Habilitation à Diriger les Recherches

Les sommes de caractères et la formule de Poisson dans la théorie des codes, des séquences et des fonctions booléennes

Philippe Langevin

Université de TOULON et du VAR

mardi 19 janvier 1999

devant le jury composé de :

C. Carlet
P. Charpin
G. Lachaud
P. Liardet
V. Pless
P. Solé
J. Wolfmann

rapporteurs :

P. Delsarte, P. Liardet, P. Solé.

Les sommes de caractères et la formule de Poisson dans la théorie des codes, des séquences et des fonctions booléennes

Philippe LANGEVIN

Author address:

G.E.C.T., UNIVERSITÉ DE TOULON-VAR

Avant-Propos

Le présent mémoire d'habilitation à diriger des recherches a été rédigé pendant mon séjour au sein de l'équipe PACOM du laboratoire I3S. Guidé par la finalité de la démarche : l'encadrement doctoral, il m'a semblé judicieux de proposer un document à l'usage des chercheurs débutants dont l'objectif pédagogique principal est de familiariser le lecteur avec les sommes de caractères, en vue d'appplications dans le contexte des codes, des séquences et des fonctions booléennes. Il en résulte un document plutôt long, écrit à l'ancienne : une succession de petits faits vite lus, vite compris mais à relire tranquillement à la maison. Les problèmes proposés sont autant de points de départs vers des thèses, les plus courageux s'aventureront sur certaines conjectures...

La synthèse de mes travaux est réalisée dans l'introduction. Elle s'adresse aux lecteurs qui manqueront de temps, je pense notamment aux rapporteurs des dossiers de qualifications et aux rapporteurs des commissions de spécialistes, je leur suggère de compléter cette lecture en pêchant ça et là quelques propositions et théorèmes. Les auteurs des propositions sont clairement identifiés, un entête [x, π_λ] signifie que je suis l'auteur ou le co-auteur de l'énoncé dont les détails sont dans l'article [x].

Je remercie mes premiers lecteurs : Iwan Duursma, Pierre Liardet, Patrick Solé, Richard Turyn, Pascal Veron, et Jean-Pierre Zanotti ; cette version finalisée doit en partie à leurs remarques, commentaires et suggestions.

P. Langevin, janvier 1999, puis 2000.

Table des matières

Introduction

La ionosphère est une couche de notre atmosphère située entre 60 et 600 km d'altitude. Sous l'action du vent solaire, les molécules y sont ionisées,

cet état lui confère la propriété de réfléchir certaines ondes électromagnétiques. Cette particularité est utilisée par les radio-amateurs pour communiquer aux quatres coins de la Terre. Elle permet d'envisager la conception d'un radar capable de voir au-delà de l'horizon. Cependant, il existe une obstruction majeure à la réalisation d'un tel projet : comme la surface des océans, la ionosphère est animée d'un mouvement de houle. Pour étudier ce phénomène, Claude Goutelard , directeur du LETTI[1], a mis au point une expérience qui repose sur la remarque suivante : un rayon électromagnétique émis de la surface terrestre en direction de la ionosphère est réfléchi vers le sol. Le point d'impact dépend de l'incidence du rayon avec la couche ionosphérique. Comme la Terre n'est pas une boule parfaitement lisse, une partie de l'onde revient du point d'impact. Si nous chronométrons le temps de retour de l'onde, nous en déduisons la distance parcourue et par suite l'angle d'incidence. L'onde de retour représente une proportion extrêmement faible de l'onde de départ. Pour pouvoir la déceler sous le bruit ambiant, on dispose de deux solutions : la première est d'envoyer un signal radar très bref mais de grande puissance :une impulsion de Dirac ; la seconde un signal de faible puissance mais plus subtil, tout en étant fortement structuré, c'est-à-dire faiblement autocorrélé. Avec la deuxième technique Claude Goutelard détecte des points d'impacts à plusieurs milliers de kilomètres en éclairant le ciel avec la puissance d'une lampe de poche ! Cette extraordinaire expérience illustre une des applications possibles de mes recherches.

*

*   *

Généralement, par signal périodique de période n, on désigne aussi bien une suite périodique $(s_i)_{i\in\mathbf{Z}}$, qu'une séquence $(s_1, s_2, \ldots, s_n)$ ou encore une application $i \mapsto s(i)$ définie sur l'ensemble des entiers modulo n. La fonction d'autocorrélation d'un signal périodique s, à valeurs complexes, de période n est la fonction définie en τ par

$$s \times s(\tau) = \sum_{j=0}^{n-1} s(\tau + j)\overline{s}(j);$$

c'est le produit scalaire de la séquence s décalée de τ positions avec elle même. La fonction d'autocorrélation de s compare le signal s avec ses différents déphasages ou décalages : *shifts*. Un signal périodique dont la fonction d'autocorrélation vaut zéro pour tous les déphasages est un signal qualifié de parfait. Pour l'expérience décrite plus haut, on doit utiliser des signaux proches du signal parfait. De plus, la vitesse de propagation du signal impose des calculs en temps réel. Une opération élémentaire en

[1]Laboratoire d'étude de l'Environnement terrestre Télécommunications Télédétection et Imagerie

mode flottant, c'est-à-dire qui manipule des nombres rationnels, coûte 100 fois plus de temps qu'une opération élémentaire en mode entier. Cette différence de temps de calcul impose l'utilisation de suites binaires, c'est-à-dire à valeur dans -1 ou $+1$. En longueur 4, il existe 8 suites parfaites, par exemple la suite associée à la séquence $(+1, +1, +1, -1)$. En calculant la fonction d'autocorrélation de quelques milliards de suites tirées au hasard, on se rend compte que les signaux binaires parfaits sont probalement très rares. En fait, les seules suites parfaites connues à ce jour sont les 8 suites de longueurs 4, et R. J. Turyn [**182**] a démontré qu'il n'existe pas de suites parfaites binaires de période inférieure à 12100, sauf pour la longueur 4.

Le rôle du G.E.C.T.[2] dans cette affaire débute ici. Jacques Wolfmann commence par étudier des suites qu'il appelle *presque-parfaites*. Ce sont des suites binaires dont la fonction d'autocorrélation vaut zéro partout sauf en deux positions, nécessairement, les positions 0 et $\frac{n}{2}$. Plus particulièrement, il étudie les suites s dont la fonction d'autocorrélation vérifie :

$$s \times s(\tau) = \begin{cases} n, & \text{si } \tau \equiv 0 \pmod n\,; \\ 4-n, & \text{si } \tau \equiv \frac{n}{2} \pmod n\,; \\ 0, & \text{sinon.} \end{cases}$$

Accidentellement, la petite suite de longueur 4 est à la fois parfaite et presque-parfaite. Mais, heureusement, il existe des suites presque-parfaites de plus grande longueur. Dans l'article [**193**], Jacques Wolfmann montre, entre autres choses, que la longueur de ces suites est nécessairement un multiple de 4, de plus, ses différentes expériences numériques, menées avec le professeur Sami Harari, le conduisent à rechercher des suites d'une forme particulière satisfaisant à la configuration « miracle ». De cette manière, ils trouvent des suites presque-parfaites pour les 25 longueurs multiples de 4 et inférieures à 100, sauf pour six valeurs exceptionnelles : 32, 44, 68, 72, 80, et 92. Depuis la recherche exhaustive programmée par R. Alexis en 1988 [**4**], on sait qu'il n'existe pas de suites presque-parfaites de longueur 32. Pour les autres valeurs, on ne sait rien, et J. Wolfmann termine l'article [**193**] publié dans le journal IEEE *Transaction on Informations Theory* par deux questions : existe-t-il des suites presques parfaites pour une de ces longueurs exceptionnelles ? Comment peut-on expliquer cette configuration remarquable ?

*

* *

Nous sommes en 1991, et je viens de terminer mon article [**119**] sur les fonctions courbes généralisées qui se situe dans le prolongement des travaux de P. V. Kumar, R. A. Scholz et L. R. Welch [**109**]. Les méthodes arithmétiques que j'utilise semblent pouvoir s'appliquer à la problématique des fonctions presque-parfaites de Jacques Wolfmann. Elle repose sur l'étude qualitative du spectre de Fourier des suites. Rappelons que si u un entier, la transformée de Fourier discrète d'une suite périodique s en u, le plus souvent notée $\hat{s}(u)$, est définie par

$$\sum_{j=0}^{n-1} s(j)\zeta_n^{ju},$$

[2]Groupe d'Etude du Codage de Toulon. Laboratoire de recherche composé de deux équipes : codes et système multimedias. `http ://www.univ-tln.fr/gect/`

où ζ_n désigne la racine n-ième principale de 1. Par un calcul simple et direct, ou encore parce que la transformée du produit de corrélation de s est égal au carré du module de la transformée de Fourier, on obtient que s est presque-parfaite si et seulement si :

$$|\hat{s}(u)|^2 = \begin{cases} 4, & \text{si } u \text{ est pair ;} \\ 2n-4, & \text{sinon.} \end{cases}$$

Ce résultat sur le module de $\hat{s}(u)$ est de nature quantitative. Mais, en y regardant de plus près, on se rend compte que $\hat{s}(u)$ est une combinaison linéaire à coefficients entiers de racines n-ièmes de l'unité. L'ensemble des combinaisons linéaires à coefficients entiers de ces nombres forment un sous-anneau du corps des nombres complexes : c'est l'anneau $\mathbf{Z}[\zeta_n]$. Cette information de nature qualitative s'avère bien souvent déterminante, elle fournit une condition nécessaire d'existence de signal parfait de longueur n en termes de solvabilité, dans l'anneau $\mathbf{Z}[\zeta_n]$, de l'équation :

$$x\bar{x} = 2n - 4. \tag{1}$$

Ce genre de question est de même nature que celle soulevée par le théorème de Pythagore à propos de la mesure de la diagonale d'un carré dont le côté mesure une unité. Un argument de valuation dyadique prouve sur le champ l'irrationalité de $\sqrt{2}$. L'anneau $\mathbf{Z}[\zeta_n]$ est la fermeture intégrale de $\mathbf{Z}$ dans le n-ième corps cyclotomique, c'est un anneau de Dedekind possèdant des valuations qui permettent de traiter l'équation (1) sans plus de difficultés que précédemment. L'étude de ce type d'anneaux a commencé à la fin du siècle dernier par des mathématiciens en quête du Graal de l'arithmétique : le grand théorème de Fermat. Dans les anneaux de Dedekind, la décomposition en produit d'idéaux premiers est unique. Les critères de décompositions sont *parfaitement* maîtrisés dans les extensions galoisiennes et en particulier dans des extensions abéliennes, comme les corps cyclotomiques. Dans mon article *almost perfect functions* [**121**], je montre à l'aide de valuations $\mathcal{P}$-adiques convenables que l'équation (1) n'a pas de solutions dans chacun des anneaux $\mathbf{Z}[\zeta_{44}]$, $\mathbf{Z}[\zeta_{68}]$ et $\mathbf{Z}[\zeta_{72}]$, et donc pour ces trois valeurs il n'existe pas de suites presques parfaites. Le cas $n = 80$ résiste à toutes mes tentatives. Suivant un principe d'Archimède : « Il est plus facile de trouver la démonstration d'une proposition quand on a déjà appris d'une façon ou d'une autre qu'elle était vraie ! », j'entreprends de faire une recherche exhaustive. Les symétries du problème permettent de réduire le champ de recherche à 2^{39} séquences... Avec un tel facteur de travail et ne disposant que de compatibles PC cadencés à 16 Mhz, il faut jouer serré. J'écris un programme en assembleur minimisant les adressages, économisant le moindre cycle. La recherche est parallélisée sur 8 machines. Une dizaine de jours après [3] le verdict tombe : il n'existe pas de suite presque-parfaite de longueur 80. Dans la semaine qui suit, je comprends pourquoi et quelques jours plus tard je prouve qu'il n'existe pas de suite presque-parfaite pour les valeurs 32, 80, et 92. Je suis en mesure d'expliquer la configuration miracle via les groupes de décomposition et l'automorphisme de Frobenius. C'est avec ce travail publié dans l'article [**121**] que s'achève ma thèse de doctorat. Ces résultats sont intéressants du point de vue théorique, mais du point de vue pratique beaucoup moins : une construction d'une grande famille

[3] À l'heure où j'écris ce mémoire, un jour suffirait. C'est une conséquence de la loi empirique de Gordon Moore, co-fondateur de la société INTEL, qui dit que la vitesse de calcul des ordinateurs double tous les deux ans. En 2028, une poignée de secondes de calcul suffira en utilisant une calculette-video-montre gadget distribuée gratuitement par LA REDOUTE pour l'achat d'un pantalon à carreaux !

de séquences presque-parfaites est souhaitée... Toutes les suites presque-parfaites trouvées jusqu'alors possèdent une propriété remarquable : si n désigne la longueur de l'une d'entre elles, alors $\frac{n}{2}-1$ est une puissance d'un nombre premier ; c'est-à-dire, la cardinalité d'un corps fini. J'oriente mes recherches vers la suite de -1 et $+1$ la plus « tordue » que l'on maîtrise depuis le debut du XIX siècle : la suite des symboles quadratiques de Legendre. Après des mois de calculs laborieux, je déduis des sommes quadratiques de Gauss et des sommes exponentielles d'Eisenstein, une construction d'une classe infinie de suites presque-parfaites. Ce résultat intuitif est publié dans les actes des Journées du PRC math-info : *Construction of almost perfect sequences* [**122**]. Une généralisation à d'autres types de suites est publiée dans les actes du colloque Finite Fields and their Applications, *Some sequences with good autocorrelation properties* [**123**]. Un petit peu plus tard, en utilisant les ensembles à différences relatifs de Ray-Chaudhuri, les chercheurs A. Pott et S. Bradley [**25**] montreront que l'existence d'une séquence presque-parfaite de longueur n est équivalente à l'existence d'une matrice de conférence négacyclique de dimension $\frac{n}{2}$. Les premiers travaux sur ces matrices remontent à Cauchy, et la majorité des résultats exposés dans [**193, 121**] étaient connus[4] sous une autre forme depuis les articles [**62, 75**], de Ph. Delsarte, J.-M. Goethals et L. J. Seidel.

*

* *

Ce que je viens de décrire dans le cadre des séquences s'inscrit dans une problèmatique plus générale. Considérons un groupe fini G. La fonction d'autocorrélation d'une application f définie sur G à valeurs dans le corps des nombres complexes est :

$$f \times f(\tau) = \sum_{x \in G} f(x+\tau)\overline{f(x)}.$$

On dit que f est parfaite du point de vue de la corrélation lorsque $f \times f$ est constante *hors-phase* c'est-à-dire sur $G - \{0\}$. Ces fonctions sont liées à des objets très particuliers de la théorie combinatoire algébrique : les ensembles à différences et les configurations tactiques (designs). Si G est cyclique nous retrouvons les séquences parfaites décrites plus haut. Dans le cas où G est un p-groupe abélien élémentaire, ce sont des fonctions courbes utilisées dans certains protocoles cryptographiques. Lorsque le groupe est abélien, ce que nous supposons pour la suite, on sait construire son groupe dual $\widehat{G}$: c'est l'ensemble des homomorphismes du groupe G dans le groupe des unités du corps des nombres complexes. Un élément χ de $\widehat{G}$ s'appelle un caractère de G. Les caractères de G forment une base orthogonale de l'espace des applications de G dans le corps des nombres complexes. Plus précisément, ils satisfont des *relations d'orthogonalité*, pour tout sous-groupe S de G :

$$\sum_{s \in S} \chi(s) = \begin{cases} |S|, & \text{si } \chi \in S^{\perp}, \\ 0, & \text{sinon}; \end{cases} \tag{2}$$

où $S^{\perp}$ est le sous-groupe de $\widehat{G}$ formé des caractères *orthogonaux* à S i.e. $\chi(s) = 1$. La transformée de Fourier de f en un caractère χ est :

$$\widehat{f}(\chi) = \sum_{g \in G} f(g)\chi(g).$$

[4]Moralité ? En matière de publications, et d'idées nouvelles, il faut rester prudent !

C'est une *somme de caractères*, on dit aussi *somme d'exponentielles*, ou encore *somme trigonométrique* parce que ce sont des sommes de racines de l'unité ! La transformée de Fourier trivialise le produit de convolution : c'est un morphisme de l'algèbre de groupe $\mathbf{C}[G]$ dans $\mathbf{C}^{\widehat{G}}$ l'algèbre des applications complexes définie sur $\widehat{G}$. En particulier, une fonction est parfaite si et seulement si le module de sa transformée de Fourier reste constant partout (et vaut $\sqrt{|G|}$ si f est à valeurs dans le cercle unité). Les relations d'orthogonalité offrent une méthode de dénombrement que j'appelle la *méthode des caractères*, pour un ensemble quelconque X et pour une fonction $f \in G^X$, le nombre de solutions $Z(f)$ de l'équation $f(x) = 0$ est donné par la somme de caractères

$$Z(f) = \frac{1}{|G|} \sum_{x \in X} \sum_{\chi \in \widehat{G}} \chi(f(x)) \tag{3}$$

Les nouveaux venus dans le monde des sommes de caractères resteront perplexes devant cette formule. Je les laisse méditer... Pour une application concrète et sans technique, je suggère la lecture de ma toute première publication *On the covering radius of RM(1,9) into RM(3,9)* [**117**] qui illustre de façon élémentaire l'intérêt de cette approche lorsqu'elle est combinée à la formule de Poisson et au théorème d'Ax. Dans cette article, je démontre que le degré de non-linéarité d'une fonction booléenne de degré au plus 3 est au moins 240.

*

* *

Le fameux théorème d'Ax qui nous renseigne sur la divisibilité du nombre des zéros d'un polynôme en fonction de son degré fut la motivation de mes premières années de recherches. Mon objectif fut d'en comprendre la démonstration, pour en déduire des conséquences aux problèmes de la théorie de l'information. Malgré une formation mathématique standard, mes connaissances initiales sur les équations algébriques et en arithmétique étaient proche de zéro ; Heureusement, nous disposons d'ouvrages de très bonnes qualités en Français : *Variétés Algébriques* de J. R. Joly [**101**] et *Théorie Algébrique des Nombres* de P. Samuel [**164**] dont les seules lectures suffisent à comprendre correctement la preuve du théorème d'Ax. Pour les applications, c'est différent. Le passage obligé par les sommes de caractères fut long et difficile. Les mauvais choix de notations, les tours de passe-passe semblent être le lot courant des utilisateurs de sommes trigonométriques. Finalement, cette discipline apparaît hermétique, et pas du tout attrayante. En fait, dans ce domaine, il n'y a ni astuce et ni hasard : seulement des groupes ! Pour rendre les calculs sur les sommes exponentielles compréhensibles il faut avoir le soucis de la concision et de l'élégance. La notion d'orthogonalité et la formule de Poisson sont des arguments clairs et simplificateurs. Dans cette voie, je me suis permis de reprendre des travaux anciens sur les codes cycliques. Le fait de remplacer les indices numériques « muets » par des variables « expressives », en faisant apparaître des sous-groupes et leurs duaux, donne une sémantique aux expressions calculatoires. Tout cela permet de voir plus clair et d'aller plus loin. Par exemple, après une brève étude des sommes de Gauss et d'Eisenstein dans le cadre des algèbres semi-simples, on réalise que les formules de McEliece concernant les poids des codes cycliques irréductibles sont valables pour les codes cycliques et même pour les codes abéliens. Cette généralisation d'un résultat de Niederreiter apparaît dans l'article *Weight of Abelian Codes* [**129**] dont le point de départ est une description « trace » des codes abéliens. Par définition, un code abélien C est un idéal d'une algèbre de groupe $K[G]$, si l'annulateur de C est dans le socle de $K[G]$ alors l'algèbre $A := k[G]/\mathrm{ann}(C)$ est semi-simple et le code est l'image de l'*encodeur*

$$\begin{aligned} \mu_{G,A} \colon A &\longrightarrow K[G] \\ a &\longrightarrow \textstyle\sum_{g\in G} \mathrm{tr}_{A/K}(ag)g^{-1} \end{aligned} \tag{4}$$

Le calcul du poids du mot μ_{GA} dépend du nombre $N(a, G, A, K)$ de solutions dans G de l'équation $\mathrm{tr}_{A/K}(ax) = 0$: c'est le cardinal d'une « section hyperplane ». Pour simplifier, supposons a inversible. La méthode de dénombrement par les caractères, fondée sur les relations d'orthogonalité conduit à l'expression

$$N(a, G, A, K) = \frac{1}{|G|} \sum_{\chi \in G^{\perp}} \sum_{\mathrm{tr}_{A/K}(ax)=0} \chi(x) \tag{5}$$

La somme interne est une *somme d'Eisenstein*, une application directe de la formule de Poisson conduit à une expression de $N(a, G, A, K)$ en termes de *sommes de Gauss*

$$N(a, G, A, K) = \frac{n}{q} + \frac{n(q-1)}{q|A^{\times}|} \sum_{\chi \in (GK^{\times})^{\perp}} G_A(\chi, \mu_A)\bar{\chi}(a) \tag{6}$$

L'objectif pédagogique de ce mémoire est de familiariser le lecteur avec la théorie des sommes de caractères en vue d'applications à la théorie des codes correcteurs, des séquences, et des fonctions booléennes. La plupart des formules liées aux sommes de caractères que l'on rencontrera dans ces domaines se déduisent de la fameuse formule de Poisson. Le document est découpé en six chapitres. Normalement, il inclut tous mes résultats, plus quelques morceaux choisis avec comme Leitmotiv la formule de Poisson. Il est écrit à l'ancienne : une succession de faits vite lus, vite compris qui donneront matière à reflexion. Les apprentis chercheurs en quête d'un sujet trouveront peut-être leur bonheur parmi les questions, problèmes et conjectures qui terminent la plupart des sections. Les trois premiers chapitres contiennent des aspects plutôt théoriques et les trois derniers des applications. Pour faire court, et parce que les bons ouvrages d'arithmétiques ne manquent pas, j'ai decidé de ne donner aucune définition arithmétique [5]. Aux deux ouvrages déjà signalés, on peut ajouter *Algebraic Number Theory* de K. Ireland et M. Rosen [**100**] qui est plus complet, et le trés précieux *Corps Locaux* de J.-P. Serre [**171**] pour les aspects locaux et complets. Indépendamment de la difficulté, j'ai choisi de rédiger quelques démonstrations pour leur caractère instructif. Certaines sont très connues, d'autres moins et peut-être inédites. Comprendre ces démonstrations est, à mon avis, une étape obligée avant d'envisager l'obtention de nouveaux résultats dans ces domaines.

ANALYSE DE FOURIER

Soit A un anneau fini commutatif. Par définition, le *degré de non-linéarité* ou la non-linéarité d'une application définie sur A^m à valeurs dans A est égale à sa distance au module des applications affines. La non-linéarité maximale d'une application est

[5] En combinatoire algébrique, comme dans tous les domaines, il est très difficile de produire un résultat nouveau. Dans cet univers pas toujours très bien balisé, le manque d'intuition peut de temps en temps être compenser par quelques connaissances en arithmétique et/ou théorie des groupes

égal au *rayon de recouvrement* du code de Reed-Muller affine qu'on note $\rho_A(m)$. Une fonction *hautement non-linéaire* est une application de non-linéarité maximale. Dans ma thèse, je dis qu'un caractère du groupe additif de A est *non-dégénéré* si son noyau ne contient qu'un seul idéal : l'idéal (0), et je donne l'estimation

$$\rho_A(m) \leq (q-1)q^{m-1} - \frac{\sqrt{n(A)}}{q(q-1)} q^{\frac{m}{2}} \tag{7}$$

où q désigne le cardinal de A et $n(A)$ le nombre de ses caractères non-dégénérés. Depuis, j'ai retrouvé cette notion dans les articles de Claasen et Goldbach [**48**] (caractère admissible [6]) et dans ceux de Wood [**196**] (caractère générateur). Le groupe $\widehat{A}$ devient un A-module en posant $a.\chi(x) = \chi_a(x) = \chi(ax)$. Un caractère χ est non-dégénéré si et seulement si l'homomorphisme $a \mapsto \chi_a$ est un isomorphisme et dans ce cas, A est un anneau *quasi-Frobenius*. Plus généralement, dans un A-module libre les notions de dualités linéaires et algébriques sont isomorphes ce qui permet d'étudier leurs sous-modules sans plus de complications que pour les espaces vectoriels. La généralisation du théorème d'extension de MacWilliams par J. Wood illustre parfaitement ce propos. La démonstration de la proposition principale de la section (19) sur le groupe d'automorphismes d'un code abélien est un autre exemple de résultat « caractériel » qui généralise celui de J. P. Zanotti [**200**].

Un anneau possède une structure additive A^+ donc des *caractères additifs* et une structure multiplicative $A^\times$ donc des *caractères multiplicatifs*. La transformée de Fourier d'un caractère additif ψ en un caractère multiplicatif χ est une *somme de Gauss*

$$G_A(\chi, \psi) = \sum_{a \in A^\times} \chi(a)\psi(a).$$

C'est une somme complète, les sommes incomplètes sont obtenues en sommant sur un sous-groupe de $A^\times$. Dans le cas quasi-Frobenius, le module d'une somme complète est assez facile à déterminer, et par la formule de Poisson, on en déduit une estimation du module d'une somme de Gauss incomplète, voir le rapport de recherche *somme de Gauss sur un anneau local* [**127**]. Dans le chapitre I, *Analyse de Fourier*, les caractères ne sont pas nécessairement à valeurs dans le corps des nombres complexes. Un anneau A est un *anneau de représentation* de G s'il est de caractéristique première avec l'ordre de G et si $A^\times$ contient un sous-groupe cyclique d'ordre $\exp(G)$. Dans cette situation, la transformée de Fourier est un isomorphisme de l'anneau de groupe $A[G]$ sur l'anneau $A^{\widehat{G}}$ qui fournit la structure des codes abéliens. Les notations proposées « crochet de dualité » ne sont pas très usuelles, c'est un mélange de celles utilisées par P. Camion [**33**], Ph. Delsarte [**57**] et de celles du *Basic Number Theory* de A. Weil [**191**]. Mis à part quelques aspects algorithmiques, les notions rappelées sont très utiles pour la lecture de tous mes articles.

SOMMES DE GAUSS

Les sommes de Gauss concentrent toutes les difficultés relatives à la résolution des équations algébriques. Abandonnons momentanément le point de vue trop général des anneaux, pour nous placer dans le cas des corps finis. Dans le calcul du cardinal

[6] C'est tellement pénible d'écrire « dégénéré » en TeX que j'adopte cette terminologie pour la suite !

de la section hyperplane rencontré plus haut (6), remplaçons A par une extension L de K.

$$N(a, G, L, K) = \frac{n}{q} + \frac{n(q-1)}{q|L^\times|} \sum_{\chi \in (GK^\times)^\perp} G_L(\chi, \mu_L)\bar{\chi}(a) \tag{8}$$

La connaissance de toutes les sommes de Gauss $G_L(\chi, \mu_L)$, $\chi \in (GK^\times)^\perp$ donne la distribution des cardinaux des sections hyperplanes et donc des poids du code cyclique irréductible encodé par l'encodeur $\mu_{L,G}$ (4). Pour chaque entier m premier avec p, résoudre le problème des sommes de Gauss d'ordre m c'est déterminer toutes les sommes de Gauss $G_L(\chi, \mu_L)$, où L est le corps des racines de $X^m - 1$ et χ d'ordre m dans $\widehat{L^\times}$. Une fois résolu, on peut utiliser la *relation de Hasse-Davenport* et la notion de *relèvement* pour trouver les valeurs des sommes de Gauss d'ordre m dans les différentes extensions de K. C.F. Gauss mit plusieurs années pour résoudre le problème[7] d'ordre 2, quant au problème des sommes de Gauss d'ordre 3, il n'est pas encore résolu ! Mais ce n'est pas une raison pour se décourager puisque la difficulté n'est pas proportionnelle à l'ordre. Par exemple, lorsque p est *auto-conjugué* modulo m, ce qui signifie que -1 est dans le sous-groupe de $(\mathbf{Z}/m\mathbf{Z})^\star$ engendré par p, les sommes de Gauss sont rationnelles et complètement déterminées. Il en résulte des codes à deux poids. La théorie de Galois montre que si le groupe engendré par p est d'indice 2 dans $(\mathbf{Z}/m\mathbf{Z})^\star$ les sommes de Gauss d'ordre m sont des nombres quadratiques et on peut utiliser le théorème de Stickelberger sur la décomposition de l'idéal engendré par une somme de Gauss pour les déterminer toutes. Notons que si p est d'indice 2 dans $(\mathbf{Z}/m\mathbf{Z})^\star$ alors m possède au plus deux facteurs premiers. Le cas d'un produit de deux nombres premiers a été traité par Van der Vlugt [**183**]. Presque au même moment, et sans encore connaître ses travaux je traitais le cas primaire publié dans *Calcul de certaines sommes de Gauss*. Le cas d'un produit de deux nombres primaires est achevé par Mbodj dans [**144**].

La lecture de [**190**] m'a donné le goût des textes anciens que j'essaye de transmettre à mon tour en commençant le chapitre II *Sommes de Gauss* par quelques démonstrations tirées du fameux *disquisitiones arithmeticae* [**73**], à côtés desquelles, les preuves plus modernes basées sur la connaissance des corps cyclotomiques mesurent tout le chemin parcouru en à peine un siècle. Les sommes de Gauss forment un pont entre la structure additive d'un corps fini et sa structure multiplicative. Quand elles sont simples, les formules relatives aux sommes de Gauss reflètent toujours des « propriétés cachées » des corps finis. Les plus remarquables sont rapportées pour que cette partie puisse servir de pense-bête. Le chapitre se terminent par l'exposé des résultats de Oumar Mbodj et ceux de mon article *Calculs de certaines sommes de Gauss* [**126**] en incluant mes travaux récents à propos des sommes de Gauss sur un anneau fini [**127**].

CORPS DE GALOIS

En général, la méthode de dénombrement par les sommes de caractères donne une expression du nombre de solutions d'une équation polynomiale en termes de sommes de Gauss. On dispose alors de trois stratégies pour analyser le nombre

[7] Le fameux problème de la détermination du signe résolu dans *sommatio quarumdam serierum singularium* et non pas dans le plus élémentaire *disquisitiones arithmeticae* comme j'ai pu souvent le lire.

obtenu : la théorie de Galois précise les bonnes conditions à imposer aux paramètres du problème pour faire apparaître des cas particuliers, la stabilité en modules des sommes de Gauss fournit une estimation, et enfin les congruences de Stickelberger donnent une approximation p-adique toujours fine. Par illustrer ce dernier point, considérons L une extension finie du corps à deux éléments, a un élément non-nul de L et un d entier. Calculons le coefficient de Fourier en a de la fonction $f(x) = \mathrm{tr}_{L/\mathbf{F}_2}(x^d)$, c'est la somme de caractères :

$$\begin{aligned}\widehat{f}_\chi(a) &= 1 + \sum_{x\in L^\times} \mu_L(x^d + ax)\\ &= 1 + \frac{1}{q-1}\sum_{\chi\in\widehat{L^\times}} G_L(\chi,\mu_L)G_L(\bar\chi^d,\mu_L)\bar\chi^d(a)\end{aligned}$$

La seconde ligne est obtenue à partir de la première, en injectant la relation $\mu_L(x) = \frac{1}{q-1}\sum_{\chi\in\widehat{L^\times}} G_L(\chi,\mu_L)\bar\chi(x)$ qui n'est rien d'autre que l'expression d'une inversion de Fourier. Le paragraphe précédent explique que le calcul explicite de $\widehat{f}_\chi(a)$ pour tout a et tout d est parfaitement utopique. Réduisons modulo q,

$$-\widehat{f}_\chi(a) \equiv \sum_{\chi\neq 1} G_L(\chi,\mu_L)G_L(\bar\chi^d,\mu_L)\bar\chi^d(a) \bmod q$$

Le théorème des *congruences de Stickelberger* affirme l'existence d'un caractère multiplicatif ω générateur du groupe $\widehat{L^\times}$ et d'un idéal premier $\mathcal{P}$ au-dessus de 2 dans le $(q-1)$-ième anneau des entiers cyclotomiques tels que

$$-G_L(\omega^j,\mu_L) = (-2)^{S(j)} \pmod{(-2)^{S(j)}\mathcal{P}}, \quad 0\leq j\leq q-2,$$

où $S(j)$ est égal au poids binaire du résidu modulo $q-1$ de l'entier j. Notons J l'ensemble des entiers $1\leq j<q-1$ minimisant $S(j)+S(-dj)$ et notons w ce minimum. La congruence précédente devient :

$$\widehat{f}_\chi(a) = 2^w\big[\sum_{j\in J}\bar\omega^{jn}(a)\big] \pmod{2^w\mathcal{P}}$$

Les coefficients de Fourier de f sont tous de valuation dyadique supérieure ou égale à w. De plus, si d est premier avec $(q-1)$ les caractères ω^{dn} sont tous distincts et indépendants modulo $\mathcal{P}$, donc il existe $a\in L$ tel que $\widehat{f}_\chi(a)$ soit de valuation dyadique w. Le procédé que je viens d'utiliser me sert à retrouver la divisibilité des codes abéliens obtenue par Delsarte et McEliece [**63**], il s'agit de manipuler des sommes de Gauss sur des algèbres semi-simples introduites dans mon article *weight of abelian codes* [**129**], voir le rapport de recherche [**128**]. Dans l'article *regular section groups* [**124**], j'utilise les congruences de Stickelberger pour déterminer les conditions nécessaires et suffisantes à imposer à G, K et L pour que les tailles des sections hyperplanes de G soient régulièrement distribuées. Dans le cas d'un anneau local A, on peut définir un sous-groupe multiplicatif très particulier $T_A^\times$: le groupe de Teichmüller. Par l'expérience, on se rend compte que les modules des sommes de Gauss incomplètes sont très dispersés. L'identification de $\{0\}\cup T_A^\times$ avec le corps résiduel K de A, permet de définir des *fonctions traciques* :

$$\mathrm{tr}_{A/\mathbf{Z}/(p^\ell)}(x) = \sum_{i=0}^{\ell-1} t_j(x)p^j.$$

La première fonction tracique est la trace usuelle de K. Dans le cas d'un anneau de Galois de caractéristique 4, 8 etc... la deuxième fonction tracique est une forme quadratique non-dégénérée dont je calcule l'invariant de Arf à partir de l'expression de la somme de Gauss « triviale » $G_T(1,\mu_A)$ ce qui est loin d'être trivial ! Cette fonction joue un rôle important dans l'étude des poids de Lee du code de Kerdock $\mathbf{Z}/4\mathbf{Z}$-linéaire. Dans le cas de la caractéristique quatre, je démontre que les sommes de Gauss incomplètes vérifient des propriétés analogues aux congruences de Stickelberger, voir [**127**].

Le chapitre III traite des corps finis et de leurs cousins : les anneaux de Galois et des extensions algébriques du corps des nombres p-adiques. La formule de Gross-Koblitz est la version actuelle des congruences de Stickelberger. Ces congruences donnent une approximation « non-archimédienne » des sommes de Gauss. Une des plus formidables applications des congruences de Stickelberger est la démonstration du théorème d'Ax par la méthode des sommes d'exponentielles.

CODES

Mes publications dans le domaine des codes sont axées sur la mise en évidence de distributions particulières. Dans *Linear Codes with Balanced Weight Distribution* [**132**], une collaboration avec J.-P. Zanotti nous contruisons des codes DPE i.e. dans lesquels tous les poids non-nuls apparaissent avec la même multiplicité. La formule de McEliece qui relie les sommes de Gauss et les poids d'un code cyclique irréductible montre que le nombre de poids non-nuls d'un code cyclique irréductible de longueur n est inférieur ou égal au nombre de classes cyclotomiques de p modulo $\frac{(q^s-1)(n,q-1)}{n(q-1)}$; c'est le *nombre de poids prescrit*. Un code cyclique irréductible dont le nombre de poids non-nuls atteint cette borne est dit *sans collisions*. Dans le mémoire, je détermine le groupe d'automorphismes des codes sans collisions. Les codes DPE sont sans collisions. Les sommes de Gauss rationnelles fournissent une large classe de codes à deux poids. Les codes en situation quadratique ont au plus trois poids, dans l'article *New Two Weight Codes* [**125**], j'utilise la relation de Hasse-Davenport pour déterminer des codes ayant un nombre de poids prescrit 3, mais avec collisions. Ce phénomène est rare : le premier exemplaire est le code Hamming binaire de longueur 7, le second est le code de Golay de longueur 11, les autres sont nouveaux.

La théorie des codes correcteurs d'erreurs est exposée dans le chapitre IV. Les codes dont il est question sont des codes en blocs qu'on utilise pour protéger les transmissions sur un canal bruité. L'identité de MacWilliams illustre bien l'intérêt qu'il faut porter envers les sommes de caractères et la formule de Poisson. Les formules de Pless s'en déduisent mais peuvent très bien être obtenues directement par une formule Poisson sur les co-poids du code.

SÉQUENCES

Les fonctions « courbes » sont définies par Rothaus comme étant des fonctions booléennes parfaites, elles sont nécessairement hautement non-linéaires et leur transformée de Fourier est de module constant. Les *fonctions courbes généralisées* ont été introduites par R. Welch et sont l'objet de la thèse de P. Kumar. Par définition, une fonction courbe généralisée est une application $f\colon (\mathbf{Z}/q\mathbf{Z})^m \to \mathbf{Z}/q\mathbf{Z}$ telle qu'il existe un caractère $\psi \in \widehat{\mathbf{Z}/q\mathbf{Z}}$ pour lequel la transformée de Fourier de f_ψ est de module constant. Dans l'article *On Generalized Bent Functions* [**119**], j'étudie ces fonctions dans le cas q premier. Du point de vue algébrique, je montre que le degré d'une fonction courbe vérifie

$$\deg(f) \leq (p-1)t + 2p - 3,$$

avec $m = 2t$ ou $m = 2t+1$ suivant la parité ; c'est une formule analogue au cas binaire. Du point de vue métrique, je constate que la non-linéarité d'une fonction courbe peut prendre deux valeurs, et donc ces fonctions ne sont pas nécessairement hautement non-linéaires. En un certain sens, une fonction courbe généralisée n'est pas courbe ! Dans l'article, *sequences with good autocorrelation properties* [**123**], je construis des séquences à autocorrélations particulières. En quelques mots, désignons par L une extension de K, α un élément d'ordre n dans $L^\times$ et χ un caractère multiplicatif de K, prolongé par la valeur nulle en zéro. Je considère les fonctions de la forme :

$$\begin{aligned} f\colon \mathbf{Z}/n\mathbf{Z} &\to \mathbf{C}^\times \\ t &\mapsto \chi\big(\mathrm{tr}_{L/K}(\alpha^t)\big) \end{aligned}$$

Le spectre de Fourier de cette séquence se calcule en fonction de sommes d'Eisenstein et finalement de sommes de Gauss. L'expression obtenue dicte les bonnes conditions à imposer aux paramètres χ, K , L et n pour obtenir des séquences à autocorrélation remarquable, d'où je tire une famille infinie de séquences presque-parfaites [**122**] dans *Construction of almost perfect sequences*. L'existence des séquences θ-presque-parfaites conditionnée par l'équation (1) est traitée dans *Almost Perfect Sequences* [**119**]. Le rapport de recherche [**127**], propose une généralisation de la notion de m-séquence. Étant donné un anneau fini commutatif A, un sous-groupe Γ de $\widehat{A}$ et un élément inversible γ, je construis la famille d'intercorrélation

$$\mathcal{F}(\gamma, A, \Gamma) = \{s(\gamma,\psi) \mid \psi \in \Gamma\}.$$

C'est une généralisation de l'approche de P. Solé, reprise par S. Boztas, et P. Kumar. Les cas des anneaux ramifiés $K[X]/X^2$ et $GR(4,f)[X]/(X^2-2,2X)$ sont examinés.

Les problèmes de corrélations sont abordés dans le chapitre V. Dans ce contexte la transformation de Fourier prend tout son sens. La formule de Poisson est un argument obligé pour la preuve du fameux *théorème des multiplieurs* de Turyn.

FONCTIONS BOOLÉENNES

Les *fonctions booléennes* dont il est question sont des fonctions à valeurs dans le corps à deux éléments définies sur $\mathbf{F}_2^m$. On cherche à construire des fonctions *hautement non-linéaires* ; c'est-à-dire à distance maximale du code de Reed-Muller du premier ordre. En dimension paire, il s'agit des fonctions *courbes* dont le degré est nécessairement dans l'intervalle $[2, \frac{m}{2}]$. Dans notre article *Results on bent functions* [**96**], nous précisons leur forme polynomiale. Aux classes de fonctions courbes connues : Maiorana-McFarland, Dillon et Carlet-Guillot, nous ajoutons un procédé de construction de fonctions courbes qui donne lieu à un algorithme d'énumération de fonctions courbes, non-déterministe décrit dans le document. En dimension impaire, le degré de non-linéarité maximal n'est pas connu à partir de la dimension 9. Dans [**117**], je montre que les cubiques ne dépassent pas la borne quadratique pour cette dimension. Les généralisations des notions de noyaux et défauts proposées dans notre article *Kernels and Defaults* [**130**] montrent que les cubiques à noyau minimal sont de bonnes candidates pour la haute non-linéarité, et maintenant, la conjecture $R_3(m) \sim 2^{\frac{m}{2}}$ me semble raisonnable. On peut munir l'ensemble des classes latérales de $\mathrm{RM}(1, m)$ d'un ordre partiel dont les éléments maximaux sont des *urcosets*. La classe d'une fonction hautement non-linéaire est un urcoset. La conjecture de Vera Pless affirme que le rayon de recouvrement du code de Reed-Muller est d'ordre impair, hypothèse confortée par X. D. Hou en utilisant ma proposition sur les urcosets de poids impairs *On the orphans and covering radius of the Reed-Muller codes* [**118**]. Dans les contrats de recherches [**133, 131**], de nombreuses expériences numériques ont été menées : analyse des urcosets de poids impairs, distance d'une cubique au code de Reed-Muller du second ordre, fonctions stables sous l'action d'un groupe, non-linéarité des fonctions traciques, co-cycliques etc... De ces expériences ressortent deux invariants affines : l'indice et la hauteur d'une fonction. Le premier est présenté dans ce mémoire, le second est étudié dans notre article *H-codes and derivations* [**97**] soumis à publication.

*

* *

CHAPITRE 1

Analyse de Fourier

Au début du XVIII siècle, Léonard Euler (1707–1783) avait déjà remarqué la décomposition de certaines fonctions en sommes de fonctions trigonométriques. Motivé par ses travaux sur l'équation de la chaleur, le baron Jean-Baptiste Fourier (1768-1830) conjecture et utilise [1] la décomposition d'une distribution thermique initiale en une somme d'une fondamentale et de ses harmoniques. Le calcul de l'amplitude des harmoniques est une transformée de Fourier. Au fil du temps cette notion s'est affinée pour s'appliquer à beaucoup de domaines. En informatique, la multiplication rapide de deux polynômes obtenue par l'implantation efficace de la transformée de Fourier est une remarquable illustration du principe algorithmique « diviser pour régner ».

Dans ce chapitre, il est question de dualité. Celle-ci est basée sur des relations d'orthogonalité et fait le lien entre deux structures d'anneaux : les anneaux de fonctions et les anneaux de groupes. La théorie des caractères introduit les sommes d'exponentielles et la transformée de Fourier. Le calcul du nombre de zéros d'une forme quadratique illustre la méthode des sommes de caractères alors que la trivialisation du produit de convolution par la transformée de Fourier nous renseigne sur la structure des anneaux de groupes. Un anneau fini commutatif possède deux structures de groupes : additive et multiplicative. La transformée de Fourier de la restriction d'un caractère additif au groupe multiplicatif est une somme de Gauss. Les sommes de Gauss jouent un rôle déterminant dans mes articles. Les caractères additifs et multiplicatifs des corps finis et des algèbres semi-simples sont détaillés pour s'appliquer à la théorie des codes abéliens. L'expression des sommes d'Einsenstein en fonction des sommes de Gauss que l'on obtient à partir de la formule de Poisson marque le début de la série des jolies identités qui se déduisent de cette relation. Toute cette technique subsiste dans le cas des groupes localement compacts et quelque chose me dit qu'il faudra creuser dans cette voie. Les anneaux quasi-Frobenius sont au carrefour de la théorie des caractères et des anneaux. Ils permettent une bonne compréhension d'un beau théorème de MacWilliams. Les programmeurs dont je suis, sont particulièrement sensibles à la finesse des algorithmes de calculs de transformée de Fourier qui clôturent ce chapitre. Ces deux derniers points témoignent de l'intérêt que je porte aux méthodes purement numériques et aux méthodes numériquement impures. Aux candides lecteurs qui sont arrivés jusqu'à ces mots je conseille de passer directement à la dernière section sur le jeu de Fourier.

1. Anneaux de fonctions

Soit A un anneau et X un ensemble. Dans ce texte, il sera souvent question d'applications *booléennes*, *numériques*, *p-adiques* etc... ayant pour codomaines respectifs

[1] La rigueur mathématique de Fourier était contestable, mais les résultats étaient au rendez-vous. Lagrange, Laplace, Poisson, Legendre, Biot, etc... mettront plusieurs années à accepter cette révolution.

le corps à deux éléments $\mathbf{F}_2$, le corps des nombres complexes $\mathbf{C}$, et son analogue p-adique $\mathbf{C}_p$ etc...

L'ensemble des applications de domaine X et de co-domaine A hérite des opérations de A pour former l'anneau A^X des fonctions de X dans A. Les opérations sont définies termes à termes. À chaque point $x \in X$ correspond une application particulière, l'*application de Dirac* δ_x nulle partout sauf en x où elle vaut 1. Le système $(\delta_x)_{x\in X}$ est libre, et lorsque X est fini, c'est une base du A-module des applications de domaine X à valeurs dans A.

Soit G un groupe fini. Un application bilinéaire du module A^G est complètement définie par son action sur la base des fonctions de Dirac. En particulier, la loi de G induit sur A^G une application bilinéaire définie par $(\delta_x, \delta_y) \mapsto \delta_{x+y}$. La loi de composition interne qui en résulte est un *produit de convolution* . Le produit de convolution des applications f et g se note $f * g$, on a :

$$f * g(c) = \sum_{a+b=c} f(a)g(b)$$

Le module des applications de domaine G, de codomaine A muni du produit de convolution forme un anneau $A[G]$ que l'on appelle l'*anneau du groupe* G à coefficients dans A. Du reste, en considérant les produits des éléments du système de Dirac, le lecteur vérifiera sans peine que si G' désigne un second groupe alors

$$A^G \otimes A^{G'} \sim A^{G\times G'}, \quad \text{et} \quad A[G] \otimes A[G'] \sim A[G \times G'].$$

2. Caractères

Soient G un groupe abélien et A un anneau commutatif dont l'élément unité est noté 1_A. Un *caractère* de G à valeurs dans A est un homomorphisme du groupe G dans $A^\times$, le groupe multiplicatif de l'anneau A. Bien sûr, l'image d'un élément de G par un des caractères de G est un élément d'ordre diviseur de $\mathrm{Exp}(G)$, l'exposant de G. On dit que A est un *anneau de représentation* de G si sa caractéristique est première avec l'ordre de G et si $A^\times$ contient un et un seul groupe cyclique d'ordre $\mathrm{Exp}(G)$. L'anneau des entiers relatifs est un anneau de représentation de $\mathbf{F}_2^m$, et certains anneaux possèdent la propriété remarquable de représenter leur groupe multiplicatif : c'est le cas des corps finis.

Proposition 2.1. *Si A est un anneau de représentation de G alors les groupes G et $\mathrm{Hom}(G, A^\times)$ sont isomorphes.*

Démonstration. D'après la théorie des facteurs invariants, le groupe G est produit de groupes cycliques $\mathbf{Z}/n_1\mathbf{Z} \times \mathbf{Z}/n_2\mathbf{Z} \times \mathbf{Z}/n_s\mathbf{Z}$ avec $n_1 \mid n_2 \mid \dots \mid n_s = \mathrm{Exp}(G)$. Soient X, Y et Z trois modules. L'isomorphime de modules

$$\mathrm{Hom}(X \times Y, Z) \sim \mathrm{Hom}(X, Z) \times \mathrm{Hom}(Y, Z)$$

permet de se restreindre au cas du groupe $\mathbf{Z}/\mathrm{Exp}(G)\mathbf{Z}$. On conclut avec l'isomorphisme

$$\mathrm{Hom}(X, Y \times Z) \sim \mathrm{Hom}(X, Y) \times \mathrm{Hom}(X, Z)$$

□

Nous continuons en supposant que A est un anneau de représentation de G. Le groupe dual de G est souvent noté $\widehat{G}$, cette notation est surtout utilisée pour une représentation à valeurs dans $\mathbf{C}$ ou $\mathbf{C}_p$. L'usage veut que les éléments de $\widehat{G}$

soient désignés par des lettres grecques. Plus tard, nous respecterons cet usage. Dans l'immédiat, nous utiliserons les notations de Weil à savoir que x^* désigne un élément générique de $\widehat{G}$ sans pour autant voir une application $x \mapsto x^*$. Le *crochet de dualité* de G dans A s'écrit :

$$\langle x, y^* \rangle_A^G = y^*(x), \qquad x \in G, \quad y^* \in \widehat{G}.$$

en abrégé $\langle x, y^* \rangle$. L'application $(x, x^*) \mapsto \langle x, x^* \rangle_A^G$ est un accouplement du groupe G avec son groupe dual ; C'est une application $\mathbf{Z}$-bilinéaire,

$$\langle x + y, z^* \rangle = \langle x, z^* \rangle \langle y, z^* \rangle, \quad \langle x, y^* + z^* \rangle = \langle x, y^* \rangle \langle x, z^* \rangle$$

et pour tout entier j, $\langle x, x^* \rangle^j = \langle x, jx^* \rangle = \langle jx, x^* \rangle$, vérifiant des *relations d'orthogonalité* :

$$\sum_{x \in G} \langle x, y^* \rangle = \begin{cases} |G|.1_A, & \text{si } y^* = 0\,; \\ 0, & \text{sinon.} \end{cases}$$

(9)

$$\sum_{y^* \in \widehat{G}} \langle x, y^* \rangle = \begin{cases} |G|.1_A, & \text{si } x = 0\,; \\ 0, & \text{sinon.} \end{cases}$$

Soit S un sous-groupe de G. Les caractères de G qui induisent sur S le caractère trivial forment un sous-groupe de $\widehat{G}$. C'est le groupe associé à S par dualité, ou encore, l'*orthogonal* de S, on le note : $S^\perp$. Par factorisation et relèvement, on obtient un isomorphisme :

$$S^\perp \sim \widehat{(G/S)}$$

Pour tout $x \in G$, l'homomorphisme d'évaluation en x : $x^* \mapsto x^*(x)$, définit un caractère du groupe $\widehat{G}$. Comme l'ordre du groupe G est égal à l'ordre du bi-dual de G, nous en déduisons un isomorphisme canonique entre G et $\widehat{\widehat{G}}$. L'identification qui en résulte se traduit par l'égalité

$$\langle x^*, x \rangle_A^{\widehat{G}} = \langle x, x^* \rangle_A^G$$

sous cette identification $S = S^{\perp\perp}$.

Soient X et Y deux groupes abéliens admettant un anneau de représentation commun A. À chaque homomorphisme Ψ du groupe X vers le groupe Y, on associe un homomorphisme Ψ^* du groupe $\widehat{Y}$ vers le groupe $\widehat{X}$ défini par l'égalité :

$$\langle \Psi(x), y^* \rangle_A^Y = \langle x, \Psi^*(y^*) \rangle_A^X.$$

Si Ψ est surjectif alors Ψ^* est injectif. Dans ce cas, le caractère $\Psi^*(y^*)$ est un *relèvement* du caractère y^* par le morphisme Ψ. Cette notion intervient dans la relation de Hasse-Davenport. Si Ψ est injectif, Ψ^* est surjectif et on parle de *restriction.*

3. La méthode des sommes de caractères

La méthode dite des *sommes de caractères* , ou encore des *sommes d'exponentielles* , permet de compter le nombre de solutions d'une équation algébrique ou non. Elle est basée sur l'emploi des relations d'orthogonalité. Considérons une application d'un ensemble X dans un groupe abélien G, notons $Z(f, a)$ le nombre d'éléments

$x \in X$ vérifiant $f(x) = a$ et posons $S(f, \psi) = \sum_{x \in X} \psi(f(x))$, les relations d'orthogonalité donnent

$$Z(f, a).1_A = \frac{1}{|G|} \sum_{\psi \in \hat{G}} S(f, \psi) \bar{\psi}(a). \tag{10}$$

Lorsque $A = \mathbf{C}$, on obtient ainsi une formule sur nombre de solutions de l'équation $f(x) = g$ qui fait intervenir des entiers cyclotomiques. L'exploitation des propriétés arithmétiques (non-archimédiennes) de l'anneau des entiers cyclotomiques dans l'étude des sommes de caractères fait partie de ce que j'appelle les méthodes qualitatives, par opposition aux méthodes quantitatives qui n'utilisent que des propriétés archimédiennes du corps des nombres complexes.

