Université de Montréal

Dénombrement des polynômes irréductibles unitaires dans les corps finis avec différentes contraintes sur les coefficients

par

Olivier Larocque

Département de mathématiques et de statistique
Faculté des arts et des sciences

Mémoire présenté à la Faculté des études supérieures
en vue de l'obtention du grade de
Maître ès sciences (M.Sc.)
en Mathématique

septembre 2014

Université de Montréal
Faculté des études supérieures

Ce mémoire intitulé

Dénombrement des polynômes irréductibles unitaires dans les corps finis avec différentes contraintes sur les coefficients

présenté par

Olivier Larocque

a été évalué par un jury composé des personnes suivantes :

Dimitris Koukoulopoulos
(président-rapporteur)

Matilde Lalín
(directeur de recherche)

Andrew Granville
(membre du jury)

Mémoire accepté le:
12 septembre 2014

SOMMAIRE

Le but de ce mémoire est de dénombrer les polynômes irréductibles unitaires dans les corps finis avec certaines conditions sur les coefficients. Notre première condition sera de fixer la trace du polynôme. Par la suite, nous choisirons la cotrace lorsque la trace sera déjà fixée à zéro. Finalement, nous discuterons du cas où la trace et le terme constant sont fixés en même temps.

Mots clés : polynôme irréductible, corps fini, dénombrement, trace, cotrace

SUMMARY

The objective of this thesis is to count the monic irreducible polynomial over finite field with some conditions related to coefficient. First, we will determine the trace of the polynomial. Thereafter, we will elect the cotrace when the trace is already fixed to zero. Finally, we will discuss the case where the trace and the constant term are fixed at the same time

Keywords : irreducible polynomial, finite field, counting, trace, cotrace

TABLE DES MATIÈRES

LISTE DES TABLEAUX

REMERCIEMENTS

Tous d'abord, merci à Matilde qui malgré la naissance de son petit garçon a trouvé le temps de travailler avec moi sur ce mémoire. Je voudrais aussi remercier mes parents qui m'ont offert l'hospitalité me permettant ainsi de me concentrer pleinement sur ce travail. Avec mes différentes responsabilités, j'ai été très occupé dans les derniers temps de préparation de ce mémoire. Je voudrais te dire merci à toi, Caroline, de m'avoir soutenu dans ce travail malgré le peu de temps que j'ai pu te consacrer au courant des derniers mois.

INTRODUCTION

Prenons un corps fini $\mathbb{F}_q$ tel que $q = p^k$ où p est un nombre premier et k un entier positif. Considérons $f(x) \in \mathbb{F}_q[x]$ un polynôme unitaire de degré n tel que

$$f(x) = x^n + a_1 x^{n-1} + \cdots + a_k x^{n-k} + \cdots + a_n. \tag{0.0.1}$$

En imposant aucune condition sur les coefficients, nous connaissons déjà le nombre de polynômes irréductibles unitaires .

Proposition. *Si* $N(n, q)$ *est le nombre de polynômes irréductibles sur* $\mathbb{F}_q$. *On a que*

$$N(n, q) = \frac{1}{n} \sum_{d|n} \mu(d) q^{n/d}.$$

Suite à ce résultat, une question des plus naturelles serait de trouver une formule lorsque nous imposons quelques conditions. En fixant ce qu'il appelle le cycle de factorisation, Cohen**[4]** a justement été en mesure de découvrir une formule asymptotique. Résumons le résultat de Cohen. On définit λ le cycle de factorisation tel que $\lambda = (d_1, d_2, \ldots, d_n)$ où les d_j sont le nombre de facteurs irréductibles de degré j d'un polynômes de degré n. Si on pose $Q(n, q)$ l'ensemble des polynômes de degré n pas nécessairement unitaire sur $\mathbb{F}_q$, on peut s'intéresser à $T_\lambda(Q(n, q))$ comme étant le nombre d'éléments de $Q(n, q)$ qui ont comme cycle de factorisation λ. Notons que le cas où $\lambda = (0, 0, \ldots, 1)$ correspond au dénombrement des polynômes irréductibles sur $Q(n, q)$. De ces définitions, Cohen a montré que

Théorème.

$$T_\lambda(Q(n, q)) = T(\lambda)|Q(n, q)| + O(q^{n+\frac{1}{2}})$$

où $T(\lambda)$ *est la proportion du nombre d'éléments dans le groupe* S_n *qui ont comme cycle* λ.

Également, Hayes **[8]** a montré, en se basant sur le travail de Artin **[1]**, que certains ensembles A dans $Q(n, q)$ ont leurs polynômes irréductibles distribués de telle sorte que $T_\lambda(A)/|A|$ est environ égal à $T(\lambda)$. Par exemple, considérons que A est l'ensemble des polynômes unitaires qui ont les s premiers et

les t derniers coefficients fixés. De plus, en imposant le cycle de factorisation à $\lambda = (0, 0, \ldots, 1)$, on déduit que $T(\lambda) = 1/n$. Ainsi, pour un certain c tel que $1/2 \leq c < 1$, on peut montrer que

$$T_n(A) = \frac{q^n}{n(q-1)q^{s+t-1}} + O(\frac{q^{nc}}{n}).$$

Ce résultat s'applique dans des contextes très généraux. Évidement, si nous prenons des conditions plus fortes, nous pourrons démontrer des résultats beaucoup plus précis. Justement, dans ce mémoire, nous allons dénombrer de manière exacte le nombre de polynômes irréductibles sur $\mathbb{F}_q$ en imposant un ou deux coefficients. En premier lieu, nous étudierons une méthode développée par Yucas pour le cas où a_1 est fixé . En posant que $N_{a_1}(n, q)$ est le nombre de polynômes unitaires dans $\mathbb{F}_q[x]$ de degré n avec a_1 fixé , nous montrerons que

Théorème. *Si* $a_1 \in \mathbb{F}_q^\star$, $n = p^r m$ *et* $p \nmid m$, *nous avons que*

$$N_{a_1}(n, q) = \frac{1}{qn} \sum_{s|m} \mu(s) q^{n/s}.$$

Dans un second temps, nous étudierons un article de Kuz'min dans lequel il réussit à dénombrer le nombre de polynômes irréductibles de la forme (0.0.1) avec $a_1 = 0$ et a_2 fixé. Pour énoncer son résultat, nous devons d'abord faire quelques définitions. Commençons par poser que

$$\left(\frac{a}{q}\right) = \begin{cases} 1 & \text{si } a \text{ est un carré dans } \mathbb{F}_q^\star, \\ -1 & \text{si } a \text{ n'est pas un carré dans } \mathbb{F}_q^\star, \\ 0 & \text{si } a = 0\,. \end{cases}$$

Ensuite, si $p \nmid n$ posons G_n tel que

$$G_n(a) = \begin{cases} q^{n-2} - \left(\frac{(-1)^{m-1} m a}{q}\right) q^{m-1} & n = 2m, \\ q^{n-2} - \left(\frac{(-1)^m n}{q}\right) q^{m-1} & n = 2m+1, \end{cases}$$

et que si $p|n$, posons G_n tel que

$$G_n(a) = \begin{cases} q^{n-2} - \left(\frac{(-1)^m}{q}\right) q^{m-1}. & n = 2m, \\ \\ q^{n-2} + \left(\frac{2a(-1)^m}{q}\right) q^m & n = 2m+1. \end{cases}$$

Avec cette notation, Kuz'min a réussi à montrer que

$$H_n(a_2) = \frac{1}{n} \sum_{\substack{d|n \\ p\nmid d}} \mu(d) G_{n/d}(-a_2/d). \tag{0.0.2}$$

où $H_n(a_2)$ est le nombre de polynômes irréductibles de la forme (0.0.1) avec $a_1 = 0$ et a_2 fixé. La preuve de cette dernière équation est le résultat principal de ce mémoire. Pour parvenir à cette démonstration, nous devrons d'abord établir plusieurs résultats importants sur les formes quadratiques dans les corps finis. Ensuite, lorsque nous aurons montré 0.0.2, nous pourrons généraliser ce résultat pour n'importe quel a_1 et a_2 fixés.

Finalement, nous étudierons un résultat de Carlitz qui dénombre les polynômes irréductibles de la forme (0.0.1) avec a_1 et a_n fixés. Pour y arriver, nous utiliserons une approche très connue en théorie analytique des nombres soit : les fonctions L. Grâce à cette théorie, nous pourrons également montrer la preuve que Kuz'min avait lui-même trouvée pour démontrer le théorème (0.0.2).

STRATÉGIE

Dans ce chapitre, nous donnerons les grandes lignes qui permettront de démontrer les théorèmes importants de ce mémoire.

0.1. STRATÉGIE POUR a_1 FIXÉ

Dans la première section du mémoire, nous allons montrer un résultat bien connu. Si nous posons que $N_{a_1}(n, q)$ est le nombre de polynômes irréductibles de degré n dans $\mathbb{F}_q$ de la forme (0.0.1) avec a_1 fixé, nous montrons avec $n = p^r m$ et $p \nmid m$ que

$$N_{a_1}(n, q) = \frac{1}{qn} \sum_{s|m} \mu(s) q^{n/s},$$

pour $a_1 \neq 0$. Notons que le cas où $a_1 = 0$ est un corollaire direct de la dernière équation. Ainsi, nous verrons que

$$N_0(n, q) = \frac{1}{qn} \sum_{d|m} \mu(d) q^{n/d} - \frac{\epsilon}{n} \sum_{d|m} \mu(d) q^{n/(dp)},$$

avec $\epsilon = 0$ si $r = 0$ et $\epsilon = 1$ si $r > 0$.

Pour montrer ce théorème dans le cas $a_1 \neq 0$, nous considérerons $B_{n,a_1}(x)$ le produit de tous les polynômes unitaires irréductibles sur $\mathbb{F}_q[X]$ dont le degré divise n et dont a_1 est fixé. Ainsi, par définition de $B_{n,a_1}(x)$ et de $N_{a_1}(n, q)$, on peut constater que

$$\deg(B_{n,a_1}(x)) = \sum_{d|n} d N_{a_1}(d, q).$$

En factorisant $B_{n,a_1}(x)$ d'une façon bien précise, nous serons en mesure de calculer $\deg(B_{n,a_1}(x))$. Par la suite, il nous suffira d'utiliser l'inversion de Mobius pour montrer notre résultat.

Bien entendu, il s'agit d'un résultat connu dans la littérature. Pourtant, il nous

sera particulièrement important d'avoir ce théorème pour la suite de ce mémoire. Voyons pourquoi. Un peu plus loin, nous allons donner une nouvelle preuve pour compter le nombre de polynômes irréductibles de la forme (0.0.1) avec $a_1 = 0$ et a_2 fixé. Pour arriver à généraliser ce dénombrement à tous a_1 et a_2 fixés, nous aurons justement besoin de bien connaître le résultat $N_{a_1}(n, q)$.

0.2. Stratégie pour $a_1 = 0$ et a_2 fixé

Comme nous l'avons précédemment mentionner dans l'introduction, le but de ce mémoire est de démontrer le nombre de polynômes irréductibles de la forme (0.0.1) avec $a_1 = 0$ et a_2 fixé. Si nous notons que cette quantité est $H_n(a_2)$, nous montrerons pour $a_2 \neq 0$ que

$$H_n(a_2) = \frac{1}{n} \sum_{\substack{d|n \\ p \nmid d}} \mu(d) G_{n/d}(-a_2/d), \tag{0.2.1}$$

avec G_n défini comme dans l'introduction. Pour ce faire, nous devrons montrer que

$$\sum_{d|n} d H_{n,d}(a_2) = q^{n-2} + (-1)^n (q^{n-2} - Q_{n-1}(-a_2)), \tag{0.2.2}$$

où $H_{n,d}(a_2)$ est le nombre de polynômes unitaires irréductibles $g(x)$ de degré d tel que

$$(g(x))^m = x^n + a_2 x^{n-2} + \cdots + a_k x^{n-k} + \cdots + a_n$$

avec $n = dm$ et où $Q_{n-1}(-a_2)$ est le nombre de solutions de la forme quadratique

$$\sum_{i=1}^{n-1} x_i^2 + \sum_{1 \leq i < j \leq n-1} x_i x_j = a_2. \tag{0.2.3}$$

L'équation (0.2.2) est la relation que nous allons étudier pour montrer l'égalité (0.2.1). Avant de s'y attaquer, nous commencerons par étudier un des termes qui la compose ; c'est a dire $Q_{n-1}(-a_2)$. Pour évaluer $Q_{n-1}(-a_2)$, nous devrons dénombrer le nombre de solutions de n'importe quelle forme quadratique de la forme

$$x^t M x = a \tag{0.2.4}$$

où M est une matrice symétrique $n \times n$ avec des valeurs de $\mathbb{F}_q$ comme entrées et $x \in \mathbb{F}_q^n$. Remarquons que l'on peut facilement écrire les formes quadratiques qui correspondent à $Q_{n-1}(-a_2)$ dans la notation (0.2.4) en prenant une matrice $(n-1) \times (n-1)$ avec des 1 sur la diagonal et des $1/2$ ailleurs. Si nous notons $K_d(a)$ le nombre de solutions de la forme (0.2.4), nous montrerons

que

$$K_d(a) = \begin{cases} q^{2m-1} - l(a)\left(\frac{\det(M)(-1)^m}{q}\right) q^{m-1} & \text{si } d = 2m \\ q^{2m} + \left(\frac{a\det(M)(-1)^m}{q}\right) q^m & \text{si } d = 2m+1 \text{ et } q \text{ est impair} \\ q^{2m} & \text{si } d = 2m+1 \text{ et } q \text{ est pair} \end{cases}$$

où

$$l(a) = \begin{cases} 1 & \text{si } a \neq 0, \\ 1-q & \text{si } a = 0. \end{cases}$$

Lorsque nous aurons montré ce résultat et que nous le combinerons avec (0.2.2), nous trouverons directement (0.2.1).

0.2.0.1. *Stratégie pour calculer* $K_d(a)$

Pour arriver à calculer $K_d(a)$ pour une forme quadratique Q tel que $Q(w) = a$, il nous suffira d'évaluer la fonction suivante pour $y = a$:

$$\nu_Q(y) := \#\{w \in V | Q(w) = y\}.$$

Pour ce faire, nous allons calculer $\gamma_Q(y)$ la transformée de Fourier de $\nu_Q(y)$ et la double transformée de Fourier de $\nu_Q(y)$. Ainsi, en considérant $\tau(x) = \sum_{s=0}^{d-1} x^{q^s}$ et $\psi(x) = e^{2\pi i \tau(x)/p}$, nous aurons respectivement que

$$\gamma_Q(y) = \sum_{x \in \mathbb{F}_q} \nu_Q(x)\psi(-xy) \tag{0.2.5}$$

$$\nu_Q(y) = \frac{1}{q} \sum_{x \in \mathbb{F}_q} \gamma_Q(x)\psi(xy) \tag{0.2.6}$$

En plus, si nous avons deux formes quadratiques Q_1 et Q_2 tel que $Q_1 + Q_2 = Q$, nous montrerons que

$$\gamma_{Q_1}(y)\gamma_{Q_2}(y) = \gamma_Q(y) \tag{0.2.7}$$

L'idée générale sera donc de calculer $\gamma_Q(y)$ pour des formes quadratiques simples et ensuite, utiliser (0.2.6) et (0.2.7) afin de trouver des $\nu_Q(y)$ plus complexes. Pour ce faire, nous allons montrer que toutes formes quadratiques peuvent s'écrire comme des sommes directes de formes quadratiques de dimension 1 ou 2. En plus, nous verrons qu'il existe seulement trois formes quadratiques ayant ces dimensions. Nous aurons donc que trois $\gamma_Q(y)$ à calculer pour généraliser $\nu_Q(y)$ à toutes formes quadratiques.

0.2.0.2. *Stratégie pour montrer l'égalité* (0.2.2)

Pour montrer l'égalité (0.2.2), nous allons utiliser des méthodes combinatoires. Tout d'abord, nous devrons considérer le nombre de polynômes qui ont certains types de factorisation. Par exemple, lorsque que nous écrirons $X_{(2,1^3)}(a)$, nous voudrons parler du nombre de polynômes de la forme (0.0.1) avec $a_1 = 0$ et $a_2 = a$ qui ont au moins un facteur de degré 2 et au moins trois facteurs différents de degré 1 dans leur factorisation. De ces considérations, on peut remarquer que

$$\sum_{e_1+\cdots+e_k=n} \frac{n!}{e_1!\cdots e_k!} X_{(1^{e_1},\ldots,1^{e_k})}(a) = Q_{n-1}(a).$$

Ainsi,

$$\sum_{d|n} dH_{n,d}(a) = q^{n-2} + (-1)^n(q^{n-2} - Q_{n-1}(-a))$$

peut se transformer en

$$\sum_{d|n} dX_{(d^{n/d})}(a) = q^{n-2} + (-1)^n \left(q^{n-2} - \sum_{e_1+\cdots+e_k=n-1} \frac{n!}{e_1!\cdots e_k!} X_{(1^{e_1},\ldots,1^{e_k})}(a) \right) \tag{0.2.8}$$

Ainsi, en considérant un certain nombre d'équations qui dépendent des $X_{(\nu)}$ et en les combinant d'une façon bien précise, nous pourrons arriver à l'équation (0.2.8). Pour ce faire, nous engendrerons une famille d'égalités que nous dénoterons comme $\mathcal{E}_w$. Ces égalités feront des relations entre les $X_\nu(a)$ (les inconnus que nous voulons trouver) et les H_i(les nombres de polynômes irréductibles sans condition sur les coefficients). Nous arriverons aux équations du type $\mathcal{E}_w$ en considérant tous les polynômes avec les premiers coefficients 0 et a qui sont divisibles par un polynôme avec un type de factorisation déterminé w. Chaque type de factorisation w de degré au plus $n-2$ donnera une équation différente $\mathcal{E}_w$. Ensuite, nous prendrons quelques combinaisons particulières de ces équations que nous appellerons A, B et C. À l'aide de quelques résultats combinatoires auxiliaires, nous démontrerons que $A + B + C$ donne l'équation (0.2.8). Finalement, nous ajouterons des exemples particuliers pour illustrer notre preuve.

0.3. STRATÉGIE POUR a_1 ET a_n FIXÉS

Dans cette section, nous donnerons les idées pour montrer que le nombre de polynômes irréductibles de la forme (0.0.1) pour a_1 et a_n fixés est

$$\frac{q^n}{nq(q-1)} + O(q^{n/2}) \tag{0.3.1}$$

L'idée de cette démonstration passe par la définition de deux caractères. D'abord posons

$$\lambda(a_1) = e^{2\pi i\tau(ba_1)/p},$$

où τ est défini comme $\tau(x) = \sum_{s=0}^{d-1} x^{q^s}$ et $b \in \mathbb{F}_q$. Ensuite pour ζ une racine primitive de (0.0.1) et pour r tel que $a_n = \zeta^r$, définissons un caractère multiplicatif pour l'élément a_n :

$$\chi(a_n) = \chi(\zeta^r) = e^{2\pi icr/(q-1)},$$

où $c \in \mathbb{F}_q$. En posant M les polynômes de la forme (0.0.1) et en définissant

$$L(s,\lambda,\chi) = \sum_M \lambda(M)\chi(M)|M|^{-s} \qquad \text{où } |M| = q^{\deg(M)} \text{ et Re(s)>1,}$$

on peut faire quelques manipulations pour arriver à

$$L(s,\lambda,\chi) = \prod_P (1-\lambda(P)\chi(P)|P|^{-s})^{-1},$$

où P sont les polynômes irréductibles unitaires de $\mathbb{F}_q[x]$. En prenant le log de chaque côté de cette équation, nous avons que

$$\log(L(s,\lambda,\chi)) = \sum_P \sum_{r=1}^{\infty} \frac{1}{r}\lambda(P^r)\chi(P^r)|P|^{-rs}, \tag{0.3.2}$$

Dans (0.3.2), nous diviserons la partie de droite en deux sommes distinctes. La première somme contiendra les polynômes P' tel que $(P')^r$ possède les coefficients $a_1 = a$ et $a_n = \ell$ où $a, \ell \in \mathbb{F}_q$ et la deuxième contiendra tous les autres polynômes. De cette façon, nous serons en mesure de faire apparaître et d'isoler $\sum_{P',r} \frac{1}{r}|P'|^{-rs}$. En posant $\mu(n,r,a,\ell)$ le nombre de polynômes P' de degré n/r tel que $(P')^r$ possède les coefficients $a_1 = a$ et $a_n = \ell$, on peut voir que

$$\sum_{P',r} \frac{1}{r}|P'|^{-rs} = \sum_{n=1}^{\infty} \sum_{r|n} \frac{1}{r}\,\mu(n,r,a,\ell)q^{-nr}.$$

En isolant $\mu(n,1,a,\ell)$, on montre la relation (0.3.1).

0.3.1. Stratégie pour a_1 et $sgn(a_n)$ fixés

En fixant a_1 et sachant si a_n est un carré ou non, nous pourrons montrer un résultat exacte. Pour ce faire, posons que

$$sgn(x) = \begin{cases} 0 & \text{si } x = 0, \\ 1 & \text{si } x \text{ est un carré dans } \mathbb{F}_q^\star, \\ -1 & \text{si } x \text{ n'est pas un carré dans } \mathbb{F}_q^\star, \end{cases}$$

Remarque 0.1. On peut voir que cette notation est équivalente au symbole $\left(\frac{x}{q}\right)$. Cependant, il est plus convivial de l'utiliser ici avec la forme $sgn(x)$.

De plus, posons $\xi(n, r, a, 1)$ est le nombre de polynômes irréductibles $\overline{P}$ de degré n/r tel que $\overline{P}^r$ a comme coefficient $a_1 = a$ et que $a_n = \ell$ un carré. Notons aussi $\xi(n, r, a, -1)$ de la même façon sauf que $a_n = \ell$ n'est pas un carré. Alors si n est pair, nous avons

$$\sum_{r|n} \frac{\xi(n, r, a, sgn(\ell))}{r} = \begin{cases} \frac{1}{2n}(q^{n-1} - 1 - q^{(n/2-1)} sgn((-1)^{n/2}\ell)(q-1)) & \text{si } a = 0, \\ \frac{1}{2n}(q^{n-1} + q^{(n/2-1)} sgn((-1)^{n/2}\ell)) & \text{si } a \neq 0, \end{cases}$$

et si n est impair, nous arrivons à

$$\sum_{r|n} \frac{\xi(n, r, a, sgn(\ell))}{r} = \begin{cases} \frac{1}{2n}(q^{n-1} - 1) & \text{si } a = 0, \\ \frac{1}{2n}(q^{n-1} + sgn((-1)^{(n-1)/2}\ell a) q^{(n-1)/2}) & \text{si } a \neq 0, \end{cases}$$

Pour montrer ceci, il faut utiliser les mêmes idées que nous avons développées au précédent théorème. Seulement, au lieu de prendre le caractère $X(a_n^c)$, nous allons utiliser le caractère

$$\bar{\chi}_m(a) = sgn(a^m).$$

Nous terminerons ce mémoire en utilisant les mêmes idées que nous venons de développer pour montrer la preuve originale que Kuz'min avait utilisée pour montrer (0.2.1).

Chapitre 1

THÉORIE DE GALOIS

Avant de commencer, nous ferons un petit rappel sur quelques éléments de la théorie de Galois.

Proposition 1.1. $x^d - 1 | x^n - 1$ *si et seulement si* $d|n$.

DÉMONSTRATION. On peut récrire $n = da + r$ avec $a \in \mathbb{F}_{q^n}$ et r entre 0 et $d-1$. Alors

$$\begin{aligned} x^n - 1 &= x^{da+r} - 1 \\ &= x^{da}x^r - x^r + x^r - 1 \\ &= x^r(x^{da} - 1) + (x^r - 1) \\ &= x^r(x^d - 1)(x^{d(a-1)} + x^{d(a-2)} + \cdots + x + 1) + (x^r - 1) \end{aligned}$$

Si $d|n$, on a que $r = 0$. Si $x^d - 1 | x^n - 1$, puisque $r < d$, r doit être égal à zéro. □

Proposition 1.2. *Pour un corps de caractéristique* p *et pour* k *un entier tel que* $q = p^k$. *Nous pouvons déduire l'égalité suivante :*

$$x^q - x = \prod_{\gamma \in \mathbb{F}_q} (x - \gamma).$$

DÉMONSTRATION.
Puisque $a^q = a$ pour $a \in \mathbb{F}_q$, tous les éléments de $\mathbb{F}_q$ satisfont $x^q - x = 0$. Puisque le polynôme a au plus q racines, le résultat est montré. □

Proposition 1.3. $\mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^n}$ *si est seulement si* $d|n$.

DÉMONSTRATION.
$\Rightarrow$ Puisque $\mathbb{F}_p \subseteq \mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^n}$, on a que

$$[\mathbb{F}_{p^n} : \mathbb{F}_p] = [\mathbb{F}_{p^n} : \mathbb{F}_{p^d}][\mathbb{F}_{p^d} : \mathbb{F}_p],$$

$$n = [\mathbb{F}_{p^n} : \mathbb{F}_{p^d}]d.$$

$\Leftarrow$ Si $d|n$, par la proposition (1.1), on sait que $p^d - 1|p^n - 1$ et encore par la même proposition que $x^{p^d-1} - 1|x^{p^n-1} - 1$. En autre, on a que $x^{p^d} - x|x^{p^n} - x$. Par la proposition (1.2), on déduit que $\mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^n}$. □

Proposition 1.4. *Si* $p(x)$ *est un polynôme irréductible de degré* d *dans* $\mathbb{F}_p$ *alors,* $p(x)|x^{p^k} - x$ *si et seulement si* $d|k$.

DÉMONSTRATION.
Soit α une racine de $p(x)$ dans la fermeture algébrique de $\mathbb{F}_p$. Puisque $[\mathbb{F}_p(\alpha) : \mathbb{F}_p] = d$, on a que $\mathbb{F}_p(\alpha) = \mathbb{F}_{p^d}$. Par la proposition (1.3), $\mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^k}$ si et seulement si $d|k$. Ainsi, α est dans $\mathbb{F}_{p^k}$ si et seulement si $d|k$.

□

Les différentes preuves ont été réalisées avec $\mathbb{F}_p$. Cependant, en changeant p pour q et avec quelques modifications mineures, toutes les démonstrations restent vraies pour $\mathbb{F}_q$.

Chapitre 2

FORMULES FIXANT UN COEFFICIENT

2.0.2. Définition et stratégie

Nous commencerons ce mémoire par un résultat de Carlitz, seulement la méthode provient d'un article de Yucas **[12]**. Considérons $f(x) \in \mathbb{F}_q[x]$ où $q = p^k$ est défini comme suit

$$f(x) = x^n - \gamma x^{n-1} + a_1 x^{n-2} + \cdots + a_{n-1}. \tag{2.0.3}$$

Le but de cette section est de donner le nombre de polynômes unitaires irréductibles pour un γ établi.

Définition 2.1. Le coefficient γ du terme x^{n-1} porte le nom de trace.

Définition 2.2. Notons $T_\gamma(n, q)$ l'ensemble des polynômes irréductibles de la forme (2.0.3) avec γ fixé. Prenons aussi $N_\gamma(n, q)$ le nombre d'éléments de $T_\gamma(n, q)$.

Voici le théorème que nous allons démontrer dans cette section.

Théorème 2.3. *Si γ n'est pas nul et $n = p^r m$ avec $p \nmid m$, nous avons alors :*

$$N_\gamma(n, q) = \frac{1}{qn} \sum_{s|m} \mu(s) q^{n/s}.$$

Pour nous donner un peu d'intuition sur ce théorème, nous allons montrer que la valeur de γ n'influence pas la valeur de $N_\gamma(n, q)$ sauf pour le cas où $\gamma = 0$.

Lemme 2.4. *Si $\gamma, \delta \in \mathbb{F}_q^\star$, on a que*

$$N_\gamma(n, q) = N_\delta(n, q)$$

DÉMONSTRATION. Considérons l'application $\kappa : T_\gamma(n, q) \to T_\delta(n, q)$:

$$\kappa(f(x)) = \left(\frac{\delta}{\gamma}\right)^n f\left(\frac{\gamma}{\delta} x\right).$$

Montrons simplement que l'application est bijective.
Définissons $\kappa^{-1} : T_\delta(n, q) \to T_\gamma(n, q)$:

$$\kappa^{-1}(f(x)) = \left(\frac{\gamma}{\delta}\right)^n f\left(\frac{\delta}{\gamma}x\right)$$

Puisque $\kappa(\kappa^{-1}(f(x))) = f(x)$ pour tous $f(x) \in T_\delta(n, q)$ et que $\kappa^{-1}(\kappa(g(x))) = g(x)$ pour tous $g(x) \in T_\gamma(n, q)$, la fonction κ est inversible et donc bijective. □

Remarque 2.5. Suite à ce résultat, on constate aisément que (2.3) n'est pas vrai lorsque $\gamma = 0$. Nous traiterons ce cas un peu plus loin.

De façon plus générale, il existe un résultat très connu lorsque nous n'imposons pas le terme γ. Puisque nous en aurons besoin un peu plus loin, profitons de cette occasion pour énoncer ce résultat.

