol{\mathcal{O}}_G(x) = \{x\}$.

7.2.5 Stabilisateurs

Définition 7.10. Soit G un groupe agissant sur un ensemble X. Soit $x \in X$. On appelle *stabilisateur* de x dans G (ou *groupe d'isotopie* de x dans G) le sous-groupe de G noté « S_x » et défini par
$$S_x \stackrel{déf.}{=} \{\mathbf{g} \in G | \mathbf{g}.x = x\} \ .$$
Il s'agit bien d'un sous-groupe de G. En effet soit $x \in X$ et notons « $\top$ » la loi de G :

1. $e_G \in S_x$ car $e_G.x = x$;

2. Si $(\mathbf{g}_1, \mathbf{g}_2) \in S_x^2$ alors $\mathbf{g}_1 \top \mathbf{g}_2.x = \mathbf{g}_1.\mathbf{g}_2.x = \mathbf{g}_1.x = x$ donc $\mathbf{g}_1 \top \mathbf{g}_2 \in S_x$;
3. Si $\mathbf{g} \in S_x$ alors $\mathbf{g}^{-1}.x = \mathbf{g}^{-1}.\mathbf{g}.x = \mathbf{g}^{-1} \top \mathbf{g}.x = e_G.x = x$ donc $\mathbf{g}^{-1} \in S_x$.

Si le stabilisateur d'un élément $x \in X$ est bien un sous-groupe de G, il n'est en général pas distingué dans G. Cependant nous avons les propriétés suivantes.

Proposition 7.2. [Wie64, Pas68] *Soit $(G, \top)$ un groupe agissant sur un ensemble (non vide) X. Soit $x \in X$. Pour tout $y \in \boldsymbol{\mathcal{O}}_G(x)$, S_x et S_y sont conjugués. Si de plus G est un groupe commutatif alors $S_x = S_y$ pour tout $(x, y) \in X^2$ tel que $y \in \boldsymbol{\mathcal{O}}_G(x)$.*

Preuve. Démontrons le premier fait. Soient $x \in X$ fixé et $y \in \boldsymbol{\mathcal{O}}_G(x)$. Il existe donc $\mathbf{g} \in G$ tel que $y = \mathbf{g}.x$.
Soit $\mathbf{h} \in S_y$ donc $\mathbf{h}.y = y$. Il en résulte que $\mathbf{h}.\mathbf{g}.x = \mathbf{g}.x$ soit encore $\mathbf{g}^{-1} \top \mathbf{h} \top \mathbf{g}.x = x$ donc $\mathbf{g}^{-1} \top \mathbf{h} \top \mathbf{g} \in S_x$ c'est-à-dire $\mathbf{g}^{-1} \top S_y \top \mathbf{g} = \Im_{\mathbf{g}^{-1}}(S_y) \subset S_x$.
Soit maintenant $\mathbf{h} \in S_x$. On définit $\mathbf{k} \in G$ par $\mathbf{k} \stackrel{déf.}{=} \Im_{\mathbf{g}}(\mathbf{h}) = \mathbf{g} \top \mathbf{h} \top \mathbf{g}^{-1}$. Montrons que $\mathbf{k} \in S_y$: $\mathbf{k}.y = \mathbf{g} \top \mathbf{h} \top \mathbf{g}^{-1}.y = \mathbf{g} \top \mathbf{h}.\mathbf{g}^{-1}.y = \mathbf{g} \top \mathbf{h}.x = \mathbf{g}.x = y$. Donc $\mathbf{h} \in \mathbf{g}^{-1} \top S_y \top \mathbf{g}$.
Finalement $S_x = \mathbf{g}^{-1} \top S_y \top \mathbf{g}$ et donc S_x et S_y sont conjugués.
Supposons de plus le groupe G commutatif. Soit $(x, y) \in X^2$ tel que $y \in \boldsymbol{\mathcal{O}}_G(x)$. D'après ce que l'on a vu il existe $\mathbf{g} \in G$ tel que l'on ait $S_x = \mathbf{g} \top S_y \top \mathbf{g}^{-1} = \mathbf{g} \top \mathbf{g}^{-1} S_y$ (par commutativité de G) $= S_y$. □

Lemme 7.3. *Soit ϕ une action transitive d'un groupe abélien $(G, \top)$ sur un ensemble (non vide) X. Alors $\forall x \in X$, $S_x = \ker(\phi)$.*

Preuve. Soit $x \in X$ fixé.
Soit $\mathbf{g} \in \ker(\phi)$ alors $\phi(\mathbf{g}) = Id_X$ et donc $\forall y \in X$, $\phi(\mathbf{g})(y) = y$ c'est-à-dire $\forall y \in X$, $\mathbf{g} \in S_y$ donc en particulier $\mathbf{g} \in S_x$ soit encore $\ker(\phi) \subset S_x$.
Soit $\mathbf{g} \in S_x$. Soit $y \in X$. Par transitivité de l'action il existe $\mathbf{h} \in G$ tel que $y = \mathbf{h}.x$. On a donc $\mathbf{g}.y = \mathbf{g}.\mathbf{h}.x = \mathbf{g} \top \mathbf{h}.x = \mathbf{h} \top \mathbf{g}.x$ (puisque G est abélien) $= \mathbf{h}.\mathbf{g}.x = \mathbf{h}.x = y$. Puisque c'est vrai pour tout $y \in X$, on en déduit que $\mathbf{g} \in \ker(\phi)$ et donc $S_x \subset \ker(\phi)$.
Les deux inclusions impliquent donc finalement que $S_x = \ker(\phi)$. □

Pour les groupes commutatifs, nous disposons d'une caractérisation pratique de la régularité des actions.

Proposition 7.3. *Soit ϕ une action fidèle et transitive d'un groupe abélien $(G, \top)$ sur un ensemble X. Alors ϕ est régulière (c'est-à-dire qu'elle est libre).*

Preuve. On sait d'après le lemme précédent que $\forall x \in X$, $S_x = \ker(\phi)$. Puisque par ailleurs l'action est fidèle on en déduit que $\forall x \in X$, $S_x = \{e_G\}$. Soit donc $x \in X$ fixé. Soit $(\mathbf{g}_1, \mathbf{g}_2) \in G^2$ tel que $\phi_x(\mathbf{g}_1) = \phi_x(\mathbf{g}_2)$. Donc $\mathbf{g}_1.x = \mathbf{g}_2.x$ soit $\mathbf{g}_2^{-1}.\mathbf{g}_1.x = x$ c'est-à-dire $\mathbf{g}_2^{-1} \top \mathbf{g}_1 \in S_x = \{e_G\}$. D'où l'on tire que $\mathbf{g}_1 = \mathbf{g}_2$ et donc que ϕ_x est injective. Cela étant vrai pour tout $x \in X$, il en résulte que l'action est libre. □

Il en résulte finalement que dans le cas des groupes commutatifs, une action régulière est une action fidèle et transitive.

Nous utilisons maintenant la notion d'équivalence entre actions afin de donner la forme canonique de certaines d'entre elles.

Proposition 7.4. [Wie64, Pas68] *N'importe quelle action transitive d'un groupe $(G, \top)$ sur un ensemble (non vide) X est isomorphe à l'action de G (par translation à gauche) sur les classes à droite de S_x pour un x quelconque dans X.*

Preuve. Soit x un élément quelconque de X. Attention, nous notons par le même symbole « . » les deux actions c'est-à-dire celle de G sur X et celle de G sur G/S_x.

On définit $\Theta : G \to G/S_x$ comme suit. Si $y \in X$ alors il existe $\mathbf{g} \in G$ tel que $\mathbf{g}.x = y$ (puisque l'action de G sur X est transitive). On définit alors $\Theta(y) \stackrel{déf.}{=} \mathbf{g}.S_x = \mathbf{g}\top S_x$ (puisque G agit à gauche sur G/S_x).
Vérifions tout d'abord que Θ est bien définie :

$$\begin{array}{rlcl} & \mathbf{g}_1.x & = & \mathbf{g}_2.x \\ \Rightarrow & \mathbf{g}_2^{-1}\top\mathbf{g}_1.x & = & x \\ \Rightarrow & \mathbf{g}_2^{-1}\top\mathbf{g}_1 & \in & S_x \\ \Rightarrow & \mathbf{g}_1\top S_x & = & \mathbf{g}_2\top S_x \ . \end{array}$$

On voit ensuite que Θ est surjective. Ceci est clair puisque pour tout $\mathbf{g}\top S_x \in G/S_x$ c'est-à-dire $y = \mathbf{g}.x$ alors $\Theta(y) = \mathbf{g}\top S_x$.
Le fait que Θ soit injective se montre comme suit. Soit $(y_1, y_2) \in X^2$,

$$\begin{array}{rcl} \Theta(y_1) = \Theta(y_2) & \Rightarrow & \text{il existe } (\mathbf{g}_1, \mathbf{g}_2) \in G^2 \text{ tel que } y_1 = \mathbf{g}_1.x, y_2 = \mathbf{g}_2.x \text{ et } \mathbf{g}_1\top S_x = \mathbf{g}_2\top S_x \\ & \Rightarrow & \mathbf{h} \stackrel{déf.}{=} \mathbf{g}_2^{-1}\top\mathbf{g}_1 \in S_x \\ & \Rightarrow & y_1 = \mathbf{g}_1.x = \mathbf{g}_2\top\mathbf{h}.x = \mathbf{g}_2.x \text{ (puisque } \mathbf{h} \in S_x) \ = y_2 \ . \end{array}$$

Ainsi Θ est une application bijective.
Finalement on souhaite vérifier que $\Theta(\mathbf{g}.y) = \mathbf{g}.\Theta(y)$ pour tout $y \in X$ et tout $\mathbf{g} \in G$, ce qui impliquera par la définition 7.3 que les deux actions sont équivalentes. Soit alors $y \in X$ et on choisit $\mathbf{h} \in G$ tel que $\mathbf{h}.x = y$ alors $\Theta(y) = \mathbf{h}\top S_x$ (par définition). Pour $\mathbf{g} \in G$ on a $\mathbf{g}.y = \mathbf{g}\top\mathbf{h}.x$ et donc $\Theta(\mathbf{g}.y) = (\mathbf{g}\top\mathbf{h}).S_x = \mathbf{g}\top\mathbf{h}\top S_x$. Donc $\Theta(\mathbf{g}.y) = \mathbf{g}.(\mathbf{h}\top S_x) = \mathbf{g}.\Theta(y)$ comme exigé. □

De ce résultat on déduit les deux corollaires suivants.

Corollaire 7.1. [Wie64, Pas68] *Si un groupe fini G agit transitivement sur un ensemble fini non vide X alors pour $x \in X$,*

$$|X| = \frac{|G|}{|S_x|} \ .$$

En particulier, $|X|$ divise $|G|$.

Preuve. Puisque que l'action de G sur X est isomorphe à l'action de G sur G/S_x par translation à gauche, en particulier G et G/S_x sont de même cardinal et donc $|X| = |G/S_x| = \frac{|G|}{|S_x|}$. □

Corollaire 7.2. [Wie64, Pas68] *Chaque groupe G n'admet, à un isomorphisme près, qu'une seule action régulière.*

Preuve. Soient $\phi_1 : G \to S(X_1)$ et $\phi_2 : G \to S(X_2)$ deux actions régulières. En particulier $\forall x_1 \in X_1$, $S_{x_1} = \{e_G\}$ et $\forall x_2 \in X_2$, $S_{x_2} = \{e_G\}$. En effet, soient $i \in \{1, 2\}$ et $\mathbf{g} \in S_{x_i}$ pour $x_i \in X_i$. Alors, par définition, $\mathbf{g}.x_i = x_i$. Comme l'action est régulière, on sait qu'il existe un et un seul $\mathbf{h} \in G$ envoyant x_i sur lui-même et il s'agit de e_G. Donc $\mathbf{g} = e_G$ et $S_{x_i} = \{e_G\}$.
Puisque les actions ϕ_1 et ϕ_2 sont toutes deux régulières, elles sont aussi en particulier transitives. Elles sont donc chacune isomorphe à l'action de G sur G/S_{x_1} et respectivement sur G/S_{x_2} par translation à gauche pour $(x_1, x_2) \in X_1 \times X_2$ fixé (d'après la proposition 7.4). Or $G/S_{x_1} = G/\{e_G\} = G/S_{x_2}$ et $G/\{e_G\}$ est isomorphe à G lui-même. Ainsi les deux actions sont isomorphes à l'action de G sur lui-même par translation à gauche. □

Ce dernier résultat est important puisqu'il signifie que lorsque l'on connaît une action régulière pour un groupe G alors toutes les autres actions régulières opèrent de la même manière.

7.2.6 Formule des classes

Il est assez facile de voir que si G est un groupe fini agissant sur un ensemble fini non vide X alors pour tout $x \in X$, on a

$$|\mathcal{O}_G(x)| = \frac{|G|}{|S_x|} .$$

Puisque les orbites forment une partition de X, on a

$$|X| = \sum_{x \in A} |\mathcal{O}_G(x)|$$

où $A \subset X$ est un *système de représentants* des classes d'équivalence suivant $\equiv_G$ (les orbites) *i.e.* A contient un et un seul représentant de chacune des orbites[2]. Il en résulte finalement :

Proposition 7.5 (Formule des classes). [Wie64, Pas68] *Soit G un groupe fini agissant sur un ensemble fini non vide X. Soit A un système de représentants suivant la relation $\equiv_G$. Alors*

$$|X| = \sum_{x \in A} \frac{|G|}{|S_x|} .$$

7.2.7 Actions k-transitives

Définition 7.11. Soient $k \in \mathbb{N}^*$ et X un ensemble fini non vide. On définit l'ensemble des *k-uplets ordonnés de X* par

$$X^{(k)} \stackrel{déf.}{=} X^k \setminus \{x \in X^k | \exists (i,j) \in \{1,\dots,k\}^2 \text{ tel que } i \neq j \text{ et } x_i = x_j\} .$$

Une action d'un groupe G sur X est dite *k-transitive* si pour tout $((x_1,\dots,x_k),(y_1,\dots,y_k)) \in X^{(k)} \times X^{(k)}$ il existe au moins un élément $\mathbf{g} \in G$ tel que $\mathbf{g}.x_i = y_i$ pour tout $i \in \{1,\dots,k\}$.
L'action sera dite *simplement k-transitive* si l'élément $\mathbf{g}$ introduit au-dessus est unique.
En particulier les actions simplement 1-transitives sont les actions régulières déjà définies.

Exemple 7.3.

1. Soit X un ensemble fini non vide alors $S(X)$ agit $|X|$-transitivement sur X ;
2. Soit $\mathbb{K}$ un corps fini. Soit le groupe des droites affines de $\mathbb{K}$ noté « $GA(\mathbb{K})$ » dont les éléments $\delta_{\alpha,\beta}$, pour $(\alpha,\beta) \in \mathbb{K} \times \mathbb{K}^*$ sont définis par $\delta_{\alpha,\beta} \stackrel{déf.}{=} \sigma_\beta \circ \tau_\alpha$ *i.e.*

$$\begin{array}{rccc} \delta_{\alpha,\beta} : & \mathbb{K} & \to & \mathbb{K} \\ & x & \mapsto & \alpha x + \beta . \end{array}$$

   Alors $GA(\mathbb{K})$ agit simplement 2-transitivement sur $\mathbb{K}$.

7.2.8 Action par automorphisme de groupe

Définition 7.12. Soit (G,H) un couple de groupes tel qu'il existe un homomorphisme de groupes $\phi : G \to Aut(H)$. Alors on dit que *G agit sur le groupe H par automorphisme de groupe*.
L'action est dite *fidèle* si ϕ est injectif.
L'action est dite *semi-régulière* si pour tout $x \in H^*$, l'application orbitale ϕ_x de x est bijective de G dans H^*.

Une action par automorphisme de groupe est en particulier une action de groupe puisque $Aut(H)$ est un sous-groupe de $S(H)$.

[2] Il s'agit d'une application directe du fameux axiome du choix.

Remarque 7.3.

1. Une action d'un groupe G sur un groupe H par automorphisme de groupe ne peut jamais être régulière puisque tout élément de G fixe l'élément neutre de H. C'est la raison pour laquelle on considère la notion de semi-régularité ;
2. Soit $\phi : G \to Aut(H)$ un homomorphisme de groupes. Si l'action de G par automorphisme de groupe sur H (par ϕ) est semi-régulière alors, l'action de groupe de G sur l'ensemble H^*, définie par $\phi' : G \to S(H^*)$ avec $\forall \mathbf{g} \in G$, $\phi'(\mathbf{g}) = \phi(\mathbf{g})|_{H^*}$, est régulière. Pour voir cela il faut tout d'abord montrer que ϕ' est bien une action de groupe. Soit donc $x \in H^*$. Alors $\phi'(\mathbf{g})(x) = \phi(\mathbf{g})|_{H^*}(x) = \phi(\mathbf{g})(x) = \phi_x(\mathbf{g}) \in H^*$ (par semi-régularité). De plus comme $\forall \mathbf{g} \in G$, $\phi(\mathbf{g})(e_H) = e_H$ et $\phi(\mathbf{g}) \in Aut(H) \subset S(H)$, $\phi'(\mathbf{g}) \in S(H^*)$. Il est facile de voir que ϕ' est en outre un homomorphisme. Il s'ensuit que ϕ' correspond bien à une action de groupe. Reste à montrer que celle-ci est régulière. Soit donc $x \in H^*$. Alors l'application orbitale ϕ'_x de x est bijective car elle est égale à ϕ_x. L'action de groupe induite par ϕ' est donc régulière ;
3. Une action ϕ de G sur H semi-régulière est fidèle.

Proposition 7.6. *Soit $\mathbb{K}$ un corps fini. Le groupe multiplicatif $\mathbb{K}^*$ du corps $\mathbb{K}$ agit par automorphisme de groupe semi-régulièrement sur le groupe additif $(\mathbb{K}, +)$.*

Preuve. On rappelle que pour $\alpha \in \mathbb{K}^*$, la translation multiplicative est

$$\begin{array}{rccc} \tau_\alpha : & \mathbb{K} & \to & \mathbb{K} \\ & x & \mapsto & \alpha x \ . \end{array}$$

Il est facile de vérifier que puisque $\alpha \in \mathbb{K}^*$ alors $\tau_\alpha \in Aut(\mathbb{K}, +)$. Soit ϕ l'application définie par

$$\begin{array}{rccc} \phi : & \mathbb{K}^* & \to & Aut(\mathbb{K}, +) \\ & \alpha & \mapsto & \tau_\alpha \ . \end{array}$$

Montrons que ϕ est une action semi-régulière.
La fait que ϕ soit une action donc un homomorphisme de groupes est évident. Il suffit donc de montrer que $\forall x \in \mathbb{K}^*$, l'application orbitale de x est bijective. Or cette application correspond à une translation par x dans le groupe multiplicatif $\mathbb{K}^*$. Elle est donc bijective et l'action est ainsi semi-régulière. □

7.2.9 Action par automorphisme de corps fini

7.2.9.1 Automorphismes d'un corps fini

Dans cette sous-section, on souhaite faire agir un groupe sur un corps fini en utilisant explicitement la structure de corps et non celles des groupes sous-jacents.

Nous débutons donc par quelques rappels sur les automorphismes d'un corps fini. Les résultats exposés dans ce paragraphe étant classiques, les preuves sont admises. Le lecteur pourra consulter [Goz97] ou [PW94] pour de plus amples détails.

Définition 7.13. Soit $\mathbb{K}$ un corps et $\mathbb{F}$ une extension de $\mathbb{K}$. Un $\mathbb{K}$-*automorphisme* de $\mathbb{F}$ est un automorphisme (de corps) κ de $\mathbb{F}$ qui laisse invariant chaque élément du corps $\mathbb{K}$ *i.e.* tel que $\forall x \in \mathbb{K}$, $\kappa(x) = x$.

Proposition 7.7. [Goz97] *On note « $Gal(\mathbb{F}/\mathbb{K})$ » l'ensemble des $\mathbb{K}$-automorphismes du corps $\mathbb{F}$ (extension de $\mathbb{K}$). L'ensemble $Gal(\mathbb{F}/\mathbb{K})$ muni de la composition des applications est un groupe. On l'appelle le* groupe de Galois *de $\mathbb{F}$ sur $\mathbb{K}$.*

Proposition 7.8. [Goz97] *Soit* $\mathbb{F}$ *un corps et* $\mathbb{K}$ *son sous-corps premier. Alors* $Aut(\mathbb{F}) = Gal(\mathbb{F}/\mathbb{K})$.

Soient p un entier premier et $k \in \mathbb{N}^*$. On pose $\mathbb{K} \stackrel{déf.}{=} \mathbb{F}_{p^k}$ l'extension de degré k de $\mathbb{F}_p$.

Proposition 7.9. [Goz97] *Soit l'application suivante*

$$\begin{array}{rccc} \kappa_F : & \mathbb{K} & \to & \mathbb{K} \\ & x & \mapsto & x^p \ . \end{array}$$

Alors $\kappa_F \in Gal(\mathbb{K}/\mathbb{F}_p)$. *Il est appelé l'*automorphisme de Frobenius.

Théorème 7.1. [PW94] *Le groupe des automorphismes de* $\mathbb{K}$ *est d'ordre* $k = [\mathbb{K} : \mathbb{F}_p]$. *Il est cyclique. Il est engendré par l'automorphisme de Frobenius i.e.* $Aut(\mathbb{K}) = \langle \kappa_F \rangle = \{\kappa_F^i \in \mathbb{K}^{\mathbb{K}} | 0 \leq i \leq k-1\}$. *En particulier* $Aut(\mathbb{K})$ *est un groupe fini commutatif.*

7.2.9.2 Action sur un corps fini par automorphisme

Définition 7.14. Soit G un groupe et $\mathbb{K}$ un corps fini de caractéristique p. On dit que G *agit sur* $\mathbb{K}$ *par automorphisme de corps* s'il existe un homomorphisme de groupes

$$\phi : G \to Aut(\mathbb{K}) \ .$$

On dit, comme d'habitude, que l'action est *fidèle* si l'application ϕ est injective.

Si ϕ est une action par automorphisme de G sur $\mathbb{K}$ alors en particulier ϕ est une action de groupe de G sur l'ensemble sous-jacent au corps $\mathbb{K}$ (puisque $Aut(\mathbb{K})$ est un sous-groupe de $S(\mathbb{K})$). Si de plus l'action par automorphisme est fidèle, il en est évidemment de même de l'action de groupe correspondante.

Remarquons que les actions ainsi définies ne sont jamais *régulières* puisque pour tout $\mathbf{g} \in G$ et pour tout $x \in \mathbb{F}_p \subset \mathbb{K}$, on a $\phi(\mathbf{g})(x) = x$ (car les automorphismes de $\mathbb{K}$ laissent invariant les éléments de son sous-corps premier).

7.3 Non linéarité parfaite basée sur une action fidèle de groupe

7.3.1 Introduction

Les fonctions parfaitement non linéaires, au sens de Carlet et Ding (voir la section 6.4), sont ces fonctions $f : G \to H$ où G et H sont deux groupes finis commutatifs (notés additivement), telles que pour tout $(\alpha, \beta) \in G^* \times H$, on ait

$$|\{x \in G | f(x+\alpha) - f(x) = \beta\}| = \frac{|G|}{|H|} \ . \tag{7.1}$$

Manifestement, cette notion traduit le comportement d'une fonction soumise à l'action régulière du groupe G sur lui-même par translation. En effet, on peut observer que la formule (7.1) se ré-écrit comme suit :

$$|\{x \in G | f(\sigma_\alpha(x)) - f(x) = \beta\}| = \frac{|G|}{|H|} \tag{7.2}$$

avec $(\alpha, \beta) \in G^* \times H$. Il devient dès lors possible de ré-interpréter naturellement ce concept dans le cadre des actions de groupe. En utilisant ce nouveau point de vue, nous généralisons les notions classiques en les plongeant dans un cadre théorique à la fois plus général et plus fondamental. Soit en effet X un ensemble fini (non vide) sur lequel G agit de manière fidèle (on note « $\mathbf{g}.x$ » l'action de G sur X évaluée en $(\mathbf{g}, x) \in G \times X$). Alors en substituant les translations

dans l'équation (7.2) par l'action de G sur X, on obtient la forme généralisée suivante de la non linéarité parfaite pour une fonction $f : X \to H$

$$\forall(\mathbf{g}, \beta) \in G^* \times H,\ |\{x \in X | f(\mathbf{g}.x) - f(x) = \beta\}| = \frac{|X|}{|H|} .$$

Dans cette section, nous nous intéressons spécifiquement aux actions de groupe (fini abélien) fidèles. La relaxation de la contrainte de régularité permet, ainsi que nous allons le voir, de construire de nouveaux objets et d'obtenir une variante graduelle de la non linéarité parfaite. Dans le cas classique nous ne disposons que d'une seule version de la non linéarité parfaite basée sur l'action régulière par translation. Notre approche, en modifiant le degré de non régularité de l'action considérée, permet de définir un ensemble (discret) de variantes de la non linéarité parfaite. Ce premier axe de généralisation envisagé est symboliquement illustré par la figure suivante.

Cas classique $\longmapsto$ Défaut de régularité de l'action de G sur X

En utilisant une version tordue du produit de convolution de fonctions à valeurs complexes, nous caractérisons le nouveau concept à l'aide de la transformée de Fourier, ce qui par dualité, aboutit à une notion de fonction courbe généralisée et étend ainsi les résultats traditionnels.

Cette section est achevée par une sous-section dans laquelle nous exposons un exemple numérique de fonction parfaitement non linéaire au sens généralisé : la transformation S_{RD} de l'AES (voir le paragraphe 2.3.2.3 du chapitre 2).

7.3.2 Définitions

On se donne un triplet (G, H, X) dans lequel G et H sont deux groupes finis (H étant noté additivement) et X un ensemble fini non vide. On suppose de plus que G agit (au moins) **fidèlement** (à gauche) sur l'ensemble X (on note « $\mathbf{g}.x$ » cette action pour $(\mathbf{g}, x) \in G \times X$).

Remarque 7.4. Nous supposons presque toujours dans la suite du manuscrit, sauf mention contraire, que le groupe sur lequel les fonctions étudiées prennent leurs valeurs, ici H, est noté additivement afin d'utiliser l'abréviation « $y - y'$ » pour l'expression « $y + (-y')$ ». Nous indiquons cela via la notation « $(H, +)$ ». De même nous utilisons préférentiellement la notation pointée pour les actions de groupe rencontrées (hormis par exemple lorsque le groupe agissant sur un ensemble X est un sous-groupe de $S(X)$).

Définition 7.15. La *dérivée* de $f : X \to H$ dans la *direction* (ou *suivant*) $\mathbf{g} \in G$ est la fonction

$$\begin{array}{rccc} D_{\mathbf{g}} f : & X & \to & H \\ & x & \mapsto & f(\mathbf{g}.x) - f(x) . \end{array}$$

La notion classique de dérivée (voir la définition 6.4 p. 106) a donc été naturellement *tordue* afin de prendre en compte une action de groupe quelconque de préférence à l'action régulière par translation.

Logiquement, en recourant à la notion étendue de dérivation, la notion de non linéarité parfaite est généralisée comme suit.

Définition 7.16. Une fonction $f : X \to H$ est dite *G-parfaitement non linéaire* si pour tout $\mathbf{g} \in G^*$, la dérivée $D_{\mathbf{g}}f$ est équilibrée *i.e.* $\forall(\mathbf{g}, \beta) \in G^* \times H$,

$$|\{x \in X | f(\mathbf{g}.x) - f(x) = \beta\}| = \frac{|X|}{|H|} .$$

Puisque l'action de G sur X est (au minimum) fidèle on sait qu'il n'existe pas de $\mathbf{g} \in G^*$ se comportant comme l'identité dans son action sur X. Ainsi il n'existe pas de $\mathbf{g} \in G^*$ tel que l'application

$$\begin{array}{rccc} D_{\mathbf{g}} : & H^X & \to & H^X \\ & f & \mapsto & D_{\mathbf{g}}f \end{array}$$

soit l'identité Id_{H^X}.

Remarque 7.5.

1. Cette définition reste valide même lorsque G est un groupe non abélien agissant à gauche sur X ;
2. Pour qu'une fonction $f \in H^X$ soit G-parfaitement non linéaire, il est bien entendu nécessaire que $|H|$ divise $|X|$;
3. Si le groupe agissant G est réduit à son élément neutre *i.e.* $G = \{e_G\}$, alors on parle de cas *trivial*. Dans cette situation toute fonction est G-parfaitement non linéaire puisque $G^* = \emptyset$;
4. Dans la suite, les références à cette notion seront en pratique effectuées par l'emploi du vocable informel « G-non linéarité parfaite » dans lequel la lettre « G » a parfois le rôle d'une variable muette désignant un groupe. On parlera aussi de non linéarité parfaite *originale*, *classique* ou *traditionnelle*, comme nous l'avons déjà fait, afin de désigner les notions présentées aux chapitres 5 et 6, et pour les distinguer des nôtres, qui sont alors qualifiées de *nouvelles*, *étendues* ou *généralisées*.

Cette approche, en utilisant une action seulement fidèle, nous permet de décrire de nouveaux objets combinatoires en jouant sur le *défaut de régularité* de l'action considérée. En effet, si par exemple $|G|$ est plus petit que $|X|$ alors le nombre d'équations que doit satisfaire une fonction afin d'être G-parfaitement non linéaire est aussi inférieur au nombre de contraintes de la non linéarité parfaite classique. Le degré de liberté ainsi obtenu par relaxation des contraintes doit logiquement nous conduire à la description d'une plus large classe d'objets. Par ailleurs, le nouveau concept proposé ici est plus flexible et graduel que l'approche traditionnelle. Dans un modèle théorique générique, il est désormais possible de décrire différentes variantes de la non linéarité parfaite, de la plus simple - l'action fidèle d'un groupe réduit à deux éléments - à la plus complexe : l'action régulière.

La proposition suivante illustre ce point de vue.

Proposition 7.10. *Soient G un groupe fini agissant fidèlement sur un ensemble (fini non vide) X, via l'homomorphisme $\phi : G \to S(X)$ et $(H, +)$ un groupe fini commutatif. Soit $f : X \to H$. Si la fonction f est G-parfaitement non linéaire alors pour tout G' sous-groupe de G, la fonction f est G'-parfaitement non linéaire (l'action de G' sur X étant définie par $\phi|_{G'}$ la restriction de ϕ à G').*

Preuve. L'homomorphisme $\phi|_{G'}$ de G' sur $S(X)$ est évidemment injectif (puisque l'action de G sur X est fidèle). Soit alors $(\mathbf{g}, \beta) \in G'^* \times H$. On a $|\{x \in X | f(\phi|_{G'}(\mathbf{g})(x)) - f(x) = \beta\}| = |\{x \in X | f(\phi(\mathbf{g})(x)) - f(x) = \beta\}| = \frac{|X|}{|H|}$ (puisque f est G-parfaitement linéaire). □

On peut interpréter cette proposition comme une extension des critères de propagation. En effet, si une fonction donnée est G-parfaitement non linéaire alors elle est aussi G'-parfaitement non linéaire pour tout G' sous-groupe de G. Néanmoins rien ne l'oblige à l'être par rapport à un autre groupe fini contenant G en tant que sous-groupe. Nous obtenons ainsi une « tour » de genres possibles de non linéarité parfaite ou mieux, une relation d'ordre entre fonctions. En ce sens les fonctions parfaitement non linéaires classiques, lorsqu'elles existent, sont les éléments maximaux. L'exemple suivant décrit par contre les éléments minimaux.

Exemple 7.4. Soit X un ensemble fini tel que $|X| \geq 4$ et $|X| \equiv 0 \pmod 4$. Soit $\boldsymbol{\sigma} \in S(X)$ une involution sans point fixe (voir dans l'annexe B la définition B.1) et $G \stackrel{déf.}{=} \langle \boldsymbol{\sigma} \rangle = \{Id_X, \boldsymbol{\sigma}\}$ le groupe (abélien) engendré par $\boldsymbol{\sigma}$. Puisque $\forall x \in X, \boldsymbol{\sigma}(x) \neq x$, l'action de G sur X est fidèle. Les orbites sous l'action de G sont de la forme $\{x, \boldsymbol{\sigma}(x)\}$ et partitionnent X en sous-ensembles de cardinal 2. Soit $A \subset X$ un système de représentants des orbites *i.e.* A contient exactement un et un seul représentant de chacune des orbites. Donc en particulier $|A| = \dfrac{|X|}{2}$. Par hypothèse sur X, $|A|$ est un entier pair. Ainsi nous pouvons choisir une partition de A en deux sous-ensembles A_1 et A_2 telle que $|A_1| = |A_2| = \dfrac{|X|}{4}$. On a donc $\boldsymbol{\sigma}(A_k) = \{\boldsymbol{\sigma}(x) \in X | x \in A_k\}$ pour tout $k \in \{1, 2\}$. On peut alors commodément vérifier que $\{A_1, A_2, \boldsymbol{\sigma}(A_1), \boldsymbol{\sigma}(A_2)\}$ est une partition de X avec $|A_k| = |\boldsymbol{\sigma}(A_k)| = \dfrac{|H|}{4}$ pour tout $k \in \{1, 2\}$. Soient $\beta \in \mathbb{F}_2$ et une fonction $f : X \to \mathbb{F}_2$ telle que $\forall x \in A_1$, $f(x) = f(\boldsymbol{\sigma}(x)) = \beta$, $\forall x \in A_2$, $f(x) = \beta$ et $f(\boldsymbol{\sigma}(x)) = 1 \oplus \beta$, autrement dit, $f = \beta \mathbf{1}_{(\boldsymbol{\sigma}(A_2))^c} \oplus (1 \oplus \beta)\mathbf{1}_{\boldsymbol{\sigma}(A_2)}$ (où $\mathbb{F}_2$ est plongé dans $\mathbb{R}$). Alors nous avons

1. $|\{x \in X | f(\boldsymbol{\sigma}(x)) \oplus f(x) = 0\}| = |A_1| + |\boldsymbol{\sigma}(A_1)| = \dfrac{|X|}{2}$;
2. $|\{x \in X | f(\boldsymbol{\sigma}(x)) \oplus f(x) = 1\}| = |A_2| + |\boldsymbol{\sigma}(A_2)| = \dfrac{|X|}{2}$.

Ainsi f est G-parfaitement non linéaire.

7.3.3 Caractérisation à l'aide de la transformée de Fourier

La motivation profonde de cette sous-section réside dans la transformation de la propriété combinatoire définie précédemment en une loi de type « conservation de l'énergie » par l'exploitation des techniques de l'analyse de Fourier (ou analyse harmonique des groupes finis). De ce fait, nous obtenons une version duale la G-non linéarité parfaite conduisant naturellement à un concept de fonction courbe généralisée. En bref, nous étendons les résultats de la section 6.4 du chapitre 6 en les déclinant au cas des actions fidèles de groupe fini abélien.

Afin d'aboutir à la caractérisation en termes de transformées de Fourier, nous introduisons une version « tordue » du produit de convolution des fonctions à valeurs complexes, en remplaçant les translations par l'action d'un groupe G sur X.

Définition 7.17. Soit G un groupe fini agissant (fidèlement) à gauche sur un ensemble fini non vide X. Soit $(\varphi, \psi) \in (\mathbb{C}^X)^2$. On définit le *$G$-produit de convolution* de φ et ψ par

$$\begin{array}{rccl} \varphi \bigstar \psi : & G & \to & \mathbb{C} \\ & \mathbf{g} & \mapsto & (\varphi \bigstar \psi)(\mathbf{g}) \stackrel{déf.}{=} \displaystyle\sum_{x \in X} \overline{\varphi(x)} \psi(\mathbf{g}.x) \end{array}$$

où l'on rappelle que « $\bar{\mathtt{z}}$ » désigne le conjugué du nombre complexe $\mathtt{z}$.

Ce produit n'est pas forcément symétrique puisque l'on a pour tout $\mathbf{g} \in G$, $(\varphi \bigstar \psi)(\mathbf{g}) = (\overline{\psi} \bigstar \overline{\varphi})(\mathbf{g}^{-1})$.

Le nom de « produit de convolution » n'est pas simplement dû à la forte ressemblance avec l'analogue classique. En effet, ainsi que nous le détaillons ci-dessous, la transformée de Fourier trivialise en un certain sens ce produit.

A partir de maintenant et jusqu'à la fin de cette sous-section, on se donne un triplet $((G,\top),(H,+),X)$ dans lequel G et H sont deux groupes finis abéliens et X un ensemble fini non vide. On suppose de plus que G agit (au moins) **fidèlement** sur l'ensemble X.

Calculons la transformée de Fourier du G-produit de convolution de $(\varphi,\psi)\in(\mathbb{C}^X)^2$. Soit $\mathbf{g}\in G$.

$$\begin{aligned}\widehat{\varphi\bigstar\psi}(\mathbf{g}) &= \sum_{\mathbf{h}\in G}(\varphi\bigstar\psi)(\mathbf{h})\chi_G^{\mathbf{g}}(\mathbf{h})\\ &= \sum_{\mathbf{h}\in G}\sum_{x\in X}\overline{\varphi(x)}\psi(\mathbf{h}.x)\chi_G^{\mathbf{g}}(\mathbf{h})\\ &= \sum_{x\in X}\overline{\varphi(x)}\sum_{\mathbf{h}\in G}\psi(\mathbf{h}.x)\chi_G^{\mathbf{g}}(\mathbf{h})\ . \qquad (7.3)\end{aligned}$$

La somme

$$\sum_{\mathbf{h}\in G}\psi(\mathbf{h}.x)\chi_G^{\mathbf{g}}(\mathbf{h})$$

satisfait la propriété suivante pour chaque $\mathbf{k}\in G$.

$$\sum_{\mathbf{h}\in G}\psi(\mathbf{h}.x)\chi_G^{\mathbf{g}}(\mathbf{h})=\sum_{\mathbf{h}\in G}\psi(\mathbf{h}\top\mathbf{k}.x)\chi_G^{\mathbf{g}}(\mathbf{h}\top\mathbf{k})=\sum_{\mathbf{h}\in G}\psi(\mathbf{h}\top\mathbf{k}.x)\chi_G^{\mathbf{g}}(\mathbf{h})\chi_G^{\mathbf{g}}(\mathbf{k})\ .$$

Alors pour tout $\mathbf{k}\in G$ on obtient

$$\begin{aligned}(7.3) &= \sum_{x\in X}\overline{\varphi(x)}\chi_G^{\mathbf{g}}(\mathbf{k})\sum_{\mathbf{h}\in G}\psi(\mathbf{h}\top\mathbf{k}.x)\chi_G^{\mathbf{g}}(\mathbf{h})\\ &= \sum_{y\in X}\overline{\varphi(\mathbf{k}^{-1}.y)}\chi_G^{\mathbf{g}}(\mathbf{h})\sum_{\mathbf{h}\in G}\psi(\mathbf{h}.y)\chi_G^{\mathbf{g}}(\mathbf{h})\ \text{(par le changement de variables : } y\overset{déf.}{=}\mathbf{k}.x)\\ &= \sum_{y\in X}\overline{\varphi(\mathbf{k}^{-1}.y)}\chi_G^{\mathbf{g}}(\mathbf{k})\widehat{\psi_y}(\mathbf{g})\end{aligned}$$

où l'on a défini la fonction

$$\begin{aligned}\psi_y:\ G &\to \mathbb{C}\\ \mathbf{g} &\mapsto \psi_y(\mathbf{g})\overset{déf.}{=}\psi(\mathbf{g}.y)\ .\end{aligned}$$

La substitution de $\mathbf{k}$ par $\mathbf{k}^{-1}$ et l'intégration sur G tout entier conduisent à

$$\begin{aligned}\sum_{\mathbf{k}\in G}\widehat{\varphi\bigstar\psi}(\mathbf{g}) &= |G|\widehat{\varphi\bigstar\psi}(\mathbf{g})\\ &= \sum_{x\in X}\sum_{\mathbf{k}\in G}\overline{\varphi(\mathbf{k}.x)}\chi_G^{\mathbf{g}}(\mathbf{k}^{-1})\widehat{\psi_x}(\mathbf{g})\\ &= \sum_{x\in X}\sum_{\mathbf{k}\in G}\overline{\varphi(\mathbf{k}.x)\chi_G^{\mathbf{g}}(\mathbf{k})}\widehat{\psi_x}(\mathbf{g})\\ &= \sum_{x\in X}\overline{\widehat{\varphi_x}(\mathbf{g})}\widehat{\psi_x}(\mathbf{g})\ .\end{aligned}$$

Avec, comme pour ψ_x,

$$\begin{array}{rccc} \varphi_x : & G & \to & \mathbb{C} \\ & \mathbf{g} & \mapsto & \varphi(\mathbf{g}.x) \ . \end{array}$$

Finalement nous obtenons la trivialisation suivante du G-produit de convolution

$$\forall \mathbf{g} \in G,\ \widehat{\varphi \bigstar \psi}(\mathbf{g}) = \frac{1}{|G|} \sum_{x \in X} \overline{\widehat{\varphi_x}(\mathbf{g})} \widehat{\psi_x}(\mathbf{g}) \ . \tag{7.4}$$

Avant d'aller plus loin, nous introduisons la définition suivante, généralisant les notations « φ_x » et « ψ_x ».

Définition 7.18. Soit G un groupe agissant à gauche sur un ensemble non vide X via l'homomorphisme de groupes ϕ de G dans $S(X)$. Soit Y un autre ensemble non vide. Pour $f : X \to Y$ et $x \in X$, on définit la fonction $f_x \in Y^G$ par $f_x \stackrel{déf.}{=} f \circ \phi_x$ où l'on rappelle que ϕ_x est l'application orbitale de x.

Nous utilisons maintenant le G-produit de convolution ainsi que sa trivialisation afin de démontrer la proposition suivante.

Proposition 7.11. *Soit G un groupe fini commutatif agissant fidèlement sur un ensemble fini non vide X. Soit $(H, +)$ un groupe fini commutatif. Soient $f : X \to H$ et $\beta \in H$. On définit l'application*

$$\begin{array}{rccc} AC_{f,\beta} : & G & \to & \mathbb{C} \\ & \mathbf{g} & \mapsto & \displaystyle\sum_{x \in X} (\chi_H^\beta \circ D_{\mathbf{g}} f)(x) \ . \end{array}$$

Alors on a $\forall \mathbf{g} \in G$,

$$\widehat{AC_{f,\beta}}(\mathbf{g}) = \frac{1}{|G|} \sum_{x \in X} |\widehat{\chi_H^\beta \circ f_x}(\mathbf{g})|^2 \ .$$

Preuve. Pour voir cela il suffit de calculer la transformée de Fourier de $AC_{f,\beta}$. Soit donc $\mathbf{g} \in G$.

$$\begin{aligned} \widehat{AC_{f,\beta}}(\mathbf{g}) &= \sum_{\mathbf{h} \in G} AC_{f,\beta}(\mathbf{h}) \chi_G^{\mathbf{g}}(\mathbf{h}) \\ &= \sum_{\mathbf{h} \in G} \sum_{x \in X} (\chi_H^\beta \circ D_{\mathbf{g}} f)(x) \chi_G^{\mathbf{g}}(\mathbf{h}) \\ &= \sum_{\mathbf{h} \in G} \sum_{x \in X} \chi_H^\beta(f(\mathbf{h}.x) - f(x)) \chi_G^{\mathbf{g}}(\mathbf{h}) \\ &= \sum_{\mathbf{h} \in G} \sum_{x \in X} \overline{(\chi_H^\beta \circ f)(x)} (\chi_H^\beta \circ f)(\mathbf{h}.x) \chi_G^{\mathbf{g}}(\mathbf{h}) \\ &= \sum_{\mathbf{h} \in G} (\chi_H^\beta \circ f \bigstar \chi_H^\beta \circ f)(\mathbf{h}) \chi_G^{\mathbf{g}}(\mathbf{h}) \\ &= (\chi_H^\beta \circ \widehat{f \bigstar \chi_H^\beta} \circ f)(\mathbf{g}) \\ &= \frac{1}{|G|} \sum_{x \in X} \overline{(\widehat{\chi_H^\beta \circ f})_x(\mathbf{g})} (\widehat{\chi_H^\beta \circ f})_x(\mathbf{g}) \text{ (d'après la formule (7.4))} \\ &= \frac{1}{|G|} \sum_{x \in X} |(\widehat{\chi_H^\beta \circ f})_x(\mathbf{g})|^2 \\ &= \frac{1}{|G|} \sum_{x \in X} |\widehat{\chi_H^\beta \circ f_x}(\mathbf{g})|^2 \ . \end{aligned}$$

□

Le théorème suivant est sans doute l'un des plus importants de cette section puisqu'il nous permet d'utiliser la transformée de Fourier afin d'identifier les fonctions G-parfaitement non linéaires.

