ADDITIVE FEATURES OF DETERMINANT VALUES OVER p-ADIC RINGS

BEN LICHTIN

ABSTRACT. This paper uses exponential sum methods to show that if $E \subset \mathcal{M}_2(\mathbb{Z}/p^r)$ is a finite set of 2×2 matrices with sufficiently large density and j is any unit in the finite ring $\mathbb{Z}/p^r$ then there exist at least two elements of E whose difference has determinant j.

1. INTRODUCTION

This article studies an additive combinatorial problem in the non commutative setting of the ring of matrices over finite p-adic rings $\mathbb{Z}_q := \mathbb{Z}/q$, where $q = p^r$ for some $r \geq 2$. Denoting the unit group by U_q and the set of 2×2 matrices with entries in $\mathbb{Z}_q$ by $\mathcal{M}_2(\mathbb{Z}_q)$ we find a simple lower bound on the density δ_E of a subset $E \subset \mathcal{M}_2(\mathbb{Z}_q)$ which insures that the following “representation" property is satisfied:

$$\textit{For each } j \in U_q \textit{ there exist } \mathbf{x}, \mathbf{y} \in E \textit{ such that} \quad det(\mathbf{x} - \mathbf{y}) = j.$$

Our conclusion, see Theorem A below, is, in an appropriate sense, uniform in $r \geq 2$ and $p \gg 1$.

This result extends to p-adic rings an earlier result of Demiroglu [D] that was proved over the finite field $\mathbb{F}_p$ using graph theoretic methods. Moreover, and perhaps more significantly, our result is rather more precise *since we also derive an explicit main term* for the number of such representations of j with an error that is *strictly smaller* provided p is sufficiently large.

One way to think of our theorem, as well as that in [L], is that it is a modest response to Tao's general challenge to extend results in additive combinatorics, proved over finite fields, to finite rings, be they commutative or non commutative. Another noteworthy aspect of Theorem A is its uniformity in $r \geq 2$, provided that p is sufficiently large. This is a property that is, perhaps, a bit stronger than might a priori be expected.

The key ingredients are the same that we needed in [ibid.] to solve appropriate analogues of Erdös' distance problem and a sum-product problem over the rings $\mathbb{Z}_q$. These involve techniques of p-adic analysis and estimates for classes of exponential sums mod p^r (see §2.2).

Defining for each $j \in U_q$ and $E \subset \mathcal{M}_2(\mathbb{Z}_q)$

$$\tau_j^{(2)}(E) := \left| \{ (\mathbf{x}, \mathbf{y}) \in E^2 : \ det(\mathbf{x} - \mathbf{y}) = j \} \right|,$$

2020 *Mathematics Subject Classification.* Primary: 11T24, 52C10.

Key words and phrases. k-point configurations, Fourier transform, exponential sum estimates, p-adic numbers.

the main result of this article is as follows, in which the meaning of the hypothesis is explained in (6) in §2. Its proof is given in §3.

Theorem A.

(1)

$$p \gg 1 \;\; \textit{and} \;\; \delta_E \gg p^{-3/2} \quad \textit{implies} \quad \tau_j^{(2)}(E) = \tfrac{|E|^2}{q} \cdot (1 + o(1)) \quad \textit{uniformly in } j \textit{ and } r \geq 2\,.$$

2. Recalling the main result from [L]

In order to make this article reasonably self contained, it seems useful to present at first a reasonably detailed overview of the proof of Theorem 1 (see §2.1). Doing so should allow the reader to appreciate more completely how the proof of Theorem A is, in fact, a simple modification of the proof of (6) (see below). As such, in this section (only) we work with subsets $E \subset \mathbb{Z}_q^n$, for any $n \geq 2$, and the "distance function"

$$P : \mathbf{x} \longrightarrow \|\mathbf{x}\| := \sum_{i=1}^{n} x_i^2\,. \tag{2}$$

Note: To simplify the task of the reader when looking over [ibid], we use throughout §2 the particular notations used in the earlier article:

For any $j \in U_q$ and $\mathbf{m} = (m_1, \ldots, m_n) \in \mathbb{Z}_q^n$ we set

$$\lambda_j^{(2)}(E) = |\{(\mathbf{x}_1, \mathbf{x}_2) \in E^2 : \|\mathbf{x}_1 - \mathbf{x}_2\| = j\}|;$$

$$\nu_{\mathbf{m}} = min_\ell\{\, ord_p\, m_\ell\} \qquad (ord_p\, 0 := r)\,;$$

$$1_j(\mathbf{x}) = \textit{characteristic function of} \;\; \{\mathbf{x} \in \mathbb{Z}_q^n : \|\mathbf{x}\| = j\}\,;$$

$$\textit{for any } y \in \mathbb{Z}_q \;\; \chi\, y := e^{2\pi i y/q}\,;$$

$$\textit{for any} \;\; \mathbf{x} = (x_1, \ldots, x_n), \mathbf{m} = (m_1, \ldots, m_n) \in \mathbb{Z}_q^n \quad \langle \mathbf{x}, \mathbf{m} \rangle := \sum_i x_i m_i\,;$$

$$\widehat{1}_j(\mathbf{m}) = q^{-n} \sum_{\mathbf{x} \in \mathbb{Z}_q^n} 1_j(\mathbf{x}) \chi \langle \mathbf{x}, -\mathbf{m} \rangle\,;$$

$$\delta_E = |E|/q^n \quad \text{and} \quad \theta = \frac{n-1}{2}.$$

The starting point is this expression

$$\lambda_j^{(2)}(E) = \sum_{(\mathbf{x}_1, \mathbf{x}_2) \in \mathbb{Z}_q^{2n}\}} 1_E(\mathbf{x}_1) \cdot 1_E(\mathbf{x}_2) \cdot 1_j(\mathbf{x}_1 - \mathbf{x}_2).$$