4. Un exemple classique

Soit E un espace vectoriel de dimension s sur un corps K à q éléments. Soit $\mathbf{q}$ une forme quadratique, ϕ la forme bilinéaire associée $\mathbf{q}(x + y) = \mathbf{q}(x) + \mathbf{q}(y) + \phi(x, y)$, $\ker(\mathbf{q})$ son *noyau* ; c'est le sous-espace vectoriel, disons de dimension k, de E formé des vecteurs $\{x \in E \mid \forall y \in E, \phi(x, y) = 0\}$. La restriction de $\mathbf{q}$ au noyau est une forme linéaire, si celle-ci n'est pas nulle, $\mathbf{q}$ est dite *défective*, ce qui ne peut arriver qu'en caractéristique 2. Soit ψ un caractère non trivial du groupe additif de K. Le calcul du module de $S(\mathbf{q}, \psi)$ est assez facile :

$$\begin{aligned} S(\mathbf{q}, \psi)\overline{S(\mathbf{q}, \psi)} &= \sum_{x,y \in E} \psi\big(\mathbf{q}(x) - \mathbf{q}(y)\big) = \sum_{x,y \in E} \psi\big(\mathbf{q}(x + y) - \mathbf{q}(y)\big) \\ &= \sum_{x,y \in E} \psi\big(\mathbf{q}(x) + \phi(x, y)\big) = \sum_{x \in E} \psi(\mathbf{q}(x)) \sum_{y \in E} \psi(\phi(x, y)) \\ &= q^s \sum_{x \in K} \psi\big(\mathbf{q}(x)\big), \end{aligned}$$

pour la dernière égalité, il faut remarquer que $y \mapsto \psi(\phi(x, y))$ est un caractère de E, trivial si et seulement si $x \in \ker(\mathbf{q})$. Mézalors, l'application $\psi \circ \mathbf{q}$ est un caractère de $\ker(\mathbf{q})$ non-trivial si et seulement si $\mathbf{q}$ est défective.

$$S(\mathbf{q}, \psi) S(\mathbf{q}, \bar{\psi}) = \begin{cases} q^{\frac{k+s}{2}}, & \text{non défective}\,; \\ 0, & \text{défective.} \end{cases} \tag{11}$$

5. Transformation de Fourier

Le groupe $\widehat{G}$ dual du groupe G étant décrit, nous pouvons définir un *opérateur de Fourier* $\mathcal{F}$ sur l'ensemble des applications de G à valeurs dans A par

$$\mathcal{F}(f)(y^*) = \sum_{x \in G} f(g) \langle x, y^* \rangle_A^G \tag{12}$$

$\mathcal{F}(f)$ est la *transformée de Fourier* le plus souvent notée $\widehat{f}$; c'est une application de $\widehat{G}$ dans A. Aux différents choix de A correspondent différentes terminologies : Walsh, Hadamard, Mattson-Solomon, Mellin... Le lecteur doit faire le lien avec la définition usuelle de la transformée de Fourier. Si f désigne une fonction réelle intégrable sur $\mathbf{R}$ alors sa transformée de Fourier en x est $\int_{\mathbf{R}} f(t) e^{ixt} dt$. Les applications $t \mapsto e^{ixt}$ sont des caractères du groupe localement compact $(\mathbf{R}, +)$ qui joue le rôle de G.

L'image par $\mathcal{F}$ de la base formée des fonctions de Dirac de G est une base de $A^{\widehat{G}}$. Notons χ_x l'image de δ_x,

$$\widehat{\delta_x}(y^*) = \chi_x(y^*) = \langle x, y^* \rangle_A^G.$$

Dans le cas $A = \mathbf{C}$, l'espace des applications de G dans $\mathbf{C}$ muni du produit scalaire usuel est un espace euclidien et les systèmes $\{\delta_x \mid x \in G\}$ et $\{\chi_x \mid x \in G\}$ en sont deux bases orthogonales. Cette « évidence » est la clef de la détermination du signe de la somme de quadratique de Gauss, voir plus loin. Le lecteur doit remarquer que la matrice de l'opérateur de Fourier dans la base $\{\delta_x \mid x \in G\}$ est

$$(\langle x, y^* \rangle_{\mathbf{C}}^G)_{x \in G, y^* \in \widehat{G}}$$

est une matrice orthogonale. Ses coefficients sont de module 1, c'est une matrice de Hadamard généralisée. La transformée de Fourier est inversible, sa réciproque s'appelle la *transformée de Fourier inverse* . L'antécédant d'une application f de $\widehat{G}$ dans A est donné par la *formule d'inversion* :

$$\bar{\mathcal{F}}(f)(y) = \frac{1}{|G|} \sum_{x^* \in \widehat{G}} f(x^*) \langle -y, x^* \rangle_A^G \tag{13}$$

Démonstration. Exercice. □

La *formule de Poisson* donne une interprétation plus générale de la formule d'inversion. Soit S un sous-groupe de G

$$\frac{1}{[G:S]} \sum_{s^* \in S^\perp} \mathcal{F}(f)(s^*) \langle -t, s^* \rangle_A^G = \sum_{s \in t+S} f(s). \tag{14}$$

Evident ! Il n'empèche que, beaucoup d'égalités et d'identités plus ou moins célèbres en découlent : formule de McEliece sur les poids des codes cycliques irréductibles, identités de McWilliams, théorème des multipliers de Turyn etc... Nous allons nous en servir pour exprimer les sommes d'Eisenstein en termes de sommes de Gauss. Pour garder en tête le facteur multiplicatif $1/[G:H]$, il faut se rappeler cette formule exprime une moyenne des coefficients de Fourier.

6. Structure des anneaux de groupes

Dans la première section, nous avons introduit deux anneaux de fonctions. L'anneau des fonctions de G dans A et l'anneau de groupe $A[G]$. La transformée de Fourier « trivialise » le produit de convolution :

$$\mathcal{F}(f * g) = \mathcal{F}(f)\mathcal{F}(g), \tag{15}$$

en d'autre termes, la transformée de Fourier est un morphisme de l'anneau $A[G]$ dans l'anneau $A^{\widehat{G}}$. C'est un isomorphisme dès que A est un anneau de représentation de G. En général, A ne contient pas assez d'inversibles pour représenter G et on a recours à une extension B de A pour représenter G. Il s'en suit l'inclusion

$$0 \longrightarrow A[G] \longrightarrow B[G] \longrightarrow B^{\widehat{G}}$$

Les idempotents de $B[G]$ se déduisent des idempotents de $B^{\widehat{G}}$ par transformée de Fourier inverse. Les idempotents minimaux de l'algèbre $B^{\widehat{G}}$ sont les fonctions de Dirac δ_{y^*}. Nous en déduisons les idempotents minimaux de $B[G]$:

$$\chi_{y^*}^* = \frac{1}{|G|} \sum_{x \in G} \langle -x, y^* \rangle \delta_x$$

les idempotents minimaux de $A[G]$ s'obtiennent par cyclotomie. Le cas des anneaux de Galois est détaillé dans la section sur les codes abéliens du chapitre IV.

THÉORÈME 6.1 (Maschke). *Soit K un corps fini, et G un groupe fini. L'algèbre de groupe $K[G]$ est semi-simple si et seulement si la caractéristique de K ne divise pas l'ordre de G.*

DÉMONSTRATION. Rappelons qu'une K-algèbre semi-simple est par définition isomorphe à un produit d'algèbres de matrice carrées à coefficients dans K. Le lecteur vérifiera que la condition est nécessaire en calculant la puissance p-ième d'un élément f satisfaisant à la condition $\sum_{x\in G} f(x) = 0$. Dans le cas commutatif, la transformation de Fourier montre la suffisance et la méthode s'adapte sans difficulté au cas non-abélien, voir [**54**]. □

Pour terminer, notons dans un coin quelques déclinaisons bien utiles de la formule de trivialisation du produit de convolution

$$\mathcal{F}(f*g) = \mathcal{F}(f)\mathcal{F}(g) \qquad \mathcal{F}(fg) = \frac{1}{|G|}\mathcal{F}(f)*\mathcal{F}(g)$$

$$\mathcal{F}(f^{(r)}) = \big(\mathcal{F}(f)\big)^r \qquad \mathcal{F}(f^r) = \frac{1}{|G|^{r-1}}\big(\mathcal{F}(f)\big)^{(r)}.$$

7. Caractères des corps finis

Dans cette section, il n'est question que de représentation à valeurs dans le corps des nombres complexes. Les représentations p-adique des corps finis seront détaillées dans le chapitre III. Un corps fini possède deux structures de groupes. La structure additive et la structure multiplicative. Le groupe multiplicatif d'un corps fini est un groupe cyclique, son groupe additif est un produit de groupes cycliques, et en un certain sens, la structure additive est plus complexe que la structure multiplicative. D'une manière générale, les caractères sont définis à partir de certaines racines de l'unités, et il en résulte une indétermination. L'un des premiers objectifs de la théorie des caractères est de lever cette ambiguïté. Pour la structure additive, nous disposons d'un caractère canonique, pour la structure multiplicative nous disposons du caractère de Teichmüller.

Soit K un corps fini de caractéristique p et de cardinal $q = p^f$. Un *caractère additif* de K est un caractère du groupe K^+. Notons ζ_p la racine p-ième principale i.e. le nombre complexe de module 1 et d'argument $\frac{2\pi}{p}$. On définit le *caractère additif canonique* de K par

$$\mu_K\colon K \to \mathbf{C}; \quad x \mapsto \zeta_p^{\mathrm{tr}_{K/\mathbf{F}_p}(x)}.$$

À ce stade, le lecteur doit avoir conscience que l'aspect « canonique » de ce caractère dépend de l'existence d'une forme linéaire canonique et d'une racine p-ième canonique. Ce dernier point qui est de nature topologique s'évanouit dans le cas p-adique. Le groupe additif de K agit sur le dual de K par $b \mapsto \psi_b$, où $\psi_b(x) = \psi(bx)$. Le choix d'un caractère non-trivial conduit à une identification de K^+ avec son dual, c'est une propriété caractéristique des anneaux quasi-Frobenius.

Un *caractère multiplicatif* de K est un caractère du groupe $K^\times$. Le procédé de Teichmüller est un moyen simple, efficace et universel de supprimer l'ambiguïté relative aux différents choix possibles des racines primitives $(q-1)$ dans le corps fini

[2] K. Soit ξ une racine primitive $(q-1)$-ième de l'unité dans une extension convenable du corps des nombres rationnels. Soit $\mathcal{P}$ un idéal premier de $\mathbf{Z}[\zeta_p, \xi]$, la surjection canonique définit un morphisme de $\mathbf{Z}[\zeta_p, \xi]^\times$ sur ${\mathbf{F}_q}^\times$, admet une section ω_K qui envoie la classe d'une racine $(q-1)$-ième de l'unité sur elle même

$$\omega_K \colon {\mathbf{F}_q}^\times \to \mathbf{Z}[\zeta_p, \xi]; \quad \xi \mod \mathcal{P} \mapsto \xi.$$

Cette section définit un caractère multiplicatif de $\mathbf{F}_q$, c'est le *caractère de Teichmüller* de $\mathbf{F}_q$. Il dépend du choix de $\mathcal{P}$.

8. Caractères des algèbres semi-simples

Soient K un corps fini de caractéristique p et de cardinal q et A une K-algèbre semi-simple. Il existe s extensions $K_1, K_2, \ldots, K_s$ du corps K telles que A soit isomorphe au produit direct $K_1 \times K_2 \times \ldots \times K_s$. Les caractères multiplicatifs et additifs de A sont les caractères produits. Si χ est un caractère multiplicatif de A alors il existe s caractères multiplicatifs $\chi_1 \in \widehat{K_1^\times}$, $\chi_2 \in \widehat{K_2^\times}$ etc... tels que $\chi = \chi_1 \times \chi_2 \times \cdots \times \chi_s$. De même, si ψ est un caractère additif de A il existe s caractères additifs $\psi_1 \in \widehat{K_1^+}$, $\psi_2 \in \widehat{K_2^+}$ etc... tels que $\psi = \psi_1 \times \psi_2 \times \cdots \times \psi_s$. Le *caractère additif canonique* de A est défini à partir de la trace de A sur K

$$\mu_A(x) = \zeta_p^{\mathrm{tr}_{A/K}(x)}.$$

On voit que ce caractère est égal au produit cartésien des caractères additifs canoniques des corps K_1, K_2 etc... $\mu_A = \mu_{K_1} \times \mu_{K_2} \times \cdots \times \mu_{K_s}$. Par analogie, le produit cartésien des caractères de Teichmüller des corps K_i est noté ω_A, son ordre est égal au PPCM des $(|K_i| - 1)$.

9. Sommes de Gauss

Soient $\chi \in \widehat{A^\times}$ et $\psi \in \widehat{A^+}$ la *somme de Gauss* des caractères χ et ψ est

$$G_A(\chi, \psi) = \sum_{a \in A^\times} \chi(a)\psi(a).$$

Souvent, ψ est égal au caractère additif canonique et pour abréger, on pose : $G_A(\chi) = \sum_{a \in A^\times} \chi(a)\mu_A(a)$. La somme de Gauss $G_A(\chi, \psi)$ est la transformée de Fourier de la restriction au groupe $A^\times$ du caractère additif ψ. À condition de prolonger tous les caractères multiplicatifs de A par 0 sur l'ensemble des non-inversibles de A, c'est aussi la transformée de Fourier de χ en ψ.

$$G_A(\chi, \psi) = \prod_{i=1}^{s} G_{K_i}(\chi_i)$$

PROPOSITION 9.1. *Soit F un corps fini. Si les caractères $\chi \in F^\times$ et $\psi \in F^+$ sont non triviaux alors la somme de Gauss $G_F(\chi, \psi)$ est de module $\sqrt{|F|}$ sinon elle vaut*

$$G_F(\chi, \psi) = \begin{cases} |F| - 1, & si\ \chi = 1\ et\ \psi = 1\,; \\ -1, & si\ \chi = 1\ et\ \psi \neq 1\,; \\ 0, & si\ \chi \neq 1\ et\ \psi = 1. \end{cases}$$

DÉMONSTRATION. Tout cela se déduit des relations d'orthogonalité. $\square$

[2] Les corps finis sont des objets terriblement abstraits !

10. Sommes d'Eisenstein

Soit G un sous-groupe de $A^\times$. L'étude des sections hyperplanes de G nous conduit à considérer le nombre $N(G,c)$ de solutions dans G de l'équation $\mathrm{tr}_{A/K}(x) = c$. Les relations d'orthogonalité donnent sur le champ

$$N(G,c) = \frac{1}{|G|} \sum_{\chi \in G^\perp} \sum_{\mathrm{tr}_{A/K}(x)=c} \chi(x).$$

La somme interne est une *somme d'Eisenstein* que nous notons

$$E(A,\chi,c) = \sum_{\mathrm{tr}_{A/K}(x)=c} \psi(x).$$

L'application trace est surjective, et donc, il existe dans A un élément z de trace c. Notons H l'hyperplan linéaire d'équation $\mathrm{tr}_{A/K}(x) = 0$, la formule de Poisson donne

$$\frac{1}{|H^\perp|} \sum_{\psi \in H^\perp} \mathcal{F}(\chi)\bar{\psi}(z) = E(A,\chi,c)$$

L'orthogonal de H est de cardinal q, c'est le sous-groupe de $\widehat{A^+}$ formé des caractères $\{\mu_{Kb} \mid b \in K\}$. D'où l'expression de $E(A,\chi,c)$ en fonction de sommes de Gauss

$$E(A,\chi,c) = \frac{1}{q} \sum_{b \in K} G_A(\chi, \mu_{Ab})\bar{\mu}_K(bc) \tag{16}$$

ce qui donne :

$$E(A,\chi,0) = \frac{1}{q}[G(\chi,1) + G_A(\chi,\mu_A)G_K(\bar{\chi},1)]$$

et pour $c \neq 0$,

$$E(A,\chi,c) = \frac{1}{q}[G(\chi,1) + G_A(\chi,\mu_A)G_K(\bar{\chi},\bar{\mu_K})]$$

L'intérêt de ces sommes de Gauss est de donner une formule sur le nombre, $N(a,G,b)$, de composantes égales à b dans le mot $\mu_{G,A}(a)$ lorsque a est inversible dans A.

Proposition 10.1. [**129**, $\pi\lambda$] *Soit A une K-algèbre commutative semi-simple, et soit a un élément inversible de A. Le nombre d'éléments g du groupe G de solution de l'equation $\mathrm{tr}_{A/K}(ag) = b$ est donné par :*

$$N(a,G,A,0) = \frac{n}{q} + \frac{n(q-1)}{q|A^\times|} \sum_{\chi \in (GK^\times)^\perp} G_A(\chi,\mu_A)\bar{\chi}(a) \tag{17}$$

et pour $c \neq 0$,

$$N(a,G,A,c) = \frac{n}{q} + \frac{n}{|A^\times|} \sum_{\chi \in G^\perp} G_A(\chi,\mu_A)\bar{\chi}(a) \tag{18}$$

Démonstration. C'est une application des sommes d'Eisenstein, et de la formule de Poisson. Voir mon article [**120**]. ☐

Si a est non-inversible, mais non nul, alors on se ramène à la proposition précédente. Tout d'abord, notons S le support de a, c'est l'ensemble $\{i \mid a_i \neq 0\}$, et notons A_S l'algèbre support : $A_S = \oplus_{i \in S} K_i$. L'image de G par la surjection canonique est notée G_S, celle de a est notée a_s. Avec ces notations, le mot $\mu_{G,A}(a)$ apparaît comme une répétition du mot $\mu_{G_S,A_S}(a_S)$. Le facteur de répétitions est égal à l'indice de G_S dans G.

11. Anneaux quasi-Frobenius

Dans ma thèse, je donne une estimation du rayon de recouvrement d'un code de Reed-Muller affine en fonction du nombre de ces *caractères non-dégénérés* . Par ailleurs, dans mon article *Weight of Abelian codes*, j'utilise des anneaux dans lesquels un idéal est caractérisé par son annulateur. Curieusement, ces deux notions se rejoignent dans le cadre des *anneaux quasi-Frobenius* .

Definition 11.1. *Soit A un anneau fini, le dual du groupe additif de A est un A-module à gauche lorsqu'il est muni de la loi externe $(a, g^*) \mapsto a.g^*$ définie par :*

$$\langle g, a.g^* \rangle^{A^+} = \langle ga, g^* \rangle^{A^+} \tag{19}$$

Un caractère g^* est dit admissible *s'il engendre le A-module $\widehat{A}$.*

Les qualificatifs admissible et non-dégénéré sont équivalents. Un caractères est admissible si et seulement si (0) est le seul idéal à gauche contenu dans son noyau. Enfin, si $n(A)$ désigne le nombre de caractères admissibles de A alors on a l'alternative : $n(A)$ est nul ou bien égal au nombre d'éléments inversibles de A.

Soit I un A-module à gauche. On dit que I est injectif si tous les diagrammes exacts de la forme :

$$\begin{array}{ccccc} (0) & \longrightarrow & M & \longrightarrow & N \\ & & \downarrow & & \\ & & I & & \end{array}$$

donne lieu à une flèche de N vers I.

Definition 11.2. *Un anneau A est dit injectif si le A-module à gauche ${}_AA$ est injectif.*

Dans un anneau A, on définit la notion d'annulateur à gauche et d'annulateur à droite. L'annulateur à gauche d'une partie P est noté $\mathrm{ann}_{\mathcal{G}}(P)$ et $\mathrm{ann}_{\mathcal{D}}(P)$ désigne l'annulateur à droite de P. Un annulateur à gauche est un idéal à gauche, et de même, un annulateur à droite est un idéal à droite.

Definition 11.3. *Un anneau A est dit quasi-Frobenius si pour tout idéal à gauche G de A et pour tout idéal à droite D de A les applications $ann_{\mathcal{G}}$ et $ann_{\mathcal{D}}$ satisfont* [3]

$$ann_{\mathcal{G}} \circ ann_{\mathcal{D}}(G) = G, \quad et \quad ann_{\mathcal{D}} \circ ann_{\mathcal{G}}(D) = D$$

Les trois définitions précédentes sont équivalentes.

Théorème 11.1. *Soit A un anneau, les assertions suivantes sont équivalences*
(i) A possède un caractère admissible ;

[3] Notons que l'annulateur à gauche d'un idéal à gauche est un idéal bilatère, ce qui ne donne pas l'envie d'appliquer $\mathrm{ann}_{\mathcal{G}}$ à G !

(ii) A est injectif;
(iii) A est un anneau quasi-Frobenius.

Démonstration. La démonstration de ce théorème demanderait l'introduction d'une quatrième définition d'un anneau quasi-Frobenius, celle de Nakayama, voir [**54, 196**]. Les anneaux injectifs sont traités dans les pages d'exercices du McDonald. Contentons nous de signaler que l'implication $(i) \implies (ii)$ est la plus facile; Elle résulte de la proposition suivante. □

Proposition 11.1. *Soit A un anneau et soit T un groupe divisible. Le A-module $\mathrm{Hom}_{\mathbf{Z}}(A, T)$ est toujours injectif.*

Démonstration. Rappelons qu'un groupe T est divisible lorque les applications $t \mapsto mt$ sont surjectives dès que $m \neq 0$; voir [**115**] page 786. □

Le point (i) du théorème est particulièrement intéressant pour prouver le caractère quasi-Frobenius d'un anneau fini A, il suffit d'exhiber un caractère admissible, le plus souvent noté μ_A. Bien entendu tous les corps finis sont quasi-Frobenius, mais aussi les anneaux résiduels $\mathbf{Z}/m\mathbf{Z}$, les anneaux de Galois, les produits d'anneaux quasi-Frobenius. Enfin, les anneaux de matrices carrées et les anneaux de groupes à coefficients dans un anneau quasi-Frobenius sont quasi-Frobenius.

Théorème 11.2. *Soit A un anneau quasi-Frobenius.*
(1) Pour tout entier n, l'anneau des matrices carrées $M_n(A)$ est quasi-Frobenius.
(2) Pour tout groupe fini G, l'anneau de groupe $A[G]$ est quasi-Frobenius.

Démonstration. On sait définir la trace d'un élément. Dans le cas, d'une matrice, c'est la somme de ses éléments diagonaux. Dans le cas d'un élément de l'anneau de groupe d'une matrice, c'est le coefficient de l'élément neutre. Dans les deux cas, on vérifie que le relèvement d'un caractère admissible par la trace fournit un caractère admissible. □

La proposition qui précède montre que les algèbres de groupes sont des anneaux quasi-Frobenius. En particulier, un idéal de $K[G]$ est complètement caractérisé par son annulateur. Cette proposition est le point de départ de mon article sur la description trace des codes abéliens.

Maintenant, terminons cette section par une proposition folklorique que j'utilise pour calculer le module d'une somme de Gauss sur anneau local.

Proposition 11.2. *Soit A un anneau local commutatif d'idéal maximal M. L'anneau A est quasi-Frobenius si et seulement s'il satisfait l'une des assertions suivantes :*
(1) A possède un unique idéal minimal, ou bien A est un corps.
(2) Les A-modules $ann(M)$ et A/M sont isomorphes.

12. Les isométries de l'espace de Hamming

Soient A un anneau et n un entier. Le *poids de Hamming* d'un vecteur x de A^n est égal au nombre de composante non-nulles de x. À partir du poids de Hamming, noté $\mathrm{wt}(x)$, on définit la *distance de Hamming*

$$d_H(x, y) = \mathrm{wt}(x - y).$$

C'est une distance invariante par translation, l'espace A^n équipé de cette distance s'appelle l'*espace de Hamming* de dimension n. L'ensemble des isométries de l'espace de Hamming forme un groupe d'ordre $n!|A|!$ puisque d'après Bonneau [**21**], une isométrie de A^n s'écrit d'une et une seule façon sous la forme (λ, σ), où λ est un n-uplet de permutations de A et $\sigma \in \Sigma_n$, son action est définie par $(\lambda, \sigma)(x_j) = \lambda_{\sigma(j)} x_{\sigma(j)}$. Dans ce qui suit, on ne considère que les isométries linéaires. Nous désignerons par $\mathrm{Aut}(M)$ le groupe des automorphismes linéaires qui conservent le sous-module M.

PROPOSITION 12.1. *Le groupe* $\mathrm{Aut}(A^n)$ *est isomorphe au groupe monomial* $S_n \ltimes (A^\times)^n$ *; c'est un groupe d'ordre* $n! \times |A^\times|!$.

DÉMONSTRATION. Trivial $\square$

L'importance des anneaux quasi-Frobenius dans la théorie des espaces métriques de Hamming apparaît clairement dans la généralisation par Wood [**197**] du théorème d'extension de Jessie MacWilliams.

THÉORÈME 12.1 (MacWilliams-Wood). *Soit M un sous-module de A^n. Si A est quasi-Frobenius alors toute isométrie linéaire de M se relève en une isométrie de A^n. En d'autres termes,la restriction définie une suite exacte*

$$\mathrm{Aut}(A^n) \longrightarrow \mathrm{Aut}(M) \longrightarrow (0)$$

DÉMONSTRATION. Soit χ un caractère admissible. Notons x_i la i-ième projection de A^n sur A et posons $y_i = x_i \circ f$. Par hypothèse, y_i est linéaire. L'application f conserve la distance de Hamming si et seulement si

$$\sum_{i=1}^{n} \sum_{a \in A} \chi_a \circ x_i = \sum_{i=1}^{n} \sum_{a \in A} \chi_a \circ y_i, \quad \text{sur } M.$$

Choisissons $k \in [1, n]$. Multiplions l'égalité par $\bar{\chi} \circ y_k$, sommons sur M et divisons par $|M|$. D'après le lemmule (12.1), la valeur numérique que nous obtenons compte le nombre de couples (a, i) tels que $ax_i = y_k$ (sur M), c'est aussi le nombre de couples (a, i) tels que $ay_i = y_k$ comme ce dernier est manifestement positif, nous en déduisons l'existence de $a \in A$ et de $\sigma(k)$ tels que $y_k = ax_{\sigma(k)}$. $\square$

Ce théorème se généralise à tous les espaces équipés d'une fonctions de poids, voir [**198**].

LEMMULE 12.1. *Soient M un A-module libre. Chaque caractère $\chi \in A^+$ permet de définir un homomorphisme du groupe M^* (dual linéaire) vers le groupe $\widehat{M}$*

$$M^* \to \widehat{M}$$
$$\pi \mapsto \chi \circ \pi$$

qui est un isomorphisme si et seulement si χ est admissible.

PROPOSITION 12.2. *Soient A un anneau quasi-Frobenius et χ un caractère admissible. Le produit scalaire usuel de A^n permet d'identifier A^n avec $\widehat{A^n}$ en posant $\chi_a(x) = \chi(a.x)$. Pour tout sous-module M de A^n on a :*

$$M^\perp = \{\chi_u \mid u \perp M\}.$$

13. Transformée de Fourier rapide

Un algorithme de transformée de Fourier rapide est un algorithme qui calcule les transformée de Fourier de façon efficace. Les algorithmes de transformée de Fourier Rapide sont utilisés dans des situations variées, par exemple : résolution d'équations différentielles, produit d'entiers, produit de polynômes, décodage de codes, compression des images etc... Dans cette section, nous présentons les algorithmes de transformées rapides de Fourier d'un groupe d'ordre 2^m dans deux situations diamétralement opposées : le cas du groupe cyclique $\mathbf{Z}/2^m\mathbf{Z}$, et le cas du groupe élémentaire $\mathbf{F}_2^m$.

13.1. Cas d'un groupe cyclique. Posons $n = 2^m$. Une fonction complexe définie sur le groupe $\mathbf{Z}/n\mathbf{Z}$ est représentée par un tableau de nombres complexes indexé par les entiers compris entre 0 et $n-1$. L'application $j \mapsto \chi_j$, avec $\chi_j(x) = \exp(2i\pi j/n)$, permet d'identifier G et son dual. On commence par écrire un algorithme récursif (FIG. 1) qui calcule la transformée de Fourier d'une fonction f définie sur le groupe $\mathbf{Z}/n\mathbf{Z}$. On suppose que la primitive DIVISER permute les valeurs du tableau f, de sorte que : si $f[2i] = a$ et $f[2i+1] = b$ alors après l'exécution de DIVISER(f, n) on a : $f[i] = a$ et $f[i + \frac{n}{2}] = b$. En d'autres termes les contenus des cellules d'index pairs glissent vers la gauche, et les contenus de celles d'index impairs vers la droite.

La correction de l'algorithme résulte du calcul :

$$\hat{f}(a) = \sum_{k=0}^{n-1} f(k)\zeta_n^{ak} = \sum_{k=0}^{\frac{n}{2}-1} f(2k)\zeta_{\frac{n}{2}}^{ak} + \zeta_n^a \sum_{k=0}^{\frac{n}{2}-1} f(2k+1)\zeta_{\frac{n}{2}}^{ak}$$

qui montre que l'on peut reconstituer la transformée de Fourier de f en fonction des transformées de Fourier des fonctions g et h définies sur $\mathbf{Z}/(\frac{n}{2})$ par $g(k) = f(2k)$ et $h(k) = f(2k+1)$. Si a est un entier inférieur strictement à $\frac{n}{2}$ alors

$$\hat{f}(a) = \widehat{g}(a) + \hat{h}(a)\zeta_n^a, \quad \hat{f}(a + \frac{n}{2}) = \hat{g}(a) - \hat{h}(a)\zeta_n^a. \tag{20}$$

Sans difficulté, la complexité de l'algorithme FOURIERCYCLIQUE est $\Theta\big(n\log(n)\big)$. Pour supprimer la récursivité, il faut interpréter l'action de l'algorithme sur la table f de la façon suivante. Tout d'abord les appels successifs de DIVISER échangent les contenus des cellules de la table f. Plus précisément, le contenu de la cellule d'index $i = i_0 2^0 + i_1 2^1 + i_2 2^2 + \dots i_{m-1}2^{m-1}$ est échangé avec celui de la cellule d'index $m(i) = i_0 2^{m-1} + i_1 2^{m-2} + i_2 2^2 + \dots i_{m-1}2^0$. L'algorithme termine en m étapes, l'étape $i = 0, 1, \dots$ faisant interagir la cellule d'index j avec celle d'index $j + 2^i$, voir le « dé-mélange parfait » page 608 de l'ouvrage [**168**].

13.2. Le cas élémentaire. Une fonction définie sur le groupe $\mathbf{F}_2^m$ est représentée par un tableau de longueur 2 indexé par les entiers compris entre 0 et $n-1$. L'image de x est placée dans la cellule d'index $x_0 2^0 + x_1 2^1 + \dots + x_{m-1}2^{m-1}$. Nous identifions G et son dual par l'intermédiaire de l'application $j \mapsto \chi_j$, avec $\chi_j(x) = (-1)^{j_0x_0 + j_1x_1 + \cdots + j_{m-1}x_{m-1}}$. L'égalité

$$\sum_{x \in \mathbf{F}_2^m} f(x)\chi_j(x) = \sum_{x \in \mathbf{F}_2^{m-1}} f(x,0)(-1)^{\sum_{i=0}^{m-2} j_i x_i} + (-1)^{j_{m-1}} \sum_{x \in \mathbf{F}_2^{m-1}} f(x,1)(-1)^{\sum_{i=0}^{m-2} j_i x_i}$$

```
Algorithme FourierCyclique(f, n);
 adresse
        f   :  une fonction;
 valeur
        n   :  entier ( une puissance de 2);
 locale
        i   :  indice;
    a, z, t :  complexe;
  debut
    si (n > 1)
      alors
        Diviser(f, n);
        FourierCyclique(f, n/2);
        FourierCyclique(f + n/2, n/2);
        z ←  la racine n-ième principale;
        a ←  1;
        i ←  0;
        tant que (i < n/2)
          faire
            t ←  f[i];
            f[i]←  t + a ∗ f[i + n/2];
            f[i+n/2] ←  t−a∗f[i+n/2];
            a ←  a ∗ z;
            i ←  i + 1;
        ftq
    fsi
  fin
```

FIG. 1. Transformée de Fourier d'un groupe cyclique

permet d'écrire un élégant code (FIG. 2) en langage C de complexité $\Theta(n\log(n))$; La suppression de la récursivité conduit à l'algorithme de transformée rapide de Fourier (FIG. 3).

14. Jeu de Fourier

Le lecteur qui souhaite se faire une idée de la nature des problèmes que je cherche à résoudre, sans pour autant rentrer dans les détails techniques doit s'essayer au « casse-tête » que j'appelle le jeu de Fourier. Pour jouer au jeu de Fourier de niveau m (m est un entier), on place $m+1$ rangées de 2^m cellules. Les cellules d'une rangée sont reliées par paires à celles de la la rangée suivante par l'intermédiaire de processeurs qui ne sont pas représentés sur la figure (FIG. 4). Chaque processeur lit dans les cellules supérieures et écrit dans les cellules inférieures. Si x est la valeur de la cellule supérieure de gauche et y celle de droite alors le processeur écrit $x-y$ dans la cellule inférieure de droite et $x+y$ dans celle de gauche.

PROBLÈME 14.1. *Comment faut-il initialiser les cellules de la première rangée avec des $+1$ et des -1 pour minimiser la valeur maximale en sortie ? Combien y-a-t-il de solutions ?*

```
void FourierElementaire(int *f, int n)
  {
    int x, tempo;
    if ( n > 1 )
        {
          FourierElementaire(f, n/2);
          FourierElementaire(&f[n/2], n/2);
          for ( x=0 ; x < n/2 ; x++)
            {
              tempo = f[x];
              f[x] = tempo + f[y];
              f[y] = tempo - f[y];
            }
        }
  }
```

FIG. 2. Transformée de Fourier du 2-groupe

```
Algorithme FourierRapide(f, n);
  adresse
       f  :  une fonction;
  valeur
       n  :  entier;
  locale
     i, d :  indice;
       t  :  entier;
   debut
     d ← 2;
     tant que (d < n)
       faire
         i ← 0;
         tant que (i < n)
           faire
             t ← f[i + d − 1];
             f[i + d − 1] ← f[i] − t;
             f[i] ← f[i] + t;
             i ← i + d;
         ftq
         d ← 2 ∗ d;
     ftq
   fin
```

FIG. 3. Transformée de Fourier Rapide

Le lecteur vérifiera que l'initialisation : $+1$, $+1$, $+1$, -1, $+1$, $+1$, $+1$, -1, $+1$, $+1$, $+1$, -1, -1, -1, -1, $+1$ est une solution du Jeu de Fourier de niveau 4. Pour m impair, le jeu est d'une redoutable difficulté. Pour m pair, il est facile. Le jeu de

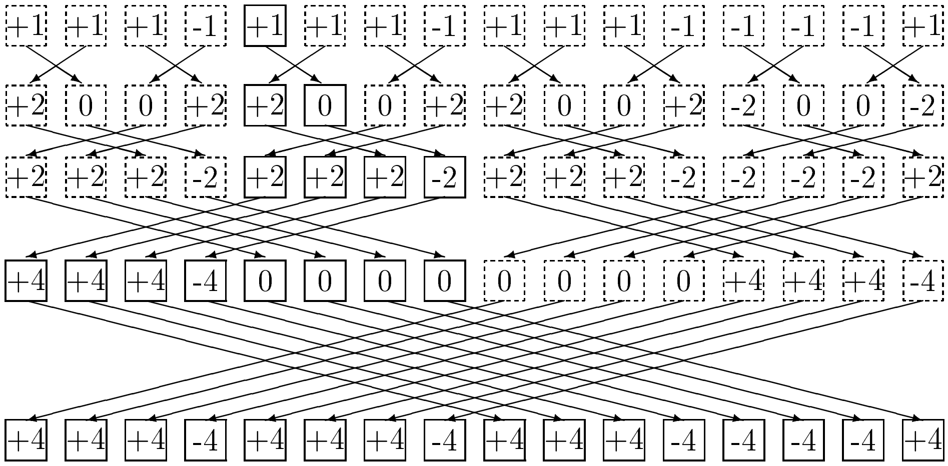

FIG. 4. Le jeu de Fourier de niveau 4

Fourier équilibré est une variante qui consiste à rechercher la meilleure des initialisations contenant autant de $+1$ que de -1 est un véritable « casse-tête » que l'on ne sait pas résoudre à partir du niveau 8. Cela tient du fait que d'une part, les solutions sont rares, et d'autre part, il est impossible de converger vers une solution : si on change le contenu d'une cellule, à l'arrivée, toutes les cellules seront affectées.

PROBLÈME 14.2. *Etudier les variantes de ce jeu, en faisant varier les connexions, et la fonction des processeurs.*

PROBLÈME 14.3. *Le jeu de Fourier est un cas trés particulier, d'une question générale qu'on peut poser pour un groupe localement compact G muni de sa mesure de Haar* $\mathrm{d}\mu$. *Pour chaque fonction f définie et intégrable sur G^m, la transformée de Fourier de f vaut* $\widehat{f}(\chi) = \int_{x \in G^m} f(x)\chi(x)\mathrm{d}\mu^m(x)$, *dans cette expression χ est un caractère produit. Que vaut* $\inf_f \sup_\chi |\widehat{f}(\chi)|$, *sur l'ensemble des fonctions à valeurs dans le cercle unité ?*

CHAPITRE 2

Sommes de Gauss

Dans le fameux *disquisitiones arithmeticae*, C.F. Gauss (1777—1855) prouve qu'un polygone régulier est constructible à la règle et au compas si et seulement si le nombre de ses côtés est un produit de nombres premiers de Fermat. La démonstration de ce théorème repose sur l'étude des périodes et des équations qui déterminent les sections angulaires, tout cela est dans la section VII de son mémoire. Ces périodes sont les ancêtres de ce que l'on appelle maintenant les sommes de Gauss. En particulier, les sommes quadratiques de Gauss sont d'une telle importance dans la théorie des séquences que j'ai décidé de rapporter point par point les sections 356 et 357 de son ouvrage. L'enthousiasme de Gauss vis-à-vis des nombres et de leurs propriétés y est très communicatif ! Aujourd'hui, les sommes de Gauss permettent de construire des séquences utilisées dans le domaine des télécommunications. Ce transfert d'une question de mathématiques pures vers une application concrète de la théorie du signal aurait enthousiasmé ce précurseur des ondes électromagnétiques qu'était C.F. Gauss. C'est pour nous, l'occasion de constater, une fois de plus, l'importance de la recherche fondamentale.

Dans ce chapitre, le calcul de la somme quadratique illustre l'efficacité de la théorie de la ramification et la théorie de Galois. Le problème de la détermination du signe de cette somme est un problème redoutable. On le résoud en faisant apparaître les sommes de Gauss comme des valeurs propres de l'opérateur de Frobenius. Heureusement, la complexité du calcul d'une somme de Gauss n'est pas une fonction croissante de l'ordre des caractères qu'elle met en jeu. L'action du groupe de Galois cyclotomique sur les sommes de Gauss et les congruences de Stickelberger nous renseignent sur les conditions qu'il faut imposer à nos paramètres pour que ces sommes soient rationnelles ou quadratiques. L'élégante relation de Hasse-Davenport relie une somme de Gauss à celle des caractères relevés. L'aspect géométriques des sommes de Gauss est abordé. Le comportement archimédien des sommes de Gauss généralisées est étudié dans le cas des anneaux quasi-Frobenius.

1. Les points 356 et 357

On doit surtout remarquer les équations auxiliaires par lesquelles on détermine, pour une valeur quelconque de n les sommes des périodes qui forment l'ensemble Ω : elles sont liées d'une manière étonnante avec les propriétés les plus abstraites du nombre n. Mais ici nous restreindrons nos considérations aux deux cas suivants : 1) à l'équation du second degré qui donne les équations des périodes de $\frac{n-1}{2}$ termes ; 2) quand $n-1$ est divisible par 3, à l'équation du troisième degré qui donne les sommes des périodes de $\frac{n-1}{3}$ termes.

Les notations se Gauss sont les suivantes : n est un entier premier impair, Ω l'ensemble des racines n-ième de l'unité. lorsque $n-1 = ef$, Gauss note (f, λ) la "période"

$$[\lambda g], [\lambda g^2], \dots [\lambda g^{f-1}]$$

où λ est non nul et g est un élément d'ordre f modulo n. Il confond aussi l'ensemble (f, λ) avec la somme de ses éléments.

Faisons, pour abréger, $\frac{1}{2}(n-1) = m$, *et désignons par* g *une racine primitive quelconque,* Ω *sera composé de deux périodes* $(m, 1)$ *et* (m, g) *; la première contenant* $[1], [g^2], \ldots [g^{n-3}]$, *et la seconde* $[g], [g^3], \ldots [g^{n-2}]$. *Supposons que les résidus minima positifs des nombres* $[g^2], [g^4], \ldots [g^{n-3}]$ *suivant le module* n, *soient* R, R', R'', *etc. abstraction faite de l'ordre, et que les résidus des nombres* $[g], [g^3], \ldots [g^{n-2}]$, *soient* N, N', N'', *etc.; les racines des périodes* $(m, 1)$ *et* (m, g) *coïncideront avec*

$$R, R', R'', \text{etc.}\; N, N', N'', \text{etc.}$$

respectivement. Or il est clair que tous les nombres $1, R, R', R''$, *etc. sont résidus quadratiques de* n *; comme ils sont différents, moindres que* n *et au nombre de* $\frac{n-1}{2}$, *il s'en suit que ceux sont effectivement tous les résidus quadratiques de* n, *positifs et plus petit que lui (n. 96). Il suit de là en même temps, que les nombres* N, N', N'', *etc. qui sont tous différents entre eux, et des nombres* $1, R, R', R''$, *etc.; et qui, joint à ces derniers, épuisent les nombres* $1, 2, 3, \ldots, n-1$, *sont tous les non résidus quadratiques positifs plus petit que lui. Si l'on suppose maintenant que l'équation dont* $(m, 1)$ *et* (m, g) *sont racines, soit*

$$x^2 - Ax + B = 0$$

on a $A = (m, 1) + (m, g) = -1$, *et* $B = (m, 1) \times (m, g)$ *; or (n. 345),*

$$(m, 1) \times (m, g) = (m, N+1) + (m, N'+1) + (m, N''+1) + \text{etc.} = W$$

et peut par conséquent être mis sous la forme $\alpha(m, 0) + \beta(m, 1) + \gamma(m, g)$. *Pour déterminer les coefficients* α,β,γ, *observons : 1) qu'on a* $\alpha + \beta + \gamma = 0$, *puisque le nombre des périodes de* W *est* m *; 2) que* $\beta = \gamma$ *(n. 350), puisque* $(m, 1) \times (m, g)$ *est une fonction invariable des sommes* $(m, 1)$ *et* (m, g) *qui composent la période plus grande* $(n-1, 1)$ *; 3) que tous les nombres* N, N', N'', *etc. étant compris entre 2 et* $n+1$, *il est clair que nulle période de* W *ne coïncidera avec* $(n, 0)$, *ou qu'il y en aura qu'une, par exemple* (m, n) *; on aura donc* $\alpha = 1$, *ou* $\alpha = 0$, *suivant que* $n-1$ *sera ou ne sera pas parmi les nombres* N, N', N'', *etc.; il suit de là que dans le premier cas on aura* $\alpha = 1$, $\beta = \gamma = \frac{m-1}{2}$ *et dans le second cas* $\alpha = 0$, $\beta = \gamma = \frac{m}{2}$ *; et comme* β *et* γ *doivent être entiers, le premier cas aura lieu, c'est à dire que* $n-1$ *ou* -1 *se trouvera parmi les non-résidus de* n *lorsque* m *sera impair, c'est à dire que* n *sera de la forme* $4n+3$ *; le second aura lieu au contraire quand* m *sera pair, c'est à dire quand* n *sera de la forme* $4n+1$. *Ainsi, comme* $(m, 0) = m$, *et* $(m, 1) + (m, g) = -1$ *; le produit cherché sera donc, suivant les mêmes circonstances,* $\frac{1}{2}(m+1)$, *ou* $\frac{-1}{2}m$, *et l'équation sera, dans le premier cas,*

$$x^2 + x + \frac{1}{4}(n+1) = 0,$$

qui donne $x = -\frac{1}{2} \pm \frac{1}{2}i\sqrt{n}$ *et dans le second*

$$x^2 + x - \frac{1}{4}(n-1) = 0,$$

qui donne $x = -\frac{1}{2} \pm \frac{1}{2}\sqrt{n}$. *Ainsi, quelle que soit la racine que l'on ait prise pour* $[1]$, *si l'on désigne* $\sum[R]$ *la somme de toutes les racines* $[1]$,$[R]$,$[R']$,*etc. et par* $\sum[N]$ *celle des racines* $[N]$,$[N']$,*etc. On aura*

$$\sum[R] - \sum[N] = \pm\sqrt{N}, \quad \text{ou} \quad \pm\, i\sqrt{N}$$

suivant que $n \equiv 1$ ou $n \equiv 3$ (mod.4), Il suit facilement de là que k étant un nombre entier quelconque non divisible par n, on a

$$\sum \cos \frac{kRP}{n} - \sum \cos \frac{kNP}{n} = \pm\sqrt{n} \quad ou \quad 0$$
$$\sum \sin \frac{kRP}{n} - \sum \sin \frac{kNP}{n} = 0 \quad ou \quad \pm\sqrt{n}$$

suivant que $n \equiv 1$ ou $n \equiv 3$ (mod. 4), théorèmes remarquables par leur élégance. Au reste, nous ferons observer que le signe supérieur a lieu quand k est l'unité, ou plus généralement quand k est un résidu quadratique de n, et le signe inférieur, quand k est non-résidus. Ces théorèmes conservent toute leur élégance, ou plutôt en acquièrent encore davantage, lorsque n est un nombre composé quelconque; mais nous sommes forcés de supprimer ces recherches qui demanderaient trop de développement, et de les réserver pour une autre occasion.

2. Sommes quadratiques de Gauss

Soit n un entier impair, notons ζ_n la racine n-ième principale. La somme trigonométrique $\sum_{k=0}^{n} \zeta_n^{k^2}$ est appelée *somme quadratique* de Gauss. Du théorème qui vient d'être démontré dans la section précédente,

$$\sum_{k=0}^{n} \zeta_n^{k^2} = \begin{cases} \pm\sqrt{n}, & \text{si } n \equiv 1 \pmod 4\,; \\ \pm\sqrt{-n}, & \text{si } n \equiv 3 \pmod 4. \end{cases} \tag{21}$$

Donnons-en une preuve arithmétique, c'est-à-dire sans calcul! Notons κ_n la somme quadratique de Gauss. L'action du groupe de Galois du corps cyclotomique $\mathbf{Q}(\zeta_n)$ montre que κ_n est un entier quadratique,

$$\mathbf{Q} \subset \mathbf{Q}(\kappa_n) \subset \mathbf{Q}(\zeta_n)$$

La théorie de Galois montre qu'il existe un et un seul sous-corps quadratique dans $\mathbf{Q}(\zeta_n)$, et la théorie de la ramification montre qu'il s'agit du corps quadratique $\mathbf{Q}(\sqrt{n^\star})$, où $n^\star = (-1)^{(n-1)/2}n$. De plus, le module du nombre complexe κ_n est n, et comme le corps quadratique $\mathbf{Q}(\sqrt{n^\star})$ ne possède que deux racines de l'unité :

$$\kappa_n = \pm\sqrt{n^\star}.$$

Il reste le fameux problème de la détermination du signe! Gauss montre dans sa publication *summatio quaraumdam serierum singularium* que le signe « plus » vaut dans les deux cas. C'est remarquable. Le lecteur trouvera la preuve originale de Gauss dans [**9**]. La section qui vient, reproduit partiellement la preuve instructive proposée par H. Niederreiter et R. Lidl dans leur fameux *Finite Fields*.

3. Détermination du signe

Par multiplicativité, on peut supposer n premier. Mais signalons la forme plus générale qui vaut sur une extension de degré s du corps fini à p éléments

$$-G_{\mathbf{F}_{p^s}}(\nu) = \begin{cases} (-1)^s\sqrt{p^s}, & \text{si } p^s \equiv 1 \pmod 4\,; \\ (-1)^s\sqrt{-p^s}, & \text{si } p^s \equiv 3 \pmod 4. \end{cases} \tag{22}$$

La détermination du signe est basée sur la démonstration de l'identité :

$$(-1)^{\frac{p-1}{2}} p^{\frac{p-3}{2}} G_{\mathbf{F}_p}(\nu) = (2\sqrt{-1})^{\frac{(p-1)(p-2)}{2}} \prod_{1\leq i<j\leq p-1} \sin\big(\frac{(j-i)\pi}{p}\big) \tag{23}$$

qui résume à elle seule la difficulté du problème. Heureusement, les problèmes de détermination de signe ne sont pas toujours aussi délicat. Dans la suite, nous supposons $p > 3$. Soit $\mathcal{F}$ l'opérateur de Fourier qui envoie la fonction complexe f sur la fonction complexe $F.f$ définie par :

$$\mathcal{F}.f(z) = \sum_{x\in{\mathbf{F}_p}^\times} f(x)\zeta_p^{xz}$$

où comme d'habitude, ζ_p désigne la racine principale d'ordre p. L'égalité s'obtient en calculant le déterminant de l'opérateur de Fourier dans deux bases adéquates. Notons ψ le caractère additif canonique de $\mathbf{F}_p$, pour tout caractère multiplicatifs χ de $\mathbf{F}_p$, on a :

$$\mathcal{F}.\chi = G_{\mathbf{F}_p}(\chi,\psi)\bar{\chi}.$$

Soit θ un générateur de $\widehat{{\mathbf{F}_p}^\times}$, de la relation $G_{\mathbf{F}_p}(\chi,\psi)G_{\mathbf{F}_p}(\bar{\chi},\psi) = \chi(-1)p$, on tire que le déterminant de $\mathcal{F}$ dans la base des caractères vaut :

$$\begin{aligned}\det(\mathcal{F}) &= G_{\mathbf{F}_p}(1,\psi)\prod_{j=1}^{\frac{p-3}{2}} \theta^j(-1)p^{\frac{p-3}{2}} G_{\mathbf{F}_p}(\nu,\psi)\\ &= \nu(-1)p^{\frac{p-3}{2}} G_{\mathbf{F}_p}(\nu,\psi)\end{aligned}$$

Dans la base des fonctions de Dirac, c'est-à-dire les indicatrices des singletons, on a $\mathcal{F}.\delta_j(t) = \zeta_p^{jt}$, soit :

$$\mathcal{F}.\delta_j = \sum_{i=1}^{p-1} \zeta_p^{ij}\delta_i$$

La matrice de F dans cette base vaut :

$$\begin{pmatrix} \zeta_p^1 & \zeta_p^2 & \dots & \zeta_p^{p-1}\\ \zeta_p^2 & \zeta_p^4 & \dots & \zeta_p^{2(p-1)}\\ \vdots & \vdots & \ddots & \vdots\\ \zeta_p^{p-1} & \zeta_p^{2(p-1)} & \dots & \zeta_p^{(p-1)^2}\end{pmatrix}$$

Factorisons ζ_p^1 dans la première colonne, puis ζ_p^2 dans la seconde, puis ζ_p^3 dans la troisième etc... Le miracle s'accomplit nous obtenons une matrice de Vandermonde dont on sait très bien calculer le déterminant [1] ;

$$\det(F) = \zeta_p^{1+2+\cdots+(p-1)} \prod_{1\leq i<j\leq p-1} (\zeta_p^j - \zeta_p^i)$$

Quelques petits calculs sont encore nécessaires pour arriver à la formule (23) : identités remarquables, formule d'Euler, sommes des carrés, et peut-être bien qu'un bachelier astucieux pourrait terminer la preuve...

[1]Le parisien Alexandre Théophile Vandermonde (1735–1796) est bien moins connu que le déterminant. Ce mathématicien qui a commencé sa carrière à 35 ans avec son ami G. Monge, n'a jamais publié à propos de ces matrices et de leur déterminant ! En fait, cette dénomination est due à H. Lebesgue

4. Sommes de Gauss et Jacobi

Considérons K un corps fini de caractéristique p et de cardinal q. Désignons par χ un caractère du groupe multiplicatif de K, et par ψ un caractère du groupe additif de K. Considérons χ comme une fonction de K dans $\mathbf{C}$ prolongée en zéro par la valeur nulle. La valeur de la transformée de Fourier de χ en ψ s'appelle la *somme de Gauss* associée au couple (χ, ψ), elle vaut :

$$G_K(\chi, \psi) = \sum_{x \in K^\times} \chi(x)\psi(x)$$

Lorsque l'un des caractères est trivial, la somme est dite triviale. Supposons que ψ et χ soient non triviaux. Des relations d'orthogonalité, on tire sur le champ que :

$$G_K(1,1) = q-1, \quad G_K(1,\psi) = -1, \quad \text{et} \quad G_K(\chi, 1) = 0. \tag{24}$$

THÉORÈME 4.1. *Soient ψ un caractère additif et χ un caractère multiplicatif. S'ils sont non-triviaux alors la somme de Gauss $G_K(\chi, \psi)$ est de module $\sqrt{q}$.*

Pour la preuve, multipliez cette somme de Gauss par son conjugué complexe, changez de variables et appliquez les relations d'orthogonalité. Derrière la simplicité de ces calculs se cachent l'un des résultats les plus profonds de la théorie des courbes algébriques. Mais nous n'en sommes pas là, alors continuons avec des choses élémentaires.