Théorème 7.2. *Soit (G, X, H) un triplet dans lequel G et H sont deux groupes finis commutatifs et X un ensemble fini non vide. Supposons que G agisse (au moins) fidèlement sur X. Soit $f : X \to H$. La fonction f est G-parfaitement non linéaire si et seulement si $\forall \mathbf{g} \in G$, $\forall \beta \in H^*$,*

$$\sum_{x \in X} |\widehat{\chi_H^\beta \circ f_x}(\mathbf{g})|^2 = |G||X| \ .$$

Preuve.
La fonction f est G-parfaitement non linéaire
$\Leftrightarrow \forall \mathbf{g} \in G^*$, la dérivée $D_{\mathbf{g}} f$ est équilibrée (par définition)
$\Leftrightarrow \forall \mathbf{g} \in G^*, \forall \beta \in H^*, \sum_{x \in X} (\chi_H^\beta \circ D_{\mathbf{g}} f))(x) = 0$ (d'après la proposition 6.7 p. 108)
$\Leftrightarrow \forall \beta \in H^*, \forall \mathbf{g} \in G^*, AC_{f,\beta}(\mathbf{g}) = 0$
$\Leftrightarrow \forall \beta \in H^*, \widehat{AC_{f,\beta}}$ est constant sur G (d'après le lemme 6.3 p. 105).

Au moyen de la relation de Parseval (formule 6.4 p. 105), on obtient $\frac{1}{|G|} \sum_{\mathbf{g} \in G} |\widehat{AC_{f,\beta}}(\mathbf{g})|^2 = \sum_{\mathbf{g} \in G} |AC_{f,\beta}(\mathbf{g})|^2 = |AC_{f,\beta}(e_G)|^2$. Ainsi puisque $\widehat{AC_{f,\beta}}$ est constant, $|\widehat{AC_{f,\beta}}(\mathbf{g})|^2 = |AC_{f,\beta}(e_G)|^2$ pour tout $\mathbf{g} \in G$. De plus $AC_{f,\beta}(e_G) = \sum_{x \in X} (\chi_H^\beta \circ D_{e_G} f))(x) = \sum_{x \in X} \chi_H^\beta(e_H) = |X|$. Alors d'après la proposition 7.11 on en déduit le résultat qu'il fallait démontrer. □

Ce résultat représente l'analogue du théorème 6.5 p. 109, énoncé par Carlet et Ding [CD04]. La différence la plus notable, outre l'utilisation des fonctions f_x, est le fait de ne pas disposer d'une caractérisation indépendante pour chacune de ces fonctions mais d'une sorte d'espérance mathématique. A la lecture de ce théorème, nous pouvons simplement dire, qu'en moyenne, les fonctions f_x sont courbes au sens de Logachev, Salnikov et Yachshenko (voir section 6.5). Ceci est essentiellement dû au fait que l'action considérée n'est pas régulière, ainsi toutes les orbites selon cette action ne jouent pas identiquement le même rôle. On pourrait se poser la question de savoir si $\sum_{x \in X} |\widehat{\chi_H^\beta \circ f_x}(\mathbf{g})|^2 = |G||X|$ implique que pour tout $x \in X$, $|\widehat{\chi_H^\beta \circ f_x}(\mathbf{g})|^2 = |G|$, soit en d'autres termes, $\forall x \in X$, la fonction $f_x : G \to H$ est parfaitement non linéaire au sens de Carlet et Ding. Néanmoins dans la dernière partie de ce chapitre, nous exposons un contre-exemple à cela (cf. la construction de G-ensemble à différences *hyperplan* p. 164). Nous verrons aussi ultérieurement, dans la section 7.4, que lorsqu'est considérée une action régulière, on obtient une caractérisation bien plus précise et très similaire à celle du cas classique.

7.3.4 Non linéarité parfaite basée sur une action par automorphisme de corps fini

Nous avions observé dans l'exemple 5.1 p. 96 que l'application $\boldsymbol{\sigma}_{inv}$, représentant essentiellement l'inverse dans un corps $\mathbb{F}_{2^m}$, est une involution presque parfaitement non linéaire. Cette fonction est d'ailleurs utilisée dans l'AES comme composante de la transformation S_{RD} (cf. chapitre 2).

Dans cette sous-section, nous montrons, à l'aide d'une analyse numérique, que S_{RD}, en plus de posséder une bonne diffusion, est aussi parfaitement non linéaire au sens généralisé par rapport à une action par automorphisme de corps.

Soit $(p,k) \in (\mathbb{N}^*)^2$ tel que p soit premier. Soit $\mathbb{K} \stackrel{déf.}{=} \mathbb{F}_{p^k}$. Soit $(H,+)$ un groupe fini commutatif. Le groupe des automorphismes de corps de $\mathbb{K}$, $Aut(\mathbb{K}) = \{\kappa_F^i \in \mathbb{K}^{\mathbb{K}} | i \in \{0,\ldots,k-1\}\}$, où l'on rappelle que κ_F est l'automorphisme de Frobenius, agit évidemment fidèlement sur $\mathbb{K}$ par automorphisme de corps. Dans ce cas, une fonction $f : \mathbb{K} \to H$ est $Aut(\mathbb{K})$-parfaitement non linéaire si $\forall i \in \{1,\ldots,k-1\}$, $\forall \beta \in H$, $|\{x \in \mathbb{K} | f(x^{p^i}) - f(x) = \beta| = \dfrac{p^k}{|H|}$.

Afin d'illustrer cette notion sont maintenant présentés des résultats numériques. Pour ce faire, plaçons-nous dans le cas où $p = 2$, $k = 8$ (donc $\mathbb{K} = \mathbb{F}_{2^8} = \mathbb{F}_{256}$) et $H = \mathbb{F}_2$. En particulier $Aut(\mathbb{F}_{256}) = \{\kappa_F^i \in \mathbb{F}_{256}^{\mathbb{F}_{256}} | i \in \{0,\ldots,7\}\}$ avec le Frobenius $\kappa_F : x \mapsto x^2$. Ainsi une fonction $f : \mathbb{F}_{256} \to \mathbb{F}_2$ est $Aut(\mathbb{F}_{256})$-parfaitement non linéaire si pour tout $i \in \{1,\ldots,7\}$ et pour tout $\beta \in \mathbb{F}_2$, $|\{x \in \mathbb{F}_{256} | f(x^{2^i}) \oplus f(x) = \beta\}| = 2^7 = 128$.

Etudions une fonction f particulière, donnant d'étonnants résultats. Il s'agit, comme indiqué en préambule, de la transformation S_{RD}. Nous avons déjà succinctement évoqué cette fonction au chapitre 2. Il nous faut maintenant la détailler avec une précision chirurgicale.

On rappelle tout d'abord la définition de la fonction $\boldsymbol{\sigma}_{inv} : \mathbb{F}_{256} \to \mathbb{F}_{256}$. Elle est déterminée pour $x \in \mathbb{F}_{256}$ par

$$\boldsymbol{\sigma}_{inv}(x) = \begin{cases} x^{-1} & \text{si } x \in \mathbb{F}_{256}^* \ , \\ 0_{\mathbb{F}_{256}} & \text{si } x = 0_{\mathbb{F}_{256}} \ . \end{cases}$$

L'inverse dans le corps fini $\mathbb{F}_{256}$ dépend naturellement du polynôme primitif choisi pour représenter le corps. Dans le cas de l'algorithme Rijndael, il s'agit de $P(\mathtt{X}) = \mathtt{X}^8 \oplus \mathtt{X}^4 \oplus \mathtt{X}^3 \oplus \mathtt{X} \oplus 1$.

Soit ensuite $\delta : \mathbb{F}_{256} \to \mathbb{F}_{256}$ la transformation affine non singulière définie par la relation matricielle suivante.

$$y = \delta(x) \Leftrightarrow \begin{pmatrix} y_8 \\ y_7 \\ y_6 \\ y_5 \\ y_4 \\ y_3 \\ y_2 \\ y_1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix} \times \begin{pmatrix} x_8 \\ x_7 \\ x_6 \\ x_5 \\ x_4 \\ x_3 \\ x_2 \\ x_1 \end{pmatrix} \oplus \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \end{pmatrix} .$$

Finalement $S_{RD} : \mathbb{F}_{256} \to \mathbb{F}_{256}$ est définie par $S_{RD} \stackrel{déf.}{=} \delta \circ \boldsymbol{\sigma}_{inv}$. Ses propriétés de non linéarité reposent évidemment sur celles de la fonction $\boldsymbol{\sigma}_{inv}$.

Pour $x \in \mathbb{F}_{2^8}$, on rappelle que $(\Theta_8^d)^{-1}(x) \in \mathbb{F}_2^8$ est l'octet correspondant à la représentation usuelle de x en base deux (où x est considéré comme un entier modulo 256) où le bit de poids fort est à droite (chapitre 4 formule (4.5) p. 47).

Finalement, on définit la fonction $f : \mathbb{F}_{256} \to \mathbb{F}_2^8$ par $f \stackrel{déf.}{=} (\Theta_8^d)^{-1} \circ S_{RD} = (\Theta_8^d)^{-1} \circ \delta \circ \boldsymbol{\sigma}_{inv}$. Pour tout $j \in \{1,\ldots,8\}$ et pour tout $i \in \{1,\ldots,7\}$, les cardinaux $|\{x \in \mathbb{F}_{256} | f_j(x^{2^i}) \oplus f_j(x) = 0\}|$ ont été numériquement calculés afin d'étudier la non linéarité parfaite éventuelle relativement à $Aut(\mathbb{F}_{256})$ des fonctions coordonnées $f_j : \mathbb{F}_{256} \to \mathbb{F}_2$. Ces résultats nous apprennent d'une part que pour chaque $j \in \{1,\ldots,8\} \setminus \{7\}$, la fonction f_j est $Aut(\mathbb{F}_{256})$-parfaitement non linéaire et, d'autre part, que pour f_7 nous avons

$$|\{x \in \mathbb{F}_{256} | f_7(x^{2^i}) \oplus f_7(x) = 0\}| = \begin{cases} 128 & \text{si } i \neq 4 \ , \\ 256 & \text{sinon} \ . \end{cases}$$

Par ailleurs, et toujours à l'aide d'une analyse numérique, on vérifie qu'aucune des fonctions coordonnées f_j n'est parfaitement non linéaire au sens classique. Nous disposons donc d'un exemple de fonction parfaitement non linéaire au sens des actions fidèles mais pas au sens classique. Dans la suite, nous exhibons d'autres constructions de telles fonctions, de manière formelle donc non numérique.

7.3.5 Conclusion

La non linéarité parfaite, notion fort pertinente en cryptographie, a été raffinée de façon très naturelle, en considérant les additions figurant dans sa définition classique comme un cas particulier d'actions de groupe : l'action par translation. Se faisant nous lui offrons un cadre à la fois plus général, plus souple et plus précis.

Dans cette section, nous nous sommes délibérement restreints à une seule hypothèse, très faible, sur les actions exploitées : leur fidélité. En relâchant les contraintes, nous disposons désormais d'une théorie de la non linéarité parfaite se déclinant et décrivant de manière *continue*[3] et dans une même unité logique toute une série de configurations[4].

Par ailleurs, une caractérisation, pour ce nouveau concept, à l'aide de la transformée de Fourier a aussi été obtenue, étendant naturellement un résultat classique sur les fonctions courbes. Ainsi une fonction vérifiant la G-non linéarité parfaite, pour G un groupe agissant fidèlement sur un certain ensemble, est *courbe en moyenne*. Ceci illustre le défaut de régularité (ou, plus rigoureusement, de transitivité) des actions considérées. Dans la section suivante, notre intérêt se porte sur les actions de groupe régulières, ce qui nous permet d'établir des résultats très similaires aux cas traditionnels.

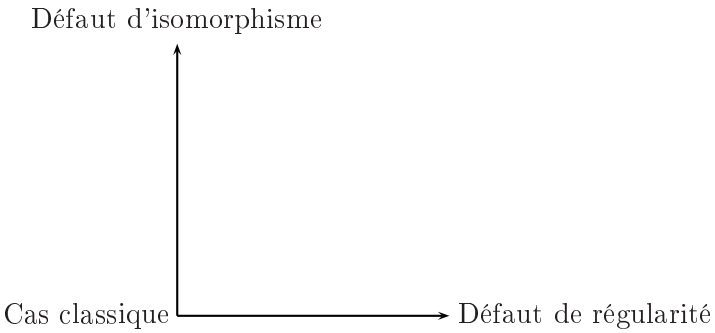
7.4 Non linéarité parfaite basée sur une action régulière de groupe

7.4.1 Introduction

L'absence de régularité de l'action de groupe, ainsi que nous venons le voir, nous permet de décliner la non linéarité parfaite sous plusieurs versions selon le groupe agissant. Il s'agit donc d'une généralisation selon une première direction. Nous négocions maintenant un virage *sinistrorsum*[5] d'angle $\frac{\pi}{2}$ par rapport à ce que nous venons de voir. Dorénavant nous imposons aux actions considérées d'être régulières. Cette distinction avec le cas évoqué dans la section précédente est décisive ainsi que nous l'observons immédiatement avec la caractérisation « duale » du concept généralisé. Toute chose étant égale par ailleurs, nous faisons maintenant varier un nouveau paramètre : la forme du groupe agissant ou plus précisément son degré ou son défaut d'isomorphisme avec un certain groupe de translations. Une action régulière se matérialise en effet de deux façons principales, selon que l'action est équivalente ou non à l'action par translation. Donnons-nous G, H_1 et H_2 trois groupes finis commutatifs tels que G agisse régulièrement sur l'ensemble sous-jacent à H_1 et attachons-nous à la description des fonctions G-parfaitement non linéaires de $H_2^{H_1}$. Evidemment dans son action régulière sur H_1, G est toujours isomorphe à l'action par translation sur lui-même (puisque pour chaque groupe il n'existe essentiellement qu'une seule action régulière). Néanmoins elle n'est pas obligatoirement équivalente à celle de $T(H_1)$ sur H_1 selon que G est ou non isomorphe à H_1 (ou $T(H_1)$). C'est ce que l'on veut dire lorsque nous parlons

[3] L'expression « discrète et de granularité très fine » serait plus juste mais tellement moins éloquente !
[4] Lesquelles configurations n'étant précisément pas formulables dans le cadre conceptuel conventionnel.
[5] Dans le sens direct.

de *défaut d'isomorphisme*. Il ne faut pas sous-estimer cette distinction fondamentale puisqu'elle nous permet de construire deux catégories de fonctions en rapport au défaut d'équivalence du groupe agissant avec les translations du groupe sur lequel on agit. Combiné à la notion étudiée dans la section précédente, nous voyons poindre un nouveau demi-axe de généralisation sur notre schéma précédent représentant désormais symboliquement un quart de plan.



L'origine du « repère », annotée par l'expression *cas classique*, permet de mesurer le défaut d'isomorphisme comme suit. Le fait de s'éloigner de l'origine suivant l'axe des ordonnées revient à affirmer que le groupe agissant G n'est pas isomorphe à $T(H_1)$ dans son action sur l'ensemble sous-jacent à un groupe H_1.

Le contenu de l'annexe B constitue une étude exhaustive d'une instance particulière - dans le cas booléen - de la non linéarité parfaite basée sur une action de groupe régulière, notion étudiée de manière systématique dans cette section. Le groupe des translations de $\mathbb{F}_2^m$ ayant été remplacé par un *groupe maximal d'involutions*. Observons que dans cette situation bien précise, les fonctions parfaitement non linéaires obtenues sont *isomorphes* à celles du cas usuel. Néanmoins nous montrons dans cette section que ce n'est pas toujours vrai. Ainsi nous exhibons une fonction $f : \mathbb{Z}_{16} \to \mathbb{F}_2$ qui est $\mathbb{F}_2^4$-parfaitement non linéaire mais non parfaitement non linéaire au sens classique. Ceci illustre pertinemment le fait que même lorsque l'action régulière n'est pas équivalente à une action par translation (ce qui est le cas de l'action de $\mathbb{F}_2^4$ sur $\mathbb{Z}_{16}$ et celle par translation de $\mathbb{Z}_{16}$ sur lui-même ainsi que nous allons le montrer), il est possible de construire des fonctions G-parfaitement non linéaires dont il est légitime d'espérer qu'elles ne soient pas parfaitement non linéaires[6].

La définition de G-non linéarité parfaite, lorsque G est un groupe fini abélien, régulier dans son action sur un ensemble X, ne varie pas de celle exposée dans la section précédente, simplement la régularité nous autorise à préciser la caractérisation de cette notion à l'aide de la transformée de Fourier de manière plus appropriée et véritablement analogue au concept de fonction courbe. Notons que pour établir cela, contrairement aux actions fidèles, à aucun moment nous ne supposons l'ensemble X muni d'une structure de groupe. C'est ce que l'on gagne grâce à la régularité. Toutefois cette hypothèse est effectuée plus loin dans cette section. Cette exigence étant capitale pour l'étude des liens entre la nouvelle notion et celle de Carlet et Ding. Mais allons donc *droit au but* dans la caractérisation précise de ce type de fonctions.

[6]Nous démontrons cette assertion pour la construction exhibée.

7.4.2 Caractérisation à l'aide de la transformée de Fourier

Si l'on suppose l'action régulière, le produit de convolution « tordu », ainsi que sa trivialisation, ne sont plus indispensables afin d'établir le concept analogue de fonction courbe. Nous pouvons donc, sans artifice technique, énoncer sur-le-champ le résultat suivant.

Théorème 7.3. *Soit $((G,\top),X,(H,+))$ un triplet dans lequel G et H sont des groupes finis commutatifs et G agit régulièrement sur l'ensemble fini (non vide) X (en particulier $|G|=|X|$). Soient $f : X \to H$ et $x_0 \in X$ quelconque. Alors la fonction f est G-parfaitement non linéaire si et seulement si $f_{x_0} : G \to H$ est parfaitement non linéaire (au sens classique de Carlet et Ding).*

Preuve. Nous montrons que pour $\mathbf{g} \in G^*$ et $\beta \in H$, $|\{x \in X | f(\mathbf{g}.x) - f(x) = \beta\}| = |\{\mathbf{h} \in G | f_{x_0}(\mathbf{g}\top\mathbf{h}) - f_{x_0}(\mathbf{h}) = \beta\}|$, ce qui est suffisant pour prouver le théorème.
Soit $x \in X = \mathcal{O}_G(x_0)$. Il existe un et un seul $\mathbf{h} \in G$ tel que $x = \mathbf{h}.x_0$ (puisque G agit régulièrement sur l'ensemble X). Il en résulte que $|\{x \in X | f(\mathbf{g}.x) - f(x) = \beta\}| = |\{\mathbf{h} \in G | f(\mathbf{g}\top\mathbf{h}.x_0) - f(\mathbf{h}.x_0) = \beta\}|$ ce qui fournit le résultat approprié. □

Remarquons que le fait que f soit G-parfaitement non linéaire ne dépend pas du choix du point $x_0 \in X$. En effet l'action de G sur l'ensemble X est régulière et ainsi tous les points $x \in X$ jouent le même rôle. En d'autres termes :
$\exists x_0 \in X$, tel que f_{x_0} soit parfaitement non linéaire $\Leftrightarrow \forall x \in X$, f_x est parfaitement non linéaire.

Comme conséquence directe du théorème précédent nous disposons du résultat ci-dessous.

Corollaire 7.3. *Sous les mêmes hypothèses que le théorème précédent, la fonction f est G-parfaitement non linéaire si et seulement si $\forall \beta \in H^*$, $\chi_H^\beta \circ f_{x_0} : G \to \mathbb{U}_{exp(H)} \subset \mathbb{U}$ est courbe au sens de Logachev, Salnikov et Yashchenko, i.e. $\forall \beta \in H^*$, $\forall \mathbf{g} \in G$,*

$$|\widehat{\chi_H^\beta \circ f_{x_0}}(\mathbf{g})| = \sqrt{|G|}\ .$$

Preuve. D'après le théorème précédent, f est G-parfaitement non linéaire si et seulement si f_{x_0} est parfaitement non linéaire au sens de Carlet et Ding. Or cette dernière proposition est formellement équivalente au fait que $\forall \beta \in H^*$, $\forall \mathbf{g} \in G$, $|\widehat{\chi_H^\beta \circ f_{x_0}}(\mathbf{g})| = \sqrt{|G|}$ (par application du théorème 6.5 p. 109). □

A contrario du cas des actions fidèles, la caractérisation ne dépend que d'une unique fonction f_x et non d'une moyenne sur tous les éléments $x \in X$. Ceci est essentiellement dû, encore une fois, à la régularité de l'action qui ne distingue aucun de ces éléments en particulier.

Le théorème 7.3 peut aussi être énoncé sous la forme suivante, parfois plus adéquat, où l'on change de point de vue en s'intéressant aux fonctions définies sur le groupe agissant.

Proposition 7.12. *Soit $((G,\top),(H,+))$ un couple de groupes finis commutatifs tel que G agisse régulièrement sur un ensemble fini non vide X. Soit $f : G \to H$. Alors f est une fonction parfaitement non linéaire au sens de Carlet et Ding si et seulement s'il existe une bijection $\Theta : X \to G$ telle que $f \circ \Theta : X \to H$ soit G-parfaitement non linéaire.*

Preuve. Puisque l'action de G sur l'ensemble X est régulière, elle est isomorphe à l'action de G sur lui-même par translation (voir corollaire 7.2). Plus précisément, il existe une bijection $\Theta : X \to G$ telle que $\forall (\mathbf{g},x) \in G \times X$, $\Theta(\mathbf{g}.x) = \mathbf{g}\top\Theta(x)$.
La fonction f est parfaitement non linéaire au sens de Carlet et Ding
$\Leftrightarrow \forall \mathbf{g} \in G^*, \forall \beta \in H, |\{\mathbf{h} \in G | f(\mathbf{g}\top\mathbf{h}) - f(\mathbf{h}) = \beta\}| = \dfrac{|G|}{|H|}$
$\Leftrightarrow \forall \mathbf{g} \in G^*, \forall \beta \in H, |\{x \in X | f(\mathbf{g}\top\Theta(x)) - f(\Theta(x)) = \beta\}| = \dfrac{|G|}{|H|}$ (par le changement de

variables $x \stackrel{déf.}{=} \Theta^{-1}(\mathbf{h})$)
$\Leftrightarrow \forall \mathbf{g} \in G^*, \forall \beta \in H, |\{x \in X | f \circ \Theta(\mathbf{g}.x) - f \circ \Theta(x) = \beta\}| = \frac{|G|}{|H|} = \frac{|X|}{|H|}$ (d'après ce qui a été dit en préambule et par hypothèse)
$\Leftrightarrow f \circ \Theta : X \to H$ est G-parfaitement non linéaire. □

Remarque 7.6. Cette proposition est strictement équivalente au théorème 7.3. Il est d'ailleurs possible de la démontrer par application de ce théorème simplement en posant $\Theta \stackrel{déf.}{=} \phi_{x_0}^{-1}$ pour $x_0 \in X$ quelconque (c'est en particulier ce que nous allons faire par la suite dans la sous-section 7.4.5). Toutefois nous avons préféré privilégier, dans la démonstration, l'aspect géométrique de l'allure d'une action régulière.

7.4.3 Interprétation de la non linéarité parfaite de Carlet et Ding

La conception de la non linéarité parfaite au sens de Carlet et Ding peut être plongée de façon canonique dans le cadre plus général établi ici. Comme conséquence du fait que l'action du groupe des translations d'un groupe G sur G est équivalente à l'action de G sur lui-même par addition, nous avons le résultat ci-dessous.

Proposition 7.13. *Soient $(G, \top)$ et H deux groupes finis commutatifs et $f : G \to H$. La fonction f est $T(G)$-parfaitement non linéaire si et seulement si elle est parfaitement non linéaire au sens de Carlet et Ding.*

Preuve. Rappelons que l'action de $T(G)$ sur l'ensemble sous-jacent au groupe G ou de manière équivalente celle de G sur lui-même par translation est régulière.
On sait d'après le théorème 7.3 que f est $T(G)$-parfaitement non linéaire si et seulement si $f_{e_G} : T(G) \to H$ est parfaitement non linéaire. Or pour $\sigma_\alpha \in T(G)$, on a $f_{e_G}(\sigma_\alpha) = f(\sigma_\alpha(e_G)) = f(\alpha \top e_G) = f(\alpha)$, soit pour tout $\alpha \in G$, $f_{e_G}(\sigma_\alpha) = f(\alpha)$. On en déduit donc aisément que f_{e_G} est parfaitement non linéaire si et seulement f l'est également. □

7.4.4 Non linéarité parfaite basée sur une action par automorphisme de groupe

Dans cette sous-section, nous abordons brièvement le cas de l'action par automorphisme de groupe. En particulier, on s'intéresse au fait que si G agit semi-régulièrement sur un groupe H alors il agit régulièrement sur l'ensemble H^* (cf. sous-section 7.2.8).

Lemme 7.4. *Soit $(G, H_1, (H_2, +))$ un triplet de groupes finis commutatifs. Supposons que G agisse fidèlement sur H_1 par automorphisme de groupe. Soit $f : H_1 \to H_2$ une fonction G-parfaitement non linéaire. Alors pour tout $\mathbf{g} \in G^*$ et pour tout $\beta \in H_2$,*

$$|\{x \in H_1^* | f(\mathbf{g}.x) - f(x) = \beta\}| = \frac{|H_1|}{|H_2|} - \mathbf{1}_{\{e_{H_2}\}}(\beta) \ .$$

Preuve. Puisque f est G-parfaitement non linéaire on a pour tout $\mathbf{g} \in G^*$ et pour tout $\beta \in H_2$, $|\{x \in H_1 | f(\mathbf{g}.x) - f(x) = \beta\}| = \frac{|H_1|}{|H_2|}$, ce qui est équivalent à $|\{x \in \{e_{H_1}\} \cup H_1^* | f(\mathbf{g}.x) - f(x) = \beta\}| = \frac{|H_1|}{|H_2|}$. Puisque $f(\mathbf{g}.e_{H_1}) - f(e_{H_1}) = f(e_{H_1}) - f(e_{H_1}) = e_{H_2}$, on en déduit que :

$$\mathbf{1}_{\{e_{H_2}\}}(\beta) + |\{x \in H_1^* | f(\mathbf{g}.x) - f(x) = \beta\}| = \frac{|H_1|}{|H_2|} \ .$$

□

Proposition 7.14. *Soit $(G, H_1, (H_2, +))$ un triplet de groupes finis commutatifs avec $|H_2| > 1$. Supposons que G agisse semi-régulièrement sur H_1 par automorphisme de groupe. Soit une fonction $f : H_1 \to H_2$. Si f est G-parfaitement non linéaire alors $f|_{H_1^*}$ n'est pas G-parfaitement non linéaire (au sens de l'action de groupe de G sur l'ensemble H_1^*).*

Preuve. Le symbole « . » dénote les deux actions (l'action de G sur l'ensemble H_1^* n'étant qu'une restriction de l'action par automorphisme de groupe de G sur H).
Supposons que les fonctions f et $f|_{H_1^*}$ soient toutes deux G-parfaitement non linéaires. En ce qui concerne la première fonction, d'après le lemme 7.4, cela revient à dire que $\forall \mathbf{g} \in G^*$, $\forall \beta \in H_2$, $|\{x \in H_1^* | f(\mathbf{g}.x) - f(x) = \beta\}| = \frac{|H_1|}{|H_2|} - \mathbf{1}_{\{e_{H_2}\}}(\beta)$. Relativement à la fonction $f|_{H_1^*}$, cela exprime que $\forall \mathbf{g} \in G^*$, $\forall \beta \in H_2$, $|\{x \in H_1^* \mid f|_{H_1^*}(\mathbf{g}.x) - f|_{H_1^*}(x) = \beta\}| = \frac{|H_1^*|}{|H_2|}$ soit encore, $\forall \mathbf{g} \in G^*$, $\forall \beta \in H_2$, $|\{x \in H_1^* | f(\mathbf{g}.x) - f(x) = \beta\}| = \frac{|H_1| - 1}{|H_2|}$ par définition de $f|_{H_1^*}$. En particulier pour $\beta \neq e_{H_2}$ (ce qui est possible puisque l'on dispose de l'hypothèse que $|H_2| > 1$), si f et $f|_{H_1^*}$ sont simultanément G-parfaitement non linéaires, on a $\frac{|H_1|}{|H_2|} = \frac{|H_1| - 1}{|H_2|}$ ce qui est impossible. □

Corollaire 7.4. *Soient $\mathbb{K}$ un corps fini et H un groupe fini commutatif tel que $|H| > 1$. Soit $f : \mathbb{K} \to H$. Si la fonction f est $\mathbb{K}^*$-parfaitement non linéaire (où l'action de $\mathbb{K}^*$ par automorphisme de groupes sur $(\mathbb{K}, +)$ est définie comme dans la proposition 7.6) alors la fonction $f|_{\mathbb{K}^*} : \mathbb{K}^* \to H$ n'est pas parfaitement non linéaire au sens de Carlet et Ding (cf. chapitre 6).*

Preuve. D'après la proposition 7.6, l'action de $\mathbb{K}^*$ sur $(\mathbb{K}, +)$ est semi-régulière. La proposition précédente peut donc être appliquée à ce cas particulier : si la fonction f est $\mathbb{K}^*$-parfaitement non linéaire alors $f|_{\mathbf{K}^*}$ n'est pas $\mathbb{K}^*$-parfaitement non linéaire. Or $f|_{\mathbf{K}^*} : \mathbb{K}^* \to H$ et l'action de $\mathbb{K}^*$ sur $(\mathbb{K}, +)$ correspond à une translation multiplicative donc l'action de $\mathbb{K}^*$ sur $\mathbb{K}^* \subset \mathbb{K}$ est l'action du groupe $\mathbb{K}^*$ sur son propre ensemble sous-jacent par translation. On en déduit donc que $f|_{\mathbf{K}^*}$ est $\mathbb{K}^*$-parfaitement non linéaire si et seulement si $f|_{\mathbf{K}^*}$ est parfaitement non linéaire au sens de Carlet et Ding (par la proposition 7.13). D'où la conclusion recherchée. □

7.4.5 Construction d'une fonction G-parfaitement non linéaire

7.4.5.1 Introduction

Au cours de cette sous-section, le degré de liberté accordé par l'aspect du groupe choisi pour agir régulièrement est mis en lumière. En effet alors même que l'action considérée est régulière, il est possible de produire de nouvelles constructions.

Afin de mettre en valeur cette constatation, il faut comparer les fonctions introduites ici avec celles issues de la théorie de Carlet et Ding. Aussi l'ensemble fini sur lequel on agit est désormais muni d'une structure de groupe fini abélien.

Deux cas principaux sont à considérer selon que l'action régulière d'un groupe G sur l'ensemble sous-jacent à un groupe H, est ou non isomorphe à l'action par translation de H sur lui-même. C'est en ce sens que l'on parle de *forme*, d'*aspect* du groupe agissant ou on évoque encore le défaut d'isomorphisme de G par rapport à $T(H)$ dans son action sur H.

Si le groupe G s'apparente au groupe des translations de H dans son action, alors nous montrons, dans le premier paragraphe de cette sous-section, que les fonctions, définies sur H, G-parfaitement non linéaires sont à une composition par une permutation près parfaitement non linéaires au sens

usuel.

Supposons maintenant que dans son action, toujours régulière, sur (l'ensemble sous-jacent à) H, G soit très dissemblable du groupe $T(H)$, au moins non isomorphe. Dans ce cas, la caractérisation précédente ne s'applique évidemment pas, autrement dit les fonctions G-parfaitement non linéaires ne sont pas équivalentes (modulo une permutation) aux fonctions parfaitement non linéaires au sens de Carlet et Ding définies sur H. Néanmoins on peut une fois de plus se rapporter aux notions traditionnelles, simplement cette fois le *transport* de la non linéarité parfaite s'effectue vers le groupe G et non en direction de H : il est possible d'interpréter les fonctions G-parfaitement non linéaires dont l'ensemble de départ est H comme des fonctions parfaitement non linéaires définies sur G. Comme l'action de G sur H est distincte de l'action de H sur lui-même par addition, il est alors naturellement légitime d'espérer découvrir des fonctions bien différentes de celles connues dans le cadre conventionnel. Ainsi nous exhibons une fonction de $\mathbb{Z}_{16} \to \mathbb{F}_2$ qui est $\mathbb{F}_2^4$-parfaitement non linéaire alors même que l'action de $\mathbb{F}_2^4$ sur l'ensemble sous-jacent à l'anneau $\mathbb{Z}_{16}$, bien que régulière, n'est pas isomorphe à l'action par translation du groupe additif de cet anneau.

7.4.5.2 Cas d'une action équivalente à une action par translation

Dans ce paragraphe est exposée l'allure générale des fonctions G-parfaitement non linéaires dans le cas particulier où l'action de G sur l'ensemble sous-jacent à un autre groupe H est isomorphe à l'action par translation de H sur lui-même.

Théorème 7.4. *Soit X un ensemble fini (non vide). Soient G et G' deux groupes commutatifs et isomorphes, sous-groupes de $S(X)$, agissant régulièrement sur l'ensemble X. Alors G et G' sont conjugués (dans $S(X)$).*

Preuve. Puisque G et G' sont des sous-groupes de $S(X)$, on suit la convention indiquée dans la remarque 7.1, du début de ce présent chapitre, pour nommer leurs éléments et les actions respectives.
Soit $\Phi : G \to G'$ l'isomorphisme de groupes. Puisque G et G' agissent tous deux régulièrement sur X, un point $x \in X$ étant choisi, chaque élément de X s'écrit de manière unique $\sigma(x)$ pour $\sigma \in G$ (en utilisant l'application orbitale de x) et il en est de même pour G'. Lorsque σ décrit G, $\sigma' \stackrel{déf.}{=} \Phi(\sigma)$ décrit G' et la correspondance

$$\begin{array}{rccc} \pi : & X = \boldsymbol{\mathcal{O}}_G(x) & \to & X = \boldsymbol{\mathcal{O}}_{G'}(x) \\ & \sigma(x) & \mapsto & \sigma'(x) \stackrel{déf.}{=} \Phi(\sigma)(x) \end{array}$$

est clairement une bijection de X dans lui-même (donc $\pi \in S(X)$).
Pour τ quelconque dans G, on a :

$$\begin{aligned} \pi \circ \tau \circ \pi^{-1}(\sigma'(x)) &= \pi \circ \tau \circ \pi^{-1}(\Phi(\sigma)(x)) \\ &= \pi \circ \tau(\sigma(x)) \\ &= \pi(\tau \circ \sigma(x)) \\ &= \Phi(\tau \circ \sigma)(x) \\ &= (\Phi(\tau) \circ \Phi(\sigma))(x) \text{ (puisque } \Phi \text{ est en particulier un homomorphisme)} \\ &= \Phi(\tau)(\sigma'(x)) \end{aligned}$$

donc $\pi \circ \tau \circ \pi^{-1} = \Phi(\tau)$ *i.e.* Φ est l'automorphisme intérieur $\Im_\pi$ et donc G et G' sont conjugués. □

Corollaire 7.5. *Soit H un groupe fini commutatif. La classe de conjugaison du groupe des translations $T(H)$ est égale à l'ensemble des sous-groupes de $S(H)$ isomorphes à $T(H)$ (ou à H).*

Preuve. Soit G un sous-groupe de $S(H)$ isomorphe à $T(H)$ (et donc à H). Alors G agit régulièrement sur l'ensemble sous-jacent à la structure de groupe de H. En effet soit $\Phi : G \to T(H)$ l'isomorphisme de groupe. Alors l'application

$$\begin{array}{rccl} \phi : & G & \to & S(H) \\ & \sigma & \mapsto & (\phi(\sigma) : x \mapsto \phi(\sigma)(x) \stackrel{déf.}{=} \Phi(\sigma)(x)) \end{array}$$

est une action régulière. En effet, nous avons tout d'abord pour tout $\sigma \in G$, $\Phi(\sigma) \in T(H) \subset S(H)$. De plus $\forall(\sigma,\tau) \in G^2$ et $\forall x \in H$, $\phi(\sigma \circ \tau)(x) = \Phi(\sigma \circ \tau)(x) = (\Phi(\sigma) \circ \Phi(\tau))(x) = \phi(\sigma)(\phi(\tau)(x))$ et $\phi(e_G)(x) = \Phi(e_G)(x) = e_{T(H)}(x) = Id_H(x) = x$. Enfin l'application orbitale de x définie pour $\sigma \in G$ par $\phi_x(\sigma) = \phi(\sigma)(x) = \Phi(\sigma)(x)$ est bien entendu bijective par composition d'applications bijectives (puisque l'action de $T(H)$ sur l'ensemble sous-jacent à H est régulière). D'après le théorème précédent, G et $T(H)$ sont conjugués. Pour résumer on vient de montrer que tout sous-groupe de $S(H)$ isomorphe à $T(H)$ est un conjugué de $T(H)$.
L'inclusion réciproque est évidente. On en déduit donc la conclusion souhaitée. □

Il est désormais possible d'établir le profil général des fonctions G-parfaitement non linéaires dans le cas où G est isomorphe au groupe des translations d'un groupe H et agit donc de manière équivalente sur H.

Proposition 7.15. *Soient $(H_1, \top)$ et $(H_2, +)$ deux groupes finis commutatifs et G un sous-groupe de $S(H_1)$ isomorphe au groupe $T(H_1)$. Soit $f : H_1 \to H_2$. La fonction f est G-parfaitement non linéaire si et seulement s'il existe $\pi \in S(H_1)$ tel que la fonction $f \circ \pi : H_1 \to H_2$ soit parfaitement non linéaire au sens de Carlet et Ding et alors $G = \pi \circ T(H_1) \circ \pi^{-1}$.*

Preuve. D'après le corollaire précédent, il existe $\pi \in S(H_1)$ tel que $G = \pi \circ T(H_1) \circ \pi^{-1}$.
La fonction f est G-parfaitement non-linéaire
$\Leftrightarrow \forall \sigma \in G^*, \forall \beta \in H_2, |\{x \in H_1 | f(\sigma(x)) - f(x) = \beta\}| = \dfrac{|H_1|}{|H_2|}$
$\Leftrightarrow \forall \sigma_\alpha \in T(H_1)^*, \forall \beta \in H_2, |\{x \in H_1 | f((\pi \circ \sigma_\alpha \circ \pi^{-1})(x)) - f(x) = \beta\}| = \dfrac{|H_1|}{|H_2|}$ (puisque $G = \pi \circ T(H_1) \circ \pi^{-1}$ donc pour tout $\sigma \in G^*$, $\exists\,!\ \sigma_\alpha \in T(H_1)^*$ tel que $\sigma = \pi \circ \sigma_\alpha \circ \pi^{-1}$)
$\Leftrightarrow \forall \alpha \in H_1^*, \forall \beta \in H_2, |\{x \in H_1 | f(\pi(\alpha \top \pi^{-1}(x))) - f(x) = \beta\}| = \dfrac{|H_1|}{|H_2|}$
$\Leftrightarrow \forall \alpha \in H_1^*, \forall \beta \in H_2, |\{y \in H_1 | f(\pi(\alpha \top y)) - f(\pi(y)) = \beta\}| = \dfrac{|H_1|}{|H_2|}$ (par le changement de variables $y \stackrel{déf.}{=} \pi^{-1}(x)$)
$\Leftrightarrow f \circ \pi$ est parfaitement non linéaire au sens de Carlet et Ding. □

7.4.5.3 Cas d'une action non équivalente à une action par translation

Dans ce paragraphe, nous construisons une fonction G-parfaitement non linéaire dans le cas où G n'est pas isomorphe dans son action sur un autre groupe H au groupe des translations $T(H)$. Donc même dans ce cas particulier, fondamentalement distinct de la non linéarité parfaite de Carlet et Ding, il est évidemment possible d'exhiber des fonctions G-parfaitement non linéaires.

Afin de réaliser cela, nous faisons agir $\mathbb{F}_2^m$, de manière régulière via des involutions sans point fixe, sur l'ensemble sous-jacent à l'anneau $\mathbb{Z}_{2^m}$. Notons tout de suite que pour $m > 1$, le groupe additif sous-jacent à l'espace vectoriel $\mathbb{F}_2^m$ et celui sous-jacent à l'anneau $\mathbb{Z}_{2^m}$ ne sont pas isomorphes (puisque tous les éléments non nuls du premier groupe sont d'ordre 2 alors que le second groupe est cyclique d'ordre 2^m).

Soit donc $m \in \mathbb{N}^*$ tel que $m > 1$. Soit la bijection, déjà présentée au chapitre 4 et utilisée dans la section précédente, Θ_m^d définie, on le rappelle, par

$$\begin{array}{rccl} \Theta_m^d : & \mathbb{F}_2^m & \to & \mathbb{Z}_{2^m} \\ & x & \mapsto & \sum_{i=1}^{m} x_i 2^{i-1} \ . \end{array}$$

Par analogie avec les automorphismes intérieurs, on introduit l'application

$$\begin{array}{rccl} \Im_{\Theta_m^d} : & S(\mathbb{F}_2^m) & \to & S(\mathbb{Z}_{2^m}) \\ & \pi & \mapsto & \Theta_m^d \circ \pi \circ {\Theta_m^d}^{-1} \ . \end{array}$$

Le fait que $\Im_{\Theta_m^d}$ transporte les permutations de $\mathbb{F}_2^m$ dans celles de $\mathbb{Z}_{2^m}$ est évident par composition d'applications bijectives.

Lemme 7.5. *$\Im_{\Theta_m^d}$ est un isomorphisme de groupes de $S(\mathbb{F}_2^m)$ dans $S(\mathbb{Z}_{2^m})$.*

Preuve. D'une part, soit $(\pi, \sigma) \in S(\mathbb{F}_2^m)^2$. On a $\Im_{\Theta_m^d}(\pi \circ \sigma) = \Theta_m^d \circ \pi \circ \sigma \circ {\Theta_m^d}^{-1} = \Theta_m^d \circ \pi \circ {\Theta_m^d}^{-1} \circ \Theta_m^d \circ \sigma \circ {\Theta_m^d}^{-1} = \Im_{\Theta_m^d}(\pi) \circ \Im_{\Theta_m^d}(\sigma)$: c'est donc un homomorphisme de groupes. D'autre part, soit $\pi \in S(\mathbb{F}_2^m)$ tel que $\forall x \in \mathbb{Z}_{2^m}$, $\Im_{\Theta_m^d}(\pi)(x) = x$. Alors $\forall x \in \mathbb{Z}_{2^m}$, $\pi({\Theta_m^d}^{-1}(x)) = {\Theta_m^d}^{-1}(x)$ ce qui est équivalent à $\forall y \in \mathbb{Z}_{2^m}$, $\pi(y) = y$ soit encore $\pi = Id_{\mathbb{F}_2^m}$. On a donc $\ker(\Im_{\Theta_m^d}) = \{Id_{\mathbb{F}_2^m}\}$ et donc que l'application $\Im_{\Theta_m^d}$ est injective. Par raison de cardinalité on en déduit que cet homomorphisme est bijectif : c'est donc un isomorphisme de groupes. □

Notre intérêt se porte maintenant sur les involutions sans point fixe de $\mathbb{F}_2^m$, en particulier sur les *groupes maximaux d'involutions (sans point fixe)*. Puisque l'annexe B leur est en partie dédiée, nous recommandons grandement la lecture *a minima* de la section B.3. Néanmoins sont résumées ci-dessous les principaux résultats les concernant.

- Soit X un ensemble fini. Une permutation $\boldsymbol{\sigma} \in S(X)$ est une *involution sans point fixe* si $\boldsymbol{\sigma}^2 = Id_X$ et $\forall x \in X$, $\boldsymbol{\sigma}(x) \neq x$. L'ensemble des involutions sans point fixe de $S(X)$ est noté « $Inv(X)$ » ;
- La décomposition en cycles d'une involution sans point fixe de X est constituée d'exactement $\dfrac{|X|}{2}$ transpositions[7] à supports disjoints ;
- Un sous-groupe G de $S(X)$ est un *groupe maximal d'involutions (sans point fixe)* si $|G| = |X|$ et $G^* \subset Inv(X)$. Un tel groupe est forcément abélien et agit régulièrement sur X.

L'objectif est de faire agir $\mathbb{F}_2^m$ sur l'ensemble sous-jacent à $\mathbb{Z}_{2^m}$ à l'aide d'involutions sans point fixe de manière à obtenir une action régulière mais non isomorphe à l'action par translation de $\mathbb{Z}_{2^m}$. Nous allons transporter, à l'aide de $\Im_{\Theta_m^d}$, l'action d'un groupe maximal d'involutions sans point fixe de $\mathbb{F}_2^m$ sur $\mathbb{Z}_{2^m}$.