Applying Fourier inversion then implies

$$\lambda_j^{(2)}(E) \;=\; q^{2n} \cdot \sum_{\mathbf{m}} \widehat{1}_E(\mathbf{m}) \cdot \widehat{1}_E(-\mathbf{m}) \cdot \widehat{1}_j(\mathbf{m}) = \mathcal{M} + \mathcal{E} \tag{3}$$

$$\text{where} \qquad \mathcal{M} \;:=\; q^{2n} \cdot \widehat{1}_E^2(\mathbf{0}) \cdot \widehat{1}_j(\mathbf{0}) \quad \text{and} \quad \mathcal{E} := q^{2n} \cdot \sum_{\mathbf{m} \neq \mathbf{0}} \widehat{1}_E(\mathbf{m}) \cdot \widehat{1}_E(-\mathbf{m}) \cdot \widehat{1}_j(\mathbf{m})\,.$$

Bounding $\mathcal{E}$ then reduces to bounding each $\widehat{1}_j(\mathbf{m})$ uniformly in $\mathbf{m} \neq \mathbf{0}$.

2.1. **Statement of main result from** [L]**.** The principal exponential sum estimate from [L] is as follows.

Theorem 1. (1) *If* $r - \nu \geq 4$ *then*

$$\nu_{\mathbf{m}} = \nu \quad \textit{implies} \quad \widehat{1}_j(\mathbf{m}) = \begin{cases} O\big(q^{-1} \cdot p^{-(r-\nu)\theta}\big) & \textit{if } r-\nu \textit{ is even} \\ O\big(q^{-1} \cdot p^{-(r-\nu-1)\theta}\big) & \textit{if } r-\nu \textit{ is odd.} \end{cases}$$

(2) *If* $1 \leq r - \nu \leq 3$ *then*

$$\nu_{\mathbf{m}} = \nu \quad \textit{implies} \quad \widehat{1}_j(\mathbf{m}) = O\big(q^{-1} \cdot p^{-(r-\nu)\theta}\big)\,,$$

where the implied constant is uniform in p, $j \in U_q$, $r \geq 2$, *and* $\mathbf{m} \neq \mathbf{0}$.

We then use the fact that there exists A (uniform over r) so that

$$\widehat{1}_j(\mathbf{0}) = q^{-1} \cdot (1 + o(1)) \quad \textit{where } \tfrac{1}{2} \leq 1 + o(1) \leq 2 \quad \textit{if } p \geq A. \tag{4}$$

It is then easy to use Theorem 1 and Plancherel's formula to show that there exist B, *uniform in* $r \geq 2$, j, n, such that $p \geq A$ implies

$$\mathcal{M} = \frac{|E|^2}{q} \cdot (1 + o(1)) \quad \text{and} \quad |\mathcal{E}| \leq B \cdot q^{n-1} \cdot p^{-\theta} \cdot |E|\,. \tag{5}$$

We conclude:

$$\frac{|\mathcal{E}|}{\mathcal{M}} \leq \frac{B \cdot q^{n-1} \cdot p^{-\theta} \cdot |E|}{\frac{|E|^2}{q} \cdot (1 + o(1))} < \frac{2\,B\,p^{-\theta}}{\delta_E} < 1 \quad \textit{implies} \quad \lambda_j^{(2)}(E) = \frac{|E|^2}{q} \cdot (1 + o(1)) > 0\,.$$

Thus,

$$(i) \quad p > \max\{A, (2\,B)^{1/\theta}\} \ \textit{implies} \ 2\,B\,p^{-\theta} < 1\,;$$

$$(ii) \quad \delta_E > (2\,B)\,p^{-\theta} \ \textit{implies} \ \lambda_j^{(2)}(E) = \frac{|E|^2}{q} \cdot (1 + o(1))\,.$$

A shorter way of stating the implications (i), (ii) is to write

$$\delta_E \gg_n p^{-\theta} \textit{ and } p \gg_n 1 \quad \textit{implies} \quad \lambda_j^{(2)}(E) = \frac{|E|^2}{q} \cdot (1 + o(1))\,, \tag{6}$$

where it is understood that the implied constant multiplied by $p^{-\theta}$ is also *strictly smaller* than 1. By (i), this can be arranged by choosing p larger than a constant that depends only upon n.

The essential property here is that the rightmost quantity in (6) is positive because the "main term" $\mathcal{M}$ dominates the "error term" $\mathcal{E}$ when $\delta_E \gg p^{-\theta}$ *uniformly in* $j \in U_q$, $r \geq 2$, *and all sufficiently large* p.

2.2. **Overview of proof of Theorem 1.** There are four parts in the proof. Each one admits a suitable analogue when *det* replaces $\|\cdot\|$ and $\mathcal{M}_2(\mathbb{Z}_q)$ replaces $\mathbb{Z}_q^n$. In Remarks 1 - 3 we have also highlighted the particular issues that are needed to extend our result to determinants of $n \times n$ matrices where $n \geq 3$.

Throughout we use the following:

Notations for p-adic integers.

1. $\mathcal{Z}_p$ = *ring of p-adic integers* and $\mathcal{U}_p$ = *units of* $\mathcal{Z}_p$.
2. $|y|_p = p^{-ord_p y} \ \ (y \in \mathcal{Z}_p)$.
3. $a = b\,(p^c)$ means $p^c \mid a - b$.
4. Each coset of a point $(\mathbf{w}, v) \in \mathcal{Z}_p^{n+1}$ of radius p^{-1} is denoted by $[\mathbf{w}]_1 \times [v]_1$, where
$[v]_1 := \{t \in \mathcal{Z}_p : t = v\,(p)\}$ and $[\mathbf{w}]_1 = \prod_\ell [w_\ell]_1$ when $\mathbf{w} = (w_1, \ldots, w_n)$.
5. The ideal generated by p in $\mathcal{Z}_p$ is denoted (p) and $(p)^{(k)} = (p) \times \cdots \times (p)$ $(k\text{-}fold)$.

