ANNALES

DE

L'INSTITUT FOURIER

Ramachandran BALASUBRAMANIAN,
Cécile DARTYGE & Élie MOSAKI

Sur la complexité de familles d'ensembles pseudo-aléatoires

Tome 64, n° 1 (2014), p. 267-296.

<http://aif.cedram.org/item?id=AIF_2014___64_1_267_0>

Ann. Inst. Fourier, Grenoble
64, 1 (2014) 267-296

SUR LA COMPLEXITÉ DE FAMILLES D'ENSEMBLES PSEUDO-ALÉATOIRES

par Ramachandran BALASUBRAMANIAN, Cécile DARTYGE & Élie MOSAKI

Résumé. — Dans cet article, on s'intéresse au problème suivant. Soient p un nombre premier, $S \subset \mathbb{F}_p$ et $\mathcal{P} \subset \{P \in \mathbb{F}_p[X] : \deg P \leqslant d\}$. Quel est le plus grand entier k tel que pour toutes paires de sous-ensembles disjoints $\mathcal{A}, \mathcal{B}$ de $\mathbb{F}_p$ vérifiant $|\mathcal{A} \cup \mathcal{B}| = k$, il existe $P \in \mathcal{P}$ tel que $P(x) \in S$ si $x \in \mathcal{A}$ et $P(x) \notin S$ si $x \in \mathcal{B}$? Ce problème correspond à l'étude de la complexité de certaines familles d'ensembles pseudo-aléatoires. Dans un premier temps, nous rappelons la définition de cette complexité et resituons le contexte des ensembles pseudo-aléatoires. Ensuite, nous exposons les différents résultats obtenus selon la nature des ensembles S et $\mathcal{P}$ étudiés. Certaines preuves passent par des majorations de sommes d'exponentielles ou de caractères sur des corps finis, d'autres combinent des arguments combinatoires avec des résultats de la théorie additive des nombres.

Abstract. — In this paper we are interested in the following problem. Let p be a prime number, $S \subset \mathbb{F}_p$ and $\mathcal{P} \subset \{P \in \mathbb{F}_p[X] : \deg P \leqslant d\}$. What is the largest integer k such that for all subsets $\mathcal{A}, \mathcal{B}$ of $\mathbb{F}_p$ satisfying $\mathcal{A} \cap \mathcal{B} = \emptyset$ and $|\mathcal{A} \cup \mathcal{B}| = k$, there exists $P \in \mathcal{P}$ such that $P(x) \in S$ if $x \in \mathcal{A}$ and $P(x) \notin S$ if $x \in \mathcal{B}$? This problem corresponds to the study of the complexity of some families of pseudo-random subsets. First we recall this complexity definition and the context of pseudo-random subsets. Then we state the different results we have obtained according to the shape of the sets S and $\mathcal{P}$ considered. Some proofs are based on upper bounds for exponential sums or characters sums in finite fields, other proofs use combinatorics and additive number theory.

1. Introduction

Dans des problèmes de simulation ou de cryptographie, on a parfois besoin de sous-ensembles de $\{1, \dots, N\}$ ou de $\mathbb{Z}_n$ qui ressemblent à des

Mots-clés : Sous-ensembles pseudo-aléatoires, complexité, sommes d'exponentielles, sommes de caractères.
Classification math. : 11K45, 11L07, 05B10.

ensembles d'entiers pris au hasard. Dartyge et Sárközy [7] et [6] ont proposé pour cela, des mesures de nature pseudo-aléatoire de sous-ensembles de $\{1,\dots,N\}$ et de $\mathbb{Z}_n$, où n et N sont des entiers donnés. Ces mesures reprennent celles de bonne corrélation et de bonne répartition dans les progressions arithmétiques définies par Hubert, Mauduit et Sárközy [18] et [15] pour les suites binaires pseudo-aléatoires.

Soit $\mathcal{R} \subset \{1,\dots,N\}$. On associe à $\mathcal{R}$ le N-uplet $(e_1,\dots,e_N)$:

$$e_n = \begin{cases} 1-\frac{|\mathcal{R}|}{N} & \text{si } n \in \mathcal{R} \\ -\frac{|\mathcal{R}|}{N} & \text{si } n \notin \mathcal{R} \end{cases} \qquad (n=1,\dots,N).$$

La mesure de bonne répartition dans les progressions arithmétiques est alors

$$W(\mathcal{R},N) = \max_{a,b,t} \Big| \sum_{j=0}^{t-1} e_{aj+b} \Big|,$$

où le maximum porte sur les entiers a,b,t tels que $1 \leqslant b \leqslant b+(t-1)a \leqslant N$. La seconde mesure est la mesure de corrélation d'ordre k :

$$C_k(\mathcal{R},N) = \max_{M,D} \Big| \sum_{n=1}^{M} e_{n+d_1} \cdots e_{n+d_k} \Big|,$$

où le maximum est sur les $D=(d_1,\dots,d_k)$ et M tels que $0 \leqslant d_1 < \cdots < d_k \leqslant N-M$. Dans le cas des sous-ensembles de $\mathbb{Z}_n$ les conditions sur a,b,D pour ces deux mesures sont légèrement différentes.

On dira alors que $\mathcal{R}$ possède de bonnes propriétés pseudo-aléatoires, si $W(\mathcal{R},N)=o(N)$ et $C_k(\mathcal{R},N)=o(N)$.

Sárközy, Szalay et les deux derniers auteurs ont donné dans les articles [5], [6] et [8] plusieurs exemples de familles d'ensembles pseudo-aléatoires. Dans certaines applications il est important de disposer de familles d'ensembles aléatoires dont la structure est riche, ou encore dont les éléments ne peuvent pas être déterminés à partir d'un faible nombre de données. Cela a conduit Ahlswede, Khachatrian, Mauduit et Sárközy [2] à définir la notion de complexité d'un ensemble de suites pseudo-aléatoires.

Dans les articles [5] et [6] cette définition a été adaptée dans le cadre de familles de sous-ensembles pseudo-aléatoires de $\{1,\dots,N\}$ de la manière suivante :

Définition 1.1. — *Soit $\mathcal{F}$ une famille de sous-ensembles de $\{1,2,\dots,N\}$. La complexité $K(\mathcal{F})$ de la famille $\mathcal{F}$ est le plus grand entier $k \in \mathbb{N}$ tel que pour tout $\mathcal{A} \subset \{1,2,\dots,N\}$ avec $|\mathcal{A}|=k$ et tout sous-ensemble $\mathcal{B}$ de $\mathcal{A}$ il existe un élément de $\mathcal{F}$ tel que $\mathcal{R} \cap \mathcal{A} = \mathcal{B}$. Autrement dit, pour tout*

$\mathcal{A} \subset \{1, 2, \ldots, N\}$ tel que $|\mathcal{A}| = k$ et toute partition

$$\mathcal{A} = \mathcal{B} \cup \mathcal{C}\ ,\ \mathcal{B} \cap \mathcal{C} = \varnothing$$

de $\mathcal{A}$ il existe $\mathcal{R} \in \mathcal{F}$ tel que

$$\mathcal{B} \subset \mathcal{R}, \text{ et } \mathcal{C} \subset \{1, \ldots, N\} \setminus \mathcal{R}.$$

L'objet de cet article est de continuer l'étude de la complexité de différentes familles étudiées dans [5] et [6].

Les ensembles construits dans [5] et [6] sont de la forme :

$$\mathcal{R}(f, S) = \{n \in \{1, \ldots, p\} : \exists h \in S \text{ tel que } f(n) \equiv h \mod p\},$$

où f est un polynôme et S est un ensemble non vide strictement contenu dans $\mathbb{F}_p$.

Les ensembles S considérés étaient des différents types suivants :

(i) $S_1 = \{r, r+1, \ldots, r+s-1\}$ avec $r \in \mathbb{F}_p$ et $s < p/2$ ([5]) ;

(ii) $S_2 = \{\bar{r}, \overline{r+1}, \ldots, \overline{r+s-1}\}$ avec la notation $x\overline{x} \equiv 1 \mod p$ ([5]), en omettant $\overline{0}$ par convention ;

(iii) S_3 est l'ensemble des puissances ℓ ièmes modulo p où ℓ est un diviseur de $p-1$ ([6]).

Les ensembles de type $\mathcal{R}(f, S_1)$ ont l'avantage d'être rapides à générer mais peuvent avoir des mauvaises mesures de corrélation (*cf.* [17] Théorème 4).

Pour les ensembles de type S_2 ou S_3, les mesures de corrélation sont plus difficiles à estimer. Dans [5] et [6] ces mesures ont été évaluées pour des polynômes de la forme $f_{\mathcal{A}}(X) = \prod_{a \in \mathcal{A}}(X - a)$ où $\mathcal{A} \subset \mathbb{F}_p$ ou plus généralement pour des polynômes f sans racine multiple mais avec en contrepartie des conditions plus contraignantes sur les rapports des corrélations.

Notons $\mathcal{P}_1(d, p)$ l'ensemble des polynômes de $\mathbb{F}_p[X]$ de degré $\leqslant d$, $\mathcal{P}_2(d, p)$ celui des polynômes sans racine multiple et de degré $\leqslant d$ et enfin $\mathcal{P}_3(d, p) = \{f_{\mathcal{A}} : \mathcal{A} \subset \mathbb{F}_p, |\mathcal{A}| = d\}$ avec la notation f_A définie ci-dessus. On a ainsi les inclusions $\mathcal{P}_3(d, p) \subset \mathcal{P}_2(d, p) \subset \mathcal{P}_1(d, p)$.

On définit également pour $i = 1, 2, 3$:

$$\mathcal{F}_i(S, d) = \{\mathcal{R}(f, S) : f \in \mathcal{P}_i(d, p)\},$$

et $K_i(S, d)$ la complexité correspondante.

En utilisant les polynômes d'interpolation de Lagrange, on voit facilement que $K_1(S, d) \geqslant d + 1$. Dans [5] nous montrons à l'aide du théorème de Cauchy-Davenport que $K_1(S, d) \geqslant d + 2$. Ce dernier résultat est valable pour tous les ensembles S tels que $\min(|S|, |S^c|)$ est assez grand ; $|S^c|$ étant le complémentaire de S dans $\mathbb{F}_p$: $S^c = \mathbb{F}_p \setminus S$. On pourrait penser que

dans le cas où S est une suite d'entiers consécutifs l'on puisse obtenir une meilleure minoration. Nous n'y sommes pas parvenus. Les sommes d'exponentielles associées à ces problèmes se calculent de manière élémentaire et sont dans certains cas de taille très importante. Ce phénomène apparaît également dans l'étude des mesures de corrélations des ensembles $\mathcal{R}(f, S_1)$ (*cf.* [17]).

Par contre, la situation est différente lorsque S est l'ensemble des inverses d'une suite d'entiers consécutifs.

THÉORÈME 1.2. — *Soient $d \geqslant 2$, $k \in \mathbb{N}^*$, $r \in \mathbb{F}_p$ et $\beta \in]0,1[$ donnés. On note $s = \lceil \beta p \rceil$. On considère le sous-ensemble $S \subset \mathbb{F}_p$ défini par*

$$S = \{\overline{r}, \overline{r+1}, \dots, \overline{r+s-1}\} \quad (\textit{on omet } \overline{0}).$$

L'inégalité $K_3(S,d) \geqslant k$ est alors vérifiée pour $p > 2/(1-\beta)$ tel que

$$\binom{p-k}{d} \min_{0 \leqslant \ell \leqslant k} \beta^\ell \Big(1 - \beta - \frac{1}{p}\Big)^{k-\ell} - (44^{4k} + 2k + 2d - 2) p^{d-1} (\log(9p))^k > 0. \tag{1.1}$$

Comme $\binom{p}{d} \sim \frac{p^d}{d!}$, on en déduit que $K_3(S,d) \geqslant k$ pour p assez grand, $p \geqslant p_0(\beta, d, k)$. Il découle de ce théorème la minoration :

$$K_3(S,d) \gg_{d,\beta} \frac{\log p}{\log\log p}. \tag{1.2}$$

Rappelons que la proposition 4.3 de [5] entraîne que $K_3(S,d) \leqslant \frac{(d+1)\log p}{\log 2}$.