Lemme 2.6. *Si* $N(n, q)$ *est le nombre de polynômes irréductibles unitaires sur* $\mathbb{F}_q$ *de degré* n. *On a que*

$$N(n, q) = \frac{1}{n}\sum_{d|n} \mu(d) q^{n/d}$$

DÉMONSTRATION. Les racines de $x^{q^n} - x$ sont exactement les éléments de $\mathbb{F}_{q^n}$. En prenant n de telle sorte que $\mathbb{F}_{q^n}$ est le corps de décomposition de $x^{q^n} - x$ sur $\mathbb{F}_q$ et puisque tous les polynômes irréductibles de $\mathbb{F}_q$ divisent $x^{q^n} - x$, on conclut que

$$x^{q^n} - x = \prod_{d|n} T(d, q)$$

où $T(d, q)$ est l'ensemble des polynômes irréductibles unitaires sur $\mathbb{F}_q$ de degré d sans que γ soit fixé. On peut voir que

$$q^n = \deg(\prod_{d|n} T(d, q)) = \sum_{d|n} dN(d, q).$$

En appliquant l'inversion de Möbius, on montre le résultat. □

Ceci étant dit, concentrons nous maintenant sur la démonstration du résultat de Yucas. L'idée générale de cette preuve passe par la définition suivante.

Définition 2.7. Posons $B_{n,\gamma}$ le produit de tous les polynômes unitaires irréductibles sur $\mathbb{F}_q$ dont le degré divise n et dont la trace est γ.

Ainsi, par définition de $B_{n,\gamma}(x)$ et de $N_\gamma(n, q)$, on peut constater que

$$\deg(B_{n,\gamma}(x)) = \sum_{d|n} dN_\gamma(d, q).$$

Dans les prochaines pages, nous trouverons donc une méthode pour calculer $\deg(B_{n,\gamma}(x))$. Ensuite, il sera aisé de trouver $N_\gamma(n, q)$ avec l'inversion de Mobius.

2.0.3. Calcul de $\deg(B_{n,\gamma}(x))$

Pour calculer explicitement $\deg(B_{n,\gamma}(x))$, nous montrerons un peu plus loin, que $\deg(B_{n,\gamma}(x))$ suit la récurrence suivante.

Définition 2.8. Pour $n \in \mathbb{N}$, posons

$$D(n) = \begin{cases} q^{n-1} + D(\frac{n}{p}) & \text{si } p|n \\ \\ q^{n-1} & \text{si } p \nmid n \end{cases}$$

Nous allons donc commencer par trouver une formule pour calculer $D(n)$.

Proposition 2.9. *Considérons,* $n = p^r m$ *où* $p \nmid m$. *Alors,*

$$D(n) = \sum_{i=0}^{r} q^{p^{r-i}m-1}.$$

DÉMONSTRATION. Nous allons faire une preuve par induction sur r. Si $r = 0$, on a que $n = p^0 m = m$, ce qui implique que $p \nmid n$ et donc

$$D(n) = q^{n-1} = \sum_{i=0}^{0} q^{p^{r-i}m-1}.$$

Si $r > 0$, en utilisant notre hypothèse d'induction, nous avons

$$D(n) = q^{p^r m-1} + D(p^{r-1}m) = q^{p^r m-1} + \sum_{i=0}^{r-1} q^{p^{r-1-i}m-1} = \sum_{i=-1}^{r-1} q^{p^{r-1-i}m-1}.$$

En posant $t = r - 1$, on conclut que

$$\sum_{i=-1}^{r-1} q^{p^{r-1-i}m-1} = \sum_{i=0}^{t} q^{p^{t-i}m-1}.$$

□

Pour montrer que $\deg(B_{n,\gamma}(x))$ suit la récurrence $D(n)$, nous allons devoir factoriser $B_{n,\gamma}(x)$ de façon judicieuse. Avec une factorisation $B_{n,\gamma}(x) = g_1(x)g_2(x)g_3(x)$ où $g_1(x), g_2(x), g_3(x) \in \mathbb{F}_q[x]$, nous aurions immédiatement

$$\deg(B_{n,\gamma}(x)) = \deg(g_1(x)) + \deg(g_2(x)) + \deg(g_3(x)).$$

Avec un choix judicieux de $g_1(x)$, $g_2(x)$ et $g_3(x)$, nous pourrons aisément montrer la récurrence. Nous utiliserons les prochaines définitions pour définir ces trois polynômes.

Définition 2.10. Posons τ_d l'application définie comme

$$\tau_d : \mathbb{F}_{q^d} \to \mathbb{F}_q, x \to \sum_{s=0}^{d-1} x^{q^s}.$$

Définition 2.11. Si L_n est l'ensemble de tous les polynômes unitaires irréductibles de $\mathbb{F}_q$ dont leur degré divise n, nous posons

$$G_1 = \{h(x) \in L_n : \deg(h) = n \text{ et } \tau_{\deg(h)}(\delta) = -\gamma, \text{où } \delta \text{ est une racine de } h(x)\}.$$

Nous définissons ainsi le polynôme

$$g_1(x) = \prod_{h \in G_1} h(x).$$

Définition 2.12. De façon analogue, on définit

$$G_2 = \{h(x) \in L_n : p | \frac{n}{\deg(h)} \text{ et } \tau_{\deg(h)}(\delta) = -\gamma, \text{où } \delta \text{ est une racine de } h(x)\},$$

$$G_3 = \{h(x) \in L_n : p \nmid \frac{n}{\deg(h)}, \deg(h) < n \text{ et } \tau_{\deg(h)}(\delta) = -\gamma, \text{où } \delta \text{ est une racine de } h(x)\},$$

Pour $i = 2$ et $i = 3$, on pose

$$g_i(x) = \prod_{h \in G_i} h(x).$$

Ainsi, on remarque que

$$B_{n,\gamma}(x) = g_1(x)g_2(x)g_3(x).$$

Nous sommes presque prêts à montrer que $\deg(B_{n,\gamma}(x))$ suit la récurrence $D(n)$. Il nous faut encore introduire un polynôme et montrer quelques propriétés.

Définition 2.13. Pour n un entier positif et $\gamma \in \mathbb{F}_q$, définissons que

$$q_{n,\gamma}(x) = \gamma + x + x^q + \cdots + x^{q^{n-1}}.$$

Lemme 2.14. *Dans $\mathbb{F}_q$, nous avons que*

$$x^{q^n} - x = \prod_{\gamma \in \mathbb{F}_q} q_{n,\gamma}(x)$$

DÉMONSTRATION. On remplace x par $x + x^q + \cdots + x^{q^{n-1}}$ dans le lemme (1.2).

$$(x + x^q + \cdots + x^{q^{n-1}})^q - (x + x^q + \cdots + x^{q^{n-1}}) = \prod_{\gamma \in \mathbb{F}_q} (x + x^q + \cdots + x^{q^{n-1}} - \gamma)$$

Puisque nous sommes en caractéristique p et que $p|q$, nous avons que

$$x^q + x^{q^2} + \cdots + x^{q^n} - x - x^q - \cdots - x^{q^{n-1}} = \prod_{\gamma \in \mathbb{F}_q} q_{n,\gamma}(x).$$

Nous concluons donc que

$$x^{q^n} - x = \prod_{\gamma \in \mathbb{F}_q} q_{n,\gamma}(x).$$

□

Définition 2.15. Posons que

$$H_{n,\gamma} = \{h(x) \in L_n : p \nmid \frac{n}{\deg(h)} \text{ et } \frac{n}{\deg(h)} \tau_{\deg(h)}(\delta) = -\gamma, \text{où } \delta \text{ est une racine de } h(x)\}$$

Nous aurons également besoin de factoriser $q_{n,\gamma}(x)$ pour montrer notre résultat.

Lemme 2.16. *Pour $\gamma \in \mathbb{F}_q^\star$, on a que*

$$q_{n,\gamma}(x) = \prod_{h(x) \in H_{n,\gamma}} h(x).$$

DÉMONSTRATION. Prenons $r(x)$ un facteur irréductible de $q_{n,\gamma}(x)$ de degré d. Nous allons montrer que $r(x) \in H_{n,\gamma}$. Par la proposition (2.14), on sait que $q_{n,\gamma}(x)|x^{q^n} - x$ et donc que $r(x)|x^{q^n} - x$. En appliquant la proposition (1.4), on sait dorénavant que $d|n$. Prenons δ une racine de $r(x)$ dans $\mathbb{F}_{q^d}^\star$. Ainsi,

$$q_{n,\gamma}(\delta) = \delta^{q^{n-1}} + \delta^{q^{n-2}} + \cdots + \delta^{q^{d-1}} + \cdots + \delta + \gamma = 0$$

Puisque, $\delta^{q^d} = \delta$ et que $d|n$, la somme $\sum_{s=0}^{d-1} x^{q^s}$ se retrouve n/d fois dans l'équation. Alors,

$$\frac{n}{d} \sum_{s=0}^{d-1} \delta^{q^s} + \gamma = 0,$$

$$\frac{n}{d} \tau_d(\delta) = -\gamma.$$

On peut déduire que $p \nmid (n/d)$, sinon, on aurait $\gamma = 0$, ce qui contredirait notre hypothèse de départ. Ainsi, $r(x) \in H_{n,\gamma}$. On peut montrer l'inclusion de l'autre côté. Prenons $h(x) \in H_{n,\gamma}$. Puisque $\frac{n}{\deg(h)} \tau_{\deg(h)}(\delta) = -\gamma$ et que $\deg(h)|n$,

on déduit que $h(x)$ est un facteur irréductible de $q_{n,\gamma}(x)$. On peut donc factoriser :

$$q_{n,\gamma}(x) = \prod_{h(x)\in H_{n,\gamma}} h(x).$$

□

Précisons encore que ce lemme s'applique seulement si $\gamma \neq 0$. Grâce à ce résultat, on peut faire la factorisation suivante : $q_{n,\gamma}(x) = g(x)g_1(x)$ où

$$g(x) = \prod_{\substack{h \in H_{n,\gamma} \\ \deg(h) < n}} h(x). \tag{2.0.4}$$

$$g_1(x) = \prod_{\substack{h \in H_{n,\gamma} \\ \deg(h) = n}} h(x),$$

Remarque 2.17. Cette définition de g_1 est équivalente à celle que nous avons à la définition (2.11).

Montrons maintenant que $B_{n,\gamma}(x)$ suit la récurrence (2.8).

Proposition 2.18. $\deg(B_{n,\gamma}(x))$ *satisfait la récurrence* $D(n)$ *de la définition* (2.8)*.*

DÉMONSTRATION. De (2.0.3), nous savons que

$$\deg(B_{n,\gamma}(x)) = \deg(g_1(x)) + \deg(g_2(x)) + \deg(g_3(x)).$$

De plus, nous savons que $g_2(x)$ est le produit de tous les polynômes irréductibles dont le degré divise n/p. En regardant la définition de $B_{n/p,\gamma}$, on déduit que $\deg(g_2) = \deg(B_{n/p,\gamma}(x))$. Par le lemme (2.4), on sait que la valeur de la trace n'influence pas le nombre de polynômes irréductibles pourvu qu'elle ne soit pas nulle. On déduit ainsi que $\deg(g_3) = \deg(g)$ où g est défini en (2.0.4). Par le lemme (2.16), on sait que $\deg(q_{n,\gamma}) = \deg(g_1) + \deg(g)$. Alors, nous avons

$$\begin{aligned}\deg(g_1(x)) + \deg(g_2(x)) + \deg(g_3(x)) &= \deg(g_1) + \deg(B_{n/p,\gamma}(x)) + \deg(g) \\ &= \deg(q_{n,\gamma}) + \deg(B_{n/p,\gamma}(x)).\end{aligned}$$

On conclut ainsi que

$$\deg(B_{n,\gamma}(x)) = q^{n-1} + \deg(B_{n/p,\gamma}(x)).$$

Si $p \nmid n$, par définition de g_2, on sait que $\deg(g_2) = 0$. En suivant le même raisonnement, on obtient que

$$\deg(B_{n,\gamma}(x)) = q^{n-1}$$

□

2.0.4. Preuve du théorème 2.3

Nous sommes désormais prêt à montrer le théorème 2.3.

Théorème. *Si* $\gamma \in \mathbb{F}_q^\star$ *et que* $n = p^r m$ *avec* $p \nmid m$

$$N_\gamma(n, q) = \frac{1}{qn} \sum_{s|m} \mu(s) q^{n/s}.$$

DÉMONSTRATION. Par la définition de $B_{n,\gamma}(x)$ et de $N_\gamma(n, q)$, on a que

$$\deg(B_{n,\gamma}(x)) = \sum_{d|n} d N_\gamma(d, q).$$

En appliquant l'inversion de Möbius sur cette égalité, nous obtenons

$$N_\gamma(n, q) = \frac{1}{n} \sum_{d|n} \mu(n/d) \deg(B_{d,\gamma}(x))$$

En combinant les propositions (2.9) et (2.18), on déduit que

$$N_\gamma(n, q) = \frac{1}{n} \sum_{d|n} \mu(n/d) \sum_{i=0}^{r_d} q^{p^{r_d - i} m_d - 1}. \tag{2.0.5}$$

Où r_d et m_d sont les valeurs associées à $d = p^{r_d} m_d$ avec $p \nmid m_d$ et $0 \leq r_d \leq r$. Puisque $n = p^r m$, on sait que :

$$\mu\left(\frac{n}{d}\right) = \mu\left(p^{r - r_d} \frac{m}{m_d}\right).$$

Si on prend $r_d < r - 2$, on conclut que

$$\mu\left(p^{r - r_d} \frac{m}{m_d}\right) = 0.$$

Puisque tous les $\mu(n/d)$ seront nuls sauf pour $d = p^r m_d$ et $d = p^{r-1} m_d$, nous pouvons séparer l'équation (2.0.5) de la façon suivante :

$$\begin{aligned} N_\gamma(n, q) &= \frac{1}{n} \sum_{d|n} \mu(n/d) \sum_{i=0}^{r_d} q^{p^{r_d - i} m_d - 1} \\ &= \frac{1}{n} \sum_{m_d|m} \left(\mu\left(\frac{p^r m}{p^r m_d}\right) \sum_{i=0}^{r} q^{p^{r-i} m_d - 1} + \mu\left(\frac{p^r m}{p^{r-1} m_d}\right) \sum_{i=0}^{r-1} q^{p^{r-1-i} m_d - 1} \right). \end{aligned}$$

Sachant que $\mu(p^r m/(p^{r-1} m_d)) = -\mu(m/m_d)$, nous pouvons poursuivre l'égalité de sorte que

$$\begin{aligned} N_\gamma(n,q) &= \frac{1}{n} \sum_{m_d|m} \mu\left(\frac{m}{m_d}\right) \left(\sum_{i=0}^{r} q^{p^{r-i} m_d - 1} - \sum_{i=0}^{r-1} q^{p^{r-1-i} m_d - 1} \right) \\ &= \frac{1}{n} \sum_{m_d|m} \mu\left(\frac{m}{m_d}\right) q^{p^r m_d - 1} \end{aligned}$$

En posant $s = m/m_d$, on conclut que

$$N_\gamma(n,q) = \frac{1}{nq} \sum_{s|m} \mu(s) q^{n/s}.$$

□

Nous venons de compléter la démonstration du théorème (2.3). Il demeure toutefois le cas où $\gamma = 0$.

Théorème 2.19. *Si* $n = p^r m$ *avec* $p \nmid m$,

$$N_0(n,q) = \frac{1}{qn} \sum_{d|m} \mu(d) q^{n/d} - \frac{\epsilon}{n} \sum_{d|m} \mu(d) q^{n/(dp)},$$

où $\epsilon = 0$ *si* $r = 0$ *et* $\epsilon = 1$ *si* $r > 0$.

DÉMONSTRATION. Puisque $N(n,q)$ est l'ensemble des polynômes irréductibles sur $\mathbb{F}_q$,

$$N(n,q) = \sum_{\gamma \in \mathbb{F}_q} N_\gamma(n,q)$$

$$N_0(n,q) = N(n,q) - \sum_{\gamma \in \mathbb{F}_q^\star} N_\gamma(n,q).$$

Par le lemme (2.4), la valeur de γ n'influence pas la valeur de $N_\gamma(n,q)$.

$$N_0(n,q) = N(n,q) - (q-1) N_\gamma(n,q)$$

Par le théorème précédent et le lemme (2.6), nous avons que

$$N_0(n,q) = \frac{1}{n} \sum_{d|n} \mu(d) q^{n/d} - \frac{q-1}{qn} \sum_{d|m} \mu(d) q^{n/d}. \tag{2.0.6}$$

Si $r = 0$, il est clair que

$$\begin{aligned} N_0(n,q) &= \frac{1}{n} \sum_{d|m} \mu(d) q^{n/d} \left(1 - \frac{q-1}{q}\right) \\ &= \frac{1}{qn} \sum_{d|m} \mu(d) q^{n/d}, \end{aligned}$$

ce qui est le résultat attendu. Si $r > 0$, on refait la même chose jusqu'à la ligne (2.0.6). De ce point, on sépare la sommation en deux parties. D'abord, nous considérons les d tel que $p \nmid d$, puis tous les autres d. Ainsi, on aura le même résultat que nous avions lorsque $r = 0$, mais avec une sommation supplémentaire.

$$N_0(n, q) = \frac{1}{qn} \sum_{d|m} \mu(d) q^{n/d} + \frac{1}{n} \sum_{\substack{d|n \\ p|d}} \mu(d) q^{n/d}.$$

Considérons $d = p^{r_d} m_d$ avec $p \nmid m_d$. Si $r_d \geq 2$, on remarque que $\mu(d) = \mu(p^{r_d} m_d) = 0$. Ainsi, nous avons

$$N_0(n, q) = \frac{1}{qn} \sum_{d|m} \mu(d) q^{n/d} + \frac{1}{n} \sum_{d|m} \mu(dp) q^{n/(dp)}.$$

Puisque $\mu(dp) = \mu(d)\mu(p) = -\mu(d)$, nous avons donc

$$N_0(n, q) = \frac{1}{qn} \sum_{d|m} \mu(d) q^{n/d} - \frac{1}{n} \sum_{d|m} \mu(d) q^{n/(dp)},$$

qui est le résultat attendu. □

Chapitre 3

FORME QUADRATIQUE SUR LES CORPS FINIS

Dans les prochains chapitres, nous traiterons des polynômes de la forme suivante :

$$f(x) = x^n + ax^{n-2} + t_1x^{n-3} + ... + t_{n-3}x + t_{n-2} \tag{3.0.7}$$

où $a \in \mathbb{F}^\star{}_q$ est fixé.

Le but est de trouver le nombre de polynômes irréductibles de la forme précédente dont les coefficients sont des éléments $\mathbb{F}_q$. Plus précisément, nous étudierons les étapes qui ont amené Kuz'min[**10**][**11**] à trouver, pour $a \neq 0$, le résultat suivant :

$$H_n(a) = \frac{1}{n} \sum_{\substack{d|n \\ p\nmid d}} \mu(d) G_{n/d}(-a/d), \tag{3.0.8}$$

où $H_n(a)$ est le nombre de polynômes irréductibles de la forme (3.0.7) et si $p \nmid n$, G_n est défini comme

$$G_n(a) = \begin{cases} q^{n-2} - \left(\frac{(-1)^{m-1}ma}{q}\right) q^{m-1} & n = 2m, \\ \\ q^{n-2} - l(a)\left(\frac{(-1)^m n}{q}\right) q^{m-1} & n = 2m+1, \end{cases} \tag{3.0.9}$$

où

$$l(a) = \begin{cases} 1 & \text{si } a \neq 0, \\ \\ 1-q & \text{si } a = 0, \end{cases}$$

et

$$\left(\frac{a}{q}\right) = \begin{cases} 1 & \text{si } a \text{ est un carré dans } \mathbb{F}_q^\star, \\ \\ -1 & \text{si } a \text{ n'est pas un carré dans } \mathbb{F}_q^\star, \\ \\ 0 & \text{si } a = 0\,. \end{cases}$$

Si $p|n$, on aurait le G_n suivant

$$G_n(a) = \begin{cases} q^{n-2} + l(a)\left(\frac{(-1)^m}{q}\right) q^{m-1}. & n = 2m, \\ q^{n-2} + \left(\frac{2a(-1)^m}{q}\right) q^m & n = 2m+1. \end{cases} \tag{3.0.10}$$

Ces résultats sont valides seulement si la caractéristique n'est pas 2.

Remarque 3.1. Nous ferrons aussi le cas où $a = 0$. Il sera fait un peu plus loin.

Pour montrer ce résultat, nous devrons faire un peu de travail. Comme énoncé dans notre stratégie, nous devrons trouver le nombre de solutions des formes quadratiques suivantes

$$\sum_{i=1}^{d} x_i^2 + \sum_{1\le i<j\le d} x_i x_j = a, \tag{3.0.11}$$

où d est la dimension de la forme quadratique. Intuitivement, on peut voir la nécessité d'étudier ce sujet en faisant les considérations suivantes. Si (3.0.7) se factorise complètement, on remarque que la somme des racines est zéro et que la somme des racines prises deux à deux est a. C'est-à-dire que si les x_i sont les n racines de (3.0.7), nous avons avec une petite manipulation que

$$x_n = -x_1 - \cdots - x_{n-1}$$

et que

$$a = \sum_{1\le i<j\le n} x_i x_j.$$

Ainsi, de ces deux équations, nous trouvons que

$$\begin{aligned} a &= \sum_{1\le i<j<n} x_i x_j + \sum_{1\le i<n} x_i x_n \\ &= \sum_{1\le i<j<n} x_i x_j - \left(\sum_{1\le i<n} x_i\right)^2 \\ &= -\sum_{1\le i<n} x_i^2 - \sum_{1\le i<j<n} x_i x_j. \end{aligned}$$

Donc, le nombre de façons de choisir le coefficient a dans (3.0.7) dépendra de cette forme quadratique. C'est donc pour cette raison que nous allons dédier ce chapitre à l'étude du dénombrement des solutions de n'importe quelles formes quadratiques.

3.1. CASSELMAN

Plus précisément, nous étudierons un théorème qui a été illustré dans un article de William Casselman[**3**], mais dont la preuve originale proviendrait d'un article de Herman Minkowski[**9**]. En fait, il s'agit d'arriver à compter le nombre de solutions de n'importe quelle forme quadratique non-dégénérée sur un corps fini tel que

$$x^t M x = a, \tag{3.1.1}$$

où M est une matrice symétrique et où le terme «non-dégénéré» signifie que le déterminant de la matrice M est non-nul.

Remarque 3.2. Pour utiliser cette forme matricielle avec la forme quadratique définie à la fin de la dernière section :

$$\sum_{i=1}^{n} x_i^2 + \sum_{1 \le i < j \le n} x_i x_j = a, \tag{3.1.2}$$

il faut simplement que M ait des 1 sur la diagonale et des $1/2$ ailleurs.

Voici le théorème que Casselman a démontré dans son article. La notation a été grandement modifiée pour en faciliter son utilisation dans ce mémoire.

Théorème 3.3. *Pour une forme quadratique non-dégénérée écrite dans la forme* (3.1.1)*, si* d *est la dimension du vecteur* x *et* K_d *est le nombre de solutions d'une forme quadratique de dimension* d*, nous concluons que si* $d = 2m$

$$K_{2m} = q^{2m-1} - l(a)\left(\frac{\det(M)(-1)^m}{q}\right) q^{m-1}, \tag{3.1.3}$$

où

$$l(a) = \begin{cases} 1 & \text{si } a \neq 0, \\ 1 - q & \text{si } a = 0. \end{cases}$$

Si $d = 2m + 1$ *et* q *est impair, alors*

$$K_{2m+1} = q^{2m} + \left(\frac{a \det(M)(-1)^m}{q}\right) q^m. \tag{3.1.4}$$

Finalement, si $d = 2m + 1$ *et* q *est pair, alors*

$$K_{2m+1} = q^{2m}. \tag{3.1.5}$$

Dans tous ces cas, $a \in \mathbb{F}_q$

Avant de donner l'idée de la démonstration, nous devons revoir quelques notions théoriques.

Définitions et Stratégie

Définition 3.4. Soit $\nabla : \mathbb{F}_q^d \times \mathbb{F}_q^d \to \mathbb{F}_q$ une forme bilinéaire de dimension d tel que

$$\nabla(x, y) = \sum_{i,j} a_{i,j} x_i y_j. \tag{3.1.6}$$

Définition 3.5. Une forme quadratique $Q : \mathbb{F}_q^d \to \mathbb{F}_q$ de dimension d est définie comme

$$Q(x) = \sum_{i \leq j} a_{i,j} x_i x_j. \tag{3.1.7}$$

Il est toujours possible de ramener cette équation pour avoir une forme matricielle comme dans le théorème (3.3). Pour l'instant, il est plus facile de travailler avec les sommations.

Il est aisé de constater le lien entre ces deux équations. D'abord, toutes formes bilinéaires sont des formes quadratiques :

$$Q_\nabla(x) = \nabla(x, x).$$

De l'autre côté, une forme quadratique définit une forme bilinéaire :

$$\nabla_Q(x, y) = Q(x + y) - Q(x) - Q(y).$$

Définition 3.6. Un espace quadratique est simplement un espace vectoriel V sur $\mathbb{F}_q$ qui possède une forme quadratique $Q(x)$. Nous noterons un tel espace (V, Q).

Définition 3.7. Un espace quadratique est appelé un plan hyperbolique ou un hyperplan s'il est de dimension 2 et que la matrice de Q est conjuguée à $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. C'est-à-dire qu'il existe une base $\{v_1, v_2\}$ telle que $Q(v_1) = 0$, $Q(v_2) = 0$ et que $\nabla(v_1, v_2) = 1$. Nous noterons un tel espace H.

Définition 3.8. Soit $\mathbb{F}_q$ le corps fini de q éléments et soit $\mathbb{F}_{q^2}$ son extension quadratique séparable, on définit $N_{\mathbb{F}_{q^2}/\mathbb{F}_q}(x) = x\bar{x} = xx^q$ la norme de l'extension $\mathbb{F}_{q^2}$ sur $\mathbb{F}_q$.

Ainsi, dans la première section de ce chapitre, nous allons montrer le théorème suivant.

Théorème 3.9. *Toutes formes quadratiques de dimension n sont des sommes directes d'hyperplans, des sommes directes d'hyperplans avec $N_{\mathbb{F}_{q^2}/\mathbb{F}_q}$ ou des sommes directes d'hyperplans avec un espace de dimension 1 qui est simplement cx^2 avec $c \in \mathbb{F}_q$. En d'autres mots, pour une forme quadratique de dimension $2n$, nous avons que $Q = nH$ ou $Q = (n-1)H \oplus N_{\mathbb{F}_{q^2}/\mathbb{F}_q}$ et pour une forme quadratique de dimension $2n+1$, nous avons que $Q = nH \oplus cx^2$.*

Nous devrons utiliser ce résultat dans la deuxième partie de ce chapitre afin de montrer le théorème (3.3) . Pour ce faire, nous devrons remarquer que

$$\nu_Q(y) := \#\{w \in V | Q(w) = y\}.$$

est exactement le nombre de solutions d'une forme quadratique Q. Ensuite, il nous sera facile de calculer la transformée de Fourier de $\nu_Q(y)$ pour les espaces de dimension 1 ou 2 que nous avons trouvés à la première section. Grâce à quelques propriétés des transformées de Fourier et aux sommes directes d'espaces quadratiques, nous pourrons calculer $\nu_Q(y)$ pour n'importe quelles formes quadratiques et ainsi, montrer le théorème (3.3).

3.1.1. Décomposition des espaces quadratiques

Dans cette section, nous voulons montrer que tous espaces quadratiques sont des sommes directes de H, $N_{\mathbb{F}_{q^2}/\mathbb{F}_q}$ et cx^2. Pour l'instant, continuons avec quelques définitions.

Définition 3.10. Un espace quadratique non-dégénéré est un espace quadratique dont la forme quadratique matricielle n'a pas un déterminant nul.

Définition 3.11. Sur un espace quadratique, il est possible d'y définir une relation d'orthogonalité à l'aide de ∇. Sur un sous-espace U, on peut donc parler d'un complément orthogonal noté $U^\perp$ et défini comme :

$$U^\perp = \{x \in V : \forall y \in U \ \ \nabla(x, y) = 0\}.$$

La prochaine proposition sera le point de départ de notre stratégie pour séparer nos formes quadratiques sommes directes de sous-espaces quadratiques.

Proposition 3.12. *Soit (V, Q) un espace quadratique sur $\mathbb{F}_q$ et U un sous-espace de V tel que la restriction de Q à U est non-dégénérée, alors : $V = U \oplus U^\perp$*

DÉMONSTRATION. Pour montrer cette proposition, il nous faut simplement une projection P de V sur U tel que $v - P(v)$ soit dans $U^\perp$. Prenons (e_i) une base de U et n'importe quel $v \in V$. Nous cherchons un u tel que $P(v) = u = \sum c_k e_k$. Pour que $v - P(v) \in U^\perp$ soit satisfait, il faut que $\nabla(v - P(v), y) = 0$ pour tous y de U. Pour faciliter notre travail, au lieu de vérifier l'équation pour tous

les y, nous le ferons simplement pour les éléments de la base. De plus, nous remplacerons $P(v)$ par sa représentation sous notre base. C'est-à-dire que nous devons trouver les c_k tels que

$$\nabla(v - \sum c_k e_k, e_j) = 0$$

pour n'importe quel e_j. Alors, sachant que Δ est une forme bilinéaire , nous avons que

$$\nabla(v - \sum c_k e_k), e_j) = \nabla(v, e_j) - \sum c_k \nabla(e_k, e_j) = 0,$$

ce qui implique que

$$\nabla(v, e_j) = \sum c_k \nabla(e_k, e_j).$$

Puisque nous sommes dans le cas non-dégénéré, nous pouvons résoudre le système d'équations et trouver les c_k recherchés.