□

2.2.1. *A local identification of $\{P = j\}$ (see (2)) as a submanifold of dimension $n-1$.* Given that $j \in \mathcal{U}_p$ and $p > 2$, a standard Hensel Lemma argument that lifts solutions mod p to $\mathcal{Z}_p$, combined with the Implicit Function Theorem and compactness of the set

$$\mathcal{G} := \bigcup_{j \in \mathcal{U}_p} \{(\mathbf{x}, j) : \mathbf{x} \in \mathcal{Z}_p \ \text{ and } \ P(\mathbf{x}) = j\} = \textit{Graph of } P\big|_{\mathcal{Z}_p^n \cap P^{-1}(\mathcal{U}_p)} .$$

implies the following.

Lemma 1. *There exists a finite set $\mathcal{B} = \{\mathbf{b} = (b_1, b_2)\}$ with $|\mathcal{B}| = O(p^n)$ satisfying these properties:*

1. *For each $\mathbf{b} = (b_1, b_2) \in \mathcal{B}$ there exist $\mathbf{x}_{b_1} = (\mathbf{x}'_{b_1}, x_{n,b_1}) \in \mathcal{Z}_p^n \setminus (p)^{(n)}$ and $j_{b_2} \in \mathcal{U}_p$ such that*
$$P(\mathbf{x}_{b_1}) = j_{b_2} \quad \textit{and} \quad \mathcal{G} = \bigsqcup_{\mathbf{b} \in \mathcal{B}} \Big(([\mathbf{x}_{b_1}]_1 \times [j_{b_2}]_1) \cap \mathcal{G} \Big) ;$$
After a suitable permutation of indices, we may also assume that $P_{x_n}(\mathbf{x}_{b_1}) \in \mathcal{U}_p$.
2. *For each b_2 the "slice"*
$$\mathcal{B}_{b_2} := \{b_1 : (b_1, b_2) \in \mathcal{B}\}$$
has cardinality $\qquad B_{b_2} := |\mathcal{B}_{b_2}| = O(p^{n-1})$.
3. *In the indexing from (1), for each $\mathbf{b}$ there exist p-adic coordinates $(\mathbf{x}', j')$ centered at $[\mathbf{x}'_{b_1}]_1 \times [j_{b_2}]_1$, and a p-adic analytic function $\varphi_{\mathbf{b}} : [\mathbf{x}'_{b_1}]_1 \times [j_{b_2}]_1 \to [x_{n,b_1}]_1$ such that*
$$[\mathbf{x}_{b_1}]_1 \times [j_{b_2}]_1 \cap \{P = j_{b_2} + j'\} = (\mathbf{x}_{b_1}, j_{b_2}) + \{(\mathbf{x}', x_n, j') : x_n = \Delta\varphi_{\mathbf{b}}(\mathbf{x}', j')\}$$
where
$$\Delta\varphi_{\mathbf{b}}(\mathbf{x}', j') := \varphi_{\mathbf{b}}(\mathbf{x}'_{b_1} + \mathbf{x}', j_{b_2} + j') - \varphi_{\mathbf{b}}(\mathbf{x}'_{b_1}, j_{b_2}) = \varphi_{\mathbf{b}}(\mathbf{x}'_{b_1} + \mathbf{x}', j_{b_2} + j') - x_{n,b_1} .$$

Remarks.

1) In other words, $P(\mathbf{x}'_{b_1}+\mathbf{x}',\varphi_{\mathbf{b}}(\mathbf{x}'_{b_1}+\mathbf{x}',j_{b_2}+j'))=j_{b_2}+j'$, and for each $j'\in(p)$:

$$\mathbf{x}_{b_1}+(\mathbf{x}',\Delta\varphi_{\mathbf{b}}(\mathbf{x}',j'))\in[\mathbf{x}_{b_1}]_1\cap\{P=j_{b_2}+j'\}.$$

2) Introducing the components

$$\mathbf{x}_{b_1}:=(\xi_1,\dots,\xi_n), \tag{7}$$

the function $\Delta\varphi_{\mathbf{b}}(\mathbf{x}',j')$ can be written more explicitly by introducing the p-adic inverse of the map

$$H: x_n\in(p)\longrightarrow y_n:=x_n(2\xi_n+x_n)\in(p)\,.$$

Since $|H'|_p=1$ on (p) its p-adic inverse $h(y_n)$ can be written out as a convergent power series

$$x_n=h(y_n)=c_1y_n+\sum_k c_ky_n^k \qquad (c_1=(2\xi_n)^{-1},\ c_2=-(2\xi_n)^{-3},\dots)\,. \tag{8}$$

Indeed, the series converges on (p) since $p>2$ and $\xi_n\in\mathcal{U}_p$ implies $c_k\in\mathcal{U}_p$ for all $k\geq 2$. It follows that

$$x_n=h\Big(\big[j'-\sum_{i=1}^{n-1}(x_i^2+2\xi_ix_i)\big]\Big)=\Delta\varphi_{\mathbf{b}}(\mathbf{x}',j'). \tag{9}$$

Thus,

$$(\mathbf{x}+\mathbf{x}_{b_1},j'+j_{b_2})\in graph\,(P)\cap\big([\mathbf{x}_{b_1}]_1\times[j_{b_2}]_1\big)\ \ iff\ \ x_n=\Delta\varphi_{\mathbf{b}}(\mathbf{x}',j')\,.\quad\square$$

2.2.2. *Expressing each $\widehat{1}_j(\mathbf{m})$ in terms of the Fourier transform of $\Delta\varphi_{\mathbf{b}}(\mathbf{x}',j')$.* On the nonsingular fiber $\{P=j\}$, which we use as simplifying notation for $\{P=j\}\cap\mathcal{Z}_p^n$, a measure determined by a global residue differential form exists. This is used to define a fiber integral and its Fourier transform, in terms of which $\widehat{1}_j(\mathbf{m})$ can be expressed in terms of an oscillating integral on $\mathcal{Z}_p^{n-1}$.