Plus d est grand plus la condition (1.1) est mauvaise. Cela est contraire à notre intuition. Ce défaut est dû aux majorations de sommes d'exponentielles que nous utilisons.

Pour $y \in \mathbb{R}$ et p premier on note $\mathbf{e}_p(x) = \exp(2i\pi x/p)$. L'une des étapes de la preuve de ce théorème est de trouver des majorations de sommes de la forme :

$$S := \sum_{\{a_1,\dots,a_d\} \subset \mathbb{F}_p} \mathbf{e}_p\Big(\sum_{m=1}^{t} h_m \prod_{j=1}^{d} \overline{b_m - a_j} \Big),$$

où chaque a_j est différent des b_m. Eichenauer-Herrmann et Niederreiter [11] ont étudié ces sommes dans le cas $d = 1$. En utilisant les majorations de Bombieri et Weil ([4]) de sommes d'exponentielles d'argument une fraction rationnelle, ils obtiennent des majorations complètement explicites.

On déduit facilement du théorème d'Eichenauer-Herrmann et Niederreiter la majoration $S \ll_{\beta,k,d} p^{d-1/2}$, où la constante implicite est calculable. Cette majoration est suffisante pour obtenir une version légèrement affaiblie du Théorème 1.2. Le deuxième terme du membre de gauche de (1.1) étant alors de l'ordre de $p^{d-1/2}(\log p)^k$.

Une question naturelle est de vérifier s'il n'est pas possible d'obtenir une meilleure majoration de S en profitant du fait d'avoir une somme sur d variables avec $d \geqslant 2$. Lorsque $t = 1$, nous verrons au paragraphe 2 que la somme S s'évalue facilement et est de l'ordre de p^{d-1}. Nous pouvons donc profiter de compensations seulement sur deux variables.

Le théorème suivant est, on l'espère, d'un intérêt intrinsèque. Il est un résultat analogue au théorème d'Eichenauer-Herrmann et Niederreiter pour des sommes en deux variables.

THÉORÈME 1.3. — *Soient $b_1, \dots, b_k$, $c_1, \dots, c_k$ des éléments de $\mathbb{F}_p$ tels que $b_i \neq b_j$ et $c_i \neq c_j$ pour tous $i \neq j$. Pour $d_1, \dots, d_k \in \mathbb{F}_p^*$, on considère la somme d'exponentielles :*

$$S(\mathbf{b}, \mathbf{c}, \mathbf{d}) = \sum_{\substack{x,y \in \mathbb{F}_p \\ x \neq b_i, y \neq c_i}} \mathbf{e}_p\left(\sum_{i=1}^{k} d_i \overline{(x - b_i)(y - c_i)} \right).$$

On a alors

$$|S(\mathbf{b}, \mathbf{c}, \mathbf{d})| \leqslant 44^{4k} p. \tag{1.3}$$

Une application directe du théorème d'Eichenauer-Herrmann et Niederreiter fournit la majoration $S(\mathbf{b}, \mathbf{c}, \mathbf{d}) = O(p^{3/2})$. Nous verrons au paragraphe 2 que le Théorème 1.3 implique la majoration $S \ll p^{d-1}$. Il faut cependant signaler que la dépendance en k de notre théorème est de moins bonne qualité que celle issue de la majoration d'Eichenauer-Herrmann et Niederreiter. Autrement dit, lorsque k est grand comparativement à p (en fait pour $k \gg \log p$) il est plus pertinent d'utiliser le Théorème d'Eichenauer-Herrmann et Niederreiter.

La preuve de ce résultat fait l'objet du premier paragraphe de cet article. Elle utilise des résultats de géométrie algébrique notamment les célèbres travaux de Dwork et de Deligne. Nous avons essayé d'adopter une approche la plus élémentaire possible en nous inspirant des travaux de Hooley [14], Adolpshon et Sperber [1] ainsi que de la présentation de la méthode de Hooley faite par Birch et Bombieri [3] dans un appendice d'un article de Friedlander et Iwaniec [12].

Cette preuve nécessite l'étude d'extensions des sommes $S(\mathbf{b}, \mathbf{c}, \mathbf{d})$ à des sommes d'exponentielles définies sur $\mathbb{F}_{p^n}$ et fournit au passage des majorations de telles sommes.

La structure de S est essentielle dans la preuve du Théorème 1.2. Pour un ensemble S général c'est plus délicat. On ne peut même pas utiliser les polynômes d'interpolation de Lagrange car rien ne dit que le polynôme alors formé sera dans $\mathcal{P}_3(d, p)$ (c'est-à-dire à racines simples dans $\mathbb{F}_p$). Le résultat

suivant donne une minoration de $K_3(S,d)$ valable pour des ensembles S quelconques.

THÉORÈME 1.4.

(i) Si S et S^c sont non vides, alors $K_3(S,d) > \lceil d/2 \rceil$ pour p assez grand ($p > p_0(d)$).

(ii) Si $\min(|S|,|S^c|) \gg p$, alors $K_3(S,d) \geqslant d-1$ pour p assez grand.

Pour démontrer ce théorème, nous utilisons des majorations de sommes de caractères multiplicatifs afin de profiter de la structure produit des polynômes $f_{\mathcal{A}}$.

La fin de cet article est dévolue à la complexité $K_2(S,d)$. Dans [6] et [5] on trouve deux arguments différents montrant que cette complexité est $K_2(S,d) \geqslant d+1$ si S et son complémentaire ont suffisamment d'éléments. Dans cet article nous améliorons ce résultat :

THÉORÈME 1.5. — *Si $4d-2 < |S| < \frac{p-d+1}{2}$ alors $K_2(S,d) \geqslant d+2$.*

La preuve de ce résultat est de nature différente de celle des précédents théorèmes. Elle est combinatoire et utilise un résultat récent de Green et Ruzsa [13] de théorie additive des nombres. Pour $x \in \mathbb{F}_p$, on note $\bar{x}$ l'inverse de x dans $\mathbb{F}_p$. Pour $n \in \mathbb{N}$, (resp. $n \in \mathbb{F}_p$), on note $r_p(n)$ le plus petit entier positif congru à n modulo p (resp. appartenant à la classe de n dans $\mathbb{F}_p$). En fait dans cet article nous ferons souvent l'amalgame entre un entier n et sa classe dans $\mathbb{F}_p$.

2. Majorations de sommes d'exponentielles

Soient $\mathbf{h} \in (\mathbb{F}_p^*)^k$, $\mathbf{b} = (b_{m,j})_{\substack{1 \leqslant m \leqslant k \\ 1 \leqslant j \leqslant d}} \in \mathcal{B}^{kd}$ où $\mathcal{B} \subset \mathbb{F}_p$.

Dans ce paragraphe, nous étudions des sommes d'exponentielles de la forme :

$$S(\mathbf{h},\mathbf{b}) = \sum_{\{a_1,\dots,a_d\} \subset \mathbb{F}_p \setminus \mathcal{B}} \mathbf{e}_p\left(\sum_{m=1}^{k} h_m \prod_{j=1}^{d} \overline{b_{m,j} - a_j} \right), \tag{2.1}$$

où pour chaque j, $b_{m,j} \neq b_{\ell,j}$ si $\ell \neq m$.

2.1. Sommes sur une variable

Pour $q = p^n$, $x \in \mathbb{F}_q$, on note encore $\overline{x}$ l'inverse de x dans $\mathbb{F}_q$. Commençons par rappeler le résultat d'Eichenauer-Herrmann et Niederreiter :

THÉORÈME 2.1 (Eichenauer-Herrmann et Niederreiter [11] Théorème 1 p. 270)). — *Soient* $\mathbf{d} \in \mathbb{F}_q^s$, $\mathbf{d} \neq 0$ *et* $\mathbf{e} = (e_1, \dots, e_s) \in \mathbb{F}_q^s$ *tels que* $e_1, \dots, e_s$ *soient distincts deux à deux. Si* ψ *est un caractère additif de* $\mathbb{F}_q$ *non trivial alors*

$$\sum_{n \in \mathbb{F}_q \setminus \{-e_1, \dots, -e_s\}} \psi\Big(\sum_{j=1}^{s} d_j \overline{n + e_j} \Big) \leqslant (2s-2)\sqrt{q} + 1.$$

Cette version est légèrement différente du théorème 1 de [11], car dans cet article la somme porte sur tous les $n \in \mathbb{F}_q$ avec la convention $\overline{x} = 0$ pour $x = 0$ ce qui crée un s en plus dans la majoration.

Dans le cas où $k = 1$, et $b_{1,j} = b$ pour $1 \leqslant j \leqslant d$, la somme $S(\mathbf{h}, \mathbf{b})$ définie par (2.1) est simplement du type :

$$S(h, b) = \sum_{\{a_1, \dots, a_d\} \subset \mathbb{F}_p \setminus \{b\}} \mathbf{e}_p\Big(h \prod_{j=1}^{d} \overline{b - a_j} \Big).$$

LEMME 2.2. — *Soit* $d \geqslant 2$. *On a l'égalité*

$$S(h, b) = -\frac{p^{d-1}}{(d-1)!} + O_d(p^{d-3/2}).$$

La preuve de ce lemme repose sur le fait que pour $(a, p) = 1$,

$$\sum_{x \in \mathbb{F}_p^*} \mathbf{e}_p(a\overline{x}) = \sum_{x \in \mathbb{F}_p} \mathbf{e}_p(ax) - 1 = -1. \tag{2.2}$$

On commence par sommer sur $a_d \in \mathbb{F}_p \setminus \{b, a_1, \dots, a_{d-1}\}$, $a_1, \dots, a_{d-1}$ étant fixés. En complétant la somme sur a_d pour utiliser (2.2) on obtient :

$$S(h, b) = -\binom{p-1}{d-1} - \sum_{i=1}^{d-1} \sum_{\{a_1, \dots, a_{d-1}\} \subset \mathbb{F}_p \setminus \{b\}} \mathbf{e}_p\left(h\overline{(b-a_i)^2} \prod_{\substack{j=1 \\ j \neq i}}^{d-1} \overline{b - a_j} \right).$$

Le premier terme est de l'ordre de $p^{d-1}/(d-1)!$ tandis que les autres termes de la somme en i, qui sont tous égaux, sont des $O(p^{d-3/2})$, d'après le Théorème 2.1 pour $d \geqslant 3$ ou d'après les majorations classiques de sommes de Gauss pour $d = 2$. Cela termine la preuve du Lemme 2.2.

Remarque. — Lorsque $d \geqslant 3$, on peut améliorer le terme d'erreur du Lemme 2.2 en appliquant (2.2) un nombre approprié de fois.

2.2. Premières étapes de la preuve du Théorème 1.3

Si $k = p$ le résultat est évident.

Soit $k < p$. Quitte à faire des changements de variables on peut supposer

$$\prod_{i=1}^{k} b_i c_i \neq 0. \tag{2.3}$$

En effet, supposons que cette condition ne soit pas réalisée. Soient $\beta \in \mathbb{F}_p \setminus \{b_1, \dots, b_k\}$ et $\gamma \in \mathbb{F}_p \setminus \{c_1, \dots, c_k\}$. En posant $x' = x - \beta$, $y' = y - \gamma$, la somme devient :

$$S(\mathbf{b}, \mathbf{c}, \mathbf{d}) = \sum_{\substack{x' \in \mathbb{F}_p \setminus \{b_1 - \beta, \dots, b_k - \beta\} \\ y' \in \mathbb{F}_p \setminus \{c_1 - \gamma, \dots, c_k - \gamma\}}} \mathbf{e}_p\left(\sum_{i=1}^{k} d_i \overline{(x' + \beta - b_i)(y' + \gamma - c_i)} \right),$$

où maintenant $b_i - \beta \neq 0$, $c_i - \gamma \neq 0$ pour $1 \leqslant i \leqslant k$; on s'est ramené à une somme vérifiant (2.3).