La somme de Gauss $G_K(\chi, \psi)$ est une somme de racines de l'unités d'ordre diviseur de $p(q-1)$, c'est un entier du corps cyclotomique $\mathbf{Q}(\zeta_p, \zeta_{q-1})$. Le groupe de Galois de ce corps est isomorphe au produit $\big(\mathbf{Z}/(q-1)\mathbf{Z}\big)^* \times {\mathbf{F}_p}^\times$, et l'action de l'élément $\sigma(u,v)$ est déterminé par :

$$\sigma(u,v)(\zeta_p) = \zeta_p^v, \qquad \sigma(u,v)(\zeta_{q_1}) = \zeta_{q-1}^u.$$

De sorte que, $\sigma(u,v)\big(G_K(\chi,\psi)\big) = G_K(\chi^u, \psi^v)$. En particulier, si ψ est égal au caractère additif canonique de K, on obtient :

$$\sigma(u,v)\big(G_K(\chi,\psi)\big) = \bar{\chi}(v) G_K(\chi, \psi). \tag{25}$$

LEMMULE 4.1. *Soit χ un caractère multiplicatif d'ordre m, trivial sur ${\mathbf{F}_p}^\times$. Le degré algébrique de $G_K(\chi,\psi)$ divise l'indice du groupe engendré par p dans $(\mathbf{Z}/m\mathbf{Z})^\star$.*

DÉMONSTRATION. C'est une application directe de la théorie de Galois. □

Les notions de transformée de Fourier et de convolution vont de paire. Le produit de convolution de deux caractères multiplicatifs χ et χ' calculé en 1 est une *somme de Jacobi*

$$J(\chi, \chi') = \chi * \chi'(1) = \sum_{x+y=1} \chi(x)\chi'(y)$$

Si τ est non-nul alors $\chi * \chi'(\tau) = \bar{\chi}(\tau)\bar{\chi}'(\tau)\chi * \chi'(1)$. En particulier, si $\chi\chi'$ n'est pas trivial

$$G_K(\chi)G_K(\chi') = G_K(\chi\chi')J(\chi,\chi') \tag{26}$$

5. Relation de Davenport-Hasse

Soit $\mathrm{Poly}(K)$ l'ensemble des polynômes unitaires à coefficients dans K, et soit $\mathrm{Place}(K)$ la partie de $\mathrm{Poly}(K)$ composée des polynômes irréductibles. Pour chaque polynôme $P(X) = a_0 + a_1X + \cdots + a_{k-1}X^{k-1} + X^k$, notons $f(P) = \chi(a_0)\psi(a_{k-1})$. La série formelle :

$$Z(K,T) = \sum_{Q\in\mathrm{Poly}(K)} f(Q)T^{\deg(Q)} = \sum_{k=1}^{\infty}\Big(\sum_{\deg(Q)=k} f(Q)\Big)T^k$$

s'appelle la *fonction zéta* de $K[X]$ associée aux caractères χ et ψ. Le terme constant vaut 1, le terme de degré 1 est égal à la somme de Gauss $G_K(\chi,\psi)$ et les relations d'orthogonalité montrent que tous les autres termes sont nuls. Par ailleurs, l'application f est multiplicative, la série se factorise en un produit eulerien

$$Z(K,T) = 1 + G_K(\chi,\psi)T = \prod_{P\in\mathrm{Place}(K)} \frac{1}{1 - f(P)X^{\deg(P)}}$$

THÉORÈME 5.1 (Davenport-Hasse). *Soit L une extension finie du corps K,*

$$-G_L(\chi\circ \mathrm{N}_{L/K}, \psi\circ \mathrm{tr}_{L/K}) = \big(-G_K(\chi,\psi)\big)^{[L:K]}$$

DÉMONSTRATION. En effet, notons $Z(L,T)$ la fonction zéta associée aux caractères $\chi\circ\mathrm{N}_{L/K}$ et $\psi\circ\mathrm{tr}_{L/K}$. La formule est exponentielle, sans perdre en généralité, on peut supposer que le degré de L sur K, est un entier premier s. Une place de K est inerte ou décomposée en produit de s facteurs dans $L[X]$, et

$$Z(L,T^s) = Z(K,T)^s \times \prod_P \frac{(1 - f(P)T^{\deg(P)})^s}{1 - f(P)^sT^{s\deg(P)})}$$

où le produit porte sur les places inertes. Notons $p(T)$ ce terme « parasite », on constate que $\prod_{\zeta^s=1} p(\zeta T) = 1$, d'où l'on tire la relation du théorème. ☐

6. Congruences de Stickelbeger

Notons $\mathcal{P}_1$, $\mathcal{P}_2$, … $\mathcal{P}_g$ les idéaux premiers au-dessus de p dans l'anneau cyclotomique $\mathbf{Z}[\zeta_p,\zeta_{q-1}]$, on sait que :

$$(p) = \mathcal{P}_1^{p-1}\mathcal{P}_2^{p-1}\dots\mathcal{P}_g^{p-1}$$

Les relations d'orthogonalité montrent que les sommes de Gauss relatives aux caractères non-triviaux sont des nombres complexes de module q. En conséquence, l'idéal principal engendré une somme de Gauss est un produit des $\mathcal{P}_i$. L'objet de cette section est de préciser cette décomposition.

Désignons par $\mathcal{P}$, l'un des idéaux au-dessus de p, et notons $\omega_{\mathcal{P}}$ le caractère de Teichmüller attaché à $\mathcal{P}$, c'est le caractère multiplicatif d'ordre $q-1$ du corps quotient $K = \mathbf{Z}[\zeta_p,\zeta_{q-1}]/\mathcal{P}$ qui envoie la classe de ζ_{q-1} sur ζ_{q-1}.

Soit a un entier rationnel, notons $a_0 + a_1p^1 + \cdots + a_{f-1}p^{f-1}$ la décomposition p-adique du résidu de a modulo $q-1$. Nous aurons besoin des deux petites fonctions arithmétiques :

$$S_p(a) = \sum_{i=0}^{f-1} a_i, \qquad R_p(a) = \prod_{i=0}^{f-1} a_i!$$

LEMMULE 6.1. *Pour tout entier a, on a :*

$$S_p(a)+S_p(-a) = (p-1)f, \qquad \mathrm{ord}_p(a!) = \frac{a - S_p(a)}{p-1} \qquad R_p(a)R_p(-a) \equiv -1 \pmod p.$$

THÉORÈME 6.1 (Congruences de Stickelberger). *Soit a un entier rationnel. Alors*

$$-G_K(\omega^{-a}, \mu_K) \equiv \frac{(\zeta_p - 1)^{S_p(a)}}{R_p(a)} \pmod{\mathcal{P}^{(p-1)S_p(a)+1}}.$$

DÉMONSTRATION. On peut faire une démonstration par récurrence sur la valeur de $S_p(a)$ qui utilise la relation de Hasse-Davenport et les sommes de Jacobi, voir par exemple [**114**]. □

Dans l'algèbre de groupe $\mathbf{Q}[(\mathbf{Z}/(q-1)\mathbf{Z})^\star]$, on introduit l'élément de Stickelberger

$$\theta(a) = \sum_{t \in (\mathbf{Z}/(q-1)\mathbf{Z})^\star} \langle \frac{at}{q-1} \rangle \sigma_t^{-1}$$

COROLLAIRE 6.1 (Décomposition de Stickelberger). *Quel que soit a dans* $[0, q-1]$, *l'élément* $(p-1)\theta(a)$ *est dans l'anneau de groupe* $\mathbf{Z}[(\mathbf{Z}/(q-1)\mathbf{Z})^\star]$ *et de plus, on a l'égalité d'idéaux :*

$$G_K(\omega_{\mathcal{P}}^{-a}) = \mathcal{P}^{(p-1)\theta(a)} = \mathcal{P}^{\sum_r S(ra)\sigma_r^{-1}},$$

où r décrit un système de représentants des classes cyclotomiques de $(\mathbf{Z}/(q-1)\mathbf{Z})^\star$ *modulo p.*

7. Interprétation géométrique des sommes de Gauss

Soit X une courbe algébrique de genre g définie sur $\mathbf{F}_q$, on note A_n le nombre de diviseurs positifs de degré n, A_1 est égal aux nombres de points rationnels de X. La fonction zéta de X

$$Z_X(T) = \sum_{n \geq 0} A_n T^n$$

est une série convergente sur $D(0, \frac{1}{q})$, où elle est rationnelle. Il existe un polynôme à coefficients entiers tel que

$$Z_X(T) = \frac{L(T)}{(1-T)(1-qT)}.$$

Le degré de L est égal à $2g$ et le théorème de Hasse-Weil affirme que les α_i sont des entiers algébriques de module $\sqrt{q}$. De plus, le nombre de points de X sur ${\mathbf{F}_q}^s$ est donné par :

$$A_s = q^s + 1 - \sum_{i=1}^{2g} \alpha_i^s$$

Cette égalité plus certaines considérations sur les entiers algébriques α_i conduisent alors à l'estimation de Hasse-Serre-Weil :

$$|N_s - (q^s + 1)| \leq 2[g\sqrt{q^s}]$$

Soit K le corps à q éléments et d un diviseur de $q-1$. Nous allons montrer que les sommes de Gauss non-triviales attachées aux caractères multiplicatifs d'ordre d sont les zéros du numérateur de la fonction zéta de la courbe d'Artin-Schreier d'équation

$$y^q - y = x^d$$

Notons L le corps à q^s élément, $N_s(a)$ le nombre de points affines (sur L) de l'ouvert $x \neq 0$, et $N_s(\infty)$. Utilisons la méthode des sommes de caractères,

$$\begin{aligned} N_s(a) &= \frac{1}{q^s} \sum_{\psi \in \widehat{L^+}} \sum_{x \in L^\times} \sum_{y \in L} \psi(x^d - y^q + y) = \sum_{\psi \in \widehat{K^+}} \sum_{x \in L^\times} \psi \circ \mathrm{tr}_{L/K}(x^d) \\ &= \sum_{\psi \in \widehat{K^+}} \sum_{\chi^d = 1} \sum_{x \in L^\times} \psi(x)\chi(x) = \sum_{\psi \in \widehat{K^+}} \sum_{\chi^d=1} G_L(\chi, \psi \circ \mathrm{tr}_{L/K}) \\ &= \sum_{\psi \neq 1} \sum_{\chi \neq 1} G_K(\chi \circ \mathrm{N}_{L/K}, \psi \circ \mathrm{tr}_{L/K}) + q^s - 1 \end{aligned}$$

La relation de Daventport-Hasse montre que le nombre total de points A_s vérifie :

(27)
$$A_s - (q^s + 1) = N_s(a) + N_s(\infty) - q^s - 1 = \sum_{\psi \neq 1} \sum_{\chi \neq 1} \big(G_K(\chi, \psi)\big)^s + N_s(\infty) - 1$$

Une égalité montrant que le modèle lisse de la courbe Artin-Schreier (7) possède un seul point à l'infini, que les Gauss les inverses des zéros du numérateur de la fonction zéta et que son genre vaut $\frac{(q-1)(d-1)}{2}$. Bien entendu, on peut calculer le genre de cette courbe d'une façon plus... canonique. Par exemple, en utilisant la formule d'Hurwitz :

$$2(g' - 1) = 2(g - 1)([F' : F]/[K' : K]) + \mathrm{Diff}(F'/F)$$

qui relie le genre g' d'une extension F' d'un corps de fonction F de genre g, K' et K sont les corps de constantes correspondants, et $\mathrm{Diff}(F'/F)$ est la différente de l'extension F'/F, que l'on calcule à l'aide de la formule :

$$\mathrm{Diff}(F'/F) = \sum_{P'} v_P\big(\varphi'_P(t_P)\big)$$

t_P est une uniformisante en la place P de F, φ_P le polynôme minimal d'une uniformisante $t_{P'}$ de la place P' au-dessus de P. Considérons la courbe d'équation $y^p \pm y = x^d$. D'une manière générale, dans la formule de la différente, la contribution des places non ramifiées est nulle. Dans l'extension $K(x, y)$ de $K(x)$, seule la place à l'infinie se ramifie, et , totalement puisque p est un nombre premier. Désignons par v_∞ la valution à l'infinie du corps F' : $pv_\infty(y) = dv_\infty(x)$. Les entiers p et d sont premiers entre eux, il existe deux entiers u et v tel que $pu + dv = 1$, et donc $t_\infty = y^u x^v$ est une uniformisante en ∞. Notons $P(T)$ le polynôme minimal de cette dernière. Les conjugués de t_∞ sont les $(y + a)^u x^v$, où a varie dans $\mathbf{F}_p$, de sorte que,

$$\varphi_\infty(T) = \prod_{a \in \mathbf{F}_p} \big(T - (y + a)^u x^v\big)$$

Ainsi,

$$\varphi'(t_\infty) = (-x)^{(p-1)v} \prod_{a \in \mathbf{F}_p{}^\times} \big(y^u - (y + a)^u\big)$$

est de valuation

$$(p-1)(vv_\infty(x)+(u-1)v_\infty(y))=(p-1)(d+1).$$

Pour terminer, il faut considérer la suite de corps définie par les équations $y_1^p-y_1=x^d$, $y_2^p-y_2=y_1$, ... , $y_s^p-y_s=y_{s-1}$, à chaque étapes une seule place se ramifie, et on vérifie sans mal que le corps $K(y_i)$ est de genre $\frac{(p^i-1)(d-1)}{2}$, d'où le résultat.

8. Sommes de Gauss rationnelles

Commençons par écrire une formule de Poisson une situation très particulière. Désignons par K un corps fini, par L une extension finie de K et par Γ l'orthogonal de $K^\times$ dans $L^\times$. On a :

$$\begin{aligned}\sum_{\chi\in\Gamma} G_L(\chi,\mu_L)\bar\chi(z) &= [L^\times:K^\times]\sum_{x\in K^\times}\mu_K(x\mathrm{tr}_{L/K}(z))\\ &= \begin{cases}|L^\times|, & \mathrm{tr}_{L/K}(z)=0\\ -[L^\times:K^\times], & \text{sinon.}\end{cases}\end{aligned}$$

Lorsque Γ et $K^\times$ sont sensiblement de même taille, l'égalité qui précède devient contraignante au point de déterminer les sommes de Gauss.

PROPOSITION 8.1. *Soit L une extension quadratique d'un corps fini K de cardinal q. Soit χ un caractère multiplicatif, générateur de l'orthogonal de $K^\times$. Alors, pour $1\le j\le q$,*

$$G_L(\chi,\mu_L)=\begin{cases}(-1)^j q, & \textit{si } q \textit{ est impair;}\\ q, & \textit{sinon.}\end{cases}$$

DÉMONSTRATION. Choisissons un élément $z\in L$ dont la trace sur K est nulle. Si q est pair, il suffit de prendre 1. Si q est impair alors $z^{q-1}+z=0$, d'où l'on tire $\chi(z)=-1$. Dans les deux cas, on obtient l'égalité :

$$\sum_{j=1}^{q} G_L(\chi^j,\mu_L)\chi^j(z)=q^2$$

En divisant par q, on obtient une somme de q nombres complexes de module 1 qui vaut q, et donc tous ces nombres valent q, c'est le résultat. □

THÉORÈME 8.1. *Soit K un corps à q éléments. Soit χ un caractère multiplicatif d'ordre m divisant $q+1$ dans une extension quadratique L de K. Si q est impair alors, pour $1\le j\le m-1$,*

$$G_L(\chi,\mu_L)=\begin{cases}(-1)^j q, & \textit{si } \frac{q+1}{m} \textit{ est impair;}\\ q, & \textit{sinon.}\end{cases}$$

sinon les sommes de Gauss valent q.

DÉMONSTRATION. C'est une conséquence directe de la proposition qui précède. □

Ainsi, nous avons trouver un sous-groupe Γ du groupe multiplicatifs sur lequel les sommes de Gauss sont toutes rationnelles. Réciproquement, dans [**?**], Baumert, Mills et Ward démontrent à l'aide des périodes cyclotomiques que : si toutes les sommes de Gauss sont rationnelles alors m est semi-primitif modulo m, c'est-à-dire que -1 est dans le groupe engendré par p modulo m. On peut être plus précis :

PROPOSITION 8.2. *Soit* Γ *un sous-groupe du groupe des caractères multiplicatifs sur lequel toutes les sommes de Gauss sont pures* [2] *. Alors les sommes sont rationnelles, et donc* p *est semi-primitif modulo l'ordre de* Γ*.*

DÉMONSTRATION. Grace au théorème de Hasse-Davenport, les sommes de Gauss sont rationnelles dans une extension convenable. □

9. Calcul de certaines sommes de Gauss

Dans l'article mon article *Calculs de certaines sommes de Gauss* [**126**], je calcule des sommes de Gauss de degré 2, généralisant un résultat de Baumert et McEliece.

Soit p et ℓ deux nombres premiers. Soit m une puissance de ℓ, désignons par L le corps des racines de $X^m - 1$ sur $\mathbf{F}_p$. Nous utiliserons les notations

$$\kappa = \frac{-1+\sqrt{-l}}{2}, \quad \text{et} \quad h = \sum_{0<x<\ell} \left(\frac{x}{\ell}\right) x$$

De sorte que, $(1, \kappa)$ est une base de l'anneau des entiers du corps quadratique $Q(\sqrt{-\ell})$ dont le nombre de classe est justement h.

LEMME 9.1. *L'ellipse d'équation* $x^2 - xy + y^2 \frac{\ell+1}{4} = p^h$ *possède une et une seule solution* (a, b) *à coordonnées entières vérifiant : p ne divise pas b, a positif, et* $2a - b \equiv -2p^{\frac{f+h}{2}}$*.*

PROPOSITION 9.1. *Avec les notations qui précèdent Si p engendre les carrés du groupe* $(\mathbf{Z}/m\mathbf{Z})^\star$ *alors il existe un caractère* χ *d'ordre d'ordre* m *tel que :*

$$G_L(\chi) = p^{\frac{f-h}{2}}(a + b\kappa) = p^f g_L(\chi)$$

De plus, et c'est remarquable, si d est un diviseur propre de m,

$$g_L(\chi^d) = g_L(\chi)^d$$

Pour $r = 1$, nous retrouvons le résultat de Baumert et McEliece que j'ai exploité dans un autre article *A New Class of Two Weight codes.*

10. Sommes de Gauss quadratiques

Soient m un entier et p un nombre premier ne divisant pas m. On suppose que le groupe engendré par p est d'indice 2 dans le groupe $(\mathbf{Z}/m\mathbf{Z})^\star$. À la lumière de l'action du groupe de Galois de $\mathbf{Q}(\zeta_m, \zeta_p)$, nous comprenons que les somme de Gauss associées aux caractères du groupe d'ordre m sont obligatoirement quadratiques.

LEMME 10.1. *Si le groupe engendré par p dans* $(\mathbf{Z}/m\mathbf{Z})^\star$ *est d'indice* 2 *alors* m *possède au plus deux facteurs premiers.*

Le cas primaire est traité dans la section précédente. Le cas d'un produit de deux nombres premiers est traité dans [**183**] par Van der Vlugt. Dans cette section, j'expose les résultats de O. Mbodj [**143, 144**] obtenus dans le cas général i.e. m possède deux facteurs premiers ℓ et μ.

$$m = \ell^r \mu^s.$$

Nécessairement, l'un des deux groupes $(\mathbf{Z}/\ell^r\mathbf{Z})^\star$ ou $(\mathbf{Z}/\mu^s\mathbf{Z})^\star$ est cyclique engendré par la classe de p, nous supposerons que c'est le second. Cette hypothèse faite, nous pouvons supposer $\ell \equiv 3 \pmod 4$, pour obtenir l'alternative :

[2]Un nombre algébrique est pur si une de ses puissances est rationnelles

(I) p d'indice 2 dans $(\mathbf{Z}/\ell^r\mathbf{Z})^\star$, avec $\mu \equiv 1, 3 \pmod 4$.

(II) p engendre $(\mathbf{Z}/\ell^r\mathbf{Z})^\star$, et $\mu \equiv 1 \pmod 4$.

Les sommes de Gauss du cas (I), se déduisent du cas résidu quadratique et rationnel. Avec les notations a, b, κ et h introduites dans la section précédente.

THÉORÈME 10.1 (Mbodj). *cas (I). Soit χ un caractère multiplicatif d'ordre m. On suppose que p n'est pas auto-conjugué modulo m. Alors, pour tout $1 \le i \le r$ et $1 \le j \le s$,*

$$G_K(\chi^{\ell^i\mu^j}) = \begin{cases} p^{f/2}\left(\frac{a+b\kappa}{p^{h/2}}\right)^{2\ell^i\mu^j}, & \left(\frac{\mu}{\ell}\right) = -1; \\ p^{f/2}, & \left(\frac{\mu}{\ell}\right) = +1; \end{cases}$$

Pour le cas (II), la somme de Gauss attachée à un caractère d'ordre m vit dans le corps quadratique imaginaire $\mathbf{Q}(\sqrt{\ell\mu})$ dont le nombre de classes est h. Notons $\omega = \frac{1+\sqrt{\ell\mu}}{2}$ et désignons par (a, b) le point à coordonnées entières de l'ellipse $a^2 - ab + \frac{m+1}{4}b^2$ défini par les conditions : p ne divise pas b et $2a - b = 2p^{h/2} \pmod \ell$.

THÉORÈME 10.2 (Mbodj). *cas (II). Soit χ un caractère multiplicatif d'ordre m. On suppose que p n'est pas auto-conjugué modulo m. Alors, pour tout $1 \le i \le r$ et $1 \le j \le s$,*

$$G_K(\chi^{\ell^i\mu^j}) = p^{f/2}\left(\frac{a + b\omega}{p^{h/2}}\right)^{\ell^i\mu^j}.$$

DÉMONSTRATION. La preuve de ces théorèmes n'est pas immédiate, voir [**144**]. □

PROBLÈME 10.1. *Caractériser l'ordre d'un sous-groupe Γ du groupe des caractères multiplicatifs d'un corps fini L dont les sommes de Gauss sont toutes de degré au plus 2.*

11. Sommes de Gauss généralisées

Soit A un anneau fini. Pour chaque homomorphisme χ du groupe multiplicatif de A dans le groupe multiplicatif du corps des nombres complexes, et pour chaque caractère ψ du groupe additif de A, on peut définir une somme de Gauss complète :

$$G_A(\chi, \psi) = \sum_{x \in A^\times} \chi(x)\psi(x)$$

De même, si X désigne une partie quelconque de A, on définit la somme de Gauss incomplète :

$$G_X(\chi, \psi) = \sum_{x \in X \cap A^\times} \chi(x)\psi(x)$$

Je renvoie le lecteur vers les articles de [**2, 1**] qui illustrent le calcul de sommes de Gauss incomplètes relatives au groupe orthogonal. Avant de supposer définitivement la commutativité de A, signalons les travaux de Lamprecht [**113**] sur les *sommes de Gauss* qui sont définies dans le cadre d'une représentation linéaire.

Un anneau fini est somme directe d'anneaux locaux ce qui ramène l'étude des sommes de Gauss à celle des sommes de Gauss sur un anneau local. Dans cette note, j'utilise des méthodes élémentaires pour obtenir des résultats sur le module des sommes de Gauss complètes et incomplètes dans le cas d'un anneau Frobenius local. Dans le cas particulier d'un anneau de Galois, et pour certaines sommes incomplètes, nous obtenons des congruences analogues aux congruences de Stickelberger.

12. Sommes sur un anneau local Frobenius

A partir de maintenant, et jusqu'à la fin A désigne un anneau commutatif, Frobenius, local d'idéal maximal M et de corps résiduel K. Le cardinal de K est q, c'est une puissance d'un nombre premier p.

On suppose que A n'est pas un corps !

$$|A| = q|M|, \quad |A^\times| = (q-1)|M|, \quad q = |K| = |\mathrm{ann}(M)|. \tag{28}$$

La réduction modulo M divise l'ordre des éléments, on en déduit qu'il existe dans A un élément d'ordre $q-1$. De sorte que, la suite exacte :

$$1 \longrightarrow 1+M \longrightarrow A^\times \longrightarrow K^\times \longrightarrow 1$$

se décompose, $A^\times$ possède un groupe cyclique d'ordre $q-1$. Ce groupe est unique puisque l'ordre du p-groupe M est premier avec $q-1$, on le note $T^\times$; c'est le groupe de Teichmüller de A que l'on identifie au groupe $K^\times$. Le groupe $T^\times$ augmenté de 0 forme un système de représentants multiplicatifs de A modulo M ; c'est l'ensemble de Teichmüller que l'on identifie à K. Chaque élément x de A s'écrit d'une et une seule façon sous la forme $= a+m$ avec $a \in T^0$ et $m \in M$, et bien sûr, x est inversible si et seulement si $a \neq 0$.

Notons r l'indice de nilpotence de A. A la chaîne d'idéaux :

$$(0) = M^r \subset M^{r-1} \subset \cdots \subset \ldots M^2 \subset M^1$$

correspond, en posant $U^{(i)} = 1 + M^i$, une filtration du groupe des unités :

$$\{1\} = U^{(r)} \subset U^{(r-1)} \subset \cdots \subset U^{(2)} \subset U^{(1)} \subset A^\times = U^{(0)}$$

Notons que $\mathrm{ann}(M)$ n'est pas forcément égal à $M^{(r-1)}$. Le sous-groupe [3] $1 + \mathrm{ann}(M)$ du groupe multiplicatif $A^\times$ joue un rôle très particulier dans la suite, nous le notons $\mathcal{U}(A)$: c'est le groupe des unités fortes de A.

Soit ψ un caractère additif arbitraire. Le caractère local de A, et les relations d'orthogonalité permettent de caculer la somme complète $G_A(1,\psi)$.

$$G_A(1,\psi) = \begin{cases} |A^\times|, & \psi = 1; \\ -|M|, & \psi \in M^\perp - \{1\}; \\ 0, & \psi \notin M^\perp. \end{cases} \tag{29}$$

PROPOSITION 12.1. *Soit ψ un caractère admissible et soit χ un caractère multiplicatif.*

$$|G_A(\chi,\psi)|^2 = \begin{cases} |A|, & \chi \not\perp \mathcal{U}(A) \\ 0, & \chi \perp \mathcal{U}(A) \end{cases}$$

[3] A n'est pas un corps.

DÉMONSTRATION.

$$\begin{aligned} |G_A(\chi,\psi)|^2 &= \sum_{x\in A^\times}\sum_{y\in A^\times}\chi(x/y)\psi(x-y) \\ &= \sum_{z\in A^\times}\sum_{y\in A^\times}\chi(z)\psi((z-1)y) \\ &= |A| - |M|\sum_{z\in\mathcal{U}(A)}\chi(z) \end{aligned} \tag{30}$$

□

De ce résultat (30) sur le module des sommes de Gauss complètes, on déduit une estimation sur les sommes incomplètes.

PROPOSITION 12.2. *Soit S un sous-groupe de $A^\times$, χ un caractère multiplicatif et ψ un caractère admissible. Si $\chi \perp \mathcal{U}(A)$ alors*

$$|G_S(\chi,\psi)| \leq \frac{q-\epsilon}{q}\sqrt{|A|}$$

où ϵ désigne le cardinal de l'intersection des groupes $\mathcal{U}(A)$ et S.

DÉMONSTRATION.

$$\begin{aligned} G_S(\chi,\psi) &= \frac{1}{|S^\perp|}\sum_{\theta\in S^\perp} G_A(\chi\theta,\psi) \\ &= \frac{1}{|S^\perp|}\sum_{\theta\perp S,\chi\theta\not\perp\mathcal{U}(A)} G_A(\chi\theta,\psi) \\ &\leq \frac{1}{|S^\perp|}|\{\theta\in S^\perp \mid \theta\not\perp\mathcal{U}(A)\}|\sqrt{|A|} \end{aligned}$$

Le cardinal de $S\mathcal{U}(A)$ vaut $\frac{q|S|}{\epsilon}$, et donc

$$\frac{|S^\perp\cap\mathcal{U}(A)^\perp|}{|S^\perp|} = \frac{\epsilon}{q}$$

d'où l'estimation proposée. □

CHAPITRE 3

Les corps finis

Un corps fini est un corps ayant un nombre fini d'éléments. Si p désigne la caractéristique d'un corps fini K alors p est un nombre premier et K est un $\mathbf{F}_p$-espace [1] vectoriel de dimension finie, disons f, par suite son cardinal q est égal à p^f. Le célèbre théorème de Wedderburn affirme que tous les corps finis sont commutatifs, les éléments non-nuls de K sont des racines de l'unité, ils forment un groupe cyclique d'ordre $(q-1)$. Finalement, dans une clôture algébrique de $\mathbf{F}_p$, il n'existe qu'un et un seul corps fini de cardinal q, noyau de l'endomorphisme $x \mapsto x^q - x$, on le note $\mathbf{F}_q$. En hommage à Evariste Galois, les anglo-saxons le notent $GF(q)$ pour « Galois Field » [2]. Dans ce chapitre, il est question des corps finis, mais surtout de leurs cousins : les anneaux locaux, les anneaux de Galois et les anneaux d'entiers p-adiques. Les caractères sont vus à valeurs dans le corps des nombres complexes p-adique. L'une des plus belles propriétés des nombres : la loi de réciprocité quadratique de Legendre se démontre en utilisant les sommes de Gauss. Les congruences de Stickelberger réalisent une approximation p-adique des sommes de Gauss que j'utilise dans l'article sur les groupes à sections régulières. Le théorème d'Ax est une conséquence directe de ces congruences. La représentation analytique des caractères additifs et la formule des traces de Dwork conduisent à la formule de Gross-Koblitz. Le groupe multiplicatif d'un anneau local contient un sous-groupe de Teichmüller qui donne lieu à des sommes de Gauss incomplètes dont on peut estimer le module dans le cas des anneaux de Galois. En caractéristique 4, elles vérifient des congruences analogues aux congruences de Stickelberger. Les fonctions traciques sont obtenues à partir du développement p-adique de la forme trace. En caractéristique paire, la deuxième fonction tracique est une forme quadratique dont on peut calculer l'invariant de Arf.

1. Caractères des corps finis

Les caractères considérés ici sont à valeurs dans le corps $\mathbf{C}_p$. Je renvoie le lecteur aux ouvrages généraux concernant les nombres p-adique, voir par exemple [**5**]. Dans ce contexte, le caractère de Teichmüller devient un caractère multiplicatif canonique alors que la construction du caractère additif canonique s'évanouit. Une fois pour toutes, faisons le choix d'une racine π de l'équation

$$X^{p-1} + p = 0$$

[1] Conformément à l'usage, $\mathbf{F}_p$ désigne le corps fini à p éléments, l'anneau infini des nombres p-adiques est noté $\mathbf{Z}_p$.

[2] D'après le *Lehrbuch der Algebra* de Weber, le mot Körper est utilisé pour la première fois par Dedekind, en 1871, dans le supplement XI à l'article *Vorlesungen uber Zahlentheorie* de Dirichlet. La terminologie sera reprise en Français, Espagnol (cuerpo), Hollandais (lichaam), Hongrois (test).... Les anglophones utilisèrent un temps le mot latin corpus, puis le mot realm (royaume, domaine). Dans le *Linear groups with an exposition of the Galois Theory*, de 1901, Dickson utilise le mot field (champ) repris en italien (campo), en russe (polye). Évariste Galois qui avait une idée précise de l'objet ne l'avait pas baptisé !

Il existe une et une seule racine p-ième de l'unité ζ_π satisfaisant la congruence $\zeta_\pi \equiv 1 + \pi \pmod{\pi^2}$ ce qui permet de définir le caractère additif $\psi_{\pi,\mathbf{F}_p}$ du corps premier $\mathbf{F}_p$ par $\psi_{\pi,\mathbf{F}_p}(x) = {\zeta_\pi}^x$. On le relève par la trace sur chaque extension K de $\mathbf{F}_p$ pour obtenir le *caractère additif standard* de K

$$\psi_{\pi,K}(x) = {\zeta_\pi}^{\mathrm{tr}_{K/\mathbf{F}_p}(x)}$$

parfois noté $\psi_{\pi,q}$, où q est le cardinal de K.

2. Le caractère quadratique

Jusqu'à la fin de cette section, K désigne un corps fini de caractéristique impaire p et de cardinal q. Le groupe des inversibles de $K^\times$ est cyclique d'ordre pair. Il existe un et un seul sous-groupe d'indice 2 dans $K^\times$, c'est le groupe des carrés de $K^\times$, son orthogonal est formé de deux caractères : le caractère trivial et le caractère quadratique de K, on le note ν_K. Le caractère quadratique appliqué à un élément non-nul x s'appelle le caractère quadratique de x. Le caractère de x vaut $+1$ si x est un carré et vaut -1 sinon. Si x est dans le corps premier de K alors $\nu_K(x) = (-1)^{(q-1)/2}$, notamment

$$\nu_K(-1) = (-1)^{(q-1)/2} = \begin{cases} +1, & p \equiv 1 \bmod 4; \\ -1, & p \equiv 3 \bmod 4; \end{cases}$$

Le caractère quadratique d'un entier x modulo p est noté $\left(\frac{x}{p}\right)$, c'est le symbole de Legendre. La loi de réciprocité quadratique énoncée par Legendre, mais démontrée par Gauss affirme que si p et q sont deux nombres premiers impairs alors

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}. \tag{31}$$

Cette loi se démontre de bien des façons. La démonstration proposée par [?] est la plus élémentaire, parmi une bonne centaine de répertoriées. La démonstration qui suit, très classique s'appuie sur les propriétés élémentaires des sommes de Gauss. Elle donne lieu à des généralisations : réciprocité cubique, réciprocité bi-quadratique, symbole d'Artin et loi de réciprocité généralisée...

DÉMONSTRATION.

$$\sigma_q\left[G_{\mathbf{F}_p}(\nu_{\mathbf{F}_p})\right] = \left(\frac{q}{p}\right) G_{\mathbf{F}_p}(\nu_{\mathbf{F}_p}) \equiv \left[G_{\mathbf{F}_p}(\nu_{\mathbf{F}_p})\right]^q \bmod q$$

La somme $G_{\mathbf{F}_p}(\nu_{\mathbf{F}_p})$ est inversible modulo q puisque son carré est égal à $\nu_{\mathbf{F}_p}(-1)p$. Après simplification, en faisant apparaître ce carré, on obtient :

$$\left(\frac{q}{p}\right) \equiv \nu_{\mathbf{F}_p}(-1)^{(q-1)/2} p^{(q-1)/2} \bmod q,$$

c'est bien ce que dit la loi de réciprocité quadratique. □

Cette loi, complétée par la connaissance du caractère quadratique de 2 modulo n'importe quel nombre premier p, à savoir

$$\left(\frac{2}{p}\right) = \begin{cases} +1, & p \equiv \pm 1 \bmod 8; \\ -1, & p \equiv \pm 3 \bmod 8; \end{cases} \tag{32}$$

permet de calculer efficacement la valeur du symbole de Legendre.

3. Groupes à sections régulières

Soient K un corps fini d'ordre q, et L une extension de degré s de K. L'intersection d'un K-hyperplan de L avec une partie X de L est une *section hyperplane* de X. Un *groupe à sections régulières* est un sous-groupe de $L^\times$ dont les sections hyperplanes sont de taille constante.

Soit G un sous-groupe du groupe multiplicatif de L de rang s sur K. Pour chaque $a \in L - \{0\}$, notons $Z(a)$ le cardinal de l'intersection de G avec l'hyperplan $\mathrm{tr}_{L/K}(ax) = 0$.

$$Z(a) = \frac{n}{q^s - 1} \sum_{\psi \in G^\perp} \bar{\psi}(a) \sum_{\mathrm{tr}_{L/K}(x)=0} \psi(x)$$

Les sommes internes sont des sommes d'Eisenstein, la formule de Poisson permet de les écrire en fonction des sommes de Gauss.

$$\sum_{\mathrm{tr}_{L/K}(x)=0} \psi(x) = \frac{1}{q} \sum_{b \in K} G_L(\psi, \mu_b)$$

où μ désigne le caractère additif canonique de L et μ_b le caractère $\chi_b(x) = \chi_L(bx)$.

$$\sum_{\mathrm{tr}_{L/K}(x)=0} \psi(x) = \frac{1}{q}\big[G_L(\psi, 1) + G_L(\psi, \mu_L) G_K(\bar{\psi}, 1)\big].$$

La contribution des caractères non-triviaux sur $K^\times$ est nulle. Pour cette raison, on introduit Γ l'orthogonal du groupe $GK^\times$. C'est un groupe d'ordre $m = \frac{(q^s-1)(n,q-1)}{n(q-1)}$,

$$Z(a) = \frac{n}{q} + \frac{n(q-1)}{q(q^s-1)} \sum_{\psi \in \Gamma} \bar{\psi}(a) G_L(\psi, \mu_L)$$

D'où la borne bien connue,

$$|Z(a) - n\frac{q^{s-1}-1}{q^s-1}| \leq \frac{(n, q-1)}{q} \frac{h-1}{h} \sqrt{q^s}$$

Notons f_Γ l'application du groupe quotient $L^\times/\Gamma^\perp$ à valeurs dans $\mathbf{C}$ qui envoie la classe de a sur $\sum_{\psi \in \Gamma} \bar{\psi}(a) G_L(\psi, \mu_L)$,

PROPOSITION 3.1. [**124**, π_λ] *Le groupe G est à sections régulières si et seulement si f_Γ est injective.*

DÉMONSTRATION. La condition est suffisante. La nécessité est un petit plus longue à établir. □

PROPOSITION 3.2. [**124**, π_λ] *L'application f_Γ est injective si et seulement si l'ordre de Γ divise $p - 1$.*

DÉMONSTRATION. Soit λ un générateur du groupe $L^\times$. Il existe une valuation $\mathcal{P}$-adique de l'anneau des entiers du corps cyclotomiques $\mathbf{Q}(\zeta_p, \zeta_{q^s-1})$ telle que

$$\mathrm{val}_{\mathcal{P}}\big(G_L(\lambda^j, \mu_L)\big) = S_p(j)$$

Les congruences Stickelberger apportent quelques précisions supplémentaires

$$G_L(\lambda^j, \mu_L) = -\frac{(\zeta_p - 1)^{S_p(j)}}{j_0! j_1! \cdots j_t!} \pmod{P^{S_p(j)+1}}$$

Le groupe S est engendré par $\gamma = \lambda^{\frac{q^s-1}{d}}$, et les congruences de Stickelberger donnent

$$\mathrm{val}_{\mathcal{P}}\big(G_L(\gamma^i,\mu_L)\big) = \sigma(\frac{p^{sr}-1}{d}i) = sr(\frac{p-1}{d}i), \quad \forall i = 0,1\ldots,d-1.$$

Soient a et b deux éléments de $L^\times$ tels que $f_S(a) = f_S(b)$.

$$\sum_{i=0}^{d-1} \bar{\gamma}^i(a)G_L(\psi,\mu_L) = \sum_{i=0}^{d-1} \bar{\gamma}^i(b)G_L(\psi,\mu_L)$$

Nous en déduisons

$$\mathrm{val}_{\mathcal{P}}\big(\gamma(a)-\gamma(b)\big) \geq sr(\frac{p-1}{d})$$

Les nombres algébriques $\gamma(a)$ et $\gamma(b)$ sont des racines de l'unités d'ordre premier avec p ce qui implique $\gamma(a) = \gamma(b)$ i.e. f_S est injective. □

Corollaire 3.1. [**124**, $\pi\lambda$] *Soit G un groupe d'ordre n dans $L^\times$. Posons*

$$h = \frac{q^s-1}{n}\frac{(q-1,n)}{q-1}.$$

Le groupe G est un groupe à sections régulières si et seulement si h divise $p-1$. Dans ce cas, le nombre de sections différentes est h.

Lorsque $h = 1$ ou 2, les valeurs possibles de $Z(a)$ sont complètement déterminée. Pour $H \geq 3$, c'est un petit peu plus compliqué. Rappelons que

$$\frac{(\zeta_p-1)^{p-1}}{p} = -1 \pmod{\mathcal{P}} \tag{33}$$

Proposition 3.3. [**124**, $\pi\lambda$] *Soit G un groupe à sections régulières avec h types de sections. Alors,*

$$n - Z(a) = q^{\frac{s}{h}-1}T(a),$$

où $T(a)$ décrit la classe de $(-1)^{\frac{sr}{h}}(\frac{p-1}{h}!)^{-sr}$ modulo le groupe d'ordre h dans $\mathbf{F}_p{}^\times$.

Démonstration. Nous pouvons supposer $h > 1$. En réduisant l'égalité (3) par $P^{2sr\frac{p-1}{h}}$, nous obtenons

$$q(n - Z(a)) = n(q-1)\bar{\gamma}(a)G_L(\gamma,\chi_L) \pmod{P}^{2sr\frac{p-1}{h}}$$

ce qui montre que $n - Z(a) = q^{\frac{s}{h}-1}T(a)$, où $T(a)$ est un entier premier avec p donné par

$$T(a) = -n(q-1)\bar{\gamma}(a)(\frac{p-1}{h}!)^{-sr}\big(\frac{(\zeta_p-1)^{p-1}}{p}\big)^{\frac{-sr}{h}} \pmod{P}$$

compte tenu de l'égalité (33)

$$T(a) = n(-1)^{\frac{sr}{h}}\bar{\gamma}(a)(\frac{p-1}{h}!)^{-sr} \pmod{P}.$$

□

4. Analyse p-adique

L'objectif de cette section est de construire un caractère canonique dans le monde p-adique, où l'expression $\exp(\frac{2i\pi}{p})$ perd son sens. La valuation p-adique d'un entier a est r si p^r est la plus grande puissance divisant a. Cette valuation se prolonge à $\mathbf{Q}$ tout entier. L'application $x \mapsto |x|_p$ est une valeur absolue de $\mathbf{Q}$, de sorte que $\mathbf{Q}$ muni de $(x, y) \mapsto |x - y|_p$ est un espace métrique que l'on sait compléter en un corps $\mathbf{Q}_p$. La complétion de la fermeture algébrique de $\mathbf{Q}_p$ est un corps algébriquement clos et complet noté $\mathbf{C}_p$. À ce stade, nous avons l'analogue des corps $\mathbf{R}$ et $\mathbf{C}$. Dans le monde p-adique, les critères de convergence sont plus simples que dans le cas complexe. La série $\sum_{n=0}^{\infty} a_n z^n$ converge en z_0 si et seulement si $|a_n z_0^n|_p$ converge vers 0, c'est-à-dire que $\mathrm{ord}_p(a_n) + n\,\mathrm{ord}_p(z_0)$ tend vers l'infini. Notamment, la série exponentielle $\exp(Z) = \sum_{n=0}^{\infty} \frac{Z^n}{n!}$ ne converge pas sur $\mathbf{Z}_p$ puisque $\mathrm{ord}_p(n!) = \frac{n-S_p(n)}{p-1}$.

Soit π un entier algébrique tel que $\pi^{p-1} = -p$. On démontre sans difficulté qu'il existe une et une seule racine p-ième de l'unité telle que $\zeta_\pi = 1+\pi \mod \pi^2$. La série de Dwork associée à π est la composée de la série $\exp(Z)$ et du polynôme $\pi Z - \pi Z^p$, i.e. $E_\pi(z) = \exp(\pi z - \pi z^p) = \sum_{n=0}^{\infty} e_n z^n$. Attention ! Il ne s'agit pas d'une composée de fonctions, d'ailleurs on montre que $\exp(0) = 1$ alors que $E_\pi(1) = \zeta_\pi$;

Proposition 4.1 (Dwork). *Les coefficients de la série $E_\pi(Z)$ vérifient : (1) $\mathrm{ord}_{e_n} \in \frac{1}{p-1}\mathbf{Z}$, (2) $\mathrm{ord}_{e_n} \geq \frac{n(p-1)}{p^2}$, (3) pour $n \geq 2$, on a $\mathrm{ord}_p e_n \geq 2$. En particulier, la série $E_\pi(Z)$ converge sur $\mathbf{Z}_p$.*

Posons

$$\mathrm{E}_{\pi,\mathrm{q}}(Z) = \exp(\pi Z - \pi Z^q) = \mathrm{E}_\pi(Z)\mathrm{E}_\pi(Z^p)\ldots\mathrm{E}_\pi(Z^{p^{f-1}})$$

Théorème 4.1 (Dwork). *Soit ξ une racine $(q-1)$-ième de l'unité. La série $\mathrm{E}_{\pi,\mathrm{q}}$ converge en ξ et fournit une représentation analytique du caractère $\psi_{\pi,q}$:*

$$\mathrm{E}_{\pi,\mathrm{q}}(\xi) = \psi_{\pi,q}(\xi \bmod p)$$

en particulier $\mathrm{E}_{\pi,\mathrm{q}}(\xi)$ est égal à l'unique racine p-ième de l'unité congrue à $1 + \mathrm{tr}_{K/\mathbf{F}_p}(\xi).\pi \bmod \pi^2$.

5. Formule de Gross-Koblitz

Pour le matériel de cette section, voir les travaux de Dwork [**69**], Koblitz [**107**], et Serre [**170**]. Les preuves proposées par Lang dans [**114**] sont élémentaires en comparaison des méthodes cohomologiques utilisées par Koblitz. On note A l'anneau des séries dont la suite des coefficients tend vers zéro. Etant donné un endomorphisme u de A, on pose pour chaque entier j, $u(Z^j) = \sum_{i=0}^{\infty} u_{i,j} Z^i$. La somme des termes diagonaux s'appelle la *trace* de l'endomorphisme u. C'est la somme infinie $\mathrm{tr}(u) = \sum_{i=0}^{\infty} u_{i,i}$ qui est bien définie dans le cas d'un opérateur *complètement continu*. L'opérateur de Frobenius $Z \mapsto \Phi_q(Z^i) = Z^{iq}$ possède un inverse à gauche noté Ψ_q.

Proposition 5.1 (Dwork). *Soit $g(Z)$ une série dont le terme général tend vers 0. La trace de l'opérateur $\Psi_q \circ Z^{-a}g(Z)$ est bien définie, elle satisfait :*

$$(q-1)\mathrm{tr}\big(\Psi_q \circ Z^{-a}g(Z)\big) = \sum_{\zeta^{q-1}=1} \zeta^{-a}g(\zeta)$$

En particulier,

$$(q-1)\mathrm{tr}\big(\Psi_q \circ Z^{-a}\mathrm{E}_{\pi,\mathrm{q}}(Z)\big) = G(\chi^{-a}, \psi_{\pi,q})$$

ce qui est le point de départ pour obtenir la formule de Gross-Koblitz.

THÉORÈME 5.1 (Gross-Koblitz). *Pour tout entier a,*

$$G_K(\omega^a, \psi_{\pi,K}) = (-1)^f q\pi^{-S_p(a)} \prod_{i=0}^{f-1} \Gamma_p\left(1 - \langle p^i a/q-1\rangle\right),$$

où $< t >$ représente la partie fractionnaire du nombre rationnel t et Γ_p est la fonction gamma p-adique.

La fonction Gamma p-adique est définie sur les entiers naturels par

$$\Gamma_p(n) = (-1)^n \prod_{\substack{1<j<n \\ (j,n)=1}} j.$$

Si x et y sont deux entiers naturels tels que $x \equiv y \pmod{p^k}$ alors $\Gamma_p(x) \equiv \Gamma_p(y) \pmod{p^k}$, ainsi l'application Γ_p est prolongeable par continuité à $\mathbf{Z}_p$ tout entier. La section suivante illustre le fonctionnement de la fonction Γ_p et la formule de Gross-Koblitz. .

6. Un petit raffinement

PROPOSITION 6.1. *Soient a et b deux entiers naturels inférieurs à p. Alors*

$$\Gamma_p(1+a+bp) \equiv (-1)^{a+b} a!\{(p-1)!\}^b \pmod{p^2}.$$

DÉMONSTRATION. Calculons modulo p^2.

$$\begin{aligned}
\prod_{\substack{1\le i\le a+bp \\ (i,p)=1}} i &\equiv a! \prod_{j=1}^{b}\prod_{k=1}^{p-1}(jp+k) \pmod{p^2}, \\
&\equiv a! \prod_{j=1}^{b}(p-1)!\big(1+\sum_{k=1}^{p-1} k^{-1}jp\big) \\
&\equiv a! \prod_{j=1}^{b}(p-1)! \\
&\equiv a!(p-1)!^b
\end{aligned}$$

□

Nous sommes en mesure de présenter une nouvelle approximation des sommes de Gauss.

PROPOSITION 6.2. [?, πλ] *Soit a un entier,*

$$G(\omega_q^a, \psi_{\pi,q}) \equiv R_p(a)(p-1)!^{S_p(a)}\pi^{S_p(-a)} \pmod{\pi^{S_p(-a)}p^2}.$$

DÉMONSTRATION. On peut supposer que $0 \leq a < q$, considérons la décomposition de a dans la base p, $a_0 + a_1 p^1 + \ldots + a_{f-1}p^{f-1}$.

$$p^i a \equiv a_i p^0 + a_{1-i}p^1 + \ldots + a_{i+1-f}p^{f-1}$$
$$-\left\langle \frac{p^i a}{q-1} \right\rangle \equiv a_i + a_{1-i}p \pmod{p^2}$$

on applique la proposition précédente

$$\Gamma_p\big(1 - \left\langle \frac{p^i a}{q-1} \right\rangle\big) \equiv (-1)^{a_{-i}+a_{1-i}}(p-1)!^{a_{1-i}} \pmod{p^2}$$

en utilisant la formule de Gross-Koblitz

$$G(\omega^a, \mu) \equiv \prod_{i=0}^{f-1}(-1)^{a_i+a_{1-i}} \prod_{i=0}^{f-1}(a_i)! \prod_{i=0}^{f-1}(p-1)!^{a_{1-i}}$$
$$\times (-1)^f q\pi^{S_p s(a)} \pmod{p^2 q \pi^{-S_p(a)}}$$

et par le lemmule (6.1)

$$\equiv R_p(a)(p-1)!^{S_p(a)}\pi^{S_p(-a)} \pmod{p^2\pi^{S_p(-a)}}$$

Le théorème de Wilson et une seconde application du lemmule (6.1) fournissent l'approximation plus faible

$$G(\omega^{-a}, \mu) = \frac{(-\pi)^{S_p(a)}}{R_p(a)} \pmod{p\pi^{S_p(a)}}$$

qui est la version $\mathcal{P}$-adique du théorème de Stickelbeger. □

7. Théorèmes d'Ax et Katz

Le théorème d'Ax [**8**] illustre l'utilisation des sommes de Gauss dans la méthode des sommes de caractères.

THÉORÈME 7.1 (AX). *Soit f un polynôme de m variables à coefficients dans le corps fini à q éléments. Le nombre de zéros de f est un multiple de q^b, où b est le plus grand entier strictement inférieur à $\frac{m}{d}$.*

Le lecteur intéressé par ce théorème dans le cas du corps à deux éléments doit consulter le chapitre VI.

Désignons par k le corps fini dont il est question, notons q son cardinal et p sa caractéristique $q = p^f$. Le polynôme f s'écrit $f(x) = \sum_{d \in D} a_d x^d$, où D est un ensemble fini de m-uplets d'entiers naturels. On suppose que les coefficients de f sont non nuls, et l'écriture x^d signifie $x_1^{d_1}x_2^{d_2}\cdots x_m^{d_m}$ avec la convention $0^0 = 1$. Notons $Z(f)$ le nombre de zéros de f, la méthode des sommes de caractères donne :

$$qZ(f) = \sum_{\psi \in \widehat{k^+}} \sum_{x \in K^m} \psi(f(x)) = \sum_{\psi \in \hat{k^+}} \sum_{x \in k^m} \prod_{d \in D} \psi(a_d x^d)$$

Pour progresser, on introduit les sommes de Gauss à l'aide de la formule

$$\psi(t) = \sum_{\chi \in \hat{k^\times}} G(\chi, \psi)\bar{\chi}(t)$$

valide sur k tout entier à la condition de prolonger par 1 ou 0 , les caractères multiplicatifs. Désignons par χ un caractère multiplicatif générateur, la convention $0^0 = 1$ passe bien au travers de la formule $\chi^i(x^j) = \chi^{ij}(x)$. Notons M l'ensemble des applications de D dans $\{0, 1, \ldots, q-2\}$, on a :

$$\begin{aligned} q(q-1)^{|D|} Z(f) &= \sum_{\psi \in \widehat{k^+}} \sum_{x \in K^m} \prod_{d \in D} \sum_{\chi \in \hat{k^\times}} G(\chi, \psi) \bar{\chi}(a_d x^d) \\ &= \sum_{\psi \in \widehat{k^+}} \sum_{x \in k^m} \prod_{d \in D} \sum_{0 \leq j < q-1} G(\chi^j, \psi) \bar{\chi}^j(a_d x^d) \\ &= \sum_{\psi \in \widehat{k^+}} \sum_{x \in k^m} \sum_{j \in M} \prod_{d \in D} G(\chi^{j(d)}, \psi) \bar{\chi}^{j(d)}(a_d x^d) \\ &= \sum_{\psi \in \widehat{k^+} - \{1\}} S(f, \psi) + q^m \end{aligned}$$

où l'on a posé :

$$\begin{aligned} S(f, \psi) &= \sum_{x \in k^m} \sum_{j \in M} \prod_{d \in D} G(\chi^{j(d)}, \psi) b_d^{j(d)} \bar{\chi}^{j(d)}(x^d) \\ &= \sum_{j \in M} \prod_{d \in D} G(\chi^{j(d)}, \psi) b_d^{j(d)} \prod_{1 \leq i \leq m} \sum_{t \in K} \chi^{\sum_{d \in D} j(d) d_i}(t) \end{aligned} \tag{34}$$

La formule

$$\sum_{t \in k} \chi^j(t) = \begin{cases} q, & j = 0 \\ q-1, & 0 < j \equiv 0 \pmod{q-1}; \\ 0, & \text{sinon}; \end{cases} \tag{35}$$

nous permet de faire fondre l'expression. Notons M' l'ensemble des applications de M tel que pour tout i, $\sum_{d \in D} j(d) d_i$ est divisible par $q-1$ et désignons par $z(j)$ le nombre de i pour lequel la somme vaut zéro. On a :

$$S(f, \psi) = \sum_{j \in M'} q^{z(j)} (q-1)^{m - z(j)} \prod_{d \in D} G(\chi^{j(d)}, \psi) b_d^{j(d)} \tag{36}$$

Soit v la valuation attachée au caractère χ par les congruences de Stickelberger. Elle est caractérisée par les égalités $v(G(\chi^j, \psi)) = S(j)$ et $v(p) = p - 1$. La valuation du terme indexé par j vaut donc $\sum_{d \in D} S(j(d) j + f(p-1) z(j)$. On sait que pour chaque i, $\sum_{d \in D} j(d) j_i$ est congru à zéro modulo $q - 1$. D'où l'on tire :

$$d \sum_{d \in D} j(d) \geq \sum_{i=1}^{m} \sum_{d \in D} j(d) j_i \geq (m - z(j))(q-1) \tag{37}$$

A ce stade, il faut remarquer que si j est dans M' alors l'application $p.j$ qui à $d \in D$ associe $[p\, j(d)]$ ($[t]$ désigne la réduction modulo $q-1$ de t) est dans M', et qu'en outre, $z(p.j) = z(j)$. Donc, pour tout entier k, on a aussi :

$$d \sum_{d \in D} [p^k j(d)] \geq (m - z(j))(q-1) \tag{38}$$

En sommant ces inégalités pour k allant de 0 jusqu'à $f-1$, on obtient :

$$\frac{q-1}{p-1}\sum_{d\in D} S(j(d)) = \sum_{k=0}^{f-1}\sum_{d\in D}[p^k j(d)] \geq f(m-z(j))(q-1) \tag{39}$$

Finalement, l'entier algébrique $S(f,\psi)$ est de valuation q-adique plus grande que le plus petit des entiers supérieurs ou égaux à $\min_{t\in\{0,1,\ldots,m\}}\{\frac{m-t}{d}+t\}$, d'où le théorème.