Notation: ω_j denotes the global $n-1$ form which, on the subset $\{P_{x_i}\neq 0\}\cap\{P=j\}$, is represented by

$$(-1)^{i-1}dx_1\cdots\widehat{dx_i}\cdots dx_n/P_{x_i}\Big|_{\{P_{x_i}\neq 0\}\cap\{P=j\}}.$$

This form induces a global measure on $\{P=j\}$, denoted as $|\omega_j|$, such that on the same open subset of $\{P=j\}$ its density equals

$$|dx_1\cdots\widehat{dx_i}\cdots dx_n|/|P_{x_i}|$$

where $|dx_1\cdots\widehat{dx_i}\cdots dx_n|$ denotes normalized Haar measure on $\mathcal{Z}_p^{n-1}$, and the denominator denotes the p-adic norm of P_{x_i}. □

Using this, the Fourier transform of the fiber integral is defined for each $j \in \mathcal{U}_p$, and $\mathbf{m} \in \mathbb{Z}_q^n$ by setting

$$\mathcal{F}_q(j, \mathbf{m}) := \int_{\{P=j\}} \Psi_q(\langle \mathbf{x}, \mathbf{m} \rangle) \, |\omega_j|, \tag{10}$$

Applying Lemma 1, this oscillatory integral is represented as an exponential sum mod q.

Using the notation in Part 1 of Lemma 1, we first define

$$\mathcal{B}(j) = \{\underline{=}(b_1, b_2) \in \mathcal{B} : j_{b_2} = j\,(p)\}. \tag{11}$$

The set of elements $\{(\mathbf{x}_{b_1}, j_{b_2})\}_{(b_1,b_2) \in \mathcal{B}(j)}$ determine *pairwise disjoint* cosets $[\mathbf{x}_{b_1}]_1 \times [j_{b_2}]_1$ over which $\mathcal{F}_q(j, \mathbf{m})$ becomes a sum of local contributions defined for any $\mathbf{b} \in \mathcal{B}(j)$:

$$\mathcal{F}_{q,\mathbf{b}}(j, \mathbf{m}) = \int_{\{P=j\} \cap [\mathbf{x}_{b_1}]_1} \Psi_q(\langle \mathbf{x}, \mathbf{m} \rangle) \, |\omega_j| \,, \tag{12}$$

Each local contribution can now be expressed as a finite exponential sum.

Recalling (7), the fact that $j_{b_2} \in \mathcal{U}_p$ implies there exists i such that $\xi_i \in \mathcal{U}_p$. Thus, for any $\boldsymbol{x} \in [\mathbf{x}_{b_1}]_1 \cap \{P = j\}$

$$P_{x_i}(\boldsymbol{x}) \in \mathcal{U}_p. \tag{13}$$

For each $\mathbf{b} \in \mathcal{B}(j)$ it follows that there exists a disjoint open cover $\mathcal{O}_{\mathbf{b}}(j) = \bigsqcup_{e \in \mathcal{E}_{\mathbf{b}}(j)} [\boldsymbol{x}_e]_r$ of $[\mathbf{x}_{b_1}]_1 \cap \{P = j\}$ such that

$$\textit{for each } e \quad |P_{x_i}|_{[\boldsymbol{x}_e]_r}|_p = 1.$$

Since $\mathbf{x} \to \Psi_q(\langle \mathbf{x}, \mathbf{m} \rangle)$ is constant on each $[\boldsymbol{x}_e]_r$ ($e \in \mathcal{E}_{\mathbf{b}}(j)$), it follows that

$$\begin{aligned} \mathcal{F}_{q,\mathbf{b}}(j, \mathbf{m}) &= q^{-(n-1)} \sum_{e \in \mathcal{E}_{\mathbf{b}}(j)} \Psi_q(\langle \boldsymbol{x}_e, \mathbf{m} \rangle) \\ \text{and} \qquad \mathcal{F}_q(j, \mathbf{m}) &= \sum_{\mathbf{b} \in \mathcal{B}(j)} \mathcal{F}_{q,\mathbf{b}}(j, \mathbf{m}) \end{aligned} \tag{14}$$

The following can now be proved (see [L], §3.2).

Lemma 2. *$p \neq 2$ implies for each $r \geq 2$, $j' \in (p) \setminus (p^r)$, and b_2*

$$\widehat{1}_{j_{b_2}+j'}(\mathbf{m}) = q^{-1} \cdot \sum_{\substack{\{\mathbf{b} \in \mathcal{B}(j) : \mathbf{b} = (b_1, b_2) \\ j = j_{b_2} + j' \text{ } mod\, q\}}} \mathcal{F}_{q,\mathbf{b}}(j_{b_2} + j', \mathbf{m}). \tag{15}$$

We now apply Lemma 1 to express each local contribution $\mathcal{F}_{q,\mathbf{b}}(j_{b_2} + j', \mathbf{m})$ as an oscillating integral in $n - 1$ variables.