Lemme 7.6. *Soit $\boldsymbol{\sigma} \in Inv(\mathbb{F}_2^m)$ alors $\Im_{\Theta_m^d}(\boldsymbol{\sigma}) \in Inv(\mathbb{Z}_{2^m})$.*

Preuve. Puisque $\Im_{\Theta_d^m}$ est en particulier un homomorphisme de groupes, $\Im_{\Theta_m^d}(\boldsymbol{\sigma})^2 = \Im_{\Theta_m^d}(\boldsymbol{\sigma}^2) = \Im_{\Theta_m^d}(Id_{\mathbb{F}_2^m})$ (puisque $\boldsymbol{\sigma}$ est une involution de $\mathbb{F}_2^m$) $= Id_{\mathbb{Z}_{2^m}}$. Supposons par ailleurs qu'il existe $x \in \mathbb{Z}_{2^m}$ tel que $\Im_{\Theta_m^d}(\boldsymbol{\sigma})(x) = x$ alors par définition on a $\Theta_m^d \circ \boldsymbol{\sigma}({\Theta_m^d}^{-1}(x)) = x$, soit en composant à gauche par ${\Theta_m^d}^{-1}$ les deux membres de l'égalité, on obtient $\boldsymbol{\sigma}({\Theta_m^d}^{-1}(x)) = {\Theta_m^d}^{-1}(x)$ et donc que ${\Theta_m^d}^{-1}(x)$ est un point fixe de $\boldsymbol{\sigma}$ ce qui est en contradiction avec les hypothèses. Finalement on a $\Im_{\Theta_m^d}(\boldsymbol{\sigma}) \in Inv(\mathbb{Z}_{2^m})$. □

[7] La transposition qui associe les points distincts x et y de X est notée « $\mathfrak{T}_{(x,\ y)}$ ».

Exemple 7.5. Soit $m = 4$. Nous pouvons donner la correspondance par $\Im_{\Theta_4^d}$ entre les translations σ_α de $\mathbb{F}_2^4$ et les versions involutives dans $\mathbb{Z}_{16}$.

Translation par	Permutation correspondante
$(0,0,0,0)$	$Id_{\mathbb{Z}_{16}}$
$(1,0,0,0)$	$\mathfrak{T}_{(0,\ 1)} \circ \mathfrak{T}_{(2,\ 3)} \circ \mathfrak{T}_{(4,\ 5)} \circ \mathfrak{T}_{(6,\ 7)} \circ \mathfrak{T}_{(8,\ 9)} \circ \mathfrak{T}_{(10,\ 11)} \circ \mathfrak{T}_{(12,\ 13)} \circ \mathfrak{T}_{(14,\ 15)}$
$(0,1,0,0)$	$\mathfrak{T}_{(0,\ 2)} \circ \mathfrak{T}_{(1,\ 3)} \circ \mathfrak{T}_{(4,\ 6)} \circ \mathfrak{T}_{(5,\ 7)} \circ \mathfrak{T}_{(8,\ 10)} \circ \mathfrak{T}_{(9,\ 11)} \circ \mathfrak{T}_{(12,\ 14)} \circ \mathfrak{T}_{(13,\ 15)}$
$(1,1,0,0)$	$\mathfrak{T}_{(0,\ 3)} \circ \mathfrak{T}_{(1,\ 2)} \circ \mathfrak{T}_{(4,\ 7)} \circ \mathfrak{T}_{(5,\ 6)} \circ \mathfrak{T}_{(8,\ 11)} \circ \mathfrak{T}_{(9,\ 10)} \circ \mathfrak{T}_{(12,\ 15)} \circ \mathfrak{T}_{(13,\ 14)}$
$(0,0,1,0)$	$\mathfrak{T}_{(0,\ 4)} \circ \mathfrak{T}_{(1,\ 5)} \circ \mathfrak{T}_{(2,\ 6)} \circ \mathfrak{T}_{(3,\ 7)} \circ \mathfrak{T}_{(8,\ 12)} \circ \mathfrak{T}_{(9,\ 13)} \circ \mathfrak{T}_{(10,\ 14)} \circ \mathfrak{T}_{(11,\ 15)}$
$(1,0,1,0)$	$\mathfrak{T}_{(0,\ 5)} \circ \mathfrak{T}_{(1,\ 4)} \circ \mathfrak{T}_{(2,\ 7)} \circ \mathfrak{T}_{(3,\ 6)} \circ \mathfrak{T}_{(8,\ 13)} \circ \mathfrak{T}_{(9,\ 12)} \circ \mathfrak{T}_{(10,\ 15)} \circ \mathfrak{T}_{(11,\ 14)}$
$(0,1,1,0)$	$\mathfrak{T}_{(0,\ 6)} \circ \mathfrak{T}_{(1,\ 7)} \circ \mathfrak{T}_{(2,\ 4)} \circ \mathfrak{T}_{(3,\ 5)} \circ \mathfrak{T}_{(8,\ 14)} \circ \mathfrak{T}_{(9,\ 15)} \circ \mathfrak{T}_{(10,\ 12)} \circ \mathfrak{T}_{(11,\ 13)}$
$(1,1,1,0)$	$\mathfrak{T}_{(0,\ 7)} \circ \mathfrak{T}_{(1,\ 6)} \circ \mathfrak{T}_{(2,\ 5)} \circ \mathfrak{T}_{(3,\ 4)} \circ \mathfrak{T}_{(8,\ 15)} \circ \mathfrak{T}_{(9,\ 14)} \circ \mathfrak{T}_{(10,\ 13)} \circ \mathfrak{T}_{(11,\ 12)}$
$(0,0,0,1)$	$\mathfrak{T}_{(0,\ 8)} \circ \mathfrak{T}_{(1,\ 9)} \circ \mathfrak{T}_{(2,\ 10)} \circ \mathfrak{T}_{(3,\ 11)} \circ \mathfrak{T}_{(4,\ 12)} \circ \mathfrak{T}_{(5,\ 13)} \circ \mathfrak{T}_{(6,\ 14)} \circ \mathfrak{T}_{(7,\ 15)}$
$(1,0,0,1)$	$\mathfrak{T}_{(0,\ 9)} \circ \mathfrak{T}_{(1,\ 8)} \circ \mathfrak{T}_{(2,\ 11)} \circ \mathfrak{T}_{(3,\ 10)} \circ \mathfrak{T}_{(4,\ 13)} \circ \mathfrak{T}_{(5,\ 12)} \circ \mathfrak{T}_{(6,\ 15)} \circ \mathfrak{T}_{(7,\ 14)}$
$(0,1,0,1)$	$\mathfrak{T}_{(0,\ 10)} \circ \mathfrak{T}_{(1,\ 11)} \circ \mathfrak{T}_{(2,\ 8)} \circ \mathfrak{T}_{(3,\ 9)} \circ \mathfrak{T}_{(4,\ 14)} \circ \mathfrak{T}_{(5,\ 15)} \circ \mathfrak{T}_{(6,\ 12)} \circ \mathfrak{T}_{(7,\ 13)}$
$(1,1,0,1)$	$\mathfrak{T}_{(0,\ 11)} \circ \mathfrak{T}_{(1,\ 10)} \circ \mathfrak{T}_{(2,\ 9)} \circ \mathfrak{T}_{(3,\ 8)} \circ \mathfrak{T}_{(4,\ 15)} \circ \mathfrak{T}_{(5,\ 14)} \circ \mathfrak{T}_{(6,\ 13)} \circ \mathfrak{T}_{(7,\ 12)}$
$(0,0,1,1)$	$\mathfrak{T}_{(0,\ 12)} \circ \mathfrak{T}_{(1,\ 13)} \circ \mathfrak{T}_{(2,\ 14)} \circ \mathfrak{T}_{(3,\ 15)} \circ \mathfrak{T}_{(4,\ 8)} \circ \mathfrak{T}_{(5,\ 9)} \circ \mathfrak{T}_{(6,\ 10)} \circ \mathfrak{T}_{(7,\ 11)}$
$(1,0,1,1)$	$\mathfrak{T}_{(0,\ 13)} \circ \mathfrak{T}_{(1,\ 12)} \circ \mathfrak{T}_{(2,\ 15)} \circ \mathfrak{T}_{(3,\ 14)} \circ \mathfrak{T}_{(4,\ 9)} \circ \mathfrak{T}_{(5,\ 8)} \circ \mathfrak{T}_{(6,\ 11)} \circ \mathfrak{T}_{(7,\ 10)}$
$(0,1,1,1)$	$\mathfrak{T}_{(0,\ 14)} \circ \mathfrak{T}_{(1,\ 15)} \circ \mathfrak{T}_{(2,\ 12)} \circ \mathfrak{T}_{(3,\ 13)} \circ \mathfrak{T}_{(4,\ 10)} \circ \mathfrak{T}_{(5,\ 11)} \circ \mathfrak{T}_{(6,\ 8)} \circ \mathfrak{T}_{(7,\ 9)}$
$(1,1,1,1)$	$\mathfrak{T}_{(0,\ 15)} \circ \mathfrak{T}_{(1,\ 14)} \circ \mathfrak{T}_{(2,\ 13)} \circ \mathfrak{T}_{(3,\ 12)} \circ \mathfrak{T}_{(4,\ 11)} \circ \mathfrak{T}_{(5,\ 10)} \circ \mathfrak{T}_{(6,\ 9)} \circ \mathfrak{T}_{(7,\ 8)}$

On rappelle que les translations de $\mathbb{F}_2^m$, mis à part l'identité, sont des involutions sans point fixe (cf. annexe B). Remarquons que leurs images dans $S(\mathbb{Z}_{16})$ ne sont généralement pas des translations de $\mathbb{Z}_{16}$. Par exemple l'image de la translation par $(1,1,0,0)$ n'est pas égale à la translation par $\Theta_4^d(1,1,0,0) = 3$ dans $\mathbb{Z}_{16}$ (la première fait correspondre 5 et 6 alors que la seconde envoie 5 sur 8 et 6 sur 9).

Lemme 7.7. *Si G est un sous-groupe de $S(\mathbb{F}_2^m)$ alors l'ensemble $\Im_{\Theta_m^d}(G) = \{\Im_{\Theta_m^d}(\pi) \in S(\mathbb{Z}_{2^m}) | \ \pi \in G\}$ est un sous-groupe de $S(\mathbb{Z}_{2^m})$. Si G est un groupe maximal d'involutions sans point fixe de $\mathbb{F}_2^m$ alors $\Im_{\Theta_m^d}(G)$ est un groupe maximal d'involutions sans point fixe de $\mathbb{Z}_{2^m}$. En particulier l'action de groupe de $\Im_{\Theta_m^d}(G)$ sur l'ensemble sous-jacent à l'anneau $\mathbb{Z}_{2^m}$ est régulière.*

Preuve. Puisque $\Im_{\Theta_d^m}$ est un isomorphisme de groupes de $S(\mathbb{F}_2^m)$ dans $S(\mathbb{Z}_{2^m})$, $\Im_{\Theta_m^d}(G)$ est un sous-groupe de $S(\mathbb{Z}_{2^m})$.
Si par ailleurs G est un groupe maximal d'involutions sans point fixe de $\mathbb{F}_2^m$, $\Im_{\Theta_m^d}(G)$ est un sous-groupe de $S(\mathbb{Z}_{2^m})$ de cardinal $|\Im_{\Theta_m^d}(G)| = |G| = 2^m = |\mathbb{Z}_{2^m}|$ tel que tout élément différent de l'identité est une involution sans point fixe de $\mathbb{Z}_{2^m}$. Il en résulte au final que $\Im_{\Theta_m^d}(G)$ est bien un groupe maximal d'involutions sans point fixe de $\mathbb{Z}_{2^m}$. On en déduit alors facilement par application de la proposition B.8 de l'annexe B que l'action de $\Im_{\Theta_m^d}(G)$ sur l'ensemble sous-jacent à l'anneau $\mathbb{Z}_{2^m}$ est régulière. □

Lemme 7.8. *Soit $\pi \in S(\mathbb{F}_2^m)$. L'application*

$$\begin{array}{rccc} \phi: & \mathbb{F}_2^m & \to & S(\mathbb{Z}_{2^m}) \\ & \alpha & \mapsto & \Im_{\Theta_m^d} \circ \Im_\pi \circ \sigma_\alpha \end{array}$$

définie une action régulière de $\mathbb{F}_2^m$ sur l'ensemble sous-jacent à $\mathbb{Z}_{2^m}$.

Preuve. L'application ϕ est bien un homomorphisme de groupes par composition d'homomorphismes de groupes. Reste à montrer que cette action est régulière. Elle est évidemment fidèle puisque

$$\begin{array}{rll} & \phi(\alpha) & = Id_{\mathbb{Z}_{2^m}} \\ \Leftrightarrow & \Theta_d^m \circ \pi \circ \sigma_\alpha \circ \pi^{-1} \circ \Theta_d^{m-1} & = Id_{\mathbb{Z}_{2^m}} \\ \Leftrightarrow & \pi \circ \sigma_\alpha \circ \pi^{-1} & = Id_{\mathbb{F}_2^m} \\ \Leftrightarrow & \sigma_\alpha & = Id_{\mathbb{F}_2^m} \\ \Leftrightarrow & \alpha & = 0_{\mathbb{F}_2^m}\ . \end{array}$$

En fait l'action ϕ est régulière puisque par construction $\{\phi(\alpha) \in \mathbb{Z}_{2^m} | \alpha \in \mathbb{F}_2^m\} = \Im_{\Theta_m^d}(\pi \circ T(\mathbb{F}_2^m) \circ \pi^{-1})$ est un groupe maximal d'involutions sans point fixe de $\mathbb{Z}_{2^m}$. Il suffit d'appliquer le lemme 7.7. □

Remarque 7.7. Nous avons ainsi construit l'action de $\mathbb{F}_2^m$ sur $\mathbb{Z}_{2^m}$ en transportant l'action régulière du groupe $\Im_\pi(T(\mathbb{F}_2^m)) = \pi \circ T(\mathbb{F}_2^m) \circ \pi^{-1}$, conjugué de $T(\mathbb{F}_2^m)$, sur $\mathbb{Z}_{2^m}$ via l'isomorphisme de groupes $\Im_{\Theta_m^d}$. L'utilisation d'une permutation π nous offre un nombre important d'actions (isomorphes) possibles.

Proposition 7.16. *Soit H un groupe fini commutatif. Soit $f : \mathbb{F}_2^m \to H$ une fonction parfaitement non linéaire au sens de Carlet et Ding. Alors pour chaque $x \in \mathbb{Z}_{2^m}$, la fonction $f \circ \phi_x^{-1} : \mathbb{Z}_{2^m} \to H$ (où ϕ_x est l'application orbitale de x au sens de l'action ϕ définie pour un π fixé dans $S(\mathbb{F}_2^m)$ comme dans le lemme 7.8) est $\mathbb{F}_2^m$-parfaitement non linéaire.*

Preuve. Il suffit d'appliquer la proposition 7.12 en montrant que l'application réciproque ϕ_x^{-1} de l'application orbitale joue correctement le rôle de la bijection dans la proposition citée ci-dessus *i.e.* $\forall(\alpha, y) \in \mathbb{F}_2^m \times \mathbb{Z}_{2^m}$, $\phi_x^{-1}(\phi(\alpha)(y)) = \alpha \oplus \phi_x^{-1}(y)$. Soit $\beta \in \mathbb{F}_2^m$ tel que $\phi_x^{-1}(\phi(\alpha)(y)) = \beta$ c'est-à-dire $\phi(\alpha)(y) = \phi(\beta)(x)$. On a donc $\phi(\alpha \oplus \beta)(x) = y$ donc $\phi_x^{-1}(y) = \alpha \oplus \beta$. Il en résulte que $\alpha \oplus \phi_x^{-1}(y) = \beta = \phi_x^{-1}(\phi(\alpha)(y))$. □

Remarquons ici que lorsque $m > 1$, le groupe additif sous-jacent au $\mathbb{F}_2$-espace vectoriel $\mathbb{F}_2^m$ n'est pas isomorphe à celui de $\mathbb{Z}_{2^m}$, il en est donc de même du groupe d'involutions sans point fixe de $\mathbb{Z}_{2^m}$, $G \stackrel{déf.}{=} \{\phi(\alpha) \in \mathbb{Z}_{2^m} | \alpha \in \mathbb{F}_2^m\}$. Ainsi l'action régulière de G sur l'ensemble sous-jacent à la structure d'anneau de $\mathbb{Z}_{2^m}$ (ou indifféremment de $\mathbb{F}_2^m$ sur $\mathbb{Z}_{2^m}$) n'est pas isomorphe à l'action par translation de $\mathbb{Z}_{2^m}$ sur lui-même (par contre elle évidemment isomorphe à celle de $\mathbb{F}_2^m$). On peut donc légitimement espérer trouver des fonctions définies sur $\mathbb{Z}_{2^m}$ qui soient $\mathbb{F}_2^m$-parfaitement non linéaire mais non parfaitement non linéaire au sens de Carlet et Ding.

Nous exposons précisément un exemple d'une telle fonction. Plaçons-nous dans le cas où $m = 4$. Nous allons utiliser $\mathbb{F}_2^4$ comme groupe régulier dans son action sur $\mathbb{Z}_{16}$ comme indiqué précédemment dans le lemme 7.8 (pour simplifier, on choisit ici pour $\pi \in S(\mathbb{F}_2^4)$ l'identité $Id_{\mathbb{F}_2^4}$). Ainsi on fait agir $\mathbb{F}_2^4$ via l'image par l'isomorphisme $\Im_{\Theta_4^d}$ de son groupe des translations. Notons une nouvelle fois que l'action de $\mathbb{F}_2^4$ sur $\mathbb{Z}_{16}$ n'est pas isomorphe à l'action de $\mathbb{Z}_{16}$ sur lui-même par translation.

Soit la fonction $f : \mathbb{F}_2^4 \to \mathbb{F}_2$ définie par $f(x, y) \stackrel{déf.}{=} x.y$ (où l'on a identifié $\mathbb{F}_2^2 \times \mathbb{F}_2^2$ avec $\mathbb{F}_2^4$ et où comme souvent le symbole « . » désigne le produit scalaire sur $\mathbb{F}_2^4$). On sait depuis les travaux de Rothaus (cf. chapitre 5) que cette fonction est courbe et donc parfaitement non linéaire. On en déduit par application de la proposition précédente que pour chaque $x \in \mathbb{Z}_{16}$ la fonction $f \circ \phi_x^{-1} : \mathbb{Z}_{16} \to \mathbb{F}_2$ est $\mathbb{F}_2^4$-parfaitement non linéaire. Par contre une simple vérification montre que, par exemple, $f \circ \phi_0^{-1}$ n'est pas parfaitement non linéaire au sens de Carlet et Ding.

En effet posons $g \stackrel{déf.}{=} f \circ \phi_0^{-1}$ et testons si, disons, $d_3 g$ est équilibrée. Ainsi on a :

$$|\{x \in \mathbb{Z}_{16} | g(x+3) \oplus g(x) = \beta\}| = \begin{cases} 10 & \text{si } \beta = 0\ , \\ 6 & \text{si } \beta = 1\ . \end{cases}$$

Puisqu'en effet on a les égalités suivantes :

$$\begin{array}{rcrcrcl}
g(3) & \oplus & g(0) & = & f(1,1,0,0) \oplus f(0,0,0,0) & = & 0\ , \\
g(4) & \oplus & g(1) & = & f(0,0,1,0) \oplus f(1,0,0,0) & = & 0\ , \\
g(5) & \oplus & g(2) & = & f(1,0,1,0) \oplus f(0,1,0,0) & = & 1\ , \\
g(6) & \oplus & g(3) & = & f(0,1,1,0) \oplus f(1,1,0,0) & = & 0\ , \\
g(7) & \oplus & g(4) & = & f(1,1,1,0) \oplus f(0,0,1,0) & = & 1\ , \\
g(8) & \oplus & g(5) & = & f(0,0,0,1) \oplus f(1,0,1,0) & = & 1\ , \\
g(9) & \oplus & g(6) & = & f(1,0,0,1) \oplus f(0,1,1,0) & = & 0\ , \\
g(10) & \oplus & g(7) & = & f(0,1,0,1) \oplus f(1,1,1,0) & = & 0\ , \\
g(11) & \oplus & g(8) & = & f(1,1,0,1) \oplus f(0,0,0,1) & = & 1\ , \\
g(12) & \oplus & g(9) & = & f(0,0,1,1) \oplus f(1,0,0,1) & = & 0\ , \\
g(13) & \oplus & g(10) & = & f(1,0,1,1) \oplus f(0,1,0,1) & = & 0\ , \\
g(14) & \oplus & g(11) & = & f(0,1,1,1) \oplus f(1,1,0,1) & = & 0\ , \\
g(15) & \oplus & g(12) & = & f(1,1,1,1) \oplus f(0,0,1,1) & = & 0\ , \\
g(0) & \oplus & g(13) & = & f(0,0,0,0) \oplus f(1,0,1,1) & = & 1\ , \\
g(1) & \oplus & g(14) & = & f(1,0,0,0) \oplus f(0,1,1,1) & = & 1\ , \\
g(2) & \oplus & g(15) & = & f(0,1,0,0) \oplus f(1,1,1,1) & = & 0\ .
\end{array}$$

Il en résulte que la dérivée de g suivant la direction 3 n'est pas équilibrée et donc g n'est pas parfaitement non linéaire. On a donc exhibé une fonction $\mathbb{F}_2^4$-parfaitement non linéaire et non parfaitement non linéaire dans le cas où l'action est régulière mais non isomorphe à l'action par translation de $\mathbb{Z}_{16}$.

7.4.6 Conclusion

Le fait de fixer le type de l'action comme étant régulier semble bien trop contraignant pour construire des fonctions fondamentalement différentes des objets conventionnels. Ceci n'est en fait que partiellement vrai. Dans le cas où l'on dispose d'un groupe G isomorphe au groupe $T(H)$ dans son action sur l'ensemble sous-jacent à H, les fonctions G-parfaitement non linéaires sont effectivement très similaires aux fonctions classiquement parfaitement non linéaires. Ce n'est pas très surprenant puisque le groupe G agit essentiellement par translation sur H.

Cependant si maintenant on suppose que le groupe agissant régulièrement G est très dissemblable du groupe des translations de H, qu'il ne lui est en particulier pas isomorphe, il est possible d'exhiber des constructions distinctes, en un certain sens, de celles traditionnellement fournies par la théorie de Carlet et Ding. En effet si dans ce cas on peut un nouvelle fois se rapporter à une action par translation, ce n'est alors plus celle de H mais bien celle de G. Bien évidemment, les objets qui en découle se trouvent ainsi être radicalement différents des fonctions parfaitement non linéaires définies sur le groupe H.

7.5 Action régulière sur l'ensemble d'arrivée

Une manière à la fois très naturelle et subtile de raffiner la notion de non linéarité parfaite basée sur l'action d'un groupe consiste à prendre en compte non seulement une action sur l'ensemble de départ mais aussi sur l'ensemble d'arrivée d'un certain type de fonctions. En effet au même titre que l'on a remplacé les translations sur les variables d'une fonction, dans la définition de la non linéarité parfaite, on peut interpréter la différence $f(\mathbf{g}.x) - f(x) = \beta$ par les égalités suivantes

$$f(\mathbf{g}.x) = \beta + f(x) = \sigma_\beta(f(x))$$

c'est-à-dire l'application d'une certaine translation sur les valeurs de la fonction f. On peut donc une nouvelle fois substituer cette action par translation par n'importe quelle action de groupe régulière. Notons que l'on souhaite obtenir une notion structurelle et non particulière à chaque fonction. Aussi on ne considère pas le cas d'une action seulement fidèle sur l'ensemble d'arrivée. Sinon nous serions contraints de n'étudier que des fonctions *respectant* les orbites. Ainsi nous nous limitons au cas des actions régulières sur l'ensemble d'arrivée.

Soient (G, H) un couple de groupes finis commutatifs et (X, Y) un couple d'ensembles finis (non vides) tels que G agisse au moins fidèlement sur X et H régulièrement sur Y.

Définition 7.19. *Une fonction $f : X \to Y$ est dite (G, H)-parfaitement non linéaire si $\forall \mathbf{g} \in G^*$, $\forall \mathbf{h} \in H$,*

$$|\{x \in X | f(\mathbf{g}.x) = \mathbf{h}.f(x)\}| = \frac{|X|}{|Y|} \left(= \frac{|G|}{|H|} \right) .$$

Bien que généralisant précisément les notions introduites dans ce chapitre, il est possible de toujours se ramener au cas où seule l'action sur l'ensemble de départ est considérée

Proposition 7.17. *Soit $y_0 \in Y$. La fonction $f : X \to Y$ est (G, H)-parfaitement non linéaire si et seulement si la fonction $g : X \to H$ définie par $g \stackrel{déf.}{=} {\phi_{y_0}^H}^{-1} \circ f$, où $\phi_{y_0}^H$ désigne l'application orbitale de y_0 au sens de l'action de H sur Y, est G-parfaitement non linéaire.*

Preuve. Notons « $\top$» la loi de H que l'on suppose multiplicative.
Soit $(\mathbf{g}, \mathbf{h}) \in G^* \times H$. Nous montrons que pour $x \in H$ fixé, $f(\mathbf{g}.x) = \mathbf{h}.f(x) \Leftrightarrow D_{\mathbf{g}}g(x) = g(\mathbf{g}.x)\top(g(x))^{-1} = \mathbf{h}$ où $(g(x))^{-1}$ est l'inverse de $g(x)$ dans le groupe H.
Nous avons la séquence suivante d'équivalences.
$f(\mathbf{g}.x) = \mathbf{h}.f(x) \Leftrightarrow g(\mathbf{g}.x).y_0 = \mathbf{h}.(g(x).y_0)$ (par définition de g) $\Leftrightarrow g(\mathbf{g}.x).y_0 = (\mathbf{h}\top g(x)).y_0 \Leftrightarrow g(\mathbf{g}.x) = (\mathbf{h}\top g(x))$ (par le lemme 7.2) $\Leftrightarrow g(\mathbf{g}.x)\top(g(x))^{-1} = \mathbf{h}$.
Alors nous avons $\{x \in X | f(\mathbf{g}.x) = \mathbf{h}.f(x)\} = \{x \in X | g(\mathbf{g}.x)\top(g(x))^{-1} = \mathbf{h}\}$ ce qui nous permet de compléter la preuve. □

Les propriétés étudiées précédemment s'appliquent donc à ce type de fonctions. Evidemment comme pour les actions régulières sur l'ensemble de départ, nous pourrions distinguer les cas où l'action sur l'ensemble d'arrivée est ou non équivalente à une action par translation. Mais seraient ainsi obtenus des résultats similaires à ceux déjà introduits. Aussi[8], dans la suite, on se circonscrit au seul cas canonique de l'action par translation sur l'ensemble d'arrivée.

7.6 G-ensembles à différences

7.6.1 Introduction

Les indicatrices des ensembles à différences de Hadamard dans $\mathbb{F}_2^m$ déterminent de manière univoque toutes les fonctions booléennes courbes (ou parfaitement non linéaires) à valeurs dans $\mathbb{F}_2$ (voir dans le chapitre 5 la sous-section 5.3.6 p. 84). Cette caractérisation est l'une de celles conservées par les généralisations. Ainsi Carlet et Ding dans [CD04] ont démontré que les fonctions parfaitement non linéaires définies sur un groupe fini abélien G et à valeurs dans $\mathbb{F}_2$ sont aussi les indicatrices des ensembles à différences de Hadamard de G (et réciproquement). Cette dernière notion est immédiatement rappelée ci-dessous.

Définition 7.20. Soit $(G, +)$ un groupe fini de cardinal v. Soit $D \subset G$ de cardinal k. D est un (v, k, λ)-*ensemble à différences* de G si pour tout $\alpha \in G^*$, l'équation $x - y = \alpha$ admet exactement

[8] Puisque *point trop n'en faut*!

λ solutions distinctes dans D^2.
Supposons qu'il existe $n \in \mathbb{N}^*$ tel que $v = 4n^2$. Un *ensemble à différences de Hadamard* D de G est un $(4n^2, 2n^2 \pm n, n(n \pm 1))$-ensemble à différences de G.

Nous allons une nouvelle fois étendre cette notion en la « tordant ». En effet comme on peut aisément le remarquer

$$x - y = \alpha \Leftrightarrow x = \sigma_\alpha(y) \ .$$

Il est donc possible de remplacer l'action par translation par une autre action fidèle ou régulière. Cette approche, déjà effectuée à plusieurs reprises dans ce chapitre, nous permet de caractériser la G-non linéarité parfaite des fonctions à valeurs dans $\mathbb{F}_2$ via des objets combinatoires. Se faisant il devient alors possible de construire de nouvelles fonctions satisfaisant les concepts généralisés.

7.6.2 Cas d'une action fidèle

7.6.2.1 Caractérisation

Commençons par généraliser la notion de support d'une fonction introduite au chapitre 4.

Définition 7.21. Soit $f : X \to \mathbb{F}_2$. Le *support* de f est l'ensemble S_f défini par

$$S_f \stackrel{déf.}{=} \{x \in X | f(x) \neq 0\} \ .$$

Soit (G, X) un couple tel que G soit un groupe fini agissant (à gauche) fidèlement sur l'ensemble fini X.

Théorème 7.5. *Soit $f : X \to \mathbb{F}_2$. Alors pour tout $\mathbf{g} \in G$,*

$$|\{x \in X | D_{\mathbf{g}} f(x) = \beta\}| = \begin{cases} |X| - 2(|S_f| - |\mathbf{g}.S_f \cap S_f|) & \text{si } \beta = 0 \ , \\ 2(|S_f| - |\mathbf{g}.S_f \cap S_f|) & \text{si } \beta = 1 \ . \end{cases}$$

où pour tout $A \subset X$, $\mathbf{g}.A \stackrel{déf.}{=} \{\mathbf{g}.x \in X | x \in A\}$.

Preuve. Notons ϕ l'homomorphisme injectif de groupes de G dans $S(X)$ représentant l'action de groupe de G sur X. On peut appliquer le lemme 5.3 p. 85 puisque pour tout $\mathbf{g} \in G$, $\phi(\mathbf{g}) \in S(X)$. On a donc $f_{\phi(\mathbf{g})}(S_f) = |S_{D_{\mathbf{g}} f}|$ soit $|S_{D_{\mathbf{g}} f}| = 2(|S_f| - |\mathbf{g}.S_f \cap S_f|)$. Le résultat s'ensuit. □

Définition 7.22. Posons $v \stackrel{déf.}{=} |X|$. Soit $D \subset X$ et $k \stackrel{déf.}{=} |D|$. L'ensemble D est appelé G-(v, k, λ)-*ensemble à différences* de X si $\forall \mathbf{g} \in G^*$, l'équation

$$x = \mathbf{g}.y$$

admet exactement λ solutions distinctes $(x, y) \in D^2$.

Remarquons que le vocable utilisé de « différence » n'est en fait valide que si X est lui-même un groupe, puisque dans ce cas l'équation $x = \mathbf{g}.y$ correspond à la différence $x - \mathbf{g}.y = e_X$.

Théorème 7.6. *Supposons que $|X| \equiv 0 \pmod 4$. Soit $f : X \to \mathbb{F}_2$. La fonction f est G-parfaitement non linéaire si et seulement si S_f est un G-(v, k, λ)-ensemble à différences de X tel que*

$$\frac{|X|}{4} = k - \lambda \ .$$

Preuve. Supposons que S_f soit un G-(v, k, λ)-ensemble à différences de X tel que $\frac{|X|}{4} = k - \lambda$. Il est facile de voir que $\lambda = |\mathbf{g}.S_f \cap S_f|$ pour tout $\mathbf{g} \in G^*$ (par le lemme 5.4). Donc en appliquant le théorème précédent, on obtient pour tout $\mathbf{g} \in G^*$:

$$|\{x \in X | D_{\mathbf{g}} f(x) = \beta\}| = \begin{cases} v - 2(k - \lambda) & \text{si } \beta = 0 \ , \\ 2(k - \lambda) & \text{si } \beta = 1 \ . \end{cases}$$

Puisque par hypothèse $\frac{|X|}{4} = \frac{v}{4} = k - \lambda$ on a $v - 2(k-\lambda) = 4(k-\lambda) - 2(k-\lambda) = 2(k-\lambda)$. Donc pour tout $\beta \in \mathbb{F}_2$, $|\{x \in X | D_{\mathbf{g}} f(x) = \beta\}| = 2(k-\lambda) = \frac{|X|}{2}$ et donc f est G-parfaitement non linéaire.
Supposons maintenant que f soit G-parfaitement non linéaire.
On a donc pour tout $\mathbf{g} \in G^*$ et tout $\beta \in \mathbb{F}_2$, $|\{x \in X | f(\mathbf{g}.x) \oplus f(x) = \beta\}| = \frac{|X|}{2}$. D'après le théorème précédent, on a $\frac{|X|}{4} = |S_f| - |\mathbf{g}.S_f \cap S_f|$. Donc pour tout $\mathbf{g} \in G^*$, $|\mathbf{g}.S_f \cap S_f| = |S_f| - \frac{|X|}{4}$. Ainsi $|\mathbf{g}.S_f \cap S_f|$ est constant lorsque $\mathbf{g}$ parcourt G^*. On note « λ » cette constante *i.e.* $\lambda \stackrel{déf.}{=} |\mathbf{g}.S_f \cap S_f| = |S_f| - \frac{|X|}{4}$. Or cet entier λ représente aussi le nombre de solutions dans S_f^2 à l'équation $x = \mathbf{g}.y$ (par le lemme 5.4). Si on pose $k \stackrel{déf.}{=} |S_f|$, il en résulte finalement que S_f est un G-(v,k,λ)-ensemble à différences de X avec $\frac{v}{4} = k - \lambda$. □

Le lecteur attentif aura observé que nous avons délibérément omis le terme « commutatif » dans ce paragraphe. Le chapitre 8 consacré au cas des groupes non abéliens nous y a fortement incité comme nous le verrons alors.

7.6.2.2 Constructions

La caractérisation précise à laquelle nous venons d'aboutir nous permet de construire toute une série de fonctions G-parfaitement non linéaires à valeurs dans $\mathbb{F}_2$. Certaines constructions étant en outre très pertinentes du point de vue de la cryptographie. Les résultats exposés ici sont tirés d'un travail de collaboration avec James Davis, professeur de Mathématiques à l'Université de Richmond [PD05].

La première construction exhibée est un cas pathologique.

Proposition 7.18. *Soit $m \in \mathbb{N}^* \setminus \{1\}$. Soit G un groupe d'involutions sans point fixe de $\mathbb{F}_2^m$ d'ordre 4. Alors il existe un G-$(2^m, 2^{m-2}, 0)$-ensemble à différences dans $\mathbb{F}_2^m$.*

Preuve. Puisque les éléments de G n'ont pas de point fixe, toutes les orbites sous l'action fidèle de G sur $\mathbb{F}_2^m$ ont exactement quatre éléments et il y a donc 2^{m-2} telles orbites. On construit D comme un système de représentants de ces orbites *i.e.* D ne contient qu'un et un seul élément de chacune des orbites. En particulier $|D| = 2^{m-2}$. Par construction, il n'y a pas de solution à l'équation $x = \boldsymbol{\sigma}(y)$ dans D^2 pour $\boldsymbol{\sigma} \in G^*$ (sinon x et y seraient dans la même orbite et donc seraient égaux par définition de G ce qui contredirait le fait que les involutions sont sans point fixe). □

Nous présentons maintenant une construction générique très intéressante mais avant nous établissons le lemme technique suivant.

Lemme 7.9. *Soit $(G, \top)$ un groupe fini et X un ensemble non vide fini sur lequel G agit régulièrement (à gauche). Posons $v \stackrel{déf.}{=} |G|$. Soit $x_0 \in X$ fixé et $D \subset X$ avec $k \stackrel{déf.}{=} |D|$. On a alors : D est un G-(v,k,λ)-ensemble à différences de $X \Leftrightarrow \phi_{x_0}^{-1}(D) = \{\phi_{x_0}^{-1}(x) \in G | x \in D\}$ est un (v,k,λ)-ensemble à différences de G.*

Preuve. L'ensemble D est un G-(v,k,λ)-ensemble à différences de $X \Leftrightarrow \forall \mathbf{g} \in G^*$, il existe exactement λ solutions à l'équation $x = \mathbf{g}.y$ dans D^2.

Puisque l'action est régulière, il existe un et un seul $(\mathbf{g}_1, \mathbf{g}_2) \in G^2$ tel que $x = \phi_{x_0}(\mathbf{g}_1) = \mathbf{g}_1.x_0$ et $y = \phi_{x_0}(\mathbf{g}_2) = \mathbf{g}_2.x_0$. Alors :

D est un G-(v,k,λ)-ensemble à différences de $X \Leftrightarrow \forall \mathbf{g} \in G^*$, il existe exactement λ solutions à l'équation $\phi_{x_0}(\mathbf{g}_1) = \mathbf{g}.\phi_{x_0}(\mathbf{g}_2)$ dans $(\phi_{x_0}^{-1}(D))^2$.

L'équation $\phi_{x_0}(\mathbf{g}_1) = \mathbf{g}.\phi_{x_0}(\mathbf{g}_2)$ peut être ré-écrite de la manière suivante,

$$\phi_{x_0}(\mathbf{g}_1) = \mathbf{g}_1.x_0 = \mathbf{g}.\phi_{x_0}(\mathbf{g}_2) = \mathbf{g}.\mathbf{g}_2.x_0 = (\mathbf{g}\top\mathbf{g}_2).x_0 = \phi_{x_0}(\mathbf{g}\top\mathbf{g}_2) \ .$$

En outre comme ϕ_{x_0} est une application bijective, l'équation $\phi_{x_0}(\mathbf{g}_1) = \mathbf{g}.\phi_{x_0}(\mathbf{g}_2)$ est équivalente à l'équation $\mathbf{g}_1 = \mathbf{g}\top\mathbf{g}_2$ et donc à l'équation $\mathbf{g}_1\top\mathbf{g}_2^{-1} = \mathbf{g}$. Nous obtenons ainsi :

D est G-(v,k,λ)-ensemble à différences de $X \Leftrightarrow \forall \mathbf{g} \in G^*$, il existe exactement λ solutions à l'équation $\mathbf{g}_1\top\mathbf{g}_2^{-1} = \mathbf{g}$ dans $(\phi_{x_0}^{-1}(D))^2$, qui est la définition d'un (v,k,λ)-ensemble à différences (classique) de G (puisque $v = |X| = |G|$ et $k = |D| = |\phi_{x_0}^{-1}(D)|$). □

Théorème 7.7. *Soit $(m,n) \in (\mathbb{N}^*)^2$ tel que $m \geq 2n$. Soit G un groupe d'involutions sans point fixe de $\mathbb{F}_2^m$ d'ordre 2^{2n}. Posons $4k^2 \stackrel{déf.}{=} 2^{2n}$. Alors pour tout $j \in \{0,\ldots,\frac{2^m}{4k^2}\}$, il existe un G-$(2^m, (2k^2-k)j + (2k^2+k)(\frac{2^m}{4k^2} - j), (k^2-k)j + (k^2+k)(\frac{2^m}{4k^2} - j))$-ensemble à différences de $\mathbb{F}_2^m$.*

Preuve. Le groupe G agit fidèlement et transitivement sur chacune de ses orbites (dans son action sur $\mathbb{F}_2^m$). La transitivité est évidente. Il en est de même pour la fidélité puisqu'aucun des éléments différents de l'identité de G n'a de point fixe.

Puisque G est un groupe abélien d'ordre $2^{2n} = 4k^2$, il possède des ensembles à différences de Hadamard [Jun92] ; les paramètres sont donc $(4k^2, 2k^2 \pm k, k^2 \pm k)$. De tels ensembles à différences avec un « $-$ » (dans les paramètres) sont les ensembles à différences de Hadamard usuels et ceux avec un « $+$ » représentent les compléments.

D'après le lemme précédent, chaque ensemble à différences de Hadamard de G correspond à un G-ensemble à différences dans une orbite $\boldsymbol{\mathcal{O}}_G(x)$ avec les mêmes paramètres. Soit alors A un sous-ensemble de $\mathbb{F}_2^m$ qui ne contienne qu'un et un seul élément de chacune des orbites (en particulier $|A| = \frac{2^m}{4k^2}$). Alors pour tout $(x_0,x_1) \in A^2$ tel que $x_0 \neq x_1$ et $\forall (D,D')$ paire d'ensembles à différences de Hadamard de G, $\phi_{x_0}(D) \cap \phi_{x_1}(D') = \emptyset$. Ceci est dû au fait que pour $i \in \{0,1\}$, $\phi_{x_i}(D) \subset \boldsymbol{\mathcal{O}}_G(x_i)$ et $\boldsymbol{\mathcal{O}}_G(x_0) \cap \boldsymbol{\mathcal{O}}_G(x_1) = \emptyset$ puisque $x_0 \neq x_1$ et par construction de A.

Pour chacune des orbites $\boldsymbol{\mathcal{O}}_G(x)$ $(x \in A)$ on choisit un ensemble à différences de Hadamard de G (éventuellement le même) dénoté par « D_x ». Si j est le nombre d'ensembles à différences de Hadamard usuels alors $\frac{2^m}{4k^2} - j$ est le nombre de compléments. Alors on définit $D \stackrel{déf.}{=} \bigcup_{x \in A} \phi_x(D_x)$. Il s'agit d'une union disjointe de G-ensembles à différences d'orbites de X avec les paramètres de type Hadamard (ceux de $\phi_x(D_x)$ correspondants à ceux de D_x).

Maintenant nous montrons que D est lui-même un G-ensemble à différences de X. Tout d'abord, $|D| = \sum_{x \in A} |D_x| = (2k^2-k)j + (2k^2+k)(\frac{2^m}{4k^2} - j)$. Soit $\boldsymbol{\sigma} \in G^*$. Pour tout $x \in A$, l'équation $y = \boldsymbol{\sigma}(z)$ a exactement λ_x solutions dans $(\phi_x(D_x))^2$, où $\lambda_x \stackrel{déf.}{=} k^2 \pm k$ selon que D_x est un ensemble à différences de Hadamard usuel ou un complément, puisque $\phi_x(D_x)$ est un G-ensemble à différences de $\boldsymbol{\mathcal{O}}_G(x)$ avec les mêmes paramètres que ceux de D_x. Comme les ensembles $\phi_x(D_x)$ sont tous mutuellement disjoints, l'équation $y = \boldsymbol{\sigma}(z)$ a exactement $\sum_{x \in A} \lambda_x = (k^2-k)j + (k^2+k)(\frac{2^m}{4k^2} - j)$

solutions dans D^2. La conclusion de la preuve s'ensuit. □

Corollaire 7.6. *Soit $(m,n) \in (\mathbb{N}^*)^2$ tel que $m \geq 2n$. Soit G un groupe d'involutions sans point fixe de $\mathbb{F}_2^m$ d'ordre 2^{2n}. Posons $v \stackrel{déf.}{=} 2^m$. Alors il existe un G-(v,k,λ)-ensemble à différences de $\mathbb{F}_2^m$ tel que $v = 4(k-\lambda)$.*

Preuve. Il suffit d'utiliser le théorème précédent et de vérifier que pour tout $j \in \{0,\ldots,\frac{2^m}{4k^2}\}$, $4\left((2k^2-k)j + (2k^2+k)(\frac{2^m}{4k^2}-j) - (k^2-k)j - (k^2+k)(\frac{2^m}{4k^2}-j))\right) = 2^m$ (où $4k^2 \stackrel{déf.}{=} 2^{2n}$), ce qui ne pose pas de difficulté particulière. □

Remarque 7.8. Pour $m \geq 2n$, il existe des groupes G d'involutions sans point fixe de $\mathbb{F}_2^m$ et d'ordre 2^{2n}. Par exemple, si l'on considère les éléments α de $\mathbb{F}_2^m$ pour lesquels les dernières $m-2n$ coordonnées sont égales à zéro. Alors les translations par de tels α ainsi que l'identité constituent un groupe du type souhaité. Il en est de même de leurs groupes conjugués.

Le théorème précédent nous permet ainsi de construire un nombre important de fonction G-parfaitement non linéaires définies sur un espace vectoriel $\mathbb{F}_2^m$ et à valeurs dans $\mathbb{F}_2$. Un exemple de la puissance et de la pertinence de ce résultat est le suivant. Si on considère le cas impair où $m = 9$ et $n = 2$, les groupes d'involutions sans point fixe considérés sont donc d'ordre 16 et la taille de $\mathbb{F}_2^m$ est 512. Le théorème précédent garantit alors l'existence de G-ensembles à différences avec les paramètres suivants : $(512,192,64)$, $(512,196,68)$, $(512,200,72)$, $(512,204,76)$, …, $(512,320,192)$. Il y a un total de 33 familles de paramètres dans ce cas, et tous les ensembles à différences sont nouveaux puisqu'il n'existe pas d'ensemble à différences de Hadamard dans un groupe d'ordre 512.