□

Pour montrer le théorème (3.9), il faudra utiliser la proposition (3.12) de façon judicieuse sur un espace quadratique (V, Q) pour obtenir que $V = U \oplus U^\perp$ avec U de dimension 2. Ensuite, on ré-applique (3.12) sur $U^\perp$ pour trouver que $U^\perp = U_1 \oplus U_1^\perp$ en s'assurant que U_1 soit encore de dimension 2. Ainsi, on aurait que $V = U \oplus U_1 \oplus U_1^\perp$. En continuant de cette façon, on pourra montrer le résultat par récurrence. Nous devrons cependant nous assurer de la nature de l'espace quadratique de dimension 2 lorsque nous utiliserons la proposition (3.12). Pour ce faire, nous allons consacrer une sous-section aux espaces quadratiques de dimension 2.

3.1.1.1. *Études des espaces quadratiques de dimension 2*

Comme nous l'avons déjà dit, les formes quadratiques de dimension 2 sont particulièrement importantes pour montrer le résultat (3.3). Nous verrons un plus loin que H et $N_{\mathbb{F}_{q^2}/\mathbb{F}_q}$ sont les seuls espaces de dimension 2 pour les formes quadratiques.

Pour l'instant, montrons comment trouver un plan hyperbolique dans un espace quadratique.

Définition 3.13. Un vecteur v est dit anisotropique si $Q(v) \neq 0$.

Définition 3.14. Un vecteur v est dit isotropique si $v \neq 0$ et $Q(v) = 0$. Un espace isotropique est un espace dont tous les vecteurs non-nuls sont isotropiques.

Proposition 3.15. *Soit (V, Q) un espace quadratique non-dégénéré et v un vecteur isotropique de V, il existe alors un plan hyperbolique dans V qui contient v.*

DÉMONSTRATION. Puisque V est non-dégénéré et que $Q(v) = \nabla(v, v) = 0$, on peut prendre n'importe quel $\bar{u} \in V$ de sorte que $\nabla(\bar{u}, v) = b$ pour un b quelconque, mais non-nul. Ainsi,

$$\nabla(\bar{u}, v) = b,$$
$$\nabla(\frac{\bar{u}}{b}, v) = 1.$$

En posant, $u = \bar{u}/b$ on obtient $\nabla(u, v) = 1$. Ensuite, avec $c \in \mathbb{F}_q^\star$ on remarque

$$\nabla(u, cv) = Q(u + cv) - Q(u) - c^2 Q(v)$$
$$\Rightarrow Q(u + cv) = Q(u) + c\nabla(u, v)$$

Avec un c bien choisi, on peut avoir $Q(u) + c\nabla(u, v) = 0$. En posant $w = u + cv$, on remarque que $Q(w) = 0$ et que

$$\begin{aligned}\nabla(w, v) &= \nabla(u + cv, v) \\ &= \nabla(u, v) + c\nabla(v, v) \\ &= 1 + cQ(v) \\ &= 1.\end{aligned}$$

Nous avons deux vecteurs isotropiques linéaires indépendants qui engendrent donc un plan hyperbolique. □

La proposition précédente est très utile. En effet, si nous avons un espace quadratique de dimension 2 et que nous trouvons un vecteur isotropique, on sait que l'espace est en fait un plan hyperbolique. Donc, pour classifier les formes quadratiques de dimension 2, il nous reste à étudier ceux qui possèdent seulement des vecteurs anisotropiques. Nous verrons que dans ce cas, l'espace est simplement $N_{\mathbb{F}_{q^2}/\mathbb{F}_q}$.

Proposition 3.16. *Tous les espaces quadratiques de dimension 2 non-dégénérés sont isomorphes à un plan hyperbolique* H *ou à* $AN_{\mathbb{F}_{q^2}/\mathbb{F}_q}$ *pour* $A \in \mathbb{F}_q$.

DÉMONSTRATION. Toutes formes quadratiques de dimension 2 s'écrivent comme $Q(x, y) = Ax^2 + Bxy + Cy^2$. Si A et C sont nuls, nous avons un plan hyperbolique. Sans perte de généralité, on peut maintenant assumer que $A \neq 0$. On peut factoriser Q comme $A(x - \alpha y)(x - \beta y)$ sur la fermeture algébrique de $\mathbb{F}_q$. Si α et β sont tous deux dans $\mathbb{F}_q$, on peut faire un changement de variable et trouver la forme suivante : $Ax(x - \gamma)$. Gamma ne peut être nul puisque la forme quadratique est non-dégénérée. Avec un autre changement de variable, on trouve la forme Axy et nous avons un plan hyperbolique. Si α et β ne sont

pas dans $\mathbb{F}_q$, ils doivent être des conjugués dans l'extension quadratique $\mathbb{F}_{q^2}/\mathbb{F}_q$ et donc $AN_{\mathbb{F}_{q^2}/\mathbb{F}_q}$.

□

3.1.1.2. *Début de la décomposition en somme directe*

Nous sommes maintenant près à exprimer notre espace quadratique comme une somme directe d'espace de dimension 2 ou 1.Pour ce faire, nous aurons besoin de montrer qu'il existe un plan hyperbolique dans tous espaces quadratiques de dimension strictement plus grande que 2. Pour ce faire, nous allons démontrer que toutes formes quadratiques de dimension strictement plus grandes que 2 possèdent un vecteur isotropique. Cette affirmation est une conséquence du théorème de Chevalley-Warning. La démonstration provient de [7]. Débutons par un petit lemme.

Lemme 3.17. *Pour tous les entiers positifs* $n < q-1$, *nous avons que*

$$\sum_{x\in\mathbb{F}_q} x^n = 0.$$

DÉMONSTRATION. Si $n = 0$, le résultat est évident. Si $n > 0$, prenons γ un générateur du groupe cyclique $\mathbb{F}_q^\star$. Puisque $n < q-1$ et que l'ordre de γ est $q-1$, on sait γ^n n'est pas l'élément neutre. Ainsi, nous avons

$$\sum_{x\in\mathbb{F}_q} x^n = \sum_{i=1}^{q-1} \gamma^{ni} = \sum_{i=0}^{q-2} \gamma^{ni} = \frac{(\gamma^n)^{q-1}-1}{\gamma^n-1} = 0.$$

□

Théorème 3.18 (Chevalley-Warning). *Soit* $f_1, f_2 \ldots, f_m \in \mathbb{F}_q[x_1, x_2, \ldots, x_n]$. *Si on a* $\sum_i \deg(f_i) < n$ *et que* $S = \{x \in \mathbb{F}_q^n | f_1(x) = f_2(x) = \cdots = f_m(x) = 0\}$, *alors* $\#(S)$ *est divisible par p.*

DÉMONSTRATION. L'astuce ici est de considérer le polynôme suivant :

$$f = \prod_i^m (1 - f_i^{q-1}).$$

On a immédiatement la relation suivante

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

Évidemment, nous avons que $\#(S) = \sum_{x\in\mathbb{F}_q^n} f(x)$ et aussi que le degré de f est strictement inférieur à $n(q-1)$. Considérons maintenant un des termes du

polynôme f soit, $x_1^{a_1}x_2^{a_2}\dots x_n^{a_n}$. On sait qu'au moins un des a_i est plus petit que $(q-1)$, car sinon f serait de degré supérieur à $(q-1)n$, ce qui est une contradiction. Sans perdre de généralité, supposons que ce a_i est le dernier élément soit a_n. Grâce au lemme précédent :

$$\sum_{x_1,\dots,x_n\in\mathbb{F}_q} x_1^{a_1}\dots x_n^{a_n} = \sum_{x_1,\dots x_{n-1}\in\mathbb{F}_q}\left(x_1^{a_1}\dots, x_{n-1}^{a_{n-1}}\sum_{x_n\in\mathbb{F}_q} x_n^{a_n}\right) = 0$$

Puisque que tous les termes f sont de cette forme, on conclut que $\#(S) = 0$. Puisque que nous sommes en caractéristique p, ceci est équivalent à ce que $\#(S)$ est divisible par p.

□

Corollaire 3.19. *Toutes formes quadratiques de dimension strictement supérieure à 2 possèdent au moins 1 vecteur isotropique.*

DÉMONSTRATION. Étant donné que le degré est inférieur à la dimension, par Chevallay-Warning, le nombre de solutions où $f(x) = 0$ est divisible par p. Puisque zéro est une solution, la cardinalité de S est non-nulle. Alors, il doit exister au moins une autre solution qui, celle-ci, serait non-triviale. □

3.1.1.3. *Nature des éléments dans les décompositions en sommes directes*

Pour la prochaine partie, nous supposerons que Q est toujours non-dégénéré et que $V = \mathbb{F}_q$. Nous allons maintenant montrer que tous les espaces quadratiques sont des sommes directes de H, $N_{\mathbb{F}_{q^2}/\mathbb{F}_q}$ ou cx^2

Lemme 3.20. *La norme $N_{\mathbb{F}_{q^2}/\mathbb{F}_q}$ est surjective.*

Nous sommes désormais prêt à faire la preuve du théorème (3.9) qui est le principal résultat de cette section.

DÉMONSTRATION DU THÉORÈME (3.9). Si la dimension est 2, on applique la proposition (3.16). Si la dimension est strictement plus grande que 2, on utilise le corollaire (3.19) combiner avec la proposition (3.12) pour le décomposer en une somme directe d'espace U_i de dimension 2. Puisqu'il existe toujours un vecteur isotropique dans les dimensions strictement plus grande que 2, les U_i sont isomorphes à H sauf 1 qui pourrait être isomorphe à $N_{\mathbb{F}_{q^2}/\mathbb{F}_q}$ ou cx^2 dépendamment de la dimension de la forme quadratique à savoir si elle est respectivement paire ou impaire.

□

Corollaire 3.21. *Un espace quadratique de dimension* $2n$ *de caractéristique impaire est une somme orthogonale de* nH *si* $\det(M)(-1)^{n-1}$ *est un carré et de* $(n-1)H \oplus N_{\mathbb{F}_{q^2}/\mathbb{F}_q}$ *sinon.*

DÉMONSTRATION. On applique le théorème précédent. Si le déterminant n'est pas un carré, il existe exactement une racine dans la fermeture de $\mathbb{F}_q$, ce qui donne alors $N_{\mathbb{F}_{q^2}/\mathbb{F}_q}$. Sinon, toutes les racines sont dans $\mathbb{F}_q$ et nous avons donc nH. □

Corollaire 3.22. *Un espace quadratique de dimension* $2n+1$ *de caractéristique impaire est une somme orthogonale de* $nH \oplus cx^2$ *où* $c = \det(M)(-1)^n$.

3.1.2. Transformées de Fourier

Faisons un rappel de notre stratégie. Nous voulons utiliser la décomposition en sommes directes des espaces quadratiques pour arriver à calculer des transformées de Fourier. Nous consacrerons donc cette sous-section pour faire toutes les définitions nécessaires pour introduire les transformées de Fourier et en montrer les propriétés utiles pour la poursuite de ce mémoire.
Nous allons réutiliser l'application τ_d d e 2.10 en modifiant quelque peu sa définition.

Définition 3.23. Soit $q = p^d$, posons τ l'application définie comme

$$\tau : \mathbb{F}_q \to \mathbb{F}_p, x \to \sum_{s=0}^{d-1} x^{p^s}.$$

Il s'agit de la même application qu'en 2.10, mais le d est omis dans l'écriture de τ

Lemme 3.24. *L'application* τ *est surjective.*

DÉMONSTRATION. Il s'agit d'une application linéaire. Il faut simplement montrer que τ n'est pas identiquement nulle. Pour y arriver, nous allons montrer par induction que si

$$\sum_{s=0}^{d-1} a_s x^{p^s} = 0,$$

$\forall x \in \mathbb{F}_q$ alors, tous les a_s sont identiquement nuls.
Si $d = 1$, le résultat est évident. Prenons donc comme hypothèse d'induction

$$\sum_{s=0}^{d-2} b_s x^{p^s} = 0.$$

$\forall x \in \mathbb{F}_q$ alors, les b_s doivent être identiquement nuls avec $d > 1$. Supposons maintenant que nous avons une combinaison linéaire telle que

$$\sum_{s=0}^{d-1} a_s x^{p^s} = 0.$$

$\forall x \in \mathbb{F}_q$. Nous avons alors aussi pour n'importe quel $y \in \mathbb{F}_q^\star$ que

$$\sum_{s=0}^{d-1} a_s (xy)^{p^s} = \sum_{s=0}^{d-1} a_s x^{p^s} y^{p^s} = 0.$$

Si on multiplie $\sum_{s=0}^{d-1} a_s x^{p^s}$ par $y^{p^{d-1}}$, on a $\sum_{s=0}^{d-1} a_s x^{p^s} y^{p^{d-1}} = 0$. En soustrayant les deux dernières équations, on réduit la somme d'un terme.

$$\sum_{s=0}^{d-2} a_s (y^{p^{d-1}} - y^{p^s}) x^{p^s} = 0.$$

Maintenant, on applique notre hypothèse d'induction, c'est-à-dire que pour que la somme soit nulle, il faut que $a_s(y^{p^{d-1}} - y^{p^s})$ soit nul pour tous s. Puisque les $y^{p^{d-1}} - y^{p^s}$ ne sont pas identiquement nuls, ce sont les a_s qui le sont. Donc l'application n'est pas identiquement nulle et elle est alors surjective.

□

Définition 3.25. À partir de τ, nous pouvons définir le caractère additif $\psi := \mathbb{F}_q \to \mathbb{C}$ tel que

$$\psi(x) := e^{2\pi i \tau(x)/p}. \tag{3.1.8}$$

Pour tous y dans $\mathbb{F}_q$, nous avons aussi le caractère additif similaire.

$$\psi_y := x \to \psi(xy)$$

Remarque 3.26. L'application $\tau(xy)$ est aussi surjective seulement si $y \neq 0$. On peut aussi préciser que si $y = 0$, $\psi(xy)$ est simplement le caractère trivial.

Lemme 3.27. *Pour $y \in \mathbb{F}_q$, nous avons*

$$\sum_{x \in \mathbb{F}_q} \psi(xy) = \begin{cases} q & \textit{si } y = 0, \\ \\ 0 & \textit{sinon}. \end{cases}$$

DÉMONSTRATION. Si $y = 0$

$$\sum_{x \in \mathbb{F}_q} \psi(xy) = \sum_{x \in \mathbb{F}_q} 1 = q.$$

Si $y \neq 0$ et puisque τ et un morphisme de groupe surjectif, nous avons

$$\sum_{x\in\mathbb{F}_q} \psi(xy) = \sum_{x\in\mathbb{F}_q} e^{2\pi i\tau(xy)/p} = [\mathbb{F}_q : \mathbb{F}_p] \sum_{n=0}^{p-1} e^{2\pi in/p} = 0.$$

□

On peut définir une transformée de Fourier de $\mathbb{C}(\mathbb{F}_q)$ sur elle-même de la façon suivante

$$\widehat{f}(y) = \frac{1}{\sqrt{q}} \sum_{x\in\mathbb{F}_q} f(x)\psi(-xy). \tag{3.1.9}$$

Proposition 3.28. *L'application* $f \in \mathbb{C}(\mathbb{F}_q)$ *suit la relation suivante*

$$\widehat{\widehat{f}}(x) = f(-x).$$

DÉMONSTRATION.

$$\begin{aligned}
\widehat{\widehat{f}}(y) &= \frac{1}{\sqrt{q}} \sum_{x\in\mathbb{F}_q} \widehat{f}(x)\psi(-xy) \\
&= \frac{1}{\sqrt{q}} \sum_{x\in\mathbb{F}_q} \frac{1}{\sqrt{q}} \sum_{z\in\mathbb{F}_q} f(z)\psi(-zx)\psi(-xy) \\
&= \frac{1}{q} \sum_{z\in\mathbb{F}_q} f(z) \sum_{x\in\mathbb{F}_q} \psi(-x(z+y)).
\end{aligned}$$

Lorsque $z = -y$, on a, par le lemme précédent, que $\sum \psi(0) = q$ et pour tous les autres z, on a que $\sum \psi(-x(z+y)) = 0$.

□

Lemme 3.29. *Pour* $f \in \mathbb{C}(\mathbb{F}_q)$

$$\sum_{x\in\mathbb{F}_q} |f(x)|^2 = \sum_{y\in\mathbb{F}_q} |\widehat{f}(y)|^2.$$

DÉMONSTRATION.

$$\begin{aligned}
\sum_{x\in\mathbb{F}_q} |f(x)|^2 &= \sum_{x\in\mathbb{F}_q} f(x)\overline{f(x)} = \sum_{x\in\mathbb{F}_q} f(x)\overline{\widehat{\widehat{f}}(-x)} \\
&= \sum_{x\in\mathbb{F}_q} f(x)\frac{1}{\sqrt{q}}\overline{\sum_{y\in\mathbb{F}_q} \widehat{f}(y)\psi(xy)} \\
&= \sum_{x\in\mathbb{F}_q} f(x)\frac{1}{\sqrt{q}} \sum_{y\in\mathbb{F}_q} \overline{\widehat{f}(y)}\psi(-xy).
\end{aligned}$$

En inversant l'ordre de sommation, nous avons

$$\begin{aligned}\sum_{x\in\mathbb{F}_q} f(x)\frac{1}{\sqrt{q}}\sum_{y\in\mathbb{F}_q}\overline{\hat{f}(y)}\psi(-xy) &= \sum_{y\in\mathbb{F}_q}\overline{\hat{f}(y)}\frac{1}{\sqrt{q}}\sum_{x\in\mathbb{F}_q} f(x)\psi(-xy)\\ &= \sum_{y\in\mathbb{F}_q}\overline{\hat{f}(y)}\hat{f}(y)\\ &= \sum_{y\in\mathbb{F}_q}|\hat{f}(y)|^2\end{aligned}$$

□

Bien que nous n'en n'avons pas discuter dans notre stratégie, nous aurons besoin de faire un peu de théorie sur les sommes de Gauss. Il s'agira simplement d'un cas particulier des transformées de Fourier

Définition 3.30. Soit χ un caractère multiplicatif sur $\mathbb{F}_q^*$ et posons $\chi(0) = 0$ pour étendre notre caractère à tous $\mathbb{F}_q$, on peut définir une somme de Gauss G comme une transformée de Fourier :

$$G_{\psi,\chi}(y) = \frac{1}{\sqrt{q}}\sum_{x\in\mathbb{F}_q}\chi(x)\psi(-xy).$$

On peut démontrer quelques propriétés pour $y \neq 0$.

Propriété 3.31.

$$G_{\psi,\chi}(y) = \chi(-y)^{-1}G_{\psi,\chi}(-1).$$

DÉMONSTRATION.

$$\begin{aligned}G_{\psi,\chi}(y) &= \frac{1}{\sqrt{q}}\sum_{x\in\mathbb{F}_q}\chi(x)\psi(-xy)\\ &= \frac{1}{\sqrt{q}}\sum_{x\in\mathbb{F}_q}\chi(-y)^{-1}\chi(-xy)\psi(-xy).\end{aligned}$$

En posant $z = xy$, on poursuit l'égalité de sorte que

$$\begin{aligned}\frac{1}{\sqrt{q}}\sum_{x\in\mathbb{F}_q}\chi(-y)^{-1}\chi(-xy)\psi(-xy) &= \frac{1}{\sqrt{q}}\sum_{z\in\mathbb{F}_q}\chi(-y)^{-1}\chi(-z)\psi(-z)\\ &= \frac{\chi(-y)^{-1}}{\sqrt{q}}\sum_{z\in\mathbb{F}_q}\chi(z)\psi(z)\\ &= \chi(-y)^{-1}G_{\psi,\chi}(-1).\end{aligned}$$

□

De ce lemme, on peut déduire que la transformée de Fourier de χ est égale à χ^{-1} à une constante près. Posons maintenant $\mathfrak{G}_\chi = \sqrt{q}G_{\psi,\chi}(-1)$.

Propriété 3.32.

$$|\mathfrak{G}_\chi| = \sqrt{q}$$

DÉMONSTRATION. On a que

$$\begin{aligned}
\sum_{x\in\mathbb{F}_q} |\chi(x)|^2 &= \sum_{x\in\mathbb{F}_q^\star} |\chi(x)|^2 \\
&= \sum_{y\in\mathbb{F}_q^\star} |\chi(-y)^{-1}G_{\psi,\chi}(-1)|^2 \\
&= \frac{|\mathfrak{G}_\chi|^2}{q} \sum_{y\in\mathbb{F}_q^\star} |\chi(-y)^{-1}|^2 \\
&= \frac{|\mathfrak{G}_\chi|^2}{q} \sum_{y\in\mathbb{F}_q} |\chi(-y)^{-1}|^2 \\
\implies \sum_{x\in\mathbb{F}_q} |\chi(x)|^2 &= \frac{|\mathfrak{G}_\chi|^2}{q} \sum_{y\in\mathbb{F}_q} |\chi(-y)^{-1}|^2
\end{aligned}$$

Ainsi, en utilisant le lemme (3.29) sur cette égalité, nous avons

$$|\mathfrak{G}_\chi| = \sqrt{q}$$

□

Propriété 3.33.

$$\mathfrak{G}_\chi\mathfrak{G}_{\chi^{-1}} = q\chi(-1)$$

DÉMONSTRATION. En ré-appliquant une deuxième fois la transformée de Fourier sur la propriété (3.31), on a

$$G_{\psi,\chi}(-1)G_{\psi,\chi^{-1}(-y)}(y) = \chi(y)G_{\psi,\chi}(-1)G_{\psi,\chi^{-1}}(-1).$$

Par la proposition (3.28), on a aussi que $G_{\psi,\chi}(-1)G_{\psi,\chi^{-1}(-y)}(y) = \chi(-y)$ puisqu'il s'agit de la transformée de Fourier appliquée deux fois. Alors, avec l'équation ci-dessus, on a

$$G_{\psi,\chi}(-1)G_{\psi,\chi^{-1}}(-1) = \chi(-1),$$

ce qui nous mène directement à :

$$\mathfrak{G}_\chi\mathfrak{G}_{\chi^{-1}} = \sqrt{q}G_{\psi,\chi}(-1)\sqrt{q}G_{\psi,\chi^{-1}}(-1) = q\chi(-1).$$

□

3.1.3. Somme des polynômes

On peut finalement s'attaquer au problème de ce chapitre qui est de trouver le nombre de solutions aux formes quadratiques dans $\mathbb{F}_q$. Considérons toujours que nous avons cette forme sur un espace quadratique (V, Q) et que Q est de dimension d.

Définition 3.34. Posons que

$$\nu_Q(x) = \#\{w \in V | Q(w) = x\}.$$

pour $x \in \mathbb{F}_q$. Nous pouvons remarquer que $\nu_Q(a)$ est exactement le résultat recherché soit le nombre de solutions d'une forme quadratique.

Définition 3.35. Posons également γ_Q, la transformée de Fourier de $\nu_Q(x)$

$$\gamma_Q(y) = \sum_{x \in \mathbb{F}_q} \nu_Q(x)\psi(-xy).$$

On a directement que

$$\gamma_Q(y) = \sum_{v \in V} \psi(-Q(v)y)$$

et donc, $\gamma_Q(0) = q^d$.

De ces définitions, on déduit directement la proposition suivante.

Proposition 3.36. *Si* $(V, Q) = (V_1, Q_1) \oplus (V_2, Q_2)$*, nous avons que*

$$\gamma_Q = \gamma_{Q_1}\gamma_{Q_2}.$$

DÉMONSTRATION.

$$\begin{aligned}
\gamma_{Q_1}(y)\gamma_{Q_2}(y) &= \sum_{v \in V_1} \psi(-Q_1(v)y) \sum_{v \in V_2} \psi(-Q_2(v)y) \\
&= \sum_{v_1 \in V_1, v_2 \in V_2} \psi(-(Q_1(v_1) + Q_2(v_2))y) \\
&= \sum_{v \in V} \psi(-Q(v)y) \\
&= \gamma_Q(y).
\end{aligned}$$

□

Nous allons maintenant calculer γ_Q pour les formes quadratiques $N_{\mathbb{F}_{q^2}/\mathbb{F}_q}$, H et cx^2. Ensuite, en utilisant le théorème (3.9) et la proposition (3.36), nous pourrons généraliser une équation pour n'importe quel γ_Q. Ensuite, à l'aide de la proposition (3.28) sur la double transformée de Fourier, nous pourrons trouver ν_Q pour toutes dimensions.

(1) Si $d = 1$, $Q(x) = cx^2$ et q est impair, on peut aisément calculer $\nu_Q(x)$

$$\nu_Q(x) = \begin{cases} 1 & \text{si } x = 0, \\ 2 & \text{si } x/c \text{ est un carré}, \\ 0 & \text{sinon.} \end{cases}$$

Pour simplifier la notation posons

$$sgn(x) = \begin{cases} 0 & \text{si } x = 0, \\ 1 & \text{si } x \text{ est un carré dans } \mathbb{F}_q^\star, \\ -1 & \text{si } x \text{ n'est pas un carré dans } \mathbb{F}_q^\star. \end{cases} \tag{3.1.10}$$

On peut maintenant ramener $\nu_Q(x)$ à

$$\nu_Q(x) = 1 + sgn(x/c).$$

Calculons maintenant γ_Q pour $y \neq 0$

$$\gamma_Q(y) = \sum_{z\in\mathbb{F}_q} \nu_Q(z)\psi(-zy) = \sum_{z\in\mathbb{F}_q} (1+sgn(z/c))\psi(-zy) = \sum_{z\in\mathbb{F}_q} sgn(z/c)\psi(-zy).$$

En posant $x = z/c$ et en utilisant les sommes de Gauss, nous avons

$$\sum_{z\in\mathbb{F}_q} sgn(z/c)\psi(-zy) = \sqrt{q}G_{\psi,sgn}(cy) = sgn(-cy)\sqrt{q}G_{\psi,sgn}(-1) = sgn(-cy)\mathfrak{G}_{sgn}.$$

Si $y = 0$,

$$\gamma_Q(0) = \sum_{x\in\mathbb{F}_q} \nu_Q(x) = q.$$

On peut réécrire

$$\gamma_Q(y) = \begin{cases} q & \text{si } y = 0, \\ sgn(-cy)\mathfrak{G}_{sgn} & \text{sinon.} \end{cases} \tag{3.1.11}$$

(2) Si $d = 1$, $Q(x) = cx^2$ et q est pair, on sait que tous les nombres sont des carrés et alors, $\nu_Q(x) = 1\ \forall x \in \mathbb{F}_q$. Ainsi,

$$\gamma_Q(y) = \sum_{x\in\mathbb{F}_q} \nu_Q(x)\psi(-xy) = \sum_{x\in\mathbb{F}_q} \psi(-xy) = \begin{cases} q & \text{si } y = 0, \\ \\ 0 & \text{sinon.} \end{cases} \tag{3.1.12}$$

(3) Si $d = 2$ et $Q = H$, il faut calculer $\nu_Q(x)$ manuellement. Pour $x = 0$, on cherche le nombre de solutions à l'hyperplan x_1x_2 tel que $x_1x_2 = 0$. Il faut donc que $x_1 = 0$ ou $x_2 = 0$, ce qui mène à $2q - 1$ solutions. Si $x \neq 0$, puisque nous sommes dans un corps, tous les éléments sauf zéro possèdent un inverse. Ainsi, on a $q - 1$ solutions. Cela implique donc que

$$\nu_Q(x) = \begin{cases} 2q-1 & \text{si } x = 0, \\ \\ q-1 & \text{sinon.} \end{cases}$$

On peut ainsi déduire que

$$\gamma_Q(y) = \sum_{x\in\mathbb{F}_q} \nu_Q(x)\psi(-xy) = 2q - 1 + (q-1)\sum_{x\in\mathbb{F}_q^\star} \psi(-xy).$$

Puisque $\psi(0) = 1$, on a $\sum_{x\in\mathbb{F}_q^\star} \psi(-xy) = -1$. On obtient

$$\gamma_Q(y) = \begin{cases} q^2 & \text{si } y = 0, \\ \\ q & \text{sinon.} \end{cases} \tag{3.1.13}$$

(4) Si $d = 2$ et $Q = N_{\mathbb{F}_{q^2}/\mathbb{F}_q}$, on peut encore calculer $\nu_q(x)$. Avec $N_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\alpha) = x$, nous avons

$$N_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\alpha) = \alpha\alpha^q = \alpha^{q+1} = x.$$

On voit que si $x = 0$, il existe une seule façon de choisir α. Si $x \neq 0$, il y a $q^2 - 1$ éléments dans $\mathbb{F}_{q^2}$ qui ne sont pas nuls. Puisque $N_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\alpha)$ est surjectif, que $q^2 - 1 = (q-1)(q+1)$ et qu'il y a $q - 1$ éléments non nuls dans $\mathbb{F}_q$, il y a donc $q + 1$ racines distinctes à $\alpha^{q+1} = x$. Ainsi, nous avons

$$\nu_Q(x) = \begin{cases} 1 & \text{si } x = 0, \\ \\ q+1 & \text{sinon.} \end{cases}$$

Maintenant, il est possible de calculer γ_Q.

$$\gamma_Q(y) = \sum_{x\in\mathbb{F}_q} \nu_Q(x)\psi(-xy) = 1 + (q+1)\sum_{x\in\mathbb{F}_q^\star} \psi(-xy) = \begin{cases} q^2 & \text{si } y = 0, \\ \\ -q & \text{sinon.} \end{cases} \tag{3.1.14}$$

Nous allons, à présent, faire le chemin inverse. Précédemment, nous utilisions des ν_Q simples pour calculer des γ_Q simples. Nous utiliserons dorénavant ces γ_Q simples pour trouver des ν_Q un peu plus compliqués. Pour ce faire, nous utiliserons le corollaire ci-dessous qui découle de la proposition (3.28).