Posons $u_i = \overline{x - b_i}$, $v_i = \overline{y - c_i}$ pour $1 \leqslant i \leqslant k$. On a alors pour $1 \leqslant i \leqslant k$:

$$u_i u_1 (b_1 - b_i) + u_i - u_1 = 0 \quad \text{et} \quad v_i v_1 (c_1 - c_i) + v_i - v_1 = 0. \tag{2.4}$$

Soit $V \subset (\mathbb{F}_p)^{2k}$ la variété définie par les équations (2.4). Étant donné que tous les u_i s'expriment en fonction de u_1 et tous les v_i en fonction de v_1, V est une variété de dimension 2.

La somme d'exponentielles $S(\mathbf{b}, \mathbf{c}, \mathbf{d})$ se réécrit alors de la manière suivante :

$$S(\mathbf{b}, \mathbf{c}, \mathbf{d}) = \sum_{\substack{u, v \in (\mathbb{F}_p^*)^k \\ (u,v) \in V}} \mathbf{e}_p\Big(\sum_{i=1}^{k} d_i u_i v_i \Big). \tag{2.5}$$

La somme $S(\mathbf{b}, \mathbf{c}, \mathbf{d})$ apparaît maintenant comme une somme d'exponentielles de la forme :

$$\sum_{\substack{0 \leqslant x_1, \dots, x_n < p \\ g_1(x_1, \dots, x_n) = \dots = g_s(x_1, \dots, x_n) = 0 \mod p}} \mathbf{e}_p(f(x_1, \dots, x_n)),$$

avec $f, g_1, \dots, g_s \in \mathbb{F}_p[X_1, \dots, X_n]$. L'étude de ce type de sommes est une branche de la géométrie arithmétique qui connaît un développement très important depuis le siècle dernier. Lorsque la somme ne porte que sur une variable, on dispose de majorations valables dans un cadre très général grâce aux travaux de Weil, puis de Deligne et Bombieri. Lorsque la somme porte sur plusieurs variables la situation est moins connue. Dans le cas où la somme est de la forme $\sum_{x_1, \dots, x_n \in \mathbb{F}_p} \mathbf{e}_p(f(x_1, \dots, x_n))$, où f est de degré d et a une composante homogène de degré d non singulière, Deligne [9] a montré que cette somme est de module inférieur à $(d-1)p^{n/2}$.

D'autres résultats très profonds ont été obtenus ces dernières décennies. Rojas-León [19] a par exemple récemment établi des majorations de telles sommes avec des hypothèses sur f moins fortes. On trouvera dans cet article d'autres références sur cette question. Malheureusement nous n'avons pas pu appliquer le résultat de Rojas-León évoqué ci-dessus.

Hooley [14] a repris les travaux de Dwork et de Deligne et a proposé une méthode pour obtenir des majorations dans un cadre assez général. Nous nous sommes inspirés de son approche ainsi que de la présentation qui en est faite dans l'appendice de Birch et Bombieri [3] d'un article de Friedlander et Iwaniec [12].

Pour $n \in \mathbb{N}$, on note $\mathbb{F}_{p^n}$ une extension de $\mathbb{F}_p$ de dimension n. Pour tout $x \in \mathbb{F}_{p^n}$ on note $\sigma_n(x)$ la trace de x sur $\mathbb{F}_p$:

$$\sigma_n(x) = x + x^p + \cdots + x^{p^{n-1}}.$$

Rappelons que $\sigma_n(u) \in \mathbb{F}_p$ si $u \in \mathbb{F}_{p^n}$.

Soit V_n l'ensemble des $(x, y) \in \mathbb{F}_{p^n}^{2k}$ vérifiant (2.4). On forme ensuite les sommes d'exponentielles sur $\mathbb{F}_{p^n}$ et $\mathbb{F}_{p^n}^*$:

$$S_n(V, \mathbf{d}) = \sum_{(x,y)\in V_n} \mathbf{e}_p\Big(\sigma_n\Big(\sum_{i=1}^{k} d_i x_i y_i\Big)\Big),$$

et

$$S_n^*(V, \mathbf{d}) = \sum_{\substack{(x,y)\in V_n \\ x,y\in(\mathbb{F}_{p^n}^*)^k}} \mathbf{e}_p\Big(\sigma_n\Big(\sum_{i=1}^{k} d_i x_i y_i\Big)\Big).$$

Si $(x, y) \in V_n$ est tel que $x_i = 0$ pour un $i \in \{1, \ldots, k\}$ donné alors d'après les équations de V, tous les x_j sont nuls. De même si l'un des y_j est nul tous les autres le sont. On en déduit l'égalité

$$S_n(V, \mathbf{d}) = S_n^*(V, \mathbf{d}) + 2(p^n - 1) + 1. \tag{2.6}$$

On considère alors les séries de Dirichlet définies formellement par

$$L(T) = \exp\Big(\sum_{r=1}^{\infty} \frac{S_r(V, \mathbf{d})T^r}{r}\Big) \text{ et } L^*(T) = \exp\Big(\sum_{r=1}^{\infty} \frac{S_r^*(V, \mathbf{d})T^r}{r}\Big).$$

Dwork [10] et Bombieri [4] ont montré que les séries $L(T)$ et $L^*(T)$ sont des fractions rationnelles dont les numérateurs et les dénominateurs appartiennent à $\mathbb{Q}(\mathbf{e}_p(1))[T]$. Cette preuve est reprise dans l'article de Hooley [14]. Il en déduit ensuite pour chaque entier r l'égalité :

$$S_r(V, \mathbf{d}) = \omega_1^r + \cdots + \omega_i^r - \omega_{i+1}^r - \cdots - \omega_\kappa^r, \tag{2.7}$$

où $\omega_1, \dots, \omega_i$ sont les zéros du numérateur, $\omega_{i+1}, \dots, \omega_\kappa$ ceux du dénominateur de L. Deligne a montré que pour chaque j, $|\omega_j| = p^{m_j/2}$ où $m_j \in \mathbb{N}$.

Ainsi, pour démontrer le Théorème 1.3, puisque

$$S(\mathbf{b}, \mathbf{c}, \mathbf{d}) = S_1^*(V, \mathbf{d}),$$

il suffit de prouver que $\kappa \leqslant 44^{4k-1}$ et $m_j \leqslant 2$ pour tout $1 \leqslant j \leqslant \kappa$, ce que nous allons faire maintenant.

2.3. Majoration du nombre κ de la formule (2.7)

Notre point de départ est le résultat suivant

THÉORÈME 2.3 (Hooley[14] Theorem 4 p. 112). — *Soit $f \in \mathbb{F}_p[X_1,...,X_N]$ de degré d. Pour $n \in \mathbb{N}$, on définit*

$$S_n(f) = \sum_{x \in \mathbb{F}_{p^n}^N} \mathbf{e}_p(\sigma_n(f(x))) \text{ et } S_n^*(f) = \sum_{x \in (\mathbb{F}_{p^n}^*)^N} \mathbf{e}_p(\sigma_n(f(x))).$$

Les sommes d'exponentielles $S_n(f)$ et $S_n^*(f)$ admettent une écriture sous la forme (2.7) *et le nombre des pôles correspondant κ vérifie*

$$\kappa \leqslant (11d + 11)^{N+1}.$$

En utilisant l'orthogonalité des caractères (comme l'a fait Hooley ([14] p. 104) pour détecter les conditions définissant V_n, on remarque que

$$S_n(V, \mathbf{d}) = \frac{1}{p^{2(k-1)n}} S_n(\phi), \tag{2.8}$$

avec pour $u=(u_1, \dots, u_k)$, $v=(v_1, \dots, v_k)$, $g=(g_2, \dots, g_k)$, $h=(h_2,..., h_k)$:

$$\phi(u, v, g, h) = d_1 u_1 v_1 + \sum_{i=2}^{k} (d_i u_i v_i + g_i(u_i u_1(b_1 - b_i) + u_i - u_1)) + \sum_{i=2}^{k} h_i(v_i v_1(c_1 - c_i) + v_i - v_1).$$

D'après le Théorème 2.3 (avec $N = 4k - 2$ et $d = 3$), le κ correspondant à $S_n(V, \mathbf{d})$ est inférieur à 44^{4k-1}.

2.4. Majorations des puissances m_j de (2.7)

Nous allons montrer que $m_j \leqslant 2$ pour tout $1 \leqslant j \leqslant \kappa$.

On procède comme Hooley [14] ou comme [3] avec un argument de valeur moyenne.

Pour $\lambda \in \mathbb{F}_{p^n}$, on considère la variété

$$W_\lambda = \Big\{(x,y) \in V_n,\ \sum_{i=1}^{k} d_i x_i y_i = \lambda\Big\}.$$

Il sera parfois utile de noter $W_\lambda(\mathbb{F}_{p^n})$ cette variété. On a vu que la définition de V_n implique que si l'un des x_i est nul alors $x_1 = \ldots = x_k = 0$. Ainsi, pour $\lambda \neq 0$,

$$W_\lambda = \Big\{(x,y) \in V_n,\ \sum_{i=1}^{k} d_i x_i y_i = \lambda, \prod_{i=1}^{k} x_i y_i \neq 0\Big\}.$$

Remarquons (*via* la correspondance $x_i = \overline{x - b_i}$ et $y_i = \overline{y - c_i}$) l'égalité pour $\lambda \neq 0$:

$$W_\lambda = \Big\{(x,y) \in \mathbb{F}_{p^n}^2 : \sum_{i=1}^{k} d_i \overline{(x-b_i)(y-c_i)} = \lambda, \prod_{i=1}^{k} (x-b_i)(y-c_i) \neq 0\Big\}.$$

(Pour $\lambda = 0$ il faut rajouter le point $(0,0)$.)

Soit $N_n(\lambda)$ le nombre de points de W_λ.

On reprend maintenant pas à pas les arguments de Hooley [14] ou de Birch et Bombieri [3] qui consistent à évaluer de deux manières différentes la quantité

$$S := \sum_{c \in \mathbb{F}_p \setminus \{0\}} |S_c|^2,$$

avec

$$S_c = \sum_{(x,y) \in V_n} \mathbf{e}_p\left(\sigma_n\Big(c \sum_{i=1}^{k} d_i x_i y_i\Big)\right).$$

Tout d'abord, en regroupant les x, y tels que $\sum_{i=1} d_i x_i y_i = \lambda$, on remarque que les sommes S_c valent :

$$S_c = \sum_{\lambda \in \mathbb{F}_{p^n}} N_n(\lambda) \mathbf{e}_p(\sigma_n(c\lambda)).$$

On obtient, en développant les carrés de la somme S,

$$\begin{aligned} S &= \sum_{c\in\mathbb{F}_p\setminus\{0\}} \sum_{\lambda,\lambda'\in\mathbb{F}_{p^n}} N_n(\lambda)N_n(\lambda')\mathbf{e}_p(\sigma_n(c\lambda)-\sigma_n(c\lambda')) \\ &= p^n \sum_{\lambda\in\mathbb{F}_{p^n}} N_n(\lambda)^2 - \Big(\sum_{\lambda\in\mathbb{F}_{p^n}} N_n(\lambda)\Big)^2, \end{aligned}$$

soit

$$S = p^n \sum_{\lambda\in\mathbb{F}_{p^n}} (N_n(\lambda)-M)^2,$$

où M est la valeur moyenne :

$$M = \frac{1}{p^n}\sum_{\lambda\in\mathbb{F}_{p^n}} N_n(\lambda) = p^n.$$

Posons

$$g_\lambda(X,Y) = \sum_{i=1}^{k} d_i \prod_{j\neq i}(X-b_j)(Y-c_j) - \lambda\prod_{i=1}^{k}(X-b_i)(Y-c_i),$$

de sorte que pour $\lambda\neq 0$,

$$W_\lambda(\mathbb{F}_{p^n}) = \Big\{(x,y)\in\mathbb{F}_{p^n}^2 : g_\lambda(x,y)=0, \prod_{i=1}^{k}(x-b_i)(y-c_i)\neq 0\Big\}.$$

Pour chaque $x\in\mathbb{F}_p^n$, $y\mapsto g_\lambda(x,y)$, est la fonction polynomiale d'un polynôme de $\mathbb{F}_{p^n}[Y]$ de degré $k-1$ ou k suivant que x soit l'un des b_i ou non. Il a donc dans $\mathbb{F}_{p^n}$ au plus k racines. On en déduit la première majoration triviale :

$$N_n(\lambda) = |W_\lambda(\mathbb{F}_{p^n})| \leqslant kp^n. \tag{2.9}$$

Nous obtenons maintenant une expression plus précise pour presque tout λ :

Proposition 2.4. — *Il existe deux constantes ν, K telles pour presque tout $\lambda\in\mathbb{F}_{p^n}$ avec au plus K exceptions, on a :*

$$|N_n(\lambda)-p^n| \leqslant \nu\sqrt{p^n}. \tag{2.10}$$

De plus, les valeurs $\nu = 2k^2$ et $K = 9(k-1)^2+4(k-1)+2$ sont admissibles.