Le théorème d'Ax est optimal. Pour chaque entier d, il existe un polynôme de degré d de m variables à coefficients dans $\mathbf{F}_q$ dont le nombre de zéros est divisible par q^b sans être divisible par une plus grande puissance de q.

Problème 7.1. *S'inspirer du théorème d'Ax pour deviner la divisibilité du nombre de zéros de l'équation $f(x)=0$ en fonction des monômes qui composent f.*

Le théorème de Katz est l'analogue du théorème d'Ax dans le cas d'un système d'équations. Contrairement aux apparences, il n'en n'est pas une conséquence.

Théorème 7.2 (Katz). *Soient f_1, f_2, ... , f_s des polynômes de m variables à coefficients dans le corps fini à q éléments. Notons respectivement d et δ la somme et le maximum de leur degré. Le nombre de zéros du système $f_1(x)=f_2(x)=\ldots=f_s(x)$ est un multiple de q^b, où b est la partie entière de $\frac{m-d}{\delta}$..*

Démonstration. voir [**105**], [**186**]. ☐

8. Deux résultats de Carlitz

Aux théorèmes de la section précédentes, il convient d'ajouter deux résultats fondamentaux. Le premier est trés connu est utilisé un petit peu partout dans mes articles il s'agit de la fameuse borne de Carlitz-Uchyama [**42**]. Le second moins connu nous a permis de déterminer le groupe d'automorphismes des codes à distribution de poids équilibrée, c'est un théorème de Carlitz, amélioré par un de ses élèves.

Théorème 8.1 (Carlitz-Uchiyama). *Soit $f\in K[X]$ un polynôme de degré d qui ne peut pas s'écrire $f(X)=g(X)^p-g(X)$. Soit χ un caractère additif non-trivial sur K. On a :*

$$|\sum_{x\in K}\mu(f(x))| \leq (d-1)\sqrt{q}$$

Démonstration. Un résultat qu'on obtient par la méthode de Stepanov, une application de la méthode des sommes de caractères, exposée dans [**136**]. ☐

Théorème 8.2 (Carlitz-McDonnell). *Soit S un sous-groupe propore de K et soit f une application de K dans K telle que :*

$$f(0)=0, \quad f(1)=1, \qquad \forall x,y\in K, \quad \frac{f(x)-f(y)}{x-y}\in S$$

alors f est un automorphisme de K i.e. $f(x)=x^{p^j}$ pour un certain entier j.

Démonstration. Un trés beau théorème, la démonstration de [**145**] mériterait d'être reprise. ☐

9. Les anneaux de Galois

Soit A l'anneau de Galois de caractéristique p^ℓ et de degré résiduel f. Soit γ un générateur du groupe de Teichmüller $T_A^\times$. L'idéal maximal de A est monogène engendré par p. L'ensemble T_A^0 est un système de représentants multiplicatifs du corps $K = A/(p)$ d'ordre $q = p^f$. Chaque élément a de A se développe d'une et une seule façon en une somme

$$a = \sum_{i=0}^{\ell-1} x_i p^i, \tag{40}$$

où les x_i sont des éléments de T_A^0. Le groupe des $\mathbf{Z}/p^\ell\mathbf{Z}$-automorphismes est engendré par l'automorphisme de Frobenius σ qui envoie x sur $\sum_{i=0}^{\ell-1} x_i^p p^i$. L'application trace $x \mapsto \mathrm{tr}_A(x) = \sum_{j=0}^{\ell-1} \sigma^j(x)$ est une forme linéaire du $\mathbf{Z}/p^\ell\mathbf{Z}$-module A. La non-dégénérescence de la forme bilinéaire $(x, y) \mapsto \mathrm{tr}_A(xy)$ permet de définir un caractère additif admissible privilégié, le caractère canonique de A,

$$\mu_A(x) = \zeta_{p^\ell}^{\mathrm{tr}_A(a)}$$

Pour travailler dans l'anneau de Galois A, on dispose de trois approches : vecteurs de Witt, relèvement de Hensel et extension du corps des nombres p-adiques.

9.1. Les vecteurs de Witt. On utilise l'application

$$x_0 + px_1 + \cdots + x_{\ell-1}p^{\ell-1} \mapsto (x_0, x_1, \ldots, x_{\ell-1}) \tag{41}$$

pour transporter les structures de A vers l'ensemble K^f des vecteurs de Witt [**171**]. Pour chaque indice j, il existe des polynômes S_j et P_j dans l'anneau $\mathbf{Z}[X_0, X_1, \ldots X_j, Y_0, Y_1, \ldots, Y_j]$ tels que

$$\begin{aligned}(x+y)_j &= S_j(x_0, x_1, \ldots, x_j, y_0, y_1, \ldots, y_j),\\ (xy)_j &= P_j(x_0, x_1, \ldots, x_j, y_0, y_1, \ldots, y_j).\end{aligned}$$

Les polynômes S_j et P_j ne dépendent pas de ℓ.

$$\begin{aligned}&S_0(x_0, y_0) = x_0 + y_0 \qquad && S_1(x_0, x_1, y_0, y_1) = x_1 + y_1 + \frac{x_0^p + y_0^p - (x_0+y_0)^p}{p}\\ &P_0(x_0, y_0) = x_0.y_0 && P_1(x_0, x_1, y_0, y_1) = y_o^p x_1 + y_1 x_0^p\end{aligned}$$

9.2. Relèvement de Hensel. La notion de relèvement de Hensel est basée sur la proposition suivante :

PROPOSITION 9.1. *Soient $P(X)$ et $Q(X)$ deux polynômes unitaires à coefficients entiers tels que $P(X)Q(X) = X^q - X$ modulo $p^{\ell-1}$. Il existe deux polynômes unitaires à coefficients entiers P_ℓ et Q_ℓ tels que :*

$$P_\ell(X) \equiv P(X) \quad Q_\ell(X) \equiv Q(X)$$
$$P_\ell(X) \equiv Q_\ell(X)$$

où toutes les équivalences sont modulo p^ℓ.

Le polynôme P_ℓ est uniquement déterminé modulo p^ℓ : c'est le relevé d'Hensel de P. Partons d'un polynôme unitaire F_1 à coefficients entiers, de degré f, dont la réduction modulo p est un polynôme primitif. Notons $F_\ell(X)$ le polynôme obtenu en partant de F_1 , après $\ell-1$ relèvements successifs. L'anneau de Galois A est isomorphe à $\mathbf{Z}[X]/(p^\ell, F_\ell(X))$, de plus la classe de X engendre le groupe de Teichmüller.

9.3. Extensions du corps $\mathbf{Q}_p$. Soit α une racine de l'unité d'ordre $q-1$ dans une extension convenable du corps des nombres p-adiques. L'extension $\mathbf{Q}_p(\alpha)$ de $\mathbf{Q}_p$ est non ramifiée de degré f. L'idéal engendré par p dans l'anneau $\mathbf{Z}_p[\alpha]$ est maximal.

$$A \sim \mathbf{Z}_p[\alpha]/(p^\ell)$$

PROPOSITION 9.2. *Si z est un élément de trace nulle dans l'anneau de Galois A alors il existe $y \in A$ tel que $\sigma(y) - y = z$.*

DÉMONSTRATION. Le groupe de Galois G est cyclique et agit sur A. Il suffit de montrer que $H^1(G, A^+) = (0)$. Pour $\ell = 1$ c'est le théorème 90 de Hilbert. La suite exacte :

$$0 \longrightarrow pA^+ \longrightarrow A \longrightarrow K \longrightarrow 0$$

donne

$$(0) \longrightarrow H^1(G, pA^+) \longrightarrow H^1(G, A) \longrightarrow H^1(G, K)$$

d'où le résultat puisque $pA^+ \sim GR(p^{\ell-1}, f)^+$. □

10. Sommes de caractères dans un anneau de Galois

Soit $F(X) = f_0(X)+p^1 f_1(X)+\cdots+p^{\ell-1} f_{\ell-1}(X)$, où les $f_i(X)$ sont des polynômes à coefficients dans $T_A^\times$. On note $\mathrm{Deg}(f)$ le *degré pondéré* de f :

$$\mathrm{Deg}(f) = \max\{p^{\ell-i} \deg(f_i) \mid 0 \le i < \ell\}$$

THÉORÈME 10.1. *L'ensemble des $\ell+1$-uplets $(y_0, y_1, \ldots, y_{\ell-1}, x)$ de $T_A^{0\,\ell} \times T_A^0$ obtenu en posant $z = \sum_{i=0}^{\ell-1} y_i p^i$ et en faisant varier (z, x) dans l'ensemble des solutions de l'equation $\sigma(z) - z = f(X)$ se déduit d'une courbe de genre $\frac{(\mathrm{Deg}(f)-1)(q-1)}{2}$ obtenue par une tour de ℓ extensions d'Artin-Schreier.*

DÉMONSTRATION. Voir [**31**]. □

Pour chaque entier s, notons A_s l'extension galoisienne de A. Pour chaque caractère additif $\psi \in A^+$, notons $\psi^{(s)} \in {A_s}^+$ le relèvement de ψ par la trace

$$\psi^{(s)} = \psi \circ \mathrm{tr}_{A_s/A}$$

THÉORÈME 10.2. *Soit ψ un caractère additif non trivial. Il existe* $\mathrm{Deg}(F)-1$ *entiers algébriques ω_i de module $\sqrt{q}$, tels que*

$$-\sum_{x \in T_{A_s}^\times} \psi^{(s)}(F(x)) = \sum_{i=1}^{\mathrm{Deg}(f)-1} \omega_i^s$$

DÉMONSTRATION. C'est une conséquence de (10.1). □

COROLLAIRE 10.1. *Soit μ le caractère additif canonique de l'anneau de Galois A,*

$$|G_{T_A^\times}(1, \mu) + 1| \le (p^{\ell-1} - 1)\sqrt{q}$$

En utilisant une variante de la méthode de Stepanov, voir [**136**], on démontre une formule analogue dans le cas multiplicatif. Pour tout caractère multiplicatif χ de l'anneau de Galois A, notons $\chi^{(s)}$ le relèvement de χ par la norme dans A_s

$$\chi^{(s)} = \chi \circ \mathrm{N}_{A_s/A}$$

THÉORÈME 10.3. *Soit ψ un caractère additif non trivial et soit χ un caractère multiplicatif non trivial sur $T_A^\times$. Il existe* $\mathrm{Deg}(f)$ *entiers algébriques ω_1, ω_2, ..., $\omega_{D(f)}$, de module au plus $\sqrt{q}$, tels que*

$$-\sum_{x\in T_{A_s}^\times} \chi^{(s)}(x)\psi^{(s)}(F(x)) = \sum_{i=1}^{D(f)} \omega_i^s$$

DÉMONSTRATION. □

PROPOSITION 10.1. *Soit μ le caractère additif canonique de l'anneau A et soit χ un non caractère non trivial du groupe $T_A^\times$*

$$|G_{T_A^\times}(\chi,\mu)| \leq p^{\ell-1}\sqrt{q}$$

Lorsque $f = 2$ et $\ell = 2$, l'estimation fournie par la proposition 3.2 est meilleure.

11. Les fonctions traciques

Soit x un Teichmüller de l'anneau de Galois A. Considérons le développement p-adique de la trace.

$$\mathrm{tr}_A(x) = \sum_{j=0}^{\ell-1} t_j(x)p^j. \tag{42}$$

où les fonctions t_j sont des fonctions de K dans $\mathbf{F}_p$. Nous dirons que les fonctions t_j sont des *fonctions traciques* . La première fonction tracique, t_0, n'est rien d'autre que la trace du corps K. Continuons dans le cas de la caractéristique 2^ℓ. À l'aide des vecteurs de Witt , on détermine facilement l'expression de la seconde fonction tracique :

$$t_1(x) = \sum_{0\leq i<j\leq f} x^{2^i+2^j} \tag{43}$$

Pour déterminer t_2 c'est un petit peu plus compliqué. Nous pouvons utiliser le relèvement de Hensel. Soit $\beta \in K$, et considérons le polynôme $P(X) = \prod_{i=0}^{f-1}(X - \beta^{p^i})$. Pour chaque entier ℓ, notons $P_\ell(X)$ le relèvement de P à coefficient dans $\mathbf{Z}/2^\ell\mathbf{Z}$, et posons

$$P_\ell(X) = \sum_{i=0}^{f} S_i^{(\ell)}(\beta)X^{f-i}.$$

On sait que :

$$P_{\ell+1}(X^2) = (-1)^f P_\ell(X)P_\ell(-X)$$

D'où l'on tire :

$$S_1^{(\ell+1)}(\beta) = 2S_2^{(\ell)}(\beta) - S_1^{(\ell)}(\beta)^2,$$
$$S_2^{(\ell+1)}(\beta) = 2S_4^{(\ell)}(\beta) - 2S_1^{(\ell)}(\beta)S_3^{(\ell)}(\beta) + S_2^{(\ell)}(\beta)^2$$

En particulier, on retrouve que $t_1(\beta) = \sum_{0\leq i<j<f} \beta^{2^i+2^j}$. Ainsi, t_1 est une forme quadratique alors que t_2 apparaît comme une fonction booléenne de degré 4.

Avant d'étudier t_1, rappelons quelques éléments de la théorie des formes quadratiques. Soit E un espace vectoriel de dimension m sur $\mathbf{F}_2$. Une forme quadratique $\mathbf{q}$ est une application de E dans $\mathbf{F}_2$ tel que l'application $(x,y) \mapsto \mathbf{q}(x+y)+\mathbf{q}(x)+\mathbf{q}(y)$ soit une forme bilinéaire ϕ. L'ensemble des vecteurs x tel que $\phi(x,y) = 0, \forall y \in {\mathbf{F}_2}^m$ est un espace vectoriel : c'est le noyau de $\mathbf{q}$, sa dimension à la même parité que m et la forme $\mathbf{q}$ est dite de rang maximal si la dimension de son noyau est 0 ou 1. Notons $Z(\mathbf{q})$ le nombre de zéros de $\mathbf{q}$.

Proposition 11.1. *Soit $\mathbf{q}$ une forme quadratique de rang maximal sur un espace de dimension paire $m = 2t$. Le nombre de zéros de $\mathbf{q}$ vaut :*

$$Z(\mathbf{q}) = 2^{m-1} - (-1)^{\mathrm{Arf}(\mathbf{q})} 2^{t-1}$$

où $\mathrm{Arf}(\mathbf{q})$ désigne l'invariant de Arf de $\mathbf{q}$.

L'invariant $\mathrm{Arf}(\mathbf{q})$ prend la valeur 0 ou 1. Il prend la valeur 1 si la quadrique n'a pas beaucoup de points : c'est le cas elliptique, l'autre cas est dit hyperbolique. Pour calculer l'invariant de Arf de $\mathbf{q}$, on utilise une base symplectique : $(u_1, v_1, u_2, v_2, \dots, u_t, v_t)$, c'est-à-dire telle que $\phi(u_i, u_j) = 0$ et $\phi(u_i, v_j) = \delta_{ij}$. L'invariant de Arf de $\mathbf{q}$ vaut

$$\mathrm{Arf}(\mathbf{q}) = \sum_{i=1}^{t} \mathbf{q}(u_i)\mathbf{q}(v_i)$$

De façon plus abstraite, l'invariant de Arf détermine l'algèbre de Clifford de la forme quadratique. La référence [**64**] est usuelle en la matière. Mais dans [**70**], on trouvera une preuve élémentaire de l'invariance de $\mathrm{Arf}(\mathbf{q})$.

Proposition 11.2. *Soit $\mathbf{q}$ une forme quadratique de rang maximal sur un espace de dimension impaire $m = 2t+1$. Le nombre de zéro de $\mathbf{q}$ vaut :*

$$Z(\mathbf{q}) = 2^{m-1} + v(\mathbf{q})2^{t-1}$$

où $v(\mathbf{q})$ vaut 0 si $\mathbf{q}$ est défective. Si $\mathbf{q}$ n'est pas défective alors $v(\mathbf{q})$ est donné par l'invariant de Arf de la restriction de $\mathbf{q}$ à $\ker(\mathbf{q})^{\perp}$.

Rappelons que la quadrique est défective, si la restriction de $\mathbf{q}$ à son noyau n'est pas nulle : la quadrique est dite parabolique. Calculons ϕ la forme bilinéaire symplectique associée à $\mathbf{q}$:

$$\begin{aligned}
\mathbf{q}(x+y) &= \sum_{i<j} (x+y)^{2^i}(x+y)^{2^j} \\
&= \mathbf{q}(x) + \mathbf{q}(y) + \sum_{i<j} x^{2^i} y^{2^j} + \sum_{i<j} y^{2^i} x^{2^j} \\
&= \mathbf{q}(x) + \mathbf{q}(y) + \sum_{i<j} x^{2^i} y^{2^j} + \sum_{j<i} y^{2^j} x^{2^i} \\
&= \mathbf{q}(x) + \mathbf{q}(y) + \sum_{j} \left(\mathrm{tr}(x) + x^{2^j}\right) y^{2^j} \\
&= \mathbf{q}(x) + \mathbf{q}(y) + \mathrm{tr}(x)\mathrm{tr}(y) + \mathrm{tr}(xy)
\end{aligned}$$

Et donc,

$$\phi(x, y) = \mathrm{tr}(x)\mathrm{tr}(y) + \mathrm{tr}(xy) \tag{44}$$

L'élément z est dans le noyau de $\mathbf{q}$ si et seulement si $\mathrm{tr}(z) + z = 0$, et donc la forme quadratique est de rang maximal.

12. Somme de Gauss triviale

Désignons par μ_A le caractère additif canonique de l'anneau de Galois $A = GR(p^\ell, f)$. Notons $T_A^\times$ le groupe des Teichmüller. La somme de Gauss incomplète $G_{T_A^\times}(1, \mu_A)$ est la *somme de Gauss triviale*. Pour tout caractères additifs ψ, $1 + G_{T_A^\times}$ est noté $S_A(\mu)$. Les calculs de la sections précédentes permettent de la déterminer explicitement, en caractéristique 4. Notons $N(a, b)$ le nombre de solutions du système : $t_0(x) = a$, et $t_1(x) = b$.

$$S_A(\mu) = 1 + G_{T_A^\times}(1, \mu_A) = \sum_{a,b \in \mathbf{F}_2} N(a, b) i^{a+2b}$$

• m pair, $m = 2t$. La forme quadratique $\mathbf{q}$ est de rang maximal. Le nombre de solution de l'equation $\mathbf{q}(x) = 0$ vaut $2^{m-1} + \alpha 2^{t-1}$. La restriction de $\mathbf{q}$ à l'hyperplan $\mathrm{tr}(x) = 0$ est encore de rang maximal. Le nombre de solutions du système :

$$\mathrm{tr}(x) = 0, \quad \mathbf{q}(x) = 0$$

vaut donc $2^{m-2} + \beta 2^{t-1}$.

Et par suite,

$$N(0,0) = 2^{m-2} + \beta 2^{t-1} \qquad N(0,1) = 2^{m-2} - \beta 2^{t-1}$$
$$N(1,0) = 2^{m-2} + (\alpha - \beta) 2^{t-1} \qquad N(1,1) = 2^{m-2} + (\beta - \alpha) 2^{t-1}$$

Et finalement,

$$1 + G_{T_A^\times}(1, \mu) = \big(\beta + (\alpha - \beta) i\big) 2^t$$

• m impair, $m = 2t + 1$. La forme quadratique $\mathbf{q}$ est non dégénérée, et le nombre de solutions de l'equation $\mathbf{q}(x) = 0$ est égal à $2^{m-1} + \beta 2^t$. De plus sa restriction à l'hyperplan d'equation $\mathrm{tr}(x) = 0$ est encore de rang maximal. Le nombre de solution du système :

$$\mathrm{tr}(x) = 0, \quad \mathbf{q}(x) = 0,$$

vaut donc $2^{m-2} + \alpha 2^{t-1}$.

Et par suite,

$$N(0,0) = 2^{m-2} + \alpha 2^{t-1} \qquad N(0,1) = 2^{m-2} - \alpha 2^{t-1}$$
$$N(1,0) = 2^{m-2} + (2\beta - \alpha) 2^{t-1} \qquad N(1,1) = 2^{m-2} - (2\beta - \alpha) 2^{t-1}$$

Et finalement,

$$1 + G_{T_A^\times}(1, \mu) = \big(\alpha + (2\beta - \alpha)\big) 2^t$$

Pour déterminer ces sommes complètement, il faut déterminer l'invariant de Arf des formes quadratiques correspondantes, et on peut procéder de deux façons. La première consiste à trouver une base symplectique, voir [**110**]. La seconde est basée sur le théorème 7.2 qui montre que

$$S_A(\mu) = 1 + G_{T_A^\times}(1, \mu_A) = -(-1)^m(1+i)^m$$

D'où l'on tire les valeurs de α et de β en fonction de la congruence modulo 8 de m. Lorsque m est pair, on a $-i^t = \beta + (\alpha - \beta)i$, et lorsque m est impair, on a $i^t(1+i) = \alpha + (2\beta - \alpha)i$.

m pair			m impair		
t	β	α	t	β	α
0	-1	-1	0	-1	$+1$
1	0	-1	1	0	-1
2	$+1$	$+1$	2	-1	-1
3	0	$+1$	3	0	$+1$

Enfin, pour être complet, signalons la relation qui lie la somme de Gauss $G_{T_A^\times}(1, \mu_\theta)$ à la somme $G_{T_A^\times}(1, \mu)$.

Proposition 12.1 (Helleseth-Yang). *Soit $\theta \in A = GR(4, f)$. On écrit $\theta = a + 2b$ avec a et b dans T_A^0,*

$$S_A(\mu_\theta) = \begin{cases} \mu_A(\frac{b}{a}) S_A(\mu_A), & a \neq 0; \\ q, & a = b = 0; \\ 0, & a = 0 \neq b. \end{cases}$$

Démonstration. La démonstration qui suit est due à Helleseth et Yang [**81**], elle repose sur la relation :

$$x \oplus y = x + y + 2\sqrt{xy} \tag{45}$$

qui donne le représentant multiplicatif de la somme de deux éléments x et y de T_f^0. En particulier,

$$\mu_A(x \oplus y) = \mu_A(x + y + 2xy)$$

$$\begin{aligned} 1 + G_{T_A^\times}(1, \mu_\theta) &= \sum_{x \in T_A^0} \mu_A\big((a+2b)x\big) \\ &= \sum_{x \in T_A^0} \mu_A\big((1 + 2\frac{b}{a})x\big) \\ &= \sum_{x \in T_A^0} \mu_A(x + 2\frac{b}{a}x) \end{aligned}$$

En appliquant la formule (45),

$$= \mu_A(b/a) \sum_{x \in T_A^0} \mu_A(x \oplus b/a)$$

□

13. Congruences en caractéristique quatre

Dans cette section, nous montrons que les sommes de Gauss sur l'anneau de Galois de caractéristique 4 satisfont des congruences analogues aux congruences de Stickelberger. Les notations sont inchangées, en particulier, μ_A et μ_K désignent les caractères additifs canoniques de $A := GR(4, f)$ et de son corps résiduel K. Le point de départ est une formule qui relie des sommes de Gauss avec la somme de caractère $H(\chi, \mu) = \sum_{s \in T_A^0 - \{0,1\}} \mu_A(s)\chi(s/s+1)$, nous obtenons la relation

$$G_{T_A^\times}(\chi, \mu_A)^2 = G_K(\chi, \mu_K)\big[1 + G_{T_A^\times}(1, \mu_A) + H(\chi, \mu_A)\big]$$

Démonstration. Soit χ un caractère multiplicatif. Prenons notre courage à deux mains et calculons le carré de la somme $G_{T_A^\times}(\chi, \mu_A)$.

$$G_{T_A^\times}(\chi, \mu_A)^2 = \sum_{x \in T_A^\times} \sum_{y \in T_A^\times} \chi(xy)\mu_A(x+y)$$

par la relation (45),

$$\begin{aligned}
&= \sum_{x,y \in T_A^\times} \chi(xy)\mu_A(x \oplus y + 2xy) \\
&= \sum_{\substack{x \oplus y = u \\ xy = v}} \chi(v)\mu_A(u + 2v) \\
&= \sum_{x \in K^\times} \chi(x^2)\mu_K(x^2) + 2 \sum_{\substack{u \in T_A^\times \\ \mathrm{tr}_{K/\mathbf{F}_2}(v/u^2)=0}} \chi(v)\mu_A(u+2v) \\
&= G_{K^\times}(\chi, \mu_K) + 2 \sum_{\substack{u \in T_A^\times \\ \mathrm{tr}_{K/\mathbf{F}_2}(w)=0}} \chi(u^2 w)\mu_A(u + 2u^2 w)
\end{aligned}$$

en changeant u par u^2,

$$\begin{aligned}
&= G_{K^\times}(\chi, \mu_K) + 2 \sum_{\substack{u \in T_A^\times \\ \mathrm{tr}_{K/\mathbf{F}_2}(w)=0}} \chi(uw)\mu_A(u + 2uw) \\
&= G_{K^\times}(\chi, \mu_K) + 2 \sum_{u \neq 0} \mu_A(u)\chi(u) \sum_{\mathrm{tr}_{K/\mathbf{F}_2}(w)=0} \chi(uw)\mu_K(uw).
\end{aligned}$$

On vérifie, par exemple avec la formule de Poisson, que

$$\begin{aligned}
\sum_{\mathrm{tr}_{K/\mathbf{F}_2}(w)=0} \chi(w)\mu_K(uw) &= \frac{1}{2}\big[G_K(\chi, \mu_{K_{u+1}}) + G_K(\chi, \mu_{K_u})\big] \\
&= \frac{1}{2}\begin{cases} \big[\bar\chi(u+1) + \bar\chi(u)\big]G_K(\chi, \mu_K), & u \neq 1; \\ G_K(\chi, \mu_K), & u = 1. \end{cases}
\end{aligned}$$

ce qui permet de continuer par

$$\begin{aligned} G_{T_A^\times}(\chi,\mu_A)^2 &= G_{K^\times}(\chi,\mu_K) + \mu_A(1) G_K(\chi,\mu_K) \\ &\qquad + G_K(\chi,\mu_K) \sum_{u\notin\{0,1\}} \mu_A(u)\chi(u)\big[\bar\chi(u+1)+\bar\chi(u)\big] \\ &= G_K(\chi,\mu_K)\big[1 + G_{T_A^\times}(1,\mu_A) + H(\chi,\mu_A)\big] \end{aligned}$$

□

PROPOSITION 13.1. [**127**, $\pi\!\lambda$] *Soit $\mathcal{P}$ un idéal premier au-dessus de 2 dans l'anneau $\mathbf{Z}[i,\xi]$. Si ω désigne le caractère du groupe des caractères de $T_A^\times$ décrit par les congruences de Stickelberger alors*

$$\mathrm{val}_{\mathcal{P}}\big(G_{T_A^\times}(\omega^a,\mu_A)\big) = S(a).$$

DÉMONSTRATION. Il suffit de vérifier que la somme de Jacobi qui intervient dans la formule (13) est un élément non-inversible modulo $\mathcal{P}$.

$$\begin{aligned} \sum_{u\notin\{0,1\}} \omega^a(u+1)\bar\omega^a(u)\mu(u) &\equiv \sum_{u\notin\{0,1\}} \omega^a(u+1)\bar\omega^a(u) \pmod{\mathcal{P}} \\ &\equiv \sum_{u\notin\{0,1\}} (u+1)^a u^{q-1-a} \equiv 1 \end{aligned}$$

□

PROBLÈME 13.1. *Les expériences numériques montrent que ce résultat est plus général, ce qui manifestement n'est pas le cas de la démonstration proposée ici.*

CHAPITRE 4

Codes

Dans les premières applications, les codes sont utilisés pour faire du contrôle de parité. Ils s'agit de détecter les erreurs : au démarrage d'un ordinateur dans la phase vérification de la mémoire, lors de communications par modem, au dos des ouvrages sous la forme de code ISBN et même sur les billets de banques. Les codes utilisés dans les missions spatiales sont plus sophistiqués, il faut détecter et corriger les erreurs. Dans les années 70, la sonde Mariner IX encode ses clichés de Mars avec le code Reed-Muller du premier ordre $\mathrm{RM}(1,5)$. Quelques années plus tard, la sonde PathFinder utilise des codes convolutionnels de Viterbi et des codes en blocs de Reed-Solomon que nous retrouvons dans le disque compact. Faites l'expérience, rayez la face sensible de votre disque favori avec une aiguille à coudre. La qualité d'écoute reste excellente. Quelque part, gardons en mémoire que les méthodes d'entrelacements et de codage qui ont permis le passage du vinyl au numérique doivent à la présence d'Evariste Galois.

La théorie des codes correcteurs d'erreurs débute avec R. W. Hamming (1915–98) et M. J. E. Golay •dans le sillage de la théorie de C. E. Shanon. À la frontière de ces deux théories, un point culminant est atteint dans les années 80 lorsque Tfasmann, Vladut, et Zink montrent que la classe des codes de Goppa géométriques dépasse la borne de Varshamov-Gilbert. Les codes en blocs intéressent plusieurs domaines des mathématiques discrètes. La connaissance même partielle de la distribution de poids d'un code permet la construction de réseaux, de graphes, de configurations tactiques et de familles de séquences.

Quelques temps forts de la théorie des codes débutent le chapitre. L'identité de MacWilliams est l'expression d'une formule de Poissson qu'il convient de ré-écrire en termes de « co-poids » pour obtenir une forme limpide. L'approche des codes cycliques irréductibles par la description trace et les sommes de Gauss se prolonge aux codes cycliques et abéliens. Dans ce contexte, les poids sont donnés en termes de sommes de Gauss sur une algèbre semi-simple d'où l'on tire des estimations archimédiennes et non-archimédiennes.

1. Codes correcteurs

Lors d'une communication entre deux points des symboles sont utilisés pour échanger des *mots*. L'ensemble A des symboles est fini, c'est l'*alphabet* de communication. Il n'y a pas lieu de distinguer entre deux alphabets de même taille. Dans le cas d'une communication hertzienne les symboles sont obtenues par modulation. Un triplet amplitude a , fréquence ω et phase ϕ caractérise un symbole par l'intermédiaire d'une vibration $t \mapsto a\sin(\omega t+\phi)$. Les vibrations sont émises pendant des intervalles de temps réguliers. Le plus souvent un seul des trois paramètres est variable et suivant le cas, on parle de modulation d'amplitude, de fréquence ou de phase... Le canal de communication est « bruité » : la suite des symboles émis E_1, E_2 etc ... et la suite des symboles reçus R_1, R_2 etc ... ne sont pas identiques.

$$
\begin{tikzcd}
a_1, a_2, \dots, a_k \arrow[d] & & b_1, b_2, \dots, b_k \\
\boxed{\text{ENCODEUR}} \arrow[r, "c_1, c_2, \dots, c_n"] & \dots \arrow[r, "r_1, r_2, \dots, r_n"] & \boxed{\text{DECODEUR}} \arrow[u] \\
& \boxed{\text{BRUIT}} \arrow[u] &
\end{tikzcd}
$$

FIG. 1. Schéma d'une communication protégée sur un canal bruité.

Cependant, les erreurs sont indépendantes des symboles et du temps. Il existe un nombre réel p tel que :

$$1 > \text{Prob}(E_i \neq R_i) = p > 0.$$

Les codes correcteurs d'erreurs permettent de protéger la communication contre ces erreurs de transitions. La figure (FIG. 1) décrit les outils et la stratégie de cette protection. Le mot *message* $\vec{a}$ est encodé pour obtenir un mot de *code* $\mu(\vec{a}) = \vec{c}$. L'encodage introduit de la *redondance* dans le mot $\vec{a}$, avec la conséquence $n \geq k$: c'est le contraire d'une compression. Le mot de code $\vec{c}$ est transmis par le canal bruité, notons $\vec{r}$ le mot effectivement reçu. Le mot $\vec{r}$ est entaché d'erreurs. Le nombre d'erreurs est égal à la distance de Hamming entre les mots $\vec{c}$ et $\vec{r}$. Enfin, le mot reçu est décodé, en un mot $\nu(r) = b$. On souhaite que $a = b$ si le nombre d'erreurs n'est pas trop grand, tout en minimisant la redondance . Cette procédure justifie la définition suivante.

Soit e un entier. Un *code correcteurs d'erreurs* , de capacité de correction e, est une partie C de A^n munie d'une application μ de A^k dans C vérifiant :

$$\forall x, y \in A^k, \quad B(\mu(x), e) \cap B(\mu(y), e) \neq \emptyset \Longrightarrow x = y \tag{46}$$

où $B(z, e)$ désigne la boule fermé de centre z et de rayon e pour la distance de Hamming. Si C est un code alors il existe un algorithme de décodage naïf permettant de retrouver le message émis à partir du message reçu, sa complexité est exponentielle.

En fait, toute partie C de A^n est un code. La capacité de correction est liée à la distance minimale entre deux mots distincts du code. On définit la *distance* du code C par

$$d(C) = \min\{d_H(x, y) \mid x, y \in C \quad \text{et} \quad x \neq y\}$$

et la capacité de correction est égale à $\big(d(C) - 1)/2\big)$. Un $(n, M, d)_q$ code est un code de longueur n de cardinal M et de distance minimale d. L'entier q est la taille de l'alphabet. On définit la *dimension* le *rendement* et la *distance !relative* :

$$
\begin{aligned}
k(C) &= \log_q(M) && \text{(dimension)} \\
R(C) &= \frac{\log_q |C|}{n} && \text{(rendement)} \\
\delta(C) &= \frac{d(C)}{n} && \text{(distance relative)}
\end{aligned}
$$

Le couple $(R(C), \delta(C))$ permet de mesurer la performance d'un code.

PROPOSITION 1.1 (Borne de Singleton). *Soit C un code ;*

$$d(C) \leq n - \lceil k(C) \rceil + 1$$

DÉMONSTRATION. Soit I un sous ensemble de $\{1, \ldots, n\}$ de cardinal $\lceil k(C) \rceil - 1$. L'inégalité $q^{|I|} < M$ montre qu'il existe deux mots x et y dans C qui coïncident sur I,

$$d(C) \leq d(x, y) \leq (n - |I|) = n - \lceil k(C) \rceil + 1,$$

□

Les codes pour lesquels (1.1) est une égalité sont des codes MDS. Leur existence est le sujet d'une des plus importantes conjectures de la théorie des codes, voir [**139**] et le "survey" de J. Hirschfeld et L. Storme [**84**].

Pour une longueur et une distance minimale données, on souhaite construire le plus gros code possible, le cardinal d'un tel code est généralement noté $A_q(n, d)$. Un code C est *maximal* si une inflation de C provoque une diminution de la distance minimale. En d'autres termes,

$$\forall C' \subset A^n, \quad C \subset C' \Longrightarrow d(C') \leq d(C).$$

Considérons un code maximal (n, M, d). Par définition, la réunion des boules centrées en les points de C et de rayon $d - 1$ recouvre l'espace tout entier. On obtient une borne inférieure sur la dimension du code :

$$n \leq k(C) + \log_q \big(V_q(n, d-1)\big) \tag{47}$$

où q désigne le cardinal de l'alphabet et $V_q(n, d-1)$ le nombre d'éléments d'une boule fermée de rayon $d - 1$:

$$V_q(n, d-1) = \sum_{i=0}^{d-1} \binom{n}{i} (q-1)^i.$$

2. Domaine des codes

À chaque code C, on associe le point $\mathcal{M}(C)$ d'abscisse $\delta(C)$ et d'ordonnée $R(C)$. L'ensemble des points $\mathcal{M}(C)$ s'appelle le *domaine des codes* ; c'est une partie du pavé unité. La frontière du domaine des codes joue un rôle important dans la théorie des codes. Cette frontière est le graphe de l'application

$$\alpha(\delta) = \limsup_{n \to \infty} \frac{1}{n} A_q(n, \delta n).$$

C'est une fonction continue de $[0, 1]$ dans $[0, 1]$. La borne de Singleton (1.1) montre que le domaine des codes est inclus dans la région : $\delta + R \leq 1$, elle fournit la borne supérieure

$$\alpha(\delta) \leq 1 - \delta, \qquad \text{(Borne de Singleton asymptotique)}$$

L'inégalité (47) donne la minoration

$$1 - H_q(\delta) \leq \alpha(\delta) \qquad \text{(Borne de Gilbert-Varshamov asymptotique)}$$

où $H_q(\delta) = \lim_{n\to\infty} \frac{1}{n} V_q(n, \delta n)$. Par ailleurs, les approximations usuelles des coefficients binomiaux fournissent l'expression de la fonction d'« entropie [1] » :

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

formule valide pour $x \in [0, \frac{q-1}{q}]$, voir [**184**, page 59]. Dans un même ordre d'idées, on dit qu'une famille infinie de codes $(C_i)_{i\in I}$ est *famille !de bons codes* si la frontière topologiquede l'ensemble $(\mathcal{M}(C_i))_{i\in I}$ contient au moins un point d'abscisse et d'ordonnée non-nulles.

3. $[n, k, d]$-codes

Soit K un corps fini de caractéristique p et de cardinal q. La structure groupe additif de K^n permet de réaliser la distance de Hamming comme une distance invariante par translation. La distance entre deux mots x et y ne dépend que leur différence, elle est égale au poids de $x - y$, le *poids de Hamming* d'un mot $z \in K$ étant :

$$\mathrm{wt}(z) = |\{i \in [1, n] \mid z_i \neq 0\}|$$

Un *code linéaire* est un sous-espace vectoriel de K. Désignons par C un code linéaire de dimension k et de distance minimale d, on dit que C est un $[n, k, d]$-code sur K. Le nombre de mots de poids i dans le code C est noté $A_i(C)$,

$$d(C) = \min\{i \in [1, n] \mid A_i(C) > 0 \quad \text{et} \quad i > 0\}$$

Les codes linéaires sont faciles à encoder. Une *matrice génératrice* de C est une matrice G de k lignes et de n colonnes dont les lignes forment une base de C. Si nous notons $c_1, c_2, \ldots, c_n$ les colonnes d'une matrice génératrice de G alors l'application de K^k dans K^n :

$$\vec{a} = (a_1, a_2, \ldots, a_k) \mapsto \vec{c} = (a_1, a_2, \ldots, a_k).G = (a.c_1, a.c2, \ldots, a.c_n)$$

est un *encodeur* . De l'algèbre linéaire, on déduit l'existence de matrices Z de n lignes par $n - k$ colonnes satisfaisant :

$$x \in C \quad \text{si et seulement si} \quad xZ = 0$$

En conséquence, le code C contient un mot de poids w si et seulement s'il existe une combinaison linéaire à coefficients non nuls de w lignes distinctes de Z qui soit nulle. De ce simple fait, on tire le

Théorème 3.1. *Les codes linéaires forment une classe de bons codes*

Démonstration. Tout d'abord, pour qu'il existe un $[n, k, d]$ il suffit que :

$$\sum_{i=1}^{d-2} C_{n-1}^{i}(q-1)^i < q^{n-k} \qquad \text{(Borne de Varshamov-Gilbert)} \tag{48}$$

En effet, il suffit de construire une matrice Z de n lignes par $n-k$ colonnes vérifiant la propriété :

(*) Toute combinaison linéaires d'au plus d lignes de Z est non nulle.

---

[1] Pour ne pas laisser le lecteur perplexe, je joins le passage de [**174**] qui aidera le lecteur : " The form H will be recognized as that of entropy as defined in certain formulations of statistical mechanics ... See, for example, R. C. Tolman,"principles of Statistical Mechanics."Oxford. Clarendon, 1938."

On construit la matrice Z en n étapes. Pour la première étape, on choisit une matrice Z_1 formée d'une ligne non nulle, Z_1 vérifie (*). Supposons construites Z_1,Z_2, ... Z_k des matrices de k lignes satisfaisant (*). A cause, de l'inégalité (47), l'ensemble des combinaisons linéaires de poids au plus $d-2$ des lignes de Z_k ne recouvrent pas tout l'espace. En ajoutant à la matrice Z_k une des lignes restantes, on obtient une matrice de $k+1$ lignes, satisfaisant (*). □

Le théorème (3.1) montre que pour faire de la protection de l'information, les codes linéaires suffisent, et c'est tant mieux : grâce à l'algèbre linéaire ils sont à priori plus facile à manipuler que les codes aléatoires de la théorie de l'information.

4. Complexité

En fait, on peut même prouver que la majorité des codes linéaires sont bons, et à ce stade, les questions algorithmiques fondamentale portent sur les deux problèmes :

• Le *problème de la distance minimale* : étant donnés une matrice de contrôle H d'un $[n,k]$ code, trouver un mot de poids minimum y satisfaisant $yH=0$ et $y \neq 0$.

• Le *problème du décodage* : étant donnés une matrice de contrôle H d'un $[n,k]$ code, et un un mot quelconque z de K^n, trouver un mot de poids minimum y satisfaisant $yH = zH$.

À ces problèmes d'optimisation sont associés les trois problèmes de décisions :

∘Decodage :

instance	:	une matrice H $n \times m$ à coefficient dans K,
		un vecteur s dans K^m ,
		un entier $w > 0$.
question	:	existe-t-il $y \in K^n$ satisfaisant $\mathrm{wt}(y) \leq w$ et $yH = s$.

∘Distribution de Poids :

instance	:	une matrice H $n \times m$ à coefficient dans K,
		un entier $w > 0$.
question	:	existe-t-il $y \in K^n$ satisfaisant $\mathrm{wt}(y) = w$ et $yH = 0$.

∘Distance Minimale :

instance	:	une matrice H $n \times m$ à coefficient dans K,
		un entier $w > 0$.
question	:	existe-t-il $y \in K^n$ satisfaisant $\mathrm{wt}(y) \leq w$ et $yH = 0$.

Théorème 4.1. *Les trois problèmes de décisions fondamentaux :* Decodage, Distribution de Poids, *et* Distance Minimale *sont tous NP-complets.*

La NP-complétude de ces problèmes est abordée pour la première fois à la fin des années 70, par Berlekamp, McEliece et Van Tilborg. Dans leur note [**14**], ils prouvent la NP-complétude des problèmes Decodage et Distribution de Poids par réduction au problème des trois mariages. Dix-huit ans plus tard, Vardy [**185**] prouve la NP-complétude du problème Distance Minimale par réduction à une version du problème sum-set.

Une conséquence importante de (4.1) est l'impossibilité **pratique** de décoder un code arbitraire, le problème du décodage est NP-Dur. Propriété qui est utilisée pour la conception de certains schémas cryptographiques. On peut montrer que la majorité des codes sont bons, mais nous sommes dans l'impossibilité pratique de construire aléatoirement une suite de bons codes. En résumé, la vision « matrice génératrice » est insuffisante pour construire des bons codes décodables, et de distance minimale connue ni même correctement estimée.

5. Définition $\mathcal{A}$-$\mathcal{B}$-$\mathcal{C}$-d

Le code de Kerdock est un excellent code non-linéaire de l'espace de Hamming ${\mathbf{F}_2}^{2n}$ voir le chapitre VI. Depuis l'article [**79**], on sait que ce code est l'image isométrique d'un code quaternaire de l'espace $(\mathbf{Z}/4\mathbf{Z})^n$ muni de la métrique de Lee. Cette remarquable description du code de Kerdock montre l'intérêt qu'il faut porter envers les codes qui sont des sous-modules dans des espaces métriques autres que l'espace de Hamming.

Soit A un alphabet qui est un anneau fini sans être nécessairement un corps. À la lumière des articles de Wood, il vaut mieux supposer l'anneau A de type quasi-Frobenius. Un *code* est la donnée d'un quadruplet $(\mathcal{A}, \mathcal{B}, \mathcal{C}, d)$ où $\mathcal{A}$ désigne un A-module libre de rang n, $\mathcal{B}$ une base du module $\mathcal{A}$, $\mathcal{C}$ un sous-module de $\mathcal{A}$ et d une distance sur K. Le module $\mathcal{A}$ est l'*espace ambiant du code* et le sous-module $\mathcal{C}$ son *support du code*. L'ensemble des coordonnées des éléments de $\mathcal{A}$ écrits dans la base $\mathcal{B}$ forme le code au sens usuel ; c'est une partie de K^n, le plus souvent identifiée au support du code. A la base $\mathcal{B} = (b_1, b_2, \dots, b_n)$ est associée la forme bilinéaire $(x, y) \mapsto < x, y >$ qui conduit à la définition du *code orthogonal* $(\mathcal{A}, \mathcal{B}, \mathcal{C}^{\perp})$. Si la distance n'est pas précisée, c'est qu'il s'agit de la distance de Hamming.

6. Paramètres fondamentaux

Soit C un code. Nous avons déjà defini trois paramètres : la longueur du code $n(C)$, la dimension du code $k(C)$ et la distance minimale $d(C)$. Dans certaines situations, la connaissance de la *distance maximale* du code est importante, on la note $D(C)$. Pour tout entier i, on note $A_i(C)$ le nombre de mots de poids i dans C.

$$d(C) = \min\{i \in [1, n] \mid A_i(C) > 0\}, \quad D(C) = \max\{i \in [1, n] \mid A_i(C) > 0\}.$$

À l'image de l'espace de Hamming, on considère que la distribution de poids moyenne d'un code suit une loi Gaussienne [2]

Dans un code « projectif » i.e un code dont la distance minimale est supérieure ou égale à trois, le poids moyen d'un mot est $(q-1)n(C)/q$. La déviation maximale, notée $l(C)$ s'appelle la *largeur* du code C :

$$l(C) = \max\{D(C) - \frac{n(C)(q-1)}{q}, \quad \frac{n(C)(q-1)}{q} - d(C)\}.$$

Le polynôme de deux variables :

$$W_C(X, Y) = \sum_{i=0}^{n} A_i(C) X^{n-i} Y^i$$

résume la distribution de poids du code ; c'est le *polynôme énumérateur de poids* . Contrairement aux apparences, cette notation n'est pas arbitraire. Elle permet d'écrire avec concision le lien entre la distribution d'un code et celle de son dual :

$$W_{C^{\perp}}(X, Y) = \frac{1}{q^k} W_C(X + (q-1)Y, X - Y)) \tag{49}$$

[2]En ce point que se différencient la théorie des codes et la théorie de l'information. Du point de vue de la théorie de l'information, un code est bon si la distribution de ses poids suit une loi Gaussienne, même si sa distance minimale est petite.

c'est l'identité de MacWilliams. Nous le verrons plus loin, cette surprenante formule est (encore !) une formule de Poisson.

Le nombre de poids non nuls du code C est un paramètre important , on le note $s(C)$:

$$s(C) = |\{i \in [1,n] \mid A_i(C) > 0\}|$$

La distance minimale de $C^\perp$ s'appelle la *distance minimale duale*, et le nombre de poids non nuls de $C^\perp$ s'appelle la *distance externe* de C. Les paramètres $d(C)$, $s(C)$, $d(C^\perp)$ et $s(C^\perp)$ sont [**58**] *quatres paramètres fondamentaux* du code C.

Le *rayon de recouvrement* de C est le plus petit entier $\rho(C)$ tel que la réunion des boules fermées de rayon $R(C)$ centrée sur des points de C recouvre l'espace de Hamming. Le dual du code $\mathcal{S}(q,r)$ est le *code de Hamming* $\mathcal{H}(q,r)$; c'est un code 1-correcteur de longueur $\frac{q^r-1}{q-1}$ de co-dimension r, son rayon de recouvrement est égal à sa capacité de correction : c'est un *code parfait* [3] . Mis à part les codes de Hamming, il existe seulement deux autres codes parfaits : les deux codes 2-correcteurs de Golay.

7. La catégorie des codes

Les définitions des codes qui précèdent ne sont pas très ambitieuses. Dans un beau et courageux article [**7**], E. Assmus reprend des travaux anciens de Whitney et Slepian. Les codes sont les objets d'une catégorie : la catégorie des codes. Les objets de la catégorie des codes sont des espaces vectoriels, et les morphismes sont des contractions linéaires. Un code C est *décomposable* si et seulement s'il existe une suite exacte de morphismes telle que

$$(0) \longrightarrow U \longrightarrow C \longrightarrow V \longrightarrow (0)$$

L'ensemble des positions couvertes par le code C s'appelle le *support* de C, c'est l'ensemble des positions $i \in [1,n]$ telle qu'il existe un mot $c \in C$ vérifiant $c_i \neq 0$. Un code est décomposable si et seulement s'il est somme directe de deux codes à supports disjoints. Un mot de C est *décomposable* s'il est somme de deux mots de C non-nuls et de supports disjoints. Dans le premier chapitre, nous avons rencontré la notion d'isométrie. L'ensemble des isométries linéaires qui fixent le code C est noté $\mathrm{Aut}(C)$: l'isométrie $(\sigma,\lambda) \in \Sigma_n \ltimes (K^{\times n})$ est dans $\mathrm{Aut}(C)$ si :

$$(\lambda_1 c_{\sigma(1)}, \lambda_2 c_{\sigma(2)}, \dots , \lambda_n c_{\sigma(n)}) = (\sigma,\lambda).\vec{c} \in C, \quad \forall \vec{c} \in C.$$

Le sous-groupe des permutations qui fixent C s'appelle *le groupe des permutations* de C. Il est noté $\mathrm{Per}(C)$. Par projection, on définit deux sous-groupes de $\mathrm{Aut}(C)$ le groupe des symétries $\mathrm{Sym}(C) = \{\sigma \in \Sigma_n \mid (\lambda,\sigma) \in \mathrm{Aut}(C)\}$ et le groupe des automorphismes diagonaux $\mathrm{Diag}(C) = \{\lambda \in K^\times \mid (\lambda,\sigma) \in \mathrm{Aut}(C)\}$

$$\mathrm{Per}(C) \subset \mathrm{Sym}(C) \subset \mathrm{Aut}(C)$$

Sur le corps à deux éléments tous ces groupes coïncident.

THÉORÈME 7.1 (Knapp-Schmidt). *On suppose que le corps de base n'est pas* $\mathbf{F}_2$. *Un code est indécomposable si et seulement si ses automorphismes diagonaux sont tous scalaires.*

THÉORÈME 7.2 (Knapp-Schmidt). *Un code non-trivial dont le groupe des symétries est primitif est indécomposable et ses automorphismes diagonaux sont tous scalaires.*

[3] La notion de rayon de recouvrement est importante pour certain jeux de hasard comme le LOTO-SPORTIF : c'est le fameux "football pool problem" que j'ai eu le plaisir d'expérimenter avec succès !

Ces deux théorèmes proviennent de l'article [**106**] traitant de la construction de codes ayant un groupe d'automorphismes donné par des méthodes cohomologiques. À l'image des codes de Golay, un « bon » code possède un groupe d'automorphismes remarquable, alors que le groupe d'automorphismes d'un code aléatoire est trivial.