Corollaire 3.37. *Sur* (V, Q)*, nous avons la relation suivante :*

$$\nu_Q(y) = \frac{1}{q}\sum_{x\in\mathbb{F}_q} \gamma_q(x)\psi(xy)$$

DÉMONSTRATION. On applique une nouvelle fois la transformée de Fourier à l'égalité $\gamma_Q(y) = \sum_{x\in\mathbb{F}_q} \nu_q(x)\psi(-xy)$ avec la proposition (3.28). □

Notons que grâce au théorème (3.9), pour calculer le nombre de solutions de n'importe quelles formes quadratiques, il nous faut seulement traiter les cas où $Q = nH$ et $Q = (n-1)H + N_{\mathbb{F}_{q^2}/\mathbb{F}_q}$ lorsque la dimension est paire et $Q = nH + cx^2$ lorsque la dimension est impaire.

(1) Si $d = 2n$ et $Q = nH$, par la proposition (3.36) et par l'équation (3.1.13), il est possible de calculer γ_Q :

$$\gamma_Q(y) = \begin{cases} q^{2n} & \text{si } y = 0, \\ \\ q^n & \text{sinon.} \end{cases}$$

Par le corollaire précédent, on a :

$$\nu_Q(y) = \frac{1}{q}\sum_{x\in\mathbb{F}_q} \gamma_Q(x)\psi(xy) = \frac{1}{q}(q^{2n} + q^n \sum_{x\in\mathbb{F}_q^\star} \psi(xy)) = \begin{cases} q^{2n-1} + q^n - q^{n-1} & \text{si } y = 0, \\ \\ q^{2n-1} - q^{n-1} & \text{sinon.} \end{cases}$$

(2) Si $d = 2n$ et $Q = (n-1)H + N_{\mathbb{F}_{q^2}/\mathbb{F}_q}$, par la proposition (3.36) et par les équations (3.1.13) et (3.1.14), on calcule γ_Q :

$$\gamma_Q(y) = \begin{cases} q^{2n} & \text{si } y = 0, \\ \\ -q^n & \text{sinon.} \end{cases}$$

Donc, par le corollaire (3.37) :

$$\nu_Q(y) = \frac{1}{q}\sum_{x\in\mathbb{F}_q}\gamma_Q(x)\psi(xy) = \frac{1}{q}(q^{2n} - q^n\sum_{x\in\mathbb{F}_q^\star}\psi(xy)) = \begin{cases} q^{2n-1} - q^n + q^{n-1} & \text{si } y = 0, \\ \\ q^{2n-1} + q^{n-1} & \text{sinon.} \end{cases}$$

On peut maintenant montrer le théorème (3.3) pour l'équation (3.1.3). On sait que pour les dimensions paires, toutes les formes quadratiques peuvent être ramenées aux deux derniers cas. Or, le corollaire (3.21), nous dit que les formes quadratiques de dimension $2n$ sont caractérisées par leur déterminant, à savoir s'ils sont des carrés ou non dans $\mathbb{F}_q$. On peut conclure que pour tous $a \in \mathbb{F}_q$:

$$\nu_Q(a) = q^{2n-1} - l(a)\left(\frac{\det(M)(-1)^n}{q}\right)q^{n-1}.$$

où

$$l(a) = \begin{cases} 1 & \text{si } a \neq 0, \\ \\ 1-q & \text{si } a = 0. \end{cases}$$

(3) Si $d = 2n+1$, $Q = nH + cx^2$ et q est impair, par la proposition (3.36) et par les équations (3.1.11) et (3.1.13), il est aisé de calculer γ_Q

$$\gamma_Q(y) = \begin{cases} q^{2n+1} & \text{si } y = 0, \\ \\ q^n sgn(-cy)\mathfrak{G}_{sgn} & \text{sinon.} \end{cases}$$

Calculons ν_Q à l'aide du corollaire (3.37)

$$\nu_Q(y) = \frac{1}{q}\sum_{x\in\mathbb{F}_q}\gamma_Q(x)\psi(xy) = \frac{1}{q}(q^{2n+1} + q^n\mathfrak{G}_{sgn}\sum_{x\in\mathbb{F}_q^\star} sgn(-cx)\psi(xy)).$$

Si $y = 0$, nous avons

$$\frac{1}{q}(q^{2n+1} + q^n\mathfrak{G}_{sgn}\sum_{x\in\mathbb{F}_q^\star} sgn(0)\psi(0)) = q^{2n}.$$

Si $y \neq 0$, grâce aux propriétés (3.31) et (3.33), on voit que

$$\begin{aligned} \frac{1}{q}(q^{2n+1} + q^n\mathfrak{G}_{sgn}\sum_{x\in\mathbb{F}_q^\star} sgn(-cx)\psi(xy)) &= q^{2n} + q^{n-1}\mathfrak{G}_{sgn}\frac{\sqrt{q}}{\sqrt{q}}\sum_{x\in\mathbb{F}_q} sgn(-cx)\psi(xy) \\ &= q^{2n} + q^{n-1}\mathfrak{G}_{sgn}sgn(-cy)\sqrt{q}G_{\psi,sgn}(-1) \\ &= q^{2n} + q^{n-1}sgn(-cx)\mathfrak{G}_{sgn}\mathfrak{G}_{sgn} \\ &= q^{2n} + q^n sgn(cx). \end{aligned}$$

On peut réécrire le tout de la façon suivante :

$$\nu_Q(y) = \begin{cases} q^{2n} & \text{si } y = 0, \\ \\ q^{2n} + q^n sgn(cy) & \text{sinon.} \end{cases}$$

De ce résultat, on peut maintenant montrer (3.1.4). Par le corollaire (3.22), on sait que $c = \det(M)(-1)^n$. Donc, on a

$$\nu_Q(a) = q^{2n} + q^n \left(\frac{a \det(M)(-1)^n}{q} \right).$$

pour $\forall a \in \mathbb{F}_q$.

(4) Si $d = 2n + 1$, $Q = nH + x^2$ et q est pair, nous pouvons calculer γ_Q à l'aide de la proposition (3.36) et des équations (3.1.12) et (3.1.13). On déduit alors que

$$\gamma_Q(y) = \begin{cases} q^{2n+1} & \text{si } y = 0, \\ \\ 0 & \text{sinon.} \end{cases}$$

On peut calculer ν_Q en utilisant, encore une fois, le corollaire (3.37) :

$$\nu_Q(y) = \frac{1}{q} \sum_{x \in \mathbb{F}_q} \gamma_Q(y)\psi(-xy) = \frac{1}{q}(q^{2n+1} + \sum_{x \in \mathbb{F}_q^\star} 0\psi(-xy)) = q^{2n},$$

ce qui montre directement (3.1.5) et par la même occasion, cela complète la démonstration du théorème 3.3 .

Chapitre 4

FORMULES FIXANT DEUX COEFFICIENTS

Nous sommes désormais prêt à nous attaquer au résultat de Kuz'min (3.0.8). Pour ce faire, nous devons encore nous munir d'une nouvelle notation.

Définition 4.1. Notons $P_n(a)$ l'ensemble des polynômes pas nécessairement irréductibles de la forme (3.0.7) sur $\mathbb{F}_q$.

Définition 4.2. Considérons $H_n(a)$ le nombre de polynômes irréductibles de $P_n(a)$.

Définition 4.3. Prenons aussi $N_i(a)$ le nombre de polynômes de $P_n(a)$ qui possèdent i différentes racines.

Nous devons aussi nous doter d'une notation pour discuter du nombre de polynômes qui ont un certain type de factorisation. Par exemple, si la factorisation d'un polynôme est $(x-\alpha)^2(x-\beta)$ avec $\alpha, \beta \in \mathbb{F}_q$ et $\alpha \neq \beta$, il sera considéré de la forme $(1^2, 1)$. Tandis que si la factorisation irréductible d'un polynôme est $(x^2 + \alpha x + \beta)(x - \gamma)$ avec $\alpha, \beta, \gamma \in \mathbb{F}_q$, il sera de la forme $(2, 1)$. Lorsque que nous écrirons $X_{(2,1)}(a)$, nous voudrons ainsi parler du nombre de polynômes dans $P_n(a)$ qui ont la factorisation $(2, 1)$.

Dans la prochaine section, nous allons donner les détails pour calculer manuellement $H_4(a)$. Le but de cette section est de montrer intuitivement la provenance du théorème suivant.

Théorème 4.4. *Si* $H_{n,d}(a)$ *est le nombre de polynômes dans* $P_n(a)$ *de la forme* $X_{(d^m)}(a)$ *avec* $dm = n$*, nous avons que*

$$\sum_{d|n} dH_{n,d}(a) = q^{n-2} + (-1)^n(q^{n-2} - Q_{n-1}(-a)), \tag{4.0.15}$$

où Q_n *est le nombre de solutions de* (3.1.2).

Remarque 4.5. En prenant $(x_1, x_2 \cdots, x_n)$ les racines d'un polynôme de la forme $P_n(a)$, nous avons le polynôme $(x - x_1)(x - x_2) \cdots (x - x_n)$ tel que

$$a = -\sum_{1 \leq i < n} x_i^2 - \sum_{1 \leq i < j < n} x_i x_j.$$

Puisque les racines ne sont pas nécessairement distinctes, ce polynôme est de la forme $(1^{e_1}, \ldots, 1^{e_k})$ avec $0 \leq e_i \leq n$. Puisqu'il existe $\frac{n!}{e_1! \cdots e_k!}$ façons de permuter les racines, en considérant tous les polynômes qui ont une factorisation du type $(1^{e_1}, \ldots, 1^{e_k})$, on remarque qu'il existe $\frac{n!}{e_1! \cdots e_k!} X_{(1^{e_1}, \ldots, 1^{e_k})}(a)$ façons de trouver une forme quadratique comme illustrée ci-haut. En sommant tous les types de factorisation possible, nous trouvons

$$\sum_{e_1 + \cdots + e_k = n} \frac{n!}{e_1! \cdots e_k!} X_{(1^{e_1}, \ldots, 1^{e_k})}(a) = Q_{n-1}(a).$$

Le théorème (4.4) est le résultat le plus important de ce mémoire. De ce résultat, nous pourrons montrer (3.0.8). Nous donnerons la preuve dans une prochaine section.

4.1. Détails du cas où $n = 4$

Nous donnerons ici les détails pour calculer le cas $H_4(a)$.

Lemme 4.6. *Si* $p \neq 2$ *et* $a \neq 0$, *nous avons alors :*

$$H_4(a) = \frac{1}{4}\left(q^2 - \left(\frac{-2a}{q}\right) q + \left(\frac{2a}{q}\right) - 1\right), \tag{4.1.1}$$

et si $p = 2$

$$H_4(a) = \frac{1}{4} q \left(q + \left(\frac{q}{3}\right) - 1\right), \tag{4.1.2}$$

où $\left(\frac{a}{q}\right)$ *est le caractère quadratique sur* $\mathbb{F}_q$.

Démonstration. Puisque $H_4(a) = X_{(4)}(a)$, que $H_{4,1}(a) = X_{(1^4)}(a)$ et que $H_{4,2}(a) = X_{(2^2)}(a)$, on voit que le théorème (4.4) devient

$$X_{(1^4)}(a) + 2X_{(2^2)}(a) + 4X_{(4)}(a) = 2q^2 - \sum_{e_1 + \cdots + e_k = 4} \frac{24}{e_1! \cdots e_4!} X_{(1^{e_1}, \ldots, 1^{e_4})}(a).$$

Notre plan pour cette démonstration sera donc de combiner un certain nombre d'équations qui contiennent des $X_{(\text{quelconque})}(a)$ pour arriver à cette dernière égalité.

Remarquons donc que dans $P_4(a)$, il existe q^2 polynômes différents et que la

somme des $N_i(a)$ est le nombre total de polynômes. En résumé, nous avons que

$$N_0(a) + N_1(a) + N_2(a) + N_3(a) + N_4(a) = q^2. \tag{4.1.3}$$

Maintenant, intéressons-nous au nombre de polynômes qui possèdent au moins une racine dans $\mathbb{F}_q$. Nous allons faire le compte de deux façons différentes. D'abord, on remarque qu'il existe également q^2 polynômes, car le choix de la racine fixera un des coefficients dans $P_4(a)$ et l'autre restera libre. On peut également compter ces polynômes en utilisant les $N_i(a)$. Effectivement, on remarque que le nombre de polynômes dans $P_4(a)$ avec au moins une racine est donné par les sommations ci-dessous.

$$\sum_{i=1}^{4} \sum_{f \in N_i(a)} \sum_{\substack{\rho \in \mathbb{F}_q \\ t.q.\, f(\rho)=0}} 1 = \sum_{i=1}^{4} \binom{i}{1} N_i(a)$$

Ainsi, nous concluons que

$$\binom{1}{1} N_1(a) + \binom{2}{1} N_2(a) + \binom{3}{1} N_3(a) + \binom{4}{1} N_4(a) = q^2. \tag{4.1.4}$$

On répète la même opération, mais en fixant deux racines distinctes. On peut voir qu'il existe $q(q-1)/2$ polynômes de $P_4(a)$. Le choix des deux racines fixera les coefficients, mais puisqu'ils sont distincts, on a q choix pour le premier et $(q-1)$ pour le deuxième. Évidemment, il faut diviser par deux pour éviter de compter les répétitions. On peut encore compter ces polynômes en utilisant les $N_i(a)$. Effectivement, on remarque que le nombre de polynômes dans $P_4(a)$ avec au moins deux racines distinctes est donné par les sommations ci-dessous.

$$\sum_{i=2}^{4} \sum_{f \in N_i(a)} \sum_{\substack{\rho, \alpha \in \mathbb{F}_q \\ t.q.\, f(\rho)=0 \text{ et } f(\alpha)=0}} 1 = \sum_{i=2}^{4} \binom{i}{2} N_i(a)$$

Ainsi, nous concluons que

$$\binom{2}{2} N_2(a) + \binom{3}{2} N_3(a) + \binom{4}{2} N_4(a) = \frac{q(q-1)}{2}. \tag{4.1.5}$$

En additionnant (4.1.3), (4.1.4), (4.1.5) avec une alternance de signes et en utilisant la formule du binôme alterné, on conclut que

$$N_0(a) + N_3(a) + 3N_4(a) = \frac{q(q-1)}{2}.$$

Si on transfert la notation $N_i(a)$ en $X_i(a)$, on obtient que

$$X_{(2^2)}(a) + X_{(2,2)}(a) + X_{(4)}(a) + X_{(1^2,1,1)}(a) + 3X_{(1,1,1,1)}(a) = \frac{q(q-1)}{2}. \tag{4.1.6}$$

Respectivement, les trois équations suivantes seront le nombre de polynômes qui comportent $(2), (1,1), (1^2)$ dans leur factorisation :

$$X_{(2,1,1)}(a) + 2X_{(2,2)}(a) + X_{(2^2)}(a) + X_{(2,1^2)}(a) = \frac{q(q-1)}{2}, \tag{4.1.7}$$

$$X_{(2,1,1)}(a) + 6X_{(1,1,1,1)}(a) + 3X_{(1^2,1,1)}(a) + X_{(1^2,1^2)}(a) + X_{(1^3,1)}(a) = \frac{q(q-1)}{2}, \tag{4.1.8}$$

$$X_{(1^4)}(a) + X_{(2,1^2)}(a) + X_{(1^2,1,1)}(a) + 2X_{(1^2,1^2)}(a) + X_{(1^3,1)}(a) = q. \tag{4.1.9}$$

En faisant $2 * (2 * (4.1.6) - (4.1.7) + (4.1.8) + (4.1.9))$, on obtient que

$$X_{(1^4)}(a) + 2X_{(2^2)}(a) + 4X_{(4)}(a) + \sum_{e_1+\cdots+e_k=4} \frac{24}{e_1! \cdots e_4!} X_{(1^{e_1},\ldots,1^{e_4})}(a) = 2q^2. \tag{4.1.10}$$

De la remarque (4.5), on sait que

$$\sum_{e_1+\cdots+e_k=4} \frac{24}{e_1! \cdots e_4!} X_{(1^{e_1},\ldots,1^{e_4})}(a) = Q_3(a).$$

Remarque 4.7. Notons que l'équation (4.1.10) correspond exactement au théorème (4.4).

On peut voir que nous sommes exactement dans les conditions du théorème (3.3). Nous allons donc calculer $Q_3(a)$. Puisque $\det(M) = \frac{1}{2}$ et que ce cas est non-dégénéré pour $p \neq 2$, nous pouvons conclure que $Q_3(a) = q^2 - \left(\frac{-2a}{q}\right) q$. Pour calculer $2X_{(2^2)}(a)$, on remarque que le seul polynôme qui satisfait la factorisation (2^2) est $(x^2 - \frac{a}{2})^2$. Pour être irréductible, $\frac{a}{2}$ ne doit pas être un carré. On obtient ainsi

$$2X_{(2^2)}(a) = 1 - \left(\frac{a/2}{q}\right) = 1 - \left(\frac{2a}{q}\right)$$

On remarque aussi que $X_{(1^4)}(a) = 0$. En remplaçant ces derniers résultats dans (4.1.10), nous trouvons (4.1.1).

Pour le cas $p = 2$, nous sommes dans un cas dégénéré. Or, nous sommes en caractéristique 2 et nous avons l'égalité suivante :

$$x_1^2 + x_2^2 + x_3^2 + x_1x_2 + x_1x_3 + x_2x_3 = (x_1 + x_2)^2 + (x_1 + x_2)(x_1 + x_3) + (x_1 + x_3)^2.$$

Avec le changement de variable $t_1 = x_1 + x_2$ et $t_2 = x_1 + x_3$, on trouve que notre forme quadratique est en fait

$$t_1^2 + t_1t_2 + t_2^2.$$

Ainsi, puisque le terme t_3 est laissé libre, on déduit que le terme Q_3 de l'équation (4.1.10) est en fait qQ_2. Puisque $\det(M) = \frac{3}{4}$ et $d = 2$, on trouve, en accord avec le théorème (3.3), que $qQ_2 = q(q - \left(\frac{q}{3}\right))$. Pour compléter la preuve, il nous reste à trouver la valeur de $2X_{(2^2)}(a)$. Les polynômes qui satisfont la factorisation (2^2) sont ceux de la forme $(x^2 + \alpha x + \beta)$. Pour être de la forme (3.0.7), il existe une seule façon de choisir α, soit $\alpha = 0$. Ainsi, il existe au total q polynômes de cette forme . Si $(x^2 + \beta)$ est réductible, alors il est égal à $(x + \delta)(x - \delta)$ pour $\delta \in \mathbb{F}_q$, ce qui nous permet de déduire que nous avons alors $\frac{q}{2}$ façons différentes de choisir δ et donc, autant de polynômes réductibles. Puisque nous avons q polynômes au total, nous avons $\frac{q}{2}$ polynômes irréductibles, ce qui nous indique que $2X_{(2^2)}(a) = q$. En considérant (4.1.10), nous pouvons conclure que (4.1.2) est vrai. □

4.2. Preuve de du théorème 3.0.8 et généralisation du résultat

Les cas $n = 5, 6, 7$ sont tout à fait analogues à celui où $n = 4$. En regardant toutes ces preuves dans l'article de Kuz'min, on peut remarquer qu'il réussit toujours à exprimer les $X_{(n)}(a)$ en fonction des polynômes qui se factorisent complètement et des polynômes de la forme $X_{(d^m)}(a)$ où $dm = n$ (comme illustrée à la ligne (4.1.10)). De façon plus précise, on conclut que le théorème (4.4) devrait être la généralisation de notre résultat. Cette démonstration sera faite prochainement. Pour l'instant, considérons que ce théorème est vrai afin de démontrer le théorème 3.0.8. Pour ce faire, nous allons montrer le lemme suivant.

Lemme 4.8. *Si* $G_n(a)$ *est défini comme en* (3.0.9) *pour* $p \nmid n$ *ou comme en* (3.0.10) *si* $p \mid n$, *nous avons que*

$$\sum_{d|n} dH_{n,d}(a) = G_n(-a).$$

Remarque 4.9. Pour montrer le théorème 3.0.8, nous n'aurons qu'à appliquer l'inversion de Mobius sur ce lemme.

Démonstration. Pour montrer le résultat, il suffit d'appliquer le théorème (3.3) au théorème (4.4). Pour utiliser (3.3), nous aurons besoin de montrer que le déterminant de la matrice de l'équation quadratique (3.1.2), de dimension n, est $(n + 1)\left(\frac{1}{2}\right)^n$. Pour ce faire, nous ferons une preuve par induction. Notons M_n la matrice de la forme quadratique (3.1.2) de dimension n. On remarque que cette matrice à des 1 sur la diagonal et des 1/2 ailleurs. Si $n = 2$, on calcule facilement que $\det(M_2) = 3/4$. Prenons comme hypothèse d'induction que

$\det(M_n) = (n+1)\left(\frac{1}{2}\right)^n$. Ainsi, on obtient

$$\det(M_{n+1}) = \overbrace{\begin{vmatrix} 1 & 1/2 & 1/2 & \dots & 1/2 \\ 1/2 & 1 & 1/2 & \dots & 1/2 \\ 1/2 & 1/2 & \ddots & & 1/2 \\ \vdots & \vdots & & & \vdots \\ 1/2 & 1/2 & 1/2 & \cdots & 1 \end{vmatrix}}^{n+1}.$$

En faisant l'opération sur les colonnes $C_1 = C_1 - C_2$, on a

$$\det(M_{n+1}) = \begin{vmatrix} 1/2 & 1/2 & 1/2 & \dots & 1/2 \\ -1/2 & 1 & 1/2 & \dots & 1/2 \\ 0 & 1/2 & \ddots & & 1/2 \\ \vdots & \vdots & & & \vdots \\ 0 & 1/2 & 1/2 & \cdots & 1 \end{vmatrix}.$$

Avec le développement de Leibniz de la première colonne, nous avons que

$$\det(M_{n+1}) = \frac{1}{2}\overbrace{\begin{vmatrix} 1 & 1/2 & 1/2 & \dots & 1/2 \\ 1/2 & 1 & 1/2 & \dots & 1/2 \\ 1/2 & 1/2 & \ddots & & 1/2 \\ \vdots & \vdots & & & \vdots \\ 1/2 & 1/2 & 1/2 & \cdots & 1 \end{vmatrix}}^{n} + \frac{1}{2}\overbrace{\begin{vmatrix} 1/2 & 1/2 & 1/2 & \dots & 1/2 \\ 1/2 & 1 & 1/2 & \dots & 1/2 \\ 1/2 & 1/2 & \ddots & & 1/2 \\ \vdots & \vdots & & & \vdots \\ 1/2 & 1/2 & 1/2 & \cdots & 1 \end{vmatrix}}^{n}.$$

En utilisant notre hypothèse d'induction dans notre première matrice et en faisant les opérations sur les lignes $L_i = L_i - L_1$ pour $2 \leq i \leq n$ dans la deuxième

matrice , nous avons que

$$\begin{aligned}\det(M_{n+1}) &= \frac{1}{2}(n+1)\left(\frac{1}{2}\right)^n + \frac{1}{2}\begin{vmatrix} 1/2 & 1/2 & 1/2 & \dots & 1/2 \\ 0 & 1/2 & 0 & \dots & 0 \\ 0 & 0 & \ddots & & 0 \\ \vdots & \vdots & & & \vdots \\ 0 & 0 & 0 & \cdots & 1/2 \end{vmatrix} \\ &= (n+1)\left(\frac{1}{2}\right)^{n+1} + \frac{1}{2}\left(\frac{1}{2}\right)^n \\ &= (n+2)\left(\frac{1}{2}\right)^{n+1},\end{aligned}$$

concluant ainsi l'étape inductive.

D'ici, nous supposerons que M_{n-1} est non-dégénéré, c'est-à-dire que : la caractéristique ne divise pas n et la caractéristique n'est pas deux. À l'aide du théorème (3.3), nous allons réécrire la partie de droite dans l'équation du théorème (4.4). Pour ce faire, il faut diviser le cas où n est pair de celui où n est impair. Commençons par le cas impair et remplaçons $n = 2m+1$ dans (4.4) :

$$\sum_{d|n} dH_{n,d}(a) = q^{2m+1-2} + (-1)^{2m+1}(q^{2m+1-2} - Q_{2m+1-1}) = Q_{2m}.$$

En utilisant (3.1.3), on a

$$\begin{aligned}Q_{2m} &= q^{2m-1} - l(a)\left(\frac{\det(M_{n-1})(-1)^m}{q}\right)q^{m-1} \\ &= q^{2m-1} - l(a)\left(\frac{n(1/2)^{n-1}(-1)^m}{q}\right)q^{m-1} \\ &= q^{n-2} - l(a)\left(\frac{(-1)^m n}{q}\right)q^{m-1}.\end{aligned}$$

On peut noter que cette égalité correspond exactement au cas impair de $G_n(a)$. Procédons maintenant avec le cas pair. Nous procèderons de la même façon en remplaçant $n = 2m$ dans (4.4) :

$$\sum_{d|n} dH_{n,d}(a) = q^{2m-2} + (-1)^{2m}(q^{2m-2} - Q_{2m-1}) = 2q^{2m-2} + Q_{2(m-1)+1}.$$

En utilisant (3.1.4), on obtient :

$$\begin{aligned}
2q^{2m-2} + Q_{2(m-1)+1} &= 2q^{2m-2} - (q^{2(m-1)} - \left(\frac{a\det(M_{n-1})(-1)^{m-1}}{q}\right) q^{m-1}) \\
&= q^{2m-2} + \left(\frac{a(-1)^{m-1}2m(1/2)^{2m-1}}{q}\right) q^{m-1}) \\
&= q^{n-2} + \left(\frac{(-1)^{m-1}ma}{q}\right) q^{m-1}.
\end{aligned}$$

On peut noter que cette égalité correspond exactement au cas pair de $G_n(a)$.