Illustrons encore nos résultats dans le cas où les fonctions parfaitement non linéaires n'existent pas. Supposons toujours que $m = 9$ et cette fois-ci posons $n = 4$ et donc $2n = 8$. Alors le groupe G est d'ordre 256 et le théorème précédent nous assure l'existence de G-ensembles à différences dans $\mathbb{F}_2^m$ de paramètres $(512,240,112)$, $(512,256,128)$ ou encore $(512,272,144)$. Comme les groupes G sont ici à un isomorphisme près des sous-groupes du groupe des translations de $\mathbb{F}_2^m$, nous pouvons interpréter ce résultat en termes cryptographiques, par le fait que nous avons construit les fonctions les plus « proches » des fonctions courbes classiques (dans un cas où ces dernières n'existent pas). Il s'agit donc d'une autre approche de la problématique que celle de fonction presque parfaitement non linéaire. En outre nous offrons un cadre algébrique standard et uniformisé aux différentes versions de la non linéarité parfaite dans les cas idéaux.

La dernière construction exposée maintenant ne repose pas sur la concaténation d'ensembles à différences de Hadamard. Elle permet en outre de s'abstraire de la condition de parité du cardinal du groupe agissant.

Lemme 7.10. *Soit $m \in \mathbb{N}^*$. Chaque $\alpha \in \mathbb{F}_2^{m\,*}$ est contenu dans $2^{m-1}-1$ sous-groupes de $\mathbb{F}_2^m$ d'ordre 2^{m-1}.*

Preuve. L'énoncé du lemme peut s'interpréter comme une question sur les espaces vectoriels, à savoir dans combien de sous-espaces vectoriels de dimension $m-1$ (sur $\mathbb{F}_2$) de $\mathbb{F}_2^m$, un vecteur non nul α donné est-il contenu ?
Nous construisons une base contenant α. Nous ne pouvons utiliser ni $0_{\mathbb{F}_2^m}$ ni α en tant que second vecteur de la base. Ainsi nous avons 2^m-2 choix possibles pour ce vecteur, noté « e_2 ». Une fois e_2 choisi, nous ne pouvons prendre aucune combinaison linéaire de α et e_2. Il en résulte que l'on a 2^m-4 choix possibles pour le troisième vecteur de la base (noté « e_3 »). En continuant de cette manière, nous aurons 2^m-2^{m-2} choix possibles pour e_{m-1} puisque nous ne pouvons utiliser aucune combinaison linéaire de la famille $\{\alpha, e_2, e_3, \ldots, e_{m-2}\}$. Afin d'obtenir le nombre correct,

il nous faut maintenant diviser par le nombre de bases pour un sous-espace V de dimension $m-1$ (contenant α). Nous avons $2^{m-1}-2$ choix pour le second vecteur d'une base de V puisque l'on ne peut prendre ni 0_V ni α. Nous avons ensuite $2^{m-1}-4$ choix pour le troisième vecteur. Nous continuons ainsi jusqu'à ce que l'on ait $2^{m-1}-2^{m-2}$ choix pour le dernier vecteur. Finalement le nombre recherché est

$$\frac{(2^m-2)(2^m-4)\dots(2^{m-1}-2^{m-2})}{(2^{m-1}-2)(2^{m-1}-4)\dots(2^{m-1}-2^{m-2})} = 2^{m-1}-1 \ .$$

□

Théorème 7.8 (Construction Hyperplan). *Soient deux entiers quelconques m et t, m étant non nul alors que t peut éventuellement l'être. Soit G un groupe d'involution sans point fixe de $\mathbb{F}_2^{2m+t}$ d'ordre 2^m. Alors il existe un G-$(2^{2m+t}, 2^t((2^{m-1}-1)(2^m-1)+1), 2^t(2^{m-1}-1)(2^{m-1}-2))$-ensemble à différences de $\mathbb{F}_2^{2m+t}$. En particulier les paramètres satisfont l'équation $v = 4(k-\lambda)$.*

Preuve. En tant que groupe G est isomorphe au groupe additif $\mathbb{F}_2^m$. Il possède donc 2^m-1 sous-groupes d'ordre 2^{m-1}, dénotés H_i pour $1 \leq i \leq 2^m-1$. On observe que chacune des orbites sous l'action de G sur $\mathbb{F}_2^{2m+t}$ possède exactement 2^m éléments puisque tout élément non nul de G agit comme une involution **sans point fixe** sur $\mathbb{F}_2^{2m+t}$, ainsi il y a exactement 2^{m+t} telles orbites dans $\mathbb{F}_2^{2m+t}$. On choisit un système de représentants de ces orbites et une énumération des représentants : pour $(i,j) \in \{1,\dots,2^m\} \times \{0,\dots,2^t-1\}$, $x_{i,j}$ est le représentant du $i+j2^m$-ième orbite $\boldsymbol{\mathcal{O}}_G(x_{i,j}) = \{\boldsymbol{\sigma}(x_{i,j}) \in \mathbb{F}_2^{2m+t} | \boldsymbol{\sigma} \in G\}$. En particulier si $x_{i,j} \neq x_{i',j'}$ alors $\boldsymbol{\mathcal{O}}_G(x_{i,j}) \cap \boldsymbol{\mathcal{O}}_G(x_{i',j'}) = \emptyset$.

Pour chaque $j \in \{0,\dots,2^t-1\}$, on associe le sous-groupe H_i à l'orbite $\boldsymbol{\mathcal{O}}_G(x_{i,j})$ (donc pour i variant de 1 à 2^m-1) et on construit l'ensemble $D_{i,j} = \{\boldsymbol{\sigma}(x_{i,j}) | \boldsymbol{\sigma} \in H_i, \boldsymbol{\sigma} \neq e_G\} \subset \boldsymbol{\mathcal{O}}_G(x_{i,j})$. Finalement on constuit $D_j = \bigcup_{i=1}^{2^m-1} (D_{i,j}) \cup \{x_{2^m,j}\}$.

Par construction, à j fixé, $D_{i,j} \cap D_{i',j} = \emptyset$ pour tout $i \neq i'$. On a en particulier $|D_j| = 1 + \sum_{i=1}^{2^m-1} |D_{i,j}|$. Or $|D_{i,j}| = |H_i| - 1 = 2^{m-1}-1$ et donc $|D_j| = (2^m-1)(2^{m-1}-1)+1$.

Puis l'on construit l'ensemble suivant :

$$D = \bigcup_{j=0}^{2^t-1} D_j \ .$$

On remarque facilement que $D_j \cap D_{j'} = \emptyset$ pour tout $j \neq j'$ et donc que D est une réunion disjointe. Son cardinal est donc égal à $\sum_{j=0}^{2^t-1} |D_j| = 2^t((2^m-1)(2^{m-1}-1)+1)$.

On a donc déjà montré que les paramètres $v = |\mathbb{F}_2^{2m+t}|$ et $k = |D|$ sont bien égaux aux valeurs données dans l'énoncé du théorème. Il suffit donc maintenant de montrer que D est un G-(v,k,λ)-ensemble à différences de $\mathbb{F}_2^{2m+t}$ avec $\lambda = 2^t(2^{m-1}-1)(2^{m-1}-2)$.

Nous montrons maintenant que pour tout $\boldsymbol{\sigma} \in G$ non nul, il y a exactement λ solutions dans D^2 à l'équation $x = \boldsymbol{\sigma}(y)$. Remarquons tout de suite que si x et y ne sont pas dans la même orbite, on a aucune solution.
Soit donc $(i,j) \in \{1,\dots,2^m\} \times \{0,\dots,2^t-1\}$. Si $i = 2^m$ alors on n'a aucune solution à l'équation $x = \boldsymbol{\sigma}(y)$ dans D^2 pour $\boldsymbol{\sigma} \in G$ non nul (puisque D ne contient alors que $x_{2^m,j}$ et que $\boldsymbol{\sigma}$ est non nul et sans point fixe). Supposons donc que $i \in \{1,\dots,2^m-1\}$.

Si $(x,y) \in \boldsymbol{\mathcal{O}}_G(x_{i,j})^2$ est une solution dans D^2 à l'équation $x = \boldsymbol{\sigma}(y)$ pour $\boldsymbol{\sigma} \notin H_i$, alors $x = \boldsymbol{\tau}(x_{i,j})$ et $y = \boldsymbol{\tau}'(x_{i,j})$ pour $(\boldsymbol{\tau}, \boldsymbol{\tau}') \in H_i^2$ implique que $\boldsymbol{\tau}(x_{i,j}) = x = \boldsymbol{\sigma}(y) = (\boldsymbol{\sigma} \circ \boldsymbol{\tau}')(x_{i,j})$. Puisque l'action de G sur ses orbites est régulière, on a alors $\boldsymbol{\tau} = \boldsymbol{\sigma} \circ \boldsymbol{\tau}'$ et donc $\boldsymbol{\sigma} = \boldsymbol{\tau} \circ (\boldsymbol{\tau}')^{-1} \in H_i$, ce qui constitue une contradiction et il n'y a donc pas de solution de cette forme.
Un argument similaire montre que pour chaque $(i,j) \in \{1, \ldots, 2^m - 1\} \times \{0, \ldots, 2^t - 1\}$ fixé, nous avons (au moins une solution) quand $(x,y) \in \boldsymbol{\mathcal{O}}_G(x_{i,j})$ et $\boldsymbol{\sigma} \in H_i$ et ce dès que $\boldsymbol{\sigma} = \boldsymbol{\tau} \circ (\boldsymbol{\tau}')^{-1}$ pour $(\boldsymbol{\tau}, \boldsymbol{\tau}') \in H_i^2$ (on a bien alors $x = \boldsymbol{\tau}(x_{i,j}) = \boldsymbol{\sigma}(y) = \boldsymbol{\sigma}(\boldsymbol{\tau}'(x_{i,j}))$ avec $(x,y) \in D_{i,j}^2 \subset D^2$ par construction). Il y a $2^{m-1} - 2$ solutions $(\boldsymbol{\tau}, \boldsymbol{\sigma} \circ \boldsymbol{\tau}) \in H_i^2$ (on a $|H_i| = 2^{m-1}$ couples $(\boldsymbol{\tau}, \boldsymbol{\sigma} \circ \boldsymbol{\tau})$ pour $\boldsymbol{\sigma}$ fixé mais on exclue les solutions $(e_G, \boldsymbol{\sigma})$ et $(\boldsymbol{\sigma}, e_G)$ puisque sinon $x = x_{i,j}$ ou bien $y = x_{i,j}$ ce qui est impossible par construction de $D_{i,j}$).
Remarquons de plus que si $(\boldsymbol{\tau}(x_{i,j_0}), (\boldsymbol{\sigma} \circ \boldsymbol{\tau})(x_{i,j_0}))$ est une solution dans D^2 à l'équation $x = \boldsymbol{\sigma}(y)$ $(\boldsymbol{\sigma} \in H_i)$ alors pour chaque $j \in \{0, \ldots, 2^t - 1\}$, $(\boldsymbol{\tau}(x_{i,j}), (\boldsymbol{\sigma} \circ \boldsymbol{\tau})(x_{i,j}))$ est une solution distincte (si $j \neq j_0$). Il y a donc 2^t telles solutions.
Enfin chaque $\boldsymbol{\sigma} \in G$ non nul est contenu dans $2^{m-1} - 1$ sous-groupes H_i (par le lemme 7.10, en utilisant le fait que G est isomorphe à $\mathbb{F}_2^m$). Au final, on a donc $\lambda = 2^t(2^{m-1} - 1)(2^{m-1} - 2)$. □

Cette dernière construction, en ce qui concerne le cas des actions fidèles, est particulièrement intéressante. En effet, si l'on suppose que m et t sont deux entiers **impairs** alors ni $f : \mathbb{F}_2^{2m+t} \to \mathbb{F}_2$ ni les fonctions $f_x : G \to \mathbb{F}_2$ (pour $x \in \mathbb{F}_2^{2m+t}$) ne sauraient être parfaitement non linéaires au sens classique. Parce que $2m + t$ est alors impair, il en résulte donc que f ne peut être booléenne courbe et puisque G est isomorphe à $\mathbb{F}_2^m$, f_x s'identifie à une fonction $g : \mathbb{F}_2^m \to \mathbb{F}_2$ et comme m est impair, g (et donc f_x) ne peut être courbe. Cette construction constitue bien le contre-exemple annoncé à la question soulevée après la preuve du théorème 7.2 p. 146. Il est donc possible de construire des fonctions G-parfaitement non linéaires définies sur un ensemble $\mathbb{F}_2^m$ et à valeurs dans $\mathbb{F}_2$ même dans les cas où m est impair et $|G|$ n'est pas un carré parfait, soit en d'autres termes, dans des cas où il n'existe pas de fonctions de $\mathbb{F}_2^{\mathbb{F}_2^m}$ ni de $\mathbb{F}_2^G$ parfaitement non linéaires au sens classique.

7.6.3 Cas d'une action régulière

De même que pour la caractérisation par la transformée de Fourier de la non linéarité parfaite, le fait de considérer une action régulière plutôt que fidèle permet, en diminuant sensiblement les degrés de liberté, de préciser l'allure des fonctions G-parfaitement non linéaires.

Soit un couple (G, X) où G est un groupe fini agissant (à gauche) régulièrement sur l'ensemble fini non vide X. Posons $v \overset{déf.}{=} |G| = |X|$.

Théorème 7.9. *Soit $f : X \to \mathbb{F}_2$. Alors la fonction f est G-parfaitement non linéaire si et seulement si S_f est un G-$(4n^2, 2n^2 \pm n, n(n \pm 1))$-ensemble à différences de H avec $|X| = 4n^2$.*

Preuve. Commençons par l'implication directe. Le fait que la fonction f soit G-parfaitement non linéaire implique que $\forall (\mathbf{g}, \beta) \in G^* \times \mathbb{F}_2$, $|\{x \in X | D_{\mathbf{g}} f(x) = \beta\}| = \dfrac{|X|}{2} = 2(|S_f| - |\mathbf{g}.S_f \cap S_f|)$ (d'après le théorème 7.5). Alors $\forall \mathbf{g} \in G^*$, $|\mathbf{g}.S_f \cap S_f|$ est constant. On désigne par « λ » cette constante. Puisque $\forall \sigma \in G^*$, il y a $|\mathbf{g}.S_f \cap S_f| = \lambda$ solutions $(x,y) \in S_f^2$ à l'équation $x = \mathbf{g}.y$, S_f est un G-$(|X|, |S_f|, \lambda)$-ensemble à différences de X. D'après le lemme 7.9, pour n'importe quel $x_0 \in X$, $\phi_{x_0}^{-1}(S_f)$ est un $(|X|, |S_f|, \lambda)$-ensemble à différences de G. Puisque $|G| = |X| = 4(|S_f| - |\mathbf{g}.S_f \cap S_f|)$, nous avons $|G| \equiv 0 \pmod 4$ et d'après [Jun92] un tel ensemble à différences n'existe que si $|G| = 4n^2$ (pour un certain n). Il s'agit d'un ensemble à différences de Hadamard *i.e.* ses paramètres ont la forme $(4n^2, 2n^2 \pm n, n(n \pm 1))$.
Démontrons l'implication de sens réciproque.

Supposons donc que S_f soit un G-$(4n^2, 2n^2 \pm n, n(n \pm 1))$-ensemble à différences de X où $|X| = 4n^2$. D'après le théorème 7.5 on en déduit rapidement le résultat. □

Comme dans le cas classique les G-ensembles à différences de type Hadamard déterminent toute les fonctions G-parfaitement non linéaires à valeurs dans $\mathbb{F}_2$ quand l'action est régulière. Par ailleurs il est possible d'utiliser le théorème précédent afin d'énoncer des résultats de non existence. Nous disposons par exemple de la proposition ci-dessous.

Proposition 7.19. *Soit X un ensemble fini tel que $|X| = 4n^2$ avec $n = 2^m$ $(m > 0)$. Soit $\pi \in S(X)$ une permutation circulaire de longueur maximale $|X|$. Alors nous disposons des trois assertions suivantes :*

1. $|\langle\pi\rangle| = |X|$;
2. $\langle\pi\rangle$ *agit régulièrement sur* X ;
3. *Il n'existe pas de fonction $f : X \to \mathbb{F}_2$ qui soit $\langle\pi\rangle$-parfaitement non linéaire.*

Preuve.

1. On a $|\langle\pi\rangle| = |X|$ puisque l'ordre de π est $|X|$;
2. Soit $(x, y) \in X^2$. Si $x = y$, l'identité envoie alors x sur y. Et il n'existe pas de $k \in \mathbb{N}^*$ tel que $k < |X|$ et $\pi^k(x) = x$ sinon π ne peut être un cycle de longueur maximale. Supposons que $x \neq y$. Ces deux éléments apparaissent une et une seule fois dans la décomposition en cycles de π (puisque la permutation π n'est composée que d'un unique cycle où toutes les valeurs de X apparaissent une fois seulement). Donc il existe un et un seul $k \in \mathbb{N}^*$ tel que $k < |X|$ et $\pi^k(x) = y$. Il en résulte que l'action de $\langle\pi\rangle$ sur X est régulière ;
3. D'après le théorème précédent si $f : X \to \mathbb{F}_2$ est $\langle\pi\rangle$-parfaitement non linéaire alors S_f est un $\langle\pi\rangle$-ensemble à différences de type Hadamard de X. Donc pour $x_0 \in X$, $\phi_{x_0}^{-1}(S_f)$ se trouve être un ensemble à différences de Hadamard de $\langle\pi\rangle$. D'après [Kra93] les ensembles à différences dans un groupe abélien de cardinal $4n^2 = 2^{2m+2}$ n'existent que si l'exposant du groupe est inférieur ou égal à $4n$ ce qui n'est pas le cas de $\langle\pi\rangle$ puisque $exp(\langle\pi\rangle) = 4n^2 > 4n$.

□

Une nouvelle fois nous avons montré que malgré la régularité de l'action, le fait d'être G-parfaitement non linéaire n'est pas strictement équivalent au fait d'être parfaitement non linéaire au sens de Carlet et Ding. En effet si pour X on choisit $\mathbb{F}_2^m$ tel que m est pair et $m > 2$. Alors on sait que des fonctions $f : \mathbb{F}_2^m \to \mathbb{F}_2$ courbes donc parfaitement non linéaires existent. Par contre d'après la proposition précédente, quelle que soit la permutation circulaire $\pi \in S(\mathbb{F}_2^m)$ de longueur 2^m, il n'existe pas de fonction $f : \mathbb{F}_2^m \to \mathbb{F}_2$ qui soit $\langle\pi\rangle$-parfaitement non linéaire.

7.6.4 Conclusion

La non linéarité parfaite classique au sens de Carlet et Ding des fonctions à valeurs dans $\mathbb{F}_2$ possède une formulation combinatoire strictement équivalente via les ensembles à différences de Hadamard. Les translations jouent un rôle fondamental dans la définition de tels ensembles. Encore une fois, de manière quasi mécanique et obsessionnelle, celles-ci ont été remplacées par des actions de groupe fidèles ou régulières.

En adaptant ces objets à nos notions algébriques généralisées, nous obtenons une nouvelle lecture de ceux-ci pour les fonctions à valeurs dans $\mathbb{F}_2$. Il se trouve ainsi que les fonctions binaires G-parfaitement non linéaires sont toutes des indicatrices de *G-ensembles à différences*, c'est-à-dire ces ensembles D pour lesquels l'équation $x = \mathbf{g}.y$ possède exactement λ solutions (pour un

certain λ) dans D^2 pour tout $\mathbf{g} \in G^*$.

Si, et ce n'est pas étonnant, la régularité des actions nous condamne à considérer, comme dans le cas classique, des paramètres (v, k, λ) de type Hadamard pour ces ensembles *i.e.* $v = 4n^2$, $k = 2n^2 \pm n$ et $\lambda = n(n \pm 1)$, la fidélité, elle, conduit à une notion moins restrictive. Ainsi il convient simplement que les paramètres satisfassent l'équation $v = 4(k - \lambda)$ pour fournir des fonctions G-parfaitement non linéaires à valeurs dans $\mathbb{F}_2$. Observons que, bien entendu, les paramètres de Hadamard vérifient aussi en particulier cette équation (le contraire eut été surprenant et paradoxal sachant qu'une action régulière est aussi fidèle), seulement dans le cas fidèle, il s'agit de l'unique contrainte à vérifier. Le degré de liberté obtenu par le passage des actions régulières aux actions fidèles permet de construire de nouveaux objets combinatoires bien différents de ceux traditionnellement rencontrés et, de fait, des fonctions G-parfaitement non linéaires elles aussi fondamentalement inédites. La pertinence et l'utilité de nos résultats sont en particulier illustrés par la construction de fonctions G-parfaitement non linéaires dans des cas où leurs versions originales au sens booléen n'existent pas.

7.7 Conclusion

Dans ce premier chapitre de la seconde partie du manuscrit nous avons répondu en partie à la question posée dans le dernier chapitre de la première partie, à savoir,

> « que se passe-t-il si on substitue aux translations un autre type de permutations ? »

Cette interrogation, à l'instar de nombreuses questions à la formulation simple, est plus complexe qu'elle n'y paraît. Aussi il nous a semblé indispensable de limiter, dans ce chapitre au moins, son champ d'application en ne considérant que des groupes de permutations commutatifs. Le cas non abélien étant pour le moment laissé de côté. Ceci étant dit, comment nous y sommes nous pris pour construire la fameuse réponse ?

Une observation élémentaire de la notion de non linéarité parfaite au sens de Carlet et de Ding révèle l'importance des translations. En prenant un peu de recul, on s'aperçoit alors qu'il est possible de les interpréter dans un cadre conceptuel plus général, celui des actions de groupe. Ainsi, le *remplacement des translations par un autre type de permutations* signifie en substance la considération d'autres actions de groupe que celle d'un groupe sur lui-même par translation. La première étape conduisant à la réponse consista ainsi en la substitution de la loi de composition interne d'un groupe par une loi « externe » basée sur l'action d'un autre groupe.

A ce stade, nous avons simplement *translaté* le problème dans un contexte plus abstrait. Mais comme souvent l'abstraction nous offre de multiples choix par particularisation. Ainsi nous avons divisé le nouveau concept en deux parties selon que l'action de groupe considérée est *fidèle* ou *régulière*. Les translations d'un groupe agissent régulièrement sur celui-ci. Cela signifie que chaque élément d'un groupe n'est atteignable depuis un autre élément que par une et une seule translation. Cela s'opposant aux actions fidèles qui soit envoient en un « coup » un point sur un autre de plusieurs manières, soit ne lient pas certains éléments entre eux. En considérant les actions fidèles nous disposons d'un panel de possibilités beaucoup plus large que celui proposé par les actions régulières. Ainsi nous avons étendu de façon très élégante le concept classique. Nous jouissons maintenant d'une structure uniforme et homogène pour représenter plusieurs situations possibles.

Nous le savons depuis le chapitre 5, la non linéarité parfaite se formule via la transformée de Fourier par la notion de fonction courbe. Aussi, par souci de complétude, nous avons étudié pour les concepts généralisés, aussi bien au sens des actions fidèles que régulières, une caractérisation

duale du même type. Pour la seconde version, la notion duale obtenue est très proche de celle du contexte traditionnel (au sens de Logachev, Salnikov et Yachshenko). Toutefois, lorsque la seule contrainte satisfaite par l'action est la fidélité, les résultats obtenus sont moins particularisés : les nouveaux concepts se représentent sous la forme de fonctions courbes *en moyenne*.

A cette étape, nous disposons d'un premier type de généralisation de la notion de non linéarité parfaite au sens des actions de groupe ainsi que d'une caractérisation duale par une formule de conservation de l'énergie. Si les actions fidèles, de fait, fournissent des fonctions différentes des objets usuellement rencontrés, qu'en est-t-il des actions régulières ? Aussi surprenant que cela puisse paraître, même dans ce cas il est possible d'aboutir à des choses nouvelles. Pour ce faire, nous avons considéré le cas d'une action régulière d'un groupe G sur un autre groupe H et pointé deux sous-cas importants selon que G, dans son opération sur H, se distingue ou non du groupe des translations de H. Si G est essentiellement équivalent à $T(H)$ tout se déroule comme dans la version classique. Au contraire, quand G est véritablement distinct de $T(H)$, des différences sensibles apparaissent naturellement. Nous avons de la sorte obtenu un nouveau type de généralisation selon que le groupe agissant ressemble ou non aux translations du groupe sur lequel il agit.

Finalement notre intérêt se porta sur l'étude d'une classe particulière de fonctions, celles à valeurs dans $\mathbb{F}_2$. En reprenant la démarche précédente consistant à remplacer les translations par des actions de groupe fini commutatif fidèles ou régulières, la notion combinatoire classique d'ensemble à différences a été généralisée. Le cas fidèle produit les résultats les plus pertinents puisque de nouveaux « ensembles à différences » ont ainsi été exhibés garantissant l'existence de fonctions parfaitement non linéaires au sens généralisé du terme dans des cas où les versions traditionnelles de ces fonctions sont impossibles.

Dans le prochain chapitre, le dernier de ce manuscrit, nous rencontrons un troisième type de généralisation en considérant le cas des groupes finis **non abéliens** et nous répondons ainsi complètement à la question rappelée au début de cette conclusion.

Chapitre 8

Non linéarité parfaite : cas non commutatif

La symétrie, c'est l'ennui.

VICTOR HUGO, *Les misérables*

Sommaire

8.1 Introduction

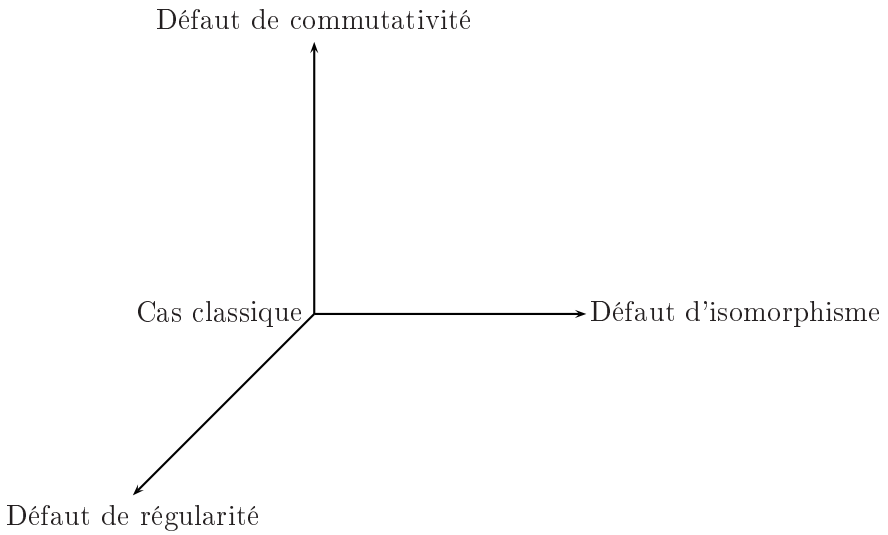
Le chapitre précédent contient une généralisation logique et élégante de la non linéarité parfaite, au sens de Carlet et Ding (cf. chapitre 6), reposant essentiellement sur la substitution de l'action naturelle par translation par une action de groupe fini commutatif quelconque. Cette approche, plus abstraite, permet d'envisager plusieurs variantes par spécialisation selon les propriétés des actions considérées. Les deux principales alternatives dépendant du fait que le groupe abélien G opère fidèlement ou régulièrement sur un ensemble fini.

Une formule de conservation de l'énergie, c'est-à-dire le fait que la transformée de Fourier d'une fonction soit constante en module, caractérise chacune de ces notions baptisées par l'expression générique *G-non linéarité parfaite*. Cet aspect dual de la même problématique nous fournit un analogue à la notion traditionnelle de fonction courbe.

Nous avons finalement clos le chapitre 7 en décrivant les fonctions G-parfaitement non linéaires à valeurs dans $\mathbb{F}_2$ à l'aide d'objets essentiellement combinatoires appelés *G-ensembles à différences*, généralisant le concept classique et bien connu d'ensemble à différences. Si dans le cas d'une action régulière nous retrouvons quasiment la notion d'ensemble de Hadamard, la considération

d'une action fidèle en revanche aboutit à de nouvelles constructions restées inconnues jusqu'à présent.

Parvenu à ce point, il pourrait être tentant d'avancer que tout doit se dérouler à peu près de la même manière lorsque le groupe agissant n'est plus commutatif. Mais la Science ne se montre guère indulgente avec le manque de symétrie. Le monde des quanta en est un exemple évident. Cet univers intrinsèquement non commutatif est très difficilement compréhensible par la pensée humaine. De fait il ne faut pas brûler les étapes et étudier minutieusement l'évolution de la G-non linéarité parfaite lorsque G est non abélien. Voici donc l'objectif que l'on s'est fixé pour ce chapitre et que l'on illustre symboliquement par le schéma suivant. Un nouvel axe de généralisation se juxtapose à ceux précédemment décrits.



Plus concrètement, dans un premier temps nous exposons la théorie des représentations linéaires, ainsi que l'analyse harmonique qui en découle, déterminant l'analogue non abélien de la notion classique de caractère. La suite de ce chapitre, complètement dévolue à l'étude de la version non commutative de la non linéarité parfaite, est essentiellement subdivisée en trois parties. La démarche suivie correspond à celle selon laquelle est logiquement élaboré l'ensemble des chapitres 6 et 7. Ainsi le concept de non linéarité parfaite au sens de Carlet et Ding est adapté au cas qui nous importe ici, à savoir celui des groupes finis non commutatifs. Ceci étant nécessaire du fait de l'absence de travaux originaux sur le sujet. Nous caractérisons notamment cette notion à l'aide de la transformée de Fourier basée sur les représentations linéaires. Le concept dual de fonction « courbe » se trouve donc aussi examiné dans ce chapitre. Les fondements étant fixés, suivant un schéma identique au chapitre 7, l'action par translation est remplacée par une action fidèle ou régulière d'un groupe fini qui, cette fois, se trouve être non abélien. En fin connaisseur de notre méthodologie, le lecteur se doute certainement qu'arrivé à ce stade, deux étapes doivent encore être franchies afin de compléter l'étude envisagée dans ce chapitre. Ainsi nous élaborons une formule de conservation de l'énergie caractérisant la notion correspondante de G-non linéarité parfaite. Finalement nos travaux s'achèvent par la présentation de constructions explicites de fonctions G-parfaitement non linéaires via l'utilisation du concept combinatoire de G-ensemble à différences adapté à la contrainte de non commutativité de ce chapitre.

8.2 Représentation linéaire des groupes finis

8.2.1 Introduction

Au chapitre précédent nous avons très largement traité le cas des groupes finis abéliens. A présent, nous souhaitons observer la situation des groupes finis non commutatifs. Cependant le défaut de commutativité est plus sérieux qu'il n'y paraît. En effet, dans ce contexte nous perdons la dualité classique ainsi que la notion de caractère. Nous ne pouvons donc plus nous appuyer sur ces outils afin d'expertiser le concept de non linéarité parfaite pour des groupes non abéliens. Néanmoins la notion de représentation linéaire permet de combler cette lacune et d'établir un nouveau type de dualité.

Cette section traite donc de la théorie des représentations des groupes finis qui permet d'étendre les notions de caractère et de transformée de Fourier aux groupes non abéliens. Cette théorie parvient à faire la liaison entre l'algèbre générale, puisque le problème initial est celui de l'étude d'un groupe abstrait, l'algèbre linéaire par réalisation de ce groupe comme un groupe de transformations linéaires, et la géométrie via l'étude des invariants pour une action de groupe donnée.

Nous consacrons cette section à la définition même de la notion de représentation, notamment la problématique de la recherche, à isomorphisme près, des représentations irréductibles.

Nous exposons ici les principales notions de manière relativement succincte et très synthétique. Pour la plupart des résultats énoncés, nous fournissons la preuve (tirée de [Pey04]). Néanmoins certaines d'entre elles, jugées soit trop complexes soit peu pertinentes, ont été volontairement omises. Le lecteur peut alors consulter la référence principale en français, le livre de J.-P. Serre [Ser66] ainsi que, bien entendu, [Pey04].

8.2.2 Premières définitions

Attention ! *Tous les espaces vectoriels rencontrés dans ce chapitre sont implicitement et sans exception de dimension finie.*

Définition 8.1. Soient $\mathbb{K}$ un corps et V un $\mathbb{K}$-espace vectoriel (de dimension finie). Une *représentation linéaire* d'un groupe fini G dans V est la donnée d'un homomorphisme de groupes $\rho : G \to GL(V)$.

Une représentation linéaire d'un groupe (fini) G dans V correspond à la donnée d'une action (à gauche) linéaire de groupe de G sur V en posant $\forall(\mathbf{g}, x) \in G \times V$, $\mathbf{g}.x \stackrel{déf.}{=} \rho(\mathbf{g})(x)$.

Définition 8.2. Une représentation ρ d'un groupe fini G sur un espace vectoriel V est dite *fidèle* si elle est injective.

Exemple 8.1. La *représentation régulière à gauche.*
Soit $(G, \top)$ un groupe fini. Pour $\mathbf{g} \in G$, on définit l'*indicatrice* de $\mathbf{g}$ (au sens de $\mathbb{K}$) $\mathbf{1}_{\{\mathbf{g}\}} : G \to \mathbb{K}$ *i.e.* l'application définie par

$$\mathbf{h} \mapsto \begin{cases} 0_{\mathbb{K}} & \text{si } \mathbf{h} \neq \mathbf{g} \ , \\ 1_{\mathbb{K}} & \text{si } \mathbf{h} = \mathbf{g} \ . \end{cases}$$

Comme dans le cas complexe on peut définir le produit de convolution sur le $\mathbb{K}$-espace vectoriel $\mathbb{K}^G$. Soit $(\varphi, \psi) \in (\mathbb{K}^G)^2$ alors on a

$$\begin{array}{rccl} (\varphi * \psi) : & G & \to & \mathbb{K} \\ & \alpha & \mapsto & \displaystyle\sum_{\substack{(x,y)\in G^2 \\ x\top y=\alpha}} \varphi(x)\psi(y) = \sum_{x\in G} \varphi(x)\psi(x^{-1}\top\alpha) \ . \end{array}$$

La représentation régulière à gauche est la représentation du groupe G dans le $\mathbb{K}$-espace vectoriel $\mathbb{K}^G$ définie par :

$$\begin{array}{rccl} \rho: & G & \to & GL(\mathbb{K}^G) \\ & \mathbf{g} & \mapsto & (\rho(\mathbf{g}) : f \mapsto \mathbf{1}_{\{\mathbf{g}\}} * f) \ . \end{array}$$

Proposition 8.1. [Pey04] *La représentation régulière à gauche est fidèle.*

Preuve. Si $\rho(\mathbf{g}) = Id_{\mathbb{K}^G}$ alors $\rho(\mathbf{g})(\mathbf{1}_{\{e_G\}}) = \mathbf{1}_{\{e_G\}}$ *i.e.* $\mathbf{1}_{\{\mathbf{g}\}} * \mathbf{1}_{\{e_G\}} = \mathbf{1}_{\{\mathbf{g}\}} = \mathbf{1}_{\{e_G\}}$ ce qui implique que $\mathbf{g} = e_G$. □

Exemple 8.2. Pour deux représentations ρ_V et ρ_W d'un même groupe $(G, \top)$ respectivement sur V et W, on définit la représentation de *morphismes* $\rho_{\mathcal{L}(V,W)}$ de G sur l'espace vectoriel $\mathcal{L}(V, W)$ des applications linéaires de V dans W par

$$\forall \mathbf{g} \in G,\ \forall \lambda \in \mathcal{L}(V,W),\ \rho_{\mathcal{L}(V,W)}(\mathbf{g})(\lambda) \stackrel{déf.}{=} \rho_W(\mathbf{g}) \circ \lambda \circ \rho_V(\mathbf{g}^{-1}) \ .$$

Vérifions que l'on définit bien de cette manière une représentation linéaire. Notons simplement « ρ » l'application $\rho_{\mathcal{L}(V,W)}$. Tout d'abord on constate que $\rho(\mathbf{g})$ est bien une application linéaire (pour tout $\mathbf{g} \in G$). Le fait que ρ soit une représentation résulte simplement du calcul pour $\lambda \in \mathcal{L}(V, W)$ et pour $\forall (\mathbf{g}, \mathbf{h}) \in G^2$ suivant :

$$\begin{array}{rcl} \rho(\mathbf{g}\top\mathbf{h})(\lambda) & = & \rho_W(\mathbf{g}\top\mathbf{h}) \circ \lambda \circ \rho_V((\mathbf{g}\top\mathbf{h})^{-1}) \\ & = & \rho_W(\mathbf{g}) \circ \rho_W(\mathbf{h}) \circ \lambda \circ \rho_V(\mathbf{h}^{-1}) \circ \rho_V(\mathbf{g}^{-1}) \\ & = & \rho(\mathbf{g}) \circ \rho(\mathbf{h})(f) \ . \end{array}$$

Afin de clore cette sous-section, voici une définition fondamentale pour la suite.

Définition 8.3. Pour deux représentations ρ_V et ρ_W d'un même groupe fini G respectivement dans les $\mathbb{K}$-espaces vectoriels V et W, on définit la représentation *somme* $\rho_{V\oplus W}$ de G dans la somme directe $V \oplus W$ par : $\forall \mathbf{g} \in G$, $\forall (x, y) \in V \times W$,

$$\rho_{V\oplus W}(\mathbf{g})(x, y) \stackrel{déf.}{=} \rho_V(\mathbf{g})(x) + \rho_W(\mathbf{g})(y) \ .$$

8.2.3 Représentations de degré 1

On se place dans le cas où $\mathbb{K} = \mathbb{C}$. Soit G un groupe fini. Une représentation de degré 1 est simplement un homomorphisme de groupes de G dans le groupe multiplicatif $\mathbb{C}^*$. En effet, on identifie $GL(\mathbb{C})$ et $\mathbb{C}^*$ par l'isomorphisme d'espaces vectoriels

$$\begin{array}{rccc} \Phi: & GL(\mathbb{C}) & \to & \mathbb{C}^* \\ & \mathbf{z}Id_{\mathbb{C}} & \mapsto & \mathbf{z} \end{array}$$

qui permet de confondre l'homothétie de rapport $\mathbf{z}$ avec $\mathbf{z}$ lui-même. Remarquons que $\Phi = tr$ où « tr » désigne la trace des applications linéaires.

Une représentation linéaire de degré 1, modulo cette identification, est donc un caractère de G comme déjà défini (voir la section 6.2 p. 100). On retrouve ainsi la théorie classique de la dualité des groupes finis.

- Dans le cas où G est commutatif, la nouvelle notion de représentation linéaire de groupe n'apporte rien d'original : on retombe uniquement sur les caractères définis auparavant. Intuitivement on sait que la dimension 1 suffit pour étudier les groupes abéliens ;
- Dans le cas non commutatif, l'ajout de « nouveaux » caractères permet de développer une théorie de Fourier généralisant celle définie dans le cas commutatif.

8.2.4 Représentations irréductibles

A partir de maintenant et jusqu'à la fin du présent chapitre on travaille avec $\mathbb{K} = \mathbb{C}$. En particulier, tous les espaces vectoriels rencontrés sont implicitement des $\mathbb{C}$-espaces vectoriels (de dimension finie).

Les représentations irréductibles sont les « briques de base », celles avec lesquelles on peut reconstruire tout l'édifice (ici toutes les représentations) à l'aide de leur somme (voir définition 8.3).

Définition 8.4. Deux représentations ρ et ρ' d'un même groupe fini G respectivement sur deux $\mathbb{C}$-espaces vectoriels V et V' sont dites *isomorphes* s'il existe un isomorphisme d'espaces vectoriels $\Phi : V \to V'$ tel que pour tout $\mathbf{g} \in G$,

$$\Phi \circ \rho(\mathbf{g}) = \rho'(\mathbf{g}) \circ \Phi \ .$$

Cela permet d'identifier les deux représentations et Φ est appelé *isomorphisme de représentations.*

Remarquons au passage que deux représentations linéaires isomorphes sont aussi isomorphes en tant qu'actions de groupe (voir définition 7.3).

La notion d'isomorphisme définit une relation d'équivalence sur les représentations linéaires d'un groupe fini G donné. Dans la suite on s'intéresse aux classes d'équivalence pour cette relation.

On expose maintenant les définitions qui permettent d'expliciter les notions primitives de « briques de base ».

Définition 8.5. Si une représentation ρ d'un groupe fini G sur V admet un sous-espace vectoriel $W \subset V$ stable pour tous les $\rho(\mathbf{g}) \in GL(V)$ (*i.e.* $\forall \mathbf{g} \in G, \forall x \in W,\ \rho(\mathbf{g})(x) \in W$), elle induit une représentation linéaire ρ_W de G sur W appelée *sous-représentation* de ρ.

Définition 8.6. Une représentation d'un groupe fini G sur un espace vectoriel V est dite *irréductible* si elle admet exactement deux sous-espaces stables $\{0_V\}$ et V tout entier (appelés sous-espaces *triviaux*).

Les représentations irréductibles sont minimales au sens de l'inclusion des sous-espaces non nuls.

Remarque 8.1. Les représentations linéaires de degré 1 constituent des représentations irréductibles particulières.

Définition 8.7. Une représentation ρ_V sur un espace vectoriel V est dite *indécomposable* si à chaque fois que l'on a un isomorphisme de représentations identifiant ρ_V avec une représentation somme $\rho_{W_1 \oplus W_2}$ alors $W_1 = \{0_{V'}\}$ ou $W_2 = \{0_{V'}\}$ (avec $V' \overset{déf.}{=} W_1 \oplus W_2$).

Proposition 8.2. [Pey04] *Soit ρ une représentation d'un groupe fini G sur un $\mathbb{C}$-espace vectoriel V. Alors ρ laisse invariant le produit hermitien suivant :*

$$\forall (x, y) \in V^2,\ \langle x, y \rangle_G \overset{déf.}{=} \sum_{\mathbf{g} \in G} \langle \rho(\mathbf{g})(x), \rho(\mathbf{g})(y) \rangle$$

où l'on a noté « $\langle ., . \rangle$ » un produit hermitien quelconque sur V.

Preuve. Notons par « $\top$ » la loi de G. Le fait que $\langle ., . \rangle_G$ soit invariant par ρ est trivial :

$$\begin{aligned} \langle \rho(\mathbf{g})(x), \rho(\mathbf{g})(y) \rangle_G &= \sum_{\mathbf{h} \in G} \langle \rho(\mathbf{h})(\rho(\mathbf{g})(x)), \rho(\mathbf{h})(\rho(\mathbf{g})(y)) \rangle \\ &= \sum_{\mathbf{h} \in G} \langle \rho(\mathbf{h} \top \mathbf{g})(x), \rho(\mathbf{h} \top \mathbf{g})(y) \rangle \\ &= \langle x, y \rangle_G \end{aligned}$$

pour tout $(\mathbf{g}, x, y) \in G \times V \times V$.
Le seul point important étant que $\langle ., . \rangle_G$ est bien un produit hermitien, comme somme (finie) de produits hermitiens sur le corps $\mathbb{C}$. □

Remarque 8.2. Le résultat précédent est équivalent au fait que les matrices $M_\rho(\mathbf{g})$ des $\rho(\mathbf{g})$ sont unitaires dans une base orthonormée pour $\langle ., . \rangle_G$, c'est-à-dire le produit $M_\rho(\mathbf{g})(M_\rho(\mathbf{g}))^*$ est égal à la matrice identité (avec « M^* » désignant la matrice adjointe de M). On dit que les représentations linéaires sont *unitaires*.

Théorème 8.1. [Pey04] *Une représentation ρ_V d'un groupe fini G sur V est irréductible si et seulement si elle est indécomposable.*

Preuve. Il est évident qu'une représentation irréductible est en particulier indécomposable, puisqu'une décomposition de V sous la forme d'une somme directe $W_1 \oplus W_2$ non triviale donne naissance à deux sous-représentations.
Intéressons-nous à la réciproque. Pour résoudre ce problème, il faut savoir si, étant donné une sous-représentation ρ_{W_1} non triviale de ρ_V (*i.e.* $W_1 \neq \{0_V\}$, $W_1 \neq V$ et W_1 est un sous-espace de V stable par ρ_V), on peut trouver un supplémentaire de W_1 stable sous l'action de G via ρ_V.
Soit donc ρ_{W_1} une sous-représentation non triviale de ρ_V. On considère $W_2 \stackrel{déf.}{=} W_1^\top$ l'orthogonal de W_1 au sens du produit hermitien $\langle ., . \rangle_G$ défini précédemment. Par conservation du produit scalaire, l'image par ρ_V d'un vecteur orthogonal à W_1 est encore orthogonal à W_1 : W_2 est bien stable sous l'action ρ_V de G. □

On énonce maintenant le résultat qui assure que les éléments fondamentaux que sont les représentations irréductibles permettent de reconstruire toutes les représentations.