8. Identités de MacWilliams

Dans cette section A désigne un anneau quasi-Frobenius de cardinal q. La composition du vecteur u de A^n est le monôme de q variables Z_a indexées par les éléments de l'anneau A :

$$Z(u) = \prod_{i=1}^{n} Z_{u_i} = \prod_{a\in A} Z_a^{\mathrm{wt}_a(u)}$$

où $\mathrm{wt}_a(u)$ désigne le nombre de composantes égale à a dans le vecteur u. La somme des compositions des éléments de C est un polynôme de q variables, noté $\mathcal{W}_C$, c'est l'*énumérateur complet* du code C. Pour obtenir une relation entre l'énumérateur complet d'un code et de son dual, il suffit de calculer la transformée de Fourier de la fonction de composition :

$$\begin{aligned}
\mathcal{F}(Z)(v) &= \sum_{x\in A^n} Z(x)\langle x, u\rangle_{\mathbf{C}}^{A^n}\\
&= \sum_{x_1\in A}\sum_{x_2\in A}\cdots\sum_{x_n\in A}\prod_{i=1}^{n}\prod_{a\in A} Z_a^{\mathrm{wt}_a(x_i)}\langle x_i, v_i\rangle_{\mathbf{C}}^{A}\\
&= \prod_{i=1}^{n}\sum_{x\in A}\prod_{a\in A} Z_a^{\mathrm{wt}_a(x)}\langle x_i, v_i\rangle_{\mathbf{C}}^{A}\\
&= \prod_{b\in A}\big(\sum_{a\in A}\langle a, b\rangle_{\mathbf{C}}^{A} Z_b\big)^{\mathrm{wt}_b(v)}
\end{aligned}$$

Convenons de noter $\widehat{Z_b} = \sum_{a\in A}\langle a, b\rangle_{\mathbf{C}}^{A} Z_a$. Le calcul précédent combiné à la formule de Poisson donne la relation :

$$\mathcal{W}_{t+C}\big((Z_b)_{b\in K}\big) = q^{k-n}\mathcal{W}_{C^\perp}\big((\widehat{Z_b})_{b\in A}\big). \tag{50}$$

Considérons deux nouvelles variables X et Y. On obtient l'énumérateur de poids du code C en substituant la variable Z_0 par X et toutes les autres variables Z_a, $a \neq 0$, par Y. Les relations d'orthogonalité donnent :

$$\hat{Z}_0 = X + (q-1)Y, \quad \text{et} \quad \hat{Z}_b = X - Y, \quad \forall b \neq 0.$$

égalités qui conduisent à la relation de MacWilliams :

$$W_C(X, Y) = q^{k-n} W_{C^\perp}(X + (q-1)Y, X - Y).$$

Une formule particulièrement utile dans la classification des codes auto-duaux via la théorie des invariants puisque l'énumérateur de poids de ces derniers est un polynôme invariant sous l'action des transformations

$$(X, Y) \mapsto \frac{1}{\sqrt{q}}\begin{pmatrix} 1 & q-1 \\ 1 & -1 \end{pmatrix}$$

9. Moments des co-poids

Voyons comment la méthode des sommes de caractère nous conduit à estimer les co-poids plutôt que les poids d'un code. L'anneau quasi-Frobenius A possède un caractère admissible μ_A. Pour x et y dans A^n, posons :

$$\langle x, y\rangle = \mu_A(x.y)$$

Soit x un vecteur de A^n, notons $Z(x)$ le nombre de composantes égales à zéro dans le vecteur x. On déduit des formules d'orthogonalité une première expression de $Z(x)$:

$$Z(x) = \frac{1}{q}\sum_{i=1}^{n}\sum_{\psi\in\widehat{A^+}}\psi(x_i)$$

comme l'anneau A est quasi-Frobenius,

$$\begin{aligned}&= \frac{1}{q}\sum_{i=1}^{n}\sum_{a\in A}\mu_A(ax_i) = \frac{1}{q}\sum_{i=1}^{n}\sum_{a\in A}\mu_A(axe_i)\\ &= \frac{1}{q}\sum_{i=1}^{n}\sum_{a\in A}\langle x, ae_i\rangle = \frac{1}{q}\sum_{s\in S}\langle x, s\rangle + \frac{n}{q}\end{aligned}$$

où S est la sphère de centre 0 et de rayon 1 dans l'espace de Hamming A^n. Cette relation suggère la définition de poids de x rapporté à la moyenne ; c'est le *co-poids* de x :

$$\mathrm{cwt}(x) = qZ(x) - n = (q-1)n - q\mathrm{wt}(x)$$

En notant $\mathbf{1}_S$ la fonction indicatrice de la sphère unité, on obtient :

$$\mathrm{cwt}(x) = \sum_{s\in S}\langle x, s\rangle$$

La transformée de Fourier de $x \mapsto \langle x, s\rangle$ n'est rien d'autre que δ_s, et, sans aucun effort, nous réalisons que la transformée de Fourier de la fonction co-poids est égale à q^n fois l'indicatrice de la sphère unité. Des formules de trivialisation et de la formule de Poisson, nous obtenons les moments d'ordre j des co-poids du z-translaté d'un code M :

$$\frac{1}{|M|}\sum_{x\in z+M}\mathrm{cwt}(x)^j = \sum_{y\in M^\perp}\mathbf{1}_S^{(j)}(y)\langle z, y\rangle \tag{51}$$

où $\mathbf{1}_S^{(j)}$ désigne le produit de convolution itéré j fois de la sphère unité et parce que $M^\perp = M^\perp$!!! On retrouve le fait que si $s \leq d'$ alors la distribution de poids est complètement déterminée. Il faut remarquer que $\mathbf{1}_S^{(j)}(y)$ est égal au nombre de chemins de longueur j pour aller de 0 à y dans le graphe de Hamming. Par exemple,

$$\mathbf{1}_S^{(1)}(0) = 0, \quad \mathbf{1}_S^{(2)}(0) = n(q-1), \quad \mathbf{1}_S^{(3)}(0) = n(2q-3). \tag{52}$$

Et si u est un vecteur de poids trois,

$$1_S^{(1)}(u) = 0, \quad 1_S^{(2)}(u) = 0, \quad 1_S^{(3)}(u) = 6.$$

Mis à part, l'approche proposée, il ne faut rien voir de nouveau dans cette formule qui a déjà été publiée plusieurs fois.

10. Codes cycliques

Soit A un alphabet. Un code cyclique de longueur n sur A est un code dont le groupe d'automorphismes contient l'opérateur de décalage vers la droite

$$(c_1, c_2, \ldots, c_n) \in C \Longrightarrow (c_n, c_1, \ldots, c_{n-1}) \in C$$

Supposons que A soit un anneau commutatif. L'identification du mot $\vec{c}$ avec le polynôme $c(X) = \sum_{i=1}^{n} c_i X^i$ permet de réaliser le décalage vers la droite comme une multiplication par X dans l'anneau quotient $A[X]/(X^n - 1)$. Il y a une correspondance entre les idéaux de $A[X]/(X^n - 1)$ et l'ensemble des codes linéaires cycliques sur A.

La classe des codes cycliques est très importante : elle contient les codes de Reed-Muller raccourcis, les codes résidus quadratiques, et les codes BCH. L'algorithme de décodage de Berlekamp rend la classe BCH attrayante du point de vue applicatif alors que du point de vue théorique la classe n'est pas bonne. Cependant, elle contient la classe des codes de Reed-Solomon qui a été utilisée par Justesen pour obtenir la première classe de bons codes.

La classe des codes cycliques à composantes dans un corps est certainement la classe de codes la plus étudiée. Le lecteur verra comment le vocabulaire des codes cycliques subsiste dans la classe des codes abéliens sur un anneau fini.

Soit K un corps fini de cardinal q et de caractéristique p. Soit n un entier naturel, un *code cyclique* de longueur n est un idéal de l'algèbre $K[X]/(X^n - 1)$. Si C est un code cyclique de longueur n, il existe un et un seul polynôme unitaire $g(X)$ diviseur de $X^n - 1$ tel que C soit l'idéal engendré par la classe de $g(X)$; c'est le *polynôme générateur* de C. Le quotient de $X^n - 1$ par $g(X)$ est noté $h(X)$. Le polynôme réciproque de $h(X)$ engendre le code orthogonal à C, c'est le *polynôme de contrôle* de C. Le code C est formé des polynômes $c(X) = c_0 + c_1 X + \cdots + c_{n_1} X^{n-1}$ qui sont multiples de $g(X)$ modulo $X^n - 1$.

Nous arrivons maintenant à un carrefour important : la caractéristique du corps des symboles divise p ou pas. Dans le second cas, l'algèbre ambiante est semi-simple ce qui facilite l'étude de ces idéaux. Dans le premier cas, on écrit $n = p^\ell N$ avec (p, N) et on déduit des codes cycliques de longueur N certaines propriétés des codes de longueur n. Par exemple, dans sa thèse [**142**], J. P. Martin démontre que la performance des codes cycliques ne dépend pas de la parité de leur longueur.

Plaçons nous dans le cas semi-simple. Soit L le corps de décomposition de $X^n - 1$. L'ensemble $Z(C)$ des racines de $g(X)$ est une partie de $L^\times$: c'est l'*ensemble des zéros* du code. Le complémentaire de $Z(C)$ dans l'ensemble des racines n-ième de l'unités s'appelle le *spectre* de C, on le note $S(C)$. L'ensemble $Z(C)$ caractérise le code C : le polynôme $c(X)$ de degré inférieur à n est dans le code C si et seulement si $c(\beta) = 0$, quelque soit β dans $Z(C)$, ou encore, si et seulement si $c(X)h(X) = 0$.

Toutes ces notions subsistent dans le cas abélien, mais avant d'étudier ces codes en général, le mieux est de s'entrainer avec la classe des codes cycliques irréductibles.

11. Codes BCH

Une importante classe de codes a été introduite indépendamment par R. C. Bose et D. K. Ray-Chaudhuri (1960) et A. Hocquenghem (1959). Il s'agit de la classe des codes BCH . Soient K un corps fini de caractéristique p et n un entier naturel premier avec p. Désignons par α une racine n-ième de l'unité dans une extension convenable de K. Le plus grand code cyclique de longueur n tel que

$$\{\alpha^0, \alpha^1, \dots, \alpha^{\delta-2}\} \subset Z(C)$$

s'appelle le *code* BCH de longueur n et de *distance prescrite* δ, on le note $\mathrm{BCH}_K(\delta, n)$.

PROPOSITION 11.1. *Le code* $\mathrm{BCH}_K(\delta, n)$ *est un code de distance minimale supérieure ou égale à* δ. *Sa dimension est au plus* $n - \delta$. *La classe des codes* BCH *n'est pas une classe de bon codes.*

DÉMONSTRATION. Soit $\sum_{i=0}^{n-1} f_i X^i$ un mot non-nul de $\mathrm{BCH}(\delta, K)$. La transformée de Mattson-Solomon permet d'exprimer f_k comme

$$\begin{aligned} f_k &= \frac{1}{n} \sum_{i=0}^{n-1} \hat{f}(i) \alpha^{-ik} \\ &= \frac{1}{n} \sum_{i=\delta-1}^{n-1} \hat{f}(i) \alpha^{-ik} \end{aligned}$$

Par raison de degré, le nombre de zéros non-nuls de la fonction $\sum_{i=\delta-1}^{n-1} \hat{f}(i) X^i$ est au plus $n - \delta$ d'où l'estimation de la distance minimale. D'autre part, la transformée de Fourier inverse, montre que le code vit dans un espace de dimension inférieure ou égale à $n - \delta + 1$. □

12. Codes cycliques irréductibles

Un code cyclique irréductible est un code cyclique non nul, minimal au sens de l'inclusion. C'est un idéal minimal de l'algèbre $K[X]/(X^n - 1)$. Si $g(X)$ est le polynôme générateur d'un code cyclique irréductible de longueur n alors le polynôme $h(X) = \frac{X^n - 1}{g(X)}$ est irréductible sur K. Soit β une de ces racines, posons $L = K(\beta)$, l'application μ de L à valeurs dans K^n définie par :

$$a \mapsto \mu(a) = \big(\mathrm{tr}_{L/K}(a\beta^1), \mathrm{tr}_{L/K}(a\beta^2), \cdots, \mathrm{tr}_{L/K}(a\beta^n)\big) \tag{53}$$

est un encodeur du code cyclique irréductible engendré par $g(X)$. Le sous-groupe Γ du groupe des caractères multiplicatifs de L orthogonal à β et $K^\times$ joue un rôle fondamental dans l'estimation des poids du code C, son ordre est $\frac{(q^f-1)(n,q-1)}{n(q-1)}$.

PROPOSITION 12.1 (McEliece). *Soit b non nul dans K. Désignons par $N(a, b)$ le nombre d'occurrences de b dans le mot $\mu(a)$.*

$$\begin{aligned} \mathrm{wt}(\mu(a)) &= \frac{n(q-1)}{q(q^f-1)} \big\{ q^f - \sum_{\chi \in \Gamma - \{1\}} G_L(\chi, \mu_L) \bar{\chi}(a) \big\} \\ N(a, b) &= \frac{n}{q} + \frac{n}{q(q^f-1)} \sum_{\chi \in G^\perp} G_L(\chi, \mu_L) G_K(\bar{\chi}) \chi(b) \bar{\chi}(a) \end{aligned}$$

Ces relations sont une conséquence de la formule de Poisson que l'on rencontre dans le cadre des sections hyperplanes d'un groupe. Dans sa thèse [**143**] O. Mbodj les attribue à juste titre à McEliece. Le lecteur trouvera une preuve dans [**148**] mais aussi dans le document ci-dessus. La largeur du code satisfait

$$l(C) \le \big(|\Gamma| - 1\big)\sqrt{q^f} + 1.$$

Le groupe $(GK^\times) \rtimes \mathrm{Gal}(L/\mathbf{F}_p)$ agit sur L par $(g,\phi).a = g\phi(a)$, cette action laisse invariante le poids de $\mu(a)$ et $(GK^\times) \rtimes \mathrm{Gal}(L/\mathbf{F}_p)$ s'identifie à un sous-groupe du groupe des isométries semi-linéaires du code cyclique. La distance duale externe est inférieure au nombre d'orbites de $L^\times$ sous cette action,

$$s(C) \leq \mathrm{NBC}\big(p, \frac{(q^f-1)(q-1)}{n(q-1,n)}\big).$$

Pour cette raison, le nombre de classes cyclotomique de p modulo $\frac{(q^f-1)(q-1)}{n(q-1,n)}$ est appelé le *nombre de poids prescrit*. Un couple (a,b) d'éléments de L forme une *collision* si les poids des mots $\mu(a)$ et $\mu(b)$ sont identiques sans que a et b ne soient sur une même orbite. L'expérience numérique montre que, le plus souvent il y a des collisions et donc le nombre de poids est strictement plus petite que le nombre de classes cyclotomiques de p modulo $\frac{(q^f-1)(q-1)}{n(q-1,n)}$.

Problème 12.1. *Caractériser les couples (n,q) tels que les codes cycliques irréductibles de longueur n sur l'alphabet $\mathbf{F}_q$ soient sans collisions ?*

13. Relation de Hasse-Davenport et codes cycliques

La relation de Hasse-Davenport justifie la construction d'une famille de codes cycliques irréductibles de dimension et longueur variables. Les notation sont celles de la section précédente. Soit L_s l'extension de degré s de L, les caractères du groupe Γ se relèvent par la norme dans le groupe des caractères multiplicatifs pour former un sous-groupe Γ_s de $\hat{L^\times}$. Désignons par m l'ordre commun de ces groupes et considérons la famille de codes cycliques irréductibles de longueurs $\frac{q^{fs}-1}{m}$. Notons α une racine primitive de $L^\times$ et dans chaque extension L_s, faisons le choix d'une racine primitive α_s telle que $\mathrm{N}_{L_s/L}(\alpha_s) = \alpha$. Pour chaque entier i, notons $w_s(i)$ le poids du mot encodé par α_s^i. La proposition (12.1) et la relation de Hasse-Davenport donnent

$$\begin{aligned} w_s(i) &= \frac{q-1}{mq}\big(q^{sf} + \sum_{\lambda \in \Gamma - \{1\}} (-G_L(\lambda))^s \bar{\lambda} \circ \mathrm{N}_{L_s/L}(\alpha_s^i)\big) \\ &= \frac{q-1}{mq}\big(q^{sf} + \sum_{\lambda \in \Gamma - \{1\}} (-G_L(\lambda))^s \bar{\lambda}(\alpha^i)\big) \end{aligned}$$

Ce qui se traduit dans le langage de l'analyse de Fourier du groupe cyclique $\mathbf{Z}/m\mathbf{Z}$ en

$$\mathcal{F}(w_s) = \frac{q-1}{mq}\big(\mathcal{F}(w_1)\big),^s$$

qui suggère de poser $E_s(Z) = \frac{q-1}{mq}\sum_{i=0}^{m-1} w_s(i) Z^i$ pour appliquer les formules de trivialisation du produit de convolution et obtenir cette superbe formule :

$$E_s(Z) = E_1(Z)^s \pmod{Z^m - 1}. \tag{54}$$

Problème 13.1. *Généraliser ce type de formule au cas des codes cycliques, des codes abéliens, des codes géométriques...*

14. Codes à deux poids

Les codes à deux poids ont retenu l'attention de nombreux chercheurs. On connaît des familles de codes à deux poids sur un alphabet donné et quelques cas isolés. Tous les codes cycliques irréductibles de poids prescrit deux sont connus. Dans mon article *A new class of two weights codes* [**125**], j'étudie les codes cycliques irréductibles à deux poids mais de poids prescrit trois.

PROPOSITION 14.1 (Delsarte). *Soit C un $[n,k]$-code projectif à deux poids non-nuls w_1 et w_2 à coefficients dans un corps de caractéristique p. Il existe deux entiers $u > 1$ et $r \geq 0$ tels que*

$$w_1 = up^r, \quad \textit{et} \quad w_2 = (u+1)p^r.$$

On construit une famille infinie de codes à deux poids de la façon suivante. Le point de départ est une chaîne de corps $\mathbf{F}_q \subset K \subset L$ telle que $[L:K] = 2$. Soit Ω une partie de L constituée de de n points deux à deux non K-colinéaire. L'image de L par l'encodeur :

$$\begin{aligned} L &\to K \\ a &\mapsto \left(\mathrm{tr}_{L/\mathbf{F}_q}(a\omega)\right)_{\omega\in\Omega} \end{aligned}$$

est un code DPE à deux poids car l'hyperplan d'équation $\mathrm{tr}_{L/\mathbf{F}_q}(ax) = 0$ contient au plus une K-droite de L.

15. Codes cycliques irréductibles à deux poids

Soient p et ℓ deux nombres premiers satisfaisant les conditions *résidus quadratiques* : ℓ est un nombre premier impair congru à 3 modulo 4, différent de 3 tel que le groupe engendré par p est dans ${\mathbf{F}_\ell}^\times$ est d'indice 2. On note L le corps de décomposition de $X^\ell - 1$ sur $K = \mathbf{F}_p$. Le degré de L sur K vaut $f = \frac{\ell-1}{2}$. Pour tout entier x, $s_p(x)$ désigne le poids p-aire de x, $s_p(x)$ est la somme des chiffres de x lu en base p. Posons

$$t = \frac{1}{p-1}s_p(\frac{q-1}{\ell}), \quad t' = \frac{1}{p-1}s_p(\frac{(q-1)(l-1)}{\ell}).$$

Les nombres t' et t sont des entiers rationnels liés par la relation $t'+t = f$. De plus, $t' > t$, nous noterons h la différence $t'-t$. Le nombre h est égal au nombre de classes d'idéaux du corps quadratique imaginaire $\mathbf{Q}(\sqrt{-\ell})$. En particulier, si ν_ℓ désigne le caractère quadratique de $\mathbf{F}_\ell$ alors

$$h = \sum_{0<x<\frac{\ell}{2}} \nu_\ell(x),$$

de plus, $t = \frac{f-h}{2}$ et $t' = \frac{f+h}{2}$. Le groupe $\mathcal{R}$ des résidus quadratiques modulo ℓ est engendré par p. Notons $\mathcal{N}$ les non résidus modulo ℓ, c'est la classe de -1 modulo $\mathcal{R}$. Nous savons

$$\sum_{x\in\mathbf{F}_\ell}\left(\frac{x}{\ell}\right)\mu_{\mathbf{F}_\ell}(x) = i\sqrt{\ell} = \sum_{r\in\mathcal{R}}\mu_{\mathbf{F}_\ell}(r) - \sum_{n\in\mathcal{N}}\mu_{\mathbf{F}_\ell}(n)$$

en particulier, si κ désigne l'élément quadratique $\frac{-1+i\sqrt{l}}{2}$ alors

ℓ	7	11	19	67	107	163	499
h	1	1	1	1	3	1	3
p	2	3	5	17	3	41	5
s	1	1	1	1	1	1	1

TAB. 1. Code à deux poids

$$\kappa^2 + \kappa + \frac{l+1}{4}, \quad \kappa = \sum_{r \in \mathcal{R}} \mu_{\mathbf{F}_\ell}(r).$$

Soit λ un caractère multiplicatif d'ordre ℓ sur L. À son conjugué près, la somme de Gauss $G_L(\lambda)$ est égale à $p^t(a+\kappa b)$, où les entiers a et b sont deux entiers rationnels complètement définis par les conditions :

$$a^2 - ab + b^2\frac{\ell+1}{4} = p^h, \quad 2a - b \equiv -2p^{t'} \, [\ell], \quad p \not| b, \quad b > 0.$$

Soient a_s et b_s les deux entiers définis par $a_s + b_s\kappa = (a + b\kappa)^s$. Le s-ième code cyclique irréductible de longueur $\frac{p^{fs}-1}{\ell}$ est un code de distance duale prescrite 3. Le poids d'un mot prend l'une des trois valeurs :

$$w_{\mathcal{R}} = \frac{p-1}{\ell p} p^{ts}\big(p^{t's} + (-1)^s(-a_s - \frac{\ell-1}{2}b_s)\big)$$
$$w_0 = \frac{p-1}{\ell p} p^{ts}\big(p^{t's} + (-1)^s\frac{\ell-1}{2}(2a_s - b_s)\big)$$
$$w_{\mathcal{N}} = \frac{p-1}{\ell p} p^{ts}\big(p^{t's} + (-1)^s(-a_s + \frac{\ell+1}{2}b_s)\big)$$

PROPOSITION 15.1. [**125**, π_λ] *Le code irréductible $I_s(\ell, L, K)$ possède une collision si et seulement si $\frac{\ell+1}{4} = p^{hs}$. Dans ce cas, les deux poids du code sont*

$$w_2 = \frac{p-1}{\ell p} p^{ts}(p^{t's} + \epsilon\frac{\ell-1}{2}) \qquad \frac{(p^{fs}-1)(\ell+1)}{2\ell} \quad \textit{fois}$$
$$w_1 = \frac{p-1}{\ell p} p^{ts}(p^{t's} - \epsilon\frac{\ell+1}{2}) \qquad \frac{(p^{fs}-1)(\ell-1)}{2\ell} \quad \textit{fois}$$

avec $\epsilon = +1$ ou -1 suivant que $p = 2$ ou non.

Les codes à deux poids obtenus de cette manière sont rares. La table (1) donne la liste des codes à deux poids pour $3 < \ell \leq 5000$. Le premier code de la liste est le code de Golay de longueur 11 sur $\mathbf{F}_3$.

CONJECTURE 15.1 (Schmidt). *La classe des codes cycliques irréductibles à deux poids dont le nombre de poids prescrit est supérieur ou égal à trois est finie.*

16. Distribution de poids équilibrée

Soit K un corps fini de caractéristique p et de cardinal q. Un code dans lequel chaque poids non-nul apparaît avec la même multiplicité est un *code à distribution de poids équilibrée*. En abrégé, un code DPE à N poids est un code à distribution de poids équilibrée qui possède N-poids non-nuls distincts. Les codes simplexes sont des codes DPE à 1 poids et inversement. Les premiers codes N-DPE avec $N > 1$ ont été remarqués par J.-P. Zanotti. Les équations de Vera Pless donnent des conditions nécessaires pour l'existence de ces codes.

PROPOSITION 16.1. *Soit C un $[n,k]$-code projectif DPE à N poids non nuls distincts : w_1, w_2 etc... La multiplicité de ces poids est $A = \frac{q^k-1}{N}$ et*

$$A\sum_{i=1}^{N} w_i = n(q-1)q^{k-1}$$

$$A\sum_{i=1}^{N} w_i^2 = q^{k-2}(q-1)n(n(q-1)+1)$$

D'où l'on tire, par exemple, que la dimension k d'un code DPE à deux poids est paire, que sa longueur est $n = (q^k-1)/2(q-1)$, et que ces poids sont de la forme $(q^t \pm 1)q^{t-1}/2$.

En choisissant correctement les paramètres de la construction des codes à deux poids de la section 14, on obtient des codes DPE à deux poids. Mais il existe des codes N-DPE avec $N \geq 3$ dans la classe des codes cycliques irréductibles.

PROPOSITION 16.2. [**133**, $\pi\lambda$] *Il existe un code cyclique irréductible de de dimension s, de longueur n à distribution de poids équilibrée et de distance duale N si et seulement si*

$$N = \frac{(q^s-1)(n,q-1)}{n(q-1)}, \quad et \quad N \text{ divise } p-1.$$

DÉMONSTRATION. La condition est suffisante, c'est une application de la section sur les groupes à section régulières. □

17. Codes abéliens

La classe des codes abéliens qui fait son apparition avec les travaux de Berman et Camion contient la classe des codes cycliques. Un *code abélien* à composantes dans un corps K est un idéal d'une K-algèbre de groupe $K[G]$ pour un certain groupe abélien G. Cette définition généralise la notion de code cyclique puisque l'algèbre $K[\mathbf{Z}/n\mathbf{Z}]$ est isomorphe à l'algèbre $K[X]/(X^n-1)$. Là encore, l'algèbre $K[G]$ est semi-simple si et seulement si p ne divise pas l'ordre de A. Le lecteur peut consulter mon rapport de recherche [**128**] pour des détails sur ces codes.

PROBLÈME 17.1. *Etudier les codes sous-modules de l'algèbre de groupe $K[G]$, avec G non-commutatif.*

Le fait de supposer que K soit simplement un anneau de Galois n'introduit pas de difficultés supplémentaires pour obtenir un théorème de structure.

PROBLÈME 17.2. *Aller à la pêche aux nouveaux codes, en considérant les sous-modules de l'anneau de groupe abélien $A[G]$, où A est un anneau fini et G commutatif.*

THÉORÈME 17.1. *Soit G un groupe abélien d'ordre premier avec un nombre premier p. Quelques soient les entiers d et ℓ, il existe s extensions $GR(p^\ell, d_i)$ de $GR(p^\ell, d)$ telles que :*

$$GR(p^\ell, d)[G] \sim \bigoplus_{i=1}^{s} GR(p^\ell, d_i)$$

DÉMONSTRATION. Nous allons définir une transformée de Fourier-Mattson-Solomon pour construire un isomorphisme. Notons n l'ordre de G, et N son exposant. Sans perdre en généralité, nous pouvons supposer :

$$G = \prod_{i=1}^{t} \mathbf{Z}/(n_i)\mathbf{Z}$$

Soit ζ un élément d'ordre N dans une extension de $GR(p^\ell, d)$. Si D désigne l'ordre de $q := p^d$ modulo N alors $GR(p^\ell, d)[\zeta] = GR(p^\ell, D)[\zeta]$. Pour chaque couple (a, b) d'éléments de A posons :

$$\langle a, b\rangle = \zeta^{\sum_{i=1}^{t} a_i b_i e_i}$$

où $e_i = \frac{N}{n_i}$. L'application $(a, b) \mapsto \langle a, b\rangle$ est un accouplement ; c'est une application $\mathbf{Z}$-bilinéaire symétrique satisfaisant $\langle a, pb\rangle = \langle pa, b\rangle = \langle a, b\rangle^p$, et la relation d'orthogonalité :

$$\sum_{x\in A} < a, x >= \begin{cases} |G|, & a = 0; \\ 0, & \text{sinon.} \end{cases}$$

La transformée de Fourier-Mattson-Solomon d'un élément f de $GR(p^\ell, d)[G]$ est la fonction $\hat{f}$ de $GR(p^\ell, D)^G$ définie par :

$$\hat{f}(u) = \sum_{a\in A} f(a) < a, u >$$

La transformée de Fourier n'est pas surjective, elle est injective son inverse à gauche est la transformée de Fourier-Mattson-Solomon inverse qui envoie la fonction g de $GR(p^\ell, D)^G$ sur :

$$\check{g}(u) = \sum_{a\in A} g(a) < a, -u >$$

Notons q le cardinal du corps résiduel de $GR(p^\ell, d)$, et notons σ l'automorphisme de $GR(p^\ell, D)$ caractérisé par $\sigma(\zeta) = \zeta^q$. L'image de $GR(p^\ell, d)[G]$ par la transformée de Fourier-Mattson-Solomon est constituée des applications g de $GR(p^\ell, d)^G$ vérifiant $g(q.a) = \sigma(g(a))$.

Désignons par Ω_1, Ω_2, ... , Ω_s les orbites de G sous l'action de la permutation $a \mapsto qa$, notons f_j le cardinal de l'orbite Ω_j. Enfin, pour chaque indice i, $1 \le i \le s$, faisons le choix d'un représentant ω_i de l'orbite Ω_i. La transformée de Fourier de f est complètement déterminé par la transformée de Fourier réduite :

$$\tilde{f} = \big(\hat{f}(\omega_1), \hat{f}(\omega_2), \ldots , \hat{f}(\omega_s)\big)$$

de là, on déduit l'isomorphisme du théorème, entre l'anneau groupe $GR(p^\ell, d)$ et le produit d'anneaux de Galois $\bigoplus_{i=1}^{s} GR(p^\ell, f_i d)$. □

Considérons un code abélien de l'anneau de groupe $GR(p^\ell, d)[G]$. Les anneaux de Galois $GR(p^\ell, d_i)$ sont principaux de hauteur ℓ. L'idéal maximal de $GR(p^\ell, d_i)$ est engendré par p. Il existe s entiers r_1, r_2 ... r_s dans l'intervalle $[0, \ell]$ tels que ,

$$\widehat{C} = \sum_{i=1}^{s} GR(p^\ell, d_i)p^{r_i}$$

Nous dirons que les éléments de Ω_i sont des *zéros* d'ordre r_i. L'union des produits cartésien $\Omega_i \times \{r_i\}$ s'appelle l'*ensemble des zéros* du code C. Le *spectre* s'obtient par passage au complément à ℓ sur les ordres. En particulier, le spectre de C est égal à l'ensemble des zéros de l'annulateur :

$$\operatorname{ann}(C) = \sum_{i=1}^{s} GR(p^\ell, d_i) p^{\ell - r_i}$$

L'opposition dans G induit une involution sur l'ensemble des classes cyclotomiques Ω_i, et donc une permutation ρ sur l'ensemble $\{1, 2, \ldots, s\}$; d'où la notion de *code réciproque* de C :

$$C^* = \sum_{i=1}^{s} GR(p^\ell, d_i) p^{r_{\rho(i)}}$$

L'anneau de groupe $GR(p^\ell, d)[G]$ est muni d'une forme bilinéaire :

$$(f, g) = \sum_{a \in A} f(a) g(a),$$

qui permet de définir l'orthogonal $C^\perp$ d'un code abélien. Le lecteur vérifiera que les opérations d'annulation et d'opposition commutent, et que :

$$\operatorname{ann}(C^*) = C^\perp = \operatorname{ann}(C)^*$$

Cette dernière relation est particulièrement utile, pour décider de l'existence de code auto-duaux dans l'anneau $GR(p^\ell, d)[G]$.

18. Représentation trace

Soit $\operatorname{ann}(C)$ l'annulateur du code abélien C. Notons A l'algèbre quotient $k[G]/\operatorname{ann}(C)$. À partir de la forme trace de A sur K, notée $\operatorname{tr}_{A/K}$, on construit un encodeur $\mu_{G,A}$ qui envoie A dans $K[G]$ de la façon suivante :

$$a \xrightarrow{\mu_{G,A}} \textstyle\sum_{g \in G} \operatorname{tr}_{A/K}(ag) g^{-1} \tag{55}$$

Cet encodeur, bien connu dans le cas des codes cycliques irréductibles, est présenté dans mon article *weight of abelian codes* [**120**]. On constate que si l'annulateur de C est sans élément nilpotent, on dit aussi que C est dans le socle de $k[G]$, alors l'algèbre A est semi-simple, et l'image de A par $\mu_{G,A}$ est exactement égal au code C, que l'algèbre $K[G]$ soit semi-simple ou pas.

PROPOSITION 18.1. [**129**, π_λ] *Si I est un idéal de $K[G]$ tel que ann(I) est radical alors l'idéal I est égal à l'image de la K-algèbre $B = k[G]/ann(I)$ par l'encodeur (55).*

C'est ce que j'appelle une *représentation trace* du code C. Cette approche, nous conduit au problème suivant. Etant donné , une algèbre semi-simple A, un sous-groupe G de $A^\times$, un élément a de A et un élément $b \in K$; Quel est le nombre $N(a, G, b)$ de solutions g de l'équation

$$\operatorname{tr}_{A/K}(ag) = b, \qquad g \in G$$

Le nombre $N(a, G, b)$ s'exprime en termes de sommes de Gauss dont les développement $\mathcal{P}$-adiques sont bien connus depuis Stickelberger, d'où l'on tire la divisibilité d'un code abélien.

19. Groupe d'automorphismes d'un code abélien

L'encodeur (55) suggère la définition d'un code abélien dans un cadre encore plus général. On se donne un anneau fini commutatif B libre sur un de ces sous-anneau quasi-Frobenius A, φ une application non-dégénérée et enfin G est un sous-groupe de $B^\times$ de rang maximal dans B. À cette situation correspond un encodeur :

$$\begin{aligned} \mu \colon B &\to A[G] \\ b &\mapsto \sum_{g \in G} \varphi(bg) X^g \end{aligned}$$

L'image par μ est notée M. À chaque automorphisme f du code M, on associe une application linéaire f^* de sorte à obtenir un diagramme commutatif

$$\begin{tikzcd} B \arrow[r, "\mu"] \arrow[d, "f^*"'] & M \arrow[d, "f"] \\ B \arrow[r, "\mu"] & M \end{tikzcd}$$

Par définition, f est un automorphisme du code M si f est un automorphisme du A-module M qui conserve le poids de Hamming. On en déduit que f^* est un automorphisme linéaire de B tel que, quelque soit $b \in B$

$$\mathrm{wt}\big(\mu(f^*.b)\big) = \mathrm{wt}\big(\mu(b)\big)$$

par la méthode des caractères, nous obtenons :

$$\sum_{\psi \in \widehat{A}} \sum_{g \in G} \psi\big(\varphi(f^*.bg)\big) = \sum_{\psi \in \widehat{A}} \sum_{g \in G} \psi\big(\varphi(bg)\big)$$

Convenons de noter ϕ l'adjoint de f^* pour le produit scalaire $(x, y) \mapsto \varphi(xy)$. Ainsi, relation d'orthogonalité oblige, quelque soit ψ et quelque soit g il existe $\psi' \in \widehat{A}$ et $g' \in G$ tels que

$$\psi \circ \varphi(b\phi(g)) = \psi' \circ \varphi(bg')$$

En particulier, l'anneau A étant quasi-Frobenius, on en déduit qu'il existe $\alpha \in A^\times$ tel que $\phi(g) = \alpha g'$. La réciproque n'est pas difficile à établir. Nous venons de généraliser un théorème de Zanotti [**200**].

Proposition 19.1. *Le groupe des automorphismes du code M est isomorphe au sous-groupe $\mathcal{G}(A, B, G)$ du groupe linéaire $\mathrm{GL}_A(B)$ formé des applications ϕ qui fixent le groupe $G.A^\times$.*

Le groupe $\mathcal{G}(A, B, G)$ contient un sous-groupe $\mathcal{G}(A, B, G)^+$ formé des applications ϕ vérifiant la condition plus restrictive :

$$\forall x \in B, \quad \phi(x) \in (G.A^\times)x$$

Dans le cas d'un code cyclique irréductible (n, K, L) sans collisions ces deux groupes sont identiques, égaux à $\mathbf{Z}/n\mathbf{Z} \rtimes \mathrm{Gal}(L/K)$. Ce qui s'applique aux codes à distributions de poids équilibrées. C'est une conséquence du très beau

Théorème 19.1 (Carlitz-McConnel). *Soient L un corps fini de caractéristique p et de cardinal q et G un sous-groupe d'ordre $d < q-1$ du groupe $L^\times$. Les applications de L dans L qui satisfont*

$$\forall x, y \in L, \quad x \neq y \Longrightarrow \frac{f(x)-f(y)}{x-y} \in G$$

sont de la forme $x \mapsto a + bx^{p^j}$, avec $a \in L$, $b \in G$ et j vérifiant $(q-1)$ divise $d(p^j - 1)$.

Démonstration. voir [**27**]. □

Problème 19.1. *Que devient le théorème précédent dans le cas d'un anneau fini ?*

20. Poids d'un code abélien

Supposons a inversible dans A. La méthode de dénombrement par les caractères, fondée sur les relations d'orthogonalité conduit à l'expression

$$N(a, G, 0) = \frac{1}{|G|} \sum_{\chi \in G^\perp} \sum_{\mathrm{tr}_{A/K}(ax)=0} \chi(x) \tag{56}$$

La somme interne est une *somme d'Eisenstein*, une application directe de la formule de Poisson conduit à une expression de $N(a, G, 0)$ en termes de *sommes de Gauss*

$$N(a, G, 0) = \frac{n}{q} + \frac{n(q-1)}{q|A^\times|} \sum_{\chi \in (GK^\times)^\perp} G_A(\chi, \mu_A)\bar{\chi}(a) \tag{57}$$

Proposition 20.1. [**129**, π_λ] *Soient B une K-algèbre commutative semi-simple, G un sous-groupe du groupe multiplicatif $B^\times$, $a \in B^\times$ et $c \in K^\times$. Le nombre $N(a, G, c)$ d'éléments $g \in G$ tel que $\mathrm{tr}_{B/K}(ga) = c$ satisfait les inégalités*

$$\left|N(a, G, 0) - \frac{n}{q} - (-1)^s \frac{q-1}{qm}\right| \leq \frac{q-1}{q}\frac{h-1}{m}\sqrt{|B|} \tag{58}$$

$$\left|N(a, G, c) - \frac{n}{q} + (-1)^s \frac{1}{qm}\right| \leq \frac{(m-h)\sqrt{q} + h - 1}{qm}\sqrt{|B|} \tag{59}$$

21. Divisibilité des codes cycliques

Rappelons que le poids du mot $c(X)$ désigne le nombre de coefficients non nuls de $c(X)$. Un code est dit d divisible si les poids de ses mots sont tous divisibles par d. On sait que la somme des poids des mots d'un code projectif de dimension k et de longueur n vaut : $(q-1)q^{k-1}n$, ce qui donne une première contrainte sur les valeurs possibles de d.Le théorème qui suit, prouvé par McEliece dans [**147**] donne une information sur la divisibilité d'un code cyclique p-aire.

Théorème 21.1 (McEliece). *Si w désigne le plus petit entier multiple de $p-1$ tel qu'il existe une séquence de w éléments dans $S(C)$: $\gamma_1, \gamma_2, \ldots, \gamma_s$ vérifiant $1 = \prod_{i=1}^s \gamma_i$ alors les poids des mots du code C sont tous de valuation p-adique supérieure ou égale à $\lambda(C) := \frac{w}{p-1} - 1$. De plus, si $h(1) \neq 0$ alors il existe un mot de valuation exactement égale à $\lambda(C)$.*

Ce théorème a été étendu a la classe des codes abéliens p-aire par Delsarte dans [**57**], puis à la classe des codes abéliens q-aire dans [**63**]. Plus récemment [**30**], A.R. Calderbank, W.-C. W. Li et B. Poonen ont donnés des résultats sur la divisibilité de certains codes cycliques construits sur des anneaux de Galois. Cet article suggère l'étude p-adique des sommes de Gauss sur un anneau de Galois, c'est un des objets de mon prochain rapport [**117**].

22. Divisibilité dans les codes abéliens

Soit a un élément de support S. Notons Γ_S l'orthogonal du groupe $G_S K^\times$. Désignons par Ω_S l'ensemble des caractères non triviaux de Γ_S dont la somme de Gauss est de valution π-adique minimale, et notons ν_S cette valeur. De la proposition (57), on tire sur le champ :

$$N(a,G,0) = \frac{n}{q}\big[1 + \frac{(q-1)(-1)^s}{|A_S^\times|} + \pi^{\nu_S} \sum_{\chi\in\Omega_S} a(\chi)\bar{\chi}(a) + O(\pi^{\nu_S})\big] \tag{60}$$

Où les $a(\chi)$ sont des inversibles dans $\mathbf{Z}_p$ qu'il est inutile de préciser. Posons $w := \inf_S\{\nu_S\}$, c'est un entier inférieur au produit $(p-1)f.f_j$ quelque soit j. Le poids du mot $\mu_{G,A}$ s'écrit :

$$W(a,G) = \frac{n}{q}\big[C(S) - \pi^{\nu_S}\sum_{\chi\in\Omega_S} a(\chi)\bar{\chi}(a) + O(\pi^{\nu_S})\big] \tag{61}$$

où $C(S)$ est un entier de valuation π-adique supérieure ou égale à $\min_{j\in S}\{(p-1)ff_j\}$, donc supérieure à w.

THÉORÈME 22.1 (Delsarte-McEliece). *Tous les poids du code C sont de valuation p-adique supérieure ou égale à celle de n augmentée de $\frac{w}{p-1} - f$. Et si n est premier avec p alors il existe un mot dont le poids est de valuation $\frac{w}{p-1} - f$*

DÉMONSTRATION. La première partie est évidente. Pour la seconde partie, rappelons que si n est premier avec p alors les caractères de G sont indépendants modulo p. □

Reste à déterminer la valeur de w. Pour chaque entier j, χ_j désigne le caractère de Teichmüller du corps $\mathbf{F}_{q_j}$. Le caractère $\times_{j\in S}\chi_j^{\alpha_j}$ est dans Γ_S si et seulement si :

$$\sum_{j\in S}\alpha_j a^{(j)} = 0, \quad \text{et} \quad \sum_{j\in S}\alpha_j \equiv 0 \pmod{q-1}. \tag{62}$$

En effet. La congruence caractérise l'orthogonalité du caractère $\times_{j\in S}\chi_j^{\alpha_j}$ par rapport à $K^\times$. Nous pouvons choisir les ζ_{n_j} de sorte que $\chi_j(\zeta_{n_j}) = \exp(\frac{2i\pi}{n_j})$. Le caractère $\times_{j\in S}\chi_j^{\alpha_j}$ est dans l'orthogonal de G_S si et seulement si :

$$\forall i,\quad \times_{j\in S}\chi_j^{\alpha_j}(e_i) = 1 \iff \forall i,\quad \sum_{j\in S}\frac{\alpha_j a_i^{(j)}}{n_j} \in \mathbf{Z} \iff \sum_{j\in S}\alpha_j a^{(j)} = 0.$$

Il résulte des congruences de Stickelberger et des conditions (62) que l'entier w du théorème est :

$$\min_{S} \min_{\alpha} \sum_{j \in S} S(\alpha_j). \tag{63}$$

où S varie dans l'ensemble des parties de $\{1, 2, \ldots, s\}$, et où pour chaque S, α décrit l'ensemble des vecteurs non nuls satisfaisant les conditions (62) .

CHAPITRE 5

Séquences

Les principes de télécommunications modernes sont fondés sur l'utilisation de signaux possèdant de « bonnes » propriétés de corrélation. L'autocorrélation intervient dans les applications de type « radar » pour résoudre des problèmes de synchronisation et de détection de canal. L'intercorrélation est au coeur des communications à accès multiples. La révolution télématique que nous vivons génère son lot d'interrogations. L'une des plus importante jamais relayée par les media : comment construire des familles de séquences idéalement intercorrélées pour désembouteiller les autoroutes de l'information du prochain millénaire ? Pour construire ces ensembles de séquences, que les ingénieurs appellent des *codes*, on utilise les objets de la théorie combinatoire algébrique : fonctions idéalement corrélées, matrices de Hadamard, ensemble à différences, et configurations tactiques dont j'utilise les notations usuelles, c'est la raison pour laquelle j'utilise la lettre v pour désigner la longueur d'une séquence.

Dans ce chapitre, après quelques notations et motivations préliminaires, j'explique comment la théorie des ensembles à différences prend en partie sa source dans un article de J. Hadamard (1865–1963). À cette occasion, nous ferons un détour inattendu jusqu'à Lewis Caroll ! Les définitions d'ensembles à différences, de fonctions parfaites et de multipleurs suivent. Une section est consacrée à quelques théorèmes de Turyn [1] tirés de l'article *Character Sums and Differences Sets*, le "multiplier theorem" est une fine conséquence de la formule de Poisson. Après quelques conjectures liées ła notion de groupe de décomposition, j'expose mes résultats sur la non-linéarité, les fonctions courbes généralisées et les séquences presque-parfaites. Le programme de construction [**127**] d'une famille d'intercorrélation à partir d'un anneau fini et d'un sous-groupe de ses caractères additifs clos le chapitre.

1. Des séquences, pourquoi faire ?

Une *séquence* de longueur v est une suite finie de v nombres complexes s_0, s_1 etc... Une séquence de longueur v s'identifie à une suite périodique de période v, ou encore à une application complexe de domaine $\mathbf{Z}/v\mathbf{Z}$. En pratique, la modulation de phase permet de transmettre des séquences à valeurs dans le cercle unité, ce sont des séquences PSK : Phase Shift Key.

Dans une application de type « synchronisation », le recepteur compare le signal reçu avec un modèle. Il utilise un corrélateur qui à chaque instant calcule le produit scalaire d'un vecteur de base $(a_0, a_1, \dots, a_{v-1})$ avec le vecteur variable $(r_0, r_1, \dots, r_{v-1})$ formé des v derniers symboles reçus. Ce vecteur est initialisé à 0, et lorsqu'un signal s de période v est envoyé vers le récepteur, la suite des nombres calculés par le corrélateur commence par une séquence de zéros, suivis de v valeurs

[1]L'un de ceux qui a fait le plus pour la théorie des ensembles à différences, R. J. Turyn est trop rarement cité. L'article dont il est question n'est pas dans les références de notre « bible » [**139**]. Son nom n'apparaît pas dans la bibliographie du *Design Theory* de Beth, Jungnickel et Lenz...

particulières $a \ltimes r(v-1)$, $a \ltimes r(v-2)$ etc...

$$a \ltimes r(\tau) = \sum_{j-i=\tau} a_i r_j^* = \sum_{i=0}^{v-1-\tau} a_i r_{i+\tau}^*, \quad 0 \leq \tau \leq v-1.$$

Les opérations qui portent sur les indices ne sont pas faites modulo v, c'est le mode *apériodique*, et $a \ltimes r(\tau)$ est le coefficient d' *intercorrélation apériodique* de a par r. Ensuite, le corrélateur rentre dans un régime *périodique* $a \times r(v-1)$, $a \times r(v-2)$ etc...

$$a \times r(j) = \sum_{j-i=\tau} a_i r_j^* = \sum_{i=0}^{v-1} a_i r_{i+\tau}^*, \quad 0 \leq \tau;$$

où les calculs sur les indices sont faits modulo v. En général, les séquences a et r sont identiques, on parle d'*autocorrélation*. Les fonctions d'autocorrélations apériodique et périodique sont liées par la relation :

$$f \times f(\tau) = f \ltimes f(\tau) + \overline{f \ltimes f(v-\tau)} \tag{64}$$

Les fonctions périodique dont la fonction d'autocorrélation reste faible hors phase sont à la base des principes de télécommunications. Une fonction idéale est une fonction dont les coefficients d'autocorrelations sont tous nuls sauf en zéro. On dit que f est à *autocorrélation parfaite*. Dans un radar, une fonction à autocorrélation parfaite est émise. L'écho est égal à un déphasage du signal émis perturbé par des erreurs. Le corrélateur détecte le décalage tant que le nombre d'erreurs reste inférieur à $\frac{v}{2}$. Dans la radio-mobile, la position du récepteur est inconnue. Pour assurer la réception, l'émission se fait dans toutes les directions. À cause des échos, le message reçu est une combinaison linéaire de tous les déphasages du message émis. Si s désigne le signal émis alors le signal reçu est vaut $\sum_\tau a_\tau s(t-\tau)$. Les a_τ caractérisent les conditions de la transmission. On les détermine par corrélation, en utilisant une séquence parfaite. Dans le téléphone cellulaire plusieurs émetteurs transmettent des signaux vers un récepteur unique qui en reçoit leur somme. Chaque poste module son message avec une séquence propre. Les séquences utilisées sont faiblement auto- et intercorrélées, de sorte que, par un calcul de corrélation, le récepteur peut déterminer les différents messages.

2. Matrice de Hadamard

Etant donné un déterminant $n \times n$

$$\Delta = \begin{matrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n,1} & a_{n,2} & \cdots & a_{n,n} \end{matrix}$$

dans lequel on sait que les éléments sont inférieurs en module à une quantité déterminée A, il y a souvent lieu de chercher une limite que le module de Δ ne puisse dépasser. À peu de choses près, c'est en ces termes que débute l'article de J. Hadamard [**78**]. On peut supposer $A = 1$, après nous avoir fait remarquer que la majoration $\Delta \leq n!$ n'est pas bonne, il utilise des propriétés « bien connues » du déterminant pour obtenir la majoration :

$$|\Delta| \leq n^{\frac{n}{2}} \tag{65}$$

L'égalité a lieu si et seulement si les vecteurs lignes sont deux à deux orthogonaux. La formule bien connue [2] à laquelle il fait allusion est la règle du révérend Charles Lutwidge Dodgson (1832–1896), sans doute plus connu sous son pseudonyme Lewis Carroll. La règle relie le déterminant $\Delta = |a_{i,j}|_{\substack{1\leq i\leq n\\ 1\leq j\leq n}}$ à cinq de ses mineurs :

$$\Delta \cdot |a_{i,j}|_{\substack{2\leq i\leq n-1\\ 2\leq j\leq n-1}} = |a_{i,j}|_{\substack{1\leq i\leq n-1\\ 1\leq j\leq n-1}} \cdot |a_{i,j}|_{\substack{2\leq i\leq n\\ 2\leq j\leq n}} - |a_{i,j}|_{\substack{1\leq i\leq n-1\\ 2\leq j\leq n}} \cdot |a_{i,j}|_{\substack{2\leq i\leq n\\ 1\leq j\leq n-1}} \qquad \text{[Alice]}$$

Les matrices qui atteignent la borne (65) sont des *matrice de Hadamard*. Une matrice de Hadamard H est une matrice à coefficients dans le cercle unité satisfaisant à l'égalité :

$$HH^* = vI_v. \tag{66}$$

Dans la littérature, les matrices de Hadamard à coefficients complexes sont des *matrices de Hadamard généralisées*, la terminologie *matrices de Hadamard complexes* est réservée aux matrices à coefficients ± 1 ou $\pm i$. Il n'est pas facile de préciser pour quelles valeurs de v il existe

une matrice de Hadamard. L'initiateur de ces questions, J. Sylvester (), avait déjà remarqué que si H_1 et H_2 désignent deux matrices Hadamard alors leur produit de Kronecker $H_1 \otimes H_2$ est une troisième matrice de Hadamard. Par exemple, à partir de la matrice réelle

$$\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

on construit une suite de matrices de Hadamard d'ordre 2^1, 2^2, 2^3...

La multiplication d'une colonne ou d'une ligne par un nombre complexe de module 1, l'échange de deux lignes, l'échange de deux colonnes et la transposition engendre un groupe de transformation qui ne change pas le caractère Hadamard d'une matrice. Deux matrices de Hadamard sont équivalentes si l'une s'obtient à partir de l'autre par une transformation de ce groupe. Sans perdre en généralité, on peut toujours supposer que les trois premières lignes d'une matrice de Hadamard réelle sont :

$$\begin{array}{cccccc} +1 & +1 & \dots & +1 & +1 & \dots \\ +1 & +1 & \dots & -1 & -1 & \dots \\ x_1 & x_2 & \dots & y_1 & y_2 & \dots \end{array} \tag{67}$$

En particulier, mis à part la dimension 2, la dimension d'une matrice de Hadamard réelle est un multiple de 4. Aujourd'hui, on sait construire des matrices de Hadamard réelles pour de nombreuses dimensions multiple de 4, voir les ouvrages [**52**][**66**].

Dans son article [**157**], Raymond Paley écrit : *It seems probable that, whenever m is divisible by 4, it is possible to construct an orthogonal matrix of order m composed of ±1, but the general theorem has every appearence of dificulty...* Le lecteur en quête de célébrité devra s'attaquer à la

CONJECTURE 2.1 (Paley). *Si v est multiple de 4, il existe une matrice d'Hadamard d'ordre v.*

PROBLÈME 2.1. *Trouver une matrice de Hadamard réelle de dimension 428 i.e. le premier cas ouvert, les autres sont 668, 716, 764 etc...*

[2] Je salue ici le mathématicien internaute R. Chapman de m'avoir signalé l'adresse de la home page de Doron Zeilberg `http ://www.math.temple.edu/zeilberg`. Le lecteur curieux y trouvera une élégante démonstration de la formule Alice.

Problème 2.2. *Quelle est la valeur maximale d'un déterminant $n \times n$ à coefficients ± 1 ? Cette question est abordée dans* [**51**].

Soit G un groupe fini d'ordre v. On dit que la matrice A est développée à partir de G par l'application f s'il est possible d'indexer les lignes et les colonnes de M par les éléments de G de sorte que :

$$A = \big(f(y-x)\big)_{x,y\in G} \quad \text{ou} \quad A = \big(f(x,y)\big)_{x,y\in G}. \tag{68}$$

suivant que le domaine de f est G ou bien le produit cartésien $G\times G$. Terminons cette section, par quelques mots sur l'approche cohomologique proposée par K. Horadam et W. de Launey dans [**96**]. On dit que le groupe E est une extension de G par A s'il existe une suite exacte

$$0 \longrightarrow A \longrightarrow E \longrightarrow G \longrightarrow 0$$

Dans ce cas, la loi de E est définie à partir de la loi de A et d'un *système de facteurs*, c'est-à-dire, une application f de $G \times G$ dans A vérifiant :

$$x.f(y,z) - f(xy,z) + f(x,yz) - f(x,y) = 0 \tag{69}$$

Dans le cas où A est un sous-groupe du groupe multiplicatif des nombres complexes, on construit une *matrice*, $\big(f(x,y)\big)_{x,y\in G}$ qui, dans certains cas, est une matrice d'Hadamard...