Traitons maintenant les cas dégénérés. On sait que le déterminant de la matrice de la forme quadratique M_{n-1} est $n(\frac{1}{2})^{n-1}$. Ainsi, on voit qu'elle est dégénérée lorsque la caractéristique divise n ou si elle divise 2. Puisque nous ne traiterons pas le cas où la caractéristique divise 2, nous supposerons que $p \neq 2$. Pour continuer nos calculs, nous allons transformer notre forme quadratique à l'aide de quelques manipulations algébriques et d'un changement de variable. Ces transformations permettront d'obtenir une forme quadratique de dimension inférieure non-dégénérée. Commençons par remarquer que

$$\begin{aligned}
\sum_{i=1}^{n-1} x_i^2 + \sum_{1\leq i<j\leq n-1} x_i x_j &= \sum_{i=1}^{n-1} x_i^2 + \sum_{i=1}^{n-2}\sum_{j=i+1}^{n-1} x_i x_j \\
&= \sum_{i=1}^{n-1} x_i \sum_{j=i}^{i} x_j + \sum_{i=1}^{n-2} x_i \sum_{j=i+1}^{n-1} x_j \\
&= \sum_{i=1}^{n-2} x_i \sum_{j=i}^{i} x_j + x_{n-1}^2 + \sum_{i=1}^{n-2} x_i \sum_{j=i+1}^{n-1} x_j \\
&= \sum_{i=1}^{n-2} x_i \left(\sum_{j=i}^{i} x_j + \sum_{j=i+1}^{n-1} x_j\right) + x_{n-1}^2 \\
&= \sum_{i=1}^{n-2} x_i \sum_{j=i}^{n-1} x_j + x_{n-1}^2 \\
&= \sum_{i=1}^{n-2} x_i \left(\left(\sum_{j=i}^{n-2} x_j\right) + x_{n-1}\right) + x_{n-1}^2
\end{aligned}$$

Maintenant, faisons le changement de variable $x_i = t_i + t_{n-1}$ pour $1 \leq i \leq n-2$ et $x_{n-1} = t_{n-1}$. Ainsi, nous avons que

$$\sum_{i=1}^{n-2} x_i \left(\left(\sum_{j=i}^{n-2} x_j \right) + x_{n-1} \right) + x_{n-1}^2 = \sum_{i=1}^{n-2} \left((t_i + t_{n-1}) \left(\left(\sum_{j=i}^{n-2} t_j \right) + (n-i)t_{n-1} \right) \right) + t_{n-1}^2$$

$$= \sum_{i=1}^{n-2} \sum_{j=i}^{n-2} t_i t_j + \sum_{i=1}^{n-2} (n-i) t_i t_{n-1} + \sum_{i=1}^{n-2} \sum_{j=i}^{n-2} t_j t_{n-1} + \sum_{i=1}^{n-2} (n-i) t_{n-1}^2 + t_{n-1}^2$$

$$= \sum_{i=1}^{n-2} \sum_{j=i}^{n-2} t_i t_j + \sum_{i=1}^{n-2} (n-i) t_i t_{n-1} + \sum_{i=1}^{n-2} i t_i t_{n-1} + \sum_{i=1}^{n-1} (n-i) t_{n-1}^2$$

$$= \sum_{i=1}^{n-2} \sum_{j=i}^{n-2} t_i t_j + \sum_{i=1}^{n-2} ((n-i) t_i t_{n-1} + i t_i t_{n-1}) + \sum_{i=1}^{n-1} t_{n-1}^2$$

$$= \sum_{i=1}^{n-2} \sum_{j=i}^{n-2} t_i t_j + n \sum_{i=1}^{n-2} t_i t_{n-1} + \frac{n(n-1)}{2} t_{n-1}^2.$$

Puisque $p \neq 2$ et $p|n$, on trouve que

$$\sum_{i=1}^{n-2} \sum_{j=i}^{n-2} t_i t_j + n \sum_{i=1}^{n-2} t_i t_{n-1} + \frac{n(n-1)}{2} t_{n-1}^2 = \sum_{i=1}^{n-2} \sum_{j=i}^{n-2} t_i t_j.$$

Maintenant, on déduit que le déterminant de cette nouvelle forme quadratique est $(n-1)(\frac{1}{2})^{n-2}$ et on voit que ce cas n'est plus dégénéré. On remarque aussi qu'il s'agit du même type de forme quadratique que (3.1.2), mais la dimension a diminué de 1. Avec cette information et en considérant qu'un coefficient sera laissé libre dans notre changement de variable, nous avons que

$$Q_n = qQ_{n-1} \tag{4.2.1}$$

Revenons maintenant au théorème 4.4. Avec nos nouvelles constatations, nous allons à nouveau manipuler la partie de droite dans l'équation de ce théorème. Cependant, nous devrons encore séparer le cas où la dimension est paire de celui où elle est impaire. Ici, supposons que la dimension est impaire, soit $n = 2m+1$. On calcule ainsi que

$$\sum_{d|n} dH_{n,d}(a) = q^{2m+1-2} + (-1)^{2m+1}(q^{2m+1-2} - Q_{2m+1-1}) = Q_{2m}.$$

En utilisant (4.2.1), le théorème (3.1.4) et le fait que $p \mid n$, nous pouvons voir que

$$\begin{aligned} Q_{2m} &= qQ_{2(m-1)+1} \\ &= q(q^{2(m-1)} + \left(\frac{a\det(M_{n-2})(-1)^{m-1}}{q}\right) q^{m-1}) \\ &= q(q^{2(m-1)} + \left(\frac{a(n-1)(1/2)^{n-2}(-1)^{m-1}}{q}\right) q^{m-1}) \\ &= q^{n-2} + \left(\frac{2a(-1)^m}{q}\right) q^m, \end{aligned}$$

ce qui est le résultat attendu. Regardons maintenant le cas où $n = 2m$ dans la partie de droite de l'équation du théorème (4.4).

$$\sum_{d|n} dH_{n,d}(a) = q^{2m-2} + (-1)^{2m}(q^{2m-2} - Q_{2m-1}) = 2q^{2m-2} - Q_{2m-1}.$$

En utilisant (4.2.1), le théorème 3.1.3 et le fait que $p \mid n$,, on arrive a

$$\begin{aligned} 2q^{2m-2} - Q_{2m-1} &= 2q^{2m-2} - qQ_{2(m-1)} \\ &= 2q^{2m-2} - q(q^{2(m-1)-1} - l(a)\left(\frac{\det(M_{n-2})(-1)^{m-1}}{q}\right) q^{m-2}) \\ &= q^{2m-2} + l(a)\left(\frac{(n-1)(1/2)^{n-2}(-1)^{m-1}}{q}\right) q^{m-1}) \\ &= q^{n-2} + l(a)\left(\frac{(-1)^m}{q}\right) q^{m-1}. \end{aligned}$$

Ainsi, dans tous les cas, nous concluons que

$$\sum_{d|n} dH_{n,d}(a) = G_n(-a).$$

□

Finalement, nous allons montrer le théorème 3.0.8.

PREUVE DE 3.0.8. Pour y arriver nous allons faire quelques manipulations sur $H_{n,d}(a)$ afin de pouvoir appliquer l'inversion de Mobius sur le lemme 4.8.

Nous allons voir que $H_{n,d}(a) = H_d(\frac{da}{n})$. En effet, en posant $\overline{X}_{(d)}(a_1)$ le nombre de polynômes de la forme $x^d + a_1x^{d-2} + \cdots + a_n$ et en sachant déjà que $X_{(d^m)}(a)$ est le nombre de polynômes $P_n(a)$, on déduit que

$$x^n + ax^{n-2} + t_1x^{n-3} + \cdots + t_{n-2} = (x^d + a_1x^{d-2} + \cdots + a_n)^m.$$

Ainsi, $\overline{X}_{(d)}(a_1)$ définit $X_{(d^m)}(a)$ pour a_1 bien choisi. En développant l'exposant m, on déduit que $ma_1 = a$ avec $dm = n$. De cette façon, on conclut que si $a_1 = \frac{ad}{n}$, nous avons que $H_{n,d}(a) = H_d(\frac{da}{n})$. Il s'en suit de (4.8) que

$$\sum_{d|n} dH_d(\frac{ad}{n}) = G_n(-a).$$

En appliquant simplement l'inversion de Mobius sur la dernière égalité, on trouve le résultat attendu qui est

$$H_n(a) = \frac{1}{n} \sum_{\substack{d|n \\ p\nmid d}} \mu(d) G_{n/d}(-a/d).$$

□

4.2.1. a_1 et a_2 fixé

Il est possible de généraliser le précédent résultat pour les polynômes de la forme (0.0.1) avec a_1 et a_2 fixés. Posons $H_n(a_1, a_2)$ le nombre de polynômes irréductibles de la forme (0.0.1) avec les termes a_1 et a_2 fixés. Si $p \nmid n$, on peut faire le changement de variable suivant $x_1 = x + \frac{a_1}{n}$ qui nous permet de déduire que

$$H_n(a_1, a_2) = H_n\left(0, a_2 - \frac{n-1}{2n} a_1^2\right).$$

Notons que ce résultat est exactement le théorème que nous venons de démontrer à la dernière section. Si $p \mid n$ et $a_1 \neq 0$ avec $x_1 = \frac{1}{a_1}\left(x - \frac{a_2}{a_1}\right)$, nous avons

$$H_n(a_1, a_2) = H_n(1, 0).$$

Pour résoudre ce cas, nous allons utiliser les résultats (2.3), (2.6) et (2.19) résumés ci-dessous. L'écriture est un peu différente, mais elle en est équivalente.

$$N(n, q) = \frac{1}{n} \sum_{d|n} \mu(d) q^{n/d} \tag{4.2.2}$$

$$N_a(n, q) = \begin{cases} \frac{1}{qn} \sum_{\substack{d|n \\ p\nmid d}} \mu(d) q^{n/d} & a \neq 0, \\ \\ \frac{1}{qn} \sum_{\substack{d|n \\ p\nmid d}} \mu(d) q^{n/d} - \frac{\varepsilon}{n} \sum_{\substack{d|n \\ p\nmid d}} \mu(d) q^{n/dp} & a = 0, \end{cases} \tag{4.2.3}$$

où $\varepsilon = 1$ si $p \mid n$ et 0 sinon. Ainsi, on peut déduire que si $p \mid n$, nous avons

$$\begin{aligned} N(n,q) = \sum_{a_1,a_2} H_n(a_1,a_2) &= \sum_{a_1\neq 0,a_2} H_n(a_1,a_2) + \sum_{a_2} H_n(0,a_2) \\ &= (q-1)qH_n(1,0) + N_0(n,q) \\ &= (q-1)qH_n(1,0) + N(n,q) - (q-1)N_1(n,q). \end{aligned}$$

Ainsi, nous concluons que

$$\begin{aligned} H_n(1,0) &= \frac{1}{q}N_1(n,q) \\ &= \frac{1}{q^2 n}\sum_{\substack{d\mid n \\ p\nmid d}} \mu(d)q^{n/d}. \end{aligned}$$

Pour compléter tous les cas possibles, il nous resterait le cas $H_n(0,0)$. On peut voir que

$$\begin{aligned} H_n(0,0) &= N_0(n,q) - \sum_{a\neq 0} H_n(0,a) \\ &= \frac{1}{qn}\sum_{\substack{d\mid n \\ p\nmid d}} \mu(d)q^{n/d} - \frac{\varepsilon}{n}\sum_{\substack{d\mid n \\ p\nmid d}} \mu(d)q^{n/dp} - \frac{1}{n}\sum_{\substack{d\mid n \\ p\nmid d}} \mu(d)\sum_{a\neq 0} G_{n/d}(-a/d). \end{aligned} \tag{4.2.4}$$

En remarquant que

$$\begin{aligned} \sum_{a\in\mathbb{F}_q^\star} G_{n/d}(-a/d) &= \sum_{a\in\mathbb{F}_q} G_{n/d}(-a/d) - G_{n/d}(0) \\ &= \sum_{a\in\mathbb{F}_q} \left(q^{n/d-2} + (-1)^{n/d}(q^{n/d-2} - Q_{n/d-1}(-a))\right) - G_{n/d}(0) \\ &= q^{n/d-1} + (-1)^{n/d}q^{n/d-1} - (-1)^{n/d}q^{n/d-1} - G_{n/d}(0) \\ &= q^{n/d-1} - G_{n/d}(0), \end{aligned}$$

et en remplacent le tout dans (4.2.4), on conclut que

$$H_n(0,0) = \frac{1}{n}\sum_{\substack{d\mid n \\ p\nmid d}} \mu(d)G_{n/d}(0) - \frac{\varepsilon}{n}\sum_{\substack{d\mid n \\ p\nmid d}} \mu(d)q^{n/dp}.$$

4.3. PREUVE ÉLÉMENTAIRE DU THÉORÈME 4.4

Voici le point central de ce mémoire. Pour s'attaquer au théorème 4.4, nous aurons besoin de modifier quelque peu la notation. D'abord, au lieu d'écrire

le nombre de factorisations sous forme de couples comme $X_{(1,2)}(a)$, nous allons les donner sous une forme matricielle. Nous noterons cette matrice $n \times n$ comme $V(\nu) = (\nu_{i,j})$ où $\nu_{i,j}$ est le nombre de factorisations de la forme i^j et ν est le type de factorisation. Par exemple, si nous sommes dans le cas où $P_6(x)$, la factorisation de $X_{(1,1,1^2,2)}(a)$ serait donnée comme suit :

$$V(1,1,1^2,2) = \begin{pmatrix} 2 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

On notera $X_{(1,1,1^2,2)}(a) = X_{V(1,1,1^2,2,)}(a)$. On peut ensuite montrer la relation suivante qui sera notre point de départ pour montrer la relation sur les $X_\nu(a)$.

Lemme 4.10. *Si $0 \leq k \leq n - \ell$. Alors, un polynôme unitaire de degré k divisera $q^{n-\ell-k}$ polynômes de la forme $P_n(a)$*

DÉMONSTRATION. Pour un polynôme $f(x) = x^n + a_1x^{n-1} + \cdots + a_\ell x^{n-\ell} + t_{\ell+1}x^{n-\ell-1} + \cdots + t_n \in P_n(a)$ et pour $g(x) = x^k + b_1x^{k-1} + \cdots + b_{k-1}x + b_k$ un polynôme choisi tel que $g(x) \mid f(x)$, on écrit $f(x) = g(x)h(x)$ avec $h(x) = x^{n-k} + c_1x^{n-k-1} + \cdots + c_{n-k-1}x + c_{n-k}$. Si nous avons les valeurs des $b_1, \ldots, b_k$, alors les $c_1, \ldots, c_{n-k}$ doivent suivre les relations suivantes :

$$\begin{cases} b_1 + c_1 = a_1 \\ b_2 + b_1c_1 + c_2 = a_2 \\ \cdots \\ b_\ell + b_{\ell-1}c_1 + \cdots + b_1c_{\ell-1} + c_\ell = a_\ell \end{cases}$$

où on fixe $b_i = 0$ si $i > k$.

Ainsi, $g(x)$ fixe ℓ coefficients de $h(x)$. Il nous reste donc $n-k-\ell$ choix pour les coefficients de $h(x)$.

□

Définition 4.11. Pour une factorisation ν en particulier, nous dirons que le degré de ν noté $\deg(\nu)$ est simplement le degré du polynôme qu'il engendre. Puisque nous utilisons une notation matricielle et sachant que les entrées $\nu_{i,j}$ d'une matrice V sont les nombres de facteurs de la forme i^j, on déduit que

$$\deg(V) := \sum_{i,j} ij\nu_{i,j}.$$

Définition 4.12. Nous noterons aussi la longueur de ν par $\lg(\nu)$ ou $\lg(V)$ par

$$\lg(V) := \sum_{i,j} j\nu_{i,j}.$$

Définition 4.13. On écrira aussi pour W, V, deux matrices $n \times n$ avec des entrées entières, que W est majoré par V si et seulement si

$$\begin{cases} w_{i,n} \leq \nu_{i,n} \\ w_{i,n} + w_{i,n-1} \leq \nu_{i,n} + \nu_{i,n-1} \\ \dots \\ w_{i,n} + \dots + w_{i,1} \leq \nu_{i,n} + \dots + \nu_{i,1} \end{cases}$$

pour tous $i = 1 \dots n$. On écrira alors que $W \preceq V$.

Ainsi, toutes les factorisations w de degré plus petit ou égal à $n - \ell$ peuvent être représentées par une matrice W avec $\sum_{i,j} ijw_{i,j} = k \leq n - \ell$. Pour tous ces w, on peut considérer tous les types de factorisations ν de degré n tel que w en est un facteur. Il s'agit simplement de l'ensemble des éléments ν tel que $W \preceq V$. En comptant le nombre de polynômes de chaque type et en utilisant (4.10), on trouve l'équation suivante :

$$\begin{aligned} &\sum_{V \succeq W} \prod_{i=1}^{n} \binom{\nu_{i,n}}{w_{i,n}} \binom{\nu_{i,n} + \nu_{i,n-1} - w_{i,n}}{w_{i,n-1}} \cdots \binom{\nu_{i,n} + \dots + \nu_{i,1} - w_{i,n} - \cdots w_{i,2}}{w_{i,1}} X_V(a) \\ &= q^{n-\ell-k} \prod_{i=1}^{n} \binom{H_i}{w_{i,1} \dots w_{i,n}} \end{aligned} \tag{4.3.1}$$

où H_i désigne le nombre de polynômes irréductibles de degré i sans aucune restriction. Plus précisément, les deux côtés de cette équation comptent les polynômes de $P_n(a)$ qui sont divisibles par un type de factorisation W. Pour trouver le côté gauche, on compte les polynômes de chaque type de factorisation donné par les matrices du type V qui majorent W. Pour le côté droit, on compte directement les polynômes en utilisant le lemme (4.10). On posera que l'équation (4.3.1) est égale à $\mathcal{E}_w(a)$ ou $\mathcal{E}_W(a)$.

4.3.1. Combinaison d'équations

Nous allons considérer un certain nombre d'équations de la forme $\mathcal{E}_w(a)$. De plus, pour satisfaire les mêmes conditions que (4.4), on prend $\ell = 2$.

Posons

$$\mathcal{W}_a = \{ \text{ les types de factorisation } w : \deg(w) \leq n - 2, w_{i,j} = 0, j > 1. \}$$

et aussi que

$$A := \sum_{w \in \mathcal{W}_a} (-1)^{\lg(w)} (n - \deg(w)) \mathcal{E}_w(a).$$

Posons également

$$\mathcal{W}_b = \{w \text{ factorization type} \mid \deg(w) \leq n-2, w_{i,j} = 0, j > 1, w_{1,1} \neq 0\}$$

et

$$B := -\sum_{w \in \mathcal{W}_b} (-1)^{\lg(w)} \mathcal{E}_w(a).$$

Considérons

$$\mathcal{W}_c = \{w \text{ factorization type} \mid \deg(w) \leq n-2, w_{i,j} = 0, i, j > 1, \exists j_0, w_{1,j_0} \neq 0\}.$$

Posons

$$\alpha_s = \sum_{j=0}^{s} j! \binom{s}{j}.$$

Posons γ une fonction de n paramètres avec des entrées entières non-négatives données par les récurrences suivantes :

– Pour $s \geq 0$,

$$\gamma(s_1, 0, 0, \ldots, 0) = \alpha_{s_1}.$$

– Lorsque nous avons $i > 1$ avec $s_i \neq 0$, nous obtenons que

$$\gamma(s_1, s_2, \ldots, s_{n-1}, s_n) = \sum_{j=1}^{n} \gamma(s_1, \ldots, s_{j-1} + 1, s_j - 1, \ldots, s_n) s_j$$

On peut remarquer que la somme commence avec $\gamma(s_1 - 1, s_2, \ldots, s_{n-1}, s_n)$ si $s_1 \neq 0$.

Considérons

$$C := \sum_{w \in \mathcal{W}_c} (-1)^{\lg(w)} \gamma(w_{1,1}, w_{1,2}, \ldots, w_{1,n}) \mathcal{E}_w(a).$$

Le but de cette section est de montrer que $A + B + C$ est le résultat attendu qui est (4.4).

4.3.2. Étude de γ

Dans cette section, nous allons montrer la propriété suivante :

Proposition 4.14. *Soit $s_1, \ldots, s_n$ des entiers non-négatifs. Définissons*

$$\begin{aligned} f(s_1, \ldots, s_n) &:= \sum_{t_i \geq 0} \gamma(t_1, t_2, \ldots, t_n) \\ &\times (-1)^{t_1 + \cdots + nt_n} \binom{s_n}{t_n} \binom{s_n + s_{n-1} - t_n}{t_{n-1}} \cdots \binom{s_n + \cdots + s_1 - t_n - \cdots - t_2}{t_1}, \end{aligned}$$

Alors, nous avons

$$f(s_1, \ldots, s_n) = (-1)^{s_1 + 2s_2 + \cdots + ns_n} \frac{(s_1 + 2s_2 + \cdots + ns_n)!}{(1!)^{s_1} (2!)^{s_2} \cdots (n!)^{s_n}}. \tag{4.3.2}$$

Avant de débuter cette preuve, nous devons montrer le lemme suivant.

Lemme 4.15. *Pour $n \geq 2$, nous avons la récurrence suivante :*

$$f(s_1, \ldots, s_n) = -\sum_{j=1}^{n} s_j f(s_1, \ldots, s_{j-1} + 1, s_j - 1, \ldots, s_n). \tag{4.3.3}$$

DÉMONSTRATION. D'abord, notons que pour $s > 0$:

$$\begin{aligned} f(s, 0, \ldots, 0) &= \sum_{0 \leq t \leq s} \alpha_t (-1)^t \binom{s}{t} \\ &= \alpha_0 + \sum_{1 \leq t \leq s} (\alpha_{t-1} t + 1)(-1)^t \binom{s}{t} \\ &= \sum_{0 \leq t \leq s} (-1)^t \binom{s}{t} + s \sum_{1 \leq t \leq s} \alpha_{t-1} (-1)^t \binom{s-1}{t-1} \\ &= -s f(s-1, 0, \ldots, 0). \end{aligned}$$

En appliquant la récurrence sur γ, on trouve :

$$\begin{aligned} f(s_1, \ldots, s_n) &= \sum_{t_i \geq 0} \sum_{j=1}^{n} \gamma(t_1, \ldots, t_{j-1} + 1, t_j - 1, \ldots, t_n) t_j \\ &\times (-1)^{t_1 + \cdots + nt_n} \binom{s_n}{t_n} \binom{s_n + s_{n-1} - t_n}{t_{n-1}} \cdots \binom{s_n + \cdots + s_1 - t_n - \cdots - t_2}{t_1}. \end{aligned}$$

On peut voir qu'il est correct d'appliquer la récurrence pour la partie de la somme qui contient le terme $\gamma(t, 0, 0, \ldots, 0)$ à cause du cas $f(s, 0, \ldots, 0)$ fait ci-dessus.

En posant

$$S = \gamma(t_1, \ldots, t_{j-1} + 1, t_j - 1, \ldots, t_n) t_j \binom{s_n + \cdots + s_j - t_n - \cdots - t_{j+1}}{t_j} \times \prod_{i=j+1}^{n} \binom{s_n + \cdots + s_i - t_n - \cdots - t_{i+1}}{t_i}$$

et pour une valeur de j fixée, on peut remarquer que

$$\begin{aligned} S &= \gamma(t_1, \ldots, t_{j-1} + 1, t_j - 1, \ldots, t_n)(s_n + \cdots + s_j - t_n - \cdots - t_{j+1}) \\ &\times \binom{s_n + \cdots + s_j - t_n - \cdots - t_{j+1} - 1}{t_j - 1} \\ &\times \prod_{i=j+1}^{n} \binom{s_n + \cdots + s_i - t_n - \cdots - t_{i+1}}{t_i}. \end{aligned}$$

Nous allons isoler le terme s_j :

$$\begin{aligned} S &= \gamma(t_1, \ldots, t_{j-1} + 1, t_j - 1, \ldots, t_n) s_j \binom{s_n + \cdots + s_j - t_n - \cdots - t_{j+1} - 1}{t_j - 1} \\ &\times \prod_{i=j+1}^{n} \binom{s_n + \cdots + s_i - t_n - \cdots - t_{i+1}}{t_i} \\ &+ \gamma(t_1, \ldots, t_{j-1} + 1, t_j - 1, \ldots, t_n)(s_n + \cdots + s_{j+1} - t_n - \cdots - t_{j+1}) \\ &\times \binom{s_n + \cdots + s_j - t_n - \cdots - t_{j+1} - 1}{t_j - 1} \\ &\times \prod_{i=j+1}^{n} \binom{s_n + \cdots + s_i - t_n - \cdots - t_{i+1}}{t_i}. \end{aligned}$$

Puis, nous allons manipuler le coefficient binomial $j+1$ dans la deuxième somme :

$$\begin{aligned}
S &= \gamma(t_1,\dots,t_{j-1}+1,t_j-1,\dots,t_n)s_j\binom{s_n+\cdots+s_j-t_n-\cdots-t_{j+1}-1}{t_j-1}\\
&\times \prod_{i=j+1}^{n}\binom{s_n+\cdots+s_i-t_n-\cdots-t_{i+1}}{t_i}\\
&+ \gamma(t_1,\dots,t_{j-1}+1,t_j-1,\dots,t_n)(s_n+\cdots+s_{j+1}-t_n-\cdots-t_{j+2})\\
&\times \binom{s_n+\cdots+s_j-t_n-\cdots-t_{j+1}-1}{t_j-1}\\
&\times \binom{s_n+\cdots+s_{j+1}-t_n-\cdots-t_{j+2}-1}{t_{j+1}}\prod_{i=j+2}^{n}\binom{s_n+\cdots+s_i-t_n-\cdots-t_{i+1}}{t_i}.
\end{aligned}$$

Nous allons isoler le facteur s_{j+1} :

$$\begin{aligned}
S &= \gamma(t_1,\dots,t_{j-1}+1,t_j-1,\dots,t_n)s_j\binom{s_n+\cdots+s_j-t_n-\cdots-t_{j+1}-1}{t_j-1}\\
&\times \prod_{i=j+1}^{n}\binom{s_n+\cdots+s_i-t_n-\cdots-t_{i+1}}{t_i}\\
&+ \gamma(t_1,\dots,t_{j-1}+1,t_j-1,\dots,t_n)s_{j+1}\binom{s_n+\cdots+s_j-t_n-\cdots-t_{j+1}-1}{t_j-1}\\
&\times \binom{s_n+\cdots+s_{j+1}-t_n-\cdots-t_{j+2}-1}{t_{j+1}}\prod_{i=j+2}^{n}\binom{s_n+\cdots+s_i-t_n-\cdots-t_{i+1}}{t_i}\\
&+ \gamma(t_1,\dots,t_{j-1}+1,t_j-1,\dots,t_n)(s_n+\cdots+s_{j+2}-t_n-\cdots-t_{j+2})\\
&\times \binom{s_n+\cdots+s_j-t_n-\cdots-t_{j+1}-1}{t_j-1}\\
&\times \binom{s_n+\cdots+s_{j+1}-t_n-\cdots-t_{j+2}-1}{t_{j+1}}\prod_{i=j+2}^{n}\binom{s_n+\cdots+s_i-t_n-\cdots-t_{i+1}}{t_i}.
\end{aligned}$$

De plus, nous allons réécrire la dernière ligne en deux produits :

$$\begin{aligned}
S &= \gamma(t_1,\dots,t_{j-1}+1,t_j-1,\dots,t_n)s_j\binom{s_n+\cdots+s_j-t_n-\cdots-t_{j+1}-1}{t_j-1}\\
&\times \prod_{i=j+1}^{n}\binom{s_n+\cdots+s_i-t_n-\cdots-t_{i+1}}{t_i}\\
&+ \gamma(t_1,\dots,t_{j-1}+1,t_j-1,\dots,t_n)s_{j+1}\binom{s_n+\cdots+s_j-t_n-\cdots-t_{j+1}-1}{t_j-1}\\
&\times \binom{s_n+\cdots+s_{j+1}-t_n-\cdots-t_{j+2}-1}{t_{j+1}}\prod_{i=j+2}^{n}\binom{s_n+\cdots+s_i-t_n-\cdots-t_{i+1}}{t_i}\\
&+ \gamma(t_1,\dots,t_{j-1}+1,t_j-1,\dots,t_n)(s_n+\cdots+s_{j+2}-t_n-\cdots-t_{j+3})\\
&\times \binom{s_n+\cdots+s_j-t_n-\cdots-t_{j+1}-1}{t_j-1}\\
&\times \prod_{i=j+1}^{j+2}\binom{s_n+\cdots+s_i-t_n-\cdots-t_{i+1}-1}{t_i}\prod_{i=j+3}^{n}\binom{s_n+\cdots+s_i-t_n-\cdots-t_{i+1}}{t_i}.
\end{aligned}$$

On répète les mêmes opérations jusqu'à ce que l'on obtienne :

$$\begin{aligned}
S &= \dots\\
&= \gamma(t_1,\dots,t_{j-1}+1,t_j-1,\dots,t_n)\binom{s_n+\cdots+s_j-t_n-\cdots-t_{j+1}-1}{t_j-1}\\
&\times \sum_{\ell=j}^{n}s_\ell\prod_{i=j+1}^{\ell}\binom{s_n+\cdots+s_i-t_n-\cdots-t_{i+1}-1}{t_i}\\
&\times \prod_{i=\ell+1}^{n}\binom{s_n+\cdots+s_i-t_n-\cdots-t_{i+1}}{t_i}.
\end{aligned}$$

En considérant tous les j dans notre équation de départ et en combinant ce qu'on vient de déduire, on a :

$$\begin{aligned}
& \gamma(t_1,\dots,t_{j-1}+1,t_j-1,\dots,t_n)t_j\prod_{i=1}^{n}\binom{s_n+\cdots+s_i-t_n-\cdots-t_{i+1}}{t_i}\\
= \;& \gamma(t_1,\dots,t_{j-1}+1,t_j-1,\dots,t_n)\prod_{i=1}^{j-2}\binom{s_n+\cdots+s_i-t_n-\cdots-t_{i+1}}{t_i}\\
\times \;& \binom{s_n+\cdots+s_{j-1}-t_n-\cdots-t_j}{t_{j-1}}\binom{s_n+\cdots+s_j-t_n-\cdots-t_{j+1}-1}{t_j-1}\\
\times \;& \sum_{\ell=j}^{n}s_\ell\prod_{i=j+1}^{\ell}\binom{s_n+\cdots+s_i-t_n-\cdots-t_{i+1}-1}{t_i}\prod_{i=\ell+1}^{n}\binom{s_n+\cdots+s_i-t_n-\cdots-t_{i+1}}{t_i}.
\end{aligned}$$

En manipulant le coefficient binomial $j-1$ dans l'équation ci-dessus, on trouve qu'elle est égale à

$$\begin{aligned}
= \;& \gamma(t_1,\dots,t_{j-1}+1,t_j-1,\dots,t_n)\prod_{i=1}^{j-2}\binom{s_n+\cdots+s_i-t_n-\cdots-t_{i+1}}{t_i}\\
\times \;& \binom{s_n+\cdots+s_{j-1}-t_n-\cdots-t_j+1}{t_{j-1}+1}\binom{s_n+\cdots+s_j-t_n-\cdots-t_{j+1}-1}{t_j-1}\\
\times \;& \sum_{\ell=j}^{n}s_\ell\prod_{i=j+1}^{\ell}\binom{s_n+\cdots+s_i-t_n-\cdots-t_{i+1}-1}{t_i}\prod_{i=\ell+1}^{n}\binom{s_n+\cdots+s_i-t_n-\cdots-t_{i+1}}{t_i}\\
- \;& \gamma(t_1,\dots,t_{j-1}+1,t_j-1,\dots,t_n)\prod_{i=1}^{j-2}\binom{s_n+\cdots+s_i-t_n-\cdots-t_{i+1}}{t_i}\\
\times \;& \binom{s_n+\cdots+s_{j-1}-t_n-\cdots-t_j}{t_{j-1}+1}\binom{s_n+\cdots+s_j-t_n-\cdots-t_{j+1}-1}{t_j-1}\\
\times \;& \sum_{\ell=j}^{n}s_\ell\prod_{i=j+1}^{\ell}\binom{s_n+\cdots+s_i-t_n-\cdots-t_{i+1}-1}{t_i}\prod_{i=\ell+1}^{n}\binom{s_n+\cdots+s_i-t_n-\cdots-t_{i+1}}{t_i}.
\end{aligned}$$

En considérant les signes, les termes qui possèdent $\gamma(t_1,\dots,t_{j-1}+1,t_j-1,\dots,t_n)$ avec $j>2$ donnent :

$$-\sum_{\ell=j}^{n}s_\ell f(s_1,\dots,s_{j-1}+1,\dots,s_\ell-1,\dots,s_n)+\sum_{\ell=j}^{n}s_\ell f(s_1,\dots,s_{j-2}+1,\dots,s_\ell-1,\dots,s_n).$$