Proposition 8.3. [Pey04] *Toute représentation peut s'écrire comme somme de représentations irréductibles.*

Preuve. On raisonne par récurrence sur la dimension de V l'espace vectoriel de la représentation ρ_V étudiée. Une représentation sur un espace vectoriel de dimension 1 est trivialement irréductible. Si V est un espace vectoriel de dimension plus grande que 1 tel que ρ_V soit irréductible, la démonstration est finie. Sinon V admet un sous-espace non trivial W, et d'après le théorème précédent, on peut trouver W_0 sous-espace de V stable tel que $V = W \oplus W_0$. En appliquant l'hypothèse de récurrence à W et W_0, on prouve ce qui était demandé. □

Remarque 8.3. Cette écriture n'est pas unique, cependant on va voir plus loin qu'elle l'est « à un isomorphisme près » au sens où si l'on a deux décompositions de V sous la forme $W_1 \oplus \ldots \oplus W_k$ et $W'_1 \oplus \ldots \oplus W'_{k'}$ alors $k = k'$ et, quitte à réordonner les indices, il existe des isomorphismes d'espaces vectoriels qui permettent d'identifier W_i et W'_i.

8.2.5 Caractères des représentations

8.2.5.1 Définitions et propriétés

Définition 8.8. Soit ρ une représentation linéaire d'un groupe fini G sur un $\mathbb{C}$-espace vectoriel V de dimension finie. On lui associe son *caractère* χ_ρ défini par

$$\forall \mathbf{g} \in G,\ \chi_\rho(\mathbf{g}) \stackrel{déf.}{=} tr(\rho(\mathbf{g}))\ .$$

Un caractère est donc une application de G dans $\mathbb{C}$.

Les caractères des représentations linéaires ne sont pas, en général, des homomorphismes de groupes de G dans $\mathbb{C}^*$. Ce ne sont donc pas des caractères au sens de la dualité des groupes finis commutatifs. Néanmoins, comme cela a déjà été souligné, si la représentation est de degré 1 alors

χ_ρ correspond bien à un caractère classique.

Les propriétés les plus importantes des caractères des représentations sont données dans la proposition qui suit.

Proposition 8.4. [Pey04] *Soit ρ une représentation linéaire d'un groupe fini $(G, \top)$ sur l'espace vectoriel V. Soit $n \stackrel{déf.}{=} \dim_{\mathbb{C}}(V)$. On a les propriétés suivantes :*

1. $\chi_\rho(e_G) = n$;
2. $\forall \mathbf{g} \in G,\ \chi_\rho(\mathbf{g}^{-1}) = \overline{\chi_\rho(\mathbf{g})}$;
3. $\forall (\mathbf{g}, \mathbf{h}) \in G^2,\ \chi_\rho(\mathbf{g} \top \mathbf{h} \top \mathbf{g}^{-1}) = \chi_\rho(\mathbf{h})$ *(invariance sur les classes de conjugaison)* ;
4. *Si ρ se décompose en somme directe de deux représentations ρ_{W_1} et ρ_{W_2} alors χ_ρ défini par $\chi_{\rho_{W_1 \oplus W_2}}$ est égal à $\chi_{\rho_{W_1}} + \chi_{\rho_{W_2}}$.*

Preuve.

1. Evident car $tr(Id_V) = \dim_{\mathbb{C}}(V) = n$;
2. Ceci vient du fait que l'on peut prendre une matrice unitaire pour représenter $\rho(\mathbf{g})$ et donc $\chi_\rho(\mathbf{g}^{-1}) = tr(\rho(\mathbf{g})^{-1}) = tr(\rho(\mathbf{g})^*) = \overline{tr(\rho(\mathbf{g}))}$;
3. Ceci vient du fait que pour tout couple (M_1, M_2) de matrices carrées de taille n, inversibles et à coefficients dans $\mathbb{C}$,
$$tr(M_2 M_1 M_2^{-1}) = tr(M_1) \ ;$$
4. Si on note « B_{W_1} » une base de W_1 et « B_{W_2} » une base de W_2, la matrice $M(\mathbf{g})$ de $\rho_{W_1 \oplus W_2}(\mathbf{g})$ s'écrit dans la base B de $W_1 \oplus W_2$ définie par $B \stackrel{déf.}{=} B_{W_1} \cup B_{W_2}$:
$$M(\mathbf{g}) = \begin{pmatrix} M_{W_1}(\mathbf{g}) & 0_{\dim_{\mathbb{C}}(W_1),\dim_{\mathbb{C}}(W_2)} \\ 0_{\dim_{\mathbb{C}}(W_2),\dim_{\mathbb{C}}(W_1)} & M_{W_2}(\mathbf{g}) \end{pmatrix}$$
où pour $i \in \{1, 2\}$, $M_{W_i}(\mathbf{g})$ est la matrice de $\rho_{W_i}(\mathbf{g})$ dans la base B_{W_i}, $0_{\dim_{\mathbb{C}}(W_1),\dim_{\mathbb{C}}(W_2)}$ et $0_{\dim_{\mathbb{C}}(W_2),\dim_{\mathbb{C}}(W_1)}$ sont des matrices de formats respectifs $\dim_{\mathbb{C}}(W_1) \times \dim_{\mathbb{C}}(W_2)$ et $\dim_{\mathbb{C}}(W_2) \times \dim_{\mathbb{C}}(W_1)$ remplies avec des zéros. D'où
$$\begin{aligned} \chi_{\rho_{W_1 \oplus W_2}}(\mathbf{g}) &= tr(M(\mathbf{g})) \\ &= tr(M_{W_1}(\mathbf{g})) + tr(M_{W_2}(\mathbf{g})) \\ &= \chi_{\rho_{W_1}}(\mathbf{g}) + \chi_{\rho_{W_2}}(\mathbf{g}) \ . \end{aligned}$$

□

8.2.5.2 Relations d'orthogonalité

Dans ce paragraphe, on se donne G un groupe fini quelconque (abélien ou non).

Définition 8.9. Soit $(\varphi, \psi) \in (\mathbb{C}^G)^2$, on définit le produit scalaire (normalisé) hermitien suivant :
$$\langle \varphi, \psi \rangle \stackrel{déf.}{=} \frac{1}{|G|} \sum_{\mathbf{g} \in G} \varphi(\mathbf{g}) \overline{\psi(\mathbf{g})} \ .$$

Il s'agit d'une généralisation du produit scalaire hermitien introduit au chapitre 6 dans le cadre des groupes finis abéliens.
Le théorème suivant, donné sans sa démonstration, étend les résultats déjà connus au sujet des caractères des groupes finis commutatifs.

Théorème 8.2. [Pey04] *Une famille de caractères de représentations irréductibles deux à deux non isomorphes forme une famille orthonormale du $\mathbb{C}$-espace vectoriel $\mathbb{C}^G$, ce qui signifie que :*
- *Si χ est un caractère d'une représentation irréductible, on a $\langle \chi, \chi \rangle = 1$;*
- *Si χ et χ' sont deux caractères de représentations irréductibles non isomorphes, on a*

$$\langle \chi, \chi' \rangle = 0 \ .$$

Corollaire 8.1. [Pey04] *Il y a un nombre fini de classes de représentations irréductibles (sous-entendu de classes pour la relation « être isomorphe »).*

Preuve. Les caractères des représentations irréductibles non isomorphes forment une famille libre, car orthogonale, de l'espace vectoriel $\mathbb{C}^G$ qui est un espace de dimension finie sur $\mathbb{C}$ (précisément $\dim_{\mathbb{C}}(\mathbb{C}^G) = |G| < \infty$). En conséquence, il y a un nombre fini de caractères, donc un nombre fini de représentations irréductibles. Leur nombre est borné par $\dim_{\mathbb{C}}(\mathbb{C}^G) = |G|$. □

8.2.6 Décomposition et dénombrement

On s'intéresse désormais d'une part à la décomposition des représentations en somme de représentations élémentaires et d'autre part, au nombre de classes d'équivalence pour la relation d'isomorphisme.

Dans la suite on se donne une famille (finie) de représentations irréductibles ρ_i sur un groupe fini G, chaque représentation ρ_i étant implicitement liée à un $\mathbb{C}$-espace vectoriel V_i tel que $\rho_i : G \to GL(V_i)$. Ceci signifie que les ρ_i sont deux à deux non isomorphes et que toute représentation irréductible ρ de G est isomorphe à un unique ρ_i. En définitive, l'ensemble de tels ρ_i est un système de représentants pour la relation d'isomorphisme. Enfin on note « χ_i » de préférence à « χ_{ρ_i} » le caractère de la représentation ρ_i.

Définition 8.10. On note « $\widehat{G}$ » (par abus de notation) l'ensemble des classes d'équivalence des représentations irréductibles sur un groupe fini G pour la relation d'isomorphisme. Par abus de langage, on confondra souvent $\widehat{G}$ avec un système de représentants $\{\rho_i \in GL(V_i)^G | i \in \{1, \ldots, k\}\}$ (avec $k \stackrel{déf.}{=} |\widehat{G}|$).

Le résultat suivant garantit l'unicité de la décomposition d'une écriture en somme de représentations irréductibles.

Proposition 8.5. [Pey04] *Soit une représentation ρ_V d'un groupe fini G sur V de caractère χ_{ρ_V}. Alors elle se décompose en la représentation linéaire de la somme directe*

$$\bigoplus_{i=1}^{k} V_i^{\oplus k_i} \tag{8.1}$$

avec $k \stackrel{déf.}{=} |\widehat{G}|$, $k_i \stackrel{déf.}{=} \langle \chi_{\rho_V}, \chi_i \rangle$ et $V_i^{\oplus k_i}$ est défini par $\underbrace{V_i \oplus \ldots \oplus V_i}_{k_i \text{ fois}}$.

Preuve. On sait déjà que la représentation ρ_V se décompose en somme de n représentations irréductibles $\{\rho_{W_j}\}_{j=1}^{n}$ (avec $\rho_{W_j} : G \to GL(W_j)$) et donc

$$V = W_1 \oplus \ldots \oplus W_n \ .$$

Donc d'après la proposition 8.4, on a :

$$\chi_{\rho_V} = \chi_{\rho_{W_1}} + \ldots + \chi_{\rho_{W_n}} \ . \tag{8.2}$$

Comme on a $\langle \chi_{\rho_V}, \chi_i \rangle = \sum_{j=1}^{n} \langle \chi_{\rho_{W_j}}, \chi_i \rangle$ et que $\langle \chi_{\rho_{W_j}}, \chi_i \rangle$ vaut 1 si ρ_{W_j} est isomorphe à ρ_i et 0 sinon, on en déduit que $\langle \chi_{\rho_V}, \chi_i \rangle$ représente le nombre de $\rho_{\rho_{W_j}}$ pour $j = 1, \ldots, n$ qui sont isomorphes à ρ_i. Or par définition il s'agit de k_i. Au final, dans l'écriture (8.2) on peut regrouper les W_j tel que ρ_{W_j} est isomorphe à ρ_i et donc écrire $V_i^{\oplus k_i}$ à la place. □

Corollaire 8.2. [Pey04] *Deux représentations sont isomorphes si et seulement si elles ont le même caractère. De plus, une représentation sur V de caractère χ_V est irréductible si et seulement si $\langle \chi_V, \chi_V \rangle = 1$.*

Preuve. Le caractère χ_V détermine entièrement la décomposition (8.1) en fonction des éléments de $\widehat{G}$, donc détermine entièrement la classe d'isomorphisme. De plus le caractère est irréductible si et seulement si sa décomposition ne possède qu'un seul terme, *i.e.* s'il existe $j \in \{1, \ldots, k\}$ tel que $k_j = 1$ et pour tout $i \in \{1, \ldots, k\}$ tel que $i \neq j$, $k_i = 0$. Ceci est équivalent à $\langle \chi_V, \chi_V \rangle = \sum_{i=1}^{k} k_i^2 = 1$. □

Remarque 8.4. On retrouve bien le fait que les caractères classiques *i.e.* les représentations linéaires de degré 1 sont irréductibles et isomorphes à aucune autre représentation irréductible. Ainsi le système de représentants choisi $\{\rho_i \in GL(V_i)^G | i \in \{1, \ldots, k\}\}$ contient forcément toutes les représentations de degré 1.

On se donne maintenant G un groupe fini et $\{\rho_i \in GL(V_i)^G | i \in \{1, \ldots, k\}\}$ (avec $k \stackrel{déf.}{=} |\widehat{G}|$) un système de représentants de $\widehat{G}$.

Le théorème suivant (dont la preuve est admise) permet notamment de déterminer si on a, ou non, trouvé toutes les représentations - à isomorphisme près - d'un groupe donné.

Théorème 8.3. [Pey04] *Soit $n_i \stackrel{déf.}{=} \dim_{\mathbb{C}}(V_i)$.*
On a les relations suivantes :

1. $\sum_{i=1}^{k} n_i^2 = |G|$;
2. *Pour $\mathbf{g} \in G^*$,* $\sum_{i=1}^{k} n_i \chi_i(\mathbf{g}) = 0$.

La proposition suivante, non démontrée, permet de dénombrer le nombre de classes d'équivalence de représentations irréductibles du groupe fini G.

Proposition 8.6. [Pey04] *Le nombre k de représentations irréductibles sur G non isomorphes, c'est-à-dire le cardinal de $\widehat{G}$, est égal au nombre de classes de conjugaison de G.*

Corollaire 8.3. [Pey04] *Le groupe G est commutatif si et seulement si toutes ses représentations irréductibles sont de degré 1.*

Preuve. Si on note « k » le nombre de classes de conjugaison, G est commutatif si et seulement si $k = |G|$. Or d'après le théorème 8.3, on a $\sum_{i=1}^{k} n_i^2 = |G|$ donc G est commutatif si et seulement si $\forall i \in \{1, \ldots, k\}$, $n_i = 1$. □

8.2.7 Conclusion

Si les homomorphismes de groupes dans $\mathbb{C}^*$ sont suffisants pour exprimer les propriétés des groupes finis commutatifs, ce n'est plus le cas dès lors que l'on s'intéresse aux groupes finis non

abéliens. Dans ce contexte, il faut utiliser une notion plus subtile. Ainsi la théorie des représentations linéaires prend la place, laissée vacante, de la notion de caractère.

Cette approche permet d'instancier des groupes abstraits sous la forme de transformations linéaires d'un espace vectoriel concret. Les propriétés algébriques se traduisent ainsi dans le langage de l'algèbre linéaire.

Au travers de cette notion de dualité, il est possible de déterminer une nouvelle théorie de Fourier reprenant dans les grandes lignes les caractéristiques fondamentales de sa devancière.

8.3 Théorie de Fourier pour des groupes non commutatifs

Dans cette courte section est succinctement exposée la théorie de Fourier, au sens des représentations linéaires, semblable à celle des caractères d'un groupe fini commutatif (voir le chapitre 6). On retrouve notamment certains résultats classiques dans ce nouveau contexte.

Dans la suite nous utilisons cette variante de la théorie de Fourier afin d'établir une formule de conservation de l'énergie caractérisant la non linéarité parfaite appliquée au cas des groupes finis non commutatifs.

Dans cette section on se donne $(G, \top)$ un groupe fini et $\{\rho_i \in GL(V_i)^G | i \in \{1, \ldots, k\}\}$ (avec $k \stackrel{déf.}{=} |\widehat{G}|$) un système de représentants de $\widehat{G}$ (que l'on identifie à $\widehat{G}$ lui-même).

Définition 8.11. Soit $\varphi \in \mathbb{C}^G$. On définit, pour ρ_V une représentation de G sur un $\mathbb{C}$-espace vectoriel V, l'application $\lambda_F(\varphi)$ par

$$\lambda_F(\varphi)(\rho_V) \stackrel{déf.}{=} \sum_{\mathbf{g} \in G} \varphi(\mathbf{g}) \rho_V(\mathbf{g}) \in End(V) \ .$$

Ceci permet de définir la *transformée de Fourier*[1] :

$$\Phi_F : \left\{ \begin{array}{rcl} \mathbb{C}^G & \rightarrow & \displaystyle\bigoplus_{i=1}^{k} End(V_i) \\ \varphi & \mapsto & \Phi_F(\varphi) = \widehat{\varphi}^G \stackrel{déf.}{=} (\lambda_F(\varphi)(\rho_1), \ldots, \lambda_F(\varphi)(\rho_k)) \ . \end{array} \right.$$

On abusera souvent de la notation en écrivant « $\widehat{\varphi}^G(\rho_i)$ » à la place de « $\lambda_F(\varphi)(\rho_i) = (\widehat{\varphi}^G)_i$ » (la $i^{ème}$ composante de $\widehat{\varphi}^G$).

Remarque 8.5. Afin de ne pas confondre la transformée de Fourier au sens des représentations de celle classique des groupes commutatifs, nous utilisons le symbole « $\widehat{\ }^G$ » plutôt que « $\widehat{\ }$ » seul.

Les deux propositions suivantes (non démontrées) généralisent des résultats classiques au sujet de la transformée de Fourier.

Proposition 8.7. [Pey04] *L'application transformée de Fourier est un homomorphisme d'algèbres de* $(\mathbb{C}^G, *)$ *dans* $\displaystyle\bigoplus_{i=1}^{k}(End(V_i), \circ)$. *Elle trivialise notamment le produit de convolution*

$$\forall \rho \in \widehat{G}, \ \forall (\varphi, \psi) \in (\mathbb{C}^G)^2, \ \widehat{\varphi * \psi}^G(\rho) = \widehat{\varphi}^G(\rho) \circ \widehat{\psi}^G(\rho) \ .$$

[1] Parfois appelée *transformée de Fourier quantique*.

Proposition 8.8. [Pey04] *L'application transformée de Fourier est un isomorphisme d'algèbres de* $(\mathbb{C}^G, *)$ *dans* $\bigoplus_{i=1}^{k}(End(V_i), \circ)$.

Nous disposons par ailleurs d'une formule d'inversion.

Théorème 8.4 (Formule d'inversion). [Pey04] *Pour* $\varphi \in \mathbb{C}^G$, *on a la formule :*

$$\forall \mathbf{g} \in G,\ \varphi(\mathbf{g}) = \frac{1}{|G|}\sum_{\rho_i \in \widehat{G}} n_i tr(\rho_i(\mathbf{g}^{-1}) \circ \widehat{\varphi}^G(\rho_i))$$

où $n_i \stackrel{déf.}{=} \dim_{\mathbb{C}}(V_i)$.

Preuve. En utilisant la linéarité des deux membres de l'égalité, il suffit de démontrer la proposition dans le cas où $\varphi = \mathbf{1}_{\{\mathbf{h}\}}$ (puisque $\{\mathbf{1}_{\{\mathbf{g}\}} \in \mathbb{C}^G | \mathbf{g} \in G\}$ est une base de $\mathbb{C}^G$). Le membre de droite de l'égalité se résume alors à

$$\frac{1}{|G|}\sum_{i=1}^{k} n_i tr(\rho_i(\mathbf{g}^{-1}) \circ \rho_i(\mathbf{h})) = \frac{1}{|G|}\sum_{i=1}^{k} n_i \chi_i(\mathbf{g}^{-1} \top \mathbf{h})$$

d'après les propriétés des caractères.
Or d'après le théorème 8.3 cette dernière quantité vaut 1 si $\mathbf{g}^{-1} \top \mathbf{h} = e_G$ (*i.e.* $\mathbf{g} = \mathbf{h}$) et 0 sinon. En regardant le membre de gauche de l'égalité qui vaut $\mathbf{1}_{\{\mathbf{h}\}}(\mathbf{g})$ on voit que c'est ce qu'il fallait montrer. □

Nous introduisons maintenant le lemme suivant, utile dans la description de la non linéarité parfaite dans le cadre des groupes finis non abéliens.

Lemme 8.1. *Soit* $\varphi : G \to \mathbb{C}$. *Alors on a :*

$$\forall \mathbf{g} \in G^*,\ \varphi(\mathbf{g}) = 0 \text{ si et seulement si } \forall \rho_i \in \widehat{G},\ \widehat{\varphi}^G(\rho_i) = \varphi(e_G) Id_{V_i}\ .$$

Preuve. Considérons tout d'abord l'implication dans le sens direct. On a alors pour $\rho_i \in \widehat{G}$

$$\begin{aligned}
\widehat{\varphi}^G(\rho_i) &= \lambda_F(\varphi)(\rho_i) = \sum_{\mathbf{g}\in G} \varphi(\mathbf{g})\rho_i(\mathbf{g}) \text{ (par définition)} \\
&= \varphi(e_G)\rho_i(e_G) \text{ (par hypothèse)} \\
&= \varphi(e_G) Id_{V_i} \text{ (puisque } \rho_i \text{ est un homomorphisme de } G \text{ dans } GL(V_i))\ .
\end{aligned}$$

Prouvons maintenant l'implication réciproque. Pour $\mathbf{g} \in G$, la formule d'inversion donne :

$$\begin{aligned}
\varphi(\mathbf{g}) &= \frac{1}{|G|}\sum_{\rho_i \in \widehat{G}} n_i tr(\rho_i(\mathbf{g}^{-1}) \circ \widehat{\varphi}^G(\rho_i)) \\
&= \frac{1}{|G|}\sum_{\rho_i \in \widehat{G}} n_i tr(\rho_i(\mathbf{g}^{-1}) \circ \varphi(e_G) Id_{V_i}) \text{ (par hypothèse)} \\
&= \frac{\varphi(e_G)}{|G|}\sum_{\rho_i \in \widehat{G}} n_i tr(\rho_i(\mathbf{g}^{-1})) \\
&= \frac{\varphi(e_G)}{|G|}\sum_{\rho_i \in \widehat{G}} n_i tr(\rho_i(\mathbf{g})^{-1}) \text{ (puisque } \rho_i \text{ est un homomorphisme)} \\
&= \frac{\varphi(e_G)}{|G|}\sum_{\rho_i \in \widehat{G}} n_i tr(\rho_i(\mathbf{g})^{*}) \text{ (puisque } \rho_i(\mathbf{g}) \text{ est unitaire)} \\
&= \frac{\varphi(e_G)}{|G|}\sum_{\rho_i \in \widehat{G}} n_i \overline{tr(\rho_i(\mathbf{g}))} \\
&= \frac{\varphi(e_G)}{|G|}\overline{\sum_{\rho_i \in \widehat{G}} n_i tr(\rho_i(\mathbf{g}))} \\
&= \frac{\varphi(e_G)}{|G|}\overline{\sum_{i=1}^{k} n_i \chi_i(\mathbf{g})} \\
&= 0 \text{ si } \mathbf{g} \neq e_G \text{ d'après le théorème 8.3.}
\end{aligned}$$

□

8.4 Non linéarité parfaite : cas non commutatif

8.4.1 Introduction

Dans le cas des groupes finis commutatifs, nous avons pu observé, au cours de ce manuscrit, que la notion de non linéarité parfaite repose d'une part sur les concepts de fonction équilibrée et de dérivée et d'autre part, qu'elle se caractérise judicieusement à l'aide de la transformée de Fourier. On souhaite maintenant savoir ce qu'il en est lorsque l'ensemble de départ des fonctions examinées est un groupe fini non abélien. Comme, à notre connaissance, peu d'études portent sur le sujet, il est nécessaire de définir la situation de base dans ce contexte.

De fait la notion de dérivée, et donc celle de non linéarité parfaite, doit sensiblement évoluer. Néanmoins ceci est anecdotique en regard de la formulation de la problématique en termes de transformée de Fourier. En effet d'après les deux premières sections de ce chapitre, il est clair que la dualité classique n'est plus assez efficace pour prendre en compte les subtilités introduites par la non commutativité. Nous devons désormais faire usage de l'outil sophistiqué de la théorie de Fourier au sens des représentations.

Le scénario de cette section est tout à fait traditionnel. Dans un premier temps nous introduisons la définition de la non linéarité parfaite d'un point de vue combinatoire puis nous la décrivons sous l'angle de la théorie de Fourier en fournissant l'analogue multi-dimensionnel d'une formule de conservation de l'énergie *i.e.* la notion convenable de fonction courbe dans ce nouveau contexte.

8.4.2 Définitions et premier résultat

Pour l'intégralité de cette section, on se donne $(G, \top)$ et $(H, +)$ deux groupes finis tels que G soit non commutatif alors que H est abélien. Observons que seul le groupe G est concerné par la perte de commutativité.

Puisque G est désormais non abélien, les translations à gauche et à droite ne sont pas identiques. Cela nécessite donc une légère mise au point des notions de dérivée et de non linéarité parfaite.

Définition 8.12. Soit $f : G \to H$.
La *dérivée à gauche* de f dans la direction $\alpha \in G$ est

$$\begin{array}{rccl} d^g_\alpha : & G & \to & H \\ & x & \mapsto & f(\alpha \top x) - f(x) \ . \end{array}$$

La *dérivée à droite* de f dans la direction $\alpha \in G$ est

$$\begin{array}{rccl} d^d_\alpha : & G & \to & H \\ & x & \mapsto & f(x \top \alpha) - f(x) \ . \end{array}$$

Définition 8.13. Soit $f : G \to H$. La fonction f est *parfaitement non linéaire à gauche* (respectivement *à droite*) si pour tout $\alpha \in G^*$, la dérivée de f à gauche (respectivement à droite) dans la direction α est équilibrée. En d'autres termes,

$$\forall \alpha \in G^*,\ \forall \beta \in H,\ |\{x \in G | d^g_\alpha f(x) = \beta\}| = \frac{|G|}{|H|}$$

(respectivement, $\forall \alpha \in G^*,\ \forall \beta \in H,\ |\{x \in G | d^d_\alpha f(x) = \beta\}| = \frac{|G|}{|H|}$).

Bien que distinctes les deux notions sont en réalité fortement dépendantes l'une de l'autre.

Proposition 8.9. *Soit $f : G \to H$. La fonction f est parfaitement non linéaire à gauche si et seulement s'il existe une permutation $\pi \in S(G)$ telle que $f \circ \pi^{-1}$ soit parfaitement non linéaire à droite.*

Preuve. L'action de G sur lui-même par translation à gauche est régulière. Il en est de même de l'action de G sur lui-même par translation à droite. D'après le corollaire 7.2 les deux actions sont isomorphes. Il existe donc un automorphisme de groupe $\Phi : G \to G$ et une permutation $\pi \in S(G)$ tels que pour tout $(\alpha, x) \in G^2$, $\pi(\alpha \top x) = \pi(x) \top \Phi(\alpha)$. Nous avons donc pour tout $\alpha \in G^*$ et tout $\beta \in H$,

$$\begin{array}{rcl} |\{x \in G | f(\alpha \top x) - f(x) = \beta\}| & = & |\{x \in G | f(\pi^{-1}(\pi(\alpha \top x))) - f(x) = \beta\}| \\ & = & |\{x \in G | f \circ \pi^{-1}(\pi(x) \top \Phi(\alpha)) - f \circ \pi^{-1}(\pi(x)) = \beta\}| \\ & = & |\{y \in G | f \circ \pi^{-1}(y \top \Phi(\alpha)) - f \circ \pi^{-1}(y) = \beta\}| \\ & & \text{(par le changement de variables } y \stackrel{déf.}{=} \pi(x)) \\ & = & |\{y \in G | f \circ \pi^{-1}(y \top \alpha') - f \circ \pi^{-1}(y) = \beta\}| \\ & & \text{(où } \alpha' \stackrel{déf.}{=} \Phi(\alpha)) \ . \end{array}$$

Or lorsque α parcourt G^*, il en est de même pour α', ce qui suffit à assurer le résultat voulu. □

La distinction entre les notions de non linéarité parfaite à gauche et à droite, bien qu'indiscutable, n'a pas d'intérêt fondé au niveau conceptuel. Il en résulte que dans la suite nous ne considérons que le cas des translations à gauche afin de simplifier les énoncés et les preuves. Les versions correspondantes à droite seront simplement exposées sans aucune démonstration.

8.4.3 Caractérisation à l'aide de la transformée de Fourier

Puisque nous nous sommes fixés comme objectif la généralisation et l'explicitation de la notion de non linéarité parfaite dans un environnement non abélien, il est justifié d'aspirer à la découverte d'un éventuel concept analogue à celui de fonction courbe. Nous accomplissons cela dans cette sous-section à l'aide des théories des représentations linéaires et de Fourier introduites précédemment.

Au même titre que dans le cas classique, nous débutons par la formulation de la notion de fonction équilibrée via la transformée de Fourier.

Lemme 8.2. *Soit $f : G \to H$. Soit $\rho_1 \in \widehat{G}$ la représentation (irréductible) de degré 1* triviale *i.e.*

$$\begin{array}{rccc} \rho_1 : & G & \to & GL(\mathbb{C}) \\ & x & \mapsto & \rho_1(x) \stackrel{déf.}{=} Id_{\mathbb{C}} \ . \end{array}$$

La fonction f est équilibrée si et seulement si $\forall \beta \in H^*$,

$$\widehat{\chi_H^\beta \circ f}^G(\rho_1) = 0_{End(\mathbb{C})} \ .$$

Preuve. On rappelle en premier lieu la définition de l'application φ_f (voir chapitre 6)

$$\begin{array}{rccc} \varphi_f : & H & \to & \mathbb{N} \subset \mathbb{C} \\ & \beta & \mapsto & |f^{-1}(\{\beta\})| \ . \end{array}$$

Calculons la transformée de Fourier de la fonction $\chi_H^\beta \circ f : G \to \mathbb{C}$ pour $\rho_1 \in \widehat{G}$:

$$\begin{array}{rcl} \widehat{\chi_H^\beta \circ f}^G(\rho_1) & = & \lambda_F(\chi_H^\beta \circ f)(\rho_1) \\ & = & \sum_{x \in G} \chi_H^\beta(f(x))\rho_1(x) \\ & = & \sum_{x \in G} \chi_H^\beta(f(x)) Id_{\mathbb{C}} \\ & = & \sum_{\gamma \in H} \varphi_f(\gamma)\chi_H^\beta(\gamma) Id_{\mathbb{C}} \ . \end{array} \tag{8.3}$$

Démontrons l'implication dans le sens direct. Soit $\beta \in H^*$ et supposons donc que f soit équilibrée. Alors $\forall \gamma \in H$, $\varphi_f(\gamma) = \frac{|G|}{|H|}$ (par définition des fonctions équilibrées). Donc d'après (8.3) on a $\widehat{\chi_H^\beta \circ f}^G(\rho_1) = \frac{|G|}{|H|} \sum_{\gamma \in H} \chi_H^\beta(\gamma) Id_{\mathbb{C}}$. Or pour tout $\beta \in H^*$, $\sum_{\gamma \in H} \chi_H^\beta(\gamma) = 0$ (voir lemme 6.2). On a donc $\widehat{\chi_H^\beta \circ f}^G(\rho_1) = 0 Id_{\mathbb{C}} = 0_{End(\mathbb{C})}$.

Démontrons l'implication réciproque. Pour ce faire calculons la transformée de Fourier de l'application φ_f. Pour $\beta \in H$, on a $\widehat{\varphi_f}(\beta) = \sum_{\gamma \in H} \varphi_f(\gamma)\chi_H^\beta(\gamma)$. Il résulte de (8.3) et par hypothèses que l'on a

$$\widehat{\varphi_f}(\beta) Id_{\mathbb{C}} = \widehat{\chi_H^\beta \circ f}^G(\rho_1) = 0_{End(\mathbb{C})}$$

pour tout $\beta \in H^*$. Il s'ensuit alors nécessairement que $\widehat{\varphi_f}(\beta) = 0$ pour tout $\beta \in H^*$. D'après les propriétés de la transformée de Fourier classique (lemme 6.3), on en déduit que $\forall \beta \in H$, $\varphi_f(\beta) = \frac{1}{|H|}\widehat{\varphi_f}(e_G)$. Or $\widehat{\varphi_f}(e_H) = \sum_{\gamma \in H} \varphi_f(\gamma)\chi_H^{e_H}(\gamma) = \sum_{\gamma \in H} \varphi_f(\gamma) = |G|$, d'où $\forall \beta \in H$, $\varphi_f(\beta) = \frac{|G|}{|H|}$ *i.e.* la fonction f est équilibrée. □

A ce stade, dans le cas classique ou celui d'une action fidèle de groupe commutatif, nous avions exposé un résultat intermédiaire, contenant le calcul de la transformée de Fourier d'une fonction d'auto-corrélation, directement utilisé dans la preuve du théorème principal fournissant la formule de conservation de l'énergie. Le lecteur ne sera donc pas surpris si une nouvelle fois nous suivons une démarche identique.

Proposition 8.10. *Soit $f : G \to H$. Soient $\beta \in H^*$ et $\mathtt{z} \in \mathbb{C}$. On définit l'application suivante :*

$$\begin{array}{rccl} AC^g_{f,\beta,\mathtt{z}}: & G & \to & \mathbb{C} \\ & \alpha & \mapsto & (\widehat{\chi^\beta_H \circ d^g_\alpha f}^{\,G}(\rho_1))(\mathtt{z}) \ . \end{array}$$

Alors pour tout $\rho_i \in \widehat{G}$, $\widehat{AC^g_{f,\beta,\mathtt{z}}}^{\,G}(\rho_i) = \mathtt{z}(\widehat{\chi^\beta_H \circ f}^{\,G}(\rho_i)) \circ (\widehat{\chi^\beta_H \circ f}^{\,G}(\rho_i))^*$.

Preuve.

$$\begin{aligned}
\widehat{AC^g_{f,\beta,\mathtt{z}}}^{\,G}(\rho_i) &= \sum_{\alpha\in G} AC^g_{f,\beta,\mathtt{z}}(\alpha)\rho_i(\alpha) \\
&= \sum_{\alpha\in G} (\widehat{\chi^\beta_H \circ d^g_\alpha f}^{\,G}(\rho_1))(\mathtt{z})\rho_i(\alpha) \\
&= \sum_{\alpha\in G}\sum_{x\in G} \chi^\beta_H \circ d^g_\alpha f(x)\rho_1(x)(\mathtt{z})\rho_i(\alpha) \\
&= \mathtt{z}\sum_{\alpha\in G}\sum_{x\in G} \chi^\beta_H(f(\alpha\top x) - f(x))\rho_i(\alpha) \text{ (par définition de } \rho_1) \\
&= \mathtt{z}\sum_{\alpha\in G}\sum_{x\in G} \chi^\beta_H(f(\alpha\top x))\overline{\chi^\beta_H(f(x))}\rho_i(\alpha) \\
&= \mathtt{z}\sum_{\alpha\in G}\sum_{x\in G} \chi^\beta_H(f(\alpha\top x))\overline{\chi^\beta_H(f(x))}\rho_i(\alpha\top x\top x^{-1}) \\
&= \mathtt{z}\sum_{\alpha\in G}\sum_{x\in G} \chi^\beta_H(f(\alpha\top x))\overline{\chi^\beta_H(f(x))}\rho_i(\alpha\top x)\circ\rho_i(x^{-1}) \ (\rho_i \text{ est un morphisme}) \\
&= \mathtt{z}\sum_{\alpha\in G}\sum_{x\in G} \chi^\beta_H(f(\alpha\top x))\overline{\chi^\beta_H(f(x))}\rho_i(\alpha\top x)\circ\rho_i(x)^{-1} \ (\rho_i \text{ est un morphisme}) \\
&= \mathtt{z}\sum_{\alpha\in G}\sum_{x\in G} \chi^\beta_H(f(\alpha\top x))\overline{\chi^\beta_H(f(x))}\rho_i(\alpha\top x)\circ\rho_i(x)^* \ (\rho_i \text{ est unitaire}) \\
&= \mathtt{z}\sum_{x\in G}(\sum_{\alpha\in G} \chi^\beta_H(f(\alpha\top x))\rho_i(\alpha\top x))\circ(\overline{\chi^\beta_H(f(x))}\rho_i(x)^*) \text{ (par linéarité)} \\
&= \mathtt{z}\sum_{x\in G}(\widehat{\chi^\beta_H \circ f}^{\,G}(\rho_i))\circ(\overline{\chi^\beta_H(f(x))}\rho_i(x)^*) \\
&= \mathtt{z}(\widehat{\chi^\beta_H \circ f}^{\,G}(\rho_i))\circ\left(\sum_{x\in G}\overline{\chi^\beta_H(f(x))}\rho_i(x)^*\right) \\
&= \mathtt{z}(\widehat{\chi^\beta_H \circ f}^{\,G}(\rho_i))\circ(\widehat{\chi^\beta_H \circ f}^{\,G}(\rho_i))^* \ .
\end{aligned}$$

□

Rigoureusement $\alpha \mapsto (\widehat{\chi^\beta_H \circ d^g_\alpha f}^{\,G}(\rho_1))$ est une application de G dans $End(\mathbb{C})$. On ne peut donc calculer sa transformée de Fourier au sens des représentations linéaires sans utiliser le paramètre complexe $\mathtt{z}$. Il s'agit donc simplement d'un procédé technique très pratique.

Remarque 8.6. De manière équivalente nous pouvons définir pour $\beta \in H^*$ et $\mathtt{z} \in \mathbb{C}$

$$\begin{array}{rccl} AC^d_{f,\beta,\mathtt{z}}: & G & \to & \mathbb{C} \\ & \alpha & \mapsto & (\widehat{\chi^\beta_H \circ d^d_\alpha f}^{\,G}(\rho_1))(\mathtt{z}) \ . \end{array}$$

Dans ce cas, nous avons pour tout $\rho_i \in \widehat{G}$,

$$\widehat{AC^d_{f,\beta,\mathbf{z}}}^{\,G}(\rho_i) = \mathbf{z}(\widehat{\chi^\beta_H \circ f}^{\,G}(\rho_i))^* \circ (\widehat{\chi^\beta_H \circ f}^{\,G}(\rho_i)) \ .$$

La démonstration de ce résultat est tout à fait symétrique à la preuve précédente.

Il est grand temps maintenant d'exposer la fameuse formule de conservation de l'énergie, qui n'en est pas vraiment une puisqu'il s'agit en fait d'une relation *matricielle*. Néanmoins le lecteur pourra constater de lui-même l'analogie avec les versions précédentes et en déduire une notion correspondante de fonction courbe.

Théorème 8.5. *Soit $f : G \to H$. La fonction f est parfaitement non linéaire à gauche si et seulement si $\forall \rho_i \in \widehat{G}$, $\forall \beta \in H^*$, $\forall \mathbf{z} \in \mathbb{C}$,*

$$\mathbf{z}(\widehat{\chi^\beta_H \circ f}^{\,G}(\rho_i)) \circ (\widehat{\chi^\beta_H \circ f}^{\,G}(\rho_i))^* = \mathbf{z}|G|Id_{V_i} \ .$$

Preuve. La fonction f est parfaitement non linéaire à gauche
$\Leftrightarrow \forall \alpha \in G^*,\ d^g_\alpha f$ est équilibrée (par définition)
$\Leftrightarrow \forall \alpha \in G^*,\ \forall \beta \in H^*,\ \widehat{\chi^\beta_H \circ d^g_\alpha f}^{\,G}(\rho_1) = 0_{End(\mathbb{C})}$ (d'après le lemme 8.2)
$\Leftrightarrow \forall \mathbf{z} \in \mathbb{C}, \forall \alpha \in G^*,\ \forall \beta \in H^*,\ (\widehat{\chi^\beta_H \circ d^g_\alpha f}^{\,G}(\rho_1))(\mathbf{z}) = 0$
$\Leftrightarrow \forall \mathbf{z} \in \mathbb{C}, \forall \alpha \in G^*,\ \forall \beta \in H^*,\ AC^g_{f,\beta,\mathbf{z}}(\alpha) = 0$ (par définition de $AC^g_{f,\beta,\mathbf{z}}$)
$\Leftrightarrow \forall \mathbf{z} \in \mathbb{C}, \forall \rho_i \in \widehat{G},\ \forall \beta \in H^*,\ \widehat{AC^g_{f,\beta,\mathbf{z}}}^{\,G}(\rho_i) = AC^g_{f,\beta,\mathbf{z}}(e_G)Id_{V_i}$ (d'après le lemme 8.1).
Or $AC^g_{f,\beta,\mathbf{z}}(e_G) = (\widehat{\chi^\beta_H \circ d^g_{e_G} f}^{\,G}(\rho_1))(\mathbf{z}) = \sum_{x\in G} \chi^\beta_H(e_H)\rho_1(x)(\mathbf{z}) = \mathbf{z}\sum_{x\in G}\chi^\beta_H(e_H) = \mathbf{z}|G|$.

Donc f est parfaitement non linéaire à gauche $\Leftrightarrow \forall \mathbf{z} \in \mathbb{C}, \forall \beta \in H^*, \forall \rho_i \in \widehat{G}, \widehat{AC^g_{f,\beta,\mathbf{z}}}^{\,G}(\rho_i) = \mathbf{z}|G|Id_{V_i}$
$\Leftrightarrow \forall \mathbf{z} \in \mathbb{C}, \forall \beta \in H^*, \forall \rho_i \in \widehat{G}, \mathbf{z}(\widehat{\chi^\beta_H \circ f}^{\,G}(\rho_i)) \circ (\widehat{\chi^\beta_H \circ f}^{\,G}(\rho_i))^* = \mathbf{z}|G|Id_{V_i}$ (par la proposition 8.10). □

De manière symétrique nous avons le théorème suivant.

Théorème 8.6. *Soit $f : G \to H$. La fonction f est parfaitement non linéaire à droite si et seulement si $\forall \rho_i \in \widehat{G}$, $\forall \beta \in H^*$, $\forall \mathbf{z} \in \mathbb{C}$,*

$$\mathbf{z}(\widehat{\chi^\beta_H \circ f}^{\,G}(\rho_i))^* \circ (\widehat{\chi^\beta_H \circ f}^{\,G}(\rho_i)) = \mathbf{z}|G|Id_{V_i} \ .$$

Si nous n'avons pas exactement obtenu une formule scalaire, cela est dû à la perte de commutativité du groupe G. De même qu'il est nécessaire d'utiliser des représentations linéaires de degré supérieur à 1 pour les groupes non commutatifs, la caractérisation de la non linéarité parfaite par la transformée de Fourier se fait via une équation linéaire non scalaire. Néanmoins, il est possible d'en déduire une véritable loi de conservation de l'énergie mais ceci ne se fait probablement pas gratuitement. Le prix à payer est peut-être[2] la perte de la condition suffisante.

Corollaire 8.4. *Soit $f : G \to H$. Si f est parfaitement non linéaire à gauche ou à droite alors $\forall \rho_i \in \widehat{G}$, $\forall \beta \in H^*$, $\forall \mathbf{z} \in \mathbb{C}$,*

$$\mathbf{z} \parallel \widehat{\chi^\beta_H \circ f}^{\,G}(\rho_i) \parallel^2 = \mathbf{z}|G| \dim_{\mathbb{C}}(V_i)$$

où pour $\lambda \in End(V)$, $\parallel \lambda \parallel^2 \stackrel{déf.}{=} tr(\lambda \circ \lambda^*)$ (en particulier $\parallel . \parallel$ définit une norme sur $End(V)$).

[2] Il s'agit là d'une interprétation intuitive et non d'une preuve formelle.