La preuve de cette proposition n'est pas immédiate. Avant de l'exposer nous proposons de montrer que cette proposition est suffisante pour démontrer le Théorème 1.3. Admettons donc provisoirement la Proposition 2.4. Nous reprenons les idées de Hooley [14] pp. 115-116. Comme nous voulons contrôler la dépendance en k, nous les reproduisons ici dans notre contexte. Il s'agit notamment de ne pas rater un "assez grand" qui dépendrait de k.

Soit $\mathcal{K}$ l'ensemble des $\lambda \in \mathbb{F}_{p^n}$ ne vérifiant pas la Proposition 2.4. On a alors

$$S = p^n \sum_{\lambda \in \mathcal{K}} (N_n(\lambda) - p^n)^2 + p^n \sum_{\lambda \notin \mathcal{K}} (N_n(\lambda) - p^n)^2 \leqslant (Kk^2 + \nu^2) p^{3n}. \tag{2.11}$$

Supposons que l'un des ω_i de la formule (2.7) soit de module $p^{m/2}$ pour un $m \geqslant 3$. Hooley a montré à partir des travaux de Deligne que les sommes S_c pour $c \in \mathbb{F}_p^*$ sont également de la forme

$$S_c = e_1 \omega_{1,c}^n + \cdots + e_L \omega_{L,c}^n,$$

où $e_1, \ldots, e_L$ sont des entiers indépendants de c et n vérifiant $|e_1| + \cdots + |e_L| = \kappa$, et les modules $|\omega_{j,c}|$ sont des puissances entières de $\sqrt{p}$; ces puissances étant indépendantes de c.

En particulier le nombre des $\omega_{i,c}$ de module supérieur à $p^{3/2}$ est le même pour chaque c. Plus précisément, si ℓ désigne le nombre d'indices i tels que $\omega_{i,c}$ soit de module supérieur à $p^{3/2}$, on a pour tout $c \in \mathbb{F}_p^*$ (quitte à changer l'ordre des $\omega_{i,c}$) :

$$S_c = e_1 \omega_{1,c}^n + \cdots + e_\ell \omega_{\ell,c}^n + E_c,$$

où E_c est un terme d'erreur de module inférieur à κp^n. Soit H tel que $p^H = \max_{1 \leqslant i \leqslant L} |\omega_{i,c}|^2$. Posons $z_{i,c} = \frac{\omega_{i,c}}{p^{H/2}}$ pour $1 \leqslant i \leqslant \ell$. Les $z_{i,c}$ sont ainsi des nombres complexes deux à deux distincts de modules inférieurs où égaux à 1. On en déduit la minoration pour tout $c \in \mathbb{F}_p^*$:

$$|S_c| \geqslant p^{3n/2} |e_1 z_{1,c}^n + \cdots + e_\ell z_{\ell,c}^n| - \kappa p^n.$$

Cela donne pour S :

$$S \geqslant \sum_{c \in \mathbb{F}_p^*} |S_c|^2 \geqslant \sum_{c \in \mathbb{F}_p^*} p^{3n} |e_1 z_{1,c}^n + \cdots + e_\ell z_{\ell,c}^n|^2 - 2\kappa^2 (p-1) p^{5n/2}.$$

L'idée suivante de Hooley est d'utiliser l'égalité :

$$\lim_{u \to +\infty} \frac{1}{u} \sum_{n \leqslant u} |e_1 z_{1,c}^n + \cdots + e_\ell z_{\ell,c}^n|^2 = |e_1^2 + \cdots + e_\ell^2| \geqslant 1,$$

qui se vérifie en développant le carré et en profitant du fait que les $z_{i,c}$ sont des nombres complexes deux à deux distincts de module inférieur à 1. Grâce à cette égalité, on observe que pour $\varepsilon > 0$ donné, il existe une infinité d'entiers n tels que

$$|e_1 z_{1,c}^n + \cdots + e_\ell z_{\ell,c}^n|^2 \geqslant 1 - \varepsilon. \tag{2.12}$$

On obtient alors pour les entiers n vérifiant (2.12) :

$$S \geqslant (p-1)p^{3n}\Big(1-\varepsilon-\frac{2\kappa^2}{p^{n/2}}\Big) \geqslant (p-1)p^{3n}(1-2\varepsilon),$$

pour n assez grand. Cette minoration est incompatible avec (2.11) lorsque $p > Kk^2+\nu^2+1$ (avec un choix de ε assez petit).

Lorsque $p \leqslant Kk^2+\nu^2+1$, le Théorème 1.3 reste vrai mais fournit en fait une majoration moins bonne que la majoration triviale ($|S(\mathbf{b},\mathbf{c},\mathbf{d})| \leqslant p^2$).

Il reste maintenant à démontrer la Proposition 2.4 pour terminer la preuve du Théorème 1.3.

Le cardinal $N_n(\lambda)$ est proche du cardinal

$$N'_n(\lambda) := |\{(x,y) \in \mathbb{F}_{p^n}^2 : g_\lambda(x,y) = 0\}|.$$

Pour obtenir une majoration de la différence $|N'_n(\lambda)-N_n(\lambda)|$, il suffit d'étudier la contribution des $x = b_i$ ou $y = c_i$ dans g_λ. Le polynôme associé à

$$g_\lambda(b_i,y) = d_i \prod_{\substack{1\leqslant j\leqslant k\\ j\neq i}} (b_i-b_j)(y-c_j)$$

a $k-1$ racines. De même, pour $1 \leqslant i \leqslant k$, $|\{x \in \mathbb{F}_{p^n} : g_\lambda(x,c_i) = 0\}| = k-1$. Ainsi,

$$|N'_n(\lambda) - N_n(\lambda)| \leqslant 2k. \tag{2.13}$$

Pour démontrer la Proposition 2.4, il suffit donc d'étudier $N'_n(\lambda) - p^n$.

Si g_λ est absolument irréductible (c'est-à -dire irréductible dans $\overline{\mathbb{F}_p}$), alors d'après un théorème de Lang et Weil [16], $N'_n(\lambda) = p^n + O(\sqrt{p^n})$. Nous ne savons pas dire que g_λ est absolument irréductible pour tout λ sauf pour au plus un nombre fini de λ. Nous utilisons plutôt les travaux d'Adolphson et Sperber [1]. Pour cela nous devons définir le polygone de Newton d'un polynôme $g \in K[X_1,\dots,X_n]$ où K est un corps fini. Écrivons g sous la forme $g = \sum_{j\in J} a_j x^j$ où $J \subset \mathbb{Z}_+^n$, et pour chaque $j = (j_1,\dots,j_n) \in J$, $a_j \neq 0$ et $x^j = x_1^{j_1}\cdots x_n^{j_n}$.

Le polygone de Newton de g est alors l'enveloppe convexe dans $\mathbb{R}^n$ de l'ensemble $J \cup \{(0,\dots,0)\}$. On le note $\Delta(g)$. La dimension de $\Delta(g)$ est celle du plus petit sous-espace vectoriel de $\mathbb{R}^n$ contenant $\Delta(g)$.

À chaque face σ de $\Delta(g)$, on associe le polynôme

$$g_\sigma = \sum_{j\in\sigma\cap J} a_j x^j.$$

DÉFINITION 2.5.

(i) Le polynôme g est non dégénéré (par rapport à $\Delta(g)$) si pour toute face σ de $\Delta(g)$ qui ne contient pas l'origine, les polynômes $\partial g_\sigma/\partial x_1, \ldots,$ $\partial g_\sigma/\partial x_n$ n'ont pas de racine commune dans $(\overline{K^*})^n$ où $\overline{K}$ désigne une clôture algébrique de K.

(ii) Le polynôme g est commode (par rapport à $\Delta(g)$) si pour tout $i \in \{1, \ldots, n\}$, il existe un entier $j_i > 0$ tel que g contienne un monôme de la forme $ax_i^{j_i}$.

Ces deux définitions sont celles de [1] page 376 adaptées à notre situation. Adolphson et Sperber ont obtenu le résultat suivant.

THÉORÈME 2.6 (Adolphson et Sperber [1] Corollary 6.9 p. 400). — *Soient K un corps fini de cardinal q et $g \in K[x_1, \ldots, x_\ell]$ non dégénéré et commode par rapport à son polygone de Newton. On suppose aussi que*

$$g, x_1\partial g/\partial x_1, \ldots, x_\ell \partial g/\partial x_\ell$$

n'ont pas de zéro commun. Soit V la variété définie par $g = 0$. Il existe $\nu(g)$ telle que

$$|V(K)| - q^{\ell-1}| \leqslant \nu(g)\sqrt{q^{\ell-1}}.$$

Remarque : la constante $\nu(g)$ est effectivement calculable. On trouvera une définition de cette constante à la page 371 de [1], elle ne dépend que du polygone de Newton de g.

Pour terminer la preuve de la Proposition 2.4, il reste à vérifier que l'on peut appliquer le Théorème 2.6 au polynôme g_λ avec $K = \mathbb{F}_{p^n}$ et $\ell = 2$ pour presque tous λ avec au plus K exceptions et déterminer les $\nu(g_\lambda)$ correspondants. Rappelons la forme de g_λ :

$$g_\lambda(X, Y) = \sum_{i=1}^{k} d_i \prod_{j\neq i} (X - b_j)(Y - c_j) - \lambda \prod_{i=1}^{k} (X - b_i)(Y - c_i).$$

Lorsque $\lambda \neq 0$, le coefficient en X^k vaut $-\lambda(-1)^k c_1 \ldots c_k \neq 0$ puisque aucun c_i n'est nul.

On vérifie de la même manière pour $\lambda \neq 0$ que le coefficient en Y^k est non nul.

Cela prouve que g_λ est commode si $\lambda \neq 0$.

Le polygone de Newton est $\Delta(g_\lambda) = [0, k] \times [0, k]$ si $\lambda \neq 0$.

En reprenant la définition de ν donnée page 371 de [1] (avec $\nu = \nu_A$ où $A = \{1, 2\}$) on obtient sans peine que

$$\nu(g_\lambda) = 2k^2 - 2k. \tag{2.14}$$

Les faces de $\Delta(g_\lambda)$ ne contenant pas $(0,0)$ sont les cotés $\sigma_1 = \{k\} \times [0,k]$ et $\sigma_2 = [0,k] \times \{k\}$.

Les polynômes associés sont $g_{\sigma_1}(X,Y) = -\lambda X^k \prod_{i=1}^k (Y - c_i)$ et $g_{\sigma_2}(X,Y) = -\lambda Y^k \prod_{i=1}^k (X - b_i)$.

Vu que les c_i sont deux à deux distincts, on vérifie facilement que $\partial g_{\sigma_1}/\partial x$ et $\partial g_{\sigma_1}/\partial y$ n'ont pas de racine commune dans $(\overline{\mathbb{F}^*_{p^n}})^2$. Cette propriété est également vérifiée par g_{σ_2} car les b_i sont deux à deux distincts. Donc g_λ est non dégénéré lorsque $\lambda \neq 0$.