D'autre part, en considérant les termes avec $\gamma(t_1-1,\dots,t_n)$, on obtient

$$-\sum_{\ell=1}^{n}s_\ell f(s_1,\dots,s_\ell-1,\dots,s_n).$$

Les termes qui possèdent $\gamma(t_1+1, t_2-1, \ldots, t_n)$ donnent

$$-\sum_{\ell=2}^{n} s_\ell f(s_1+1, \ldots, s_\ell-1, \ldots, s_n) + \sum_{\ell=2}^{n} s_\ell f(s_1, \ldots, s_\ell-1, \ldots, s_n).$$

En rassemblant toutes nos sommations, nous trouvons :

$$\begin{aligned}
f(s_1, \ldots, s_n) &= -\sum_{j=1}^{n}\sum_{\ell=j}^{n} s_\ell f(s_1, \ldots, s_{j-1}+1, \ldots, s_\ell-1, \ldots, s_n) \\
&\quad + \sum_{j=2}^{n}\sum_{\ell=j}^{n} s_\ell f(s_1, \ldots, s_{j-2}+1, \ldots, s_\ell-1, \ldots, s_n) \\
&= -\sum_{j=1}^{n}\sum_{\ell=j}^{n} s_\ell f(s_1, \ldots, s_{j-1}+1, \ldots, s_\ell-1, \ldots, s_n) \\
&\quad + \sum_{h=1}^{n-1}\sum_{\ell=h+1}^{n} s_\ell f(s_1, \ldots, s_{h-1}+1, \ldots, s_\ell-1, \ldots, s_n) \\
&= -\sum_{j=1}^{n} s_j f(s_1, \ldots, s_{j-1}+1, s_j-1, \ldots, s_n),
\end{aligned}$$

ce qui montre la récurrence pour $f(s_1, \ldots, s_n)$. □

PREUVE DE LA PROPOSITION (4.14). D'abord, notons pour $s = 0$, $f(0, \ldots, 0) = 1$. Si nous supposons $s > 0$, nous avons que

$$\begin{aligned}
f(s, 0, \ldots, 0) &= \sum_{t\geq 0} \gamma(t, 0, \ldots, 0)(-1)^t \binom{s}{t} \\
&= \sum_{t\geq 0} \alpha_t (-1)^t \binom{s}{t} \\
&= \sum_{t=0}^{s}\sum_{j=0}^{t} j! \binom{t}{j} (-1)^t \binom{s}{t}
\end{aligned}$$

On peut changer l'ordre de sommation et nous trouvons :

$$= \sum_{j=0}^{s} j! \binom{s}{j} \sum_{t=j}^{s} (-1)^t \binom{s-j}{t-j}.$$

On peut remarquer que la deuxième somme de la partie de droite nous donne zéro sauf si $s = j$ et dans ce cas, elle est égale à $(-1)^s$. Alors, nous avons

$$f(s, 0, \dots, 0) = (-1)^s s! = (-1)^s \frac{s!}{(1!)^s}.$$

Nous allons à présent procéder par induction pour $k = s_1 + 2s_2 + \cdots + ns_n$. Il est à noter que nous avons déjà montré le cas $k = s_1$. Remarquons de $f(s_1, \dots, s_{j-1}+1, s_j - 1, \dots, s_n)$ que nous avons $s_1 + \cdots + (j-1)(s_{j-1}+1) + j(s_j - 1) + \cdots + ns_n = k - 1$. Alors, par la récurrence (4.3.3) et par notre hypothèse d'induction, on a

$$\begin{aligned}
f(s_1, \dots, s_n) &= -\sum_{j=1}^{n} s_j f(s_1, \dots, s_{j-1} + 1, s_j - 1, \dots, s_n) \\
&= -\sum_{j=1}^{n} s_j (-1)^{s_1 + 2s_2 + \cdots + ns_n - 1} \frac{(s_1 + 2s_2 + \cdots + ns_n - 1)!}{(1!)^{s_1} \cdots ((j-1)!)^{s_{j-1}+1} (j!)^{s_j - 1} \cdots (n!)^{s_n}} \\
&= (-1)^{s_1 + 2s_2 + \cdots + ns_n} \frac{(s_1 + 2s_2 + \cdots + ns_n - 1)!}{(1!)^{s_1} \cdots (n!)^{s_n}} \sum_{j=1}^{n} s_j \frac{j!}{(j-1)!} \\
&= (-1)^{s_1 + 2s_2 + \cdots + ns_n} \frac{(s_1 + 2s_2 + \cdots + ns_n)!}{(1!)^{s_1} \cdots (n!)^{s_n}}.
\end{aligned}$$

ce qui conclut la preuve de la proposition (4.14). □

4.3.3. $A + B + C$

Pour montrer (4.4), il nous faut calculer le coefficient de tous les $X_v(a)$ dans $A + B + C$. Nous aurons besoin des deux équations suivantes qui seront très importantes dans cette section :

$$\sum_{k=0}^{s} (-1)^k \binom{s}{k} = 0, \qquad s \neq 0, \tag{4.3.4}$$

$$\sum_{k=0}^{s} (-1)^k k \binom{s}{k} = 0, \qquad s \neq 1. \tag{4.3.5}$$

4.3.3.1. *Le terme* A

Le coefficient de $X_v(a)$ dans A est donné par

$$\sum_{0 \leq w_{1,1} + \cdots + nw_{n,1} \leq n-2} (n - (w_{1,1} + \cdots + nw_{n,1})) \prod_{i=1}^{n} (-1)^{w_{i,1}} \binom{v_{i,n} + \cdots + v_{i,1}}{w_{i,1}}.$$

À cause des équations (4.3.4) et (4.3.5), nous obtenons

$$(4.3.6)\qquad \sum_{0\le w_{1,1}+\cdots+nw_{n,1}\le n} (n-(w_{1,1}+\cdots+nw_{n,1}))\prod_{i=1}^{n}(-1)^{w_{i,1}}\binom{v_{i,n}+\cdots+v_{i,1}}{w_{i,1}}=0$$

sauf si $v_{i,n}+\cdots+v_{i,1}=0$ pour tous i. Cette possibilité n'est pas envisageable puisque $n>0$. Cependant, il y aurait un autre cas qui empêcherait que la somme ne soit pas égale à zéro ; soit un certain i_0 tel que $v_{i_0,n}+\cdots+v_{i_0,1}=1$ et $v_{i,n}+\cdots+v_{i,1}=0$ pour tous $i\neq i_0$. Puisque $\deg(v)=n$, la seule possibilité est que $v_{i_0,n/i_0}=1$ et que le reste soit zéro. Nous obtenons donc i_0 comme coefficient de $X_{(i_0^{n/i_0})}(a)$.

Pour le reste des $X_v(a)$, la contribution de A au coefficient doit être

$$-\sum_{w_{1,1}+\cdots+nw_{n,1}=n-1}\prod_{i=1}^{n}(-1)^{w_{i,1}}\binom{v_{i,n}+\cdots+v_{i,1}}{w_{i,1}}.$$

Puisque nous avons $w_{i,1}\le v_{i,n}+\cdots+v_{i,1}$, nous obtenons

$$n-1=w_{1,1}+\cdots+nw_{n,1}\le\sum_{i,j}iv_{i,j}$$

et

$$\sum_{i,j}ijv_{i,j}-1\le\sum_{i,j}iv_{i,j}$$

implique

$$\sum_{i,j}i(j-1)v_{i,j}\le 1.$$

Ceci peut arriver seulement si $v_{i,j}=0$ pour $j>1$ sauf peut-être pour $v_{1,2}$ qui pourrait être égal à 1. On peut aussi voir que $v_{i,1}$ peut prendre n'importe quelle valeur. Alors, la contribution au coefficient est

$$-\sum_{w_{1,1}+\cdots+nw_{n,1}=n-1}(-1)^{w_{1,1}}\binom{v_{1,2}+v_{1,1}}{w_{1,1}}\prod_{i=2}^{n}(-1)^{w_{i,1}}\binom{v_{i,1}}{w_{i,1}}.$$

On peut maintenant séparer le tout en deux cas. D'abord, supposons que $v_{i,j}=0$ pour $j>1$. Puisque $w_{i,1}\le v_{i,1}$, pour que $w_{1,1}+\cdots+nw_{n,1}=n-1$ arrive, il faut que $w_{i,1}=v_{i,1}$ pour $i>1$ et $w_{1,1}=v_{1,1}-1$. Nous trouvons donc

$$(-1)^{v_{1,1}+\cdots+v_{n,1}}v_{1,1}.$$

Ensuite, supposons que $v_{i,j}=0$ pour tous $j>1$ sauf pour $v_{1,2}=1$. Encore une fois, il faut que $w_{i,1}\le v_{i,1}$ pour $i>1$ et $w_{1,1}\le v_{1,1}+1$. Alors, $w_{1,1}+\cdots+nw_{n,1}=n-1$ arrive seulement si $w_{1,1}=v_{1,1}+1$, $w_{i,1}=v_{i,1}$ pour $i>1$. Alors, le coefficient est égal à

$$(-1)^{v_{1,1}+\cdots+v_{n,1}}.$$

4.3.3.2. *Le terme* B

Regardons maintenant l'expression B. Le coefficient $X_\nu(a)$ est donné par

$$-\sum_{\substack{0\le w_{1,1}+\cdots+nw_{n,1}\le n-2\\ w_{1,1}\neq 0}}\prod_{i=1}^{n}(-1)^{w_{i,1}}\binom{\nu_{i,n}+\cdots+\nu_{i,1}}{w_{i,1}}.$$

À cause des équations (4.3.4) et (4.3.5), on déduit que

$$-\sum_{0\le w_{1,1}+\cdots+nw_{n,1}\le n}\prod_{i=1}^{n}(-1)^{w_{i,1}}\binom{\nu_{i,n}+\cdots+\nu_{i,1}}{w_{i,1}}=0$$

sauf si $\nu_{i,n}+\cdots+\nu_{i,1}=0$ pour tous i. Cependant, on peut conclure que ce cas est impossible puisque $n>0$.

Pour le cas où $w_{1,1}+2w_{2,1}+\cdots+nw_{n,1}\ge n-1$ et en utilisant les conditions $w_{i,1}\le\nu_{i,n}+\cdots+\nu_{i,1}$ pour tous i, on peut déduire que

$$\sum_{i,j}ij\nu_{i,j}-1=n-1\le w_{1,1}+2w_{2,1}+\cdots+nw_{n,1}\le\sum_{i,j}i\nu_{i,j}$$

ce qui nous donne

$$\sum_{i,j}i(j-1)\nu_{i,j}\le 1.$$

Ainsi, on peut déduire que $\nu_{i,j}=0$ pour tous $j>1$ sauf pour $\nu_{1,2}$ qui pourrait être égal à 1 ou 0. Dans tous ces cas, on peut remarquer que $\nu_{i,1}$ peut prendre n'importe quelle valeur. Ainsi, on peut réécrire le coefficient comme :

$$\sum_{w_{1,1}+2w_{2,1}+\cdots+nw_{n,1}=n-1,n}(-1)^{w_{1,1}}\binom{\nu_{1,2}+\nu_{1,1}}{w_{1,1}}\prod_{i=2}^{n}(-1)^{w_{i,1}}\binom{\nu_{i,1}}{w_{i,1}} \quad (4.3.6)$$

$$+\sum_{2w_{2,1}+\cdots+nw_{n,1}\le n-2}\prod_{i=2}^{n}(-1)^{w_{i,1}}\binom{\nu_{i,1}}{w_{i,1}}. \quad (4.3.7)$$

Pour continuer les simplifications, nous allons d'abord assumer que $\nu_{i,j}=0$ pour $j>1$. Puisque $w_{i,1}\le\nu_{i,1}$, le cas $w_{1,1}+\cdots+nw_{n,1}=n-1$ arrive seulement si $w_{i,1}=\nu_{i,1}$ pour $i>1$ et $w_{1,1}=\nu_{1,1}-1$. On peut aussi déduire que le cas $w_{1,1}+\cdots+nw_{n,1}=n$ arrive seulement si $w_{i,1}=\nu_{i,1}$. On détermine que la partie (4.3.6) serait

$$-(-1)^{\nu_{1,1}+\cdots+\nu_{n,1}}\nu_{1,1}+(-1)^{\nu_{1,1}+\cdots+\nu_{n,1}}.$$

Maintenant, assumons que $\nu_{i,j}=0$ pour tous $j>1$ sauf pour $\nu_{1,2}$ qui serait égal à 1. Encore une fois, on a que $w_{i,1}\le\nu_{i,1}$ pour $i>1$ et $w_{1,1}\le\nu_{1,1}+1$. Ainsi, le cas $w_{1,1}+\cdots+nw_{n,1}=n-1$ arrive seulement si $w_{1,1}=\nu_{1,1}+1$ et $w_{i,1}=\nu_{i,1}$ pour $i>1$ et le cas $w_{1,1}+\cdots+nw_{n,1}=n$ n'arrive jamais. Alors, la contribution

(4.3.6) serait égale à

$$-(-1)^{\nu_{1,1}+\cdots+\nu_{n,1}}.$$

Analysons maintenant la contribution de la partie (4.3.7). Nous avons alors :

$$\sum_{0\leq 2w_{2,1}+\cdots+nw_{n,1}\leq n-2}\prod_{i=2}^{n}(-1)^{w_{i,1}}\binom{\nu_{i,n}+\cdots+\nu_{i,1}}{w_{i,1}}.$$

On peut déduire que

$$\sum_{0\leq 2w_{2,1}+\cdots+nw_{n,1}\leq n}\prod_{i=2}^{n}(-1)^{w_{i,1}}\binom{\nu_{i,n}+\cdots+\nu_{i,1}}{w_{i,1}}=0 \tag{4.3.8}$$

sauf si $\nu_{i,n}+\cdots+\nu_{i,1}=0$ pour $i>1$ et donc la somme serait égale à 1. En isolant, on peut aussi déduire de l'équation (4.3.8) :

$$-\sum_{2w_{2,1}+\cdots+nw_{n,1}=n-1,n}\prod_{i=2}^{n}(-1)^{w_{i,1}}\binom{\nu_{i,n}+\cdots+\nu_{i,1}}{w_{i,1}}.$$

Avec les constatations précédentes et avec le fait que $\nu_{1,1}$ doit être positif pour être dans cette sommation, on sait que cette contribution apparait si $\nu_{1,1}=1$ et $\nu_{i,j}=0$ pour $j>1$. La seule possibilité est que $w_{1,1}=0$, nous obtenons

$$-(-1)^{\nu_{2,1}+\cdots+\nu_{n,1}}=(-1)^{\nu_{1,1}+\cdots+\nu_{n,1}}.$$

4.3.3.3. *Le terme* C

Finalement, regardons l'expression C :

$$\begin{aligned}
&\sum_{\substack{0\leq w_{1,1}+2w_{1,2}+\cdots+nw_{1,n}\leq n-2\\ \exists j_0, w_{1,j_0}\neq 0}}\gamma(w_{1,1},w_{1,2},\ldots,w_{1,n})\\
\times\quad&(-1)^{w_{1,1}+\cdots+nw_{1,n}}\binom{\nu_{1,n}}{w_{1,n}}\binom{\nu_{1,n}+\nu_{1,n-1}-w_{1,n}}{w_{1,n-1}}\cdots\binom{\nu_{1,n}+\cdots+\nu_{1,1}-w_{1,n}-\cdots w_{1,2}}{w_{1,1}}\\
\times\quad&\sum_{0\leq 2w_{2,1}\cdots+nw_{n,1}\leq n-2-(w_{1,1}+2w_{1,2}+\cdots+nw_{1,n})}\prod_{i=2}^{n}(-1)^{w_{i,1}}\binom{\nu_{i,n}+\cdots+\nu_{i,1}}{w_{i,1}}.
\end{aligned}$$

À cause des équations (4.3.4) et (4.3.5), nous avons

$$\begin{aligned}
&\sum_{0\le w_{1,1}+2w_{1,2}+\cdots+nw_{1,n}\le n} \gamma(w_{1,1},w_{1,2},\ldots,w_{1,n})\\
\times\quad &(-1)^{w_{1,1}+\cdots+nw_{1,n}}\binom{\nu_{1,n}}{w_{1,n}}\binom{\nu_{1,n}+\nu_{1,n-1}-w_{1,n}}{w_{1,n-1}}\cdots\binom{\nu_{1,n}+\cdots+\nu_{1,1}-w_{1,n}-\cdots w_{1,2}}{w_{1,1}}\\
\times\quad &\sum_{0\le 2w_{2,1}\cdots+nw_{n,1}\le n-(w_{1,1}+2w_{1,2}+\cdots+nw_{1,n})}\ \prod_{i=2}^{n}(-1)^{w_{i,1}}\binom{\nu_{i,n}+\cdots+\nu_{i,1}}{w_{i,1}}=0
\end{aligned}$$

sauf si $\nu_{i,n}+\cdots+\nu_{i,1}=0$ pour tous $i>1$. Dans ce cas, on obtient

$$\begin{aligned}
&\sum_{\substack{0\le w_{1,1}+2w_{1,2}+\cdots+nw_{1,n}\le n-2\\ \exists j_0, w_{1,j_0}\neq 0}} \gamma(w_{1,1},w_{1,2},\ldots,w_{1,n})\\
\times\quad &(-1)^{w_{1,1}+\cdots+nw_{1,n}}\binom{\nu_{1,n}}{w_{1,n}}\binom{\nu_{1,n}+\nu_{1,n-1}-w_{1,n}}{w_{1,n-1}}\cdots\binom{\nu_{1,n}+\cdots+\nu_{1,1}-w_{1,n}-\cdots w_{1,2}}{w_{1,1}}\\
=\quad &f(\nu_{1,1},\ldots,\nu_{1,n})-\sum_{0\le w_{1,1}+2w_{1,2}+\cdots+nw_{1,n}=0,n-1,n} \gamma(w_{1,1},w_{1,2},\ldots,w_{1,n})\\
\times\quad &(-1)^{w_{1,1}+\cdots+nw_{1,n}}\binom{\nu_{1,n}}{w_{1,n}}\binom{\nu_{1,n}+\nu_{1,n-1}-w_{1,n}}{w_{1,n-1}}\cdots\binom{\nu_{1,n}+\cdots+\nu_{1,1}-w_{1,n}-\cdots w_{1,2}}{w_{1,1}}.
\end{aligned}$$

Dans le cas $w_{1,1}+2w_{1,2}+\cdots+nw_{1,n}=n-1$ avec les conditions $w_{1,i}+\cdots+w_{1,n}\le\nu_{1,i}+\cdots+\nu_{1,n}$ pour tous i et aussi pour $\nu_{1,1}+2\nu_{1,2}+\cdots+n\nu_{1,n}=n$, on a qu'il existe $j_0>1$ tel que $w_{1,j_0-1}=\nu_{1,j_0-1}+1$ et $w_{1,j_0}=\nu_{1,j_0}-1$ ou $w_{1,1}=\nu_{1,1}-1$. On obtient le terme

$$\begin{aligned}
&-\sum_{j=1}^{n}\gamma(\nu_{1,1},\ldots,\nu_{1,j-1}+1,\nu_{1,j}-1,\ldots,\nu_{1,n})(-1)^{\nu_{1,1}+\cdots+n\nu_{1,n}-1}\nu_{1,j}\\
=\quad &(-1)^{\nu_{1,1}+\cdots+n\nu_{1,n}}\gamma(\nu_{1,1},\ldots,\nu_{1,n})
\end{aligned}$$

pourvu qu'il existe un $i_0>1$ tel que $\nu_{1,i_0}\neq 0$. Sinon nous aurions le cas suivant :

$$(-1)^{\nu_{1,1}}\nu_{1,1}\gamma(\nu_{1,1}-1,0,\ldots,0)=(-1)^{\nu_{1,1}}\alpha_{\nu_{1,1}}-(-1)^{\nu_{1,1}}.$$

Pour le cas $w_{1,1}+2w_{1,2}+\cdots+nw_{1,n}=n$, les conditions $w_{1,i}+\cdots+w_{1,n}\le\nu_{1,i}+\cdots+\nu_{1,n}$ pour tous i et $\nu_{1,1}+2\nu_{1,2}+\cdots+n\nu_{1,n}=n$ nous permettent de déduire $w_{1,j}=\nu_{1,j}$ pour tous j et donc

$$-(-1)^{\nu_{1,1}+\cdots+n\nu_{1,n}}\gamma(\nu_{1,1},\ldots,\nu_{1,n}).$$

On peut remarquer que $\nu_{1,j}=0$ pour $j>1$. Alors, on obtient

$$-(-1)^{\nu_{1,1}}\alpha_{\nu_{1,1}}=-(-1)^{\nu_{1,1}}\gamma(\nu_{1,1},0,...,0).$$

Maintenant, regardons le cas où $\nu_{i_0,n} + \cdots + \nu_{i_0,1} \neq 0$ pour certains $i_0 > 1$. En séparant le cas où $w_{1,1} = \cdots = w_{1,n} = 0$ de la sommation, on trouve

$$\begin{aligned}
& - \sum_{w_{1,1}+2w_{1,2}+\cdots+nw_{1,n}+2w_{2,1}\cdots+nw_{n,1}=n-1,n} \gamma(w_{1,1}, w_{1,2}, \ldots, w_{1,n}) \\
\times \quad & (-1)^{w_{1,1}+\cdots+nw_{1,n}} \binom{\nu_{1,n}}{w_{1,n}} \binom{\nu_{1,n}+\nu_{1,n-1}-w_{1,n}}{w_{1,n-1}} \cdots \binom{\nu_{1,n}+\cdots+\nu_{1,1}-w_{1,n}-\cdots w_{1,2}}{w_{1,1}} \\
\times \quad & \prod_{i=2}^{n} (-1)^{w_{i,1}} \binom{\nu_{i,n}+\cdots+\nu_{i,1}}{w_{i,1}} \\
& -\gamma(0,\ldots,0) \sum_{2w_{2,1}\cdots+nw_{n,1}\leq n-2} \prod_{i=2}^{n} (-1)^{w_{i,1}} \binom{\nu_{i,n}+\cdots+\nu_{i,1}}{w_{i,1}}.
\end{aligned}$$

Le cas $w_{1,1} + 2w_{1,2} + \cdots + nw_{1,n} + 2w_{2,1} \cdots + nw_{n,1} \geq n - 1$ implique que

$$\sum_{i,j} ij\nu_{i,j} - 1 \leq w_{1,1} + 2w_{1,2} + \cdots + nw_{1,n} + 2w_{2,1} \cdots + nw_{n,1} \leq \sum_{j} j\nu_{1,j} + \sum_{i>1,j} i\nu_{i,j}$$

ce qui nous donne

$$\sum_{i>1,j} i(j-1)\nu_{i,j} \leq 1.$$

On conclut alors que $\nu_{i,j} = 0$ pour $i, j > 1$. En revenant à l'équation

$$\begin{aligned}
& - \sum_{w_{1,1}+2w_{1,2}+\cdots+nw_{1,n}+2w_{2,1}\cdots+nw_{n,1}=n-1,n} \gamma(w_{1,1}, w_{1,2}, \ldots, w_{1,n}) \\
\times \quad & (-1)^{w_{1,1}+\cdots+nw_{1,n}} \binom{\nu_{1,n}}{w_{1,n}} \binom{\nu_{1,n}+\nu_{1,n-1}-w_{1,n}}{w_{1,n-1}} \cdots \binom{\nu_{1,n}+\cdots+\nu_{1,1}-w_{1,n}-\cdots w_{1,2}}{w_{1,1}} \\
\times \quad & \prod_{i=2}^{n} (-1)^{w_{i,1}} \binom{\nu_{i,1}}{w_{i,1}},
\end{aligned}$$

on peut voir que $w_{i,1} \leq \nu_{i,1}$ pour $i > 1$ et $w_{1,i} + \cdots + w_{1,n} \leq \nu_{1,i} + \cdots + \nu_{1,n}$ pour tous i. Dans le cas où $w_{1,1} + 2w_{2,1} + \cdots + nw_{n,1} + 2w_{1,2} + \cdots + nw_{1,n} = n$, la seule possibilité est que $w_{i,1} = \nu_{i,1}$ pour $i > 1$ et $w_{1,i} + \cdots + w_{1,n} = \nu_{1,i} + \cdots + \nu_{1,n}$ pour tous i, ce qui implique $w_{1,i} = \nu_{1,i}$. Dans le cas où $w_{1,1} + 2w_{2,1} + \cdots + nw_{n,1} + 2w_{1,2} + \cdots + nw_{1,n} = n - 1$, les seules possibilités sont que $w_{i,1} = \nu_{i,1}$ pour tous $i > 1$ ou que $w_{1,j_0} = \nu_{1,j_0} - 1$ et que $w_{1,j_0-1} = \nu_{1,j_0-1} + 1$ pour un unique j_0 fixé et que $w_{1,j} = \nu_{1,j}$ pour les autres j.

Ainsi, la contribution au coefficient devient

$$(-1)^{\nu_{2,1}+\cdots+\nu_{n,1}+\nu_{1,1}+\cdots+n\nu_{1,n}} \sum_{j=1}^{n} \gamma(\nu_{1,1},\ldots,\nu_{1,j-1}+1,\nu_{1,j}-1,\ldots,\nu_{1,n})\nu_{1,j}$$
$$- \quad (-1)^{\nu_{2,1}+\cdots+\nu_{n,1}+\nu_{1,1}+\cdots+n\nu_{1,n}}\gamma(\nu_{1,1},\nu_{1,2},\ldots,\nu_{1,n}).$$

Ce terme est égal à 0, sauf si $\nu_{1,j} = 0$ pour tous $j > 1$. Dans ce cas, il serait égal à

$$-(-1)^{\nu_{1,1}+\nu_{2,1}+\cdots+\nu_{n,1}}.$$

Regardons maintenant le terme qui contient $w_{1,1} = \cdots = w_{1,n} = 0$:

$$-\gamma(0,\ldots,0) \sum_{0\le 2w_{2,1}\cdots+nw_{n,1}\le n-2} \prod_{i=2}^{n} (-1)^{w_{i,1}} \binom{\nu_{i,n}+\cdots+\nu_{i,1}}{w_{i,1}}.$$

On peut remarquer que

$$-\gamma(0,\ldots,0) \sum_{0\le 2w_{2,1}\cdots+nw_{n,1}\le n} \prod_{i=2}^{n} (-1)^{w_{i,1}} \binom{\nu_{i,n}+\cdots+\nu_{i,1}}{w_{i,1}} = 0$$

sauf si $\nu_{i,n} + \cdots + \nu_{i,1} = 0$ pour tous i. Dans ce cas, il resterait simplement le terme $-\gamma(0,\ldots,0)$ qui serait égal à -1. Sinon, on peut réécrire notre somme de la façon suivante :

$$\gamma(0,\ldots,0) \sum_{2w_{2,1}\cdots+nw_{n,1}=n-1,n} \prod_{i=2}^{n} (-1)^{w_{i,1}} \binom{\nu_{i,n}+\cdots+\nu_{i,1}}{w_{i,1}}.$$

Avec la somme $2w_{2,1}\cdots+nw_{n,1} \ge n-1$, on déduit que

$$\sum_{i,j} ij\nu_{i,j} - 1 = n-1 \le 2w_{2,1}\cdots+nw_{n,1} \le \sum_{i>1,j} i\nu_{i,j},$$

ce qui implique

$$\sum_{j} j\nu_{1,j} + \sum_{i>1,j} i(j-1)\nu_{i,j} \le 1.$$

Alors, $\nu_{i,j} = 0$ pour $j > 1$ et $\nu_{1,1} = 1$. On peut noter que le terme $\nu_{1,1}$ ne peut être égal à zéro puisqu'un des $\nu_{i,j}$ doit être non-nul. De plus, puisque $w_{1,1} = 0$, nous avons que $2w_{2,1}\cdots+nw_{n,1} = n-1$ arrive seulement si $w_{i,1} = \nu_{i,1}$. Notons que le cas $2w_{2,1}\cdots+nw_{n,1} = n$ ne peut jamais arriver.

On conclut donc que la contribution devient

$$(-1)^{\nu_{2,1}+\cdots+\nu_{n,1}} = -(-1)^{\nu_{1,1}+\nu_{2,1}+\ldots+\nu_{n,1}}.$$

4.3.3.4. *Combinaison des termes*

Il nous reste à calculer $X_\nu(a)$ en faisant $A+B+C$ avec tous les cas que nous avons trouvés.

Si $\nu_{i,j} \neq 0$ pour quelques $i,j > 1$, alors le coefficient est 0, sauf pour le cas $X_{(d^{n/d})}$ où alors le coefficient serait d.

Le reste des coefficients non-nuls correspondent aux $\nu_{i,j} = 0$ pour tous $i,j > 1$. Le tableau à la page suivante résume l'ensemble des cas possibles en considérant $n \geq 2$. Le symbole $*$ signifie que toutes valeurs sont permises, $\nu_{i,1} > 0$ (resp. $\nu_{1,j} > 0$) signifie que l'inégalité est vraie pour un sous-index tel que $i > 1$ (resp. $j > 2$) et f est une abréviation de $f(\nu_{1,1}, \ldots, \nu_{1,n})$.