Preuve. Si la fonction f est parfaitement non linéaire à gauche (respectivement à droite) d'après le théorème 8.5 (respectivement le théorème 8.6) on a $\forall \rho_i \in \widehat{G}, \forall \beta \in H^*, \forall \mathtt{z} \in \mathbb{C}$, $\mathtt{z}(\widehat{\chi_H^\beta \circ f}^G(\rho_i)) \circ (\widehat{\chi_H^\beta \circ f}^G(\rho_i))^* = \mathtt{z}|G|Id_{V_i}$ (respectivement $\mathtt{z}(\widehat{\chi_H^\beta \circ f}^G(\rho_i))^* \circ (\widehat{\chi_H^\beta \circ f}^G(\rho_i)) = \mathtt{z}|G|Id_{V_i}$). Donc par passage à la trace dans les deux de membres de chacune des égalités précédentes, on obtient $\forall \rho_i \in \widehat{G}, \forall \beta \in H^*, \forall \mathtt{z} \in \mathbb{C}$,

$$\begin{array}{rrcl} & tr(\mathtt{z}(\widehat{\chi_H^\beta \circ f}^G(\rho_i)) \circ (\widehat{\chi_H^\beta \circ f}^G(\rho_i))^*) & = & tr(\mathtt{z}|G|Id_{V_i}) \\ \Leftrightarrow & \mathtt{z} \parallel \widehat{\chi_H^\beta \circ f}^G(\rho_i) \parallel^2 & = & \mathtt{z}|G| \dim_{\mathbb{C}}(V_i) \end{array}$$

ainsi que respectivement

$$\begin{array}{rrcl} & tr(\mathtt{z}(\widehat{\chi_H^\beta \circ f}^G(\rho_i))^* \circ (\widehat{\chi_H^\beta \circ f}^G(\rho_i))) & = & tr(\mathtt{z}|G|Id_{V_i}) \\ \Leftrightarrow & \mathtt{z} \parallel \widehat{\chi_H^\beta \circ f}^G(\rho_i) \parallel^2 & = & \mathtt{z}|G| \dim_{\mathbb{C}}(V_i) \ . \end{array}$$

□

8.4.4 Conclusion

Dans ce manuscrit, combien de versions particulières de la non linéarité parfaite - hormis cette dernière - ont-elles été étudiées jusqu'à présent ? Six, à savoir les déclinaisons booléenne, de Carlet et Ding, k-aire, d'Ambrosimov ainsi que celles basées sur les actions de groupe fidèles ou régulières et toutes dans un milieu favorable commutatif. Pour chacune d'entre elles, la même démarche a été adoptée :

- Définition de la non linéarité parfaite via une notion de dérivée ;
- Formulation de la notion de fonction équilibrée via la transformée de Fourier en « zéro » ;
- Caractérisation de la non linéarité parfaite via une formule de conservation de l'énergie faisant intervenir la transformée de Fourier.

Aussi n'est-il pas surprenant qu'en ce qui concerne la non linéarité parfaite des fonctions définies sur un groupe (fini) non abélien G et à valeurs dans un groupe (fini) commutatif H, nous ayons appliqué exactement le même protocole.

Ce qui peut paraître étonnant en revanche est la notion de fonction courbe établie ici. En effet, dans les cas précédents, une fonction était parfaitement non linéaire si sa transformée de Fourier (modulo une composition par un caractère et éventuellement par une fonction orbitale) était de module constant[3]. Mais la perte de commutativité induit un degré de complexité supplémentaire pour la caractérisation des fonctions parfaitement non linéaires en termes de leurs transformées de Fourier. Ainsi la relation finalement obtenue n'est pas, en général, de type scalaire mais matricielle. En définitive, cela discrimine réellement le cas non abélien des versions commutatives. Nous disposons donc maintenant d'une variante relativement complète de la non linéarité parfaite dans un cadre non commutatif. Comme cela a été réalisé au chapitre 7, nous lui appliquons maintenant la substitution de l'action[4] par translation par une action de groupe (fini non abélien) fidèle ou régulière.

[3] La célèbre formule de conservation de l'énergie.

[4] Il serait plus juste d'utiliser le pluriel puisque sont disponibles les actions à gauche et à droite.

8.5 Non linéarité parfaite basée sur une action d'un groupe fini non commutatif

8.5.1 Introduction

Ayant défini la non linéarité parfaite dans le cas non abélien, au même titre que ce qui a été fait au chapitre précédent, nous pouvons tordre cette notion de manière à prendre en compte une action d'un groupe non commutatif de préférence aux translations.

La non commutativité des groupes impliquent rigoureusement l'existence de deux notions de la non linéarité parfaite symétriques selon que les groupes agissent à gauche ou à droite. Néanmoins, puisque l'on passe très facilement d'une action à droite à une action à gauche (cf. chapitre 7), nous nous restreignons à la considération des seules actions à gauche. Par convention, toutes les actions considérées seront ainsi à gauche par défaut. L'explicitation des résultats symétriques sont donc laissés au lecteur (comme exercice ou comme jeu intellectuel).

L'organisation de cette section est la suivante. En premier lieu, contrairement au plan du chapitre précédent, nous exposons le cas d'une action régulière d'un groupe fini sur un ensemble (fini non vide). Puis nous abordons la caractérisation à l'aide de la transformée de Fourier de la non linéarité parfaite basée sur une action fidèle. A l'issue de cette section, la non linéarité parfaite basée sur une action de groupe non abélien et sa version duale seront complètement connues.

8.5.2 Cas d'une action régulière

Soit $((G,\top),(H,+),X)$ un triplet dans lequel G est un groupe fini non abélien agissant (à gauche) **régulièrement** sur l'ensemble fini non vide X et H est un groupe fini commutatif.

Les définitions énoncées au chapitre 7 dans la sous-section 7.3.2 p. 141, en particulier la notion de G-non linéarité parfaite, ainsi que la définition 7.18 p. 145 restent valides[5]. Davantage que cela, il s'avère que le théorème 7.3 p. 150 est (presque) vrai dans ce nouveau contexte. Si en toute rigueur, nous ne pouvons évidemment plus nous appuyer ni sur les travaux de Carlet et de Ding ni sur ceux de Logachev, Salnikov et Yashchenko puisque reposant sur des groupes finis abéliens et qu'il faille utiliser les résultats similaires dans le cadre non commutatif énoncés dans la section précédente, nous obtenons une assertion très proche, que ce soit dans son énoncé ou dans sa preuve, du théorème 7.3 et de son corollaire.

Proposition 8.11. *Soient $f : X \to H$ et $x_0 \in X$. La fonction f est G-parfaitement non linéaire si et seulement si la fonction $f_{x_0} : G \to H$ est parfaitement non linéaire (à gauche).*

Preuve. La fonction $f : X \to H$ est G-parfaitement non linéaire $\Leftrightarrow \forall \mathbf{g} \in G^*, \forall \beta \in H, |\{x \in X | D_{\mathbf{g}} f(x) = \beta\}| = \dfrac{|X|}{|H|}$

$\Leftrightarrow \forall \mathbf{g} \in G^*, \forall \beta \in H, |\{x \in X | f(\mathbf{g}.x) - f(x) = \beta\}| = \dfrac{|G|}{|H|}$ (par définition de $D_{\mathbf{g}} f$ et le fait que $|G| = |X|$)

$\Leftrightarrow \forall \mathbf{g} \in G^*, \forall \beta \in H, |\{\mathbf{h} \in G | f(\mathbf{g}.\mathbf{h}.x_0) - f(\mathbf{h}.x_0) = \beta\}| = \dfrac{|G|}{|H|}$ (puisque par régularité de l'action tout élément $x \in X$ s'écrit de manière unique sous la forme $\mathbf{h}.x_0$ pour un $\mathbf{h} \in G$)

$\Leftrightarrow \forall \mathbf{g} \in G^*, \forall \beta \in H, |\{\mathbf{h} \in G | f_{x_0}(\mathbf{g} \top \mathbf{h}) - f_{x_0}(\mathbf{h}) = \beta\}| = \dfrac{|G|}{|H|}$

[5] Nous avions alors sciemment tu le terme « commutatif » afin de disposer de définitions génériques.

$\Leftrightarrow \forall \mathbf{g} \in G^*, \forall \beta \in H, |\{\mathbf{h} \in G | d_{\mathbf{g}}^g f_{x_0}(\mathbf{h}) = \beta\}| = \dfrac{|G|}{|H|}$

$\Leftrightarrow f_{x_0}$ est parfaitement non linéaire à gauche. □

Remarque 8.7. En toute rigueur nous aurions dû introduire une notation du genre « $D_{\mathbf{g}}^g f$ » pour la dérivée au sens de l'action à gauche de G sur X de la fonction f suivant la direction $\mathbf{g}$ et symétriquement pour une éventuelle action à droite. Néanmoins puisque l'on s'est fixé comme convention de n'étudier que les actions à gauche, cela serait tout à fait superflu.

La version « courbe » de la proposition précédente est exposée ci-dessous.

Corollaire 8.5. *Soient $f : X \to H$ et $x_0 \in X$. La fonction f est G-parfaitement non linéaire si et seulement si $\forall \rho_i \in \widehat{G}$, $\forall \beta \in H^*$, $\forall \mathbf{z} \in \mathbb{C}$,*

$$\mathbf{z}(\widehat{\chi_H^\beta \circ f_{x_0}}^G(\rho_i)) \circ (\widehat{\chi_H^\beta \circ f_{x_0}}^G(\rho_i))^* = \mathbf{z}|G| Id_{V_i} \ .$$

En particulier, si f est G-parfaitement non linéaire alors $\forall \rho_i \in \widehat{G}$, $\forall \beta \in H^*$, $\forall \mathbf{z} \in \mathbb{C}$,

$$\mathbf{z} \parallel \widehat{\chi_H^\beta \circ f_{x_0}}^G(\rho_i) \parallel^2 = \mathbf{z}|G| \dim_{\mathbb{C}}(V_i) \ .$$

Preuve. La preuve est évidente par applications du théorème 8.5 et de son corollaire 8.4. □

Cette caractérisation usant de l'action par translation (à gauche) de G sur lui-même est fondamentalement liée au fait qu'il n'existe - modulo équivalence - qu'une seule action régulière pour un groupe donné.

Contrairement au chapitre 7, nous en restons là en ce qui concerne la caractérisation de la non linéarité parfaite basée sur une action régulière. En particulier, on ne s'étend pas sur la subtile distinction entre une action de G isomorphe ou non à l'action par translation de X sur lui-même (quand X est muni d'une structure de groupe). Néanmoins il est pertinent de remarquer que cela peut être raisonnablement réalisé de la même manière.

8.5.3 Cas d'une action fidèle : caractérisation par la transformée de Fourier

8.5.3.1 Résultats préliminaires

Il est possible de caractériser la notion de G-non linéarité parfaite dans le cadre des groupes non abéliens - avec une action (à gauche) fidèle sur un ensemble fini non vide X - à l'aide d'une formule mettant en jeu des transformées de Fourier. Le lecteur pourra avoir l'étrange impression de déjà vu corroborée par la démarche suivie ici, très semblable à celle du chapitre 7.

Pour l'intégralité de cette sous-section est donné un triplet $((G, \top), (H, +), X)$ dans lequel G est un groupe fini non abélien agissant à gauche au moins **fidèlement** sur l'ensemble fini non vide X et H est un groupe fini commutatif.

La caractérisation de la G-non linéarité parfaite en termes de transformée de Fourier dépend, comme au chapitre 7, du G-produit de convolution - dont la définition reste valide dans le contexte actuel - et de sa trivialisation. Néanmoins cette dernière devant être prise au sens de la théorie de Fourier basée sur les représentations linéaires, il est nécessaire d'effectuer de nouveaux calculs. Rappelons donc tout d'abord que le G-produit de convolution de deux fonctions φ et ψ de $\mathbb{C}^X$ est défini (voir la définition 7.17 p. 143) pour $\mathbf{g} \in G$ par :

$$(\varphi \bigstar \psi)(\mathbf{g}) = \sum_{x \in X} \overline{\varphi(x)} \psi(\mathbf{g}.x) \ .$$

En tant qu'élément de $\mathbb{C}^G$, il est possible de calculer sa transformée de Fourier. Soient donc $(\varphi,\psi)\in(\mathbb{C}^X)^2$ et $\rho_i\in\widehat{G}$.

$$\begin{aligned}\widehat{(\varphi\bigstar\psi)}^G(\rho_i) &= \sum_{\mathbf{g}\in G}(\varphi\bigstar\psi)(\mathbf{g})\rho_i(\mathbf{g})\\ &= \sum_{\mathbf{g}\in G}\sum_{x\in X}\overline{\varphi(x)}\psi(\mathbf{g}.x)\rho_i(\mathbf{g})\\ &= \sum_{x\in X}\overline{\varphi(x)}\sum_{\mathbf{g}\in G}\psi(\mathbf{g}.x)\rho_i(\mathbf{g})\ .\end{aligned}$$

Or pour tout $\mathbf{h}\in G$, on a $\sum_{\mathbf{g}\in G}\psi(\mathbf{g}.x)\rho_i(\mathbf{g})=\sum_{\mathbf{g}\in G}\psi(\mathbf{g}\top\mathbf{h}.x)\rho_i(\mathbf{g}\top\mathbf{h})$. On en déduit donc que pour chaque $\mathbf{h}\in G$,

$$\begin{aligned}\widehat{(\varphi\bigstar\psi)}^G(\rho_i) &= \sum_{x\in X}\overline{\varphi(x)}\sum_{\mathbf{g}\in G}\psi(\mathbf{g}\top\mathbf{h}.x)\rho_i(\mathbf{g}\top\mathbf{h})\\ &= \sum_{x\in X}\left(\sum_{\mathbf{g}\in G}\psi(\mathbf{g}\top\mathbf{h}.x)\rho_i(\mathbf{g})\right)\circ(\overline{\varphi(x)}\rho_i(\mathbf{h}))\\ &= \sum_{y\in X}\left(\sum_{\mathbf{g}\in G}\psi(\mathbf{g}.y)\rho_i(\mathbf{g})\right)\circ(\overline{\varphi(\mathbf{h}^{-1}.y)}\rho_i(\mathbf{h}))\\ &\quad\text{(par le changement de variables } y\overset{déf.}{=}\mathbf{h}.x)\\ &= \sum_{y\in X}\widehat{\psi_y}^G(\rho_i)\circ\overline{\varphi(\mathbf{h}^{-1}.y)}\rho_i(\mathbf{h})\ .\end{aligned}$$

La dernière égalité étant vraie pour tout $\mathbf{h}\in G$, elle l'est en particulier pour tout $\mathbf{h}^{-1}$ *i.e.*

$$\widehat{(\varphi\bigstar\psi)}^G(\rho_i)=\sum_{y\in X}\widehat{\psi_y}^G(\rho_i)\circ\overline{\varphi(\mathbf{h}.y)}\rho_i(\mathbf{h}^{-1})=\sum_{y\in X}\widehat{\psi_y}^G(\rho_i)\circ(\varphi(\mathbf{h}.y)\rho_i(\mathbf{h}))^*\ .$$

Une nouvelle fois cette égalité est valide pour tout $\mathbf{h}\in G$. Ainsi en sommant chaque membre de l'égalité sur G tout entier, on obtient :

$$\begin{aligned}\sum_{\mathbf{h}\in G}\widehat{(\varphi\bigstar\psi)}^G(\rho_i) &= |G|\widehat{(\varphi\bigstar\psi)}^G(\rho_i)\\ &= \sum_{y\in X}\widehat{\psi_y}^G(\rho_i)\circ(\sum_{\mathbf{h}\in G}\varphi(\mathbf{h}.y)\rho_i(\mathbf{h}))^*\\ &= \sum_{y\in X}\widehat{\psi_y}^G(\rho_i)\circ(\widehat{\varphi_y}^G(\rho_i))^*\ .\end{aligned}$$

En récapitulant, on a donc la forme suivante de trivialisation du G-produit de convolution, sensiblement voisine de celle du chapitre 7 :

$$\widehat{(\varphi\bigstar\psi)}^G(\rho_i)=\frac{1}{|G|}\sum_{x\in X}\widehat{\psi_x}^G(\rho_i)\circ(\widehat{\varphi_x}^G(\rho_i))^*\ . \tag{8.4}$$

8.5.3.2 Caractérisation duale

Soit une application $f:X\to H$. Pour chaque $\beta\in H$, on définit (comme dans la proposition 7.11) l'application

$$\begin{array}{rccc} AC_{f,\beta}: & G & \to & \mathbb{C}\\ & \mathbf{g} & \mapsto & \sum_{x\in X}(\chi_H^\beta\circ D_{\mathbf{g}}f)(x)\ .\end{array}$$

Calculons sa transformée de Fourier au sens des représentations. Soit alors $\rho_i \in \widehat{G}$.

$$\begin{aligned}
\widehat{AC_{f,\beta}}^G(\rho_i) &= \sum_{\mathbf{g}\in G} AC_{f,\beta}(\mathbf{g})\rho_i(\mathbf{g}) \\
&= \sum_{\mathbf{g}\in G}\sum_{x\in X} \chi_H^\beta(f(\mathbf{g}.x) - f(x))\rho_i(\mathbf{g}) \\
&= \sum_{\mathbf{g}\in G}\sum_{x\in X} \overline{\chi_H^\beta(f(x))}\chi_H^\beta(f(\mathbf{g}.x))\rho_i(\mathbf{g}) \\
&= \sum_{\mathbf{g}\in G} (\chi_H^\beta \circ f \bigstar \chi_H^\beta \circ f)(\mathbf{g})\rho_i(\mathbf{g}) \\
&= \widehat{(\chi_H^\beta \circ f \bigstar \chi_H^\beta \circ f)}^G(\rho_i) \\
&= \frac{1}{|G|}\sum_{x\in X} \widehat{(\chi_H^\beta \circ f)_x}^G(\rho_i) \circ (\widehat{(\chi_H^\beta \circ f)_x}^G(\rho_i))^* \text{ (d'après la formule (8.4))} \\
&= \frac{1}{|G|}\sum_{x\in X} \widehat{\chi_H^\beta \circ f_x}^G(\rho_i) \circ (\widehat{\chi_H^\beta \circ f_x}^G(\rho_i))^* \ .
\end{aligned}$$

On peut se rendre compte que l'on n'a pas eu besoin de recourir à l'utilisation d'un paramètre complexe $\mathbf{z}$, contrairement à la proposition 8.10. En effet dans le cas présent, la fonction $AC_{f,\beta}$ est à valeurs dans le corps des complexes lui-même et non dans $End(\mathbb{C})$. Sa transformée de Fourier est utilisée directement dans la preuve du théorème suivant qui précise la formule de conservation de l'énergie dans ce cas spécifique.

Théorème 8.7. *Soit $f : X \to H$. La fonction f est G-parfaitement non linéaire si et seulement si $\forall \rho_i \in \widehat{G}$, $\forall \beta \in H^*$*

$$\sum_{x\in X} \widehat{\chi_H^\beta \circ f_x}^G(\rho_i) \circ (\widehat{\chi_H^\beta \circ f_x}^G(\rho_i))^* = |G||X| Id_{V_i} \ .$$

En particulier si f est G-parfaitement non linéaire alors $\forall \rho_i \in \widehat{G}$, $\forall \beta \in H^*$

$$\sum_{x\in X} \| \widehat{\chi_H^\beta \circ f_x}^G(\rho_i) \|^2 = |G||X| \dim_{\mathbb{C}}(V_i) \ .$$

Preuve. La fonction f est G-parfaitement non linéaire
$\Leftrightarrow \forall \mathbf{g} \in G^*$, $D_{\mathbf{g}}f$ est équilibrée
$\Leftrightarrow \forall \beta \in H^*, \forall \mathbf{g} \in G^*, \sum_{x\in X} (\chi_H^\beta \circ D_{\mathbf{g}}f)(x) = 0$ (d'après la proposition 6.7)
$\Leftrightarrow \forall \beta \in H^*, \forall \mathbf{g} \in G^*, AC_{f,\beta}(\mathbf{g}) = 0$
$\Leftrightarrow \forall \beta \in H^*, \forall \rho_i \in \widehat{G}, \widehat{AC_{f,\beta}}^G(\rho_i) = AC_{f,\beta}(e_G) Id_{V_i}$ (par le lemme 8.1)
$\Leftrightarrow \forall \beta \in H^*, \forall \rho_i \in \widehat{G}, \frac{1}{|G|}\sum_{x\in X} \widehat{\chi_H^\beta \circ f_x}^G(\rho_i) \circ (\widehat{\chi_H^\beta \circ f_x}^G(\rho_i))^* = AC_{f,\beta}(e_G)$ (d'après le calcul de la transformée de Fourier de $AC_{f,\beta}$).
Or $AC_{f,\beta}(e_G) = \sum_{x\in X} (\chi_H^\beta \circ D_{e_G}f)(x) = \sum_{x\in X} \chi_H^\beta(e_H) = |X|$. D'où la fonction f est G-parfaitement non linéaire si et seulement si $\forall \beta \in H^*, \forall \rho_i \in \widehat{G}, \sum_{x\in X} \widehat{\chi_H^\beta \circ f_x}^G(\rho_i) \circ (\widehat{\chi_H^\beta \circ f_x}^G(\rho_i))^* = |G||X| Id_{V_i}$.
En particulier par un simple passage à la trace on en déduit le dernier fait. □

La formule de conservation de l'énergie du théorème précédent ressemble, et ce n'est pas surprenant, à la fois à celle dans le cas d'une action fidèle énoncée au chapitre 7 et à celle concernant la non linéarité parfaite de la section précédente. En particulier, elle peut être interprétée comme une espérance mathématique (non scalaire).

8.5.4 Conclusion

Au cours de la section précédente, nous avions défini la notion de non linéarité parfaite dans le cas de fonctions définies sur un groupe fini non abélien et à valeurs dans un groupe fini abélien et exhibé sa caractérisation en termes de transformée de Fourier au sens des représentations linéaires. La substitution des translations par un autre type d'actions de groupe abstrait est, dans ce contexte, tout aussi valide que dans celui du chapitre 7.

La non commutativité règne sans partage sur ce présent chapitre. Il est donc clair que les actions à considérer sont définies sur des groupes finis non abéliens. Hormis cette différence capitale, à l'instar du chapitre 7, deux cas principaux se rencontrent selon que l'action de groupe est régulière ou seulement fidèle.

Lorsque le groupe non abélien, disons G, opère régulièrement, il est possible de formuler la G-non linéarité parfaite basée sur cette action à l'aide de celle sur G au sens des translations via l'utilisation d'une fonction orbitale. Fondamentalement les choses demeurent en somme inchangées par rapport au chapitre 7. Seul le langage de la théorie de Fourier a évolué passant des caractères aux représentations linéaires.

Si maintenant le groupe G n'agit que fidèlement sur un ensemble X nous obtenons une caractérisation par la théorie de Fourier reposant sur un genre de moyenne statistique de transformées de Fourier. En ce sens, elles apparaît très clairement similaire à celle du chapitre 7 et sous-tend fondamentalement le fait qu'une action fidèle ne « voit » pas les éléments de X de manière globale - comme les actions régulières - mais les localise simplement au sein d'orbites.

8.6 G-ensembles à différences : cas non commutatif

8.6.1 Observations

Dans la section 7.6 du chapitre 7, nous avions identifié les fonctions G-parfaitement non linéaires à valeurs dans $\mathbb{F}_2$ avec les indicatrices d'objets combinatoires appelés G-ensembles à différences. Nous avions alors en outre pris soin d'énoncer et de démontrer les résultats - hormis ceux directement en rapport avec les constructions explicites - sans perte de généralité en utilisant la seule hypothèse algébrique sur G : un groupe fini agissant (fidèlement ou régulièrement) à gauche sur un certain ensemble (fini non vide). Il en résulte immédiatement que la portée de ces résultats dépasse le chapitre 7 et garantit leur légitimité dans le contexte non abélien évoqué ici.

Puisque la caractérisation de la G-non linéarité parfaite des fonctions à valeurs dans $\mathbb{F}_2$ demeure fondée lorsque l'on passe des groupes abéliens aux groupes non commutatifs, il est suffisant de simplement se la remémorer.

Caractérisation par les G-ensembles à différences
Soient G un groupe fini (commutatif ou non) et X un ensemble fini non vide sur lequel G agit (à gauche). Supposons en outre que $|X| \equiv 0 \pmod 4$. Soit une fonction $f : X \to \mathbb{F}_2$.

1. *Supposons que l'action soit fidèle. Alors la fonction f est G-parfaitement non linéaire si et seulement si S_f est un G-(v, k, λ)-ensemble à différences de X tel que $\frac{v}{4} = k - \lambda$;*
2. *Supposons que l'action soit régulière. Alors la fonction f est G-parfaitement non linéaire si et seulement si S_f est un G-$(4n^2, 2n^2 \pm n, n(n \pm 1))$-ensemble à différences de X avec $|X| = 4n^2$.*

Nous allons maintenant utiliser ces résultats afin de construire quelques exemples de fonctions G-parfaitement non linéaires.

8.6.2 Quelques exemples

8.6.2.1 Cas d'une action régulière

Nous nous intéressons ici au cas de la G-non linéarité parfaite d'une fonction f à valeurs dans $\mathbb{F}_2$ lorsque le groupe fini non abélien G agit régulièrement (à gauche) sur un certain ensemble X. Comme nous le savons, pour que de telles fonctions existent il faut et il suffit qu'existent des G-$(4n^2, 2n^2 \pm n, n(n \pm 1))$-ensembles à différences de X avec $|X| = 4n^2$. Les fonctions indicatrices de tels ensembles étant évidemment G-parfaitement non linéaires.

Par ailleurs le lemme 7.9 du chapitre 7 nous apprend qu'il est possible de transporter sur X les ensembles à différences (classiques) de G en utilisant la fonction orbitale ϕ_x (pour un élément x quelconque appartenant à X). Les objets alors obtenus sont des G-ensembles à différences de X de mêmes paramètres que les ensembles originaux. Il est donc clair que l'existence d'ensembles à différences de Hadamard dans le groupe non abélien G mène inévitablement à la construction de fonctions G-parfaitement non linéaires. Il convient donc de vérifier la présence d'ensembles de Hadamard dans G *i.e.* dont les paramètres vérifient $(v, k, \lambda) = (4n^2, 2n^2 \pm n, n(n \pm 1))$ avec $|G| = |X| = v = 4n^2$.

De nombreux travaux ont été effectués concernant la problématique des ensembles à différences de Hadamard dans les groupes finis non abéliens (voir par exemple [DS94]). Aussi nous nous contentons ici de ne citer que quelques résultats. Pour ce faire nous rappelons au préalable la notion classique de groupe défini par générateurs et relations.

Le *commutant* de deux éléments x et y d'un groupe noté multiplicativement est défini par $[x, y] \stackrel{déf.}{=} xyx^{-1}y^{-1}$. On note « A » un *alphabet* fini (c'est-à-dire un ensemble fini) et « $G_{\mathcal{L}}(A)$ » le groupe *libre* engendré par A *i.e.* les éléments de ce groupe sont les suites finies (ou *mots*) d'éléments de la forme x ou x^{-1} pour $x \in A$. La loi de composition des mots est la *concaténation*. Cette loi, associative, n'est pas commutative. On convient de noter « 1 » le mot vide, qui représente l'élément neutre du groupe. Enfin on définit $x^n \stackrel{déf.}{=} \underbrace{x \dots x}_{n \ fois}$ pour $x \in A$. La définition d'un groupe défini par générateurs et relations s'obtient comme suit. Soit X_R une partie du groupe libre $G_{\mathcal{L}}(A)$ et H le sous-groupe distingué engendré par la partie X_R. Les éléments de X_R sont appelés les *relations*. Le groupe quotient $G_{\mathcal{L}}(A)/H$ est alors le *groupe défini par les générateurs de A et les relations X_R*. Généralement X_R se représente à l'aide d'égalités avec 1. Si $A = \{x, y, z, \dots\}$ et $X_R = \{x_1 \in G_{\mathcal{L}}(A) | x_1 = 1\} \cup \dots \cup \{x_n \in G_{\mathcal{L}}(A) | x_n = 1\}$, on pose simplement $\langle x, y, z, \dots | x_1 = \dots = x_n = 1 \rangle \stackrel{déf.}{=} G_{\mathcal{L}}(A)/H$. Par convention si $X \subset G_{\mathcal{L}}(A)/H$ et $x' \in A$ alors $Xx' \stackrel{déf.}{=} \{xx' | x \in X\}$.

Nous listons maintenant des exemples d'ensembles à différences de Hadamard dans des groupes non commutatifs.

1. L'ensemble

$$\begin{array}{rcl} D & = & \{1, x, x^4\} \cup \{1, x\}y \cup \{1, x, x^3, x^4\}y^2 \cup \{1, x, x^2, x^3\}y^3 \cup \{1, x^4\}y^4 \\ & \cup & (\{x^2, x^4, x^4y, x^3y^2\} \cup \{1, x^2\}y \cup \{x, x^2, x^3, x^4\}y^4)z \\ & \cup & (\{a^4\} \cup \{1, x, x^2, x^4\}y \cup \{x, x^4\}y^2 \cup \{1, x^2, x^4\}y^3 \cup \{x^3y^4\})z^2 \\ & \cup & (\{x^3, x^4\} \cup \{1, x^4\}y \cup \{x^3y^2\} \cup \{x, x^2, x^3, x^3, x^4\}y^3 \cup \{xy^4\})z^3 \end{array}$$

est un $(100, 45, 20)$-ensemble à différences du groupe non commutatif :

$$\langle x, y, z | x^5 = y^5 = z^4 = [x, y] = zxz^{-1}x^{-2} = zyz^{-1}y^{-2} = 1 \rangle \ .$$

Il n'existe pas d'ensembles à différences avec ces paramètres dans des groupes commutatifs (voir [McF89, Smi95]) ;

2. Les ensembles à différences de paramètres $(16, 6, 2)$. Il y a 14 groupes non isomorphes d'ordre 16. Parmi eux certains possèdent des ensembles à différences de Hadamard (voir [Kib78]). En ce qui concerne les groupes non commutatifs nous avons la liste suivante (la numérotation des groupes et des ensembles à différences est identique à celle de [Kib78]) :

Groupe	Ensemble à différences
$G_1 = \langle x, y, z \mid x^4 = z^2 = y^2x^2 = x^3yx^{-1}y^{-1} = [x, z] = [y, z] = 1 \rangle$	$D_{11} = \{1, x, x^2, y, z, xyz\}$ $D_{12} = \{1, x, x^2, y, xz, x^2yz\}$
$G_2 = \langle x, y, z \mid x^4 = y^4 = z^4 = x^2y^2z^2 = x^3yx^{-1}y^{-1} = [x, z] = [y, z] = 1 \rangle$	$D_{13} = \{1, x, x^2, y, xz, yz\}$ $D_{14} = \{1, x, y, xy, z, x^2yz\}$
$G_3 = \langle x, y, z \mid x^4 = y^2 = z^2 = yxyx = [x, z] = [y, z] = 1 \rangle$	$D_9 = \{1, x, x^2, y, xz, x^2yz\}$ $D_{10} = \{1, x, y, x^2y, z, x^3z\}$
$G_4 = \langle x, y, z \mid x^4 = y^2 = yz^2 = x^3yzx^{-1}z^{-1} = [x, y] = 1 \rangle$	$D_{15} = \{1, x, x^2, xy, z, x^2yz\}$ $D_{16} = \{1, x, x^2, xy, xz, x^3yz\}$ $D_{17} = \{1, x, y, x^3y, xz, x^3z\}$ $D_{18} = \{1, x, x^2, x^3y, xz, xyz\}$
$G_5 = \langle x, y \mid x^4 = y^4 = x^3yx^{-1}y^{-1} = 1 \rangle$	$D_{19} = \{1, x, x^2, y, xy^2, x^2y^3\}$ $D_{20} = \{1, x, x^2, y, y^3, x^3y, x^5y\}$ $D_{21} = \{1, x, y, x^2y, y^2, x^3y^2\}$
$G_6 = \langle x, y \mid x^8 = y^2 = x^5yx^{-1}y^{-1} = 1 \rangle$	$D_{22} = \{1, x, x^2, x^5, x^2y, x^4y\}$ $D_{23} = \{1, x, x^3, x^4, x^3y, x^5y\}$
$G_7 = \langle x, y \mid x^8 = y^4 = x^4y^2 = x^3yx^{-1}y^{-1} = 1 \rangle$	$D_{24} = \{1, x, x^2, x^5, y, x^2y\}$ $D_{25} = \{1, x, x^3, x^4, xy, x^3y\}$
$G_8 = \langle x, y \mid x^8 = y^4 = x^4y^2 = x^7yx^{-1}y^{-1} = 1 \rangle$	$D_{26} = \{1, x, x^2, x^5, y, x^2y\}$ $D_{27} = \{1, x, x^3, x^4, y, x^2y\}$

8.6.2.2 Cas d'une action fidèle

Dans ce paragraphe est exhibée la construction générique d'un G-ensemble à différences lorsque G est un groupe fini non commutatif agissant (à gauche) fidèlement sur un certain ensemble fini non vide. Plus précisément nous nous inspirons de résultats tirés du paragraphe 7.6.2.2 du chapitre 7 en les généralisant de manière astucieuse.

Soit donc $(G, \top)$ un groupe fini non abélien dont on suppose qu'il possède des ensembles à différences de Hadamard. En particulier, $|G| = 4n^2$ pour un certain entier n. Pour chaque $i \in \mathbb{N}$, on définit l'ensemble $X_i \stackrel{déf.}{=} G \times \{i\}$.

Lemme 8.3. *Soit $i \in \mathbb{N}$. L'action (à gauche) de $(G, \top)$ sur X_i définie par*

$$\begin{array}{rccl} \phi : & G & \to & S(X_i) \\ & \mathbf{g} & \mapsto & \phi(\mathbf{g}) : (\mathbf{h}, i) \mapsto (\mathbf{g} \top \mathbf{h}, i) \end{array}$$

est régulière.

Preuve. Tout d'abord on introduit l'application suivante :

$$\begin{array}{rccl} \Theta : & G & \to & X_i \\ & \mathbf{g} & \mapsto & (\mathbf{g}, i) \ . \end{array}$$

Il s'agit évidemment d'une correspondance biunivoque entre G et X_i et sa bijection réciproque vérifie $\forall (\mathbf{g}, i) \in X_i$, $\Theta^{-1}(\mathbf{g}, i) = \mathbf{g}$ (c'est-à-dire que Θ^{-1} est le première projection de X_i). Soit

maintenant l'application

$$\begin{array}{rccc} \Im_\Theta : & S(G) & \to & S(X_i) \\ & \pi & \mapsto & \Theta \circ \pi \circ \Theta^{-1} \ . \end{array}$$

Il est facile de vérifier que $\Im_\Theta$ est en fait un isomorphisme de groupes (il suffit essentiellement d'établir que $\ker(\Im_\Theta) = \{Id_{S(G)}\}$ ce qui ne pose pas de difficulté particulière). En utilisant ces diverses applications, on peut écrire que pour tout $\mathbf{g} \in G$, $\phi(\mathbf{g}) = \Im_\Theta \circ \sigma_{\mathbf{g}}^g$ (où « $\sigma_{\mathbf{g}}^g$ » est le nom de la translation (à gauche) par $\mathbf{g}$ dans G). Alors ϕ est un homomorphisme de groupes par composition d'homomorphismes (l'application $\mathbf{g} \in G \mapsto \sigma_{\mathbf{g}}^g$ est un isomorphisme de groupes de G dans son groupe des translations à gauche). Soit $(\mathbf{g}, i) \in X_i$. L'application orbitale $\phi_{(\mathbf{g},i)}$ est bijective puisque $\phi_{(\mathbf{g},i)} = \Theta \circ \sigma_{\mathbf{g}}^d$. Il en résulte que ϕ est bien une action régulière (à gauche) de G sur X_i. □

Soit maintenant $m \in \mathbb{N}^*$ fixé. On définit $X \stackrel{déf.}{=} \bigcup_{i=1}^{m} X_i$. Par construction, il s'agit d'une union disjointe et $|X| = m|G| = m4n^2$.

Pour chaque $i \in \{1, \ldots, m\}$, on choisit D_i un ensemble à différences de Hadamard dans G (puisque de tels ensembles existent par hypothèse). Si la lettre « j » désigne le nombre d'ensembles à différences de Hadamard usuels (*i.e.* les paramètres sont $(4n^2, 2n^2 - n, n(n-1))$) choisis alors $m - j$ est le nombre de compléments (les paramètres sont $(4n^2, 2n^2 + n, n(n+1))$). Soit $\mathbf{g} \in G$ fixé. Alors on définit $D \stackrel{déf.}{=} \bigcup_{i=1}^{m} \phi_{(\mathbf{g},i)}(D_i)$. Il s'agit d'après le lemme 7.9 d'une union disjointe de G-ensembles à différences des X_i avec les paramètres de type Hadamard (ceux de $\phi_{(\mathbf{g},i)}(D_i)$ correspondant à ceux de D_i).

Maintenant nous montrons que D est lui-même un G-ensemble à différences de X. Tout d'abord, $|D| = \sum_{i=1}^{m} |D_i| = (2n^2 - n)j + (2n^2 + n)(m - j)$. Soit $\mathbf{h} \in G^*$. Pour chaque $i \in \{1, \ldots, m\}$, l'équation $(\mathbf{g}_1, i) = (\mathbf{h} \top \mathbf{g}_2, i)$ a exactement λ_i solutions dans $(\phi_{(\mathbf{g},i)}(D_i))^2$, où $\lambda_i \stackrel{déf.}{=} n^2 \pm n$ selon que D_i est un ensemble à différences de Hadamard usuel ou un complément, puisque $\phi_{(\mathbf{g},i)}(D_i)$ est un G-ensemble à différences de X_i avec les mêmes paramètres que ceux de D_i. Comme les ensembles $\phi_{(\mathbf{g},i)}(D_i) \subset X_i$ sont tous mutuellement disjoints, l'équation $(\mathbf{g}_1, i) = (\mathbf{h} \top \mathbf{g}_2, i)$ a exactement $\sum_{i=1}^{m} \lambda_i = (n^2 - n)j + (n^2 + n)(m - j)$ solutions dans D^2. En définitive nous venons ainsi de démontrer le théorème suivant.

Théorème 8.8. *Avec les hypothèses sur G et la définition de X, pour tout $j \in \{0, \ldots, m\}$, il existe un G-$(m4n^2, (2n^2-n)j+(2n^2+n)(m-j), (n^2-n)j+(n^2+n)(m-j))$-ensemble à différences de X. En particulier ces G-ensembles à différences satisfont l'équation sur les paramètres $v = 4(k - \lambda)$.*

Ce résultat nous assure donc l'existence de fonctions G-parfaitement non linéaires dans le cas d'une action fidèle (à gauche) dès lors que G possède des ensembles à différences de Hadamard classiques. Observons que dès que $m > 1$ les G-ensembles obtenus ne sont pas équivalents à des ensembles de Hadamard. On a donc bien exhibé une toute nouvelle série d'objets n'existant pas dans l'approche classique que ce soit de la non linéarité parfaite ou des ensembles à différences.

8.7 Conclusion

L'issue de ce chapitre coïncide pratiquement avec la fin du manuscrit et constitue notamment le point final des recherches exposées dans la seconde partie. Cette dernière avait été introduite, rappelons-le, par une question à la fois simple, très générale et peu précise : « que se passe-t-il si l'on substitue dans la définition de la non linéarité parfaite les translations par d'autres types de permutations ? ». La réponse, inversement plus complexe que l'interrogation, a été construite en deux phases distinctes, chacune incarnée par un chapitre, de niveau de difficulté croissant. La première, exposée dans le chapitre 7, consiste en une généralisation de la non linéarité parfaite au travers de l'utilisation d'actions de groupe fini commutatif et se fonde dans une large mesure sur l'outillage théorique classique présenté dans la première partie du manuscrit. La seconde phase est quant à elle contenue dans ce 8^{e} et ultime chapitre[6] de la thèse. Nous affirmions plus haut que le degré de complexité, entre les 7^{e} et 8^{e} chapitres, allait en s'accentuant. En particulier nous perdons ici la propriété de commutativité des groupes envisagés. Ceci n'est pas un détail. Ainsi une grande partie des concepts exploités précédemment dans un cadre abélien deviennent complètement inutiles dans ce nouveau contexte. Afin de combler ces lacunes et de généraliser la dualité des groupes finis commutatifs, la théorie des représentations linéaires ainsi que la théorie de Fourier correspondante ont été introduites. Ces outils sophistiqués jouent dans ce chapitre un rôle au moins aussi primordial que celui de la théorie des caractères et la transformée de Fourier discrète au chapitre 7. Ils permettent notamment d'envisager les concepts sous un angle différent mais complémentaire de celui de l'approche purement combinatoire. L'outillage théorique fondamental acquis, nous avons ensuite abordé et formulé le problème proprement dit de la non linéarité parfaite au sens non commutatif. Ainsi le développement relativement complet, d'une part, d'une extension de la non linéarité parfaite au sens des groupes non abéliens et de son interprétation selon la théorie de Fourier, et d'autre part, sa propre généralisation au sens des actions de groupe, selon le même *modus operandi* qu'au chapitre 7, a été exposé. Ce chapitre de part sa trame représente symboliquement l'analogue dans un contexte non commutatif des contenus des chapitres 6 et 7. En définitive nous avons su répondre avec précision et rigueur à la question reprise au début de cette conclusion. A l'issue de ce présent chapitre, nous disposons d'une théorie de la non linéarité parfaite prenant en compte dans une même unité conceptuelle les cas des actions à gauche ou à droite, fidèles ou régulières des groupes finis non abéliens et se caractérisant, tout le temps, sous l'allure de formules de conservation de l'énergie et, parfois, sous la forme d'objets combinatoires appelés G-ensembles à différences.

[6] Le chapitre de conclusion étant mis à part.

Chapitre 9

Conclusion et perspectives

Je regarde vers mon futur car mon passé est derrière moi.

TUPAC AMARU SHAKUR, *Only God Can Judge Me*

Conclusion

Le point de départ des travaux exposés dans ce manuscrit est la notion de non linéarité parfaite au sens de Carlet et Ding (voir le chapitre 6). Soient G et H deux groupes finis commutatifs (en notation additive) et $f : G \to H$. La fonction f est *parfaitement non linéaire* si et seulement $\forall(\alpha, \beta) \in G^* \times H$,

$$|\{x \in G | f(x+\alpha) - f(x) = \beta\}| = \frac{|G|}{|H|} .$$

Constatant que cette notion était fondamentalement liée à celle d'action de groupe, nous l'avons interprétée dans un cadre à la fois plus général et plus abstrait, baptisé *G-non linéarité parfaite*, en remplaçant les translations par une action de groupe quelconque. Soient G un groupe fini, H un groupe fini commutatif, X un ensemble fini non vide sur lequel G opère au moins fidèlement (pour $(\mathbf{g}, x) \in G \times X$, on dénote par « $\mathbf{g}.x$ » l'action de G sur X) et $f : X \to H$. La fonction f est *G-parfaitement non linéaire* si et seulement si $\forall(\mathbf{g}, \beta) \in G^* \times H$,

$$|\{x \in X | f(\mathbf{g}.x) - f(x) = \beta\}| = \frac{|X|}{|H|} .$$

Cette nouvelle approche conceptuelle, de part son universalité et sa richesse descriptive, a permis l'élaboration d'un modèle unique et standard dans lequel se déclinent plusieurs variantes possibles de la non linéarité parfaite parmi lesquelles la version traditionnelle notamment formulée par Carlet et Ding.

L'aspect dual de cette généralisation a aussi été largement développé dans nos contributions. Ainsi chacun des types principaux de non linéarité parfaite généralisée se caractérise à l'aide d'une formule de conservation de l'énergie *i.e.* la notion de fonction courbe appropriée, comme dans le cas classique dans lequel la fonction $f : G \to H$ est parfaitement non linéaire si et seulement si $\forall(\alpha, \beta) \in G \times H^*$,

$$|\widehat{\chi_H^\beta \circ f}(\alpha)| = \sqrt{|G|} .$$

La notion duale de la non linéarité parfaite généralisée s'exprime de différentes manières selon que le groupe agissant est abélien ou non abélien.

Action de groupe fini commutatif

Le tableau ci-dessous récapitule les formules de conservation de l'énergie obtenues pour une fonction G-parfaitement non linéaire $f : X \to H$ avec G et H deux groupes finis **commutatifs** et G agissant au moins fidèlement sur l'ensemble fini non vide X.