La dernière condition du Théorème 2.6 est plus difficile à vérifier.

Commençons par traiter le cas où $x = b_i$ pour un $i \in \{1, \dots, k\}$. Alors

$$g_\lambda(b_i, Y) = d_i \prod_{j \neq i} (b_i - b_j)(Y - c_j)$$

s'annule pour $Y = c_j$ avec $j \neq i$. Mais

$$\frac{\partial g_\lambda}{\partial x}(b_i, c_j) = d_j (c_j - c_i) \prod_{\ell \neq i,j} (b_i - b_\ell)(c_j - c_\ell) \neq 0.$$

Donc pour tout λ, il n'existe pas de point singulier de la forme (b_i, y). De même, il n'existe pas de point singulier de la forme (x, c_i).

Pour $x \notin \{b_1, \dots, b_k\}$, $y \notin \{c_1, \dots c_k\}$, on vérifie que $g_\lambda(x,y) = 0$ si et seulement si

$$\lambda = \sum_{i=1}^k d_i \overline{x - b_i} \overline{y - c_i}. \tag{2.15}$$

Pour la dérivée partielle en y, cela entraîne :

(2.16)

$$\begin{aligned} \frac{\partial g_\lambda}{\partial y}(x,y) &= \sum_{i=1}^k d_i \prod_{j \neq i} (x - b_j) \sum_{j \neq i} \prod_{\ell \neq i,j} (y - c_\ell) - \lambda \prod_{i=1}^k (x - b_i) \sum_{i=1}^k \prod_{j \neq i} (y - c_j) \\ &= -\prod_{i=1}^k (x - b_i)(y - c_i) \sum_{i=1}^k d_i \overline{(x - b_i)(y - c_i)^2}. \end{aligned}$$

De même,

$$\frac{\partial g_\lambda}{\partial x}(x,y) = -\prod_{i=1}^k (x - b_i)(y - c_i) \sum_{i=1}^k d_i \overline{(x - b_i)^2 (y - c_i)}.$$

Tout d'abord, on considère le cas où $xy = 0$. Pour $(x,y) = (0,0)$ le système devient

$$g_\lambda(0,0) = 0 \Leftrightarrow \sum_{i=1}^k d_i \prod_{j \neq i} b_j c_j - \lambda \prod_{i=1}^k b_i c_i = 0, \tag{2.17}$$

ce qui n'arrive que pour une seule valeur de λ puisque les b_i et les c_i ne sont pas nuls.

Lorsque $x = 0$ et $y \neq 0$, on doit résoudre le système

$$g_\lambda(0,y) = \frac{\partial g_\lambda}{\partial y}(0,y) = 0. \tag{2.18}$$

La deuxième équation devient (rappelons que $y \notin \{c_1, \dots, c_k\}$)

$$\sum_{i=1}^{k} d_i \overline{b_i (y-c_i)^2} = 0$$

ou encore en multipliant par $\prod_{i=1}^{k}(y-c_i)^2$:

$$\sum_{i=1}^{k} d_i \overline{b_i} \prod_{j\neq i} (y-c_j)^2 = 0.$$

Comme les c_j sont deux à deux distincts et les b_i ne sont pas nuls ce polynôme ne s'annule pas en $y = c_1$. Il n'est donc pas identiquement nul, et admet au plus $2(k-1)$ racines y. On en déduit en utilisant (2.15) qu'il n'y a au plus que $2(k-1)$ valeurs de λ telles que le système (2.18) ait des solutions.

On vérifie de la même façon que le système

$$g_\lambda(x,0) = \frac{\partial g_\lambda}{\partial x}(x,0) = 0 \tag{2.19}$$

admet des solutions pour au plus $2(k-1)$ valeurs de λ.

Il reste maintenant à étudier le système

$$g_\lambda(x,y) = \frac{\partial g_\lambda}{\partial y}(x,y) = \frac{\partial g_\lambda}{\partial y}(x,y) = 0, \tag{2.20}$$

avec $x \notin \{b_1, \dots, b_k\}$, $y \notin \{c_1, \dots, c_k\}$.

En reprenant le calcul précédent, on remarque que ce système est équivalent à :

$$\begin{cases} \displaystyle\sum_{i=1}^{k} d_i \overline{(x-b_i)(y-c_i)} = \lambda \\ \displaystyle\sum_{i=1}^{k} d_i \prod_{j\neq i} (x-b_j)^2 (y-c_j) = 0 \\ \displaystyle\sum_{i=1}^{k} d_i \prod_{j\neq i} (x-b_j)(y-c_j)^2 = 0. \end{cases} \tag{2.21}$$

Soit $P_1(x,y) = \sum_{i=1}^{k} d_i \prod_{j\neq i}(x-b_j)^2(y-c_j)$ et $P_2(x,y) = \sum_{i=1}^{k} d_i \prod_{j\neq i} (x-b_j)(y-c_j)^2$.

Pour montrer que les deux dernières lignes du système n'ont qu'un nombre fini de solutions (x, y) il suffit de vérifier que les polynômes P_1 et P_2 sont premiers entre eux. Notons $T = (P_1, P_2)$ puis $P_1 = TR_1$ et $P_2 = TR_2$. Si T n'est pas constant, alors quitte à échanger les rôles de x et de y, on peut supposer que le degré partiel en y pour T est supérieur à 1.

Le degré en y de P_1 est inférieur à $k-1$ c'est donc aussi le cas pour T et R_1. De plus, le degré partiel en y de R_1 est au plus $k-2$. Comme les c_j sont deux à deux distincts, les polynômes $\prod_{j\neq i}(y-c_j)$ forment une base de l'espace vectoriel des polynômes de $\mathbb{F}_{p^n}[Y]$ de degré au plus $k-1$.

On en déduit que T et R_1 s'écrivent sous la forme :

(2.22)
$$T(X,Y)=\sum_{i=1}^{k}\alpha_i(X)\prod_{j\neq i}(Y-c_j),\quad R_1(X,Y)=\sum_{i=1}^{k}\beta_i(X)\prod_{j\neq i}(Y-c_j),$$

où $\alpha_i(X), \beta_i(X) \in \mathbb{F}_{p^n}[X]$ pour $1 \leqslant i \leqslant k$. Comme T divise P_2, pour tout $1 \leqslant i \leqslant k$ le polynôme $T(X, c_i) = \alpha_i(X)\prod_{j\neq i}(c_i - c_j)$ divise $P_2(X, c_i) = d_i \prod_{j\neq i}(X - b_j)(c_i - c_j)^2$. On en déduit que $\alpha_i(X)$ est de la forme $\alpha_i(X) = s_i \prod_{j\in L_i}(X - b_j)$ avec $s_i \in \mathbb{F}_{p^n}$ et $L_i \subset \{1, \dots, k\} \setminus \{i\}$.

On a alors

$$P_1(X,c_i)=d_i\prod_{j\neq i}(X-b_j)^2(c_i-c_j)=s_i\prod_{j\in L_i}(X-b_j)\beta_i(X)\prod_{j\neq i}(c_i-c_j)^2.$$

Ainsi le polynôme β_i est de la forme

$$\beta_i(X)=t_i\prod_{j\neq i}(X-b_j)\prod_{j\notin L_i\cup\{i\}}(X-b_j).$$

Le coefficient du terme en Y^{k-1} dans l'écriture de R_1 dans (2.22) est $\sum_{i=1}^{k}\beta_i(X)$. Ce coefficient doit être nul car R_1 est de degré au plus $k-2$ en Y. Or, pour $1 \leqslant i \leqslant k$,

$$0=\sum_{m=1}^{k}\beta_m(b_i)=\beta_i(b_i)=t_i\prod_{j\neq i}(b_i-b_j)\prod_{j\notin L_i\cup\{i\}}(b_i-b_j).$$

Cela entraîne que $t_i = 0$ puisque les b_j sont deux à deux distincts. Ainsi, chaque β_i et par suite R_1 et P_1 sont identiquement nuls. Cela n'est pas possible. Par conséquent P_1 et P_2 sont premiers entre eux.

Les polynômes homogènes associés $P_1(X : Y : Z) = Z^{3(k-1)}P_1(X/Z, Y/Z)$, $P_2(X : Y : Z) = Z^{3(k-1)}P_2(X/Z, Y/Z)$ sont alors premiers entre eux. En effet leur pgcd h est un polynôme homogène vérifiant $h(X : Y : 1) = 1$ et est donc de la forme $h(X : Y : Z) = aZ^t$ ce qui n'est possible que

pour $t = 0$. On en déduit par un résultat classique sur les intersections de courbes planes (Théorème de Bézout, cf [22] ou [23]) que

$$|\{(x,y) \in \mathbb{F}_{p^n}^2 : P_1(X,Y) = 0 = P_2(X,Y)\}| \leqslant \deg P_1 \times \deg P_2 \leqslant 9(k-1)^2.$$

Le Théorème 2.6 s'applique donc pour presque tous les λ avec au plus $K = 9(k-1)^2+4(k-1)+2$ exceptions. On rappelle que le terme $4(k-1)+1$ correspond aux λ pour lesquels il existe un couple (x,y) tels que $xy = 0$ et solutions d'un des systèmes (2.17), (2.18) ou (2.19) et le $+1$ supplémentaire tient compte du cas $\lambda = 0$. En tenant compte de (2.13) on obtient la Proposition 2.4 et cela termine la preuve du Théorème 1.3.

3. La complexité K_3 dans le cas où S est l'ensemble des inverses d'une suite d'entiers consécutifs

Dans ce paragraphe, nous démontrons le Théorème 1.2 relatif aux polynômes à racines simples dans $\mathbb{F}_p$. Pour $\mathcal{A} \subset \mathbb{F}_p$, on reprend la notation $f_{\mathcal{A}}(X) = \prod_{a\in\mathcal{A}}(X-a)$.

On remarque que $|\mathcal{P}_3(d,p)| = \binom{p}{d}$. La condition $p > 2/(1-\beta)$ implique que $p \geqslant 3$.

Soient $\mathcal{B}$ et $\mathcal{C}$ deux sous-ensembles disjoints de $\mathbb{F}_p$:

$$\mathcal{B} = \{b_1, \dots, b_\ell\}, \quad \mathcal{C} = \{b_{\ell+1}, \dots, b_k\}.$$

Nous devons montrer qu'il existe $f \in \mathcal{P}_3(d,p)$ tel que $r_p(\overline{f(b_i)}) \in \{r, \dots, r+s-1\}$ pour $1 \leqslant i \leqslant \ell$ et $r_p(\overline{f(b_i)}) \notin \{r, \dots, r+s-1\}$ pour $\ell < i \leqslant k$. Ici et dans la suite nous considérons des polynômes $f = f_{\mathcal{A}}$ tels que $\mathcal{A} \cap (\mathcal{B} \cup \mathcal{C}) = \emptyset$.

Pour $\beta \in]0,1[$ on définit la fonction $h_\beta(x)$ pour $x \in \mathbb{Z}$ par

$$h_\beta(x) = \begin{cases} 1 & \text{si } 0 \leqslant r_p(x) < \beta p \\ 0 & \text{sinon.} \end{cases}$$

En adaptant la preuve du lemme 2.2 de [5], on montre que

$$h_\beta(x) = \sum_{|h|<p/2} \alpha_h \mathbf{e}_p(hx), \tag{3.1}$$

avec

$$\alpha_0 = \frac{\lceil \beta p \rceil}{p} \text{ et } \alpha_h = \frac{1 - \mathbf{e}_p(-h\lceil \beta p \rceil)}{p(1-\mathbf{e}_p(-h))} \text{ pour } h \neq 0.$$

On a ensuite remarqué dans [5] que $|\alpha_h| \leqslant 1/(2h)$ pour $h \neq 0$.

Il suffit de montrer que la quantité

$$T := \sum_{\substack{f\in\mathcal{P}_3(d,p)\\ \prod_{i=1}^k f(b_i)\neq 0}} \prod_{i=1}^{\ell} h_\beta(\overline{f(b_i)}-r) \prod_{i=\ell+1}^{k} (1-h_\beta(\overline{f(b_i)}-r))$$

est strictement positive.