After a possible permutation we may assume the index in (13) is $i = n$. Thus, for each $j' \in (p) \setminus (p^r)$:

$$|\omega_{j_{b_2}+j'}|\big|_{[\mathbf{x}_{b_1}]_1} = |d\mathbf{x}'|\big|_{[\mathbf{x}_{b_1}]_1 \cap \{P = j_{b_2}+j'\}} \qquad (\mathbf{x}' = (x_1, \ldots, x_{n-1}))\,.$$

It follows that (see (9))

$$\begin{aligned}\mathcal{F}_{q,\mathbf{b}}(j_{b_2}+j',\mathbf{m}) &= \Psi_q(\langle \mathbf{x}_{b_1},\mathbf{m}\rangle)\cdot\int_{(p)^{n-1}}\Psi_q\Big(\Delta\varphi_{\mathbf{b}}(\mathbf{x}',j')\cdot m_n+\langle \mathbf{x}',\mathbf{m}'\rangle\Big)|d\mathbf{x}'| \\ &:= \Psi_q(\langle \mathbf{x}_{b_1},\mathbf{m}\rangle)\cdot\int_{(p)^{n-1}}\Psi_q\big(f_{\mathbf{b}}(\mathbf{x}',j',\mathbf{m})\big)|d\mathbf{x}'|\,. \end{aligned}\tag{16}$$

Moreover, since j_{b_2} is fixed when $\mathbf{b}$ is fixed, we introduce a more concise notation by denoting the slice $\mathcal{B}_{b_2}(j_{b_2}+j')$ and left side of (16) as $\mathcal{B}_{b_2}(j')$ and $\mathcal{F}_{q,\mathbf{b}}(j',\mathbf{m})$.

With this notational convention, we now know that for all $j'\in(p)\setminus(p^r)$

$$\begin{aligned}\widehat{1}_{j_{b_2}+j'}(\mathbf{m}) &= q^{-1}\cdot\sum_{\substack{\mathbf{b}=(b_1,b_2)\in\mathcal{B}\\ b_1\in\mathcal{B}_{b_2}(j')}}\Psi_q(\langle \mathbf{x}_{b_1},\mathbf{m}\rangle)\cdot\int_{(p)^{n-1}}\Psi_q\big(f_{\mathbf{b}}(\mathbf{x}',j',\mathbf{m})\big)|d\mathbf{x}'| \\ &:= q^{-1}\cdot\sum_{\substack{\mathbf{b}=(b_1,b_2)\in\mathcal{B}\\ b_1\in\mathcal{B}_{b_2}(j')}}\mathcal{F}_{q,\mathbf{b}}(j',\mathbf{m})\,.\end{aligned}\tag{17}$$

2.2.3. *Overview of proof of Theorem 1 Part 1.* We first must specify those $\mathbf{m}$ with fixed p-adic order ν by setting

$$\begin{aligned}\mathcal{L}_q(\nu) &= \{\mathbf{m}\neq\mathbf{0}\in\mathbb{Z}_q^n : min_\ell\{\,ord_p\, m_\ell\}=\nu\}; \\ \mathcal{L}_q &= \bigcup_{\nu=0}^{r-1}\mathcal{L}_q(\nu)\,.\end{aligned}$$

A nontrivial estimate for any $\mathcal{F}_{q,\mathbf{b}}(j',\mathbf{m})$ that depends only upon that value of ν for which $\mathbf{m}\in\mathcal{L}_q(\nu)$. was proved in [L] §3.3-3.4. The estimate is weaker for larger ν. This reflects the fact that the number of oscillating terms within the exponential sum shrinks by a factor of $p^{\nu n}$.

Lemma 3. *1) For each $\mathbf{b}\in\mathcal{B}$ and $0\le\nu\le r-4$*

$$\mathcal{F}_{q,\mathbf{b}}\big|_{\mathcal{L}_q(\nu)}(j',\mathbf{m})=\begin{cases}O\big(p^{-\frac{(r-\nu)(n-1)}{2}}\big) & r-\nu \text{ even,}\\[2ex] O\big(p^{-\frac{(r-\nu-1)(n-1)}{2}}\big) & r-\nu \text{ odd}\end{cases}\tag{18}$$

where the implied constant is uniform in ,$j'\in(p)$, and $\mathbf{m}\in\mathcal{L}_q(\nu)$.

2)

$$\sum_{\mathbf{b}\in\mathcal{B}_{b_2}(j')}\mathcal{F}_{q,\mathbf{b}}(j',\mathbf{m})=O(p^{-(n-1)}) \text{ uniformly in } b_2, j'\in(p), \text{and } \ \mathbf{m}\in\textstyle\bigcup_{0\le\nu\le r-4}\ \mathcal{L}_q(\nu).\tag{19}$$

Since any $j\in U_q$ equals $j_{b_2}+j'$ $mod\, q$ for some b_2 and $j'\in(p)$, the following is now immediate.

Corollary 1.

$$\widehat{1}_j(\mathbf{m}) = O(q^{-1}\cdot p^{-(n-1)}) \quad \textit{uniformly in } j\in U_q \textit{ and } \mathbf{m}\in \textstyle\bigcup_{0\le\nu\le r-4}\ \mathcal{L}_q(\nu). \tag{20}$$

Remarks:

1) Implicit in Part 2 of the Lemma is the fact that when $\nu \le r-4$ it suffices to use the trivial estimate for $|\mathcal{B}_{b_2}(j')|$ to prove (2). However, when $r-3\le \nu \le r-1$, this is too coarse an estimate and a different argument, given in §2.2.4, is needed.

2) When $1\le \nu\le r-4$, the argument is easily seen to follow from the verification of (18) when $\nu = 0$. □

Proof of Part 1 of Lemma 3 ($\nu = 0$). The argument is a natural variant of that worked out in [L2]. There are two goals. The first is to find subcosets of $[\mathbf{x}_{b_1}]_1$ over which the oscillating integral in the Lemma *vanishes*. The second is to use a stationary phase type argument on those cosets over which the oscillating integral need not vanish.

To do this, we need to understand the rank of the Hessian of the phase function $f_{\mathbf{b}}(\mathbf{x}', j', \mathbf{m})$ mod p (see (16)).