3. Ensemble à différences

Soit G un groupe fini d'ordre v et soit D un sous-ensemble de G de cardinal k. On dit que D est un (v,k,λ) *ensemble à différences* si pour tout élément non nul g de G, il existe λ couples (x,y) dans le produit cartésien $D \times D$ tels que $x - y = g$. Le petit lemme du « berger fou » donne immédiatement

la condition nécessaire :

$$k^2 = \lambda(v-1) + k = \lambda v + n, \tag{70}$$

où $n = k - \lambda$ est l'*ordre* de l'ensemble à différences. Les sous-ensembles de cardinaux 0, 1, $v-1$ et v sont des ensembles

à différences. On les appelle les *ensembles triviaux*. Notons A la matrice développée à partir de G par la fonction indicatrice de D :

$$A(x,y) = \mathbf{1}_D(y-x), \quad \forall x,y \in G$$

On vérifie que $AA^t = kI_v + \lambda J_v$, en passant au déterminant, on obtient une seconde condition nécessaire :

$$\boxed{\text{l'entier } n^{v-1} \text{ est un carré parfait.}}$$

4. Fonctions parfaites

Soit G un groupe fini d'ordre v. Une application f à valeurs complexes définie sur G est une fonction à *autocorrélation parfaite* si

$$f \times f(g) = \begin{cases} k, & \text{si } g = 0\,; \\ \lambda, & \text{sinon.} \end{cases} \tag{71}$$

On dit que la fonction est (k,λ)-*parfaite*. Si f est une application parfaite alors pour tout couple (a,b) de nombres complexes, la fonction $af+b$ est parfaite. En particulier, si f est une fonction (k, λ)-parfaite alors la fonction $1-f$ est $(v-k, v-2k+\lambda)$-parfaite.

L'indicatrice d'un ensemble à différences est une fonction parfaite. Réciproquement, si f est une fonction

parfaite à valeurs dans $\{0,1\}$ son support $\{d \in G \mid f(g) = 1\}$ est un (v, k, λ)-ensemble à différences. Ainsi, le complémentaire d'un (v, k, λ)-ensemble à différences est un $(v, v-k, v-2k+\lambda)$-ensemble à différences de même ordre.

La fonction $(1-2f)$ est à valeurs dans $\{-1, +1\}$ et vérifie

$$(1-2f) \times (1-2f) = \begin{cases} v, & \text{si } g = 0; \\ v - 4n, & \text{sinon.} \end{cases}$$

La matrice carrée développée à partir de G par la fonction $(-1)^{f(y-x)}$ est une matrice de Hadamard si et seulement

si $n = \frac{v}{4}$. Dans ce cas, on démontre que n est un carré, et, si nous posons $n = u^2$, alors le support de f est un $(4u^2, 2u^2 \pm u, u^2 \pm u)$ ensemble à différences. Naturellement, un tel ensemble s'appelle un *ensemble à différences de Hadamard*.

5. Multiplieurs

Soit f une fonction complexe définie sur un groupe fini G. Un automorphisme σ du groupe G est un *multipleur* de f s'il existe un élément

$a_\sigma \in G$ tel que

$$f_\sigma(x) = f(x^\sigma) = f(x + a_\sigma)$$

Si σ est une multiplication par un entier (nécessairement premier avec l'ordre de G), on parle de *multiplieur numérique*. Clairement, les multipleurs de f forment

un sous-groupe du groupe des automorphismes de G.

Tous les translatés de f ont le même

groupe de multiplieurs. D'après Jungnickel, le théorème qui suit est un résultat profond de la théorie des ensembles à différences.

THÉORÈME 5.1 (MacFarland). *Si f est l'indicatrice d'un ensemble à différence alors il existe un translaté de f fixé par tous les multiplieurs de f.*

DÉMONSTRATION. Voir par exemple [**141**]. □

Cette notion joue un rôle très important dans l'étude

des ensembles à différences : existence et construction. Curieusement, tous les ensembles à différences répertoriés à ce jour possèdent un multiplieur non trivial.

CONJECTURE 5.1. *Le groupe des multiplieurs d'un ensemble à différences n'est pas trivial.*

6. Transformée de Fourier

Dans le cas d'un groupe abélien, la transformée de Fourier se révèle être un outil puissant pour traiter des conditions d'existence d'un ensemble à différences. Soit G un groupe abélien, nous avons déjà défini la transformée de Fourier d'une application complexe.

PROPOSITION 6.1. *Soit f une application numérique, f et une fonction (k,λ)-idéalement autocorrélée si et seulement si*

$$|\widehat{f}(\chi)|^2 = \begin{cases} k^2, & si\ \chi = 1\,; \\ n, & sinon. \end{cases}$$

DÉMONSTRATION. C'est une conséquence des formules d'orthogonalité. □

De sorte que, l'existence d'un (v,k,λ)-ensemble à différences dans un groupe abélien d'ordre v dépend en tout premier lieu du nombre de solutions, dans l'anneau des entiers cyclotomiques $\mathbf{Z}[\zeta_v]$, de l'équation :

$$xx^* = n. \tag{72}$$

Un nombre premier p est dit *auto-conjugué* modulo v s'il existe une puissance de p égale à -1 modulo v. Le lemme qui suit joue un rôle fondamental :

LEMME 6.1. *Soient n et v deux entiers. S'il existe nombre premier p satisfaisant aux trois conditions suivantes (1) la valuation p-adique de n est impaire, (2) p est premier avec v, (3) p est auto-conjugué modulo v alors il n'existe pas d'entier cyclotomique de $\mathbf{Z}[\zeta_v]$ de module $\sqrt{n}$.*

DÉMONSTRATION. Dans l'anneau $\mathbf{Z}[\zeta_v]$, l'idéal engendré par p se décompose en un produit d'idéaux premiers. Soit $\mathcal{P}$ l'un d'entre-eux. L'ensemble des automorphismes du corps $\mathbf{Q}[\zeta_v]$ qui fixent $\mathcal{P}$ est un groupe cyclique engendré par l'automorphisme de Frobenius σ_p. La condition (3) dit que la conjugaison usuelle est dans le groupe de décomposition de p. Notons $\mathrm{val}_{\mathcal{P}}$ la valuation $\mathcal{P}$-adique. L'égalité (72) imposerait

$$\mathrm{val}_{\mathcal{P}}(x) + \mathrm{val}_{\mathcal{P}}(x^*) = \mathrm{ord}_p(n)$$

On conclut en remarquant que

$$\mathrm{val}_{\mathcal{P}}(x^*) = \mathrm{val}_{\mathcal{P}^*}(x) = \mathrm{val}_{\mathcal{P}}(x)$$

□

PROBLÈME 6.1. *Etudier la réciproque du lemme précédent. C'est-à-dire, donner une condition nécessaire et suffisante d'existence d'un entier cyclotomique de module n dans $\mathbf{Z}[\zeta_v]$.*

7. Quelques résultats de Turyn

Dans les articles [**182, 181**] expose des résultats fondamentaux sur l'existence d'ensemble à différences basés sur l'exploitation habile de la notion d'auto-conjugaison et du lemme qui en découle. Certains résultats portent sur les valeurs possibles des paramètres v, k et λ. D'autres plus fins, donnent des conditions sur le nombre de sous-groupes de Sylow.

Le premier théorème généralise un résultat de Hall.

THÉORÈME 7.1. *Soit f l'indicatrice d'un (v,k,λ)-ensemble à différence d'un groupe abélien G. Soit σ un automorphisme du groupe G. On suppose que pour tout caractère de G, σ fixe d'idéal principal engendré par $\widehat{f}(\chi)$ dans $\mathbf{Z}[\zeta_v]$. S'il existe un diviseur*

m de n tel que $m > \lambda$ et $(m,v) = 1$, alors σ est un multiplieur de f.

DÉMONSTRATION. Tout d'abord, pour chaque caractère χ, nous avons :

$$\sigma\big(\widehat{f}(\chi)\big)\overline{\widehat{f}(\chi)} \equiv \widehat{f}(\chi)\overline{\widehat{f}(\chi)} \equiv 0 \pmod m$$

Par la formule d'inversion de Fourier, nous obtenons que

$$v\, f_\sigma \times f(t) \equiv k^2 \pmod m$$

Mais $k^2 = \lambda v + n$, donc :

$$v\,(f_\sigma \times f(t) - \lambda) \equiv 0 \pmod m$$

Comme v est inversible modulo m, on en déduit l'existence d'une application g à valeurs entières telle que

$$f_\sigma \times f(t) = \lambda + m\, g(t)$$

La fonction g est parfaite puisque sa transformée de Fourier est constante. La condition $m > \lambda$ implique que g soit positive. Ainsi g est une fonction positive et parfaite, c'est donc un Dirac. Il existe $a \in G$ et un entier A tel que : $f_\sigma \times f = \lambda + A\delta_a$. Il suffit de calculer la transformée de Fourier en zéro pour réaliser que $A = k - \lambda$, et donc que $f_\sigma(x) = f(x+a)$, i.e. σ est un multiplieur. □

CONJECTURE 7.1. *La condition $m > \lambda$ est superplue.*

Le second théorème est une application de la formule de Poisson et de la proposition (7.1) qui estime la valeur maximale d'une somme de caractère.

THÉORÈME 7.2. *Soit G un groupe d'ordre v, Σ un sous-groupe d'ordre a de G^*, ψ un caractère de G et f l'indicatrice d'une partie de G. On note b le plus petit entier non nul tel que $\psi^b \in \Sigma$. Si m divise la transformée de Fourier de f sur $\psi\Sigma$ sans être nulle alors*

$$m \leq \frac{2^{\mathrm{NBD}(b)} v \|f\|_\infty}{2ab}.$$

où NBD(b) *désigne le nombre de diviseurs premier de b.*

DÉMONSTRATION. Notons S l'orthogonal de Σ dans G. La transformée de Fourier de $f\psi$ en χ est égale à la transformée de Fourier de f en $\psi\chi$. La formule de Poisson donne :

$$\frac{1}{|\Sigma|}\sum_{\chi\in\Sigma}\widehat{f}(\chi\psi) = \sum_{s\in S} f(s)\psi(s) = \sum_{u\in U}\Big(\sum_{v\in V} f(u+v)\Big)\psi(u)$$

L'entier b n'est rien d'autre que l'ordre la restriction à S de ψ. L'entier m est premier avec $|\Sigma|$: il divise le membre droit de cette égalité. la proposition (7.1) permet de conclure. □

COROLLAIRE 7.1. *Soit D un ensemble à différences dans un groupe G d'ordre v. Supposons qu'il existe un diviseur a de v et un diviseur m de n tels que $m^2 \mid n$ et m auto-conjugué modulo a alors $am \leq 2^{r-1}v$, où r est le nombre de diviseurs premiers de (m,a).*

PROPOSITION 7.1. *Soit S un groupe fini cyclique d'ordre N, f une fonction à valeurs entière définie sur S, et χ un caractère d'ordre b. Si $\widehat{f}(\chi)$ n'est pas nulle et si un entier m divise $\widehat{f}(\chi)$ alors*

$$m \leq \frac{2^{\mathrm{NBD}(b)} N \|f\|_\infty}{b}.$$

Si de plus f est positive alors

$$m \leq \frac{2^{\mathrm{NBD}(b)} N \|f\|_\infty}{2b}.$$

où NBD(b) *désigne le nombre de diviseurs premier de b.*

8. La conjecture de Ryser

Soit s une séquence de longueur v, c'est-à-dire une fonction définie sur le groupe $\mathbf{Z}/v\mathbf{Z}$. Du point de vue des télécommunications, une séquence idéale doit posséder une fonction d'autocorrélation nulle partout hors phase. On dit que c'est une *séquence à autocorrélation parfaite.*

CONJECTURE 8.1. *Il n'existe pas de séquence à autocorrélation parfaite binaire de longueur* > 4. *Il n'existe pas de matrice de Hadamard cyclique de dimension* > 4.

Le problème est de prouver la non existence d'ensemble à différences de Hadamard cyclique pour un groupe d'ordre $v > 4$. Dans [**181**] Turyn démontre que si le groupe cyclique $\mathbf{Z}/v\mathbf{Z}$ possède un ensemble de Hadamard alors $v = 4u^2$ avec u impair. En utilisant les théorèmes de la section précédente, il prouve la non existence d'ensemble de Hadamard pour v compris entre 5 et 12100. [3]

CONJECTURE 8.2 (Ryser). *Il n'existe pas de* (v, k, λ)*-ensemble à différences cyclique avec* $(v, n) > 1$.

9. Séquences de Barker

L'analogue d'une séquence à autocorrélation parfaite dans le cas apériodique s'appelle une séquence de Barker. Une séquence de longueur v est une *séquence de Barker* lorsque sa fonction d'autocorrélation apériodique reste en module inférieure à 1. En imposant la condition plus forte,

$$s \ltimes s(\tau) \in \{0, -1\}, \qquad \forall \tau \quad 0 < \tau < v;$$

Barker trouve des séquences de longueurs 3, 7 et 11. Indépendamment, Storer et Turyn [**178**], et Poliak et Moshetov, ont prouvé qu'il n'existe pas d'autres séquence de Barker de longueur impaire. Le cas de la longueur paire est lié à la conjecture de Ryser par la

PROPOSITION 9.1. *Soit s une séquence de longueur paire. Si s est une séquence de Barker alors s est une séquence à autocorrélation parfaite.*

DÉMONSTRATION. Il faut utiliser la relation (64). □

CONJECTURE 9.1. *Il n'existe pas de séquence de Barker de longueur paire supérieure à* 4.

Soit K un corps fini. Le sous-anneau $K[Z, \frac{1}{Z}]$ des fractions à une indéterminée est principal. De ce fait purement algébrique, Eliahou et Kervaire déduisent [**71**] que la longueur d'une séquence de Barker ne peut pas être divisible par un nombre premier congru à 3 modulo 4. Cette condition s'ajoute aux conditions de Turyn pour vérifier la conjecture jusqu'à $v = 2.10^9$. Ici encore, on peut faire beaucoup mieux avec les travaux récents de Bernhard Schmidt [**165**]. Il existe des pistes non arithmétiques comme la conjecture de D. J. Newman dans [**182**] ou bien l'approche ergodique [**156**] que m'a signalée Yves Lacroix.

[3] On peut faire beaucoup mieux, c'est-à-dire ajouter un « 0 », avec les travaux de Bernhard Schmidt [**165**], mais ils sont différents et trop récents pour être rapportés dans ce mémoire.

10. Groupes de décomposition

Soient n et v deux entiers. Le *groupe de décomposition* de n relativement à v est l'intersection

$$G(n,v) = \bigcap_{p|n} D(p,v),$$

où $D(p,v)$ désigne le groupe de décompostion du nombre premier p dans la la v-ième extension cyclotomique. Ce groupe joue un rôle fondamental dans l'étude d'un (v,k,λ) ensemble à différence. Avec Préscilia et Julien, nous nous sommes amusés à calculer le groupe de décomposition $G(n,n)$ pour tous les entiers compris entre 2 et 1050. Ce groupe est trivial seulement 8 fois pour : 2, 310, 390,546, 620, 780, 903, 930.

PROBLÈME 10.1. *Etudier la distribution des ordres des groupe $G(n,v)$ en faisant varier n et v..*

PROBLÈME 10.2. *Etudier une condition suffisante pour qu'un élément σ de $G(n,v)$ soit un multiplieur.*

PROBLÈME 10.3. *Les groupes de ramifications, voir* [**171**] *n'interviennent jamais dans l'étude des ensembles à différences. Pourquoi ?*

11. Degré de non-linéarité

Soit A un anneau fini commutatif de cardinal q. L'ensemble des applications de A^m dans A est muni de sa métrique de Hamming. La *non-linéarité* d'une application f définie sur A^m mesure sa complexité. Elle est définie par

$$\delta(f) = \max_{\phi} d_H(f,\phi)$$

où ϕ décrit l'ensemble de toutes les fonctions affines de A^m dans A. La non-linéarité maximale d'une fonction n'est rien d'autre que le rayon de recouvrement $\rho_A(m)$ du code de Reed-Muller affine de m variables d'alphabet A, voir [**120**]. Une fonction de non-linéarité maximale est dite *hautement non-linéaire.*

LEMME 11.1. *Si χ est un caractère admissible de A alors*

$$\sum_{a\in A^m} |\hat{f}_\chi(a)|^2 = q^{2m}. \tag{73}$$

DÉMONSTRATION. Par définition, l'application $a \mapsto \chi_a$ permet de décrire tous les caractères de A^m en faisant varier a dans A^m et l'identité de Parseval :

$$\sum_{\psi\in\widehat{A^m}} |\hat{f}(\psi)|^2 = q^m \sum_{x\in A^m} |f(x)|^2 = q^{2m}. \tag{74}$$

permet de conclure. □

Soient $a \in A^m$ et $b \in A$. Pour calculer la distance de Hamming entre la forme affine $x \mapsto a.x + b$ et la fonction f, on introduit la somme de caractères

$$\mathrm{SF}(f,a,b) = \sum_{\chi\neq 1} \hat{f}_\chi(a)\bar{\chi}(b).$$

On vérifie que la distance de Hamming entre la forme affine $x \mapsto a.x+b$ et la fonction f vaut :

$$(q-1)q^{m-1} - \frac{1}{q}\mathrm{SF}(f,a,b). \tag{75}$$

Théorème 11.1. [**119**, ?] *Le rayon de recouvrement du code de Reed-Muller affine de m variables sur l'anneau A vérifie*

$$\rho_A(m) \leq (q-1)q^{m-1} - \frac{\sqrt{n(A)}}{q(q-1)}q^{\frac{m}{2}} \tag{76}$$

où $n(A)$ est le nombre de caractères admissibles de A, c'est le cardinal de $A^\times$ si A est quasi-Frobenius et 0 *sinon.*

Démonstration. Voir [**120, 119**] □

Soient $u \in A^m$ et f une application de A^m dans A. La fonction $D_u f : x \mapsto f(x+u) - f(x)$ s'appelle la *dérivée* de f dans la direction de u. Cette notion est étudiée en détail dans la section •du chapitre VI. Une fonction *parfaitement non-linéaire* est une application de A^m dans A telle que pour tout $u \neq 0$, la dérivée de f dans la direction de u est équilibrée i.e. $D_u f$ prend toutes les valeurs de A avec la même multiplicité. En d'autres termes, f_χ est une fonction numérique à autocorrélation parfaite quel que soit $\chi \in \widehat{A^+} - \{1\}$. Les fonctions parfaitement non-linéaires sont de bonnes candidates pour la non-linéarité maximale.

Proposition 11.1. *Si f est une fonction parfaitement non-linéaire alors*

$$\delta(f) \leq (q-1)q^{m-1} - \frac{1}{q}\sqrt{q-1}q^{m/2}. \tag{77}$$

Démonstration. Nouv avons

$$\Sigma(f) = q(q-1)q^{2m},$$

il ne reste plus qu'à appliquer le lemme précédent. □

Problème 11.1. *Améliorer ces bornes dans le cas des anneaux « usuels ». Dans quelle situation, les notions de fonctions parfaitement non-linéaire et de fonctions hautement non-linéaire sont équivalentes ?*

12. Fonction courbes généralisées

Les fonctions courbes généralisées sont introduites dans l'article [**109**]. Une application f de domaine $(\mathbf{Z}/n\mathbf{Z})^m$ à valeurs dans $\mathbf{Z}/n\mathbf{Z}$ est une *fonction courbe généralisée* s'il existe un caractère générateur χ de $\widehat{\mathbf{Z}/n\mathbf{Z}}$ tel que pour tout vecteur $a \in A^m$, le coefficient de Fourier de f_χ en a

$$\widehat{f_\chi}(a) = \sum_{x \in (\mathbf{Z}/n\mathbf{Z})^m} \chi(f(x) + ax)$$

est de module $q^{m/2}$.

Cette définition ne dépend pas du choix du caractère. On dit que la fonction courbe est est *régulière* en a si le quotient $\widehat{f_\chi}(a)/q^{m/2}$ est une racine q-ième de l'unité. Une fonction courbe régulière est une fonction régulière en tout point.

Problème 12.1. *Que devient cette définition dans le cas d'un anneau quasi-Frobenius ?*

Dans l'article *On generalized bent function*, j'étudie ces fonctions du point de vue métrique i.e. distance au code de Reed-Muller affine et du point de vue du degré. Il apparaît que les fonctions courbes généralisées ont des propriétés algébriques proches des fonctions courbes de Rothaus, sans pour autant être hautement non-linéaires.

13. Non-linéarité d'une fonction courbe

On suppose que p est un nombre premier impair. La dimension du corps cyclotomique $\mathbf{Q}(\zeta_p)$ est suffisamment grande par rapport à p pour rendre possible le calcul de la non-linéarité d'une fonction courbe, voir [**155**] et [**119**]. Contrairement à ce que l'on aurait pu imaginer, les fonctions courbes ne sont pas nécessairement hautement non-linéaires.

Soient $a \in \mathbf{F}_p{}^m$ et $b \in \mathbf{F}_p$ et f une application de $\mathbf{F}_p{}^m$ vers $\mathbf{F}_p$. La distance entre f et la fonction affine $x \mapsto ax + b$ est donnée par le formule

$$\begin{aligned} d_H(f, u.x + b) &= (p-1)p^{m-1} - \frac{1}{p}\mathrm{SF}(f, u, b) \\ &= (p-1)p^{m-1} - \frac{1}{p}\mathrm{tr}_{\mathbf{Q}(\zeta_p)/\mathbf{Q}}\left[\hat{f}_\chi(u)\bar{\chi}(b)\right] \end{aligned} \tag{78}$$

où χ est un caractère non-trivial de $\mathbf{F}_p$ et ζ_p la racine principale d'ordre p. Comme l'extension $\mathbf{Q}(\zeta_p)$ est totalement ramifiée en p, il existe une unité $\lambda(u)$ qui est forcément une racine de l'unité telle que

$$\hat{f}_\chi(u) = \lambda(u)\sqrt{p}^m \tag{79}$$

si m est pair $\lambda(u)$ est dans $\mathbf{Q}(\zeta_p)$ et si m est impair la somme quadratique de Gauss montre que

$$\sum_{k=0}^{p-1} \zeta_p^{k^2} = \theta\sqrt{p} \quad \text{avec} \quad \theta = \begin{cases} 1, & \text{si } p \equiv 1[4]\,; \\ i, & \text{si } p \equiv 3[4]\,; \end{cases}$$

et donc $\frac{\lambda(u)}{\theta}$ est une racine de l'unité dans $\mathbf{Q}(\zeta_p)$.

PROPOSITION 13.1. [**119**, πλ] *Soit m pair. Lorsque b décrit $\mathbf{F}_p$,*

$$\mathrm{SF}(f, a, b) = \begin{cases} -p^{\frac{m}{2}}, & p-1 \textit{ fois}\,; \\ (p-1)p^{\frac{m}{2}}, & 1 \textit{ fois.} \end{cases} \tag{80}$$

si f est régulière en a.

$$\mathrm{SF}(f, a, b) = \begin{cases} p^{\frac{m}{2}}, & p-1 \textit{ fois}\,; \\ -(p-1)p^{\frac{m}{2}}, & 1 \textit{ fois.} \end{cases} \tag{81}$$

sinon.

PROPOSITION 13.2. [**119**, πλ] *Soit m impair. Lorsque b décrit $\mathbf{F}_p$,*

$$\mathrm{SF}(f, a, b) = \begin{cases} -p^{\frac{m+1}{2}}, & \frac{p-1}{2} \textit{ fois}\,; \\ 0, & 1 \textit{ fois}\,; \\ p^{\frac{m+1}{2}}, & \frac{p-1}{2} \textit{ fois}\,; \end{cases} \tag{82}$$

THÉORÈME 13.1. *Le rayon de recouvrement du code de Reed-Muller affine de m variables sur l'alphabet $\mathbf{F}_p$ satisfait aux inégalités :*

$$(p-1)p^{m-1} - p^{[\frac{m-1}{2}]} \leq \rho_{\mathbf{F}_p}(m) \leq (p-1)p^{m-1} - \frac{1}{\sqrt{p-1}} p^{\frac{m}{2}-1} \tag{83}$$

DÉMONSTRATION. La minoration est obtenue à l'aide de la forme quadratique $sx_1^2 + x_2^2 + \ldots + x_m^2$ qui est une fonction courbe non régulière dès que s n'est pas un carré. La majoration a été établie dans la section sur la non-linéarité. $\square$

14. Degré des fonctions courbes

On écrit $m = 2t$ ou $m = 2t + 1$ suivant la parité de m.

PROPOSITION 14.1. [**119**, $\pi\lambda$] *Soient S un sous-espace de dimension k et f une fonction courbe généralisée. Si $k \geq t+2$ alors f est orthogonale à $\mathbf{1}_S$.*

DÉMONSTRATION. Soit $b \in \mathbf{F}_p$, désignons par $n(b)$ le nombre de $s \in S$ tel que $f(x) = b$. On exprime $n(b)$ au moyen d'une somme de caractères

$$p\, n(b) = \sum_{s \in S} \sum_{\chi \in \widehat{\mathbf{F}_p}} \chi(f(s) - b)$$

et donc

$$n(b) = p^{k-1} - \frac{1}{p} \sum_{\chi \neq 1} \chi(f(s) - b)$$

en appliquant la formule de Poisson

$$\sum_{s \in S} \chi(f(s)) = p^{k-m} \sum_{t \in S^\perp} \hat{f}_\chi(t)$$

L'idéal (p) est complètement ramifié dans $\mathbf{Z}[\zeta_p]$:

$$(p) = P^{(p-1)}$$

P l'idéal principal engendré par$(1-\zeta_p)$. Comme la conjugaison complexe $z \mapsto \bar{z}$ est dans le groupe de décomposition de P, la valuation P-adic de $\hat{f}_\chi(s)$ vérifie :

$$\nu_P(\hat{f}_\chi(s)) = \frac{(p-1)m}{2}$$

et donc,

$$\begin{aligned} \nu_P(p^{k-m-1} \sum_{t \in S^\perp} \hat{f}_\chi(t)\bar{\chi}(b)) &\geq (k-m-1)(p-1) + (p-1)\frac{m}{2} \\ &\geq (p-1)(k - \frac{m}{2} - 1) \end{aligned}$$

l'hypothèse faite sur la dimension de S donne

$$> 0$$

L'entier $n(b)$ est multiple de p. Par ailleurs,

$$f.1_S = \sum_{b \in \mathbf{F}_p} n(b) \equiv 0 \mod p$$

les vecteurs f et 1_S sont orhogonaux. $\square$

PROPOSITION 14.2 (Delsarte). *Les indicatrices des variétés affines de co-dimension k engendrent le code de Reed-Muller d'ordre $(p-1)k$.*

COROLLAIRE 14.1. *Si f est une fonction courbe généralisée alors* $\deg(f) \leq (p-1)t + 2p - 3$

DÉMONSTRATION. Des calculs qui précèdent, nous déduisons que f appartient au dual de l'espace engendré par les indicatrices des varitiétés affines de dimensions $t+2$

$$f \in \mathrm{RM}_{\mathbf{F}_p}((p-1)(m-t-2), m)^{\perp} = \mathrm{RM}_{\mathbf{F}_p}((p-1)(t+2)-1, m)$$

Finalement,

$$\deg(f) \leq (p-1)t + 2p - 3.$$

□

PROBLÈME 14.1. *En dimension 1, les fonctions courbes sont des fonctions quadratiques, voir Gabidulin* [**72**]. *Etudier le degré des fonctions courbes en dimension supérieure.*

15. Suites ternaires

L'absence de séquences binaires à autocorrélations parfaites conduit à la recherche de *séquences ternaires* i.e. à valeurs dans $\{-1, 0, +1\}$ et plus généralement les séquences à valeurs dans le cercle unité augmenté de l'origine. Deux types d'autocorrélations retiennent mon attention :

$$\text{type I,} \quad s \times s(t) = \begin{cases} m, & t = 0; \\ 0, & t \neq 0. \end{cases} \quad \text{type II,} \quad s \times s(t) = \begin{cases} m, & t = 0; \\ -m, & t = \frac{n}{2}; \\ 0, & \text{sinon.} \end{cases}$$

L'entier m est le *poids de la séquence* c'est le nombre de valeurs non-nulles de la séquence. Des familles infinies de séquences de type I sont construites par Ipatov [**99**] ainsi que Hoholdt et Justesen [**85**].

Dans l'article some sequences with good autocorrelation properties, j'explore la corrélation des séquences de la forme $s(k) = \chi \circ \mathrm{tr}_{L/K}(\alpha^k)$, où K est un corps fini de caractéristique p et de cardinal q, L une extension de degré s de K, α une racine primitive n-ième de l'unité dans L et χ un caractère multiplicatif de K prolongé par 0 en 0. L'objectif est de caractériser des séquences de type I et II. Pour cela, on introduit la transformée de Fourier de s en u

$$\hat{s}(u) = \sum_{x \in \mathbf{Z}/n\mathbf{Z}} s(x) \zeta_n^{ux}$$

où comme d'habitude, ζ_n désigne la racine n-ième principale de l'unité. La séquence est de type I si et seulement si le module de la transformée de Fourier est constant égal à $\sqrt{m}$. Elle est de type II si et seulement si la transformée de Fourier est nulle pour les entiers pairs et de module constant égal à $\sqrt{2m}$ pour les entiers impairs.

Calculons la transformée de Fourier de la séquence s.

$$\hat{s}(u) = \sum_{k \in \mathbf{Z}/n\mathbf{Z}} \chi \circ \mathrm{tr}_{L/K}(\alpha^k) \zeta_n^{uk}$$

Soit γ un caractère multiplicatif générateur de $\widehat{L^{\times}}$ tel que $\gamma(\alpha) = \zeta_n$. Pour tout $\psi \in \widehat{L^{\times}}$, posons $S(\psi) = \sum_{x^n=1} \chi \circ \mathrm{tr}_{L/K}(x)\psi(x)$, la somme porte sur le groupe des racine n-ième de l'unité dans L. De sorte que $\hat{s}(u)$ est égal à $S(\gamma^u)$. Pour calculer cette somme de caractères, nous introduisons l'annulateur A de α,

$$A = \{\psi \in \widehat{L^\times}; \psi(\alpha) = 1\};$$

c'est un groupe cyclique d'ordre $\frac{q^s-1}{n}$ engendré par γ^n, et

$$\begin{aligned} S(\lambda) &= \frac{n}{q^s-1} \sum_{\psi \in A} \sum_{x \in L} \chi \circ \operatorname{tr}_{L/K}(x) \psi(x) \lambda(x) \\ &= \frac{n}{q^s-1} \sum_{c \in K} \chi(c) \sum_{\psi \in A} \sum_{\operatorname{tr}_{L/K}(x)=c} \psi(x)\lambda(x) \end{aligned}$$

Les sommes qui émergent sont des sommes d'Eisenstein que nous avons décrit dans la section (10) du premier chapitre. Elles s'expriment en termes des sommes de Gauss

$$\sum_{\operatorname{tr}_{L/K}(x)=c} \theta(x) = q^{s-1}\theta(c) \frac{G_K(\theta)}{G_L(\theta)} = \frac{1}{q} G_L(\theta) G_K(\theta)^* \theta(c),$$

Finalement, nous obtenons

$$S(\lambda) = \frac{n(q-1)}{q(q^s-1)} \sum_{\psi\lambda\chi=1} G_K(\psi\lambda)^* G_L(\psi\lambda)$$

où la somme porte sur tous les caractères ψ de A tels que la restriction à K du produit $\psi\lambda\chi$ soit trivial. Il ne reste plus qu'a cueillir les séquences de type I et II comme des fruits mûrs !

Proposition 15.1. [**123**, $\pi\lambda$] *Si la restriction de A dans $\widehat{K^\times}$ est bijective alors s est de type I, tel est le cas si $n = \frac{q^s-1}{q-1}$ et* PGCD$(s, q-1) = 1$.

Démonstration. La restriction doit être surjective. Soit $u \in \mathbf{Z}/n\mathbf{Z}$, il existe un et un seul caractère $\psi \in A$ tel que $\psi\lambda^u\chi$ soit trivial sur K. Donc,

$$\hat{s}(u) = S(\lambda^{-u}) = \frac{n(q-1)}{q(q^s-1)} G_K(\bar{\chi})^* G_L(\psi\lambda^u)$$

qui est de module constant égal à

$$\frac{nq^{\frac{s-1}{2}}(q-1)}{q^s-1}.$$

Par ailleurs, sous les conditions mentionnées, l'ordre de $\tilde{\gamma}^n$ est $q-1$ et celui de A aussi, i.e. la restriction est bijective. $\square$

Proposition 15.2. [**123**, $\pi\lambda$] *Si la restriction de A dans $\widehat{K^\times}$ est une bijection vers le groupe engendré par $\tilde{\gamma}^2$, c'est le cas si $n = 2\frac{q^s-1}{q-1}$ et* PGCD$(2s, q-1) = 2$, *et si de plus l'ordre de χ ne divise pas $\frac{q-1}{2}$ alors la séquence s est de type II*

Démonstration. Soit $u \in \mathbf{Z}/n\mathbf{Z}$. La condition sur l'ordre de χ implique que χ ne vit pas dans le groupe engendré par $\tilde{\gamma}^2$ et comme ce groupe est l'image de A par la restriction, nous en déduisons que l'équation $\psi\gamma^u\chi = 1$ a une solution si u est impair et pas de solution si u est pair. $\square$

Problème 15.1. *Etudier l'intercorrélation des sequences de type I de la famille $s_{\beta,t}(k) = \chi \circ \operatorname{tr}_{L/K}(\beta\alpha^{kt})$, β variant dans L, et $t \in (\mathbf{Z}/n\mathbf{Z})^\star$.*

PROBLÈME 15.2. *Que se passe-t-il si la restriction est une surjection dont le noyau contient* 2 *éléments ?*

16. séquences θ-presque-parfaites

La non-existence probable de suites binaires parfaites a conduit J. Wolfmann à l'étude des suites binaires dont la fonction d'autocorrélation est égale à zéro sauf au plus en deux positions. Si s est une suite presque parfaite alors sa transformée de Fourier en zéro est paire, et en notant $\hat{f}(0) = 2\theta$, on obtient :

$$f \times f(z) = \begin{cases} v, & \text{si} z = 0\,; \\ 4\theta^2 - n, & \text{si} z = \frac{v}{2}\,; \\ 0, & \text{sinon.} \end{cases}$$

On dit que la suite est *θ-presque parfaite* . La transformée de Fourier de f prend la valeur $4\theta^2$ sur le groupe d'indice 2 et $2v - 4\theta^2$ ailleurs. L'argument (67) est toujours valable, une séquence à autocorrélation presque parfaite est de longueur multiple de 4. Mis à part le cas $\theta = 1$, on ne connaît qu'un nombre fini de séquences θ-presque parfaite. Dans sa thèse, J.-P. Martin [**142**] prouve qu'il n'en existe pas pour $\theta = 0$. Il existe des séquences 2-presque parfaite de longueur :8, 12 et 28 [**6**], mais pas de plus longue [**135**]. On peut utiliser la notion de multiplieur pour trouver des séquences, c'est l'objet de l'expérience numérique ci-dessous.

PROBLÈME 16.1. *Déterminer les couples* $(a, b) \in (\mathbf{Z}/v\mathbf{Z})^\star \times \mathbf{Z}/v\mathbf{Z}$ *tels que le groupe des transformations de* $\mathbf{Z}/v\mathbf{Z}$ *engendré par* $x \mapsto ax + b$ *soit de rang assez petit (inférieur à* 40*), puis calculer les propriétés de corrélations des séquences fixées par ce groupe.*

PROBLÈME 16.2. *Quelle est la plus grande valeur de* θ *pour laquelle il existe une séquence* θ*-presque parfaite ?*

17. séquences presque-parfaites

Pour abréger, on dit séquence *presque-parfaite* plutôt que séquences 1-presque parfaites. Les séquences presque-parfaites sont légions mais il n'en existe pas pour toutes les longueurs multiples de 4. Par exemple, il existe des séquences presque-parfaite de période multiple de 4 inférieur à 100 sauf pour 32, 44, 68, 72, 80, et 92. L'existence est établie par l'expérience numérique de Wolfmann [**193**], le cas des six valeurs exceptionnel est traité dans mon article [**121**]. Les méthodes que j'utilise sont proches des méthodes de R. Turyn, mais à ce moment, je ne connaissais pas Turyn et encore moins ses travaux !

PROPOSITION 17.1. [**122**, π_λ] *Soient* K *un corps fini à* q *éléments,* L *l'extension quadratique de* K *; on suppose que* $q \equiv 3 \mod 4$. *Si* γ *est un élément d'ordre* $2(q+1)$ *dans* $L^\times$ *alors la séquence*

$$s_i = \nu_L\big(\mathrm{tr}_{L/K}(\alpha^i)\big)$$

où ν *désigne le caractère quadratique de* L *prolongé en* 0 *par* 1, *est une séquence presque-parfaite.*

La preuve de cette proposition découle du résultat (15.2) concernant les séquences de type II. Récemment, Carine Boursier a adapté cette construction au cas $q \equiv 1 \mod 4$, voir [**22**].

CONJECTURE 17.1. *Il existe une séquence presque-parfaite de longueur v si et seulement si $\frac{v}{2} - 1$ est un entier primaire i.e. une puissance d'un nombre premier.*

Pott et Bradley montrent dans [**25**] que l'existence des suites presque-parfaites est équivalente à celle de certains ensembles à différences relatifs, elle même équivalente à celle des matrices négacycliques. Ces objets sont décrits dans les prochaines sections. Le *multiplier theorem* de Belevitch [**12**] explique la configuration particulière des séquences presque-parfaites.

THÉORÈME 17.1 (Belevitch). *Si f une fonction presque-parfaite alors $t = \frac{v}{2} - 1$ est un multiplieur de f. Plus précisément,*

$$f(tx) = (-1)^{(t-1)/2} f(x)$$

DÉMONSTRATION. Ecrivons $v = 2\ell$, et considérons $\tau \in [1, \frac{v}{4}[$. Sans perdre en généralité, on peut remplacer $f(0)$ et $f(\ell)$ par 0 de sorte à obtenir une séquence de poids $v - 2$, de type II vérifiant :

$$f(x + \ell) = -f(x), \quad \forall x.$$

La nullité de l'autocorrélation en τ conduit à l'égalité :

$$\sum_{i=0}^{\ell-1} f(x) f(x + \tau) = 0;$$

sans compter les termes nuls, cette somme contient $\ell - 2$ termes égaux à ± 1 dont le produit vaut $(-1)^{\frac{\ell-2}{2}}$. Par ailleurs, remplaçons $f(x + \tau)$ par $-f(x + \tau - \ell)$ dès que $x + \tau \geq \ell$. Abstraction faite des $\tau - 1$ changement de signes, chaque valeur $f(x)$ apparaît deux fois, sauf $f(\tau)$ et $f(\ell - \tau)$. Finalement,

$$(-1)^{\frac{\ell}{2}} = (-1)^{\tau} f(\tau) f(\ell - \tau)$$

expression qui conduit à la relation demandée. $\square$

18. Ensemble à différences relatifs et matrices négacycliques

Soit R une partie de G de cardinal k. On dit que R est un
(v, k, λ, μ)
ensemble à différences relativement à un sous-groupe N de G, si
la fonction d'autocorrélation de l'indicatrice f de R prend
au plus trois valeurs :

$$D \times D(\tau) = \begin{cases} v, & \text{si } \tau = 0\,; \\ \mu, & \text{si } \tau \in H \setminus \{0\}\,; \\ \lambda, & \text{sinon.} \end{cases}$$

Cette notion qui manifestement généralise celle d'ensembles à différences semble avoir été inventée par R. Chauduri. La transformée de Fourier f de vérifie :

$$|\widehat{f}(\chi)|^2 = \begin{cases} v\lambda + |N|(\mu - \lambda) + k - \mu, & \chi = 1; \\ |N|(\mu - \lambda) + k - \mu, & \chi \perp H; \\ k - \mu, & \chi \not\perp H; \end{cases}$$

Considérons s une séquence θ-presque-parfaite,$f = \frac{1+s}{2}$ est l'indicatrice d'un ensemble à différence relatif de paramètres $N = \{0, \frac{v}{2}\}$, $k = \frac{v}{2}$, $\mu = \theta^2+\theta$ et $\lambda = \frac{v}{4}+\theta$.

Notons m la moitié de v, et supposons $\theta = 1$, il existe une et une seule position $0 \leq i \leq m-1$ telle que $s_i = s_{i+m}$ sans perdre en généralité, on peut supposer que $i = 0$. La matrice négacyclique

$$C = \begin{pmatrix} 0 & s_1 & \dots & s_{m-1} \\ -s_{m-1} & 0 & \dots & s_{m-2} \\ \vdots & \vdots & \ddots & \vdots \\ -s_1 & -s_2 & \dots & 0 \end{pmatrix}$$

satisfait l'égalité $CC^t = (m-1)\, I_m$: c'est une matrice de conférence. Le théorème de Belevitch affirme une symétrie « tordue ». Les matrices de conférences négacycliques. Les matrices de conférences négacycliques de petites longueurs sont étudiées dans [**62**]. Il y a une correspondance bijective entre matrice de conférences négacycliques de dimension m et séquences 1-presque-parfaite de longueur $2m$. Dans cette correspondance, les séquences construites dans la section précédente sont des matrices de Paley [**157**].

19. Famille d'intercorrélation

Un $q-(M, L, \theta_a, \theta_i)$ ensemble d'intercorrélation $\mathcal{F}$ est un ensemble de M séquences de longueurs L à valeurs dans l'ensemble des racines q-ième de l'unité dont l'autocorrélation hors phase n'excède pas θ_a, et telles que l'intercorrélation de deux séquences distinctes de dépasse pas θ_i. On note

$$\theta(\mathcal{F}) = \max\{\theta_a, \theta_i\}.$$

En télécommunication, pour θ fixé et pour une période donnée, on souhaite construire une famille d'intercorrélation maximale.

Proposition 19.1 (Sidelnikov). *Soit s un entier naturel. Supposons qu'il existe un $q-(M, L, \theta, \theta)$ ensemble d'intercorrélation.*

(1) Si $q = 2$ alors

$$\theta^2 > (2s+1)(L-s) + s - \frac{2^s L^{2s+1}}{M(2s)!\binom{L}{s}}$$

(2) Si $q > 2$ alors

$$\theta^2 > \frac{(s+1)}{2}(2L-s) - \frac{2^s L^{2s+1}}{M(s!)^2\binom{2L}{s}}$$

Démonstration. C'est le résultat de Sidelnikov, voir [**175**]. □

En posant $s = 2$ dans ces expressions, nous obtenons les bornes dites de Welch [**192**] :

$$\theta^2 > \begin{cases} 3L - 2 - \frac{L^2}{M}, & \text{si } q = 2. \\ 2L - 1 - \frac{L^2}{M}, & \text{si } q > 2. \end{cases}$$

Dans les années 60, Gold [**76**] donne une famille de séquences binaires optimale du point de vue de la borne de Welch. Cette famille, $\mathcal{G}$, est construite à partir du corps à $q = 2^f$ éléments. Elle est formée des $M = q+1$ éléments :

$$s_a(i) = (-1)^{\mathrm{tr}_{\mathbf{F}_q/\mathbf{F}_2}(\gamma^{3i}+a\gamma^i)}, \quad s_\infty(i) = (-1)^{\mathrm{tr}_{\mathbf{F}_q/\mathbf{F}_2}(\gamma^i)}.$$

où γ désigne un élément d'ordre $2^f - 1$ et a varie dans $\mathbf{F}_q$. On vérifie sans peine que pour tout $\alpha \in \mathbf{F}_q{}^\times$ l'application booléenne $x \mapsto \mathbf{q}(x) = \mathrm{tr}_{\mathbf{F}_q/\mathbf{F}_2}(\alpha x^3)$ est une forme dont le noyau est de dimension 1 ou 2 suivant que f est impair ou pair. D'où l'on tire :

$$\theta(\mathcal{G}) \leq -1 + 2^{\lceil \frac{f+1}{2} \rceil}$$

En fait, on peut remplacer $\mathbf{q}(x)$ par d'autre type de fonctions booléennes, voir par exemple les articles de Boztas et Kumar [**24**].

Plus tard, Solé [**3**] puis Boztas, Hammons et Kumar [**23**] construisent des séquences analogues mais à partir de l'anneau de Galois $GR(4, f)$.

• Famille $\mathcal{A}$. Soit γ un générateur du groupe des Teichmüller de $A = GR(4, f)$. Soit X un système de représentants de $A \setminus \{0\}$ modulo l'action du groupe des Teichmüller. La première famille est formée des séquences quaternaires de la forme :

$$s_a(j) = i^{\mathrm{tr}_A(a\gamma^j)}, \qquad a \in X.$$

où γ est un élément générateur du groupe des Teichmüller de l'anneau de Galois $GR(4, f)$. Les calculs de la sections précédentes donnent les paramètres d'intercorrélations de cette famille. Notons $S(a)$ la somme triviale $\sum_{x \in T_A^0} \mu_A(ax)$. La valeur du coefficient d'autocorrélation de $s_a \times s_b(\tau)$ est donnée par :

$$1 + s_a \times s_b(\tau) = S(a\gamma^\tau - b)$$

qui reste de module au plus $\sqrt{q}$. Cette famille a pour paramètres :

$$L = q - 1, \quad M = q + 1 = L + 2, \quad \theta \leq 1 + \sqrt{L+1} = 1 + \sqrt{q}$$

• La famille $\mathcal{B}$ est un construite de manière similaire. On se donne un élément $\delta \in T_A^\times$ de sorte que $1+2\delta$ est d'ordre 2 et $\omega = \gamma(1+2\delta)$ est d'ordre $2(q-1)$. Ensuite, on considère les séquences de la forme $s_a(j) = \mu_A(a\omega)^j)$. Les calculs d'intercorrélations nous ramènent aux sommes triviales :

$$\begin{aligned} 2 + s_a \times s_b(\tau) &= S_A\big(a\omega^\tau - b\big) + S_A\big((a\omega^\tau - b)(1+2\delta))\big) \\ &= S_A(u + 2v) + S_A(u + 2(u\delta + v)) \end{aligned}$$

Pour $a \not\sim b$, on écrit $u + 2v = a\omega^\tau$. Si u est nul on obtient 0 sinon

$$S_A(1)[1 + \mu_A(\delta)]\mu_A(v/u)$$

qui en module reste inférieur à $\sqrt{2q}$. Le groupe d'ordre $2(q-1)$ n'agit pas fidèlement sur les éléments non-inversibles. En prenant des éléments deux à deux non équivalents dans $A^\times$, on obtient une famille de paramètres :

$$L = 2(q-1), \quad M = \frac{q+1}{2} = \frac{L+2}{4}, \quad \theta \leq 2 + \sqrt{L+2} = 2 + \sqrt{2q}$$

qui atteint encore la borne de Welch.

20. Généralisations

Soient A un anneau fini, ω un élément inversible, G le groupe engendré par ω et Γ une partie de $\widehat{A^+}$. Le groupe G agit sur l'ensemble des caractères, on suppose que le fixateur d'un élément arbitraire de Γ est G. Que peut-on dire des propriétés d'intercorrélations de l'ensemble de séquences :

$$\mathcal{F}(A, \omega, \Gamma) = \{s(\omega, \mu) \mid \mu \in \Gamma\}?$$

	A	ω	$<\omega>.X$	X'
$\mathcal{A}$	$GR(4,f)$	γ	$A\setminus\{0\}/G$	$GR(4,f)$
$\mathcal{B}$	$GR(4,f)$	$\gamma+2$	$GR(4,f)^\times$	$GR(4,f)$
$\mathcal{G}$	$K\times K$	(γ,γ^3)	$P^1(K)$	$K\times K$

TAB. 1. structures des familles $\mathcal{A},\mathcal{B},\mathcal{G}$.

Pour chaque caractère ψ posons $S(\psi)=\sum_{x\in G}\psi(x)$ et considérons Γ' le sous-groupe de $\widehat{A^+}$ engendré par les orbites de Γ. L'intercorrélation maximale de la famille ci-dessus satisfait

$$\theta(\mathcal{F})\leq \sup_{\psi\in\Gamma'-\{1\}}|S(\psi)|$$

Pour simplifier notre tâche, nous pouvons supposer A quasi-Frobenius que l'on identifie à son dual moyen d'un caractère admissible μ_A. Convenons de noter $s(a,\omega)$ la séquence $s_a(i)=\mu_A(a\omega^i)$, $S_G(a)$ la somme de Gauss triviale $\sum_{x\in G}\mu_A(ax)$. Soit X une partie de A constituée d'éléments deux à deux inéquivalents modulo l'action de G, les paramètres d'intercorrélation de la famille $\mathcal{F}(A,\omega,X)=\{s(a,\omega)\mid a\in X\}$ sont $q\leq|A|$, $M=|X|$, $L=|G|$ et

$$\theta\leq \sup_{a\in X'-\{1\}}|S_G(a)|$$

où X' est le sous-groupe de A engendré par les orbites des éléments de X.

Les familles $\mathcal{A}$, $\mathcal{B}$ et $\mathcal{G}$ sont bien de ce type. C'est évident pour les deux premières. Pour la troisième, il suffit de considérer l'anneau $K\times K$, $\omega=(\gamma^3,\gamma)$, et $X=P^1(K)=\{(1,\alpha)\mid\alpha\in K\}\cup\{(0,1)\}$.

21. Exemples

• Soit K une extension de degré f du corps à deux éléments. Considérons l'anneau :

$$A=K[X]/(X^2)$$

c'est anneau de valuation quasi-Frobenius. L'idéal principal engendré la classe de X, disons π, est à la fois minimal et maximal, c'est l'unique idéal propre de A. Tout élément de A s'écrit d'une et une seule façon sous la forme $a+b\pi$, le caractère

$$\mu_A(a+b\pi)=\mu_K(\beta)$$

est un caractère admissible.

Quelle famille peut-on construire avec le groupe $T_A^\times$? Désignons par γ un caractère générateur du groupe des Teichmüller.

$$S_{T_A^\times}(a+b\pi)=\sum_{x\in T_A^\times}\mu_K(bx)=\begin{cases}q-1, & b=0;\\ -1, & b\neq 0.\end{cases}$$

La partie X cherchée doit satisfaire $M\cap X'=\{0\}$ et nous n'avons pas beaucoup de possibilités : $X=\{u\}$ avec $u\in A^\times$. Nous n'avons pas plus de chance avec un groupe G d'ordre $2(q-1)$; c'est-à-dire engendré par $\omega = (1+\pi\delta)\gamma$, en effet

$$\begin{aligned}
S_G(a+b\pi) &= \sum_{i=0}^{2(q-1} \mu_A\big((a+b\pi)\omega^i\big) \\
&= S_{T_A^\times}(a+b\pi) + S_{T_A^\times}\big(a+(a\delta+b)\big) \\
&= \begin{cases} 2(q-1), & a=b=0; \\ q-2, & a\neq 0 = b, a \neq 0 = a+b\delta; \\ -2, & \text{autre.} \end{cases}
\end{aligned}$$

- Considérons l'anneau :

$$B = GR(4,f)[X]/(X^2-2, 2X)$$

C'est un anneau de valuation quasi-Frobenius d'idéal maximal principal engendré par la classe de X, encore notée π. Chaque élément x de B se décompose d'une et une seule manière comme une somme $x = a + b\pi + c\pi^2$, où a, b et c sont des représentants multiplicatifs de K. En particulier, la structure additive de B est isomorphe au produit $GR(4,f) \times K$. Notons $A = GR(4,f)$ et remarquons que le caractère de B défini par

$$\mu_B(a+b\pi+c\pi^2) = \mu_A(a+c\pi^2)$$

est un caractère admissible de B.

Avec les groupes d'ordre $q-1$ et $2(q-1)$ nous retrouverions les séquences des familles $\mathcal{A}$ et $\mathcal{B}$. Considérons un élément ω d'ordre $4(q-1)$ que l'on peut supposer sous la forme $\omega = (1+\pi\delta)\gamma$, où γ est un générateur du groupe des Teichmüller et $\delta \in T_B^\times$.

$$\begin{aligned}
S(a+b\pi+c\pi^2) &= \sum_{i=0}^{4q-3} \mu_B((a+b\pi+c\pi^2)\omega^i) \\
&= \sum_{r=0}^{3}\sum_{j=0}^{q-1} \mu_B((a+b\pi+c\pi^2)\omega^{4j}(1+\pi\delta)^r) \\
&= S_{T_A^\times}\big(a+2c\big) + S_{T_A^\times}\big(a+2(b\delta+c)\big) \\
&\quad + S_{T_A^\times}\big(a+2(a\delta^2+c\big) + S_{T_A^\times}\big(a+2(a\delta^2+b\delta+c)\big)
\end{aligned}$$

Comme dans le cas de la famille $\mathcal{B}$, il faut choisir δ tel que $\mathrm{tr}_A(\delta) = 1,3$. La partie $X = \{1+x\pi+x\pi^2 \mid x \in T_B^0\}$ contient $q-2$ points deux à deux inéquivalents modulo le groupe engendré par ω. En conclusion, si $\delta \neq 1$ on peut construire une famille de paramètres :

$$L = 4(q-1), \quad M \geq q-2 = \frac{L-4}{4}, \quad \theta \leq 4 + 2\sqrt{2q} = 4+\sqrt{2L}$$

Il n'est pas évident de savoir si nous pouvons faire mieux. Pour valider cette approche par les anneaux finis, il serait souhaitable de procéder à l'expérience numérique suivante. On se donne un anneau fini A, un élément ω d'ordre L dans $A^\times$ et un paramètre θ. On construit le graphe dont les sommets sont les séquences $s(a,\omega)$ acceptables du point de vue de l'autocorrélation. Deux séquences sont adjacentes si leur intercorrélation ne dépasse pas θ. Il ne reste plus qu'a utiliser un algorithme de recherche de cliques maximales pour extraire une famille d'intercorrélation.