On développe les produits ci-dessus en utilisant (3.1) et en isolant le terme principal :

$$\begin{aligned} T =& \binom{p-k}{d} \frac{\lceil \beta p\rceil^{\ell}\,(p-\lceil\beta p\rceil)^{k-\ell}}{p^k} \\ &+ \sum_{\substack{0\leqslant t\leqslant \ell\\ 0\leqslant t'\leqslant k-\ell\\ (t,t')\neq(0,0)}} \frac{\lceil \beta p\rceil^{\ell-t}\,(p-\lceil\beta p\rceil)^{k-\ell-t'}}{p^{k-t-t'}}(-1)^{t'} \\ &\times \sum_{\substack{1\leqslant i_1<\ldots<i_t\leqslant \ell\\ \ell<i_{t+1}<\ldots<i_{t+t'}\leqslant k}} \sum_{0<|h_1|,\ldots,|h_{t+t'}|<p/2} \Big(\prod_{i=1}^{t+t'}\alpha_{h_i}\Big)\mathbf{e}_p\Big(-r\sum_{m=1}^{t+t'}h_m\Big) \\ &\qquad\qquad \times U(h_1,\ldots,h_{t+t'}), \end{aligned}$$

avec

$$\begin{aligned} U(h_1,\ldots,h_{t+t'}) &= \sum_{\substack{f\in\mathcal{P}_3(d,p)\\ \prod_{i=1}^k f(b_i)\neq 0}} \mathbf{e}_p\Big(\sum_{m=1}^{t+t'} h_m\overline{f(b_{i_m})}\Big) \\ &= \sum_{\{a_1,\ldots,a_d\}\subset\mathbb{F}_p\setminus(\mathcal{B}\cup\mathcal{C})} \mathbf{e}_p\Big(\sum_{m=1}^{t+t'} h_m\prod_{j=1}^{d}\overline{b_{i_m}-a_j}\Big). \end{aligned}$$

On fixe les $d-2$ premières variables et on somme sur les deux dernières :

$$\begin{aligned} &|U(h_1,\ldots,h_{t+t'})| \\ &\leqslant \sum_{\{a_1,\ldots,a_{d-2}\}\subset\mathbb{F}_p\setminus(\mathcal{B}\cup\mathcal{C})} \Bigg|\sum_{\substack{\{a_{d-1},a_d\}\subset\mathbb{F}_p\setminus\mathcal{B}\cup\mathcal{C}\\ a_i\neq a_j \text{ si } i\neq j}} \mathbf{e}_p\Big(\sum_{m=1}^{t+t'} h_m\prod_{j=1}^{d}\overline{b_{i_m}-a_j}\Big)\Bigg| \\ &\leqslant \sum_{\{a_1,\ldots,a_{d-2}\}\subset\mathbb{F}_p\setminus(\mathcal{B}\cup\mathcal{C})} \Bigg|\sum_{a_{d-1},a_d\in\mathbb{F}_p\setminus(\mathcal{B}\cup\mathcal{C})} \mathbf{e}_p\Big(\sum_{m=1}^{t+t'} h_m\prod_{j=1}^{d}\overline{b_{i_m}-a_j}\Big)\Bigg| \\ &\qquad + 2(k+d-1)p^{d-1}. \end{aligned}$$

Ce terme $2(k+d-1)p^{d-1}$ est une majoration de la contribution des $(a_1,\dots,a_d)$ tels que $a_d = a_{d-1}$, ou $a_{d-1}, a_d \in \mathcal{B}\cup\mathcal{C}\cup\{a_1,\dots,a_{d-2}\}$. D'après le Théorème 1.3, la somme intérieure sur a_{d-1}, a_d est majorée par $44^{4k}p$. On en déduit la majoration :

$$|U(h_1,\dots,h_{t+t'})| \leqslant (44^{4k}+2k+2d-2)p^{d-1}.$$

Cela donne pour T (la constante implicite dans la formule suivante est de valeur absolue inférieure à 1) :

$$\begin{aligned}T =& \binom{p-k}{d}\frac{\lceil\beta p\rceil^{\ell}(p-\lceil\beta p\rceil)^{k-\ell}}{p^k}\\ &+ O\Bigg(\sum_{\substack{0\leqslant t\leqslant \ell\\ 0\leqslant t'\leqslant k-\ell\\ (t,t')\neq(0,0)}}\frac{\lceil\beta p\rceil^{\ell-t}(p-\lceil\beta p\rceil)^{k-\ell-t'}}{p^{k-t-t'}}(-1)^{t+t'}\\ &\times\sum_{\substack{1\leqslant i_1<\dots<i_t\leqslant \ell\\ \ell<i_{t+1}<\dots<i_{t+t'}\leqslant k}}\ \sum_{0<|h_1|,\dots,|h_{t+t'}|<p/2}\Big(\prod_{i=1}^{t+t'}|\alpha_{h_i}|\Big)(44^{4k}+2k+2d-2)p^{d-1}\Bigg).\end{aligned}$$

Comme $|\alpha_h| \leqslant (2h)^{-1}$ lorsque $h\neq 0$, les sommes sur les h_i sont inférieures à $\log(3p)$. On obtient donc :

$$\begin{aligned}T =& \binom{p-k}{d}\frac{\lceil\beta p\rceil^{\ell}(p-\lceil\beta p\rceil)^{k-\ell}}{p^k}\\ &+ O\Bigg(\Big(\frac{\lceil\beta p\rceil}{p}+\log(3p)\Big)^{\ell}\Big(\frac{p-\lceil\beta p\rceil}{p}+\log(3p)\Big)^{k-\ell}(44^{4k}+2k+2d-2)p^{d-1}\Bigg)\\ =& \binom{p-k}{d}\frac{\lceil\beta p\rceil^{\ell}(p-\lceil\beta p\rceil)^{k-\ell}}{p^k}+O\Big(\log(9p)^k(44^{4k}+2k+2d-2)p^{d-1}\Big),\end{aligned}$$

où la constante implicite du O est inférieure à 1 en valeur absolue. Lorsque p vérifie (1.1) $T>0$ et ainsi $K_3(S,d)\geqslant k$. Cela termine la démonstration du Théorème 1.2.

4. La complexité K_3 dans le cas général

Dans ce paragraphe, on étudie $K_3(S,d)$ où S est maintenant un sous-ensemble de $\mathbb{F}_p$ vérifiant les hypothèses du Théorème 1.4.

Soit $k\leqslant d/2$. Soient $\mathcal{B},\mathcal{C}$ deux sous-ensembles de $\mathbb{F}_p$ disjoints tels que $|\mathcal{B}|=\ell, |\mathcal{C}|=k-\ell$ pour un certain $0\leqslant\ell\leqslant k$. Nous devons montrer qu'il

existe un sous-ensemble $\mathcal{A} \subset \mathbb{F}_p$ de cardinal d tel que $\mathcal{B} \subset \mathcal{R}(f_{\mathcal{A}}, S)$ et $\mathcal{C} \cap \mathcal{R}(f_{\mathcal{A}}, S) = \emptyset$.

Notons $\mathcal{B} = \{b_1, \dots, b_\ell\}$, $\mathcal{C} = \{b_{\ell+1}, \dots, b_k\}$.

• Si $S = \{0\}$, alors on peut prendre $f_{\mathcal{A}}(X) = \prod_{i=1}^{\ell}(X - b_i)\prod_{i=\ell+1}^{d}(X - b'_i)$ avec $\{b'_{\ell+1}, \dots, b'_d\} \cap (\mathcal{B} \cup \mathcal{C}) = \emptyset$, ce qui est possible lorsque $k + d < p$. De même, pour $S^c = \{0\}$, $f_{\mathcal{A}}(X) = \prod_{i=1}^{d-\ell-1}(X - b'_i)\prod_{i=\ell+1}^{k}(X - b_i)$ avec $\{b'_1, \dots, b'_{d-\ell-1}\} \cap (\mathcal{B} \cup \mathcal{C}) = \emptyset$ convient.

• Nous supposons maintenant que $S \neq \{0\}, \mathbb{F}_p^*$. Il existe $s \in S \setminus \{0\}$ et $r \in S^c \setminus \{0\}$.

Pour terminer la preuve du Théorème 1.4, il suffit de trouver $\mathcal{A} \subset \mathbb{F}_p$ de cardinal d tel que

$$f_{\mathcal{A}}(x) \in \begin{cases} S \setminus \{0\} & \text{si } x \in \mathcal{B} \\ S^c \setminus \{0\} & \text{si } x \in \mathcal{C}. \end{cases} \tag{4.1}$$

Soit $T_2(S, d)$ le nombre de sous-ensembles $\mathcal{A}$ vérifiant (4.1).

On a alors d'après l'orthogonalité des caractères sur $\mathbb{F}_p$:

$$\varphi(p)^k T_2(S,d) = \sum_{\{a_1,\dots,a_d\}\subset\mathbb{F}_p} \prod_{j=1}^{\ell} \left(\sum_{\chi} \sum_{r\in S\setminus\{0\}} \chi\Big(\prod_{i=1}^{d}(b_j - a_i)\Big)\overline{\chi}(r)\right) \times \prod_{j=\ell+1}^{k} \left(\sum_{\chi} \sum_{s\in S^c\setminus\{0\}} \chi\Big(\prod_{i=1}^{d}(b_j - a_i)\Big)\overline{\chi}(s)\right),$$

où dans les différentes sommes, χ parcourt l'ensemble des caractères de $\mathbb{F}_p^*$, et $\overline{\chi}$ est le caractère conjugué de χ. A priori, la somme devrait être restreinte aux sous-ensembles $\mathcal{A} = \{a_1, \dots, a_d\} \subset \mathbb{F}_p$ tels que $\mathcal{A} \cap (\mathcal{B} \cup \mathcal{C}) = \emptyset$, mais la contribution des $a_i = b_j$ étant nulle, nous pouvons oublier cette condition. Soit χ_0 le caractère principal de $\mathbb{F}_p$. En développant la ligne ci-dessus et en isolant le terme où tous les χ valent χ_0, on obtient :

$$\varphi(p)^k T_2(S,d) = \binom{p-k}{d} |S \setminus \{0\}|^{\ell} |S^c \setminus \{0\}|^{k-\ell} + O(E),$$

où le terme d'erreur E est défini par

$$E = \sum_{\substack{0\leqslant t\leqslant \ell \\ 0\leqslant t'\leqslant k-\ell \\ (t,t')\neq(0,0)}} |S \setminus \{0\}|^{\ell-t} |S^c \setminus \{0\}|^{k-\ell-t'} \sum_{\substack{1\leqslant i_1<\dots<i_t\leqslant \ell \\ \ell<i_{t+1}<\dots<i_{t+t'}\leqslant k}} \sum_{\chi_1\neq\chi_0} \cdots \sum_{\chi_{t+t'}\neq\chi_0} |Z(\bar{\chi}_1, \dots, \bar{\chi}_{t+t'})||V(\chi_1, \dots, \chi_{t+t'})|,$$

avec

$$V(\chi_1,\dots,\chi_{t+t'}) = \sum_{\mathcal{A}=\{a_1,\dots,a_d\}\subset\mathbb{F}_p} \prod_{j=1}^{t+t'} \chi_j(f_{\mathcal{A}}(b_{i_j})),$$

$$Z(\chi_1,\dots,\chi_{t+t'}) = \prod_{j=1}^{t}\Big(\sum_{r\in S}\chi_j(r)\Big)\prod_{j=t+1}^{t+t'}\Big(\sum_{s\notin S}\chi_j(s)\Big),$$

et la constante implicite est de module inférieur à 1. Pour majorer les sommes $V(\chi_1,\dots,\chi_{t+t'})$, nous utilisons le lemme suivant.