À l'aide de ce tableau, lorsque $\nu_{i,j} = 0$ pour tous $i,j > 1$, on voit que le coefficient de $X_\nu(a)$ est égal à 0 si $\nu_{i_0,1} > 0$ pour certains $i_0 > 1$ tandis que dans les autres cas, il est égal à $f(\nu_{1,1}, \ldots, \nu_{1,n})$. Maintenant, la proposition (4.14) nous donne que le côté gauche de $A+B+C$ est égal à :

$$A+B+C = \sum_{d|n} dX_{(d^{n/d})}(a) + \sum_{\substack{\nu \\ \nu_{i,j}=0, i>1}} (-1)^n \frac{n!}{(1!)^{\nu_{1,1}}(2!)^{\nu_{1,2}} \cdots (n!)^{\nu_{1,n}}} X_\nu(a).$$

Il nous reste à trouver que le côté droit est $q^{n-2} + (-1)^n q^{n-2}$. Si on refait les mêmes opérations, mais pour $\ell = 0$ (pas de condition sur les coefficients) et puisque nous connaissons déjà le résultat pour $\ell = 0$, nous concluons que

$$\sum_{d|n} dX_{(d^{n/d})} + \sum_{\substack{\nu \\ \nu_{i,j}=0, i>1}} (-1)^n \frac{n!}{(1!)^{\nu_{1,1}}(2!)^{\nu_{1,2}} \cdots (n!)^{\nu_{1,n}}} X_\nu = q^n + (-1)^n q^n.$$

Quand nous prenons $\ell = 2$, il y aura simplement une division du côté droit par q^2. Nous montrons ainsi que

$$\sum_{d|n} dX_{(d^{n/d})}(a) + \sum_{\substack{\nu \\ \nu_{i,j}=0, i>1}} (-1)^n \frac{n!}{(1!)^{\nu_{1,1}}(2!)^{\nu_{1,2}} \cdots (n!)^{\nu_{1,n}}} X_\nu(a) = q^{n-2} + (-1)^n q^{n-2}.$$

TABLE 4.1. Résumé des résultats

$\nu_{1,1}$	$\nu_{1,2}$	$\nu_{1,j}, j>2$	$\nu_{i,1}, i>1$	A	B	C	A + B + C
0	$\neq 1$	$*$	>0	0	0	0	0
$*$	$*$	>0	0	0	1	$f-1$	f
0	1	0	0	1	0	$f-1$	f
$*$	1	0	>0	$(-1)^{\nu_{1,1}+\cdots+\nu_{n,1}}$	$-(-1)^{\nu_{1,1}+\cdots+\nu_{n,1}}$	0	0
0	1	>0	>0	0	0	0	0
0	>1	$*$	0	0	1	$f-1$	f
1	0	0	>0	$(-1)^{\nu_{1,1}+\cdots+\nu_{n,1}}$	$(-1)^{\nu_{1,1}+\cdots+\nu_{n,1}}$	$-2(-1)^{\nu_{1,1}+\cdots+\nu_{n,1}}$	0
$\neq 0$	$*$	>0	>0	0	0	0	0
1	1	0	0	-1	2	$f-1$	f
1	>1	0	0	0	1	$f-1$	f
$*$	>1	0	>0	0	0	0	0
>1	0	0	0	$(-1)^{\nu_{1,1}}\nu_{1,1}$	$1-(-1)^{\nu_{1,1}}\nu_{1,1}+(-1)^{\nu_{1,1}}$	$f-1-(-1)^{\nu_{1,1}}$	f
>1	0	0	>0	$(-1)^{\nu_{1,1}+\cdots+\nu_{n,1}}\nu_{1,1}$	$-(-1)^{\nu_{1,1}+\cdots+\nu_{n,1}}\nu_{1,1}+(-1)^{\nu_{1,1}+\cdots+\nu_{n,1}}$	$-(-1)^{\nu_{1,1}+\cdots+\nu_{n,1}}$	0
>1	1	0	0	$(-1)^{\nu_{1,1}}$	$1-(-1)^{\nu_{1,1}}$	$f-1$	f

4.3.4. Cas particuliers

Pour illustrer comment la preuve fonctionne, nous allons faire le cas où $n = 4$ et $n = 5$. Pour simplifier la notation, nous allons omettre le a dans $\mathcal{E}_w(a)$.

4.3.5. $n = 4$

On peut trouver que $\gamma(1,0) = \gamma(0,1) = 2$ et $\gamma(2,0) = 5$.
On a donc :

$$\begin{aligned} A &: 4\mathcal{E}_{(0)} - 3\mathcal{E}_{(1)} - 2\mathcal{E}_{(2)} + 2\mathcal{E}_{(1,1)}, \\ B &: \mathcal{E}_{(1)} - \mathcal{E}_{(1,1)}, \\ C &: -2\mathcal{E}_{(1)} + 2\mathcal{E}_{(1^2)} + 5\mathcal{E}_{(1,1)}. \end{aligned}$$

Alors,

$$A + B + C = 4\mathcal{E}_{(0)} - 4\mathcal{E}_{(1)} + 2\mathcal{E}_{(1^2)} - 2\mathcal{E}_{(2)} + 6\mathcal{E}_{(1,1)}. \tag{4.3.9}$$

La tableau suivant nous donne toutes les équations nécessaires pour calculer $A + B + C$. L'acronyme CG indique le côté gauche de l'équation et réciproquement l'acronyme CD indique le côté droit de l'équation.

TABLE 4.2. Calcul de $A + B + C$ quand $n = 4$

ν	CG $\mathcal{E}_\nu$	CD $\mathcal{E}_\nu$
(0)	$X_{(1,1,1,1)} + X_{(1,1,1^2)} + X_{(1,1^3)} + X_{(1^2,1^2)} + X_{(1^4)} + X_{(1,1,2)}$ $+X_{(1^2,2)} + X_{(2,2)} + X_{(2^2)} + X_{(1,3)} + X_{(1,3)} + X_{(4)}$	q^2
(1)	$4X_{(1,1,1,1)} + 3X_{(1,1,1^2)} + 2X_{(1^2,1^2)} + 2X_{(1,1^3)} + X_{(1^4)} + 2X_{(1,1,2)}$ $+X_{(1^2,2)} + X_{(1,3)}$	q^2
(1^2)	$X_{(1,1,1^2)} + 2X_{(1^2,1^2)} + X_{(1,1^3)} + X_{(1^4)} + X_{(1^2,2)}$	q
(2)	$X_{(1,1,2)} + X_{(1^2,2)} + 2X_{(2,2)} + X_{(2^2)}$	$\frac{q(q-1)}{2}$
$(1,1)$	$6X_{(1,1,1,1)} + 3X_{(1,1,1^2)} + X_{(1^2,1^2)} + X_{(1,1^3)} + X_{(1,1,2)}$	$\frac{q(q-1)}{2}$

Nous arrivons donc à :

$$4X_{(4)} + 2X_{(2^2)} + 24X_{(1,1,1,1)} + 12X_{(1,1,1^2)} + 4X_{(1,1^3)} + 6X_{(1^2,1^2)} + 2X_{(1^4)} = 2q^2,$$

ce qui est le résultat attendu.

4.3.6. $n = 5$

On peut calculer

TABLE 4.3. Liste des γ lorsque $n = 5$

$\gamma(1,0,0)$	$\gamma(0,1,0)$	$\gamma(0,0,1)$	$\gamma(2,0,0)$	$\gamma(1,1,0)$	$\gamma(3,0,0)$
2	2	2	5	7	16

Dans ce cas, nous avons que

$$\begin{aligned}
A &: 5\mathcal{E}_{(0)} - 4\mathcal{E}_{(1)} - 3\mathcal{E}_{(2)} - 2\mathcal{E}_{(3)} + 3\mathcal{E}_{(1,1)} + 2\mathcal{E}_{(1,2)} - 2\mathcal{E}_{(1,1,1)},\\
B &: \mathcal{E}_{(1)} - \mathcal{E}_{(1,1)} - \mathcal{E}_{(1,2)} + \mathcal{E}_{(1,1,1)},\\
C &: -2\mathcal{E}_{(1)} + 2\mathcal{E}_{(1^2)} - 2\mathcal{E}_{(1^3)} + 5\mathcal{E}_{(1,1)} - 7\mathcal{E}_{(1,1^2)} + 2\mathcal{E}_{(1,2)} - 16\mathcal{E}_{(1,1,1)}.
\end{aligned}$$

Alors, on voit que

$$\begin{aligned}
A + B + C &= 5\mathcal{E}_{(0)} - 5\mathcal{E}_{(1)} + 2\mathcal{E}_{(1^2)} - 2\mathcal{E}_{(1^3)} - 3\mathcal{E}_{(2)} - 2\mathcal{E}_{(3)}\\
&\quad +7\mathcal{E}_{(1,1)} + 3\mathcal{E}_{(1,2)} - 7\mathcal{E}_{(1,1^2)} - 17\mathcal{E}_{(1,1,1)}. \qquad (4.3.10)
\end{aligned}$$

La tableau suivant nous donne toutes les équations nécessaires pour calculer $A + B + C$.

TABLE 4.4. Calcul de $A + B + C$ quand $n = 5$

ν	CG $\mathcal{E}_\nu$	CD $\mathcal{E}_\nu$
(0)	$X_{(1,1,1,1,1)} + X_{(1,1,1,1^2)} + X_{(1,1^2,1^2)} + X_{(1,1,1^3)} + X_{(1,1^4)} + X_{(1^5)} + X_{(1,1,1,2)}$ $+X_{(1,1^2,2)} + X_{(1^3,2)} + X_{(1,2,2)} + X_{(1,2^2)} + X_{(1,1,3)} + X_{(1^2,3)} + X_{(1,4)} + X_{(2,3)} + X_{(5)}$	q^3
(1)	$5X_{(1,1,1,1,1)} + 4X_{(1,1,1,1^2)} + 3X_{(1,1^2,1^2)} + 3X_{(1,1,1^3)} + 2X_{(1,1^4)} + X_{(1^5)} + 3X_{(1,1,1,2)}$ $+2X_{(1,1^2,2)} + X_{(1^3,2)} + X_{(1,2,2)} + X_{(1,2^2)} + 2X_{(1,1,3)} + X_{(1^2,3)} + X_{(1,4)}$	q^3
(1^2)	$X_{(1,1,1,1^2)} + 2X_{(1,1^2,1^2)} + X_{(1,1,1^3)} + X_{(1,1^4)} + X_{(1^5)} + X_{(1,1^2,2)} + X_{(1^3,2)} + X_{(1^2,3)}$	q^2
(1^3)	$X_{(1,1,1^3)} + X_{(1,1^4)} + X_{(1^5)} + X_{(1^3,2)}$	q
(2)	$X_{(1,1,1,2)} + X_{(1,1^2,2)} + X_{(1^3,2)} + 2X_{(1,2,2)} + X_{(1,2^2)} + X_{(2,3)}$	$\frac{q^2(q-1)}{2}$
(3)	$X_{(1,1,3)} + X_{(1^2,3)} + X_{(2,3)}$	$\frac{q(q^2-1)}{3}$
$(1,1)$	$10X_{(1,1,1,1,1)} + 6X_{(1,1,1,1^2)} + 3X_{(1,1^2,1^2)} + 3X_{(1,1,1^3)} + X_{(1,1^4)} + 3X_{(1,1,1,2)}$ $+X_{(1,1^2,2)} + X_{(1,1,3)}$	$\frac{q^2(q-1)}{2}$
$(1,2)$	$3X_{(1,1,1,2)} + 2X_{(1,1^2,2)} + X_{(1^3,2)} + 2X_{(1,2,2)} + X_{(1,2^2)}$	$\frac{q^2(q-1)}{2}$
$(1,1^2)$	$3X_{(1,1,1,1^2)} + 4X_{(1,1^2,1^2)} + 2X_{(1,1,1^3)} + X_{(1,1^4)} + X_{(1,1^2,2)}$	$q(q-1)$
$(1,1,1)$	$10X_{(1,1,1,1,1)} + 4X_{(1,1,1,1^2)} + X_{(1,1^2,1^2)} + X_{(1,1,1^3)} + X_{(1,1,1,2)}$	$\frac{q(q-1)(q-2)}{6}$

En additionnant tous les termes, on trouve

$$5X_{(5)} - 120X_{(1,1,1,1,1)} - 60X_{(1,1,1,1^2)} - 30X_{(1,1^2,1^2)} - 20X_{(1,1,1^3)} - 5X_{(1,1^4)} = 0,$$

ce qui est le résultat attendu.

Chapitre 5

AUTRES RÉSULTATS UTILISANT LES FONCTIONS L

Dans ce chapitre, nous fixerons en même temps la trace et le terme constant des polynômes. La première section portera d'abord sur un résultat asymptotique et la deuxième section nous permettra d'étendre nos recherches sur un résultat exact. Pour arriver à ces résultats, nous utiliserons les fonctions L. Ce sont deux résultats qui proviennent d'un article de Carlitz [**2**]. Bien que le sujet semble un peu différent de ce que nous avons fait jusqu'à maintenant, les méthodes développées dans ce chapitre seront très utiles dans la prochaine section. Effectivement, avec ces connaissances, nous pourrons montrer la preuve originale que Kuz'min avait développée pour le théorème (3.0.8).

5.1. RÉSULTAT ASYMPTOTIQUE

Dans un premier cas, nous montrons le théorème suivant.

Théorème 5.1. *Le nombre de polynômes irréductibles de la forme* (0.0.1) *avec les coefficients* a_1 *et* a_n *fixés dans* $\mathbb{F}_q$ *est donné par*

$$\frac{q^n}{nq(q-1)} + O(q^{n/2}) \tag{5.1.1}$$

où $q = p^k$

5.1.1. Définition et stratégie

Si on étudie $M = x^n + a_1x^{n-1} + ... + a_ix^{n-i} + \cdots + a_n$ et en reprenant le caractère ψ défini en (3.1.8), on pose :

$$\lambda(M) = \lambda_b(M) = \psi(ba_1),$$

un caractère pour un polynôme M de la forme (0.0.1) de degré plus grand ou égal à 1 avec un $b \in \mathbb{F}_q$ fixé. De même, pour ζ une racine primitive de M,

définissons un caractère multiplicatif pour un élément a de la forme $a = \zeta^r$:

$$X(a) = e^{2\pi ir/(q-1)}$$

Pour définir X sur tout le corps, posons $X(0) = 0$ pour $x \nmid M$. Maintenant, définissons

$$\chi(M) = \chi_c(M) = X(a_n^c) \tag{5.1.2}$$

pour un c fixé. Ainsi, de χ, on constate que

$$\sum_{\chi} \chi(M) = \begin{cases} q-1 & \text{si } a_n = 1, \\ 0 & \text{sinon,} \end{cases} \tag{5.1.3}$$

et de λ, on constate que

$$\sum_{\lambda} \lambda(M) = \begin{cases} q & \text{si } a_1 = 0, \\ 0 & \text{sinon.} \end{cases} \tag{5.1.4}$$

Le résultat (5.1.4) est simplement une réécriture du lemme (3.27). Pour montrer (5.1.3), on refait les mêmes opérations que nous avons faites pour montrer (3.27), mais en utilisant le caractère χ. De ces deux résultats, on déduit directement ces deux corollaires :

$$\sum_{\chi} \overline{\chi}(b)\chi(M) = \begin{cases} q-1 & \text{si } a_n = b, \\ 0 & \text{sinon,} \end{cases}$$

$$\sum_{\lambda} \overline{\lambda}(t)\lambda(M) = \begin{cases} q & \text{si } a_1 = t, \\ 0 & \text{sinon.} \end{cases}$$

Ensuite, en fixant le degré du polynôme M à m et si $m \geq 1$, on peut constater que

$$\sum_{\deg(M)=m} \lambda(M) = 0 \qquad \text{si } \lambda \neq \lambda_0, \tag{5.1.5}$$

$$\sum_{\deg(M)=m} \chi(M) = 0 \qquad \text{si } \chi \neq \chi_0. \tag{5.1.6}$$

On peut aussi montrer que ces deux fonctions sont multiplicatives. Lorsqu'on multiplie deux polynômes unitaires M et N de trace a_1 et $\bar{a}_1$, la nouvelle trace sera simplement $a_1 + \bar{a}_1$. Donc,

$$\lambda(MN) = \lambda(b(a_1 + \bar{a}_1)) = e^{\frac{2\pi i\tau(b(a_1+\bar{a}_1))}{p}}$$

$$= e^{\frac{2\pi i\tau(ba_1)}{p}} e^{\frac{2\pi i\tau(b\bar{a}_1)}{p}} = \lambda(ba_1)\lambda(b\bar{a}_1) = \lambda(M)\lambda(N).$$

La preuve est analogue pour le caractère χ.

Définition 5.2. Posons :

$$L(s,\lambda,\chi)=\sum_{M}\lambda(M)\chi(M)|M|^{-s} \qquad \text{où } |M|=q^{\deg(M)} \text{ et Re(s)>1.}$$

De cette définition, nous pouvons conclure :

Lemme 5.3.

$$L(s,\lambda,\chi)=\prod_{P}(1-\lambda(P)\chi(P)|P|^{-s})^{-1}, \tag{5.1.7}$$

où P *sont les polynômes irréductibles unitaires de* $\mathbb{F}_q[x]$.

DÉMONSTRATION. On a que

$$\prod_{P}(1-\lambda(P)\chi(P)|P|^{-s})^{-1}=\prod_{P}\sum_{r=0}^{\infty}(\lambda(P)\chi(P)|P|^{-s})^{r}$$

Puisque λ et χ sont multiplicatifs, lorsque que nous ferons la distributivité, on remarquera que tous les polynômes de $\mathbb{F}_q[x]$ seront atteints exactement une fois. Le résultat est donc montré. □

5.1.1.1. *Stratégie*

En simplifiant (5.1.7), nous allons être en mesure de faire apparaître la quantité qui nous intéresse. Pour travailler plus aisément, nous appliquons le log de chaque coté de l'équation (5.1.7). Nous avons que

$$\log L(s,\lambda,\chi)=-\sum_{P}\log(1-\lambda(P)\chi(P)|P|^{-s}).$$

De plus, en développant le tout avec la série de Taylor de $\log(1-x)$, nous obtenons :

$$\log(L(s,\lambda,\chi))=\sum_{P}\sum_{r=1}^{\infty}\frac{1}{r}\lambda(P^r)\chi(P^r)|P|^{-rs}$$

Maintenant, divisons la partie de droite en deux sommes distinctes. D'abord, prenons les polynômes P' tels que $(P')^r$ possèdent les coefficients $a_1=a$ et $a_n=\ell$ où $a,\ell\in\mathbb{F}_q$ sont fixés selon notre choix. L'autre somme sera celle qui contient les autres polynômes. Nous avons alors

$$\log(L(s,\lambda,\chi))=\psi(ba)X(\ell^c)\sum_{P',r}\frac{|P'|^{-rs}}{r}+\sum_{P_{autre},r}\frac{1}{r}\lambda(P^r)\chi(P^r)|P|^{-rs}.$$

Donc,

$$\psi(-ba)X(\ell^{-c})\log(L(s,\lambda,\chi))=\sum_{P',r}\frac{|P'|^{-rs}}{r}+\psi(-ba)X(\ell^{-c})\sum_{P_{autre},r}\frac{1}{r}\lambda(P^r)\chi(P^r)|P|^{-rs}.$$

À présent, on somme les deux côtés sur tous les λ et les χ indépendamment l'un de l'autre. Dans la deuxième somme de la partie de droite, pour un P et un r fixés, il n'y a aucune chance que l'intérieur des fonctions λ et χ soit nul. Par exemple, supposons que dans P^r, $a_1 = d$. Alors, nous avons que

$$\psi(-ba)\lambda(P^r) = \psi(-ba)\lambda(d) = \psi(b(d-a)).$$

Puisque a est dans la première somme, d ne peut être égal à a. Ainsi, $\psi(b(d-a))$ ne peut être égal à zéro. Puisqu'on peut effectuer le même raisonnement avec χ, à l'aide de (5.1.3) et (5.1.4), on déduit que

$$\sum_{\lambda,\chi} \psi(-ba)X(\ell^{-c}) \log(L(s,\lambda,\chi)) = q(q-1) \sum_{P',r} \frac{1}{r} |P'|^{-rs}. \tag{5.1.8}$$

En posant $\mu(n,r,a,\ell)$ le nombre de polynômes P' de degré n/r tel que $(P')^r$ possède les coefficients $a_1 = a$ et $a_n = \ell$, on a

$$\begin{aligned}
\sum_{\lambda,\chi} \psi(-ba)X(\ell^{-c}) \log(L(s,\lambda,\chi)) &= q(q-1) \sum_{P',r} \frac{1}{r} |P'|^{-rs} \\
&= q(q-1) \sum_{r=1}^{\infty} \frac{1}{r} \sum_{P'} |P'|^{-rs} \\
&= q(q-1) \sum_{n=1}^{\infty} \sum_{r|n} \frac{1}{r}\, \mu(n,r,a,\ell) q^{-ns}. \quad (5.1.9)
\end{aligned}$$

Remarquons maintenant que pour montrer le résultat (5.1), nous n'avons qu'à isoler $\mu(n,1,a,\ell)$. Pour ce faire, nous allons calculer quelques valeurs de la partie gauche de l'équation (5.1.9).

5.1.2. Simplification de $\sum_{\lambda,\chi} \psi(-ba)X(\ell^{-c}) \log(L(s,\lambda,\chi))$

Plus particulièrement, nous travaillerons seulement sur le terme $\log(L(s,\lambda,\chi))$. Pour y arriver, nous devrons traiter séparément les cas qui contiennent des λ_0 et des χ_0.

(1) $\lambda = \lambda_0$ et $\chi = \chi_0$

Puisque $\chi_0(0)$=0, nous allons retirer le cas où $a_n = 0$. Ainsi, on a que

$$L(s,\lambda_0,\chi_0) = \sum_{a_n \neq 0} |M|^{-s}.$$

On sait que chaque $|M|$ pour un degré fixé m nous donnera la même valeur et puisqu'il existe $q^{(m-1)}(q-1)$ polynômes de degré m avec

$a_n \neq 0$. Ainsi, nous avons que

$$\begin{aligned} L(s,\lambda_0,\chi_0) &= \sum_{a_n\neq 0} |M|^{-s} \\ &= 1+\sum_{m=1}^{\infty}(q-1)q^{(m-1)}q^{-ms} \\ &= 1+q^{-1}(q-1)\sum_{m=1}^{\infty}(q^{(1-s)})^m \\ &= 1+q^{-1}(q-1)q^{(1-s)}\sum_{m=0}^{\infty}(q^{(1-s)})^m \\ &= 1+q^{-1}(q-1)q^{(1-s)}(1-q^{(1-s)})^{-1} \\ &= (1-q^{-s})(1-q^{(1-s)})^{-1}. \end{aligned}$$

En prenant le log de chaque côté et en développant avec la série de Taylor de $\log(1-x)$, on déduit que

$$\log(L(s,\lambda_0,\chi_0)) = \sum_{r=1}^{\infty}\frac{1}{r}(q^r-1)q^{-sr}. \tag{5.1.10}$$

(2) $\lambda = \lambda_0$ et $\chi \neq \chi_0$

Avec (5.1.6) et puisque que $|M|$ est constant sur un degré fixé, on a

$$\begin{aligned} L(s,\lambda_0,\chi) &= \sum_{M}\chi(M)|M|^{-s} \\ &= \sum_{m=0}^{\infty}q^{-ms}\sum_{\deg(M)=m}\chi(M) \\ &= \sum_{\deg(M)=0}\chi(M) \\ &= 1. \end{aligned}$$

En prenant le log de chaque côté, on obtient

$$\log(L(s,\lambda_0,\chi)) = 0. \tag{5.1.11}$$

(3) $\lambda \neq \lambda_0$ et $\chi = \chi_0$
On peut voir que

$$\begin{aligned} L(s,\lambda,\chi_0) &= \sum_M \lambda(M)\chi_0(M)|M|^{-s}, \\ &= \sum_{a_n \neq 0} \lambda(M)|M|^{-s}, \\ &= \sum_M \lambda(M)|M|^{-s} - \sum_M \lambda(xM)|xM|^{-s}, \\ &= \sum_M \lambda(M)|M|^{-s} - q^{-s}\sum_M \lambda(xM)|M|^{-s}. \end{aligned}$$

Puisque $\lambda(xM) = \lambda(M)$, nous avons que

$$\begin{aligned} L(s,\lambda,\chi_0) &= \sum_M \lambda(M)|M|^{-s} - q^{-s}\sum_M \lambda(M)|M|^{-s}, \\ &= (1-q^{-s})\sum_M \lambda(M)|M|^{-s}. \end{aligned}$$

En utilisant (5.1.4) et (5.1.5), nous avons

$$L(s,\lambda,\chi_0) = 1 - q^{-s}$$

En prenant le log de chaque côté et en développant avec la série avec la série de Taylor de $\log(1-x)$, on trouve :

$$\log(L(s,\lambda,\chi_0)) = \sum_{r=1}^{\infty} \frac{-q^{-rs}}{r} \tag{5.1.12}$$

(4) $\lambda \neq \lambda_0$ et $\chi \neq \chi_0$

Posons,

$$\tau_m = \tau_m(\lambda,\chi) = \sum_{\deg(M)=m} \lambda(M)\chi(M).$$

Avec cette définition, on peut arriver à :

$$L(s,\lambda,\chi) = \sum_{m=0}^{\infty} \tau_m(\lambda,\chi)q^{-ms}.$$

Maintenant, regardons τ_m pour $m > 1$. On remarque qu'il y a m coefficients dans M. Cependant, on voit bien que le premier et le dernier sont déjà fixés dans la sommation. Alors, nous avons donc seulement $m-2$ qui sont laissés libres. Ceci implique que

$$\tau_m = q^{(m-2)} \sum_{a_1, a_m \in \mathbb{F}_q} \psi(ba_1)\chi(a_m^c).$$

Puisque les a_1 et a_m sont sommés indépendamment, on conclut par (5.1.3) et (5.1.4) que $\tau_m = 0$ et donc que

$$L(s, \lambda, \chi) = \sum_{m=0}^{\infty} \tau_m(\lambda, \chi) q^{-ms} = 1 + \tau_1(\lambda, \chi) q^{-s}.$$

En prenant le log de chaque côté et en développant avec la série de Taylor de $\log(1+x)$, on déduit que

$$\log(L(s, \lambda, \chi)) = \sum_{r=1}^{\infty} \frac{(-1)^{r-1} \tau_1^r(\lambda, \chi) q^{-rs}}{r}. \tag{5.1.13}$$

Nous sommes prêts à simplifier la partie gauche de (5.1.9). À l'aide de (5.1.10), (5.1.11), (5.1.12) et (5.1.13), on déduit que

$$\begin{aligned}
&\sum_{\lambda, \chi} \psi(-ba)\chi(\ell^{-c}) \log(L(s, \lambda, \chi)) \\
&= \psi(0)\chi(\ell^0) \log(L(s, \lambda_0, \chi_0)) + \sum_{a \neq 0} \psi(-ba)\chi(\ell^0) \log(L(s, \lambda, \chi_0)) \\
&+ \sum_{c \neq 0} \psi(0)\chi(\ell^{-c}) \log(L(s, \lambda_0, \chi)) + \sum_{a \neq 0, c \neq 0} \psi(-ba)\chi(\ell^{-c}) \log(L(s, \lambda, \chi)) \\
&= \sum_{r=1}^{\infty} \left(\frac{(q^r - 1) q^{-sr}}{r} - \sum_{b \neq 0} \frac{\psi(-ba) q^{-rs}}{r} + \sum_{a \neq 0, c \neq 0} \frac{(-1)^{r-1} \psi(-ba)\chi(\ell^{-c}) \tau_1^r(\lambda, \chi) q^{-rs}}{r} \right) \\
&= \sum_{r=1}^{\infty} \frac{q^{-rs} W_r}{r}
\end{aligned} \tag{5.1.14}$$

$$\text{où } W_r = q^r - 1 - \sum_{b \neq 0} \psi(-ba) + (-1)^{r-1} \sum_{a \neq 0, c \neq 0} \psi(-ba)\chi(\ell^{-c}) \tau_1^r(\lambda, \chi).$$

5.1.3. Isoler le terme $\mu(n, 1, a, \ell)$ dans l'équation (5.1.9)

Voici les étapes finales pour monter le théorème 5.1. Commençons par combiner (5.1.14) et (5.1.9). Ainsi, nous avons

$$\sum_{r=1}^{\infty} \frac{q^{-rs} W_r}{r} = q(q-1) \sum_{n=1}^{\infty} \sum_{r \mid n} \frac{1}{r} \mu(n, r, a, \ell) q^{-ns}, \tag{5.1.15}$$

qui implique directement

$$q(q-1)\sum_{r|n}\frac{\mu(n,r,a,\ell)}{r}=\frac{W_n}{n}. \tag{5.1.16}$$

Nous allons maintenant borner la somme $q(q-1)\sum_{r|n,r>1}\frac{\mu(n,r,a,\ell)}{r}$. Si $r=2$, on voit que les polynômes ont au plus $n/2-2$ coefficients libres puisque que les polynômes sont unitaires et que a et l sont fixés. Ainsi, nous avons que

$$q(q-1)\frac{\mu(n,2,a,\ell)}{2}=O(q^{n/2}).$$

Si $r>2$, on peut conclure avec un raisonnement similaire que

$$q(q-1)\sum_{r|n,r>2}\frac{\mu(n,r,a,\ell)}{r}=O(q^{n/3}\sum_{r|n}\frac{1}{r})=O(q^{n/2}).$$

Alors, nous avons

$$q(q-1)\sum_{r|n,r>1}\frac{\mu(n,r,a,\ell)}{r}=O(q^{n/2}) \tag{5.1.17}$$

Nous utiliserons (5.1.17) un peu plus loin. Maintenant que nous avons simplifié $\sum_{r|n,r>1}\frac{\mu(n,r,a,\ell)}{r}$, nous allons faire de même avec W_n. Pour pour ce faire, nous allons borner τ_1. D'abord, en utilisant les sommes de Gauss, on peut remarquer que :

$$\tau_1(\psi,\chi)=\sum_{a\in\mathbb{F}_q}\psi(ba)\chi(a)=G_{\psi,\chi}(-b)\sqrt{q}$$

En utilisant (3.31), on a que

$$G_{\psi,\chi}(-b)\sqrt{q}=\sqrt{q}\chi(-b)^{-1}G_{\psi,\chi}(-1)$$

Avec (3.32), on déduit que

$$|\tau_1(\psi,\chi)|=|\sqrt{q}\chi(-b^c)^{-1}G_{\psi,\chi}|=\sqrt{q}=q^{1/2}.$$

Avec cette majoration, on trouve que

$$\sum_{a\neq0,c\neq0}\psi(-ba)X(a^{-c})\tau_1^n(\lambda,\chi)=O(q^{n/2+2}),$$

et ainsi

$$W_n=q^n-1-\sum_{a\neq0}\psi(-ba)+O(q^{n/2+2}) \tag{5.1.18}$$

En partant de (5.1.16) et en le combinant avec (5.1.17) et (5.1.18), nous trouvons

$$q(q-1)\sum_{r|n}\frac{\mu(n,r,a,\ell)}{r}=\frac{W_n}{n}$$

$$q(q-1)\left(\mu(n,1,a,\ell)+\sum_{r|n,r>1}\frac{\mu(n,r,a,\ell)}{r}\right)=\frac{q^n-1-\sum_{a\neq 0}\psi(-ba)+O(q^{n/2+2})}{n}$$

$$q(q-1)\mu(n,1,a,\ell)+O(q^{n/2})=\frac{q^n-1-\sum_{a\neq 0}\psi(-ba)+O(q^{n/2+2})}{n}$$

Puisque $-\sum_{a\neq 0}\psi(-ba)=1$, on trouve

$$\mu(n,1,a,\ell)=\frac{q^n}{nq(q-1)}+O(q^{n/2}),$$

démontrant ainsi le théorème 5.1.