Recall that $\mathbf{x}' = (x_1,\ldots,x_{n-1})\in (p)^{(n-1)}$ as in the proof of Lemma 1. Writing

$$\mathbf{x}' = p\mathbf{x}'_1 + p^2\mathbf{x}'_2 + p^3\mathbf{x}'_3 + \cdots \qquad \text{and} \qquad \mathbf{m} = (\mathbf{m}', m_n)\,,$$

where each $\mathbf{x}'_u\in\{0,\ldots,p-1\}^{n-1}$, we apply Taylor's formula (in $\mathbf{x}'$) for each fixed j' (where $\mathbf{0}'$ denotes $\mathbf{x}'_{b_1}$ in the $\mathbf{x}'$ coordinates and 't' refers to transpose). This gives:

$$\begin{aligned} f_{\mathbf{b}}(\mathbf{x}', j', \mathbf{m}) &= f_{\mathbf{b}}(\mathbf{0}', j') + \big\langle \nabla f_{\mathbf{b}}(\mathbf{0}', j'), \sum_{i\ge 1} p^i \mathbf{x}'_i\big\rangle + \ldots \\ &= m_n\cdot\Delta\varphi_{\mathbf{b}}(\mathbf{0}', j') + p\cdot \big\langle m_n\cdot\nabla\Delta\varphi_{\mathbf{b}}(\mathbf{0}', j') + \mathbf{m}', \mathbf{x}'_1\big\rangle \qquad (21)\\ &\quad + p^2\Big[(\mathbf{x}'_1)\,\mathcal{H}_{\mathbf{b}}(\mathbf{0}', j', \mathbf{m})\,(\mathbf{x}'_1)^t + \big\langle m_n\cdot\nabla\Delta\varphi_{\mathbf{b}}(\mathbf{0}', j') + \mathbf{m}', \mathbf{x}'_2\big\rangle\Big] + \cdots \end{aligned}$$

where

$$\mathcal{H}_{\mathbf{b}}(\mathbf{0}', j', \mathbf{m}) := m_n\cdot\left(\frac{\partial^2\Delta\varphi_{\mathbf{b}}}{\partial x_j\partial x_k}(\mathbf{0}', j')\right)_{1\le j,k\le n-1}.$$

Since $\nu = 0$ it suffices to restrict attention to those $\mathbf{m}$ such that $|m_n|_p = 1$ since

$$|m_n|_p < 1 \ \textit{ implies } \ \mathbf{m}'\ne\mathbf{0}'\,(p) \ \text{ and } \ f_{\mathbf{b}}(\mathbf{x}', j', \mathbf{m}) = \langle\mathbf{m}', \mathbf{x}'\rangle\,(p^2).$$

A straightforward application of the implicit function theorem that uses (7) and (9) now shows :

$$\mathcal{H}_{\mathbf{b}}(\mathbf{0}', \mathbf{j}', \mathbf{m}) = \frac{-m_n}{\varphi_{\mathbf{b}}(\mathbf{x}'_{b_1}, j')^3}\cdot\Big(\varphi_{\mathbf{b}}(\mathbf{x}'_{b_1}, j')^2 Id_{n-1} + \left(\xi_j\xi_k\right)_{1\le j,k\le n-1}\Big)\,. \tag{22}$$

Applying the "matrix-determinant lemma" we conclude that

$$|j_{b_2} + j'|_p = |m_n|_p = 1 \ \textit{ implies } \ \ |det\mathcal{H}_{\mathbf{b}}(\mathbf{0}', \mathbf{j}', \mathbf{m})|_p = 1\,.$$

Thus,

$$ord_p\, det(\mathcal{H}_{\mathbf{b}}(\mathbf{0}', \mathbf{j}', \mathbf{m}) = 0 \quad \text{and} \quad \text{rank}\,\big(\mathcal{H}_{\mathbf{b}}(\mathbf{0}', \mathbf{j}', \mathbf{m})\, mod\, p\big) = n-1\,. \tag{23}$$

We next define the integer

$$\ell_0 = \begin{cases} \frac{r}{2} & \text{if } r \text{ is even} \\ \\ \frac{r-1}{2} & \text{if } r \text{ is odd.} \end{cases} \tag{24}$$

It follows from the argument presented in [L] §3.3 that ℓ_0 represents the *smallest* integer ℓ over which we cannot do any better, in general, than estimate the oscillating integral over any coset $[\mathbf{y}]_\ell$ (mod p^ℓ) by the trivial bound which equals the Haar measure of the coset:

$$\int_{[\mathbf{y}]_\ell} \Psi_q(f_{\mathbf{b}}(\mathbf{x}', \mathbf{j}', \mathbf{m})|d\mathbf{x}'| = O(p^{-\ell(n-1)})\,.$$

On the other hand, outside the union of cosets mod p^{ℓ_0} it *is* possible to find subsets over which the oscillating integral *vanishes*. These are the cosets mod p^u for some $u < \ell_0$ of *nonsingular points* of the phase function.

What we must then estimate for each $u < \ell_0$ is how many cosets mod p^u there are of singular points mod p^u of $\mathbf{x}' \to f_{\mathbf{b}}(\mathbf{x}', \mathbf{j}', \mathbf{m})$ that also contain a singular point mod p^{u+1}. The number of chains of such points

$$\mathbf{x}_0 := \mathbf{x}_{b_1} \; mod\, p \to \mathbf{x}_1 = \mathbf{x}_0 + p\mathbf{z}_1 \; mod\, p^2 \to \cdots \to \mathbf{x}_{\ell_0 - 1} = \mathbf{x}_{\ell_0-2} + p^{\ell_0-1}\mathbf{z}_{\ell_0-1} \; mod\, p^{\ell_0}$$

then serves as our bound for the contribution to the oscillatory integral $\mathcal{F}_{q,\mathbf{b}}\big|_{\mathcal{L}_q(0)}(\mathbf{j}', \mathbf{m})$ over $[\mathbf{x}_{b_1}]_1$ (see (12)). *This depends entirely upon the corank $\kappa_{\mathbf{b}}(\mathbf{m})$ of the Hessian $\mathcal{H}_{\mathbf{b}}(\mathbf{0}', \mathbf{j}', \mathbf{m})$ mod p. When $\kappa_{\mathbf{b}}(\mathbf{m}) = 0$*, as is the case here because of the expression for P,

$$\begin{aligned} \mathcal{F}_{q,\mathbf{b}}\big|_{\mathcal{L}_q(0)}(j', \mathbf{m}) &= O\big(p^{-\ell_0(n-1)}\big) \\ &= \begin{cases} O\big(p^{-\frac{r(n-1)}{2}}\big) & r \; even \\ \\ O\big(p^{-\frac{(r-1)(n-1)}{2}}\big) & r \; odd\,. \end{cases} \end{aligned} \tag{25}$$

It is then not difficult to show that when $\mathbf{m} \in \mathcal{L}_q(\nu),\; 1 \le \nu \le r-4$, it is necessary to replace r by $r - \nu$. This ends the proof of Part 1.