LEMME 4.1. — *Soient p un nombre premier, χ un caractère non principal d'ordre d (avec $d|(p-1)$), $f(X)\in\mathbb{F}_p[X]$. Notons m le nombre de racines distinctes de $f(X)$ dans $\overline{\mathbb{F}_p}$. Si $f(X)$ n'est pas une puissance d ième alors*

$$\Big|\sum_{x\in\mathbb{F}_p}\chi(f(x))\Big| \leqslant (m-1)\sqrt{p}.$$

Il s'agit du théorème 2C' p. 43 de [21] dans le cas où $q=p$.

Avant d'utiliser ce lemme, nous devons faire un travail préparatoire analogue à [6] dont les idées de base se trouvent dans [20]. La difficulté ici est que nous travaillons avec plusieurs variables que nous devons rendre *indépendantes*.

Comme $\mathbb{F}_p^*$ est cyclique, chaque caractère χ_m peut s'écrire sous la forme χ^{α_m} où χ est un caractère d'ordre $p-1$. Ainsi pour des caractères $\chi_1,\dots,\chi_{t+t'}$ différents de χ_0, il existe des entiers compris entre 1 et $p-2$ $\alpha_1,\dots,\alpha_{t+t'}$ tels que

$$V(\chi_1,\dots,\chi_{t+t'}) = V(\chi^{\alpha_1},\dots,\chi^{\alpha_{t+t'}}) = W(\alpha_1,\dots,\alpha_{t+t'}),$$

avec

$$W(\alpha_1,\dots,\alpha_{t+t'}) = \sum_{\{a_1,\dots,a_d\}\subset\mathbb{F}_p}\prod_{j=1}^{t+t'}\chi^{\alpha_j}\Big(\prod_{m=1}^{d}(b_{i_j}-a_m)\Big).$$

Nous appliquons maintenant le Lemme 4.1 pour majorer les sommes sur chaque a_d. Cependant, le fait que les a_j soient deux à deux distincts rend les calculs un peu plus difficiles.

Dans une première étape, on écrit

(4.2)

$$\begin{aligned} W(\alpha_1,\dots,\alpha_{t+t'}) &= \sum_{\{a_1,\dots,a_{d-1}\}\subset\mathbb{F}_p}\prod_{j=1}^{t+t'}\chi^{\alpha_j}\Big(\prod_{m=1}^{d-1}(b_{i_j}-a_m)\Big)\\ &\qquad\times\sum_{a_d\in\mathbb{F}_p\setminus\{a_1,\dots,a_{d-1}\}}\chi^{\alpha_j}\Big(\prod_{j=1}^{t+t'}(b_{i_j}-a_d)\Big)\\ &=\sum_{\{a_1,\dots,a_{d-1}\}\subset\mathbb{F}_p}\prod_{j=1}^{t+t'}\chi^{\alpha_j}\Big(\prod_{m=1}^{d-1}(b_{i_j}-a_m)\Big)\sum_{a_d\in\mathbb{F}_p}\chi^{\alpha_j}\Big(\prod_{j=1}^{t+t'}(b_{i_j}-a_d)\Big)\\ &\quad-\sum_{h=1}^{d-1}\sum_{\{a_1,\dots,a_{d-1}\}\subset\mathbb{F}_p}\prod_{j=1}^{t+t'}\chi^{\alpha_j}\Big(\prod_{\substack{m=1\\ m\neq h}}^{d-1}(b_{i_j}-a_m)\Big)\chi^{2\alpha_h}\Big(\prod_{m=1}^{d-1}(b_{i_h}-a_m)\Big). \end{aligned}$$

Dans cette deuxième ligne, la variable a_d est indépendante des autres. En itérant ce procédé au bout de d étapes, on obtient un nombre fini (au plus $d!$) de sommes de la forme

(4.3)

$$T(\boldsymbol{\alpha},\boldsymbol{\lambda}) := \Big(\sum_{a_1\in\mathbb{F}_p}\prod_{j=1}^{t+t'}\chi(b_{i_j}-a_1)^{\alpha_j\lambda_1}\Big)\cdots\Big(\sum_{a_h\in\mathbb{F}_p}\prod_{j=1}^{t+t'}\chi(b_{i_j}-a_h)^{\alpha_j\lambda_h}\Big),$$

où $1\leqslant h\leqslant d$ et $\lambda_1,\dots,\lambda_h$ sont des entiers strictement positifs tels que

$$\lambda_1+\cdots+\lambda_h=d.$$

Dans la suite, nous utiliserons le fait que

$$h=d-\sum_{m=1}^{h}(\lambda_m-1). \tag{4.4}$$

Notons le pgcd $\alpha=(\alpha_1,\dots,\alpha_{t+t'})$ et $\alpha_i'=\alpha_i/\alpha$. Pour chaque $m\in\{1,\dots,h\}$, on a :

$$\sum_{a_m\in\mathbb{F}_p}\prod_{j=1}^{t+t'}\chi(b_{i_j}-a_m)^{\alpha_j\lambda_m}=\sum_{a_m\in\mathbb{F}_p}\chi^{\alpha\lambda_m}\Big(\prod_{j=1}^{t+t'}(b_{i_j}-a_m)^{\alpha_i'}\Big).$$

On peut appliquer le Lemme 4.1 si $\chi^{\alpha\lambda_m}\neq\chi_0$. Comme $(\alpha_1',\dots,\alpha_{t+t'}')=1$, on a :

$$\sum_{a_m\in\mathbb{F}_p}\prod_{j=1}^{t+t'}\chi(b_{i_j}-a_m)^{\alpha_j\lambda_m}\leqslant\begin{cases}(k-1)\sqrt{p} & \text{si } \alpha\lambda_m\not\equiv 0 \mod (p-1)\\ p & \text{sinon.}\end{cases}$$

Comme $(p-1) \not| \alpha$, lorsque $\lambda_m = 1$, la somme est de module inférieur à $(k-1)\sqrt{p}$. Dans le cas où $\lambda_m \geqslant 2$, nous majorons la somme trivialement par p. Notons $u(\boldsymbol{\lambda})$ le nombre d'indices m tels que $\lambda_m \geqslant 2$. On a :

$$T(\boldsymbol{\alpha}, \boldsymbol{\lambda}) \leqslant ((k-1)\sqrt{p})^{h-u(\boldsymbol{\lambda})} p^{u(\boldsymbol{\lambda})} \leqslant (k-1)^d \sqrt{p}^{(h+u(\boldsymbol{\lambda}))}.$$

Mais d'après (4.4), $h + u(\boldsymbol{\lambda}) \leqslant d$ puisque $u(\boldsymbol{\lambda}) \leqslant \sum_{1 \leqslant m \leqslant h} (\lambda_m - 1)$. Cela prouve que $T(\boldsymbol{\alpha}, \boldsymbol{\lambda}) \leqslant (k-1)^d p^{d/2}$.

On obtient alors :

(4.5)

$$\begin{aligned} M &:= \Big| \varphi(p)^k T_2(S,d) - \binom{p-k}{d} |S \setminus \{0\}|^\ell |S^c \setminus \{0\}|^{k-\ell} \Big| \\ &\ll d!(k-1)^d p^{d/2} \sum_{\substack{0 \leqslant t \leqslant \ell \\ 0 \leqslant t' \leqslant k-\ell \\ (t,t') \neq (0,0)}} \sum_{\substack{1 \leqslant i_1 < \cdots < i_t \leqslant \ell \\ \ell < i_{t+1} < \cdots < i_{t+t'} \leqslant k}} |S \setminus \{0\}|^{\ell - t} |S^c \setminus \{0\}|^{k-\ell-t'} \\ &\quad \times \sum_{\chi_1 \neq \chi_0} \cdots \sum_{\chi_{t+t'} \neq \chi_0} \prod_{j=1}^{t} \Big| \sum_{s \in S} \overline{\chi}_j(s) \Big| \prod_{j=t+1}^{t+t'} \Big| \sum_{s \in S^c} \overline{\chi}_j(s) \Big|. \end{aligned}$$

Lorsque S et S^c sont de taille suffisamment grande, on peut obtenir des majorations intéressantes des sommes de caractères sur S et S^c. On commence par appliquer l'inégalité de Cauchy-Schwarz :

$$\begin{aligned} \sum_{\chi \neq \chi_0} \Big| \sum_{s \in S} \chi(s) \Big| &= \sum_{\chi} \Big| \sum_{s \in S} \chi(s) \Big| - |S \setminus \{0\}| \\ &\leqslant p^{1/2} \Big(\sum_{\chi} \Big| \sum_{s \in S} \chi(s) \Big|^2 \Big)^{1/2} - |S \setminus \{0\}|. \end{aligned} \tag{4.6}$$

On développe le carré puis on profite de l'orthogonalité des caractères :

$$\sum_{\chi} \Big| \sum_{s \in S} \chi(s) \Big|^2 = \sum_{\chi} \sum_{s_1, s_2 \in S} \chi(s_1) \overline{\chi}(s_2) = \varphi(p) |S \setminus \{0\}|.$$

On en déduit l'inégalité :

$$\sum_{\chi \neq \chi_0} \Big| \sum_{s \in S} \chi(s) \Big| \leqslant \sqrt{p \varphi(p) |S \setminus \{0\}} \leqslant p \sqrt{|S \setminus \{0\}|}.$$

On obtient de la même façon une majoration de $\sum_{\chi\neq\chi_0}\Big|\sum_{s\in S^c}\chi(s)\Big|$. Finalement,

(4.7)

$$M \ll d!(k-1)^d p^{d/2} \sum_{\substack{0\leqslant t\leqslant \ell\\ 0\leqslant t'\leqslant k-\ell\\ (t,t')\neq(0,0)}} |S|^{\ell-t}|S^c|^{k-\ell-t'}(p\sqrt{|S|})^t(p\sqrt{|S^c|})^{t'} \sum_{\substack{1\leqslant i_1<\cdots<i_t\leqslant \ell\\ \ell<i_{t+1}<\cdots<i_{t+t'}\leqslant k}} 1$$

$$\ll d!(k-1)^d p^{d/2}\big[(|S|+p\sqrt{|S|})^\ell(|S^c|+p\sqrt{|S^c|})^{k-\ell}$$

$$\ll d!(k-1)^d 2^k p^{k+d/2}|S|^{\ell/2}|S^c|^{(k-\ell)/2}.$$

Remarquons que le terme principal est de l'ordre de $\approx p^d|S^\ell||S^c|^{k-\ell}$. Quitte à échanger les rôles de S et S^c, on peut supposer que $|S|\leqslant|S^c|$.

Dans ce cas, la majoration que nous venons d'obtenir est la plus mauvaise quand $\ell=k$. Notre majoration est alors pertinente si

$$p^k \ll_{k,\ell,d} p^{d/2}|S|^{k/2},$$

où la constante implicite dépend de k,ℓ,d. Lorsque $|S|=O(1)$, cela impose $k<d/2$. Lorsque $|S|\gg p$, cela impose $k<d$. Cela termine la preuve du théorème.

5. La complexité K_2, preuve du Théorème 1.5

Pour tout sous-ensemble $\mathcal{A}\subset\mathbb{F}_p$ et tout $x\in\mathbb{F}_p$ nous utiliserons la notation suivante :

$$x+\mathcal{A}=\{x+a : a\in\mathcal{A}\}=\mathcal{A}+x \quad x\mathcal{A}=\{xa : a\in\mathcal{A}\}=\mathcal{A}x.$$

Soit $\mathcal{A}\subset\mathbb{F}_p$ de la forme $\mathcal{A}=\mathcal{B}\cup\mathcal{C}$ avec $\mathcal{B}=\{a_1,\dots,a_\ell\}$ et $\mathcal{C}=\{a_{\ell+1},\dots,a_{d+2}\}$, où $0\leqslant\ell\leqslant d+2$, de sorte que $|\mathcal{A}|=d+2$. On veut trouver $g\in\mathbb{F}_p[X]$ de degré plus petit ou égal à d, sans racine multiple, tel que $g(a_i)\in S$ pour tout $1\leqslant i\leqslant\ell$ et $g(a_i)\in S^c$ pour tout $\ell+1\leqslant i\leqslant d+2$. Nous allons considérer le cas $\ell=1$ puis le cas $\ell\geqslant 2$.