CHAPITRE 6

Fonctions booléennes

Nos *fonctions booléennes*[1] sont des applications de domaines $\mathbf{F}_2^m$ à valeurs dans le corps à deux éléments. Elles sont les ingrédients de certaines recettes cryptographiques. Par exemple, en aval de la méthode de chiffrement « au fil de l'eau » , une fonction booléenne est utilisée pour masquer la clef de l'utilisateur. La sécurité du système, repose sur les propriétés de distribution et de non-linéarité de celle-ci. La distance de Hamming d'une fonction à l'espace des fonctions affines mesure le degré de non-linéarité. Les fonctions de non-linéarité maximale sont dites *hautement non-linéaire*, elles ont un degré de non-linéarité égal au rayon de recouvrement $\rho(m)$ du code de Reed-Muller du premier ordre. En dimension paire, il est assez facile d'obtenir des fonctions hautement non-linéaires. Ce sont les *fonctions courbes* de Rothaus [**163**] et le problème est plus de les analyser et de les classifier comme dans les travaux de Dillon [**65**], Carlet et Guillot [**41**], Hou et Langevin [**96**]. Dans le cas impair, la situation est très différente : on ne connaît pas le rayon de recouvrement du code de Reed-Muller affine en dimension ≥ 9. La non-linéarité des fonctions quadratiques est facile à obtenir, et conduit à une minoration : la borne quadratique. En 1980 [**152**] Mykkelveit détermine $\rho(7)$, et conjecture que la non-linéarité d'une fonction ne peut pas être supérieure à la borne quadratique. Hypothèse, mise en défaut trois en plus tard par le fameux contre-exemple de Patterson et Wiedeman [**158**] : il existe une fonction dépassant la borne quadratique en dimension 15. Le calcul du degré de non-linéarité des fonctions de degré trois est encore ouvert. L'approche générale proposée par Langevin et Solé [**130**] suggère la possibilité pour une cubique de dépasser la borne quadratique. À la lumière des articles de Hou [**87, 90**] et Langevin [**117**], la dimension ambiante doit être au moins égale à 15. La problèmatique liée à la recherche de fonctions équilibrées de non-linéarité maximale est plus récente. Le rayon de recouvrement du code de Reed-Muller affine parmi les fonctions équilibrées $\rho_B(m)$ est inconnu à partir de la dimension 8, quelque soit la parité. L'astucieux procédé d'*équilibrage* appliqué aux fonctions courbes par Seberry, Zhang et Zheng [**167**], puis Dobbertin [**67**], donne une première estimation. L'absence de résultats théoriques pousse à l'exploration expérimentale de l'espace des fonctions booléennes. Les résultats numériques les plus significatifs sont : la classification de toutes les fonctions de 6 variables par Maiorana [**140**], la classification par Hou des formes cubiques homogènes de 8 variables [**92**], la recherche des fonctions stables sous l'action de certains groupes [**131**] et la mise en évidence de la particularité des urcosets de poids impair dans [**133**].

1. Degré de non-linéarité

L'ensemble des fonctions booléennes est équipé de la fonction de poids de Hamming. Le poids $\mathrm{wt}(f)$ d'une fonction de f est égal au cardinal de son support $\mathrm{supp}(f) = \{x \in \mathbf{F}_2^m \mid f(x) = 1\}$. Les fonctions booléennes affines forment un

[1] De Boole, George Boole (1815–1864), théologien et mathématicien.

code de longueur n et de dimension $m+1$ qu'on appelle le code de Reed-Muller affine, ses paramètres sont faciles à déterminer sauf son rayon de recouvrement. En cryptographie, on souhaite utiliser des fonctions qui diffèrent le plus possible des fonctions affines. La distance $\delta(f)$ entre une fonction booléenne f et l'ensemble des applications affines mesure cette différence ; c'est le *degré de non-linéarité* de f.

$$\delta(f) = \inf_{\phi \text{ affines}} d_H(f, \phi).$$

Le coefficient de Fourier de f_χ en a et la distance de f à la fonction $\phi_{a,b}$ sont liés par la formule simple mais fondamentale :

$$d(f, \phi_{a,b}) = 2^{m-1} - \frac{\chi(b)}{2}\widehat{f_\chi}(a).$$

Pour cette raison, nous introduisons l'*amplitude spectrale* de f, $A(f) = \sup_{a \in \mathbf{F}_2{}^m} |\widehat{f_\chi}(a)|$. On a :

$$\delta(f) = 2^{m-1} - \frac{1}{2}A(f).$$

Par définition, le rayon de recouvrement du Reed-Muller affine est égal à la non-linéarité maximale que peut prendre une fonction.

$$\rho(m) = \sup_f \delta(f) = 2^{m-1} - \frac{1}{2}R(m). \tag{84}$$

où $R(m)$ est le *rayon spectral* du code de Reed-Muller du premier ordre :

$$R(m) = \inf_f A(f)$$

Considérons f une fonction booléenne, et laissons la magie des sommes de caractères opérer... La formule de Parseval donne :

$$\sum_{a \in \mathbf{F}_2{}^m} \widehat{f_\chi}(a)^2 = 2^m \sum_{a \in \mathbf{F}_2{}^m} f_\chi(a)^2 = 2^{2m}.$$

Ainsi, la valeur moyenne des carrés des coefficients de Fourier vaut $2^{\frac{m}{2}}$, d'où la borne dite de Parseval :

$$R(m) = \inf_{f \in B(m)} A(f) \geq 2^{\frac{m}{2}}. \tag{85}$$

Plus loin, nous montrerons que l'amplitude spectrale d'une forme quadratique non-dégénérée vaut $2^{\lceil \frac{m}{2} \rceil}$ ce qui montre que le rayon de recouvrement du code de Reed-Muller affine est complètement déterminé en dimension paire.

2. Le contre-exemple de Patterson et Wiedemann

En dimension impaire, on sait depuis [**152**] que $R(7) = 16$, voir aussi [**91**] et les calculs précédents montrent que

$$2^{\lceil \frac{m}{2} \rceil} \geq R(m) \geq 2^{\frac{m}{2}}.$$

Pour $m = 9$, 11 et 13, mais...

PROPOSITION 2.1 (Patterson-Wiedeman). *Il existe une fonction d'amplitude spectrale* 216 *dans* $\mathbf{F}_2^{\mathbf{F}_2^{15}}$, *et donc si* $m \geq 15$ *désigne un entier impair*

$$\frac{216}{256} \times 2^{\lceil \frac{m+1}{2} \rceil} \leq R(m) \leq 2^{\frac{m}{2}}.$$

DÉMONSTRATION. Après avoir identifié ${\mathbf{F}_2}^{15}$ au corps $\mathbf{F}_{2^{15}}$, Patterson et Wiedemann construisent toutes[2]les fonctions de 15 variables stables
sous l'action du groupe engendré par les transformations :
$x \mapsto x^2$,$x \mapsto \alpha x$,avec $\alpha \in \mathbf{F}_8^\times \cup \mathbf{F}_{32}^\times$. Ils trouvent deux applications booléennes d'amplitudes spectrales 216. □

Le groupe des transformations linéaires agit sur les fonctions booléennes et numériques. Le groupe stabilisateur de f est constitué des automorphismes linéaires fixant f

$$\mathrm{stab}(f) = \{\phi \in GL(m, \mathbf{F}_2) \mid f(\psi(x)) = f(x), \quad \forall x \in \mathbf{F}_2^m\}$$

Si f est une fonction booléenne stable sous l'action de G alors le support de f est une réunion d'orbites de $\mathbf{F}_2^m$ sous l'action de G. De plus, la transformée de Fourier de f est stable sous l'action du groupe $G^\star$ dont les éléments sont les adjoints de ceux de G.

PROPOSITION 2.2. *Les rangs de G et $G^\star$ sont égaux. En particulier, le nombre de valeurs prises par $\widehat{f_\chi}$ est inférieur au rang du groupe* $\mathrm{stab}(f)$.

DÉMONSTRATION. On peut démontrer ce résultat en utilisant le lemme de Burnside et le fait qu'une matrice carrée est semblable à sa transposée. Je remercie au passage D. Augot et P. Camion de m'avoir souflé cette indication. □

PROBLÈME 2.1. *D'autres expériences numériques ont été réalisées* [**53, 133, 131, ?**], *mais sans succès. Analyser la non-linéarité des fonctions stabilisées par un sous-groupe G aléatoire de rang faible.*

3. Conjectures

CONJECTURE 3.1. *Le rayon spectral $R(m)$ est équivalent à $2^{\frac{m}{2}}$.*

Pour confirmer cette conjecture, on doit prouver l'existence d'une suite de fonctions booléennes $(f_m)_{m\in\mathbf{N}}$ telle que pour tout m, f_m soit définie sur $\mathbf{F}_{2^m}$ et telle que la limite supérieure de la suite $\frac{A(f_m)}{2^{m/2}}$ soit égal à 1.

Pour construire cette suite de fonctions, j'ai proposé deux solutions. La première est dans ma thèse, il s'agit de fixer un polynôme $f(X)$ à coefficients dans une extension finie L de $\mathbf{F}_2$, et de considérer les fonctions $f_m(x) = \mathrm{tr}_{L_m/L}(f(X))$. La seconde provient de l'article *Kernels and Defaults* [**130**]. Il s'agit de construire une suite de cubiques à noyau minimal.

CONJECTURE 3.2. *Le rayon de recouvrement de* $\mathrm{RM}(1, m)$ *est pair.*

Cette conjecture proposée dans [**26**] est confortée par X.-D. Hou dans [**93**]. En utilisant le résultat (14.2), il montre que si $\rho(m)$ est impair alors le code $\mathrm{RM}(1, m)$ est anormal. À ce jour aucun code anormal n'est connu, voir la section sur les cubiques.

CONJECTURE 3.3. *Le logarithme du nombre de fonctions hautement non-linéaire est* $\mathrm{O}(\binom{m}{t})$.

Cette conjecture est basée sur les contraintes que doivent satisfaire les coefficients d'une fonction courbe.

[2]il y en a à peine $2^{12} = 4096$

```
Algorithme FormeAlgebrique(f, n);
 adresse
   f  :  une fonction ;
 valeur
   n  :  entier ( une puissance de 2);
 locale
   i  :  indice;
  debut
    si (n > 1)
      alors
        n ←  n/2;
        FormeAlgebrique(f, n);
        FormeAlgebrique(f + n, n);
        i ←  0;
        tant que (i < n)
          faire
            f[i+n] ←  f[i+n/2]+f[i];
            i ←  i+1;
        ftq
    fsi
  fin
```

FIG. 1. Forme algébrique de f.

PROBLÈME 3.1. *Soit f une fonction booléenne définie sur un $\mathbf{F}_2$-espace de dimension infinie E. On suppose que E est localement compact, ce qui nous permet de parler des caractères de E. Pour chaque sous-espace S de dimension finie, on pose : $R(S) = \sup_{\psi\in\hat{E}} |\sum_{s\in S} f_\chi(s)\psi(s)|$. On dit que f est une fonction universelle si*

$$R(S) \sim \sqrt{|S|}$$

Existe-t-il une fonction universelle ? Quel est le lien avec la conjecture (3.1) ?

4. Forme polynomiale

L'ensemble des fonctions booléennes hérite des opérations de $\mathbf{F}_2$ pour former une algèbre $\mathbf{F}_2^{\mathbf{F}_2^m}$ de dimension 2^m. Le noyau du morphisme qui envoie un polynôme de $\mathbf{F}_2[X_1, X_2, \ldots, X_m]$ sur sa fonction polynomiale est engendré par les polynômes $X_i^2 - X_i$. Il est surjectif, et toute fonction $f \in \mathbf{F}_2^{\mathbf{F}_2^m}$ possède une forme algébrique

$$f(X) = \sum_{S\subset[1,m]} a_S X_S$$

où X_S désigne le monôme $\prod_{i\in S}^m X_i$; c'est un polynôme *réduit* ses degrés partiels sont au plus 1, son degré total est le *degré* de la fonction f, noté $\deg(f)$. Le coefficient de X_S dans l'expression polynomiale de f est donné par la formule : $a_S = \sum_{\mathrm{supp}(x)\subset S} f(x)$. L'ensemble des parties de $[1, m]$ s'identifie à $\mathbf{F}_2^m$ et on peut écrire $f(X) = \sum_{u\in\mathbf{F}_2^m} \dot{f}(u)X^u$, l'application $f \mapsto \dot{f}$ est une involution de $\mathbf{F}_2^{\mathbf{F}_2^m}$ qu'on détermine en $\Theta(mn)$ par l'algorithme (1).

On vérifie sans peine que l'ensemble des fonctions de degré au plus k est un espace vectoriel de dimension $\sum_{i=0}^{k}\binom{m}{i}$. C'est le support du *code de Reed-Muller* d'ordre k en m variables. On le note $\mathrm{RM}(k,m)$. Le code $\mathrm{RM}(k,m)$ est un code de longueur 2^m, de dimension $\sum_{i=0}^{k}\binom{m}{i}$, de distance minimum 2^{m-k}.

THÉORÈME 4.1. *Pour k compris entre 1 et $m-2$, le groupe des automorphismes du code $\mathrm{RM}(k,m)$ est égal au groupe des transformations affines de $\mathbf{F}_2^m$.*

La démonstration de ce résultat de P. Delsarte n'est pas très difficile, voir [**120**]. En fait, un code dont le groupe des isométries contient le groupe des transformations affines est un code de Reed-Muller. On obtient alors le résultat fondamental :

PROPOSITION 4.1. *Le code de Reed-Muller d'ordre k est engendré par les indicatrices des variétés affines de codimension k.*

Les distributions de poids des codes de Reed-Muller d'ordre 0,1, 2 sont connues. Notons que $\mathrm{RM}(m-1-k,m)$ est le dual de $\mathrm{RM}(k,m)$ et que l'on peut déterminer les distributions des codes de Reed-Muller d'ordre $m-1$, $m-2$, $m-3$ par la transformée de MacWilliams.

5. Théorèmes d'Ax et Katz

Nous avons déjà rencontré le théorème d'Ax dans le cadre général des corps finis. L'énoncé de ce théorème, et surtout sa preuve, dans le cas particulier du corps à deux éléments mérite un détour. Avant de commencer, remarquons que le poids d'une fonction booléenne est lié à la somme de caractère $\widehat{f}_\chi(0)$ par la relation :

$$\mathrm{wt}(f) = 2^{m-1} - \frac{1}{2}\widehat{f}_\chi(0). \tag{86}$$

THÉORÈME 5.1 (Ax). *Si f est une fonction booléenne de degré s en m variables alors son poids est multiple de $2^{\lceil \frac{m}{s}\rceil -1}$*

DÉMONSTRATION. Ecrivons $f(x) = \sum_{d\in D} x^d$, et calculons la transformée de Fourier de f en 0 :

$$\begin{aligned}\widehat{f}_\chi(0) &= \sum_{x\in\mathbf{F}_2{}^m}\chi(\sum_{d\in D})x^d = \sum_{x\in\mathbf{F}_2{}^m}\prod_{d\in D}\chi(x^d) = \sum_{t\in\{0,1\}^m}\prod_{d\in D}(1-2t^d)\\ &= \sum_{t\in\{0,1\}^m}\sum_{j\in M}\prod_{d\in D}(-2t^d)^{j(d)}\end{aligned}$$

où M désigne l'ensemble des applications de D dans $\{0,1\}\subset\mathbf{C}$,

$$\begin{aligned}&= \sum_{j\in M}(-2)^{\sum_{d\in D} j(d)}\prod_{i=1}^{m}\sum_{t\in\{0,1\}}(t)^{\sum_{d\in D} j(d)d_i}\\ &= \sum_{j\in M}(-2)^{\sum_{d\in D} j(d)}(2)^{z(j)}\end{aligned}$$

où $z(j)$ désigne le nombre de i tel que la somme $\sum_{d\in D} j(d)d_i$ soit nulle. On a alors

$$s\sum_{d\in D} j(d) \geq \sum_{i=1}^{m}\sum_{d\in D} j(d)d_i \geq (m - z(j))$$

Ainsi les valuations dyadiques des termes de cette somme sont toutes plus grandes que $\min_{0\leq t\leq m} \frac{m-t}{s}+t$, c'est-à-dire $\lceil \frac{m}{s} \rceil$. □

Rappelons que ce théorème est le meilleur possible. En effet, posons $m = bs + r$, et considérons la fonction

$$x_{bs+1}x_{bs+2}\dots x_{bs+r} + \sum_{i=0}^{b-1} x_{is+1}x_{is+2}\dots x_{is+s}$$

La transformée de Fourier en zéro de cette fonction se calcule sans difficulté. Si r est non nul, on obtient $(2^d-2)^b(2^r-2)$, et sinon c'est : $(2^d-2)^b$.

Théorème 5.2 (Katz). *Soient f_1, f_2, ... ,f_s, s fonctions booléennes de degré respectif d_1,d_2, ... ,d_s. Notons d la somme des d_i, et δ le plus grand des d_i. Le poids de l'intersection $f_1f_2\cdots f_s$ est multiple de $2^{\lceil \frac{m-d}{\delta}\rceil}$*

Là encore, ce théorème est le meilleur possible. Notons que le degré du produit est majoré par d, et que l'application directe du théorème d'Ax ne conduit pas à un résultat si fin. Pour une démonstration de ce théorème dans le cas général, il faut essayer [**105**], et plus simplement [**186**].

Corollaire 5.1. *Soit f une fonction de degré s. La transformée de Fourier de f est à valeurs multiples de $2^{\lceil \frac{m}{s}\rceil}$. De plus,*

$$\widehat{f_\chi}(a) \equiv \widehat{f_\chi}(0) \pmod{2^{\lceil \frac{m+1}{s}\rceil+1}}$$

quel que soit $a \in \mathbf{F}_2^m$.

Démonstration. Le premier point résulte du théorème d'Ax et de la formule (86). Le second point résulte du théorème de Katz en notant que

$$\mathrm{wt}(f+\phi) = \mathrm{wt}(f) + \mathrm{wt}(\phi) - 2\mathrm{wt}(\phi f)$$

□

6. Lacunes dans les poids

Le théorème d'Ax a ses limites. En effet, le poids minimum du code $\mathrm{RM}(k,m)$ est 2^{m-k}, et pour des raisons de divisibilité, $2^{m-k}+2^{\lceil \frac{m}{k}\rceil-1}$ semble être le deuxième poids non-nul mais c'est faux ! Par exemple, considérons le code de Reed-Muller d'ordre 2, en $m = 2t$ variables. Le deuxième poids candidat est $2^{m-2}+2^{t-1}$. Nous devons l'exclure, car les poids du Reed-Muller d'ordre 2 sont de la forme : $2^{m-1} \pm 2^{\frac{m+i}{2}} \geq 2^{m-2}$, où i est un entier pair. Ce phénomène lacunaire a été étudié par T. Kasami et T. Tokura dans [**104**], prolongeant des travaux de E. R. Berlekamp et N. J. A. Sloane[**15**] ; Ils montrent que les poids compris entre 2^{m-s} et 2^{m-s+1} du code de Reed-Muller d'ordre s en m variables sont de la forme :

$$w = 2^{m+1-s} - 2^{m+1-s-\mu}, \quad \mu \leq \max\big\{\frac{m-s+2}{2}, \min(m-s,s)\big\}.$$

Problème 6.1. *Retrouver ce résultat à partir de la formule utilisée dans la preuve du théorème d'Ax. Préciser les poids supérieurs.*

7. Dérivations

La dérivée d'une fonction booléenne f dans la direction d'un vecteur de $v \in \mathbf{F}_2^m$ est la fonction :

$$D_v f(x) = f(x+v) + f(x)$$

La notion de dérivation joue un rôle important dans la théorie des fonctions booléennes. Une fonction est courbe si et seulement si toutes ses dérivées d'ordre 1 sont équilibrées. Plus généralement, si V désigne un système de r vecteurs
$v_1, v_2, \ldots, v_r$. La dérivée de f dans la direction de V est
la fonction notée $\partial_V f$ définie en x par

$$\partial_V f(x) = \sum_{\lambda_1,\lambda_2,\ldots,\lambda_r} f(x + \sum_{i=1}^{r} \lambda_i v_i),$$

où les λ_i varient dans $\mathbf{F}_2$. Ce n'est pas à proprement parler une dérivation.
Heureusement d'ailleurs puisque la seule dérivation sur l'algèbre des fonctions booléennes, au sens habituelle, est l'application nulle.
Cependant,

$$\partial_{e_1,e_2,\ldots,e_r} f(x) = \frac{\partial^r}{\partial_{X_1}\partial_{X_2}\ldots\partial_{X_r}} f(x),$$

ce qui justifie la terminologie. Si V est un système de vecteurs liés alors
$D_V F$ est nulle, sinon
$\partial_{v_1,v_2,\ldots,v_r} f$ est égal au produit de convolution de f par la fonction indicatrice de S, l'espace engendrés par les v_i. Au sens de Dillon [**65**], ce produit est la dérivée de f dans la direction du sous-espace S, nous dirons que c'est une dérivation d'ordre r.

Supposons que f soit une fonction booléenne de degré s. La dérivée de f une direction arbitraire est de degré au plus $s-1$. Pour tout entier r, la fonction de r variables $D_{x_1,x_2,\ldots,x_r} f$ est à valeurs dans $\mathrm{RM}(s-r,m)$ son terme constant est :

$$\lambda^{(r)}(f)(x_1,x_2,\ldots,x_r) = \sum_{\lambda_1,\lambda_2,\ldots,\lambda_r} f(\sum_{i=1}^{r} \lambda_i v_i).$$

Cette fonction est un cas particulier de ce que Ward appelle la polarisation combinatoire, voir [**187**]. Dans ma thèse, on trouvera les détail, à propos des définitions qui suivent. La fonction $\lambda^{(s)}(f)$ est une application s-linéaire alternée ; c'est la *forme multilinéaire associée* à f. Les notions de noyaux et de défauts que l'on rencontre dans la théorie des formes quadratiques se généralisent : le *noyau* de f est l'ensemble des $s-1$-uplets $(x_1,x_2,\ldots,x_{s-1})$ tels que

$$\lambda^{(s)}(f)(x_1,x_2,\ldots,x_{s-1},z) = 0, \quad \forall z \in \mathbf{F}_2^m$$

Le noyau de f est noté $\ker(f)$. La pré-image de 1 par $\lambda^{(s-1)}$ dans $\ker(f)$ s'appelle le *défaut* de f :

$$\mathrm{def}(f) = \{(x_1,x_2,\ldots,x_{s-1})) \in \ker(f) \mid \lambda^{(s-1)}(x_1,x_2,\ldots,x_{s-1}) = 1\}$$

Le noyau de f n'est pas nécessairement un sous-espace vectoriel ! Mais la restriction de $\lambda^{(s-1)} f$ à $\ker(f)$ est une $r-1$-linéaire, et donc , le cardinal du défaut est toujours inférieur au cardinal du noyau. Par ailleurs, les applications :

$$f \mapsto |\mathrm{def}(f)|, \quad \text{et} \quad f \mapsto |\ker(f)|,$$

sont deux invariants affines.

8. Invariants affines

Le degré fournit une première classification des fonctions booléennes. On sait calculer le poids des fonctions affines et quadratiques, mais pas celui des cubiques. Pour comprendre pourquoi, il suffit de regarder l'action du groupe affine. Deux fonctions f et g sont dites équivalentes $(f \sim g)$ s'il existe une transformation affine A telle que $f = g \circ A$. Le groupe affine $\mathrm{GA}_m(\mathbf{F}_2)$ est d'ordre

$$2^{m+1} \prod_{i=1}^{m-1} (2^m - 2^i) = \Theta(2^{(m-1)m/2}),$$

alors que le nombre de fonction de degré au plus 3 vaut $2^{C_m^3 + C_m^2 + m + 1}$, et le nombre de classes de cubiques explose : le degré est une notion trop vague pour classifier efficacement les fonctions. Une application j définie sur l'espace des fonctions booléennes satisfaisant $j(f) = j(f \circ \phi)$ pour toute fonction f et pour tout $\phi \in \mathrm{GA}_m(\mathbf{F}_2)$ est un *invariant affine*. Le poids et le degré sont des invariants affines. Le spectre et la non-linéarité sont deux autres invariants affines standards. Pour progresser, il faut inventer d'autres invariants pertinents, et si possible numériquement calculables.

Dans les rapports [**133, 131**], nous avons introduit et étudié trois nouveaux invariants : le stabilisateur, l'indice et la hauteur. Soit f une fonction, le *stabilisateur* linéaire (affine) de f est formé des transformations linéaires (affines) fixant f son ordre est un invariant linéaire (affine). La dimension du plus grand plus grand espace affine sur lequel f est constante est l'*indice* de f. Enfin, la hauteur de f est égale à l'ordre de la plus petite dérivation annulant f.

PROBLÈME 8.1. *Ces invariants sont pertinents, mais numériquement inutilisables si la dimension ambiante est supérieure à* 10. *Démontrez-le ! Inventez d'autres invariants.*

9. Indice d'une fonction

L'indice d'une fonction booléenne f est aussi égal au plus grand entier s tel qu'il existe $m - s$ fonctions g_i vérifiant :

$$f \sim \sum_{S \in [1,m]} X_i \, g_i(X).$$

L'indice d'une fonction constante vaut m, celui d'une application affine non constante vaut $m - 1$ et celui d'une forme quadratique de rang maximal en dimension paire $m = 2t$ vaut t. En effet, si f est une forme quadratique de rang maximal alors f est de la forme :

$$x_1 x_{t+1} + x_2 x_{t+2} + \ldots + x_t x_{t+t} + \epsilon$$

ainsi f est constante sur le sous espace de dimension t d'équations $x_1 = x_2 = \cdots = x_t = 0$. La réciproque provient de la proposition :

PROPOSITION 9.1. *Soit f une fonction booléenne alors l'indice de f satisfait :*

$$\mathrm{ind}(f) \leq \log_2(|\widehat{f}_\chi|_\infty)$$

DÉMONSTRATION. Il suffit d'appliquer la formule de Parseval. □

Les fonctions courbes d'indice t jouent un rôle important dans l'article de Dobbertin [**67**] dans lequel il conjecture que les fonctions courbes sont toutes d'indice t et pourtant, on ne connaît pas de fonction d'indice plus petit que t ! Or ces fonctions sont susceptibles de posséder des propriétés de non-linéarité intéressantes. Clairement le nombre de fonctions d'indice t est majoré par :

$$\begin{bmatrix} m \\ t \end{bmatrix} 2^{2^m - 2^t + t + 1}, \tag{87}$$

où $\begin{bmatrix} m \\ t \end{bmatrix}$ est le nombre de sous-espaces linéaires de dimension t dans un espace de dimension m. C'est

$$\begin{bmatrix} m \\ t \end{bmatrix} = \prod_{i=0}^{t-1} \frac{2^m - 2^i}{2^t - 2^i}.$$

La table 1 ci-dessous montre qu'il existe certainement des fonctions d'indice plus petit que t pour m supérieur ou égal à 12.

t	3	4	5	6
$\log \begin{bmatrix} m \\ t \end{bmatrix}$	10,5	17,6	26,7	37,7
$2^t - 1$	7	15	31	63
$2^t - 1 - t$	4	11	26	57

TAB. 1. Estimation du nombre de sous-espaces de dimension fixée.

La construction de fonctions d'indice faible pose des problèmes analogues à la construction des bons codes correcteurs. Pour une petite dimension, $m \leq 10$, il est très facile de calculer l'indice d'une fonction car le nombre de sous-espaces est réduit, mais il n'existe probablement pas de fonction d'indice $\frac{m}{2}$. Par contre, pour les grandes dimensions les fonctions d'indice $\frac{m}{2}$ existent mais le calcul de l'indice d'une fonction semble impossible.

Nous introduisons la fonction $I(k, m)$, c'est l'indice minimal d'une application de degré k en m variables.

$$I(k, m) = \min_{\deg(f) \leq k} \operatorname{ind}(f)$$

On note plus simplement $I(m)$ pour $I(m, m)$. Le lecteur vérifiera que $I(2) = I(3) = 1$, et $I(4) = I(5) = 2$. Pour les autres valeurs de m, je ne sais pas, sur la base d'expériences numériques :

CONJECTURE 9.1.

$$I(6) = I(7) = 3, \quad I(8) = I(9) = 4.$$

PROBLÈME 9.1. *Comment construire une fonction d'indice inférieur à 6 en dimension 12 ? En existe-t-il pour* $t \in \{3, 4, 5\}$ *?*

PROBLÈME 9.2. *Soit* $Ind(m)$ *le problème qui consiste à calculer l'indice d'une fonction booléenne de* m *variables. Quelle est la complexité de* $Ind(m)$ *? Applications en cryptographie ?*

k/m	1	2	3	4	5	6	7
0	1	1	1	1	1	1	1
1	x	1	1	1	1	1	1
2		x	2	2	2	2	2
3			x	2	2	2	2
4				x	3	3	3
5					x	3	?
6						?	4

TAB. 2. Quelques valeurs de la fonction $h(k, m)$.

10. Hauteur d'une fonction

La *hauteur* d'une fonction booléenne f est égal au plus petit entier s tel que :

$$f \sim \sum_{[1,s] \not\subset S} a_S X_S$$

On la note $\mathrm{ht}(f)$, alors que $h(k, m)$ désigne la hauteur maximale d'une fonction de degré k en m variables. Dans notre article [**97**], nous étudions la fonction h au moyen de des dérivations. On démontre sans difficulté que $h(1, m) = 1$ pour $m > 1$, $h(2, m) = 2$ pour $m > 2$ et $h(3, m) = 2$ pour $m > 3$. De même, mais c'est plus délicat $h(4, m) = 3$ pour $m > 4$. Les valeurs connues de $h(k, m)$ sont résumées par la table (2).

PROPOSITION 10.1. [**97**, πλ] *Pour m plus grand que 2,*

$$h(m, m+1) = h(m-2, m) + 1 \tag{88}$$

PROPOSITION 10.2 (Charpin-Hou-Langevin). *Soit $l(m)$ le plus grand entier i tel que $i + 2^{i-1} \leq m$. Pour tout entier k et m, $1 \leq k < m$, on a :*

$$\lceil \frac{k+1}{2} \rceil \leq h(k, m) \leq m - l(m)$$

La majoration provient de l'article [**45**] de Pascale Charpin. Pour la minoration, et quelques améliorations de la majoration, voir [**97**].

PROBLÈME 10.1. *Compléter la table 2. Est-ce que $m \mapsto h(k, m)$ est une fonction constante ?*

11. Fonctions courbes

Dans cette section, on suppose que m est pair disons $m = 2t$. Comme nous l'avons vu $R(m)$ est parfaitement déterminé. On a $R(m) = 2^t$ et le problème consiste à trouver des fonctions hautement non-linéaires. Depuis l'article [**163**] les fonctions hautement non-linéaires en dimension paire sont dites *courbes*. Cette terminologie due à Rothaus ne vaut qu'en dimension paire. Les fonctions courbes jouissent d'un grand nombre de propriétés. Retenons les équivalences :

(1) f est courbe,
(2) f_χ est une fonction à autocorrélation parfaite,
(3) le support de f est un ensemble à différence de Hadamard,
(4) Pour tout v non nul, $D_v f(x)$ est équilibrée,
(5) La matrice $\big(\chi(x+y)\big)_{x,y \in \mathbf{F}_2{}^m}$ est une matrice de Hadamard.

Par ailleurs, si f est une fonction courbe, alors pour toute fonction affine $\phi \in \mathrm{RM}(1,m)$ et pour toute transformation affine Ψ , l'application $\phi + f \circ \Psi$ est encore courbe. Le groupe $\mathrm{GA}_m(\mathbf{F}_2) \ltimes \mathrm{RM}(1,m)$ agit sur l'ensemble des fonctions courbes. Une *classe* de fonctions courbes est un ensemble de fonctions courbes stable sous l'action du groupe $\mathrm{GA}_m(\mathbf{F}_2) \ltimes \mathrm{RM}(1,m)$.

Si f est courbe alors il existe une fonction booléenne $\tilde{f}$, c'est la fonction *duale* de f, telle que : $\widehat{f_\chi}(a) = \tilde{f}_\chi(a)2^t$, la fonction $\tilde{f}$ est elle même courbe et l'application $f \mapsto \tilde{f}$ est une involution de l'ensemble des fonctions courbes. Une classe de fonctions courbes stable sous cette action est dite *autoduale*.

- L'ensemble $\mathcal{Q}$ des fonctions quadratiques courbes forme une classe. Le groupe $\mathrm{GA}_m(\mathbf{F}_2) \ltimes \mathrm{RM}(1,m)$ agit fidèlement sur la classe $\mathcal{Q}$. En d'autres termes, toutes les fonctions quadratiques courbes se déduisent de la forme quadratique :

$$< x, y >= x_1y_1 + x_2y_2 + \cdots + x_ty_t$$

Des cardinaux du groupe linéaire et du groupe symplectique, voir par exemple [**64, 179**], on déduit le nombre d'éléments de la classe $\mathcal{Q}$:

$$|\mathrm{GL}_m(\mathbf{F}_2)| = 2^{2t^2-t}\prod_{i=1}^{m}(2^i-1), \quad |\mathrm{Sp}_m(\mathbf{F}_2)| = 2^{t^2}\prod_{i=1}^{t}(2^{2i}-1), |\mathcal{Q}| = 2^{t^2+t+1}\prod_{i=0}^{t-1}(2^{2i+1}-1)$$

Le calcul (93) de la duale d'une forme quadratique en fonction de son invariant de Arf montre que la classe $\mathcal{Q}$ est autoduale.

- Identifions ${\mathbf{F}_2}^m$ au produit ${\mathbf{F}_2}^t \times {\mathbf{F}_2}^t$. Soit π une permutation de ${\mathbf{F}_2}^t$ et soit g une fonction booléenne définie sur ${\mathbf{F}_2}^t$. La fonction booléenne $(x,y) \mapsto < x, \pi(y) > +g(y)$ est courbe, et sa duale est la fonction $(x,y) \mapsto < \pi^{-1}(x), y > +g \circ \pi^{-1}(x)$. La classe $\mathcal{M}$ des fonctions courbes engendrées par ces fonctions et leur duale s'appelle la classe de Maiorana-MacFarland. Clairement la classe $\mathcal{M}$ est autoduale, et

$$|\mathcal{M}| \geq 2^{2^t}(2^t)!$$

Les degrés des fonctions de la classe de Maiorana-MacFarland couvrent l'intervalle $[2,t]$. Réciproquement,

PROPOSITION 11.1. [**120, 117**, π_λ] *Soit f une fonction booléenne. Si les valeurs de la transformée de Fourier de f sont divisibles par s alors f est de degré au plus $m-s+1$. Plus précisément, ces valeurs sont toutes de valuation 2-adique s alors f est de degré $m-s$. En particulier, le degré d'une fonction courbe est compris entre 2 et t.*

- Soit E un ensemble de 2^t+1 sous-espaces vectoriels , tous de dimension t, et deux à deux supplémentaires. On dira que E est un *bon recollement* de ${\mathbf{F}_2}^m$. L'ensemble des fonctions numériques

$$\sum_{S\in E} a(S)1_S,$$

obtenu en faisant varier a dans l'ensemble des fonctions de E à valeurs dans $\{-1,+1\}$ et satisfaisant : $\sum_S a(S) = \pm 1$ génère une classe de fonctions courbes. C'est la classe $\mathcal{PS}(E)$. Pour être effectif, il faut trouver un bon recollement. Par exemple, l'ensemble des 2^t+1 droites vectorielles de $\mathbf{F}_{2^m}$ considéré comme un $\mathbf{F}_{2^t}$-espace vectoriel est un bon recollement de ${\mathbf{F}_2}^m$.

En dimension paire, le stabilisateur d'une fonction courbe de degré 2 est le groupe orthogonal O^ϵ. On sait que les groupes orthogonaux sont de rang trois : le nombre d'orbite de $\mathbf{F}_{2^m}$ sous l'action de O^ϵ est égal à trois.

PROPOSITION 11.2 (Langevin-Solé-Solé). *Soit f une fonction courbe. Si* $\operatorname{stab}(f)$ *est de rang trois alors f est une forme quadratique.*

DÉMONSTRATION. C'est une conséquence immédiate de l'article (difficile) de Martin W. Liebeck sur la classification des groupes de rang trois [**137**]. ☐

L'ordre du stabilisateur affine d'une fonction courbe quadratique est très important mais par l'expérience numérique, on constate que le stabilisateur d'une fonction courbe peut-être beaucoup plus petit.

12. Coefficients des fonctions courbes

Les articles de Claude Carlet et Philippe Guillot [**39, 41**] sur une caractérisation des fonctions courbes sont à l'origine des résultats de cette section, développés dans l'article [**96**]. On commence par remarquer, en utilisant la formule de Parseval, qu'une fonction booléenne f est courbe si et seulement si les valeurs de la transformée de Fourier de f_χ sont des multiples impairs de 2^t.

Notons $\mathcal{A}_m$ l'idéal de $\mathbf{Z}[\mathbf{F}_2^m]$ formé des applications dont la transformée de Fourier est multiple de 2^t. La fonction f est courbe si et seulement si [3] f est dans la classe de $2^{t-1}\delta_0$ modulo $\mathcal{A}_m$. En particulier, la donnée d'une base ou d'un système générateur de l'idéal $\mathcal{A}_m$ conduit à une *caractérisation* des fonctions courbes. Pour trouver cette base, utilisons la fonction de Moebius et la formule d'inversion de Rota. En quelques mots, la *fonction de Moebius* d'un ensemble fini ordonné $(E, \leq)$ est l'unique application de $E \times E$ dans $\mathbf{Z}$ satisfaisant :

$$\sum_{x\leq z\leq y} \mu(x,z) = \sum_{x\leq z\leq y} \mu(z,y) = \begin{cases} 1, \text{si } x = y; \\ 0, \text{sinon}; \end{cases}$$

nulle si x n'est pas inférieur à y. Considérons une application g de E vers un groupe Abélien G et posons $f(x) = \sum_{y\leq x} g(y)$. La formule d'*inversion de Rota* permet de retrouver g à partir de f :

$$g(x) = \sum_{y\leq x} f(y)\mu(y,x)$$

La fonction de Moebius du produit de deux ensembles ordonnés est égale au produit des fonctions de Moebius. La fonction de Moebius de $\{0,1\}$ vaut $(-1)^{(x+y)}$ pour $x \leq y$, et donc la fonction de Moebius de $\mathbf{F}_2^m$ muni de l'ordre produit est :

$$\mu(x,y) = \begin{cases} \chi(x+y), & x \leq y; \\ 0, & \text{sinon.} \end{cases}$$

Pour chaque vecteur u, notons E_u la fonction exponentielle de base u ; c'est l'indicatrice du sous-espace vectoriel de $\mathbf{F}_2^m$ formé des vecteurs dont le support est inclus dans celui de u.

$$E_u(x) = u^x = \begin{cases} 1, & \text{si} \quad x \leq u; \\ 0, & \text{sinon.} \end{cases}$$

[3] Ici, et souvent dans cette section, j'utilise le même symbole pour désigner une fonction booléenne et sa fonction numérique à valeurs dans $\{0,1\} \subset \mathbf{Z}$. Le contexte permet de faire la différence.

La fonction E_u est de degré $m - \mathrm{wt}(u)$ comme le montre sa forme algébrique polynomiale : $E_u(x_1, x_2, \ldots, x_m) = \prod_{i|u_i=0}(x_i+1) = \sum_{v\leq\bar{u}} x_v$. En particulier, le système $(E_u \pmod 2)_{u\in\mathbf{F}_2^m})$ est une base de l'espace des fonctions booléennes, c'est un $\mathbf{Z}$-système libre de l'anneau $\mathbf{Z}[\mathbf{F}_2^m]$. La formule de Rota montre que c'est une base, le coefficient de E_u dans l'expression de la fonction entière g est donné par :

$$\sum_{x\leq u} g(x)\chi(x+u)$$

Notons $\bar{u}$ le complément de u. La transformée de Fourier de E_u est égale à $2^{\mathrm{wt}(u)}E_{\bar{u}}$. La base $(E_u)_{u\in\mathbf{F}_2^m}$ est une base adaptée à l'idéal $\mathcal{A}_m$. En utilisant une seconde fois la formule de Rota, on obtient sans peine que le système $\big(a(u)E_u\big)_{u\in\mathbf{F}_2^m})$ est une base $\mathcal{A}_m$, où $a(u)$ désigne l'entier $2^{\max\{0,t-\mathrm{wt}(u)\}}$.

Proposition 12.1 (Carlet-Guillot). *La fonction booléenne f est courbe si et seulement s'il existe des entiers m_u tel que*

$$f = 2^{t-1}\delta_0 + \sum_{u\in\mathbf{F}_2^m} m_u a(u)E_u. \tag{89}$$

Pour u de poids inférieur à t, $a(u)$ est pair, et la réduction modulo 2 de l'égalité (89) efface les termes degré supérieur à t. Ainsi, on retrouve bien que le degré d'une fonction courbe est au plus t (11.1). Cependant, l'équation peut nous en dire plus. Soit f une fonction entière de $2^{t-1}\delta_0 + \mathcal{A}_m$. Elle s'écrit d'une et une seule façon :

$$f = A_0 + \sum_{0<u\in\mathbf{F}_2^m} A_u E_u,$$

où les coefficients A_u sont des entiers satisfaisant $\mathrm{ord}_2(A_u) \geq t - \mathrm{wt}(u)$, sauf A_0 qui est de valuation $t-1$. De plus, f est à valeur dans $\{0,1\}$ si et seulement si :

$$\sum_{u*v=w} A(u)A(v) = A(w). \tag{90}$$

De cela, on tire :

Proposition 12.2. [**96**, ${\pi\!\!\lambda}$] *Soit $f(x) = \sum_{S\subset[1,m]} a_S X_S$ une fonction booléenne. Si f est courbe alors pour chaque partie V dont le cardinal est au moins t, les coefficients de f satisfont à l'équation quadratique :*

$$\sum_{S\cup T=V} a_S a_T = 0,$$

où V

Dans le cas où $V = [1,m]$, l'équation (12.2) se déduit immédiatement de l'équation (90). En effet,

$$f(x) = \sum_{\mathrm{wt}(u)=t} a(u)e_u(x) \equiv \sum_{\mathrm{wt}(u)=t} a(u)x_{\bar{u}} + \pmod{\mathrm{RM}(t-1,m)}$$

Par ailleurs, les coefficients $A(u)$ sont presque tous pairs, et l'équation :

$$\sum_{u*v=w} A(u)A(v) = A(0),$$

se réduit à

$$\sum_{u*v=0\mathrm{wt}(u)=\mathrm{wt}(v)=t} a(u)a(v) = 0.$$

Pour les autres valeurs de V, c'est un petit peu plus compliqué. Voir aussi [**95**].

PROBLÈME 12.1. *Determiner toutes les fonctions courbes de* RM(4, 8).

PROBLÈME 12.2. *Cette démarche s'applique-t-elle aux fonctions courbes généralisées ?*

13. Construction de fonctions courbes

Soit π une application de $\mathbf{F}_2^m$ dans $\mathbf{F}_2^m$. Notons π_i la i-ième projection de π. Rappelons [**65**] que π est une permutation si et seulement si les combinaisons linéaires à coefficients non tous nuls des fonctions booléennes π_i sont toutes équilibrées. On définit le *degré* de π :

$$\deg(\pi) = \max_{1 \leq i \leq m} \deg(\pi_i)$$

PROPOSITION 13.1 (Hou). [**94**] *Soit π une permutation.*

$$\deg(\pi^{-1}) \leq \frac{(\deg(\pi) - 1)m + 1}{\deg(\pi)}$$

Soient f et g deux fonctions booléennes de même poids. Il existe une permutation ψ de $\mathbf{F}_2^m$ tel que $g = f \circ \psi$. Ecrivons,

$$\psi^{-1}(x) = (\phi_1(x), \phi_2(x), \ldots, \phi_m(x))$$

La transformée de Fourier de g en a vaut :

$$\begin{aligned} \widehat{g_\chi}(a) &= \sum_{x \in \mathbf{F}_2^m} \chi\big(f(\psi(x)) + a.x\big) \\ &= \sum_{x \in \mathbf{F}_2^m} \chi\big(f(x) + a_1.\phi_1(x) + a_2.\phi_2(x) + \ldots + a_m.\phi_m(x)\big) \end{aligned} \tag{91}$$

Dans le but de construire une fonction g de non-linéarité supérieure ou égale à celle de f, le calcul (91) suggère la définition de l'ensemble :

$$C(f) = \{\lambda \mid |\widehat{(f + \lambda)}_\chi(0)| \leq A(f)\}$$

PROPOSITION 13.2. [**96**, $\pi\lambda$] *Soit S un code de dimension m inclus dans $C(f)$. Si S est équivalent au code simplex alors pour toute base ϕ_1, ϕ_2, ... ,ϕ_m de S l'application $\pi = (\phi_1, \phi_2, \ldots, \phi_m)$ est une bijection et la non-linéarité de $f \circ \pi^{-1}$ est plus grande que celle de f.*

Le problème est de déterminer $C(f)$ et des sous-espaces S convenables. Ce problème théoriquement difficile se simplifie lorsque la fonction est une cubique courbe. En effet, si f est courbe alors pour toute matrice inversible A et pour tous vecteurs a, b la fonction $x \mapsto f(A.x + b) + f(x) + a.x$ est dans $C(f)$. En particulier, on dispose d'un algorithme non déterministe (FIG. 2) pour construire une nouvelle fonction courbe à partir d'une cubique courbe. La correction de l'algorithme repose sur la proposition (13.3). Pour garantir le bon fonctionnement de cet algorithme, à l'entrée , f doit être courbe de degré 3, et dans ce cas , la fonction résultat est dans $\mathrm{RM}(\lceil \frac{m+1}{2} \rceil, m)$, c'est une conséquence de (13.1). Pour chaque vecteur u, notons $D_u f$ la dérivée de f dans la direction de u : $D_u f(x) = f(x + u) + f(x)$.

PROPOSITION 13.3. [**96**, $\pi\lambda$] *L'espace engendré par les fonctions affines et les dérivées de f est inclus dans $C(f)$.*

```
Algorithme Permutation(f);
 adresse
              f  :  une fonction ; ;
 locale
   φ1, . . . , φm  :  fonctions booléennes ;;
          a, b  :  vecteur ;;
  debut
    repeter
      pour i ∈ [1, m] faire
        Choisir a et b au hasard;
        φi ← f(x + a) + f(x) + b.x;
      fdpour
    jusqua [φ1, φ2, . . . , φm] bijective ;
    f ← [φ1, φ2, . . . , φm]^(−1);
  fin
```

FIG. 2. construction d'une fonction courbe

DÉMONSTRATION. Les fonctions concernées sont dans $C(f)$. Il suffit de montrer que pour chaque couple (u, v) la fonction $D_u f + D_v f$ est bien dans $C(f)$. Or, $D_{u+v} f = D_u f + D_v f \pmod{\mathrm{RM}(\deg(f) - 2, m)}$. □

PROBLÈME 13.1. *Implanter une version efficace de l'algorithme.*

14. Urcosets

Soit f une application booléenne. On dit que f est un *leader*, si f est de poids minimum dans le translaté $f + \mathrm{RM}(1, m)$. On note $\mathrm{L}(f)$ l'ensemble des leaders g contenus dans la classe de f. L'union des supports des leaders de f est noté $\mathrm{supp}^+(f)$.

$$\mathrm{supp}^+(f) = \cup_{g \in \mathrm{L}(f)} \mathrm{supp}(g).$$

Soient f et g deux fonctions booléennes. On dit que la classe de f est inférieure à la classe de g s'il existe un leader $l \in \mathrm{L}(f)$ et un leader $l' \in \mathrm{L}(g)$ tels que $\mathrm{supp}(l) \subset \mathrm{supp}(l')$. On démontre , voir [**26**], que cette relation est une relation d'ordre partiel sur l'ensemble des translatés du code de Reed-Muller affine. La classe de f est un élément maximal pour cette relation si et seulement si $\mathrm{supp}^+(f) = \mathbf{F}_2^m$. De ceci, on déduit un algorithme pour tirer un urcoset au hasard. Le translaté d'un élément maximal est appelé un *urcoset* du Reed-Muller affine par Assmus et Mattson, *orphelin* par Vera Pless et *classe latérale maximale* dans ma thèse ! Le translaté d'une fonction hautement non-linéaire est un urcoset. Il suffit d'appliquer la proposition (14.1) pour réaliser que la réciproque est fausse. Dans une version préliminaire de leur article, V. Pless et R. Brualdi conjecturent que les urcosets de $\mathrm{RM}(1, m)$ sont tous de poids pairs. C'est faux, X.-D. Hou a construit un contre-exemple en dimension 11. En fait, il existe des urcosets à poids impairs dès que m est supérieur ou égal à 6. Cependant, et je n'ai pas d'explication, les urcosets de poids impairs sont beaucoup plus rares que ceux de poids pairs, ce phénomène est illustré par la figure (TAB. 3) qui résume le résultat d'une expérience numérique. Sur un tirage aléatoire de 20 millions d'urcosets en dimension 7 (FIG. **??**), nous en obtenons 629176 de poids impairs : à peine 3%.

F. max	Distrib.	F. max	Distrib.
16	231	30	1
18	18	32	37692
20	5869094	34	0
22	611026	36	1187
24	12526617	38	0
26	16944	40	23
28	937167		

TAB. 3. Distribution des urcosets $m = 7$.

PROPOSITION 14.1. [**118**, $\pi\lambda$] *Soit f une fonction booléenne et k un entier. Si la transformée de Fourier de f prend ses valeurs dans l'ensemble $\{-2^{\frac{m+k}{2}}, 0, 2^{\frac{m+k}{2}}\}$, alors la classe de f est un urcoset du code de Reed-Muller affine.*

On déduit de cette proposition que les fonctions strictement quadratiques définissent toujours des urcosets. Ce résultat a été généralisé par Hou dans [**93**]. Une fonction strictement de degré s définit un urcoset du code de Reed-Muller d'ordre $s-1$.

PROPOSITION 14.2. [**118**, $\pi\lambda$] *Si f est une fonction booléenne de poids impaire, c'est-à-dire strictement de degré m alors il existe une position $a \in \mathbf{F}_2^m$ telle que*

$$l \in \mathrm{L}(f) \quad \Longrightarrow \quad l(a) = 1.$$

X.-D. Hou utilise cette proposition dans [**93**] pour montrer que l'existence d'une fonction hautement non-linéaire de poids impair impliquerait le caractère anormal du code de Reed-Muller du premier ordre. Le fait qu'aucun code anormal n'ait encore été répertorié motive la conjecture (3.2).

15. Formes quadratiques

La théorie des formes quadratiques permet de calculer la distribution de poids du code de Reed-Muller du second ordre. Pour nous, une forme quadratique est une fonction de degré 2 sans terme constant, et donc, q est une forme quadratique si et seulement s'il existe une forme bilinéaire symplectique ϕ telle que :

$$q(0) = 0, \qquad q(x+y) = q(x) + q(y) + \phi(x,y), \quad \forall x, y \in \mathbf{F}_2^m,$$

que l'on appelle la *forme bilinéaire associée* à q. L'ensemble des vecteurs $z \in \mathbf{F}_2^m$ tels que $\phi(x,z) = 0$ s'appelle le *noyau* de q, c'est un espace vectoriel, noté $\ker(q)$. La co-dimension de $\ker(q)$ est toujours paire, c'est le *rang de la forme quadratique* . La forme q est dite de rang maximal si son noyau est de dimension au plus 1. La restriction de q à son noyau est linéaire. Si cette restriction est non-nulle alors la forme est dite *défective*. On définit l'ensemble des *défauts* de q par

$$\mathrm{def}(q) = \mathrm{supp}(q) \cap \ker(q).$$

On distingue trois types de formes quadratiques : les formes *paraboliques* qui sont équilibrées, les formes *elliptique* de poids élevés et les formes *hyperboliques* de poids faible. La table (4) donne le poids d'une forme quadratique en fonction de son rang et de son type.

PROPOSITION 15.1. *Soit q une forme quadratique de rang $2r$. La transformée de Fourier de q prend les valeurs :*

$\widehat{q_\chi}(0)$	type	poids	exemple
<0	elliptique	$2^{m-1}+\frac{1}{2}2^{(m+k)/2}$	$xy+x+y$
$=0$	parabolique	2^{m-1}	$xy+z$
>0	hyperbolique	$2^{m-1}-\frac{1}{2}2^{(m+k)/2}$	xy

TAB. 4. Les trois types de formes quadratiques.

valeur	*multiplicité*
$+2^{(m+k)/2}$	$\frac{1}{2}\left(2^{m-k}+2^{(m-k)/2}\right)$
0	$2^m-2^{(m-k)}$
$-2^{(m+k)/2}$	$\frac{1}{2}\left(2^{m-k}-2^{(m-k)/2}\right)$

DÉMONSTRATION. C'est une conséquence de la formule de Parseval. □

De cette proposition, on déduit la distribution de poids du Reed-Muller du second ordre, car on sait calculer le nombre de formes symplectiques de rang $2r$.