Remark 1. It is therefore important to know how larger values of the corank will modify the bound in (25). Using [L2], Prop. 2.8 (in which n should change to $n-1$ in order to apply to our situation), this is given as follows:

$$\mathcal{F}_{q,\mathbf{b}}\big|_{\mathcal{L}_q(0)}(j', \mathbf{m}) = O\big(p^{-\frac{r(n-1-\kappa_{\mathbf{b}}(\mathbf{m}))}{2} - \kappa_{\mathbf{b}}(\mathbf{m})}\big) \quad uniformly\ in\ \mathbf{m}\,. \tag{26}$$

Proof of Part 2. By Part 1, we see immediately that

$$\mathcal{F}_{q,\mathbf{b}}(j', \mathbf{m}) = O(p^{-2(n-1)}) \quad uniformly\ in\ b_2,\ j',\ and\ \ \mathbf{m} \in \textstyle\bigcup_{0 \le \nu \le r-4} \mathcal{L}_q(\nu).$$

Since

$$|\mathcal{B}_{b_2}(j')| := \big|\mathcal{B}_{b_2}(j_{b_2} + j')\big| = O(p^{n-1}) \quad (uniformly\ in\ b_2, j').$$

it follows that by *trivially estimating* the sum over $\{\mathbf{b} : b_1 \in \mathcal{B}_{b_2}(j')\}$, we conclude

$$\sum_{\{\mathbf{b}:b_1\in\mathcal{B}_{b_2}(j')\}} \mathcal{F}_{q,\mathbf{b}}\Big|_{\bigcup_{0\le\nu\le r-4}\mathcal{L}_q(\nu)}(j',\mathbf{m}) = O(p^{-(n-1)}) \quad \textit{uniformly in } b_2, j', \mathbf{m}. \quad \square$$

Proof of Corollary 1. The assertion follows immediately from (17).

2.2.4. *Uniform estimate of the* $\mathcal{F}_{q,\mathbf{b}}(j',\mathbf{m})$ *(*$r-3 \le \nu \le r-1$*).* In addition to the notations introduced in §2.2.3, it will be convenient to define

$$\widehat{\mathbf{m}} := p^{-\nu}\mathbf{m} = (\widehat{\mathbf{m}}', \widehat{m}_n) \quad \textit{for any } \mathbf{m} \in \mathcal{L}_q(\nu).$$

The three possibilities for ν are analyzed separately.
(I) $\nu = r-1$.

Lemma 4. *If* $n \ge 2$ *and* $\nu = r-1$ *then:*

$$\sum_{\{\mathbf{b}:b_1\in\mathcal{B}_{b_2}(j')\}} \mathcal{F}_{q,\mathbf{b}}|_{\mathcal{L}_q(r-1)}(j',\mathbf{m}) = O(p^{-\frac{n-1}{2}}) \qquad \textit{uniformly in } b_2,\ j' \in (p), \textit{ and } \mathbf{m};$$

$$\widehat{1}_j(\mathbf{m}) = O(q^{-1}\cdot p^{-\frac{n-1}{2}}) \quad \textit{uniformly in } j \in U_p \textit{ and } \mathbf{m}.$$

Proof. Since $p^{\nu-r} = p^{-1}$ and $\mathbf{x}' \in (p)^{(n-1)}$ it follows that $p \mid f_{\mathbf{b}}(\mathbf{x}', j', \mathbf{m})$ and the integrand for $\mathcal{F}_{q,\mathbf{b}}(j',\mathbf{m})$ equals 1. Thus, for each b_2, (16) implies:

$$\sum_{\{\mathbf{b}:b_1\in\mathcal{B}_{b_2}(j')\}} \mathcal{F}_{q,\mathbf{b}}(j',\mathbf{m}) = p^{-(n-1)} \sum_{\{\mathbf{x}_{b_1}:\overline{P}(\mathbf{x}_{b_1})=\bar{j}_{b_2}\}} \Psi_p(\langle \mathbf{x}_{b_1}, \widehat{\mathbf{m}}\rangle). \tag{27}$$

where the sum on the right equals an exponential sum taken over the $\mathbb{F}_p$ rational points of the hypersurface $\{\overline{P} = \bar{j}_{b_2}\}$.

A fundamental observation from [CIP] (see proof of Lemma 2.0.9 and §2 of [IR]) uses bounds for Gaussian sums, a method of Salié [S] to bound Kloosterman sums (in one variable), and the fact that $\bar{j}_{b_2} \ne 0$ to show that the right side of (27) is bounded as follows:

$$p^{-(n-1)} \sum_{\{\mathbf{x}_{b_1}:\overline{P}(\mathbf{x}_{b_1})=\bar{j}_{b_2}\}} \Psi_p(\langle \mathbf{x}_{b_1}, \widehat{\mathbf{m}}\rangle) = O(p^{-(n-1)}\cdot p^{\frac{n}{2}-\frac{1}{2}}) = O(p^{-\frac{n-1}{2}}), \tag{28}$$

where the implied constant is *uniform* in $p > 2$, $\mathbf{m}$ and $\mathbf{b}$. □

Remark 2. This exponential sum can also be bounded via a very general method due to Katz [K]. This estimates exponential sums mod p over affine varieties in $\mathbb{F}_p^n$ whose projective closure has a singular intersection with the hypersurface defined by the phase function at infinity.