Action de G sur X	Formule de conservation de l'énergie
Régulière	$\forall(\alpha,\beta,x) \in G \times H^* \times X,\ \widehat{|\chi_H^\beta \circ f_x(\alpha)|} = \sqrt{|G|}$
Fidèle	$\forall(\alpha,\beta) \in G \times H^*,\ \sum_{x\in X} \widehat{|\chi_H^\beta \circ f_x(\alpha)|^2} = |G||X|$

Pour $x \in X$, l'application f_x figurant dans le tableau précédent est définie par :

$$\begin{array}{rccc} f_x : & G & \to & H \\ & \mathbf{g} & \mapsto & f(\mathbf{g}.x)\ . \end{array}$$

Cas non abélien

Dès lors que le groupe fini G agissant est non abélien, il nous est impossible de nous appuyer ni sur la théorie de la dualité des groupes finis commutatifs et la transformée de Fourier discrète ni sur les travaux de Carlet et Ding. Nous avons donc développé dans un premier temps le pendant non abélien de ces travaux en faisant abstraction d'une quelconque action de groupe, autrement dit, on s'est restreint à l'action par translation (à gauche) de G sur lui-même. Puis en utilisant la théorie des représentations des groupes finis, analogue non abélien de la théorie des caractères, nous avons exhibé une formulation duale. Le défaut de commutativité est alors largement mis en évidence par l'allure de la formule de conservation de l'énergie obtenue, qui n'est plus de type scalaire mais matriciel. Ainsi $f : G \to H$ est une fonction parfaitement non linéaire (avec G non abélien et H commutatif) si et seulement si $\forall(\rho_i,\beta,\mathbf{z}) \in \widehat{G} \times H^* \times \mathbb{C}$,

$$\mathbf{z}(\widehat{\chi_H^\beta \circ f}^{\,G}(\rho_i)) \circ (\widehat{\chi_H^\beta \circ f}^{\,G}(\rho_i))^* = \mathbf{z}|G|Id_{V_i}$$

où $\widehat{\varphi}^G$ est la transformée de Fourier au sens des représentations linéaires d'une fonction $\varphi : G \to \mathbb{C}$ et V_i est un $\mathbb{C}$-espace vectoriel de dimension finie implicitement lié à la représentation ρ_i de G. Cette notion non commutative de la non linéarité parfaite a ensuite été généralisée en remplaçant les translations par d'autres types d'actions de groupe fini non abélien, d'une manière analogue à ce qui a été réalisé avec la version de Carlet et Ding dans un contexte commutatif. Dans ce cas, nous obtenons deux formules de conservation de l'énergie, listées ci-dessous pour une fonction G-parfaitement non linéaire $f : X \to H$ avec G un groupe fini **non commutatif** agissant au moins fidèlement sur l'ensemble fini non vide X et H un groupe fini commutatif.

Action de G sur X	Formule de conservation de l'énergie
Régulière	$\mathbf{z}(\widehat{\chi_H^\beta \circ f_x}^{\,G}(\rho_i)) \circ (\widehat{\chi_H^\beta \circ f_x}^{\,G}(\rho_i))^* = \mathbf{z}\|G\|Id_{V_i}$
Fidèle	$\sum_{x\in X} (\widehat{\chi_H^\beta \circ f_x})^{G}(\rho_i) \circ ((\widehat{\chi_H^\beta \circ f_x})^{G}(\rho_i))^* = \|G\|\|X\|Id_{V_i}$

La première formule du tableau doit être satisfaite pour tout $(\rho_i,\beta,x,\mathbf{z}) \in \widehat{G} \times H^* \times X \times \mathbb{C}$ et la seconde pour tout $(\rho_i,\beta) \in \widehat{G} \times H^*$.

G-ensembles à différences

En parallèle à cela et que ce soit dans le contexte commutatif ou non commutatif, nous avons en outre généralisé la caractérisation combinatoire particulière des fonctions parfaitement non linéaires à valeurs dans $\mathbb{F}_2$ basée sur les ensembles à différences. Afin d'expliciter cela, plaçons-nous dans le cas où G est un groupe fini (abélien ou non) agissant au moins fidèlement sur un ensemble fini non vide X. Un sous-ensemble D de X est un G-(v, k, λ)-*ensemble à différences* de X si $v = |X|$, $k = |D|$ et pour chaque $\mathbf{g} \in G^*$, l'équation $x = \mathbf{g}.y$ admet exactement λ solutions dans D^2. Il s'agit donc simplement de la définition des ensembles à différences classiques dans laquelle, une nouvelle fois, les translations ont été remplacées par l'action de groupe de G sur X. Nous avons alors démontré que les fonctions G-parfaitement non linéaires $f : X \to \mathbb{F}_2$ sont toutes sans exception les indicatrices de G-ensembles à différences de X dont les paramètres satisfont $v = 4(k - \lambda)$. A l'aide de tels objets, nous avons été en mesure d'exhiber des fonctions pertinemment distinctes de celles tirées de la théorie traditionnelle, notamment dans des cas où les fonctions classiquement courbes n'existent pas (par exemple dans le cas de la longueur impaire).

Afin d'illustrer ces propos et de fixer les idées, plaçons-nous dans le contexte des fonctions définies sur $\mathbb{F}_2^9$ et à valeurs dans $\mathbb{F}_2$. Il n'existe donc pas de fonction parfaitement non linéaire (ni courbe bien entendu) dans ce cas puisque le nombre de variables - neuf en l'occurrence - est impair. Toutefois nous avons construit des G-ensembles à différences dont les paramètres appartiennent à l'une des trois familles $(512, 240, 112)$, $(512, 256, 128)$ et $(512, 272, 144)$ et où le groupe G, d'ordre 256, est isomorphe dans son action fidèle (et non régulière) sur $\mathbb{F}_2^9$ à un sous-groupe de translations de $\mathbb{F}_2^9$. Les indicatrices de ces fonctions étant G-parfaitement non linéaires, nous complétons ainsi, par ces nouvelles familles de fonctions, les zones d'ombre non traitées par l'exploitation de la théorie classique.

Perspectives

Nos travaux reposent essentiellement sur la généralisation de trois caractérisations équivalentes de la non linéarité parfaite, à savoir, la définition combinatoire de la G-non linéarité parfaite, sa formulation à l'aide de la transformée de Fourier et l'approche utilisant les G-ensembles à différences. La question de savoir si d'autres représentations équivalentes existent se pose alors naturellement. Dans le cas des involutions sans point fixe (annexe B), nous avons ainsi abordé le cas de la distance des fonctions G-parfaitement non linéaires à un ensemble de fonctions « affines », étendant le résultat connu sur les fonctions courbes et le rayon de recouvrement du code de Reed-Muller. Peut-on effectuer un travail similaire pour d'autres configurations ? Cette question semble très difficile même en ne considérant que le cas des fonctions à valeurs dans $\mathbb{F}_2$.

Des constructions explicites de fonctions G-parfaitement non linéaires ont été exposées. Néanmoins nous ne les avons pas étudiées de manière systématique semblablement à la classification en classes des fonctions booléennes courbes. Une autre approche de cette même problématique consisterait à examiner quelles sont les classes transposables dans le cadre abstrait de la G-non linéarité parfaite et ainsi déceler celles intrinsèquement liées à la structure de $\mathbb{F}_2$-espace vectoriel.

Dans la seconde partie du manuscrit, nous avons souvent mis l'accent sur la relaxation des contraintes apportée par la considération d'actions de groupe fidèles seulement plutôt que régulières. Au contraire de cela, nous pouvons traiter des propriétés plus fortes, notamment celle de k-transitivité des actions. Néanmoins en réduisant immodérément les degrés de liberté, nous risquons de rendre impossible l'existence de fonctions G-parfaitement non linéaires dans ces configurations particulières.

Les contributions apportées peuvent paraître à première vue très éloignées de la cryptographie, néanmoins il faut se souvenir que leur fondement théorique est la notion de non linéarité parfaite permettant de formaliser les fonctions maximalement résistantes face à l'attaque différentielle. De la sorte nous avons fondamentalement établi des critères de résistance à des cryptanalyses non encore explicitées. Afin de fixer les idées, supposons que G soit un groupe fini agissant fidèlement sur $\mathbb{F}_2^m$. Intuitivement, en nous référant à l'attaque différentielle classique, pour attaquer efficacement de manière « G-différentielle » une fonction $f : \mathbb{F}_2^m \to \mathbb{F}_2^n$, il est nécessaire que celle-ci ne soit pas G-parfaitement non linéaire, autrement dit, il faut trouver une « G-différentielle » $(\mathbf{g}, \beta) \in G^* \times \mathbb{F}_2^n$ pour laquelle, $|\{x \in \mathbb{F}_2^m | f(\mathbf{g}.x) \oplus f(x) = \beta\}|$ soit le plus grand possible afin de maximiser sa fréquence d'occurrence. En poussant le raisonnement jusqu'au bout, en l'appliquant à un chiffrement itéré, de fonction de ronde f, constitué de k tours et utilisant des blocs de m bits, nous pouvons décrire l'algorithme idéal d'une cryptanalyse G-différentielle. On note alors « (M, M') » un couple de messages clairs et « $C_1, \ldots, C_{k-1}, C_k$ » les chiffrés de M en sortie de chacune des k rondes *i.e.* $C_1 = f(M, K_1)$ et pour $i = 2, \ldots, k$, $C_i = f(C_{i-1}, K_i)$, « K_i » désignant la sous-clef utilisée dans la $i^{ème}$ ronde. On note « $C'_1, \ldots, C'_{k-1}, C'_k$ » les chiffrés correspondants pour M'. Le principe est alors de déceler un lien statistique entre $\Delta M = \mathbf{g} \in G$ tel que $M = \mathbf{g}.M'$ et $\Delta C_{k-1} = C_{k-1} \oplus C'_{k-1}$ assez discriminant pour découvrir la sous-clef K_k du $k^{ième}$ tour.

L'attaque G-différentielle se décrit alors en quatre étapes constituant l'algorithme ci-dessous.

1. Trouver une G-différentielle $(\mathbf{g}, \beta) \in G^* \times \mathbb{F}_2^m$ au $k-1^{ième}$ tour telle que la probabilité
$$\Pr(\Delta \mathbf{C}_{k-1} = \beta | \Delta \mathbf{M} = \mathbf{g})$$
soit très largement supérieure à l'équiprobabilité quand $\mathbf{M}$ est une variable aléatoire uniformément distribuée ;
2. Choisir aléatoirement un texte chiffré M et soumettre M et $\mathbf{g}.M$ au chiffrement. On obtient alors deux couples clairs-chiffrés (M, C_k) et $(M' = \mathbf{g}.M, C'_k)$;
3. Déterminer toutes les valeurs possibles K'_k de la dernière sous-clef telles que $f^{-1}_{K'_k}(M) \oplus f^{-1}_{K'_k}(M') = \beta$;
4. Itérer les étapes 3. et 4. jusqu'à ce que l'une des valeurs de K'_k apparaisse plus souvent que les autres. On considérera alors cette valeur comme étant effectivement la sous-clef de la $k^{ième}$ ronde.

Un nouvel indice nous laisse à penser que la réalisation concrète d'une telle cryptanalyse est proche d'être effectuée. En effet très récemment avec Cyril Prissette de l'Université du Sud Toulon-Var nous avons découvert une structure remarquable dans les boîtes-S du DES dont les critères de construction ne sont encore de nos jours que partiellement connus. Soit une $S : \mathbb{F}_2^6 \to \mathbb{F}_2^4$ l'une quelconque des huit boîtes-S du DES. Alors on peut construire une involution sans point fixe *ad hoc* $\boldsymbol{\sigma}_S \in S(\mathbb{F}_2^6)$ telle que pour tout $x \in \mathbb{F}_2^6$ on ait
$$S(x) \oplus S(\boldsymbol{\sigma}_S(x)) = (0, 0, 0, 0)$$
c'est-à-dire que la différence en sortie de S pour des messages clairs qui ne diffèrent que par l'application d'une certaine permutation $\boldsymbol{\sigma}_S$ est toujours nulle.

Enfin la caractérisation duale de la G-non linéarité parfaite est quant à elle susceptible d'être exploitée dans une attaque G-linéaire dérivée de l'attaque classique correspondante.

Annexe A

Table des notations

Notation	Signification	Page
$H(\mathbf{X})$	Entropie de la variable aléatoire $\mathbf{X}$	12
$H(\mathbf{X}\|\mathbf{Y})$	Entropie conditionnelle de $\mathbf{X}$ sachant $\mathbf{Y}$	12
π_f	Permutation de Feistel associée à la fonction f	17
$\Lambda(S)$	Complexité linéaire de la suite S	26
$\stackrel{déf.}{=}$	Egalité par définition	36
Y^X	Ensemble des applications de X dans Y	39
$f\|_A$	Restriction d'une fonction f à un sous-ensemble A	39
$S(X)$	Groupe des bijections (symétrique) de l'ensemble X (fini)	40
A^c	Complémentaire ensembliste de A	40
Id_X	Application identité de l'ensemble X	40
$\mathbf{1}_A$	Fonction indicatrice d'une partie A	40
$\|X\|$	Cardinal de l'ensemble fini X	40
min	Minimum	40
max	Maximum	40
$\|x\|$	Valeur absolue d'un nombre réel x	41
$\|\mathtt{z}\|$	Module d'un nombre complexe $\mathtt{z}$	41
$\overline{\mathtt{z}}$	Conjugué d'un nombre complexe $\mathtt{z}$	41
e_G	Elément neutre du groupe G	41
G^*	Le groupe G privé de son élément neutre	41
$Aut(G)$	Groupe des automorphismes de groupe de G	41
ker	Noyau d'un homomorphisme	41
$\langle x \rangle$	Sous-groupe engendré par x	41
σ_α	Translation par α	41
$T(G)$	Groupe des translations de G	41
$\dim_{\mathbb{K}}(V)$	Dimension du $\mathbb{K}$-espace vectoriel V	42
$\mathcal{L}(V,W)$	Ensemble des applications linéaires de V dans W	42
$End(V)$	Ensemble des endomorphismes de V	42
$GL(V)$	Groupe linéaire de V	42
λ^*	Application linéaire adjointe de λ	42

Notation	Signification	Page
$V \oplus W$	Somme directe d'espaces vectoriels	42
$A^{\perp}$	Orthogonal de l'ensemble A	42
l_{α}	Forme linéaire	42
$\mathbb{Z}_m$	Anneau d'entiers modulo m	42
$\mathbb{Z}_m^{\times}$	Groupe des entiers inversibles	42
$Aut(\mathbb{K})$	Groupe des automorphismes (de corps) du corps $\mathbb{K}$	43
$\mathbb{F}_m$	Corps fini à m éléments	42
$[\mathbb{F} : \mathbb{K}]$	Degré de l'extension (finie) de $\mathbb{F}$ sur $\mathbb{K}$	43
τ_{α}	Translation multiplicative par α	43
$\oplus$	Addition dans l'espace $\mathbb{F}_2^m$ et le corps $\mathbb{F}_{2^m}$	46
$e^{(i)}$	Elément de la base canonique de $\mathbb{F}_2^m$	46
d_H	Distance de Hamming	47
w_H	Poids de Hamming	47
$\overline{x}$	Complémentaire booléen	47
Φ_B	Plongement de $\mathbb{F}_2^m$ dans $\mathbb{F}_{2^m}$	47
Θ_m^d	Ecriture d'un entier en base deux	47
$\overline{f}$	Négation de la fonction f	48
S_f	Support de la fonction f	48
P_f	Forme algébrique normale (FAN) de f	50
$\underset{\sim}{f}$	Transformée de Möbius de f	50
$\deg(f)$	Degré algébrique de f	51
$R(k,m)$	Code de Reed-Muller d'ordre k de $\mathbb{F}_2^m$	51
$tr_{\mathbb{F}/\mathbb{K}}$	Trace de $\mathbb{F}$ sur $\mathbb{K}$	52
tr	Trace absolue	52 et 102
$\langle \varphi, \psi \rangle$	Produit scalaire	53 et 103
$\widehat{\varphi}$	Transformée de Fourier de φ	53 et 104
Φ_F	Application transformée de Fourier	53, 104 et 178
$*$	Produit de convolution	56 et 105
φ_f	Compteur de pré-images de f	59 et 107
$\Pr^{(m)}$	Mesure de probabilité uniforme de $\mathbb{F}_2^m$	61
I_k	Ensemble des parties de $I = \{1, \ldots, m\}$ de cardinal k	62
N_f	Non linearité de f	65
$\| \varphi \|_{\infty}$	Norme du max de la fonction φ	65
$\rho(1,m)$	Rayon de recouvrement de $R(1,m)$	66
$d_{\alpha} f$	Dérivée de f suivant α	67 et 106
$GA(\mathbb{F}_2^m)$	Ensemble des fonctions affines bijectives	68
V_f^{SL}	Ensemble des structures linéaires de f	68
$PC(n)$	Critère de propagation de degré n	69
SL_m	Fonctions de $\mathbb{F}_2^{\mathbb{F}_2^m}$ ayant une structure linéaire non nulle	70
L_f	Distance de linéarité de f	70
$\Delta_f(\alpha, \beta)$	$\{x \in G \mid d_{\alpha} f(x) = \beta\}$	75
P_f	Probabilité de non linéarité de f	75
$k_f(\alpha, \beta)$	$\lvert\{x \in \mathbb{F}_2^m \mid \alpha.x \oplus \beta.f(x) = 0\}\rvert - 2^{m-1}$	77
R_f	Résistance à la cryptanalyse linéaire de f	77
$\tilde{f}$	Fonction courbe duale de f	81
$\mathcal{B}_m$	Ensemble des fonctions courbes de $\mathbb{F}_2^{\mathbb{F}_2^m}$	81
$\otimes$	Produit tensoriel de fonctions	83

Notation	Signification	Page
$q^{(m)}$	Fonction quadratique courbe canonique	91
$\mathcal{Q}_m$	Ensemble des fonctions quadratiques courbes	91
$\widehat{G}$	Dual de G	101 et 176
$exp(G)$	Exposant du groupe G	101
$\mathbb{U}_m$	Groupe des racines $m^{ièmes}$ de l'unité dans $\mathbb{C}$	101
ω_m	Racine primitive $m^{ième}$ de l'unité $\mathsf{e}^{\frac{2\imath\pi}{m}}$ dans $\mathbb{C}$	101
χ_G^α	Caractère du groupe G	102
$\mathbb{U}$	Ensemble des nombres complexes de module 1	105
$\Pr^{(G)}$	Mesure de probabilité uniforme de G	106
$\mathcal{B}_G$	Ensemble des fonctions de $\mathbb{U}^G$ courbes	110
$\pi^{(n)}$	Permutation $x \mapsto x^n$	119
$G^{(puiss)}$	Ensemble des permutations puissances	119
$\mathbf{g}.x$	Action de groupe évaluée en $(\mathbf{g}, x)$	132
$\mathcal{O}_G(x)$	Orbite de x sous l'action de G	133
ϕ_x	Application orbitale de x	133
X/G	Ensemble des orbites	133
σ_α^g	Translation à gauche par α	135
σ_α^d	Translation à droite par α	135
$\Im_\alpha$	Automorphisme intérieur de conjugaison par α	135
$X^{(k)}$	Ensemble des k-uplets ordonnés de X	138
$GA(\mathbb{K})$	Groupe des droites affines de $\mathbb{K}$	138
$\delta_{\alpha,\beta}$	Droite affine $x \mapsto \alpha x + \beta$	138
$D_{\mathbf{g}}f$	Dérivée de f suivant $\mathbf{g}$	141
$\bigstar$	G-produit de convolution	143
f_x	Fonction $f \circ \phi_x$	145
tr	Trace des applications linéaires	172
ρ_i	Représentation irréductible	176
λ_F	Fonction coordonnée de la transformée de Fourier	178
$\widehat{\varphi}^G$	Transformée de Fourier de φ au sens des représentations	178
$d_\alpha^g f$	Dérivée à gauche de f suivant α	181
$d_\alpha^d f$	Dérivée à droite de f suivant α	181
$\|\ .\ \|$	Norme basée sur tr	184
$[x, y]$	Commutant de x et y	191
$\mathfrak{T}_{(i,\ j)}$	Transposition associant i et j	205
$Inv(X)$	Ensemble des involutions sans point fixe de X	206

Annexe B

Fonctions booléennes courbes au sens des involutions sans point fixe

Donnez-moi un point fixe et un levier et je soulèverai la Terre.

ARCHIMÈDE, *De l'équilibre des plans*

Sommaire

Préambule

Une étude spécifique et complète de la non linéarité parfaite généralisée (cf. chapitre 7) dans le cadre booléen au sens d'une action régulière par involution sans point fixe est présentée ici. La quasi totalité des résultats exposés étant tirés de [PH04], cette annexe est essentiellement une traduction en langue française du contenu, légèrement remanié et substantiellement complété, de cet article. En outre puisqu'il s'agit d'un cas particulier des travaux exposés au chapitre 7, nous supposons connus les résultats qui y sont énoncés et nous y faisons souvent référence. L'intérêt fondamental de cette annexe est l'étude des involutions sans point fixe qui y est effectuée et particulièrement l'exposé des propriétés de ce type de permutations dont certaines ont déjà été utilisées au chapitre 7.

B.1 Introduction

Considérez une photographie sur film et son négatif. Ils représentent tous deux la même image, seulement, dans le second nommé, les valeurs des tons sont inversées. Cette situation métaphorique se transpose à l'identique dans le contexte des fonctions booléennes parfaitement non

linéaires et courbes. A une nuance près, ces deux notions sont identiques.

D'un côté donc, les fonctions exhibant la meilleure résistance à la cryptanalyse différentielle qui vérifient les conditions

$$\forall \alpha \in \mathbb{F}_2^{m\,*},\ \forall \beta \in \mathbb{F}_2^n,\ |\{x \in \mathbb{F}_2^m | f(x \oplus \alpha) \oplus f(x) = \beta\}| = 2^{m-n} \tag{B.1}$$

où f est une fonction de $\mathbb{F}_2^m$ dans $\mathbb{F}_2^n$.

D'un autre côté, les fonctions maximalement résistantes contre l'attaque linéaire, définies via leur transformée de Fourier (ou plus rigoureusement de Walsh) par

$$\forall \beta \in \mathbb{F}_2^{n\,*},\ \forall \alpha \in \mathbb{F}_2^m,\ \widehat{\chi_{\mathbb{F}_2^n}^{\beta} \circ f}(\alpha) = \pm 2^{\frac{m}{2}}\ .$$

Ces deux notions sont donc rigoureusement équivalentes, duales l'une de l'autre par la transformée de Fourier.

Maintenant soit σ_α la translation par α de $\mathbb{F}_2^m$. On peut naturellement ré-écrire la formule (B.1)

$$\forall \alpha \in \mathbb{F}_2^{m\,*},\ \forall \beta \in \mathbb{F}_2^n,\ |\{x \in \mathbb{F}_2^m | f(\sigma_\alpha(x)) \oplus f(x) = \beta\}| = 2^{m-n}\ .$$

Ainsi le concept de non linéarité parfaite est indubitablement lié à l'action par translation de $\mathbb{F}_2^m$ sur lui-même. Or ces translations sont un cas très particulier de permutations. Ce sont en effet des involutions sans point fixe. Il existe donc une manière naturelle d'étendre, en même temps, la notion de non linéarité parfaite et, par dualité, celle de fonction courbe. Supposons que G soit un groupe dont tous les éléments, le neutre mis à part, soient des involutions sans point fixe de $\mathbb{F}_2^m$ et agissant régulièrement sur $\mathbb{F}_2^m$. Alors, dans cette annexe, sont étudiées les fonctions $f : \mathbb{F}_2^m \to \mathbb{F}_2^n$ satisfaisant

$$\forall \boldsymbol{\sigma} \in G^*,\ \forall \beta \in \mathbb{F}_2^n,\ |\{x \in \mathbb{F}_2^m | f(\boldsymbol{\sigma}(x)) \oplus f(x) = \beta\}| = 2^{m-n}\ .$$

Evidemment cette approche n'est qu'un cas particulier de celle exposée au chapitre 7 concernant la non linéarité parfaite basée sur une action régulière de groupe fini abélien. Toutefois la notion évoquée ici présente quelques particularités intéressantes à relever.

Organisation de l'annexe

Dans la section suivante certaines propriétés de base des classes de conjugaison dans le groupe symétrique sont rappelées. Des définitions et des résultats sur les involutions sans point fixe sont par la suite exposés dans la section B.3. Puis dans la section B.4, nous donnons les principaux résultats concernant la notion de G-non linéarité parfaite pour G un groupe dit *maximal d'involutions sans point fixe*. Ces mêmes résultats sont utilisés afin d'interpréter les fonctions hyper-courbes dans ce nouveau contexte (section B.5). Finalement la section B.6 est dévolue à l'étude de la distance des fonctions booléennes G-parfaitement non linéaires à un certain ensemble d'applications « affines », permettant d'établir un résultat identique à celui concernant les fonctions courbes originales.

B.2 Classes de conjugaison du groupe symétrique

Nous rappelons ici plusieurs propositions sans en donner les démonstrations : le lecteur pourra consulter son cours d'algèbre général favori (voir aussi le livre [Rau00] par exemple).

Soient m un entier strictement positif et $I \stackrel{déf.}{=} \{1, \ldots, m\}$. Soient $n \in \mathbb{N}^*$ tel que $n \leq m$ et $(i_1, \ldots, i_n) \in I^{(n)}$ *i.e.* $(i_1, \ldots, i_n) \in I^n$ tel que $\forall (j,k) \in \{1, \ldots, n\}^2$, $j \neq k$, on a $i_j \neq i_k$. Soit l'élément $\pi \in S(I)$ défini par $\pi(i_k) = i_{k+1}$ pour $1 \leq k < n$, $\pi(i_n) = i_1$ et $\pi(i) = i$ pour tout $i \in I \setminus \{i_1, \ldots, i_n\}$. Alors π est un *cycle* de *support* $\{i_1, \ldots, i_n\}$. L'entier n est la *longueur* du cycle. On pourra noter qu'un cycle de longueur 1 est en fait l'identité de I. Une *transposition* $\mathfrak{T}$ est un cycle de longueur 2 *i.e.* il existe deux éléments $i \neq j$ dans I tels que $\mathfrak{T}(i) = j$, $\mathfrak{T}(j) = i$ et $\mathfrak{T}(k) = k$ si $k \in I \setminus \{i, j\}$. On note « $\mathfrak{T}_{(i,\ j)}$ » la transposition $\mathfrak{T}$.

Proposition B.1. *Soit $\pi \in S(I)$. Alors il existe des cycles $\pi_1, \ldots, \pi_n$ uniques dans $S(I)$ tels que l'ensemble de leurs supports constitue une partition de I et $\pi = \pi_1 \circ \ldots \circ \pi_n$. En d'autres termes, toute permutation se décompose en un produit de cycles à supports disjoints et cette décomposition est unique à l'ordre près d'apparition des cycles. On dit que les π_j sont les* cycles de la permutation π *et que l'écriture $\pi = \pi_1 \circ \ldots \circ \pi_n$ est la* décomposition de π en cycles *(on remarque par ailleurs que les π_j commutent entre eux).*

Dans la décomposition de π en cycles on peut évidemment omettre les cycles π_j qui sont égaux à Id_I, *i.e.* ceux dont le support est réduit à un singleton. Dans ce cas on obtient une décomposition de π comme produit de cycles non triviaux de supports deux à deux disjoints.

Proposition B.2. *Pour tout $\pi \in S(I)$ et $j \in I$ on note « $k_j(\pi)$ » le nombre de cycles de longueur j de π. On a donc $m = \sum_{j=1}^{m} j k_j(\pi)$.*

Alors deux éléments π et π' de $S(I)$ sont conjugués (voir définition 7.9) si et seulement si $k_j(\pi) = k_j(\pi')$ pour tout $j \in I$.

Corollaire B.1. *Le nombre de classes de conjugaison du groupe $S(I)$ est égal au nombre de* partitions *de l'entier m, i.e. au nombre de façons d'écrire m comme $m = \sum_{k=1}^{n} m_k$ avec $0 < m_n \leq \ldots \leq m_2 \leq m_1$ (une telle partition est identifiée au n-uplet d'entiers $(m_1, \ldots, m_n)$).*

Proposition B.3. *Soit $x = (m_1, \ldots, m_n)$ une partition de l'entier m et pour tout $j \in I$, soit $k_j(x)$ le nombre de termes m_i égaux à j. Alors le cardinal de la classe de conjugaison correspondant à x (i.e. la classe de conjugaison dont les éléments π vérifient $k_j(\pi) = k_j(x)$ pour tout $j \in I$) est*

$$\frac{m!}{\prod_{j=1}^{m} k_j(x)! j^{k_j(x)}} .$$

Une classe de conjugaison regroupe donc les permutations de même *forme*.

Remarquons que toutes ces propriétés restent vraies lorsque l'on remplace $S(I)$ par $S(X)$ avec X un ensemble non vide de cardinal fini puisque $S(X)$ et $S(\{1, \ldots, |X|\})$ sont alors isomorphes.

B.3 Involutions sans point fixe

Dans cette section sont exposés un certain nombre de résultats généraux au sujet des involutions sans point fixe.

Définition B.1. Soit X un ensemble fini non vide. Un élément $\boldsymbol{\sigma} \in S(X)$ est une involution sans point fixe de X si

1. $\boldsymbol{\sigma}$ est *involutive i.e.* $\boldsymbol{\sigma}^2 = Id_X$ ou de manière équivalente $\boldsymbol{\sigma}^{-1} = \boldsymbol{\sigma}$;
2. $\boldsymbol{\sigma}$ *est sans point fixe i.e.* $\forall x \in X$, $\boldsymbol{\sigma}(x) \neq x$.

Remarquons immédiatement que pour que de telles involutions sans point fixe existent il est nécessaire que $|X| > 1$. Dans la suite on supposera toujours vraie cette condition minimale. On se donne donc X un ensemble fini tel que $|X| > 1$.

Proposition B.4. *Une permutation $\boldsymbol{\sigma} \in S(X)$ est une involution sans point fixe si et seulement si sa décomposition en cycles est constituée d'exactement $\frac{|X|}{2}$ transpositions à supports disjoints.*

Preuve. Démontrons tout d'abord l'implication directe. Le groupe engendré par $\boldsymbol{\sigma}$ vérifie $\langle \boldsymbol{\sigma} \rangle = \{Id_X, \boldsymbol{\sigma}\}$ (puisque $\boldsymbol{\sigma}$ est une involution sans point fixe). Pour tout $x \in X$, l'orbite de x sous l'action de $\langle \boldsymbol{\sigma} \rangle$ est alors $\boldsymbol{\mathcal{O}}_{\langle \boldsymbol{\sigma} \rangle}(x) = \{x, \boldsymbol{\sigma}(x)\}$ et $|\boldsymbol{\mathcal{O}}_{\langle \boldsymbol{\sigma} \rangle}(x)| = 2$. Donc l'ensemble des orbites $X/\langle \boldsymbol{\sigma} \rangle$ est une partition de X en $\frac{|X|}{2}$ sous-ensembles chacun de cardinal 2. Soit $A \subset X$ contenant exactement un et un seul représentant de chacune des orbites. Par définition de A, $\forall (x, y) \in A^2$ tel que $x \neq y$, $\mathfrak{T}_{(x,\ \boldsymbol{\sigma}(x))} \neq \mathfrak{T}_{(y,\ \boldsymbol{\sigma}(y))}$ et plus précisément leurs supports sont disjoints. Il y a donc $\frac{|X|}{2}$ telles transpositions à supports disjoints. Enfin $\boldsymbol{\sigma}$ s'écrit comme la composition de ces transpositions puisque $\forall x \in A$, $\boldsymbol{\sigma}|_{\boldsymbol{\mathcal{O}}_{\langle \boldsymbol{\sigma} \rangle}(x)} = \mathfrak{T}_{(x,\ \boldsymbol{\sigma}(x))}$.

Réciproquement, supposons que $\boldsymbol{\sigma} = \mathfrak{T}_1 \circ \ldots \circ \mathfrak{T}_{\frac{|X|}{2}}$ où les $\mathfrak{T}_i$ sont des transpositions à supports disjoints. Soit $x \in X$ alors $\exists\ !\ i \in \{1, \ldots, \frac{|X|}{2}\}$ tel que x appartienne au support de $\mathfrak{T}_i$. Alors $\boldsymbol{\sigma}(x) = \mathfrak{T}_i(x) \neq x$ et $\boldsymbol{\sigma}^2(x) = \mathfrak{T}_i^2(x) = x$. D'où l'on déduit que $\boldsymbol{\sigma}$ est une involution sans point fixe. □

Corollaire B.2. *L'ensemble des involutions sans point fixe de X forme une classe de conjugaison de $S(X)$. Plus précisément, il s'agit de la classe de conjugaison associée à la partition $\underbrace{(2, \ldots, 2)}_{\frac{|X|}{2}\ fois}$ de l'entier $|X|$.*

Preuve. D'après les propositions B.4 et B.2, il est évident que l'ensemble des involutions forme une classe de conjugaison de $S(X)$. Puisque par ailleurs la décomposition en cycles d'une involution sans point fixe est constituée de $\frac{|X|}{2}$ transpositions, on en déduit immédiatement le second point. □

On note « $Inv(X)$ » la classe de conjugaison dans $S(X)$ des involutions sans point fixe de X. D'après la proposition B.3 et le corollaire précédent, on a

$$|Inv(X)| = \frac{|X|!}{\frac{|X|}{2}! 2^{\frac{|X|}{2}}} .$$

Exemple B.1. Soient $X = \mathbb{F}_2^m$ et $\alpha \in \mathbb{F}_2^{m*}$. Alors la translation σ_α par α est une involution sans point fixe de $\mathbb{F}_2^m$. Puisque pour $m > 2$, $|Inv(\mathbb{F}_2^m)| = \frac{2^m!}{2^{m-1}! 2^{2^{m-1}}} > |T(\mathbb{F}_2^m)| = 2^m$, il existe de nombreuses involutions sans point fixe non affines. Remarquons que l'on peut calculer directement le nombre d'involutions sans point fixe de $\mathbb{F}_2^m$. Rappelons la définition des coefficients binomiaux $C_n^k = \frac{n!}{k!(n-k)!}$ représentant le nombre de sous-ensembles de cardinal k d'un ensemble de cardinal n et, en particulier, $C_n^n = 1$. Pour construire une involution sans point fixe de $\mathbb{F}_2^m$ il faut choisir 2^{m-1} sous-ensembles de 2 éléments, tous deux à deux d'intersection vide. Ces ensembles correspondent aux orbites.

- En ce qui concerne le premier ensemble on a $C_{2^m}^2$ possibilités de choix. On choisit donc $\{x_1, x_2\}$ parmi ces $C_{2^m}^2$ possibilités ;

- Pour le second, on doit choisir un sous-ensemble de $\mathbb{F}_2^m$ à 2 éléments qui ne contienne ni x_1 ni x_2 on a donc $C^2_{2^m-2}$ possibilités ;
- Pour le troisième on a $C^2_{2^m-4}$ possibilités ;
- Pour le $n^{ième}$ (avec $n \leq 2^{m-1}$), en raisonnant de la même manière, on a $C^2_{2^m-2(n-1)}$ choix possibles ;
- Pour le $(2^{m-1})^{ième}$ il reste donc $C^2_{2^m-2^m+2} = C^2_2 = 1$ choix possible.

Finalement on a $\prod_{k=1}^{2^{m-1}} C^2_{2^m-2(k-1)} = \frac{2^m!}{2 \times (2^m-2)!} \times \frac{(2^m-2)!}{2 \times (2^m-4)!} \times \ldots \times \frac{4!}{2 \times 2} \times \frac{2}{2} = \frac{2^m!}{2^{2^{m-1}}}$ manières distinctes de prendre 2^{m-1} sous-ensembles de cardinal 2 tous deux à deux d'intersection vide. Comme l'ordre ne compte pas dans la décomposition en cycles, il faut diviser ce nombre par le nombre de permutations possibles de ces 2^{m-1} parties, à savoir $2^{m-1}!$. Il en résulte que l'on (re-)trouve $|Inv(\mathbb{F}_2^m)| = \frac{2^m!}{2^{m-1}! 2^{2^{m-1}}}$.

Remarquons que $|Inv(\mathbb{F}_2^m)| = \frac{2^m!}{2^{2^{m-1}}} \times \frac{1}{|S(\mathbb{F}_2^{m-1})|} \in \mathbb{N}^*$ pour $m > 1$. Puisque l'on a aussi $\frac{2^m!}{2^{2^{m-1}}} \in \mathbb{N}^*$, il en résulte que $|Inv(\mathbb{F}_2^m)| \geq |S(\mathbb{F}_2^{m-1})|$. Comme par ailleurs $\forall m > 2$, $|S(\mathbb{F}_2^{m-1})| > |2^m|$, on vérifie bien que $\forall m > 2$, $|Inv(\mathbb{F}_2^m)| > |T(\mathbb{F}_2^m)| = 2^m$.

Les involutions sans point fixe peuvent s'organiser en groupes. Certaines propriétés de tels groupes sont maintenant énoncées.

Définition B.2. Soit G un sous-groupe de $S(X)$. G est appelé *groupe d'involutions sans point fixe* (ou plus simplement *groupe d'involutions*) de X si $G^* \subset Inv(X)$.

Exemple B.2. Soit $X = \mathbb{F}_2^m$. On peut vérifier que $T(\mathbb{F}_2^m)^* \subset Inv(\mathbb{F}_2^m)$ et donc $T(\mathbb{F}_2^m)$ est un groupe d'involutions de $\mathbb{F}_2^m$.

Proposition B.5. *Soit G un sous-groupe de $S(X)$ qui soit un groupe d'involutions de X. Alors G est abélien.*

Preuve. Soit $(\boldsymbol{\sigma}, \boldsymbol{\tau}) \in G^2$. Puisque $\boldsymbol{\sigma} \circ \boldsymbol{\tau} \in G$ alors on a soit $\boldsymbol{\sigma} \circ \boldsymbol{\tau} = Id_X$, soit $\boldsymbol{\sigma} \circ \boldsymbol{\tau} \in Inv(X)$. Dans le premier cas, $\boldsymbol{\sigma} = \boldsymbol{\tau}^{-1} = \boldsymbol{\tau}$ et donc $\boldsymbol{\sigma} \circ \boldsymbol{\tau} = \boldsymbol{\sigma}^2 = \boldsymbol{\tau} \circ \boldsymbol{\sigma}$. Dans le second cas, $(\boldsymbol{\sigma} \circ \boldsymbol{\tau})^2 = Id_X \Leftrightarrow \boldsymbol{\sigma} \circ \boldsymbol{\tau} \circ \boldsymbol{\sigma} \circ \boldsymbol{\tau} = Id_X \Leftrightarrow \boldsymbol{\tau} \circ \boldsymbol{\sigma} \circ \boldsymbol{\tau} = \boldsymbol{\sigma}^{-1} = \boldsymbol{\sigma} \Leftrightarrow \boldsymbol{\sigma} \circ \boldsymbol{\tau} = \boldsymbol{\tau}^{-1} \circ \boldsymbol{\sigma} = \boldsymbol{\tau} \circ \boldsymbol{\sigma}$. La proposition s'ensuit. □

Proposition B.6. *Si G est un groupe d'involutions de X alors $|G| \leq |X|$.*

Preuve. Raisonnons par contradiction et supposons que $|G| > |X|$.
Soit $x_0 \in X$ fixé. On peut montrer qu'il existe $(\boldsymbol{\sigma}, \boldsymbol{\tau}) \in G^2$ tel que $\boldsymbol{\sigma} \neq \boldsymbol{\tau}$ et $\boldsymbol{\sigma}(x_0) = \boldsymbol{\tau}(x_0)$. Si ce n'était pas le cas alors l'application orbitale ϕ_{x_0} de x_0 serait injective et donc $|\phi_{x_0}(G)| = |\boldsymbol{\mathcal{O}}_G(x_0)| = |G| \leq |X|$ ce qui est impossible par hypothèse.
Soit donc $(\boldsymbol{\sigma}, \boldsymbol{\tau}) \in G^2$ tel que $\boldsymbol{\sigma} \neq \boldsymbol{\tau}$ et $\boldsymbol{\sigma}(x_0) = \boldsymbol{\tau}(x_0)$. Alors $\boldsymbol{\sigma} \circ \boldsymbol{\tau}(x_0) = \boldsymbol{\sigma} \circ \boldsymbol{\sigma}(x_0) = \boldsymbol{\sigma}^2(x_0) = x_0$. Par conséquent x_0 est un point fixe de $\boldsymbol{\sigma} \circ \boldsymbol{\tau}$. Puisque $\boldsymbol{\sigma} \neq \boldsymbol{\tau}$, $\boldsymbol{\sigma} \circ \boldsymbol{\tau} \neq Id_X$ et comme G est un groupe d'involutions sans point fixe, $\boldsymbol{\sigma} \circ \boldsymbol{\tau}$ n'a pas de point fixe. Ainsi on obtient une contradiction avec l'hypothèse que $|G| > |X|$. □

Corollaire B.3. *Soit G un groupe d'involutions (sans point fixe) d'un ensemble fini X. Alors son groupe dual $\widehat{G}$, isomorphe à G, est l'ensemble des homomorphismes de groupes de G dans $\mathbb{U}_2 = \{\pm 1\}$. En particulier les caractères de G sont à valeurs réelles.*

Preuve. D'une part on sait que G est un groupe fini (son cardinal est inférieur ou égal à $|X|$). D'autre part il est abélien. Il en résulte que $\widehat{G}$ est isomorphe à G et que $\forall \chi \in \widehat{G}$, χ est un homomorphisme de groupes de G dans $\mathbb{U}_{exp(G)}$. Or tous les éléments de G, hormis bien entendu l'identité Id_X, sont par définition d'ordre 2, donc $exp(G) = 2$ et $\mathbb{U}_{exp(G)} = \mathbb{U}_2 = \{\pm 1\}$. Ils sont donc tous à valeurs réelles. □

Proposition B.7. *Pour $m > 2$, il existe un groupe d'involutions (sans point fixe) G de $\mathbb{F}_2^m$ tel que $|G| = 2^m$ et $G \neq T(\mathbb{F}_2^m)$.*

Preuve. Si $m = 1$ ou $m = 2$ nous avons seulement un groupe d'involutions de cardinal maximum 2 ou 4 à savoir $T(\mathbb{F}_2)$ et $T(\mathbb{F}_2^2)$. Plus précisément on a $Inv(\mathbb{F}_2) \subset T(\mathbb{F}_2)$ et $Inv(\mathbb{F}_2^2) \subset T(\mathbb{F}_2^2)$. Plaçons-nous donc sous l'hypothèse que $m > 2$. Dans ce cas (voir exemple B.1) il existe des involutions sans point fixe qui ne sont pas des translations. Soient $\alpha \in \mathbb{F}_2^{m\,*}$ et $\sigma_\alpha \in T(\mathbb{F}_2^m)$ la translation correspondante (en particulier $\sigma_\alpha \neq Id_{\mathbb{F}_2^m}$). Soit $\boldsymbol{\tau} \in Inv(\mathbb{F}_2^m) \setminus T(\mathbb{F}_2^m)$. Puisque $\boldsymbol{\tau}$ et σ_α sont conjugués dans $S(\mathbb{F}_2^m)$ il existe $\pi \in S(\mathbb{F}_2^m)$ tel que $\boldsymbol{\tau} = \Im_\pi(\sigma_\alpha) = \pi \circ \sigma_\alpha \circ \pi^{-1}$. Il est facile de voir que le groupe $\pi \circ T(\mathbb{F}_2^m) \circ \pi^{-1}$ conjugué par π de $T(\mathbb{F}_2^m)$ est lui-même un groupe d'involutions (sans point fixe) tel que $|\pi \circ T(\mathbb{F}_2^m) \circ \pi^{-1}| = 2^m$ et $\pi \circ T(\mathbb{F}_2^m) \circ \pi^{-1} \neq T(\mathbb{F}_2^m)$ (puisque $\boldsymbol{\tau} \in \pi \circ T(\mathbb{F}_2^m) \circ \pi^{-1}$ et $\boldsymbol{\tau} \notin T(\mathbb{F}_2^m)$). □

Définition B.3. Un groupe d'involutions (sans point fixe) G d'un ensemble fini X tel que $|G| = |X|$ est appelé *groupe maximal d'involutions* de X.

Exemple B.3.

1. Le groupe des translations $T(\mathbb{F}_2^m)$ est un groupe maximal d'involutions de $\mathbb{F}_2^m$;
2. Tous les groupes conjugués de $T(\mathbb{F}_2^m)$ *i.e.* les groupes $\pi \circ T(\mathbb{F}_2^m) \circ \pi^{-1}$ pour $\pi \in S(\mathbb{F}_2^m)$ sont des groupes maximaux d'involutions de $\mathbb{F}_2^m$.