16. Invariant de Arf

Supposons m pair, $m=2t$ et condidérons une forme quadratique q de rang maximal. Nous savons que $\widehat{q_\chi(a)}$ vaut $\pm 2^t$, mais comment déterminer le signe ? Si par chance la forme bilinéaire ϕ coincide avec la forme $(x,y)\mapsto x.y$, alors

$$
\begin{aligned}
\widehat{q_\chi}(a) &= \sum_{x\in\mathbf{F}_2^m}\chi(q(x)+a.x)\\
&= q_\chi(a)\sum_{x\in\mathbf{F}_2^m}\chi(q(x)+q(a)+a.x) \qquad (92)\\
&= q_\chi(a)\widehat{q_\chi}(0).
\end{aligned}
$$

En particulier la fonction q_χ est un vecteur propre de la transformée de Fourier. Dans le cas général, c'est plus délicat, il faut utiliser l'invariant de Arf de q. Une *base symplectique* pour la forme symplectique ϕ est une base $(e_1,e_2,\dots,e_m)$ telle que :

$$\phi(e_i,e_j)=\begin{cases}1, & j\equiv i+t \pmod m;\\ 0, & \text{sinon.}\end{cases}$$

On démontre, c'est bien sûr dans [**64**], mais je préfère l'article de trois pages de Dye [**70**], que la quantité :

$$\mathrm{Arf}(q)=\sum_{i=1}^{t} q(e_i)q(e_{i+t}),$$

ne dépend pas de la base symplectique : c'est l'invariant de Arf de la forme quadratique q. On détermine le poids de q en se rappelant que la forme q est de poids élevé si $\mathrm{Arf}(q)=1$:

$$\widehat{q_\chi}(0)=(-1)^{\mathrm{Arf}(q)}2^t$$

Maintenant, notons q_a la forme quadratique $q(x)+a.x$. On a

$$\mathrm{Arf}(q_a)=\mathrm{Arf}(q)+a\sum_{i=1}^{m}q(e_i)e_{i+t}+\sum_{i=1}^{t}(a.e_i)(a.e_{i+t}). \qquad (93)$$

EXERCICE 16.1. *Combien de fonctions de degré* 2 *sont courbes et vecteur propre de l'opérateur de Fourier.*

17. Le code de Kerdock

Soit C un $[n,k,d]$ code sur l'alphabet K. On suppose que son rayon de recouvrement ρ est supérieur à sa distance minimale d. Désignons par $\mathcal{V}$ un ensemble de vecteurs à distance ρ de C tel que

$$\forall (x,y) \in \mathcal{V}\times\mathcal{V}, \qquad x=y, \quad \text{ou} \quad d(x-y,C)=\rho \tag{94}$$

L'union du code C et des translatés $\bigcup_{x\in\mathcal{V}} x+C$ est une *extension gloutonne* de C. C'est un code non-linéaire de distance minimale ρ et de cardinal $2^k(1+|\mathcal{V}|)$.

Supposons $m=2t$. En faisant varier $a\in {\mathbf{F}_{2^m}}^{\times}$ dans l'expression :

$$x\mapsto \mathrm{tr}_{\mathbf{F}_{2^m}/\mathbf{F}_2}\big(\sum_{i=1}^{t}(ax)^{1+2^i}\big),$$

on obtient un ensemble de formes quadratiques de rang maximal satisfaisant la propriété 94. Ces formes quadratiques sont des fonctions courbes et l'extension gloutonne qui en résulte $\mathcal{K}(m)$ s'appelle la version Delsarte-Goethals du code de Kerdock.

PROPOSITION 17.1. *Soit $\kappa(m)$ le rayon de recouvrement du code de Kerdock $\mathcal{K}(m)$ vérifie l'inégalité*

$$2^{m-1}-2^{m/2}\leq \kappa(m)\leq 2^{m-1}-\frac{1}{2}\sqrt{32^m-2}$$

DÉMONSTRATION. Pour la minoration, c'est le « super code lemma ». Soient f et g deux applications booléennes, notons $S(f,g)=\sum_{x\in\mathbf{F}_{2^m}}\chi\big(f(x)+g(x)\big)$ le « coefficient de Fourier de f en g ». Suivant une note non publiée de C. Carlet, les moments d'ordres 2 et 4 des coefficients $S(f,g)$ avec g parcourant le code de Kerdock sont faciles à calculer

$$\sum_{g\in\mathcal{K}m} S(f,g)^2=2^{2m}, \qquad \sum_{g\in\mathcal{K}m} S(f,g)^4=2^{3m}(3\,2^m-2),$$

d'où la majoration. □

18. Fonctions équilibrées

Une fonction booléenne *équilibrée* est une fonction de poids 2^{m-1}. Les fonctions équilibrées sont de poids pairs et donc de degré au plus $m-1$. D'après la formule de MacWilliams, le nombre de fonctions équilibrées de degré au plus $m-2$ est égal au coefficient de $X^{n/2}Y^{n/2}$ du polynôme

$$\frac{1}{n}\big[(X+Y)^n+2(n-1)(X^2-Y^2)^{n/2}+(X-Y)^n\big]$$

c'est donc $\frac{2}{n}\big[C_n^{n/2}+(n-1)C_{n/2}^{n/4}\big]$ et il faut s'attendre à ce que les fonctions hautement non-linéaires équilibrées soient de degrés élevés. Le *rayon équilibré* du code de Reed-Muller du premier ordre est égal à la distance maximale d'une fonction équilibrée au code $\mathrm{RM}(1,m)$. De même le *rayon spectral équilibré* est égal à l'amplitude spectrale maximale d'une fonction équilibrée, of course

$$\rho_B(m)=2^{m-1}-\frac{1}{2}RB(m)$$

Les fonctions courbes ne sont pas équilibrées et la détermination de $RB(m)$ est encore plus difficile que celle de $R(m)$. Les bornes de Parseval et quadratiques deviennent

$$2^{\frac{m}{2}} + 4 \leq RB(m) \leq 2^{\frac{m+1}{2}}$$

On établit sans peine

$$\forall m, m' \in \mathbf{N}, \quad RB(m+m') \leq RB(m)\, R(m').$$

Notons $\Delta(f)$ la valeur minimale du module de la transformée de Fourier de f. Une fonction g est un *équilibrage* de f si $\Delta(g) = 0$ et si g se déduit de f en dépensant le moins d'énergie possible i.e. il existe une troisième fonction h de poids au plus $\frac{\Delta(f)}{2}$ telle que $g = f + h$ et, dans ce cas,

$$A(g) \leq A(f) + \Delta(f)$$

Mais on peut espérer construire des fonctions équilibrées loin du Reed-Muller du premier ordre en équilibrant des fonctions hautement non-linéaires. Par exemple, il existe un équilibrage du contre-exemple de Patterson et Wiedemann d'amplitude spectrale 244, d'où l'on tire

PROPOSITION 18.1. [**131**, $\pi\!\lambda$] *Si m est un entier impair supérieur ou égal à* 15 *alors*

$$RB(m) \leq \frac{61}{64} 2^{\frac{m+1}{2}} < 2^{\frac{m+1}{2}} \tag{95}$$

19. Equilibrage des fonctions courbes

Dans [**67**] Dobbertin complète le travail de Seberry, Zhang et Zheng [**167**] pour obtenir la proposition suivante.

PROPOSITION 19.1 (DSZZ). *Soit f une fonction courbe d'indice t. Il existe un équilibrage de g de f tel que $A(g) \leq 2^t + RB(t)$. Et donc, en écrivant $m = 2^r s$ ($r > 0$ et s impair) on obtient la borne*

$$RB(m) \leq 2^{m/2} + 2^{m/4} + \cdots + 2^s + 2^{\frac{s+1}{2}} \tag{96}$$

DÉMONSTRATION. Sans perdre en généralité, on peut supposer que f est constante égale à 0 sur un espace vectoriel S de dimension t. En appliquant la formule de Poisson, on réalise que

$$\sum_{a \in S^b ot} \widehat{f}(a) = 2^m f_\chi(0) = 2^m,$$

mezalors comme f est courbe $\widehat{f}(a) = 2^t$ sur $S^\perp$. Donnons nous n'importe quelle fonction booléenne h équilibrée sur S d'amplitude spectrale $RB(t)$. La somme $S(h,a) = \sum_{x \in S} \chi\big(h(x) + ax\big)$ est un coefficient de Fourier de h, et si nous notons g la fonction définie par

$$g(x) = \begin{cases} f(x) + h(x), & x \in S; \\ f(x), & x \notin S. \end{cases}$$

$$\widehat{g}(a) = \widehat{f}(a) - \sum_{x \in S} \chi(ax) + \sum_{x \in S} \chi\big(h(x) + ax\big) = \begin{cases} \widehat{f}(a) + S(h,a), & a \notin S^\perp; \\ S(h,0), & a \in S^\perp. \end{cases}$$

□

m	3	4	5	6	7	8
$RB(m)$	4	4	8	12	15	20 ou 24
$\rho_B(m)$	2	6	12	26	56	118 ou 116

TAB. 5. Les premières valeurs de $RB(m)$.

Cette proposition est constructive car il existe des fonctions courbes d'indices t. Plus curieusement, à ce jour, on ne connaît pas de fonction courbe qui ne soit pas d'indice t ! Dobbertin conjecture qu'il n'en existe pas, plus prudemment, je suggère :

PROBLÈME 19.1. *Construire une fonction courbe d'indice inférieur à t.*

La proposition (DSZZ) et les inégalités de la section qui précède permettent de dresser la table (5) qui nous montre que la plus petite valeur de m pour laquelle $RB(m)$ est inconnue est $RB(8)$.

PROBLÈME 19.2. *Calculer $RB(8)$.*

20. fonctions définies à partir de la trace

Lors d'une implantation, quand m est grand, les fonctions ne peuvent pas être mise en table. Le temps nécessaire pour calculer l'image d'un point par une fonction f doit rester faible, et en un certain sens, on souhaite utiliser des fonctions de *faible complexité* du point de vue temps de calculs. Pour cette raison, les fonctions de la formes $x \mapsto \mathrm{tr}_{\mathbf{F}_{2^m}/\mathbf{F}_2}\big(P(x)\big)$, où $P(X)$ est un monôme, à la rigueur un binôme, doivent retenir notre attention. Dans le cas d'un monôme, on choisit un entier d premier avec (2^m-1) ainsi, l'application $x \mapsto \mathrm{tr}_{\mathbf{F}_{2^m}/\mathbf{F}_2}(x^d)$ est une fonction booléenne équilibrée, notons $\mathcal{L}(d,m)$ son amplitude spectrale.

20.1. le cas m impair.

PROPOSITION 20.1. *Si m est impair alors l'amplitude spectrale de $\mathcal{L}(d,m)$ est supérieure ou égale à la borne quadratique. Les entiers connus qui atteignent cette borne sont listés dans la table (6).*

DÉMONSTRATION. C'est une conséquence de la borne de Sidel'nikov. □

	d
Gold [**77**]	2^k+1 $(0<k<m/2,\ (k,m)=1)$
Kasami [**102**]	$2^{2k}-2^k+1$ $(0<k<m/2,(k,m)=1)$
[**35**]	$2^{m-1}+3$

TAB. 6. Entiers d vérifiant $\mathcal{L}(d,m)=2^{(m+1)/2}$, m impair

CONJECTURE 20.1 (Niho). *Si*

$$d = \begin{cases} 2^{(m-1)/2} + 2^{(m-1)/4} - 1, & m \equiv 1 \bmod 4, \\ 2^{(m-1)/2} + 2^{(3m-1)/4} - 1, & m \equiv 3 \bmod 4 \end{cases}$$

alors $\mathcal{L}(d,m) = 2^{\frac{m+1}{2}}$

	d	cond. sur m
Lachaud & Wolfmann [**112**]	-1	
Niho [**154**]	$2^{m/2+1}-1$	$m \equiv 0 \bmod 4$
Dobbertin [**68**]	$\sum_{i=0}^{m/2} 2^{ik}$ $(0 < k < m/2,\ (k,m)=1)$	$m \equiv 0 \bmod 4$
Cusick & Dobbertin [**55**]	$2^{m/2}+2^{(m+2)/4}+1$	$m \equiv 2 \bmod 4$
Cusick & Dobbertin [**55**]	$2^{m/2}+2^{m/2-1}+1$	$m \equiv 2 \bmod 4$
Dobbertin [**68**]	$2^{m/2}+2^{m/4}+1$	$m \equiv 4 \bmod 8$

TAB. 7. Entiers d vérifiant $\mathcal{L}(d,m) = 2^{m/2+1}$, m pair

20.2. le cas m pair.

CONJECTURE 20.2 (Welch). *Si m est pair alors l'amplitude spectrale de $x \mapsto \mathrm{tr}_{\mathbf{F}_{2^m}/\mathbf{F}_2}(x^d)$ est supérieure ou égale à $2^{\frac{m+2}{2}}$.*

À une équivalence près la table (TAB. 7) liste les entiers d connus pour lesquels cette borne est atteinte. Le lecteur curieux de connaître la distribution du spectre de Fourier de ces fonctions peut consulter [**68**].

PROBLÈME 20.1. *Etudier la non-linéarité d'applications $x \mapsto \mathrm{tr}_{\mathbf{F}_{2^m}/\mathbf{F}_2}\big(P(x)\big)$ dans le cas d'un binôme.*

21. Cubiques

Alors que l'on sait tout des fonctions de degré deux, on ne sait presque rien de la non-linéarité des fonctions de cubiques. Dans [**37**] Carlet montre que le calcul du poids d'une fonction de $\mathrm{RM}(s,m)$ se ramène à celui d'une cubique à condition d'augmenter le nombre de variables. L'étude de l'amplitude spectrale minimale d'une fonction de degré 3 commence dans mon article [**117**]. Dans cet article, je montre qu'une fonction de degré 3 en 9 variables ne dépasse pas la borne quadratique.

PROPOSITION 21.1 (Hou-Langevin). *Soit $m \leq 14$, on a :*

$$R_3(m) = R_2(m) = 2^{\lceil \frac{m}{2} \rceil}$$

Cette proposition montre qu'il sera difficile de trouver une fonction de degré 3 hautement non-linéaire en dimension impaire. La formule (97) lie les moments d'ordre 4 d'une fonction de degré 3 à la taille de son noyau et de son défaut : c'est une bonne piste pour trouver une cubique hautement non-linéaire.

PROPOSITION 21.2. [**130**, $\pi\!\lambda$] *Soit f une fonction de degré 3, on a :*

$$\sum_{a \in \mathbf{F}_2^m} \widehat{f}_\chi(a)^4 = 2^{2m}\big(|\ker(f)| - 2|\mathrm{def}(f)|\big). \tag{97}$$

En particulier, si $|\ker(f)| - 2|\mathrm{def}(f)| \geq 2^{m+1}$ alors f ne dépasse pas la borne quadratique.

Notons $r(v)$ le rang de la forme symplectique associée à la fonction de quadratique $D_v f$. On montre sans difficulté que le cardinal du noyau d'une cubique f satisfait :

$$|\ker(f)| = \sum_{v \in \mathbf{F}_2^m} 2^{r(v)} \geq \begin{cases} 5.2^m - 4, & \text{si } m \text{ pair}\,; \\ 3.2^m - 2, & \text{si } m \text{ impair}. \end{cases}$$

$d \setminus m$	6	7	8	9	10
3	6	12	32	349	$\sim 10^7$
4	2	12	999	$\sim 10^{15}$	$\sim 10^{34}$

TAB. 8. Quelques valeurs de $n(s, m)$

$r.m$	1	2	3	4	5	6	7	8	9
1	0	1	2	6	12	28	56	120	240–244
2		0	1	2	6	18	40–42	84–100	171–220

TAB. 9. Rayon de recouvrement de $\mathrm{RM}(2, m)$, $1 \leq m \leq 9$.

PROBLÈME 21.1. *A la lumière des articles* [**74, 60**], *les estimations ci-dessus ne sont pas si mauvaises. Comment construire une cubique à noyau minimal ?*

Pour chaque entier $s \in [0, m]$, le groupe linéaire agit sur le code de Reed-Muller d'ordre s et donc, sur l'espace quotient $\mathrm{RM}(s, m)/\mathrm{RM}(s-1, m)$, notons $n(s, m)$ le nombre d'orbite. Quelque soit m, $n(1, m) = 2$ et $n(2, m) = [m/2] + 1$. L'explosion combinatoire du nombre $n(3, m)$ se produit pour $m = 10$, voir la table (8). La valeur de $n(3, 6)$ est 6 et non pas 5 comme le laisser penser l'article de Rothaus [**163**]. Dans son article, X.-D. Hou construit 32 représentants des cubiques de 8 variables, notés F_1, F_2 etc... À partir desquels, on peut calculer la distribution des noyaux des cubiques de 7 variables, voir [**130**]. Quelques jours de calculs suffisent pour déterminer le degré de non-linéarité des cubiques de la forme $F_i(X) + Q(X)$, en faisant varier Q dans l'espace des formes quadratiques homogènes, le facteur de travail vaut : $2^5 \times 2^{28} \times 2^{11}$. Six classes contiennent des fonctions courbes : F_1, F_2, F_3, F_5, F_7 et F_9. Par ailleurs, la cubique F_{27} se trouve à distance 88 du code du Reed-Muller du second ordre ce qui permet d'améliorer la borne inférieure du rayon de recouvrement du code de Reed-Muller de la table (9) tirée du survey [**50**].

PROPOSITION 21.3. *Le rayon de recouvrement du Reed-Muller du second ordre en* 8 *variables est supérieur ou égal à* 88.

PROBLÈME 21.2. *Déterminer un système de représentants de* $\mathrm{RM}(s, m)/\mathrm{RM}(s-1, m)$ *dans les deux cas numériquement accessibles :* $s = 3$ *et* $m = 9$, *et* $s = 4$ *et* $m = 8$.

22. Fonctions traciques

Désignons par $GR(2^\ell, m)$ l'anneau de Galois de caractéristique 2^ℓ et de degré m. Notons $q = 2^m$ le cardinal de son corps résiduel. C'est l'anneau quotient $\mathbf{Z}[X]/(f(X), 2^\ell)$, où f est un diviseur de $X^q - X$ dont la réduction modulo 2 est un polynôme primitif de degré m dans $\mathbf{F}_2[X]$. L'ensemble $T = \{0, 1, X, \ldots, X^{q-2}\}$ est une partie multiplicative de $GR(2^\ell, m)$ que l'on identifie à l'ensemble du corps $\mathbf{F}_q$. Un élément z de $GR(2^\ell, m)$ se décompose d'une et une seule façon sous la forme

$$z = x_0 + x_1 p + \cdots + x_{\ell-1} p^{\ell-1}$$

où les x_i sont des éléments de T. Le groupe des automorphismes de l'anneau $GR(2^\ell, m)$ est cyclique de cardinal m engendré par l'automorphisme de Frobenius σ :

$$\sigma(z) = x_0^p + x_1^p p + \cdots + x_{\ell-1}^p p^{\ell-1}$$

Degré des fonctions traciques									
m :j	0	1	2	3	4	5	6	7	8
6	1	2	4	6	6	6	6	6	6
7	1	2	4	7	7	5	7	5	6
8	1	2	4	8	6	7	7	7	6
9	1	2	4	8	7	9	9	8	9

TAB. 10. $\deg(t_j)$, $0 \leq j \leq 8$ et $6 \leq m \leq 9$.

Amplitudes spectrales fonctions traciques								
m :j	1	2	3	4	5	6	7	8
6	8 (8)	16 (0)	34 (2)	18 (2)	22 (2)	46 (2)	30 (2)	10 (6)
7	16 (0)	28 (4)	70 (2)	30 (2)	68 (4)	42 (2)	28 (4)	28 (0)
8	16 (16)	52 (4)	34 (2)	68 (4)	36 (0)	84 (0)	36 (0)	92 (4)
9	32 (0)	72 (0)	68 (0)	72 (0)	150 (2)	146 (2)	96 (0)	106 (2)

TAB. 11. Amplitude et (déséquilibre) de la fonction tracique t_j de m variables, pour $1 \leq j \leq 8$ et $6 \leq m \leq 9$.

à partir duquel, on définit la trace de $GR(2^\ell, m)$ par $\mathrm{Tr}(z) = \sum_{i=1}^{f} \sigma(z)$.

PROPOSITION 22.1. *L'anneau de Galois $GR(2^\ell, m)$ est un $\mathbf{Z}/2^\ell\mathbf{Z}$-module et l'application* Tr *est une forme $\mathbf{Z}/2^\ell\mathbf{Z}$-linéaire surjective. De plus, $(x, y) \mapsto \mathrm{Tr}(xy)$ est une application $\mathbf{Z}/2^\ell\mathbf{Z}$-bilinéaire non dégénérée.*

On peut écrire

$$\mathrm{Tr}(z) = t_0(z) + t_1(z)2 + \ldots + t_{\ell-1}(z)2^{\ell-1} \tag{98}$$

la restriction de t_j à T définit une fonction booléenne de m variables, c'est la j-ième *fonction tracique* . La fonction t_0 n'est rien d'autre que la trace du corps $\mathbf{F}_{2^m}$ sur $\mathbf{F}_2$: c'est une fonction de degré 1. La fonction t_1 est une fonction quadratique 2, c'est même une forme quadratique de rang maximal qui joue un rôle important [**79**] dans la description du code de Kerdock comme code $\mathbf{Z}/4\mathbf{Z}$ linéaire. On peut déterminer l'invariant de Arf de t_1, directement comme dans [**110**] ou bien en utilisant les sommes de caractères [**127**]. A l'exception de t_1, les fonctions booléennes traciques ne sont pas remarquables du point de vue de la non-linéarité. Dans la table (10), on trouvera le degré de la j-ième fonction tracique en m variables. La table (11) donne leur déséquilibre et leur amplitude spectrale.

23. Fonctions booléennes cocycliques

Pour se familiariser avec les notions cohomologiques, le lecteur peut consulter les pages d'exercices du chapitre 20 de [**115**]. Le chapitre 4 de [**20**] devrait satisfaire le lecteur curieux de faire un lien entre la cohomologie des groupes et le théorème de Wedderburn. Soit G un groupe fini et soit A un groupe abélien. On suppose que G agit sur A, et on note $g.a$ l'action de G sur a. Un élément de A s'appelle une cochaîne de degré 0. Une *cochaîne* de degré $q > 0$ est une application de G^q dans A satisfaisant la condition de covariance :

$$x.f(x_1, x_2, \ldots, x_q) = f(x.x_1, x.x_2, \ldots, x.x_q)$$

L'*opération de cobord* d envoie f, une cochaîne de degré q, sur la cochaîne df de degré $q+1$ définie par :

$$(99)\qquad \begin{aligned} df(x_1,x_2,\dots,x_{q+1}) =& x_1.f(x_2,\dots,x_{q+1}) \\ & - \sum_{j=1}^{q}(-1)^j f(x_1,\dots,x_jx_{j+1},\dots,x_{q+1}) \\ & + (-1)^{q+1}f(x_1,\dots,x_q) \end{aligned}$$

Si a est une cochaîne de degré 0 alors $da(x) = x.a - a$. On vérifie que $d\circ d = 0$. On note $B(q)$ l'ensembles des *bords* de degré q : c'est l'image par d des cochaîne de degré $q-1$. On note $Z(q)$ l'ensemble *cocycles* de degré q : c'est l'ensemble des cochaîne de degré q dont les images par d valent 0. On vérifie que $B(q)$ est un sous-groupe de $Z(q)$ et le quotient $Z(q)/B(q)$ est le q-ième *groupe de cohomologie* de G à valeurs dans A.

Un 0-cocycle est un élément de A invariant par G. Un 1-cocycle est une application de G dans A tel que :

$$f(xy) = x.f(y) + f(x)$$

c'est un *homomorphisme croisé*. Un 2-cocycle de G à valeur dans A est une application f de $G\times G$ dans A satisfaisant :

$$x.f(y,z) - f(xy,z) + f(x,yz) - f(x,y) = 0, \quad \forall x,y,z\in G.$$

Les éléments $f(x,y)$ sont des *systèmes de facteurs* . Il est normalisé si $f(1,1) = 0$, ce qui entraine $f(x,0) = f(0,x) = 0, \forall x\in G$. Une fonction booléenne f de ${\mathbf{F}_2}^{tr}$ est dite *q-cocyclique* s'il existe un groupe G de cardinal 2^t une application $x\mapsto \bar{x}$ de ${\mathbf{F}_2}^t$ dans G et un q-cocycle g tel que :

$$(100)\qquad f(x_1,x_2,\dots,x_q) = g(\bar{x}_1,\bar{x}_2,\dots,\bar{x}_q);$$

Je reconnais que cette définition est un petit peu tortueuse, mais je ne fais qu'écrire dans le contexte des fonctions booléennes, la notion de *matrices cocycliques* de K. Horadam et W. De Launey [**86**]. Par exemple, si $G = {\mathbf{F}_2}^t$ agit trivialement sur $\mathbf{F}_2$ alors l'application $f(x,y) = x.y$ est bilinéaire, et c'est un 2-cocycle :

$$f(x,y) + f(x+y,z) = f(x,y) + f(x,z) + f(y,z) = f(x,y+z) + f(y,z)$$

C'est aussi une fonction courbe. On vérifie [**86**] qu'un 2-cocycle est g est complètement déterminé par la donnée des $2^t - t - 1$ éléments $g(x,b)$, où $0 < x < b$ et b est de poids 1 ; et des $t(t-1)/2$ éléments $g(a,b)$, oú $a\le b$ sont de poids 1.

Dans le rapport [**131**], nous avons déterminé numériquement les fonctions 2-cocycliques de 4, 6 et 8 variables. La table (3) donne la non-linéarité des fonctions 2-cocycliques en 8 variables. J'ai vérifié que toutes les fonctions courbes obtenues sont des fonctions quadratiques.

PROBLÈME 23.1. *Est-ce que les fonctions 2-cocycliques courbes sont nécessairement de degré 2 ?*

PROBLÈME 23.2. *Comment déterminer tout les 3-cocycles de ${\mathbf{F}_2}^3$. Quelle est la non-linéarité des fonctions 3-cocycliques de neuf variables ?*

$A(f)$	$\Delta(f)$	Freq.	$A(f)$	$\Delta(f)$	Freq.
256	0	4	28	4	17456
20	12	48	100	4	1480
84	4	1952	108	4	3992
128	0	516	60	4	121844
112	0	260	76	4	7796
16	16	40704	116	4	260
80	0	26452	52	4	209708
32	0	498208	124	4	44
64	0	153304	44	4	1176624
56	8	110080	68	4	107356
40	8	872960	36	4	447808
48	0	394664	44	12	783

FIG. 3. Amplitude spectrale, déséquilibre et fréquence des fonctions 2-cocycliques de 8 variables.

Bibliographie

[1] In Sok Lee D. S. Kim. Gauss sums for $o^+(2n,q)$. *Acta Arithmetica*, LXXVIII.1 :75–89, 1996.

[2] D. S. Kim. Gauss sums for $o^-(2n,q)$. *Acta Arithmetica*, LXXX.4 :343–365, 1997.

[3] P. Solé. A quaternary cyclic code and a family of quadriphase sequence with low correlation properties. volume 388, 1989.

[4] Alexis R. Search for sequences with zero autocorrelation. volume 311. Springer-Verlag, 1988.

[5] Amice Y. *Les nombres p-adiques*, volume 14 of *Le mathématicien*. Presses Universitaires de France, 1978.

[6] Arasu K. T., Ma S. L. and Voss N. J. On a class of almost perfect sequences. *Journal of algebra*, 192 :641–650, 1997.

[7] Assmus E. F., Jr. The category of linear codes. *preprint*, xxx :xxx, 1998.

[8] Ax J. Zeroes of polynomials over finite fields. *American Journal of Mathematics*, 86 :256–261, 1964.

[9] B. C. Berndt and R. J. Evans and K. S. Williams. *Gauss and Jacobi sums*, volume 21. Wiley & sons, 1998.

[10] Baumert L. D., McEliece R. J. Weights of irreducible cyclic codes. *Information and Control*, 20 :158–175, 1976.

[11] Baumert L. D., Mykkelveit J. Weights distribution of some irreducible cyclic codes. *D.S.N. report*, 16 :128–131, 1973.

[12] Belevitch V. Synthesis of four-wire conference networks and related problems. volume xxx, pages 175–195, 1955.

[13] Berger T., Charpin P. Groupes d'automorphismes des codes de reed-muller q-aires. *Comptes Rendus Académie Sciences Paris*, 313 :883–886, 1991.

[14] Berlekamp E. R., McEliece R. J., Van Tilborg H. C. A. On the inherent intractability of certain coding problems. ieee *transactions on Information Theory*, 24(3) :384–386, 1978.

[15] Berlekamp E. R., Sloane N. J. A. Restrictions on the weight distributions of the reed-muller codes. *Information and Control*, 14 :442–446, 1969.

[16] Berlekamp E. R., Welch L. R. Distributions of the cosets of the $(32,6)$ reed-muller code. ieee *Transactions on Information Theory*, 13(1) :203–207, 1972.

[17] Berman S. D. On the theory of group codes. *Kibernetica*, 1 :31–39, 1967.

[18] Berndt B.C., Evans R.J. Sums of gauss, jacobi, and jacobsthal. *Journal of Number Theory*, 11 :349–398, 1979.

[19] Birch B. J. *Cyclotomic Fields and Kummer Extensions*. Academic Press, 1967.

[20] Blanchard A. *Les corps non commutatifs*, volume 9 of *Collection SUP, le mathématicien*. Presses Universitaires de France, 1972.

[21] Bonneau P. G. A. *Codes et Combinatires*. PhD thesis, université Pierre et Marie Curie, Paris VI, 1984.

[22] Boursier C. Multiplicative Characters and Design of Sequences with Good autocorrelation. *preprint*, x :x, 1999.

[23] Boztas S., Hammons R., Kumar P. V. 4-phase sequences with near-optimum correlation properties. ieee *transactions on Information Theory*, 38(3) :1101–1113, 1992.

[24] Boztas S., Kumar P. V. Binary sequences with gold-like correlation but larger linear span. ieee *trans. Info. Theory.*, 40(2), 1994.

[25] Bradley S. P., Pott A. Existence and non-existence of almost perfect autocorrelation sequences. ieee *Transactions on Information Theory*, 41(1) :301–304, 1995.

[26] Brualdi R. A.,Cai N., Pless V. S. Orphans of the first order Reed-Muller codes. ieee *Transactions on Informattion Theory*, 36 :399–401, 1990.

[27] Bruen A. , Levinger B. A theorem on permutations of a finite field. *Canadian Journal of Mathematics*, xxv(5) :1060–1065, 1973.

[28] Cahn C. R. and Stalder J. E. Bounds for correlation peaks of periodic digital sequences. volume x, pages 1262–1263, 1964.

[29] Calderbank A. R., McGuire G. Proof of a conjecture of sarwate and pursley regarding pairs of binary m-sequence. *IEEE transactions on Inf. Theory*, 41(4) :1153–1155, 1995.

[30] Calderbank A. R.,Li W.-C. W. and Poonen B. A 2-adic approach to the analysis of cyclic codes. *IEEE trans. Inf. th.*, 43(3) :977–986, 1997.

[31] Calderbank A.R., Helleseth T., Kumar P.V. An upper bound for weil exponential sums over galois rings and applications. ieee *transactions on Information Theory.*, 41(2), 1995.

[32] Calderbank R., Kantor W. M. The geometry of two-weight codes. Technical report, Bell Laboratory, 1978.

[33] Camion P. Abelian codes. Technical report, 1971.

[34] Camion P. Etude de codes binaires abélien modulaires autoduaux de petites longueurs. *Revue de Cethedec*, NS-79-2 :3–24, 1979.

[35] Canteaut A., Charpin P. et Dobbertin H. Couples de suites binaires de longueur... *CRAS*, x :x, 1999.

[36] Carlet C. *Codes de Reed-Muller, codes de Kerdock et de Preparata*. PhD thesis, xxx, 1990.

[37] Carlet C. A transformation on boolean functions, its consequences on some problems related to reed-muller codes. In *Eurocode 90*, volume 514, pages 42–50. Springer-Verlag, 1991.

[38] Carlet C. Partially bent functions. *Designs, Codes and Cryptography*, 3 :135–145, 1993.

[39] Carlet C. Generalized partial spreads. *IEEE Transactions on Information Theory*, 41 :1482–1487, 1995.

[40] Carlet C. A new generalization of bent functions to the odd case, 1997.

[41] Carlet C., Guillot Ph. A characterization of binary bent functions. *Journal of Combinatorial Theory (A)*, 76 :328–335, 1996.

[42] Carlitz L. et Uchiyama S. Bounds for exponential sums. 1956.

[43] Cassel J.W.S., Frolich A. *Algebraic Number Theory*. Academic Press, 1987.

[44] Charpin P. *Codes cycliques étendus invariants sous le groupe affine*. PhD thesis, Université de Paris VI, 1987.

[45] Charpin P. Self-dual codes which are principal ideals of the group algebra $\mathbf{F}_2[\{\mathbf{F}_{2^m}, +\}]$. *Journal of Statistical Planning and Inference*, xxx :xxx, xxx.

[46] Chung F. R. K. Diameters and eigenvalues. *Journal of the American Math. Soc.*, 2(2), 1989.

[47] Chung H., Kumar P. V. A new general construction for generalized bent functions. ieee *transactions on Information Theory*, 35(1), 1989.

[48] Claasen H. C., Goldbach R. W. A field-like property of finite rings. *Indag. Math. NS*, 3 :11–26, 1992.

[49] Cohen G. D., Karpovsky M. G., Mattson H. F. Jr, Schatz J. R. Covering radius—surveys and recent results. ieee *Transactions on Information Theory*, 31 :328–343, 1985.

[50] Cohen G., Honkala I., Litsyn S., Lobstein A. *Covering Codes*, volume 54 of *North-Holland Mathematical Library*. North-Holland, 1997.

[51] Cohn J. H. E. On the value of determinants. *xxx*, xxx(xxx), 1962.

[52] Colburn C. J., Dinitz J. H. *The CRC Handbook of Combinatorial Design*. CRC Press, 1996.

[53] Constantin J., Courteau B., Wolfmann J. Numerical experiments related to the covering radius of some Reed-Muller codes. In Lecture Notes in Computer Science, editor, *Algebraic Algorithms and Error-Correcting Codes*, volume 229, pages 69–75. 3rd International Conference AAECC, 1986.

[54] Curtis C. W., Reiner I. *Representation Theory of Finite Groups and Associative Algebras*. Wiley Classics Library. Wiley & sons, 1988.

[55] Cusick T., Dobbertin H. Some new 3-valued crosscorrelation functions of binary m-sequences. ieee *Transactions on Information Theory*, 42 :1238–1240, 1996.

[56] Delsarte P. A geometrical approach to a class of cyclic codes. *Journal of Combinatorial Theory*, 6 :340–358, 1969.

[57] Delsarte P. Weight of p-ary abelian codes. *Philips Res. Rep.*, 26(xxx) :145–153, 1971.

[58] Delsarte P. Four fundamental parameters of a code and their combinatorial signifiance. *Information and Control*, 23 :47–64, 1972.

[59] Delsarte P. Weight of linear codes and strongly regular normed spaces. *Discrete Math.*, 3 :47–77, 1972.

[60] Delsarte P., Goethals J.-M. Alternating bilinear forms over $gf(q)$. *Journal of combinatorial theory (A)*, 19 :26–50, 1975.

[61] Delsarte P., Goethals J. M. ,Mac Williams F. J. . On generalized Reed-Muller Codes and their relatives. *Information and Control*, 16 :403–443, 1970.

[62] Delsarte P., Goethals J. M., Seidel J. J. Orthogonal matrices with zero diagonal ii. *Canadian Journal of Mathematics*, xxiii(5) :816–832, 1971.

[63] Delsarte P., McEliece R.J. Zeros of functions in finite abelian group algebras. *Amer. Journal of Math.*, 98(xxx) :197–224, 226.

[64] Dieudonné J. *La géométrie des groupes classiques*. Ergebnisse der Mathematik und ihrer Grenzgebiete. Springer-Verlag, 1971.

[65] Dillon J. F. *Elementary Hadamard Difference Sets*. PhD thesis, University of Maryland, 1974.

[66] Dinitz J. H., Stinson D. R. *Contemporary Design Theory*. Wiley Interscience Publication. Wiley & sons, 1972.

[67] Dobbertin H. Construction of bent functions and balanced boolean functions with high nonlinearity. In *Workshop on cryptographic Algorithms*, volume 1008, pages 61–74. Springer-Verlag, 1995.

[68] Dobbertin H. one-to-one highly non-linear power functions on finite fields. *Applicable Algebra in Engineering, Communication and Computing*, xxx :xxx, 199x.

[69] Dwork B. On the zeta function of a hypersurface. *Publ. Math. IHES*, 12 :5–68, 1962.

[70] Dye R. H. On the arf invariant. *Journal of Algebra*, 53 :36–39, 1977.

[71] Eliahou S. and Kervaire M. Barker sequences and difference sets. *L'Enseignement Mathématique*, 38 :345–382, 1992.

[72] Gabidulin E. M. Partial classification of sequences with perfect auto-correlation and bent functions. In *IEEE Transactions on Information Theory*, page 467. IEEE International Symposium on Information Theory, 1995.

[73] Gauss C. F. *Disquisitiones Arithmeticae*, volume section VII. 1807.

[74] Goethals J.-M. Nonlinear codes and quadratic forms. *Information and Control*, 31(1) :43–75, 1976.

[75] Goethals J. M., Seidel J. J. Orthogonal matrices with zero diagonal. *Canadian Journal of Mathematics*, 19 :1001–1010, 1967.

[76] Gold R. Optimal binary sequences for spread spectrum multiplexing. *IEEE transactions on Information Theory*, 13 :154–156, 1967.

[77] Gold R. Maximal recursive sequences with 3-valued crosscorrelation functions. *IEEE transactions on Information Theory*, 14 :154–156, 1968.

[78] Hadamard J. Résolution d'une question relative aux déterminants. *Bulletin des Sciences Mathématiques*, 17(2) :241–246, 1893.

[79] Hammons A. R., Kumar P. V., & al. The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethal, and related codes. ieee *Transactions on Information Theory*, 40(2) :301–319, 1994.

[80] Hasse H. *Vorlesungen uber Zahlentheorie*. Springer-Verlag, 1964.

[81] Helleseth T. and Yang Y. On the weight hierarchy of preparata codes over Z4. *IEEE transactions on Inf. Theory*, 43(06), 1997.

[82] Helleseth T., Klove T., Mykkelveit J. On the covering radius of binary codes. *IEEE Transactions on Information Theory*, 24(5) :2, 1978.

[83] Helleseth T., Mattson H. F. On the cosets of the simplex codes. *Discrete Mathematics*, 56 :169–189, 1985.

[84] Hirschfeld J. W. S. and Storme L. The packing problem in statistics, coding theory and finite projective spaces. *Journal of Statist. Plann.Inference*, to appear.

[85] Hoholdt T., Justesen J. Sequences with perfect periodic autocorrelation. ieee *Trans. Inform. Theory*, 29(4), 1983.

[86] Horadam K, De Launey W. Generation of cocyclic Hadamard matrices. *Computational Algebra and Number Theory*, pages 279–290, 1995.

[87] Hou X.-D. On the covering radius of $r(1, m)$ into $r(3, m)$. *preprint*.

[88] Hou X. D. *On covering radius of codes.* PhD thesis, xxx, 1990.

[89] Hou X. D. Classification of cosets of the Reed-Muller code $R(m-3,m)$. *Discrete Mathematics*, 128(1–3) :203–224, 1994.

[90] Hou X. D. The covering radius of $R(1,9)$ in $R(4,9)$. *Designs, Codes and Cryptography*, 8(3) :285–292, 1995.

[91] Hou X.-D. Covering radius of the reed-muller code $r(1,7)$ — a simpler proof. *J. Combin. Theory*, 74, 1996.

[92] Hou X.-D. $gl(m,2)$ acting on $r(r,m)/r(r-1,m)$. *Discrete Mathematics*, 149 :99–122, 1996.

[93] Hou X. D. On the norm and covering radius of the first order Reed-Muller codes. 1996.

[94] Hou X.-D. New constructions of bent functions. *preprint*, xxx :xxx, 1999.

[95] Hou X.-D. On the coefficients of binary bent functions. *preprint*, xxx :xxx, 1999.

[96] Hou X.-D., Langevin Ph. Results on bent functions. *Journal of Combinatorial Theory (A)*, 80(2) :232–246, 1997.

[97] Hou X.-D., Langevin Ph. H-code and derivations. *soumis*, 1999.

[98] Hua L. K. *Introduction to number theory.* Springer-Verlag, 1982.

[99] Ipatov V. P. Ternary sequences with ideal periodic autocorrelation properties. *Radio Eng. Electron. Phys.*, 24, 1979.

[100] Ireland L., Rosen M. *A Classical Introduction to Modern Number Theory*, volume 84 of *Graduate Texts in Mathematics.* Springer-Verlag.

[101] Joly J. R. Equations et variétés algébriques sur un corps fini. *L'enseignement mathématique*, xix, fasc 1–2 :xxx, 1974.

[102] Kasami T. The weight enumerators for several classes of subcodes of the 2-nd reed-muller codes. *Information and Control*, 18 :369–394, 1971.

[103] Kasami T., Lin S., Peterson W. New generalisations or the Reed-Muller Codes, Part I : Primitive Codes. IEEE *Transactions on Informormation Theory*, 14 :xxx, 1968.

[104] Kasami T., Tokura N. On the weight structure of reed-muller codes. IEEE *Transactions on Information Theory*, 16(6) :752–759, 1970.

[105] Katz N. On a theorem of ax. *American Journal of Mathematics*, 93 :485–499, 1971.

[106] Knapp W., Schmid P. Codes with prescribed permutation group. *Journal of Algebra*, 67 :415–435, 1980.

[107] Koblitz N. *p-adic Analysis a Short Course on Recent Work*, volume 46 of *LMS Lect. Notes Series.* Cambridge University Press, 1980.

[108] Koblitz N. Jacobi sums irreducible zeta-polynomial, and cryptography. *Canadian Mathematics Bulletin*, 34 :229–235, 1991.

[109] Kumar P.V., Scholtz R.A., Welch L.R. Generalized bent functions and their properties. *Journal of Combinatorial Theory (A)*, 40 :90–107, 1985.

[110] Kuzmin A.S., Netchaev A.A. Trace-function on a galois ring in coding theory. pages 277–290.

[111] Lachaud G. Exponential sums as discrete fourier transform of invariant phase functions. In *Algebraic and Combinatorial Coding Theory (ACCT-2)*, pages 127–131, 1990.

[112] Lachaud G., Wolfmann J. Sommes de kloosterman, courbes elliptiques et codes cycliques en caractéristique 2. *Comptes rendus de l'académie des sciences*, 305 :881–883, 1987.

[113] Lamprecht E. Calculation of general gauss sums and quadratic gauss sums in finite rings. *théorie des nombres*, xxx(xxx) :561–573, 1989.

[114] Lang S. *Cyclotomic fields I and II*, volume 121 of *Graduate Texts in Mathematics.* Springer-Verlag, 1990.

[115] Lang S. *Algebra.* Addison-Wesley, 1993.

[116] Langevin Ph. `http ://www.univ-tln.fr/ langevin@univ-tln.fr`. Technical report.

[117] Langevin Ph. The covering radius of $r(1,9)$ in $r(3,9)$. In *Eurocode 90*, volume 514, pages 51–61. Springer-Verlag, 1990.

[118] Langevin Ph. On the orphans and covering radius of the reed-muller codes. In *AAECC 9*, volume 539, pages 234–240, 1991.

[119] Langevin Ph. On generalized bent functions. In *Eurocode 92*, volume 339, pages 147–157, 1992.

[120] Langevin Ph. *Rayon de recouvrement des codes de Reed-Muller affines.* PhD thesis, Université de Limoges, 1992.

[121] Langevin Ph. Almost perfect sequences. *Applicable Algebra in Engineering, Communication and Computing*, 4 :95–102, 1993.

[122] Langevin Ph. Construction of almost perfect sequences. In *Complexité, Codage, Compression Cryptographie*, volume xxx, pages 175–185, 1993.

[123] Langevin Ph. Some sequences with good autocorrelation properties. In *Finite Fields*, volume 168, pages 175–185, 1994.

[124] Langevin Ph. Regular section groups. *Finite Fields and their Applications*, 1(4) :405–412, 1995.

[125] Langevin Ph. A new class of two weight codes. In *Finite Fields and Applications*, volume 233, pages 181–187. Cambridge, university press, 1996.

[126] Langevin Ph. Calcul de certaines sommes de gauss. *Journal of Number Theory*, 62 :59–64, 1997.

[127] Langevin Ph. Sommes de gauss sur un anneau local. Technical Report RR 98-26, laboratoire I3S, 1998.

[128] Langevin Ph. Sur un théorème de Delsarte et McEliece. Technical Report RR 98-10, laboratoire I3S, 1998.

[129] Langevin Ph. Weight of abelian codes. *Designs, Codes and Cryptography*, 14(3) :239–247, 1998.

[130] Langevin Ph., Solé P. Kernels and defaults. In G. L. Mullen R. C. Mullin, editor, *Finite Fields : Theory, Applications and Algorithms*, volume 225, pages 77–87. AMS, 1998.

[131] Langevin Ph., Veron P., Zanotti J.P. Fonction booléennes équilibrés (ii). Technical report, SCSSI, 1998.

[132] Langevin Ph., Zanotti J.P. Linear codes with balanced weight distribution. *Applicable Algebra in Engineering, Communication and Computing*, 6(4-5) :299–307, 1995.

[133] Langevin Ph., Zanotti J.P. Fonction booléennes équilibrés (i). Technical report, SCSSI, 1996.

[134] Lehmer E. The quintic character of order 2 and 3. *Duke Mathematical Journal*, 18 :11–18, 1951.

[135] Leung K. H., Ling S., Ma S. L. and Tay K. B. Almost perfect sequences with $\theta = 2$. *Archiv. Math.*, 70 :128–131, 1998.

[136] Lidl R., Niederreiter H. *Finite Fields*, volume 20 of *Encyclopedia of Mathematics and its Applications*. Addison-Wesley, 1983.

[137] Liebeck M. W. The affine permutation groups of rank three. *Proceeding of the London Mathematical Society*, 54(3) :477–516, 1987.

[138] MacWilliams F. J., Seery J. The weight distributions of some minimal cyclic codes. IEEE *Transactions on Information Theory*, 27 :796–806, 1981.

[139] MacWilliams F. J., Sloane N. J. A. *The Theory of Error-Correcting Codes*, volume 16 of *Mathematical Library*. North-Holland, 1977.

[140] Maiorana J. A. A classification of the cosets of the reed-muller code $r(1,6)$. *Mathematics of Computation*, 57(195) :403–414, 1991.

[141] Mann H. B. *addition theorems...*, volume 18 of *Tracts in Mathematis Number*. Iinterscience, 1965.

[142] Martin J.P. *Codes et Suites à Racines Multiples*. PhD thesis, université de Toulon, 1994.

[143] Mbodj O. *Codes cycliques et sommes de Gauss*. PhD thesis, Université de Toulon-Var, 1997.

[144] Mbodj O. Gauss sums of index 2. *Finite Fields and their Applications*, xxx, 1998.

[145] McConnel R. Pseudo-ordered polynomials over a finite field. *acta arithmetica*, VIII :127–151, 1963.

[146] McDonald B. R. *Finite rings with identity*, volume 28 of *Pure and Applied Mathematics*. Marcel Dekker, Inc., 1974.

[147] McEliece R. J. Weight congruences for p-ary cyclic codes. *Discr. Math.*, 3 :177–192, 1972.

[148] McEliece R. J. Irreducible cyclic codes and gauss sums. *Mathematical centre tracts*, 55 :179–196, 1974.

[149] McEliece R. J., Rumsey H. C., Jr. Euler product, cyclotomy and coding. *Journal of Number Theory*, 4 :302–311, 1972.

[150] Mitani M. On the transmission of numbers in a sequential computer. National Convention of the Inst. of Elect. Engineers of Japan, 1951.

[151] Muller D. E. Application of boolean algebra to switching circuit design and to error detection. IEEE *Trans. Computers*, 3 :6–12, 1954.

[152] Mykkelveit J. J. The covering radius of the $(128, 8)$ reed-muller codes is 56. *IEEE Transactions on Information Theory*, 26(3) :359–362, 1980.

[153] Niederreiter H. Weights of cyclic codes. *Inform. and Control*, 34(2) :130–140, 1977.

[154] Niho Y. *Multi-valued cross correlation functions between two maximal linear recursive sequences.* PhD thesis, University of Southern California, 1972.

[155] Nyberg K. Constructions of bent functions and differerence sets. 1989.

[156] Onarowicz T. and Lacroix Y. Merit factors and morse sequences. *preprint*, x :x, 1998.

[157] Paley R. E. A. C. On orthogonal matrices. *Journal Math. Phys.*, 12 :311–320, 1933.

[158] Patterson N. J., Wiedemann D. H. The covering radius of the $(1, 15)$ Reed-Muller code is at least 16276. *IEEE Transactions on Information Theory*, 29 :354–356, 1983.

[159] Peterson W. W., Weldon E. J. *Error-Correcting Codes.* The M.I.T. Press, 1972.

[160] Pless V. Power moment identities on weight distribution in error correcting codes. *Information and Control*, 6 :147–152, 1963.

[161] Pursley M. B., Sarwate D. V. Cross correlation properties of pseudo-random and related sequences. *Proc. IEEE*, 68 :593–619, 1980.

[162] Reed I. S. A class of multiple-error-correcting codes and the decoding scheme. IEEE *Transactions on Information Theory*, 4 :38–49, 1954.

[163] Rothaus O. S. On bent functions. *Journal of Combinatorial Theory (A)*, 20 :300–305, 1976.

[164] Samuel P. *Théorie Algébrique des Nombres.* Hermann, 1971.

[165] Schmidt B. Cyclotomic integers and finite geometry. *preprint*, x(x) :x, 1998.

[166] Schmidt W. M. *Equations over Finite Fields. An Elementary Approach*, volume 536 of *Lecture Notes in Mathematics.* Springer-Verlag, 1976.

[167] Seberry J., X.-Zhang M., Zheng Y. Nonlinearly balanced boolean functions and their propagation characteristics. In *CRYPTO'93*, pages 49–60, 1993.

[168] Sedgewick R. *Algorithmes en Langage C*, volume xxx of *IIA*. Addison-Wesley Europe, 1991.

[169] Segal R., Ward R. L. Weight distributions of some irreducible cyclic codes. *Mathematics of Computation*, 46(173) :341–354, 1986.

[170] Serre J.-P. Endomorphismes complètement continus des espaces de banach p-adique. *Publ. Math. IHES*, 12, 1962.

[171] Serre J.-P. *Corps locaux*, volume 1296 of *Actualités Scientifiques et Industrielles.* Hermann, 1968.

[172] Serre J.-P. *Cours d'arithmétique*, volume 2 of *Le mathématicien.* PUF, 1977.

[173] Serre J.-P. *Représentations linéaires des groupes finis.* Hermann, troisième edition, 1978.

[174] Shanon C. E. A mathematical theory of communication. *The Bell system technical journal*, xxvii(3) :379–656, 1948.

[175] Sidel'Nikov V. M. On the mutual correlation of sequences. *Soviet Math. Dokl.*, 12 :197–201, 1971.

[176] Stichtenoth H. *Algebraic function fields and codes.* Universitext. Springer-Verlag, 1993.

[177] Stickelberger J. Uber eine verallgemeinerung der kreistheilung. *Math. Ann.*, 37 :321–367, 1890.

[178] Storer J. and Turyn R. on binary sequences. *Proc. Amer. Math. Soc.*, 12 :394–399, 1961.

[179] Taylor D. E. *The Geometry of the classical groups*, volume 9 of *Sigma Series in Pure Mathematics.* Heldermann Verlag, 1992.

[180] Tietavaïnen A. Covering radius and dual distance. *Design, Codes and Cryptography*, 1 :31–46, 1991.

[181] Turyn R. Characters sums and difference sets. *Pacific Journal of Mathematics*, 15 :319–346, 1965.

[182] Turyn R. Sequences with small correlation. In H.B. Mann Editor, editor, *Error Correcting*, pages 195–228. Wiley, 1968.

[183] Van der Vlugt M. Hasse-davenport curves, gauss sums and weight distributions of irreducible cyclic codes. *Journal of Number Theory*, 55(2) :145–159, 1995.

[184] Van Lint J. H. *Introduction to coding theory*, volume 86 of *Graduate Texts in Mathematics.* Springer-Verlag, 1992.

[185] Vardy A. The intractability of computing the minimum distance of a code. IEEE *Transactions on Information Theory*, xx(xx) :xx, 1998.

[186] Wan D. An elementary proof of a theorem of katz. *American Journal of Mathematics*, 111 :1–8, 1989.

[187] Ward H. N. Combinatorial polarization. *Discrete Math.*, 26 :185–197, 1979.

[188] Warusfel A. *Structures algébriques finies.* Classiques Hachette, xxx.

[189] Washington L. C. *Introduction to cyclotomic fields*, volume 83 of *Graduate Text in Mathematics*. Springer-Verlag, 1980.

[190] Weil A. La cyclotomie jadis et naguère.

[191] Weil A. *Basic Number Theory*, volume 144 of *Die Grundlehren der mathematischen Wissensschaften in Einzeldarstellungen*. Springer-Verlag, 1974.

[192] Welch L. R. Lower bounds on the maximum cross correlation of signals. *IEEE transactions on Information Theory*, 20(3) :397–399, 1974.

[193] Wolfmann. Almost perfect auto-correlation sequences. IEEE *transactions on Information theory*, 38(4) :xxx, 1992.

[194] Wolfmann J. Codes projectifs deux poids, "caps" complets et ensembles de différences. *Journal of Combinatorial Theory (A)*, 23 :209–222, 1977.

[195] Wolfmann J. New bounds on cyclic codes from algebraic curves. *Lecture Notes in Computer Science*, 388 :47–62, 1989.

[196] Wood J. Duality for modules over finite rings and applications to coding theory. *preprint*.

[197] Wood J. Extensions theorems for linear codes over finite rings. In H. F. Mattson T. Mora, editor, *Applied Algebra, Algebraic Algorithms and Error Correcting Codes*, volume 1255, pages 329–340. Springer-Verlag, 1997.

[198] Wood J. Weight functions over finite rings. In G. L. Mullen R. C. Mullin, editor, *Finite Fields : Theory, Applications and Algorithms*, volume 225, pages 231–243. AMS, 1998.

[199] Zanotti J.-P. *Codes à Distribution de Poids Équilibrée*. PhD thesis, Université de Toulon-Var, 1995.

[200] Zanotti J.-P. Automorphism groups of bwd codes. *Journal of Combinatorial Theory (A)*, 78(2) :303–308, 1997.

Index

Notations