• Supposons d'abord $\ell=1$. Notons pour chaque $i\in\{2,3,\dots,d+2\}$ le polynôme d'interpolation f_i de degré plus petit ou égal à d tel que

$$\begin{cases} f_i(a_1)=0\\ f_i(a_j)=1 \quad \text{si} \quad 2\leqslant j\leqslant d+2,\ j\neq i.\end{cases}$$

Si $f_i(a_i)=0$ pour tout $i\in\{2,3,\dots,d+2\}$, on forme alors le polynôme $f=f_2+f_3+\cdots+f_{d+2}$. On a

$$\begin{cases} f(a_1)=0\\ f(a_i)=d+1\neq 0 \quad \text{si} \quad i\in\{2,3,\dots,d+2\}.\end{cases}$$

On fixe alors $v \in S \setminus \{0\}$ et on choisit $u \notin R(v)$, où

$$R(v) = \{-v\overline{f(z_j)}, j \text{ tel que} f(z_j) \neq 0\} \cup \{(s-v)\overline{(d+1)} : s \in S\},$$

$z_1, \ldots, z_m$, $m \leqslant d-1$, représentant les racines distinctes du polynôme $f'(x)$. Cela est possible, car $|R(v)| \leqslant d-1+|S| < p$. Le polynôme $g(x) = uf(x)+v$ répond alors au problème.

Sinon $f_{i_0}(a_{i_0}) \neq 0$ pour un certain $i_0 \in \{2, 3, \ldots, d+2\}$; on choisit alors g de la forme $g(x) = uf_{i_0}(x) + v$ en fixant $v \in S \setminus \{0\}$ et en choisissant $u \notin R(v)$,

$$R(v) = \{-v\overline{f_{i_0}(z_j)}, j \text{ tel que} f_{i_0}(z_j) \neq 0\} \cup \{s - v : s \in S\} \cup \{(s-v)\overline{f_{i_0}(a_{i_0})} : s \in S\},$$

où $z_1, \ldots, z_m$, $m \leqslant d-1$, représentent les racines distinctes du polynôme $f'(x)$. Cela est possible, car $|R(v)| \leqslant d-1+2|S| < p$.

• Considérons dorénavant $\ell \geqslant 2$. Notons pour tout $i \in \{1, 2, \ldots, \ell\}$ le polynôme d'interpolation f_i de degré plus petit ou égal à d tel que

$$\begin{cases} f_i(a_j) = 0 & \text{si} \quad 1 \leqslant j \leqslant \ell,\ j \neq i \\ f_i(a_j) = 1 & \text{si} \quad \ell+1 \leqslant j \leqslant d+2. \end{cases}$$

Si $f_i(a_i) = 1$ pour tout $i \in \{1, 2, \ldots, \ell\}$, alors le polynôme $f = f_1 + f_2 + \cdots + f_\ell - 1$ vérifie

$$\begin{cases} f(a_j) = 0 & \text{si} \quad 1 \leqslant j \leqslant \ell \\ f(a_j) = \ell - 1 \neq 0 & \text{si} \quad \ell+1 \leqslant j \leqslant d+2, \end{cases}$$

et l'on conclut comme dans un cas précédent, en prenant $v \in S \setminus \{0\}$ et en choisissant $u \notin R(v)$, où

$$R(v) = \{-v\overline{f(z_j)}, j \text{ tel que} f(z_j) \neq 0\} \cup \{(s-v)\overline{(\ell-1)} : s \in S\}.$$

Le polynôme $g(x) = uf(x) + v$ convient alors.

Sinon, il existe $i_0 \in \{1, 2, \ldots, \ell\}$ tel que $\alpha := f_{i_0}(a_{i_0}) \neq 1$. Ainsi on désire trouver $g(x) = uf_{i_0}(x) + v$ (qui est de degré inférieur ou égal à d) sans racine multiple vérifiant

$$\begin{cases} v \in S \\ \alpha u + v \in S \\ u + v \notin S\,. \end{cases}$$

On peut supposer $\alpha \neq 0$ car autrement les deux premières équations sont équivalentes et on a déjà vu qu'un tel polynôme g existait. Notons $s = v$

et $s' = \alpha u + v$. Alors

$$\left\{ \begin{array}{l} v \in S \\ \alpha u + v \in S \\ u + v \notin S \end{array} \right. \iff \left\{ \begin{array}{l} s, s' \in S \\ (1-\overline{\alpha})s + \overline{\alpha} s' \notin S. \end{array} \right.$$

g sans racine multiple signifie que $uf_{i_0}(z_j)+v = (1-\overline{\alpha}f_{i_0}(z_j))s+\overline{\alpha}f_{i_0}(z_j)s' \neq 0$ pour les racines z_j de f'_{i_0}. Il n'est pas difficile de voir que l'égalité $(1-\overline{\alpha}f_{i_0}(z_j))s+\overline{\alpha}f_{i_0}(z_j)s' = 0$ est vérifiée pour au plus $|S|$ couples (s, s'). Ainsi une condition suffisante pour terminer la preuve du théorème est :

$$|\{(s, s') \in S^2 : (1-\overline{\alpha})s + \overline{\alpha} s' \notin S\}| > |S|(d-1)\,. \tag{5.1}$$

Soit les ensembles $S_1 = (1-\overline{\alpha})S$ et $S_2 = \overline{\alpha}S$ de cardinalité $|S|$ (puisque α est différent de 0 et 1). Pour $n \in \mathbb{F}_p$ notons $r(n)$ le nombre de représentations $n = s_1 + s_2$ avec $s_1 \in S_1$ and $s_2 \in S_2$. D'après un résultat de Green and Ruzsa ([13], Proposition 6.1) qui est une généralisation d'un théorème de Pollard, on a, pour tout $t \leqslant |S|$

$$\begin{aligned} \sum_{n\in\mathbb{F}_p} \min(t, r(n)) &\geqslant t \min(p, |S_1| + |S_2| - 1 - t) = t \min(p, 2|S| - 1 - t) \\ &\geqslant t(2|S| - 1 - t) \quad \text{car} \quad 2|S| - 1 - t \leqslant p. \end{aligned}$$

Par ailleurs,

$$\sum_{n\in S} \min(t, r(n)) \leqslant t|S|\,.$$

Donc

$$\begin{aligned} \sum_{n\notin S} r(n) &\geqslant \sum_{n\notin S} \min(t, r(n)) = \sum_{n\in\mathbb{F}_p} \min(t, r(n)) - \sum_{n\in S} \min(t, r(n)) \\ &\geqslant t(2|S| - 1 - t) - t|S| = t(|S| - 1 - t) =: \phi(t). \end{aligned}$$

La minoration est optimale pour $t_0 = \frac{|S|-1}{2}$. t_0 ou $t_0 + 1/2$ étant un entier, on obtient

$$\sum_{n\notin S} r(n) \geqslant \phi(t_0 + 1/2) = \frac{|S|}{2}\left(\frac{|S|}{2} - 1\right).$$

Or, $\frac{|S|}{2}\left(\frac{|S|}{2} - 1\right) > |S|(d-1)$ car par hypothèse $|S| > 4d+2$. En définitive, on a bien l'inégalité voulue (5.1).

BIBLIOGRAPHIE

[1] A. Adolphson & S. Sperber, « Exponential sums and Newton polyhedra : cohomology and estimates », *Ann. of Math. (2)* **130** (1989), n° 2, p. 367-406.

[2] R. Ahlswede, L. H. Khachatrian, C. Mauduit & A. Sárközy, « A complexity measure for families of binary sequences », *Period. Math. Hungar.* **46** (2003), n° 2, p. 107-118.

[3] B. J. Birch & E. Bombieri, « Appendix : On some exponential sums », *Annals of Math.* **121** (1985), p. 345-350.

[4] E. Bombieri, « On exponential sums in finite fields », *Amer. J. Math.* **88** (1966), p. 71-105.

[5] C. Dartyge, E. Mosaki & A. Sárközy, « On large families of subsets of the set of the integers not exceeding N », *Ramanujan J.* **18** (2009), n° 2, p. 209-229.

[6] C. Dartyge & A. Sárközy, « Large families of pseudorandom subsets formed by power residues », *Unif. Distrib. Theory* **2** (2007), n° 2, p. 73-88.

[7] ———, « On pseudo-random subsets of the set of the integers not exceeding N », *Period. Math. Hungar.* **54** (2007), n° 2, p. 183-200.

[8] C. Dartyge, A. Sárközy & M. Szalay, « On the pseudo-randomness of subsets related to primitive roots », *Combinatorica* **30** (2010), n° 2, p. 139-162.

[9] P. Deligne, « La conjecture de Weil. I », *Inst. Hautes Études Sci. Publ. Math.* (1974), n° 43, p. 273-307.

[10] B. Dwork, « On the rationality of the zeta function of an algebraic variety », *Amer. J. Math.* **82** (1960), p. 631-648.

[11] J. Eichenauer-Herrmann & H. Niederreiter, « Bounds for exponential sums and their applications to pseudorandom numbers », *Acta Arith.* **67** (1994), n° 3, p. 269-281.

[12] J. B. Friedlander & H. Iwaniec, « Incomplete Kloosterman sums and a divisor problem », *Ann. of Math. (2)* **121** (1985), n° 2, p. 319-350, With an appendix by Bryan J. Birch and Enrico Bombieri.

[13] B. Green & I. Z. Ruzsa, « Sum-free sets in abelian groups », *Israel J. Math.* **147** (2005), p. 157-188.

[14] C. Hooley, « On exponential sums and certain of their applications », in *Number theory days, 1980 (Exeter, 1980)*, London Math. Soc. Lecture Note Ser., vol. 56, Cambridge Univ. Press, Cambridge, 1982, p. 92-122.

[15] P. Hubert & A. Sárközy, « On p-pseudorandom binary sequences », *Period. Math. Hungar.* **49** (2004), n° 1, p. 73-91.

[16] S. Lang & A. Weil, « Number of points of varieties in finite fields », *Amer. J. Math.* **76** (1954), p. 819-827.

[17] C. Mauduit, J. Rivat & A. Sárközy, « Construction of pseudorandom binary sequences using additive characters », *Monatsh. Math.* **141** (2004), n° 3, p. 197-208.

[18] C. Mauduit & A. Sárközy, « On finite pseudorandom binary sequences. I. Measure of pseudorandomness, the Legendre symbol », *Acta Arith.* **82** (1997), n° 4, p. 365-377.

[19] A. Rojas-León, « Purity of exponential sums on $\mathbb{A}^n$. II », *J. Reine Angew. Math.* **603** (2007), p. 35-53.

[20] A. Sárközy, « A finite pseudorandom binary sequence », *Studia Sci. Math. Hungar* **38** (2001), p. 377-384.

[21] W. M. Schmidt, *Equations over finite fields. An elementary approach*, Lecture Notes in Mathematics, Vol. 536, Springer-Verlag, Berlin, 1976, ix+276 pages.

[22] M. Waldschmidt, « Le théorème de Bézout et le résultant de deux polynômes », Revue de Mathématiques Spéciales, 2003–2004, Numéro 114-1.

[23] R. J. Walker, *Algebraic curves*, Springer-Verlag, New York, 1978, Reprint of the 1950 edition, x+201 pages.

Manuscrit reçu le 6 avril 2012,
accepté le 28 novembre 2012.

Ramachandran BALASUBRAMANIAN
Institute of Mathematical Sciences
C.I.T. Campus
Taramani, Chennai 600113 (India)
balu@imsc.res.in

Cécile DARTYGE
Université de Lorraine
Institut Élie Cartan
BP 70239
54506 Vandœuvre-lès-Nancy Cedex (France)
cecile.dartyge@univ-lorraine.fr

Élie MOSAKI
Université de Lyon
Université Lyon 1
Institut Camille Jordan CNRS UMR 5208
43, boulevard du 11 Novembre 1918
69622 Villeurbanne (France)
mosaki@math.univ-lyon1.fr