Proposition B.8. *Soit G un groupe maximal d'involutions d'un ensemble fini X. L'action ϕ de G sur X, naturellement définie par l'injection canonique de G dans $S(X)$, est régulière.*

Preuve. On considère pour $x \in X$ fixé, la fonction orbitale ϕ_x de x et on montre qu'elle est bijective de G dans X.
Soit $(\boldsymbol{\sigma}, \boldsymbol{\tau}) \in G^2$ tel que $\boldsymbol{\sigma} \neq \boldsymbol{\tau}$. Si $\phi_x(\boldsymbol{\sigma}) = \phi_x(\boldsymbol{\tau})$ alors on a la chaîne d'équivalences suivante qui conduit à une contradiction :

$$\boldsymbol{\sigma}(x) = \boldsymbol{\tau}(x) \Leftrightarrow \boldsymbol{\tau} \circ \boldsymbol{\sigma}(x) = x \Leftrightarrow x \text{ est un point fixe de } \boldsymbol{\tau} \circ \boldsymbol{\sigma}$$

chose impossible puisque $\boldsymbol{\tau} \circ \boldsymbol{\sigma} \neq Id_X$. Il en résulte ainsi que ϕ_x est injective. Puisque par ailleurs $|G| = |X|$, on en déduit que ϕ_x est bijective. Cela étant vrai pour n'importe quel $x \in X$, l'action de G sur X est régulière. □

B.4 Non linéarité parfaite par rapport à un groupe d'involutions de $\mathbb{F}_2^m$

Soit G un groupe maximal d'involutions sans point fixe de $\mathbb{F}_2^m$. L'objectif de cette section est l'étude des fonctions de $\mathbb{F}_2^m$ dans $\mathbb{F}_2^n$ qui sont G-parfaitement non linéaires. Puisque G agit régulièrement sur $\mathbb{F}_2^m$, les résultats de la section 7.4 et plus particulièrement ceux du paragraphe 7.4.5.2 p. 153 du chapitre 7 restent valides. En outre nous disposons de la proposition suivante permettant de caractériser toutes les fonctions G-parfaitement non linéaires de $\mathbb{F}_2^{m\,\mathbb{F}_2^m}$.

Proposition B.9. *La classe de conjugaison du groupe des translations $T(\mathbb{F}_2^m)$ est égale à l'ensemble des groupes maximaux d'involutions sans point fixe de $\mathbb{F}_2^m$.*

Preuve. Si G est un groupe conjugué de $\mathbb{F}_2^m$, il est évidemment isomorphe à $T(\mathbb{F}_2^m)$. Supposons maintenant que G soit un groupe maximal d'involutions sans point fixe de $\mathbb{F}_2^m$. Alors G est un groupe abélien, de cardinal 2^m dont tous les éléments, hormis $Id_{\mathbb{F}_2^m}$, sont d'ordre 2 (*i.e.* G est un groupe abélien 2-élémentaire), il est donc isomorphe à $\mathbb{F}_2^m$ et à $T(\mathbb{F}_2^m)$. Il en résulte que l'ensemble des sous-groupes de $S(\mathbb{F}_2^m)$ qui sont isomorphes à $T(\mathbb{F}_2^m)$ est égal à l'ensemble des groupes maximaux d'involutions sans point fixe de $\mathbb{F}_2^m$. Par application du corollaire 7.5 on en déduit immédiatement le résultat. □

Il est désormais clair que les fonctions G-parfaitement non linéaires de $\mathbb{F}_2^m$ dans $\mathbb{F}_2^n$ n'admettent qu'une forme bien précise.

Proposition B.10. *Soit $f : \mathbb{F}_2^m \to \mathbb{F}_2^n$. La fonction f est G-parfaitement non linéaire si et seulement s'il existe $\pi \in S(\mathbb{F}_2^m)$ tel que $G = \pi \circ T(\mathbb{F}_2^m) \circ \pi^{-1}$ et tel que $f \circ \pi : \mathbb{F}_2^m \to \mathbb{F}_2^n$ soit courbe (au sens classique).*

Preuve. Puisque G est un groupe maximal d'involutions sans point fixe de $\mathbb{F}_2^m$, il s'agit en particulier d'un groupe conjugué de $T(\mathbb{F}_2^m)$ (d'après la proposition précédente). Il existe donc $\pi \in S(\mathbb{F}_2^m)$ tel que $G = \pi \circ T(\mathbb{F}_2^m) \circ \pi^{-1}$. Par la proposition 7.15 (chapitre 7), la fonction f est G-parfaitement non linéaire si et seulement si $f \circ \pi : \mathbb{F}_2^m \to \mathbb{F}_2^n$ est parfaitement non linéaire au sens classique ce qui revient à dire que $f \circ \pi$ est (boolénne) courbe. □

Puisque, pour G un groupe d'involutions sans point fixe, si une fonction $f : \mathbb{F}_2^m \to \mathbb{F}_2^n$ est G-parfaitement non linéaire alors à une composition par une permutation près, elle est aussi courbe au sens classique, les conditions d'existence de telles fonctions sont les mêmes que celles énoncées dans le cadre traditionnel (voir la proposition 5.3 p. 78).

Corollaire B.4. *Pour tout groupe d'involutions sans point fixe G de $\mathbb{F}_2^m$, les fonctions G-parfaitement non linéaires de $\mathbb{F}_2^{n\,\mathbb{F}_2^m}$ n'existent que si $m \geq 2n$ et m est pair.*

Preuve. Le résultat est évident d'après le corollaire précédent et par application de la proposition 5.3. □

B.5 Lien avec les fonctions hyper-courbes

On rappelle (voir la sous-section 6.7.4 du chapitre 6) qu'une fonction $f : \mathbb{F}_{2^m} \to \mathbb{F}_2$ est hyper-courbe si pour tout $n \in \{1, \ldots, 2^m - 1\}$ tel que $pgcd(n, 2^m - 1) = 1$ et pour tout $\alpha \in \mathbb{F}_{2^m}$,

$$\sum_{x \in \mathbb{F}_{2^m}} (-1)^{f(x^n)} (-1)^{tr(\alpha x)} = \pm 2^{\frac{m}{2}}$$

i.e. $\forall n \in \mathbb{Z}_{2^m-1}^{\times}$, $f \circ \pi^{(n)}$ est courbe[1] au sens d'Ambrosimov (cf. chapitre 6).

Soit B une base du $\mathbb{F}_2$-espace vectoriel de $\mathbb{F}_2^m$. Pour $n \in \mathbb{Z}_{2^m-1}^{\times}$, $\Phi_B \circ \pi^{(n)} \circ \Phi_B^{-1} \in S(\mathbb{F}_2^n)$ (où Φ_B est l'isomorphisme d'espaces vectoriels de $\mathbb{F}_{2^m}$ dans $\mathbb{F}_2^n$ défini p. 47). On définit alors $\pi^{(n)\prime} \stackrel{déf.}{=} \Phi_B \circ \pi^{(n)} \circ \Phi_B^{-1}$. On a en particulier $(\pi^{(n)\prime})^{-1} = \Phi_B \circ \pi^{(n)^{-1}} \circ \Phi_B^{-1}$. Enfin on pose $G_{\pi^{(n)\prime}} \stackrel{déf.}{=} \Im_{\pi^{(n)\prime}}(T(\mathbb{F}_2^m)) = \pi^{(n)\prime} \circ T(\mathbb{F}_2^m) \circ (\pi^{(n)\prime})^{-1}$.

Théorème B.1. *Soit $f : \mathbb{F}_{2^m} \to \mathbb{F}_2$. La fonction f est hyper-courbe si et seulement si la fonction $f \circ \Phi_B^{-1} : \mathbb{F}_2^m \to \mathbb{F}_2$ est $G_{\pi^{(n)\prime}}$-parfaitement non linéaire pour tout $n \in \mathbb{Z}_{2^m-1}^{\times}$.*

Preuve. La fonction f est hyper-courbe
$\Leftrightarrow \forall n \in \mathbb{Z}_{2^m-1}^{\times}$, $f \circ \pi^{(n)}$ est courbe au sens d'Ambrosimov
$\Leftrightarrow \forall n \in \mathbb{Z}_{2^m-1}^{\times}$, $f \circ \pi^{(n)} \circ \Phi_B^{-1}$ est courbe au sens classique (cf. proposition 6.14)
$\Leftrightarrow \forall n \in \mathbb{Z}_{2^m-1}^{\times}$, $f \circ \Phi_B^{-1} \circ \Phi_B \circ \pi^{(n)} \circ \Phi_B^{-1}$ est courbe au sens classique
$\Leftrightarrow \forall n \in \mathbb{Z}_{2^m-1}^{\times}$, $f \circ \Phi_B^{-1} \circ \pi^{(n)\prime}$ est courbe au sens classique
$\Leftrightarrow \forall n \in \mathbb{Z}_{2^m-1}^{\times}$, $f \circ \Phi_B^{-1}$ est $G_{\pi^{(n)\prime}}$-parfaitement non linéaire (d'après la propostion B.10). □

[1] Rappelons que $\pi^{(n)} \in S(\mathbb{F}_{2^m})$ et vérifie $\pi^{(n)} : x \mapsto x^n$.

B.6 Distance à l'ensemble des fonctions « affines »

On a vu au chapitre 5 que les fonctions booléennes courbes possèdent une distance maximum à l'ensemble des fonctions affines (code de Reed-Muller d'ordre 1). Dans cette section nous montrons un résultat similaire. Les fonctions courbes au sens de leur définition généralisée atteignent la plus grande distance par rapport à un certain type de fonctions affines.

Soit G un groupe maximal d'involutions de $\mathbb{F}_2^m$. On définit l'ensemble des fonctions *G-affines* par

$$\begin{aligned} T(\mathbb{U}_2)(\widehat{G}) &\stackrel{déf.}{=} \{\varphi : G \to \{\pm 1\} | \exists (\chi, x) \in \widehat{G} \times \{\pm 1\} \text{ tel que } \varphi = \sigma_x \circ \chi\} \\ &= \{\pm \chi_G^{\boldsymbol{\sigma}} \in \mathbb{R}^G | \boldsymbol{\sigma} \in G\} \end{aligned}$$

i.e. $T(\mathbb{U}_2)(\widehat{G})$ est l'ensemble des translatés des caractères de G par les translations σ_1 et σ_{-1} du groupe multiplicatif $\mathbb{U}_2 = \{\pm 1\}$.

Soit $(\beta, x) \in {\mathbb{F}_2^m}^* \times \mathbb{F}_2^m$. Nous avons pour $f : \mathbb{F}_2^m \to \mathbb{F}_2^n$,

$$\begin{aligned} \widehat{\chi_{\mathbb{F}_2^n}^{\beta} \circ f_x}(\boldsymbol{\sigma}) &= \sum_{\boldsymbol{\tau} \in G} \chi_{\mathbb{F}_2^n}^{\beta}(f(\boldsymbol{\tau}(x))) \chi_G^{\boldsymbol{\sigma}}(\boldsymbol{\tau}) \\ &= |\{\boldsymbol{\tau} \in G | \chi_{\mathbb{F}_2^n}^{\beta}(f(\boldsymbol{\tau}(x))) = \chi_G^{\boldsymbol{\sigma}}(\boldsymbol{\tau})\}| - |\{\boldsymbol{\tau} \in G | \chi_{\mathbb{F}_2^n}^{\beta}(f(\boldsymbol{\tau}(x))) \neq \chi_G^{\boldsymbol{\sigma}}(\boldsymbol{\tau})\}| \\ &\quad \text{(puisque } \chi_{\mathbb{F}_2^n}^{\beta} \text{ et } \chi_G^{\boldsymbol{\sigma}} \text{ sont tous deux à valeurs dans } \{\pm 1\}) \\ &= |G| - 2 d_H(\chi_{\mathbb{F}_2^n}^{\beta} \circ f_x, \chi_G^{\boldsymbol{\sigma}}) \ . \end{aligned}$$

Ainsi nous obtenons

$$d_H(\chi_{\mathbb{F}_2^n}^{\beta} \circ f_x, \chi_G^{\boldsymbol{\sigma}}) = 2^{m-1} - \frac{1}{2} \widehat{\chi_{\mathbb{F}_2^n}^{\beta} \circ f_x}(\boldsymbol{\sigma}) \ .$$

Calculons $d_H(\chi_{\mathbb{F}_2^n}^{\beta} \circ f_x, -\chi_G^{\boldsymbol{\sigma}})$:

$$\begin{aligned} d_H(\chi_{\mathbb{F}_2^n}^{\beta} \circ f_x, -\chi_G^{\boldsymbol{\sigma}}) &= |\{\boldsymbol{\tau} \in G | \chi_{\mathbb{F}_2^n}^{\beta}(f(\boldsymbol{\tau}(x))) \neq -\chi_G^{\boldsymbol{\sigma}}(\boldsymbol{\tau})\}| \\ &= |\{\boldsymbol{\tau} \in G | \chi_{\mathbb{F}_2^n}^{\beta}(f(\boldsymbol{\tau}(x))) = \chi_G^{\boldsymbol{\sigma}}(\boldsymbol{\tau})\}| \\ &= |G| - |\{\boldsymbol{\tau} \in G | \chi_{\mathbb{F}_2^n}^{\beta}(f(\boldsymbol{\tau}(x))) \neq \chi_G^{\boldsymbol{\sigma}}(\boldsymbol{\tau})\}| \\ &= |G| - d_H(\chi_{\mathbb{F}_2^n}^{\beta} \circ f_x, \chi_G^{\boldsymbol{\sigma}}) \\ &= 2^{m-1} + \frac{1}{2} \widehat{\chi_{\mathbb{F}_2^n}^{\beta} \circ f_x}(\boldsymbol{\sigma}) \ . \end{aligned}$$

Il s'ensuit que $d_H(\chi_{\mathbb{F}_2^n}^{\beta} \circ f_x, \{\pm \chi_G^{\boldsymbol{\sigma}}\}) = \min\{d_H(\chi_{\mathbb{F}_2^n}^{\beta} \circ f_x, \chi_G^{\boldsymbol{\sigma}}), d_H(\chi_{\mathbb{F}_2^n}^{\beta} \circ f_x, -\chi_G^{\boldsymbol{\sigma}})\} = 2^{m-1} - \frac{1}{2} |\widehat{\chi_{\mathbb{F}_2^n}^{\beta} \circ f_x}(\boldsymbol{\sigma})|$.

Puisque $T(\mathbb{U}_2)(\widehat{G}) = \bigcup_{\boldsymbol{\sigma} \in G} \{\pm \chi_G^{\boldsymbol{\sigma}}\}$, nous avons

$$\begin{aligned} d_H(\chi_{\mathbb{F}_2^n}^{\beta} \circ f_x, T(\mathbb{U}_2)(\widehat{G})) &= \min_{\varphi \in T(\mathbb{U}_2)(\widehat{G})} d_H(\chi_{\mathbb{F}_2^n}^{\beta} \circ f_x, \varphi) \\ &= \min_{\boldsymbol{\sigma} \in G} d_H(\chi_{\mathbb{F}_2^n}^{\beta} \circ f_x, \{\pm \chi_G^{\boldsymbol{\sigma}}\}) \\ &= \min_{\boldsymbol{\sigma} \in G} (2^{m-1} - \frac{1}{2} |\widehat{\chi_{\mathbb{F}_2^n}^{\beta} \circ f_x}(\boldsymbol{\sigma})|) \\ &= 2^{m-1} - \frac{1}{2} \max_{\boldsymbol{\sigma} \in G} |\widehat{\chi_{\mathbb{F}_2^n}^{\beta} \circ f_x}(\boldsymbol{\sigma})| \ . \end{aligned} \tag{B.2}$$

Proposition B.11. *Soient G un groupe maximal d'involutions de $\mathbb{F}_2^m$ et $f : \mathbb{F}_2^m \to \mathbb{F}_2^n$. La fonction f est G-parfaitement non linéaire si et seulement si $\exists x \in \mathbb{F}_2^m$ tel que $\forall \beta \in {\mathbb{F}_2^n}^*$,*

$$d_H(\chi^{\beta}_{\mathbb{F}_2^n} \circ f_x, T(\mathbb{U}_2)(\widehat{G})) = 2^{m-1} - 2^{\frac{m}{2}-1} \ .$$

Preuve.

⇐) Soient $g : \mathbb{F}_2^m \to \mathbb{F}_2^n$, $\beta \in {\mathbb{F}_2^n}^*$ et $x \in \mathbb{F}_2^m$. D'après la relation de Parseval nous avons $\sum_{\boldsymbol{\sigma} \in G} |\widehat{\chi^{\beta}_{\mathbb{F}_2^n} \circ g_x}(\boldsymbol{\sigma})|^2 = |G| \sum_{\boldsymbol{\sigma} \in G} |\chi^{\beta}_{\mathbb{F}_2^n} \circ g_x(\boldsymbol{\sigma})|^2 = |G|^2$ (puisque $\chi^{\beta}_{\mathbb{F}_2^n}$ est à valeurs dans $\{\pm 1\}$). Ainsi $\max_{\boldsymbol{\sigma} \in G} |\widehat{\chi^{\beta}_{\mathbb{F}_2^n} \circ g_x}(\boldsymbol{\sigma})| \geq \sqrt{|G|} = 2^{\frac{m}{2}}$ et alors $\min_{g:\mathbb{F}_2^m \to \mathbb{F}_2^n} \max_{\boldsymbol{\sigma} \in G} |\widehat{\chi^{\beta}_{\mathbb{F}_2^n} \circ g_x}(\boldsymbol{\sigma})| \geq 2^{\frac{m}{2}}$. Comme on suppose qu'il existe $x \in \mathbb{F}_2^m$ tel que pour tout $\beta \in {\mathbb{F}_2^n}^*$ on ait $d_H(\chi^{\beta}_{\mathbb{F}_2^n} \circ f_x, T(\mathbb{U}_2)(\widehat{G})) = 2^{m-1} - 2^{\frac{m}{2}-1}$, alors d'après la formule (B.2), on en déduit que $\forall \beta \in {\mathbb{F}_2^n}^*$, $\max_{\boldsymbol{\sigma} \in G} |\widehat{\chi^{\beta}_{\mathbb{F}_2^n} \circ f_x}(\boldsymbol{\sigma})| = 2^{\frac{m}{2}}$. Alors $\forall \boldsymbol{\sigma} \in G$, $|\widehat{\chi^{\beta}_{\mathbb{F}_2^n} \circ f_x}(\boldsymbol{\sigma})| \leq 2^{\frac{m}{2}}$. La borne inférieure absolue exhibée précédemment implique alors que $\forall \boldsymbol{\sigma} \in G$, $|\widehat{\chi^{\beta}_{\mathbb{F}_2^n} \circ f_x}(\boldsymbol{\sigma})| = 2^{\frac{m}{2}}$. Le résultat est donc donné par le corollaire 7.3 (p. 150).

⇒) Par le corollaire 7.3, si f est G-parfaitement non linéaire alors $\exists x \in \mathbb{F}_2^m$ tel que $\forall \beta \in {\mathbb{F}_2^n}^*$ et $\forall \boldsymbol{\sigma} \in G$, $|\widehat{\chi^{\beta}_{\mathbb{F}_2^n} \circ f_x}(\boldsymbol{\sigma})| = 2^{\frac{m}{2}}$. D'où le résultat en appliquant la formule (B.2).

□

Corollaire B.5. *Soit G un groupe maximal d'involutions de $\mathbb{F}_2^m$. Soit $f : \mathbb{F}_2^m \to \mathbb{F}_2^n$. Si f est G-parfaitement non linéaire alors $\forall (\beta, x) \in {\mathbb{F}_2^n}^* \times \mathbb{F}_2^m$, $\chi^{\beta}_{\mathbb{F}_2^n} \circ f_x$ vérifie $d_H(\chi^{\beta}_{\mathbb{F}_2^n} \circ f_x, T(\mathbb{U}_2)(\widehat{G})) = \max_{g:\mathbb{F}_2^n \to \mathbb{F}_2^n} d_H(\chi^{\beta}_{\mathbb{F}_2^n} \circ g_x, T(\mathbb{U}_2)(\widehat{G}))$.*

Preuve. Supposons que f soit G-parfaitement non linéaire alors $\forall x \in \mathbb{F}_2^m$, $\forall \beta \in {\mathbb{F}_2^n}^*$ et $\forall \boldsymbol{\sigma} \in \mathbb{F}_2^m$, $|\chi^{\beta}_{\mathbb{F}_2^n} \circ f_x(\boldsymbol{\sigma})| = 2^{\frac{m}{2}}$. Comme dans la démonstration de la proposition précédente on a $|\widehat{\chi^{\beta}_{\mathbb{F}_2^n} \circ f_x}(\boldsymbol{\sigma})| = \min_{g:\mathbb{F}_2^m \to \mathbb{F}_2^n} \max_{\boldsymbol{\sigma} \in G} |\widehat{\chi^{\beta}_{\mathbb{F}_2^n} \circ g_x}(\boldsymbol{\sigma})| = 2^{\frac{m}{2}}$. Alors $\forall g : \mathbb{F}_2^m \to \mathbb{F}_2^n$, d'après la formule (B.2), $d_H(\chi^{\beta}_{\mathbb{F}_2^n} \circ f_x, T(\mathbb{U}_2)(\widehat{G})) \geq 2^{m-1} - \frac{1}{2} \max_{\boldsymbol{\sigma} \in G} |\widehat{\chi^{\beta}_{\mathbb{F}_2^n} \circ g_x}(\boldsymbol{\sigma})| = d_H(\chi^{\beta}_{\mathbb{F}_2^n} \circ g_x, T(\mathbb{U}_2)(\widehat{G}))$. □

B.7 Conclusion

Dans cette annexe a été étudiée une instanciation concrète du concept de non linéarité parfaite basée sur une action de groupe régulière (voir le chapitre 7). En effet, dans le cadre booléen, les translations sont des involutions sans point fixe. Ainsi une généralisation naturelle revient à remplacer l'action par translation par une action basée sur ce type d'involutions. Les groupes agissant considérés sont les *groupes maximaux d'involutions* et dans leur action sur $\mathbb{F}_2^m$ ils sont réguliers.

Ces groupes G d'involutions sont en fait tous conjugués du groupe des translations $T(\mathbb{F}_2^m)$. Il en résulte naturellement que les fonctions G-parfaitement non linéaires se trouvent être, à une composition par une permutation près, des fonctions classiquement courbes. Ce résultat nous permet en outre d'interpréter la notion de fonction hyper-courbe via le concept de G-non linéarité parfaite. Finalement, en considérant le translaté par $\mathbb{U}_2$ du dual d'un groupe maximal d'involutions G, il est possible de caractériser les fonctions G-parfaitement non linéaires par leur distance à cet ensemble de fonctions « affines », à l'instar des fonctions courbes usuelles puisque cette distance est maximale.

Bibliographie

[AGH+92] N. Alon, O. Goldreich, J. Hastad, R. Peralta : Simple constructions for almost k-wise independant random variable. Dans *Journal of Random Structures and Algorithms*, vol.3, no. 3, p. 289-304, 1992

[Amb94] A. S. Ambrosimov : Properties of bent functions of q-valued logic over finite fields. Dans *Discrete Mathematics and Applications*, vol. 4, no. 4, p. 341-350, 1994

[B-AB96] I. Ben-Aroya, E. Biham : Differential cryptanalysis of Lucifer. Dans *Journal of Cryptology*, vol. 9, no. 1, p. 21-34, 1996

[BD94] T. Beth, C. Ding : On almost perfect nonlinear permutations, Dans *Advances in Cryptology - Eurocrypt '93*, vol. 765 de *Lecture Notes in Computer Science*, p. 65-76, Springer, 1994

[Ber68] E. R. Berlekamp : Algebraic coding theory. *McGraw-Hill Book Co.*, 1968

[BKR97] J. Borst, L.R. Knudsen, V. Rijmen : Two attacks on reduced IDEA. Dans *Advances in Cryptology - Eurocrypt '97*, vol. 1233 de *Lecture Notes in Computer Science*, p. 1-13, Springer, 1997

[Bou70] N. Bourbaki : Eléments de mathématique - Théorie des ensembles, Nouvelle édition, Hermann, 1970

[BS91] E. Biham, A. Shamir : Differential cryptanalysis of DES-like cryptosystems. Dans *Journal of Cryptology*, vol. 4, no. 1, p. 3-72, 1991

[BS93] E. Biham, A. Shamir : Differential cryptanalysis of the full 16-round DES. Dans *Advances in cryptology - Crypto '92*, vol. 740 de *Lecture Notes in Computer Science*, p. 487-496, Springer, 1993

[Car94] C. Carlet : Two new classes of bent functions. Dans *Advances in Cryptology - Eurocrypt '93*, vol. 765 de *Lectures Notes in Computer Science*, p. 77-101, Springer, 1994

[Car95] C. Carlet : Generalized Partial Spreads. Dans *IEEE Transactions on Information Theory*, vol. 41, no. 5, p. 1482-1487, 1995

[Car99a] C. Carlet : Recent results on bent functions. Dans *Proceedinds of the International Conference on Combinatorics, Information Theory and Statistics*, p. 275-291, 1999

[Car99b] C. Carlet : On cryptographic propagation criteria for Boolean functions. Dans *Information and Computation*, vol. 151, p. 32-56, 1999

[CC96] P. Camion, A. Canteaut : Construction of t-resilient functions over a finite alphabet. Dans *Advances in Cryptology - Eurocrypt '96*, vol. 1070 de *Lecture Notes in Computer Science*, p. 283-293, Springer, 1996

[CCC+92] P. Camion, C. Carlet, P. Charpin, N. Sendrier : On correlation-immune functions. Dans *Crypto 1991*, vol. 576 de *Lecture Notes in Computer Science*, p. 86-100, Springer, 1992

[CCC+00] A. Canteaut, C. Carlet, P. Charpin, C. Fontaine : Propagation characteristics and correlation-immunity of highly nonlinear Boolean functions. Dans *Proceedings of Eurocrypt 2000*, vol. 1807 de *Lecture Notes in Computer Science*, p. 507-522, Springer, 2000

[CD00] C. Carlet, S. Dubuc : On generalized bent and q-ary perfect nonlinear functions. Dans *D. Jungnickel, H. Niederreiter (Eds.), Finite Fields and Applications, Proceedings of Fq5*, p. 81-94, Springer, 2000

[CD04] C. Carlet, C. Ding : Highly nonlinear mappings. Dans *Journal of Complexity*, vol. 20, no. 2, p. 205-244, 2004

[CDL+03] A. Canteaut, M. Daum, G. Leander, H. Dobbertin : Normal and non normal bent functions. Dans *Proceedings of the 2003 International Workshop on Coding and Cryptography, WCC 2003*, p. 91-100, 2003

[CG98] C. Carlet, P. Guillot : An alternate characterization of the bentness of binary functions, with uniqueness. Dans *Designs, Codes and Cryptography*, vol. 14, p. 130-140, 1998

[CG04] C. Carlet, P. Gaborit : Hyper-bent functions and cyclic codes. Dans *Proceedings 2004 IEEE International Symposium on Information Theory*, p. 499, 2004.

[CK89] H. Chung, P. V. Kumar : A new general construction for generalized bent functions. Dans *IEEE Transactions on Information Theory*, vol. 35, no. 1, p. 206-209, 1989

[Cou04] N. Courtois : Feistel schemes and bi-Linear cryptanalysis. Dans *Advances in Cryptology - Crypto 2004*, vol. 3152 de *Lecture Notes in Computer Science*, p. 23-40, Springer, 2004

[CP02] N. Courtois, J. Pieprzyk : Cryptanalysis of block ciphers with overdefined systems of equations. Dans *Advances in Cryptology - Asiacrypt 2002*, vol. 2501 de *Lecture Notes in Computer Science*, p. 267-287, Springer, 2002

[CV94] F. Chabaud, S. Vaudenay : Links between differential and linear cryptanalysis. Dans *Advances in Cryptology - Eurocrypt '94*, vol. 950 de *Lecture Notes in Computer Science*, p. 356-365, Springer, 1994

[DH76] W. Diffie, E. Hellman : New directions in cryptography. Dans *IEEE Transactions on Information Theory*, vol. IT-22, no. 6, p. 644-654, 1976

[DH04] J.F. Dillon, H. Dobbertin : New cyclic difference sets with Singer parameters. Dans *Finite Fields and Applications*, p. 342-389, 2004

[DHL03] M. Daum, H. Dobbertin, G. Leander : An Algorithm for checking normality of Boolean functions. Dans *Proceedings of the 2003 International Workshop on Coding and Cryptography, WCC 2003*, p. 133-142, 2003

[Dil74] J. F. Dillon : Elementary Hadamard difference sets. Thèse de doctorat, Université du Maryland, 1974

[Dob95] H. Dobbertin : Construction of bent functions and balanced Boolean functions with high nonlinearity. Dans *Fast Software Encryption*, vol. 1008 de *Lecture Notes in Computer Science*, p. 61-74, Springer, 1995

[Dob98] H. Dobbertin : One-to-one highly nonlinear power functions with characteristic 2. Dans *Appl. Algebra Eng. Commun. Comput.*, vol. 9, p. 139-152, 1998

[Dob99a] H. Dobbertin : Almost perfect nonlinear power functions on $GF(2^n)$: the Niho case. Dans *Information and Computation*, vol. 151, p. 57-72, 1999

[Dob99b] H. Dobbertin : Almost perfect nonlinear power functions on $GF(2^n)$: the Welch case, *IEEE Transactions on Information Theory*, vol. 45, no. 4, p. 1271-1275, 1999

[DR02] J. Daemen, V. Rijmen : The design of Rijndael : AES - The Advanced Encryption Standard. *Information Security and Cryptography*, Springer, 2002

[DS94] J. A. Davis, K. Smith : A construction of difference sets in high exponent 2-groups using representation theory. Dans *Journal of Algebraic Combinatorics*, vol. 3, p. 137-151, 1994

[Eve88] J.-H. Evertse : Linear structures in blockciphers. Dans *Advances in Cryptology - Eurocrypt '87*, vol. 304 de *Lecture Notes in Computer Science*, p. 249-266, Springer, 1988

[Fei70] H. Feistel : Cryptographic coding for data-bank privacy. *Rapport technique 2827 d'IBM*, 1970

[Fei73] H. Feistel : Cryptography and computer privacy. Dans *Scientific American*, vol. 228, p. 15-23, 1973

[Gal87] J. H. Gallier : Logic for computer science - Foundations of automatic theorem proving. *John Wiley and Sons, Inc.*, 1987

[Gef73] P. R. Geffe : How to protect data with ciphers that are really hard to break. *Electronics*, vol. 46, no. 1, p. 99-101, 1973

[GGN+89] J. Y. Girard, K. Gödel, E. Nagel, J. R. Newman : Le théorème de Gödel. *Editions du Seuil*, 1989

[GN94] R. Göttfert, H. Niederreiter : On the linear complexity of products of shift-register sequences. Dans *Advances in cryptology - Eurocrypt '93*, vol. 765 de *Lecture Notes in Computer Science*, p. 151-158, Springer, 1994

[Goz97] I. Gozard : Théorie de Galois. Dans la collection *Mathématiques 2^e cycle*, Ellipses, 1997

[Gui01] P. Guillot : Completed GPS covers all bent functions. Dans *Journal of Combinatorial Theory*, Serie A, vol. 93, p. 242-266, 2001

[GW99] O. Grošek, W. Wei : Bent-like functions on groupoids. Dans *Pure Mathematics and Applications (Algebraic Systems)*, vol. 10, no. 3, p. 267-278, 1999

[HKM97] C. Harpes, G. Kramer, J. L. Massey : A Generalization of linear cryptanalysis and the applicability of Matsui's piling-up lemma. Dans *Advances in Cryptology - Eurocrypt '95*, vol. 921 de *Lecture Notes in Computer Science*, p. 13-27, Springer, 1997

[HL97] X. D. Hou, P. Langevin : Results on bent functions. *Journal of Combinatorial Theory A*, vol. 80, p. 232-246, 1997

[HM97] C. Harpes, J. L. Massey : Partitioning cryptanalysis. Dans *Fast Software Encryption*, vol. 1267 de *Lecture Notes in Computer Science*, p. 13-27, Springer, 1997

[Hou98] X.-D. Hou : q-ary bent functions constructed from chain rings. Dans *Finite Fields and their Applications*, vol. 4, p. 55-61, 1998

[Hou00] X.-D. Hou : Bent functions, partial difference sets and quasi-Frobenius local rings. Dans *Designs, Codes and Cryptography*, vol. 20, no. 3, p. 251-268, 2000

[JK97] T. Jacobsen, L. R. Knudsen : The interpolation attack on block ciphers. Dans *Fast Software Encryption*, vol. 1267 de *Lecture Notes in Computer Science*, p. 28-40, Springer, 1997

[Jun92] D. Jungnickel : Difference sets. Dans *J. Dinitz and D. R. Stinson Eds., Contemporary Design Theory : A Collection of Surveys*, John Wiley & Sons, 1992

[Ker1883] A. Kerckhoffs : La cryptographie militaire. Dans *Journal des sciences militaires*, vol. IX, p. 5-38, 1883

[Kib78] R. E. Kibler : A summary of noncyclic difference sets, $k < 20$. Dans *Journal of Combinatorial Theory A*, vol. 25, p. 62-67, 1978

[Knu95] L. Knudsen : Truncated and higher order differentials. Dans *Fast Software Encryption*, vol. 1008 de *Lecture Notes in Computer Science*, p. 196-211, Springer, 1995

[Kra93] R. Kraemer : A result on Hadamard difference sets. Dans *Journal of Combinatorial Theory*, Serie A, vol. 63, p. 1-10, 1993

[KSW85] P. V. Kumar, R. A. Scholtz, L. R. Welch : Generalized bent functions and their properties. Dans *Journal of Combinatorial Theory A*, vol. 40, p. 99-107, 1985

[Lan92] P. Langevin : On generalized bent functions. Dans *CISM Courses and Lectures*, vol. 339, p. 147-157, 1992

[LH94] S. K. Langford, M. E. Hellman : Differential-linear cryptanalysis. Dans *Advances in Cryptology - Crypto '94*, vol. 839 de *Lecture Notes in Computer Science*, p. 17-25, Springer, 1994

[LM91] X. Lai, J. L. Massey : A proposal for a new block encryption standard. Dans *Advances in Cryptology - Eurocrypt '90*, vol. 473 de *Lecture Notes in Computer Science*, p. 389-404, Springer, 1991

[LMM91] X. Lai, J. L. Massey, S. Murphy : Markov ciphers and differential cryptanalysis. Dans *Advances in Cryptology - Eurocrypt '91*, vol. 547 de *Lecture Notes in Computer Science*, p. 17-38, Springer, 1991

[LN97] R. Lidl, H. Niederreiter : Finite fields. Dans *Encyclopedia of Mathematics and its Applications*, vol. 20, Cambridge Univeristy Press, seconde édition, 1997

[LR88] M. Luby, C. Rackoff : How to construct pseudorandom permutations. Dans *SIAM Journal and Computing*, vol. 17, no. 2, p. 373-386, 1988

[LSY97] O. A. Logachev, A. A. Salnikov, V. V. Yashchenko : Bent functions on a finite Abelian group. Dans *Discrete Mathematics and Applications*, vol. 7, no. 6, p. 547-564, 1997

[Lub96] M. Luby : Pseudorandomness and cryptographic applications. Dans *Princeton Computer Science Notes*, Priceton University Press, 1996

[Luc96] S. Lucks : Faster Luby-Rackoff ciphers. Dans *Fast Software Encryption,* , vol. 1039 de *Lecture Notes in Computer Science*, p. 189-203, Springer, 1996

[LW87] G. Lachaud, J. Wolfmann : Sommes de Kloosterman, courbes elliptiques et codes cycliques en caractéristiques 2. Dans *C. R. Acad. Sci. Paris*, vol. 305, p. 881-883, 1987

[LW90] G. Lachaud, J. Wolfmann : The weights of the orthogonal of the extended quadratic binary Goppa codes. Dans *IEEE Transactions on Information Theory*, vol. 36, p. 686-692, 1990

[Mas69] J. L. Massey : Shift-register synthesis and BCH decoding. Dans *IEEE Transactions on Information Theory*, vol. IT-15, p. 122-127, 1969

[Mas88] J. L. Massey : An introduction to comtempory cryptography. Dans *IEEE proceedings*, vol.76, no. 5, p. 533-549, 1988

[Mat94] M. Matsui : Linear cryptanalysis method for DES cipher. Dans *Advances in cryptology - Eurocrypt '93*, vol. 765 de *Lecture Notes in Computer Science*, p. 386-397, Springer, 1994

[McF73] R. L. McFarland : A family of difference sets in non-cyclic groups. Dans *Journal of Combinatorial Theory*, vol. 15, p. 1-10, 1973

[McF89] R. L. McFarland : Difference sets in Abelian groups of order $4p^2$. Dans *Mitt. Math. Sem. Giessen*, vol. 192, p. 1-70, 1989

[MS89] W. Meier, O. Staffelbach : Nonlinearity criteria for cryptographic functions. Dans *Advances in cryptology - Eurocrypt '89*, vol. 434 de *Lecture Notes in Computer Science*, p. 204-213, Springer, 1989

[NBS80] National Burau of Standards : Data Encryption Standard. Federal Information Processing Standard (FIPS), Publication 46, *National Bureau of Standards, U.S. Department of Commerce*, Washington D.C., 1980

[NK93] K. Nyberg, L. Knudsen : Provable security against differential cryptanalysis. Dans *Advances in Crytpology - Crypto '92*, vol. 740 de *Lecture Notes in Computer Science*, p. 566-574, Springer, 1993

[Nyb91] K. Nyberg : Constructions of bent functions and difference sets. Dans *Advances in Cryptology - Eurocrypt '90*, vol. 473 de *Lecture Notes in Computer Science*, p. 151-160, Springer, 1991

[Nyb92] K. Nyberg : Perfect nonlinear S-boxes. Dans *Advances in Cryptology - Eurocrypt '91*, vol. 547 de *Lecture Notes in Computer Science*, p. 378-386, Springer, 1992

[Nyb94] K. Nyberg : Differentially uniform mappings for cryptography. Dans *Advances in Cryptology - Eurocrypt '93*, vol. 765 de *Lecture Notes in Computer Science*, p. 55-64, Springer, 1994

[Pas68] D. S. Passman : Permutation groups. *W. A. Benjamin, Inc.*, 1968

[Pey04] G. Peyré : L'algèbre discrète de la transformée de Fourier. Dans *Collection Mathématiques à l'Université*, Ellipses, 2004

[PD05] L. Poinsot, J. Davis : Correspondances privées, 2005

[PH04] L. Poinsot, S. Harari : Generalized Boolean bent functions. Dans *Progress in Cryptology - INDOCRYPT 2004*, vol. 3348 de *Lecture Notes in Computer Science*, p. 107-119, Springer, 2004

[PH05] L. Poinsot, S. Harari : Group actions based perfect nonlinearity. Dans *The Internation Workshop on Coding and Cryptography, WCC 2005*, p. 335-344, 2005

[Pom03] K. Pommerening : Fourier analysis of Boolean maps. A tutorial. Disponible à l'adresse *www.staff.uni-mainz.de/pommeren/Kryptologie/Bitblock/A_ Nonlin/Fourier.pdf*, 2003

[PvLvL+91] B. Preneel, W. Van Leekwijck, L. Van Linden, R. Govaerts, J. Vandewalle : Propagation characteristics of Boolean functions. Dans *Advances in Cryptology - Eurocrypt '90*, vol. 473 de *Lecture Notes in Computer Science*, p. 161-173, Springer, 1991

[PW94] O. Papini, J. Wolfmann : Algèbre discrète et code correcteurs. Dans la collection *Mathématiques & Applications* 20, Springer-Verlag, 1994

[Rau00] G. Rauch : Les groupes finis et leurs représentations. Dans la collection *Mathématiques 2^e cycle*, Ellipses, 2000

[Rot76] O. S. Rothaus : On bent functions. Dans *Journal of Combinatorial Theory A*, vol. 20, p. 300-365, 1976

[RS86] R. A. Rueppel, O. Staffelbach : Products of linear reccuring sequences with maximum complexity. Dans *Abstract of Papers : Eurocrypt '86*, p. 30-32, 1986

[RSA78] R. L. Rivest, A. Shamir, L. Adleman : A method for obtaining digital signatures and public-key cryptosystems. Dans *Comm. ACM*, vol. 21, no. 2, p. 120-126, 1978

[Sch91] L. Schwartz : Analyse II - Théorie des ensembles et topologie. Dans la *Collection Enseignements des sciences*, Hermann, 1991

[Ser66] J.-P. Serre : Représentations linéaires des groupes finis. Hermann, 1966

[Sha48] C. E. Shannon : A mathematical theory of communication. Dans *Bell System Technical Journal*, vol. 27, p. 379-423 et 623-656, 1948

[Sha49] C. E. Shannon : Communication theory of secrecy systems. Dans *Bell System Technical Journal*, vol. 28, p. 656-715, 1949

[Sie84] T. Siegenthaler : Correlation-immunity of nonlinear combining functions for cryptographic applications. Dans *IEEE Transactions on Information Theory*, vol. 30, no. 5, p. 776-780, 1984

[SK96] B. Schneier, J. Kelsey : Unbalanced Feistel networks and block-cipher design. Dans *Fast Software Encryption*, vol. 1039 de *Lecture Notes in Computer Science*, p. 121-144, Springer, 1996

[Smi95] K. W. Smith : Nonabelian Hadamard difference sets. Dans *Journal of Combinatorial Theory A*, vol. 70, p. 144-156, 1995

[Sti01] D. Stinson : Cryptographie - Théorie et pratique. Vuibert Informatique, 2001

[SZZ95] J. Seberry, X.-M. Zhang, Y. Zheng : Relationships among nonlinearity criteria. Dans *Advances in Cryptology - Eurocrypt '94*, vol. 950 de *Lecture Notes in Computer Science*, p. 376-388, Springer, 1995

[Ver26] G. Vernam : Cipher printing telegraph systems for secret wire and radio telegraph communications. Dans *J. Am. Inst. of Electrical Engineers*, vol. 45, p. 109-115, 1926

[Wie64] H. Wielandt : Finite permutation groups. Academic Press, 1964

[Wol99] J. Wolfmann : Bent functions and coding theory. Dans *A. Pott, P. V. Kumar, T. Helleseth and D. Jugnickel Eds, Difference Sets, Sequences and their Correlations Properties*, p. 393-417, Kluwer, 1999

[WT86] A. Webster, S. Tavares : On the design of S-boxes. Dans *Advances in Cryptology - Crypto '85*, vol. 218 de *Lecture Notes in Computer Science*, p. 523-534, Springer, 1986

[XM88] G.-Z. Xiao, J. Massey : A spectral characterization of correlation-immune combining functions. Dans *IEEE Transactions on Information Theory*, vol. IT 34, p. 569-571, 1988

[YG01] A. M. Youssef, G. Gong : Hyper-bent functions. Dans *Advances in Cryptology - Eurocrypt 2001*, vol. 2045 de *Lecture Notes in Computer Science*, p. 406-419, Springer, 2001

[ZM73] N. Zierler, W. H. Mills : Products of linear recurring sequences. Dans *J. Algebra*, vol. 27, p. 147-157, 1973

Résumé

Les notions de fonctions parfaitement non linéaires et courbes sont particulièrement pertinentes en cryptographie puisqu'elles formalisent les résistances maximales face aux très efficaces attaques différentielle et linéaire. Cette thèse est ainsi consacrée à l'étude de ces objets cryptographiques. Nous interprétons ces notions de manière très naturelle essentiellement en substituant les translations figurant dans la définition de la non linéarité parfaite par une action de groupe quelconque. Les propriétés de ces actions telles que la fidélité ou la régularité permettent de décliner en plusieurs variantes ce nouveau concept.
Nous développons de surcroît sa caractérisation duale à l'aide de la transformée de Fourier ce qui aboutit à la notion appropriée de fonction courbe. En particulier dans le cas d'une action de groupe non abélien, nous faisons usage de la théorie des représentations linéaires afin d'établir une version duale *matricielle*.
Nous généralisons par ailleurs selon le même principe ces objets combinatoires appelés *ensembles à différences* qui caractérisent la non linéarité parfaite des fonctions à valeurs dans $\mathbb{F}_2$. Cela nous permet d'exhiber des constructions de fonctions satisfaisant nos critères généralisés, en particulier dans ces cas où les fonctions courbes au sens classique n'existent pas.

Mots-clefs : cryptographie, fonctions parfaitement non linéaires, fonctions courbes, actions de groupe, ensembles à différences, représentations linéaires, analyse harmonique.

Abstract

Notions of perfect nonlinear and bent functions are particularly relevant in cryptography because they formalize maximal resistances against the very efficient differential and linear attacks. This thesis is then dedicated to the study of these cryptographic objects.
We naturally interpret these notions in a more abstract and theoretical framework essentially by the substitution of the translations which occur in the definition of perfect nonlinearity by any group action. The properties of these actions as fidelity and regularity allow to decline this new concept into several alternatives.
We develop as well its dual characterization using the Fourier transform that leads to an adapted notion of bentness. In particular in the case of a non Abelian group action, we use the linear representations theory to establish a dual *matrix* version.
Furthermore, following the same principle, we generalize those combinatorics objects called *difference sets* which characterize perfect nonlinearity of $\mathbb{F}_2$-valued functions. This allows us to exhibit some constructions of functions which satisfy our generalized criteria, in particular in those cases where bent functions in the usual sense do not exist.

Keywords : cryptography, perfect nonlinear functions, bent functions, group actions, difference sets, linear representations, harmonic analysis.