5.2. RÉSULTAT EXACT

En modifiant quelques éléments qui nous mènent au théorème précédent, on peut arriver à un résultat exact partiel. On doit toujours choisir un coefficient a_1, mais pour le coefficient a_n, il faudra statuer à savoir s'il s'agit d'un carré dans $\mathbb{F}_q$. Il sera donc convivial d'utiliser le caractère $\mathrm{sgn}(a)$ défini au chapitre 3.

Théorème 5.4. *Pour $p\neq 2$, soit $\xi(n,r,a,1)$ le nombre de polynômes irréductibles $\overline{P}$ de degré n/r tel que $\overline{P}^r$ a comme coefficient $a_1=a$ et a_n un carré. Notons aussi $\xi(n,r,a,-1)$ de la même façon sauf que a_n n'est pas un carré. Alors si n est pair, nous avons que*

$$\sum_{r|n}\frac{\xi(n,r,a,\mathrm{sgn}(\ell))}{r}=\begin{cases}\frac{1}{2n}(q^{n-1}-1-q^{(n/2-1)}\mathrm{sgn}((-1)^{n/2}\ell)(q-1)) & \text{si } a=0,\\ \frac{1}{2n}(q^{n-1}+q^{(n/2-1)}\mathrm{sgn}((-1)^{n/2}\ell)) & \text{si } a\neq 0,\end{cases}$$

et que si n est impair, nous arrivons à :

$$\sum_{r|n}\frac{\xi(n,r,a,\mathrm{sgn}(\ell))}{r}=\begin{cases}\frac{1}{2n}(q^{n-1}-1) & \text{si } a=0,\\ \frac{1}{2n}(q^{n-1}+\mathrm{sgn}((-1)^{(n-1)/2}\ell a)q^{(n-1)/2}) & \text{si } a\neq 0,\end{cases}$$

Il s'agit presque de la même preuve que nous venons de faire pour le théorème 5.1. La différence est que nous changeons le caractère χ par le caractère sgn défini en (3.1.10). Nous définissons

$$\bar{\chi}(a)=\bar{\chi}_m(a)=\mathrm{sgn}(a^m),$$

seulement pour les cas où m égale 0 ou 1. De cette façon, on peut voir que

$$\tau_1(\lambda, sgn) = \sum_a \psi(-ba) sgn(a),$$

On remarque que $\tau_1(\lambda, sgn)$ est une somme de Gauss. Pour uniformiser la notation, posons

$$G(-b) = \sum_a \psi(-ba) sgn(a).$$

Des propriétés (3.31) et (3.33), on obtient immédiatement

$$G(-b) = sgn(b)G(1), \tag{5.2.1}$$

$$G^2(1) = sgn(-1)q. \tag{5.2.2}$$

En posant $\overline{P}'$ l'ensemble des polynômes qui satisfont la définissions de $\xi(n, r, a, sgn(\ell))$, nous pouvons refaire des manipulations similaires à celles que nous avons faites pour trouver l'égalité (5.1.8). L'équation sera sensiblement la même sauf pour la partie de droite. En effet, puisque m peut être seulement égal à un ou deux, nous trouvons

$$\sum_{\lambda, sgn} \psi(-ba) sgn(\ell^m) \log(L(s, \lambda, sgn)) = 2q \sum_{P', r} \frac{1}{r} |\overline{P}'|^{-rs}. \tag{5.2.3}$$

Maintenant, si nous faisons à nouveau les manipulations que nous avons faites pour trouver (5.1.15), nous obtenons

$$2q \sum_{P', r} \frac{1}{r} |\overline{P}'|^{-rs} = \sum_{r=1}^{\infty} \frac{q^{-rs} \overline{W}_r}{r}$$

$\overline{W}_r$ sera presque identique à W_r. Seule la définition de τ_1 apportera une modification. Effectivement, on obtient

$$\overline{W}_r = q^r - 1 - \sum_{b \neq 0} \psi(-ba) + (-1)^{r-1} \sum_{b \neq 0} \psi(-ba) sgn(\ell) G^r(-b)). \tag{5.2.4}$$

Nous obtenons ainsi

$$2q \sum_{r|n} \frac{\xi(n, r, a, \ell)}{r} = \frac{\overline{W}_n}{n}. \tag{5.2.5}$$

Pour continuer, nous devons simplifier $\overline{W}_n$. Pour ce faire, nous allons séparer le cas où n est pair de celui où il est impair.

(1) n est pair

Si on regarde la dernière somme de $\overline{W}_n$ et qu'on utilise (5.2.1) et (5.2.2),

on peut constater que

$$(-1)^{n-1}\sum_{b\neq 0}\psi(-ba)sgn(\ell)G^n(-b) = -\sum_{b\neq 0}\psi(-ba)sgn(\ell)(sgn(b)G(1))^n$$
$$= -\sum_{b\neq 0}\psi(-ba)sgn(\ell)sgn(b)^n(sgn(-1)q)^{n/2}.$$

Puisque n est pair, on sait que $sgn(b)^n = 1$. On conclut donc que

$$(-1)^{n-1}\sum_{b\neq 0}\psi(-ba)sgn(\ell)G^n(-b) = -q^{n/2}sgn((-1)^{n/2}\ell)\sum_{b\neq 0}\psi(-ba). \quad (5.2.6)$$

Puisque nous avons

$$-1-\sum_{b\neq 0}\psi(-ba) = -\sum_{\lambda}\psi(-ba),$$

on peut récrire $\overline{W}_n$ à l'aide de (5.1.4) et (5.2.6) pour obtenir

$$\overline{W}_{n_{pair}} = \begin{cases} q^n - q - q^{n/2}sgn((-1)^{n/2}\ell)(q-1) & \text{si } a = 0, \\ \\ q^n + q^{n/2}sgn((-1)^{n/2}\ell) & \text{si } a \neq 0. \end{cases} \quad (5.2.7)$$

(2) Si n est impair

Avec une méthode plutôt similaire au dernier cas et toujours avec (5.2.1) et (5.2.2), on peut simplifier la dernière somme dans $\overline{W}_n$. On remarque

$$(-1)^{n-1}\sum_{b\neq 0}\psi(-ba)sgn(\ell)G^n(-b) = \sum_{b}\psi(-ba)sgn(\ell)(sgn(b)G(1))^n.$$

Puisque n est impair, on a $sgn(b)^n = sgn(b)$. De cette façon, on arrive à

$$\sum_{b}\psi(-ba)sgn(\ell)(sgn(b)G(1))^n = sgn(\ell)G^n(1)\sum_{b}\psi(-ba)sgn(b)$$
$$= sgn(\ell)G^n(1)G(a)$$
$$= sgn(\ell)G^n(1)sgn(-a)G(-1)$$
$$= sgn(-\ell a)(sgn(-1)q)^{(n+1)/2}$$
$$= sgn((-1)^{(n-1)/2}\ell a)q^{(n+1)/2}.$$

Ainsi, de la dernière égalité et en utilisant (5.1.4), on peut déterminer que

$$\overline{W}_{n_{\text{impair}}} = \begin{cases} q^n - q & \text{si } a = 0, \\ q^n + sgn((-1)^{(n-1)/2}\ell a)q^{(n+1)/2} & \text{si } a \neq 0. \end{cases} \tag{5.2.8}$$

Nous sommes maintenant prêt à montrer le théorème principale de cette section.

PREUVE DU THÉORÈME (5.4). En utilisant (5.2.5) et en le combinant avec (5.2.7) et (5.2.8), nous pourrons montrer directement le résultat. Commençons par supposer que n est pair et que $a = 0$.

$$\begin{aligned} 2q \sum_{r|n} \frac{\xi(n, r, a, \ell)}{r} &= \frac{\overline{W}_n}{n} \\ \sum_{r|n} \frac{\xi(n, r, a, \ell)}{r} &= \frac{q^n - q - q^{n/2} sgn((-1)^{n/2}\ell)(q-1)}{2qn} \\ &= \frac{1}{2n}(q^{n-1} - 1 - q^{(n/2-1)} sgn((-1)^{n/2}\ell)(q-1)). \end{aligned}$$

Ce résultat correspond au théorème pour n pair et $a = 0$. Toujours avec n pair, traitons maintenant le cas où $a \neq 0$

$$\begin{aligned} 2q \sum_{r|n} \frac{\xi(n, r, a, \ell)}{r} &= \frac{\overline{W}_n}{n} \\ \sum_{r|n} \frac{\xi(n, r, a, \ell)}{r} &= \frac{q^n + q^{n/2} sgn((-1)^{n/2}\ell)}{2qn} \\ &= \frac{1}{2n}(q^{n-1} + q^{(n/2-1)} sgn((-1)^{n/2}\ell)). \end{aligned}$$

Ce résultat est la seconde partie du théorème pour le cas où n est pair. Maintenant, traitons le cas où n est impair et $a = 0$:

$$\begin{aligned} 2q \sum_{r|n} \frac{\xi(n, r, a, \ell)}{r} &= \frac{\overline{W}_n}{n} \\ \sum_{r|n} \frac{\xi(n, r, a, \ell)}{r} &= \frac{q^n - q}{2qn} \\ &= \frac{1}{2n}(q^{n-1} - 1), \end{aligned}$$

ce qui est le résultat auquel on s'attendait. Finalement pour terminer la preuve, il nous reste à vérifier quand $a \neq 0$:

$$\begin{aligned} 2q \sum_{r|n} \frac{\xi(n,r,a,\ell)}{r} &= \frac{\overline{W}_n}{n} \\ \sum_{r|n} \frac{\xi(n,r,a,\ell)}{r} &= \frac{q^n + sgn((-1)^{(n-1)/2}\ell a) q^{(n+1)/2}}{2qn} \\ &= \frac{1}{2n}(q^{n-1} + sgn((-1)^{(n-1)/2}\ell a) q^{(n-1)/2}), \end{aligned}$$

ce qui montre le théorème. □

On peut souligner que ce résultat est particulièrement utile lorsque n est un nombre premier.

Chapitre 6

UNE PREUVE DE LA FORMULE QUI FIXE DEUX COEFFICIENTS EN UTILISANT LA FONCTION L

Nous allons montrer la preuve originale de (3.0.8) faite par Kuz'min qu'il a publié dans [**11**]. Pour y arriver, nous devrons faire une construction similaire à celle de Carlitz, mais avec un caractère différent.

Avant tout, observons que $f(x) \in \mathbb{F}_q[x]$ est irréductible si et seulement si $f^*(x) = x^{\deg f} f(1/x)$ est irréductible. On peut remarquer que cette opération ne fait que renverser les coefficients. On conclut que compter le nombre de polynômes irréductibles de la forme :

$$x^n + a_1 x^{n-1} + a_2 x^{n-2} + t_3 x^{n-3} + \cdots + t_n$$

est équivalent à le faire avec cette forme

$$t_n x^n + \cdots + a_2 x^2 + a_1 x + 1.$$

Notre problème peut donc se réécrire comme : compter le nombre de polynômes irréductibles (pas nécessairement unitaires) dans $\mathbb{F}_q[x]$ tel que

$$f(x) \equiv a_2 x^2 + 1 \,(\mathrm{mod}\, x^3).$$

Définissons la relation d'équivalence suivante sur les polynômes unitaires dans $\mathbb{F}_q[x]$:

$$f \sim g \qquad \Longleftrightarrow f^*(x) \equiv g^*(x) \,(\mathrm{mod}\, x^3).$$

Soit $\mathcal{P}$ l'ensemble des polynômes unitaires de $\mathbb{F}_q[x]$, alors $\Gamma = \mathcal{P}/\sim$ est un groupe d'ordre q^2 avec l'opération

$$(a_1, a_2) \cdot (b_1, b_2) = (a_1 + b_1, a_2 + b_2 + a_1 b_1).$$

(le neutre est $(0, 0)$ et $(a_1, a_2)^{-1} = (-a_1, a_1^2 - a_2)$.)

Nous allons aussi reprendre notre caractère ψ :

$$\psi(a) = e^{\frac{2\pi i \tau(a)}{p}}.$$

Posons également :

$$\chi_{\lambda_1,\lambda_2}(a_1, a_2) = \psi(\lambda_1 a_1 + \lambda_2(a_2 - a_1^2/2)).$$

Remarque 6.1. On peut rappeler ici que nous ne traitons pas le cas où la caractéristique est 2. On remarque justement qu'il faudrait adapter notre caractère pour traiter ce cas.

Ceci nous donne q^2 différentes fonctions et en particulier $\chi_{0,0} \equiv 1$. Notons que

$$\sum_{\lambda_1,\lambda_1} \chi_{\lambda_1,\lambda_2}(a_1, a_2) = \begin{cases} 0 & (a_1, a_2) \neq (0, 0), \\ \\ q^2 & (a_1, a_2) = (0, 0). \end{cases}$$

En plus, nous avons pour $(\lambda_1, \lambda_2) \neq (0, 0)$,

$$\sum_{a_1,a_2} \chi_{\lambda_1,\lambda_2}(a_1, a_2) = 0.$$

Maintenant, posons la fonction L

$$L(s, \chi) = \sum_M \chi(M)|M|^{-s} = \prod_P (1 - \chi(P)|P|^{-s})^{-1}$$

où P sont les polynômes irréductibles de $\mathbb{F}_q[x]$.

Nous avons alors

$$L(s, \chi_{0,0}) = \sum_M |M|^{-s} = \sum_{n=0}^{\infty} \sum_{\deg(M)=n} q^{-ns} = \sum_{n=0}^{\infty} q^{n(1-s)} = (1 - q^{1-s})^{-1}.$$

On peut ainsi réécrire

$$L(s, \chi) = \sum_{m=0}^{\infty} t_m(\chi) q^{-sm},$$

où

$$t_m(\chi) = \sum_{\deg M=m} \chi(M),$$

On remarque $t_m(\chi) = 0$ pour $m > 2$ et $\chi \neq \chi_{0,0}$. Ainsi, nous obtenons

$$L(s, \chi) = 1 + t_1(\chi) q^{-s}, \qquad \chi \neq \chi_{0,0}. \tag{6.0.9}$$

En appliquant la série de Taylor du $\log(1+x)$, on a

$$\log((L(s,\chi))) = \sum_{P}\sum_{r=1}^{\infty}\frac{(-1)^{r-1}}{r}\chi(P^r)|P|^{-rs}.$$

En fixant (a_1, a_2) et en appliquant une méthode similaire à celle pour trouver (5.1.9), on obtient

$$\begin{aligned}\sum_{\lambda_1,\lambda_2}\chi_{\lambda_1,\lambda_2}(a_1,a_2)^{-1}\log(L(s,\chi_{\lambda_1,\lambda_2})) &= q^2\sum_{\substack{P\\ P^r\sim x^2+a_1x+a_2}}\sum_{r=1}^{\infty}\frac{1}{r}|P|^{-rs}\\ &= q^2\sum_{n=1}^{\infty}\sum_{d|n}\frac{d}{n}\nu(n,d,a_1,a_2)q^{-sn},\end{aligned}$$

où $\nu(n,d,a_1,a_2)$ indique le nombre de polynômes P de degré d tel que $P^{n/d}\sim x^2+a_1x+a_2$. Ainsi, $\nu(n,n,0,a_2)=H_n(a_2)$.

Avec (6.0.9) et en appliquant une méthode similaire à (5.1.14), on a aussi

$$\begin{aligned}&\sum_{\lambda_1,\lambda_2}\chi_{\lambda_1,\lambda_2}(a_1,a_2)^{-1}\log(L(s,\chi_{\lambda_1,\lambda_2}))\\ =\ &\sum_{n=1}^{\infty}\frac{q^{-sn}}{n}\left(q^n-\sum_{(\lambda_1,\lambda_2)\neq(0,0)}(-1)^n t_1(\chi_{\lambda_1,\lambda_2})^n\chi_{\lambda_1,\lambda_2}(a_1,a_2)^{-1}\right).\end{aligned}$$

En égalisant nos deux équations, on trouve :

$$q^2\sum_{d|n}d\nu(n,d,a_1,a_2)=q^n-(-1)^n\sum_{(\lambda_1,\lambda_2)\neq(0,0)}t_1(\chi_{\lambda_1,\lambda_2})^n\chi_{\lambda_1,\lambda_2}(a_1,a_2)^{-1}.$$

On peut calculer

$$\begin{aligned}t_1(\chi_{\lambda_1,\lambda_2}) &= \sum_{\deg M=1}\chi_{\lambda_1,\lambda_2}(M)\\ &= \sum_{a\in\mathbb{F}_q}\chi_{\lambda_1,\lambda_2}(a,0)\\ &= \sum_{a\in\mathbb{F}_q}\psi\left(\lambda_1 a-\frac{\lambda_2}{2}a^2\right).\end{aligned}$$

Si $\lambda_2=0$, nous obtenons 0 pourvu que $\lambda_1\neq 0$

Si $\lambda_2 \neq 0$, on peut voir que

$$\begin{aligned}\sum_{a\in\mathbb{F}_q} \psi\left(\lambda_1 a - \frac{\lambda_2}{2}a^2\right) &= \psi\left(\frac{\lambda_1^2}{2\lambda_2}\right)\sum_{a\in\mathbb{F}_q}\psi\left(-\frac{\lambda_2}{2}\left(a-\frac{\lambda_1}{\lambda_2}\right)^2\right)\\ &= \psi\left(\frac{\lambda_1^2}{2\lambda_2}\right)\sum_{a\in\mathbb{F}_q}\psi\left(-\frac{\lambda_2 a^2}{2}\right).\end{aligned}$$

Avec une petite manipulation sur la sommation, on voit que

$$\begin{aligned}\psi\left(\frac{\lambda_1^2}{2\lambda_2}\right)\sum_{a\in\mathbb{F}_q}\psi\left(-\frac{\lambda_2 a^2}{2}\right) &= 2\psi\left(\frac{\lambda_1^2}{2\lambda_2}\right)\sum_{\substack{x\in\mathbb{F}_q\\ x \text{ est un carré}}}\psi\left(-\frac{\lambda_2 x}{2}\right)\\ &= \psi\left(\frac{\lambda_1^2}{2\lambda_2}\right)\sum_{x\in\mathbb{F}_q}\left(1+\left(\frac{x}{q}\right)\right)\psi\left(-\frac{\lambda_2 x}{2}\right)\\ &= \psi\left(\frac{\lambda_1^2}{2\lambda_2}\right)\sum_{x\in\mathbb{F}_q}\left(\frac{x}{q}\right)\psi\left(-\frac{\lambda_2 x}{2}\right).\end{aligned}$$

En posant $G_\psi(b) = \sum_{a\in\mathbb{F}_q}\left(\frac{a}{q}\right)\psi(-ba)$ où $\left(\frac{a}{q}\right)$ est le caractère quadratique et à l'aide des relations suivantes :

$$G_\psi(-b) = \left(\frac{b}{q}\right)G_\psi(1),$$

$$G_\psi^2(1) = \left(\frac{-1}{q}\right)q,$$

on conclut que

$$\begin{aligned}\psi\left(\frac{\lambda_1^2}{2\lambda_2}\right)\sum_{a\in\mathbb{F}_q}\psi\left(\frac{\lambda_2 a^2}{2}\right) &= \psi\left(\frac{\lambda_1^2}{2\lambda_2}\right)G_\psi\left(\frac{\lambda_2}{2}\right)\\ &= \psi\left(\frac{\lambda_1^2}{2\lambda_2}\right)\left(\frac{\frac{\lambda_2}{2}}{q}\right)G_\psi(1).\end{aligned}$$

En mettant tous ces résultats ensemble, on a

$$\begin{aligned}q^2\sum_{d|n} d\nu(n,d,0,a) &= q^n - (-1)^n\sum_{\lambda_1}\sum_{\lambda_2\neq 0}\psi\left(\frac{\lambda_1^2}{2\lambda_2}\right)^n\left(\frac{2\lambda_2}{q}\right)^n G_\psi(1)^n\psi(-\lambda_2 a)\\ &= q^n - (-1)^n G_\psi(1)^n\sum_{\lambda_1}\sum_{\lambda_2\neq 0}\psi\left(\frac{n\lambda_1^2}{2\lambda_2}\right)\left(\frac{2\lambda_2}{q}\right)^n\psi(-\lambda_2 a).\end{aligned}$$

Si $p \nmid n$, nous avons

$$\begin{aligned} q^2 \sum_{d|n} d\nu(n,d,0,a) &= q^n - (-1)^n G_\psi(1)^n \sum_{\lambda_2 \neq 0} G_\psi\left(-\frac{n}{2\lambda_2}\right)\left(\frac{2\lambda_2}{q}\right)^n \psi(-\lambda_2 a) \\ &= q^n - (-1)^n G_\psi(1)^{n+1} \sum_{\lambda_2 \neq 0} \left(\frac{-\frac{n}{2\lambda_2}}{q}\right)\left(\frac{2\lambda_2}{q}\right)^n \psi(-\lambda_2 a). \end{aligned}$$

Si $n = 2m$ et $a \neq 0$, on obtient

$$\begin{aligned} q^2 \sum_{d|n} d\nu(n,d,0,a) &= q^n - G_\psi(1)^{n+1} \sum_{\lambda_2 \neq 0} \left(\frac{-m\lambda_2}{q}\right) \psi(-\lambda_2 a) \\ &= q^n - G_\psi(1)^{n+1} \left(\frac{-m}{q}\right) \sum_{\lambda_2 \neq 0} \left(\frac{\lambda_2}{q}\right) \psi(-\lambda_2 a) \\ &= q^n - G_\psi(1)^{n+1} \left(\frac{-m}{q}\right) G_\psi(a) \\ &= q^n - q^{m+1} \left(\frac{(-1)^m m a}{q}\right). \end{aligned}$$

Si $n = 2m+1$ et $a \neq 0$, on trouve

$$\begin{aligned} q^2 \sum_{d|n} d\nu(n,d,0,a) &= q^n + G_\psi(1)^{n+1} \left(\frac{-n}{q}\right) \sum_{\lambda_2 \neq 0} \psi(-\lambda_2 a) \\ &= q^n - G_\psi(1)^{n+1} \left(\frac{-n}{q}\right) \\ &= q^n - q^{m+1} \left(\frac{(-1)^m n}{q}\right). \end{aligned}$$

Maintenant, considérons $p \mid n$

$$q^2 \sum_{d|n} d\nu(n,d,0,a) = q^n - (-1)^n G_\psi(1)^n \, q \sum_{\lambda_2 \neq 0} \left(\frac{2\lambda_2}{q}\right)^n \psi(-\lambda_2 a).$$

Si $n = 2m$ et $a \neq 0$, on a

$$\begin{aligned} q^2 \sum_{d|n} d\nu(n,d,0,a) &= q^n - G_\psi(1)^n \, q \sum_{\lambda_2 \neq 0} \psi(-\lambda_2 a) \\ &= q^n + G_\psi(1)^n \, q \\ &= q^n + q^{m+1} \left(\frac{(-1)^m}{q}\right). \end{aligned}$$

Si $n = 2m + 1$ et $a \neq 0$, on trouve

$$\begin{aligned} q^2 \sum_{d|n} d\nu(n, d, 0, a) &= q^n + G_\psi(1)^n q \left(\frac{2}{q}\right) \sum_{\lambda_2 \neq 0} \left(\frac{\lambda_2}{q}\right) \psi(-\lambda_2 a) \\ &= q^n + G_\psi(1)^{n+1} q \left(\frac{2}{q}\right) \left(\frac{a}{q}\right) \\ &= q^n + q^{m+2} \left(\frac{2a(-1)^{m+1}}{q}\right). \end{aligned}$$

En combinant tous ces résultats, nous arrivons exactement sur le théorème (3.0.8).

CONCLUSION

Suite à ces démonstrations sur le théorème de Kuz'min, nous pourrions tenter de continuer à fixer des coefficients dans les polynômes. Par exemple, au lieu de fixer les deux premiers coefficients, nous pourrions prendre les trois premiers. Dans ce cas, les techniques que nous avons appliquées dans ce mémoire seraient beaucoup plus difficiles à utiliser.

Effectivement, dans la première preuve que nous avons développée, le lemme (4.10) avec $\ell = 2$ nous impose deux conditions. Cependant, le cas où $\ell = 3$ nous imposerait trois conditions. Cela limite les possibilités des équations $\mathcal{E}_w(a)$ que nous pouvons utiliser dans les termes A, B, et C, car maintenant il faut que $\deg(w) \leq n - 3$ au lieu de la condition initiale $\deg(w) \leq n - 2$. De cette façon, il est beaucoup plus complexe de poser des équations pour les termes A, B et C. À la fin, ces termes nous donneraient une combinaison de $X_v(a)$ telle que V n'a pas seulement la première rangée non-nulle, mais la deuxième aussi. En d'autres mots, on y trouverait des factorisations du type $(1^{e_1}, \ldots, 1^{e_k}, 2^{f_1}, \ldots, 2^{f_l})$ et nous aurions besoin d'une théorie plus forte que celle des formes quadratiques pour les traiter.

Pour le preuve de Kuz'min, la difficulté repose sur le choix des caractères. Effectivement, pour y arriver, il nous faudrait un troisième caractère pour inclure la nouvelle condition imposée. Ce changement modifie grandement toute l'approche de résolution. Globalement, pour généraliser ce problème, il nous faudrait une large adaptation de nos idées.

BIBLIOGRAPHIE

[1] Artin, E. " Quadratische Korper in Gebiete der hoheren Kongruenzen ", Math. Z., 19 (1924), 207-246.

[2] Carlitz Leonard, “A theorem of Dickson on irréductible polynomial”, Proc. Amer. math. Soc., t. 3, 1952, p. 693-700.

[3] Casselman Bill,“Quadratic forms over finite fields”, University of British Columbia, 5 février 2011, 1-16

[4] Cohen Stephen D., “The distribution of polynomials over finite fields”, Acta Arith., 17 (1970), 255-271.

[5] Cohen Stephen D., “Explicit theorems on generator polynomial”,Finite Fields and Their Applications, University of Glasgow, 15 decembre 2004, p. 337-357,

[6] Cohen Stephen D., “Uniform distribution of polynomial over finite fields”, J. London Math Soc., University of Glasgow, 18 août 1970, p. 93-102,

[7] Cohm, P.M, “Algebra seconde edition volume 3”, University of Glasgow,1991

[8] Hayes,D. R. "The distribution of irreducibles in GF(q,x)", Trans. Amer. Math. Soc, 117 (1965), 101-127.

[9] Hermann Minkowski, “Grundlagen für eine Theorie quadratischen Formen mit ganzahligen Koeffizienten”, in Gesammelte Abhandlungen, 3-145. Originally published in 1911, now available in the Chelsea series, published by the American Mathematical Society.

[10] Kuz’min E. N., “Irreducible polynomials over a finite field”, Vol. 30, No. 6, 21 février 1989,98-109

[11] Kuz’min, E. N., On irreducible polynomials over a finite field. (Russian) *Sibirsk. Mat. Zh.* **30** (1989), no. 6, 98–109 ; translation in *Siberian Math. J.*

[12] Yucas Joseph L.“Irreducible polynomials over finite fields with prescribed trace/prescribed constant term”,Finite Fields and Their Applications, Southerne Illinois University, 31 may 2005, 211-221