To apply this bound to our problem, we note that its context is an open subset of the projective quadric $\mathcal{X}_{\bar{j}_{b_2}} = \{\|\mathbf{X}\|^2 - \bar{j}_{b_2}X_0^2 = 0\}$ (of (projective) dimension $n-1$ in

$\mathbf{P}^n(\mathbb{F}_p)$), obtained by deleting the hyperplane $L = \{X_0 = 0\}$ at infinity. Defining the function $H_{\widehat{\mathbf{m}}}(X_0, \mathbf{X}) = \langle (0, \widehat{\mathbf{m}}), (X_0, \mathbf{X}) \rangle$, it follows that

$$\sum_{(X_0,\mathbf{X}) \in \mathcal{X}_{\bar{j}_{b_2}} - \mathcal{X}_{\bar{j}_{b_2}} \cap L} \Psi_p\big(H_{\widehat{\mathbf{m}}}(X_0, \mathbf{X})\big) = \sum_{\{\mathbf{x}_{b_1} : \overline{P}(\mathbf{x}_{b_1}) = \bar{j}_{b_2}\}} \Psi_p\big(\langle \mathbf{x}_{b_1}, \widehat{\mathbf{m}} \rangle\big) = O(p^{\frac{n}{2}})\,. \tag{29}$$

The exponent of p in the estimate (29) is, in Katz' notation, $\frac{n+\delta}{2}$, where δ equals the projective dimension of the singular locus (“at infinity") of $\mathcal{X}_{\bar{j}_{b_2}} \cap L \cap \{H_{\widehat{\mathbf{m}}} = 0\}$. This can be at most 0 since if it is nonempty, which can occur, then it consists of a single (affine) line inside the hyperplane L at infinity in the direction $(0, \widehat{\mathbf{m}})$, given that $p > 2$. The implied constant is also uniform in $p > 2$. □

(II) $\nu = r - 2$.

Lemma 5.

$$\sum_{\{\mathbf{b} : b_1 \in \mathcal{B}_{b_2}(j')\}} \mathcal{F}_{q,\mathbf{b}}\big|_{\mathcal{L}_q(r-2)}(j', \mathbf{m}) = O(p^{-(n-1)}) \qquad \textit{uniformly in } b_2, j' \in (p), \textit{ and } \mathbf{m};$$

$$\widehat{1}_j(\mathbf{m}) = O(q^{-1} \cdot p^{-(n-1)}) \quad \textit{uniformly in } j \in U_q \textit{ and } \mathbf{m}.$$

Proof. Using (9), we note that the phase function for $\mathcal{F}_{q,\mathbf{b}}(j', \mathbf{m})$ equals

$$\widehat{m}_n \cdot [j' - \langle 2\,\mathbf{x}'_{b_1}, \mathbf{x}' \rangle] + \langle \widehat{\mathbf{m}}', \mathbf{x}' \rangle \; mod\; p^2.$$

Since $\mathbf{x}' \in (p)^{(n-1)}$, *only one (of two) possibilities* can at all contribute to the sum of $\mathcal{F}_{q,\mathbf{b}}(j', \mathbf{m})$. This occurs if

$$\widehat{\mathbf{m}}' - 2\,\widehat{m}_n\,\mathbf{x}'_{b_1} = 0\,(p). \tag{30}$$

If this property fails to hold then the phase function for each $\mathcal{F}_{q,\mathbf{b}}(j', \mathbf{m})$ is a *nonzero linear function mod* p^2, in which case $\mathcal{F}_{q,\mathbf{b}}(j', \mathbf{m}) = 0$.

Defining

$$\mathcal{A}^*(j', \mathbf{m}) = \sum_{\substack{\{\mathbf{b} : b_1 \in \mathcal{B}_{b_2}(j') \\ \widehat{\mathbf{m}}' - 2\,\widehat{m}_n\,\mathbf{x}'_{b_1} = 0\,(p)\}}} \mathcal{F}_{q,\mathbf{b}}(j', \mathbf{m}).$$

we then note that $\mathcal{F}_{q,\mathbf{b}}(j', \mathbf{m}) = p^{-(n-1)}$ since the integral equals the measure of $(p)^{(n-1)}$. Moreover, if $\widehat{m}_n \neq 0(p)$ then

$$\big|\{\mathbf{x}'_{b_1} : \mathbf{x}'_{b_1} = \frac{\widehat{\mathbf{m}}'}{2\,\widehat{m}_n}(p)\}\big| = O(1) \quad \textit{uniformly in } \mathbf{m} \quad \textit{implies} \quad \mathcal{A}^*(j', \mathbf{m}) = O(p^{-(n-1)}).$$

If, however, $\widehat{m}_n = 0(p)$ then the exponent of p in the denominator of the phase function equals $2 (= r - \nu)$ while the numerator is a non zero linear function of $\mathbf{x}'$. Thus, in this event $\mathcal{F}_{q,\mathbf{b}}(j', \mathbf{m}) = 0$.

Putting everything together finishes the proof of the Lemma. □

(III) $\nu = r - 3$.

Lemma 6.

$$\sum_{\{\mathbf{b}:b_1\in\mathcal{B}_{b_2}(j')\}} \mathcal{F}_{q,\mathbf{b}}\big|_{\mathcal{L}_q(r-3)}(j',\mathbf{m}) = O(p^{-\frac{3(n-1)}{2}}) \qquad \textit{uniformly in } b_2, j'\in(p), \textit{ and } \mathbf{m};$$

$$\widehat{1}_j(\mathbf{m}) = O(q^{-1}\cdot p^{-\frac{3(n-1)}{2}}) \quad \textit{uniformly in } j\in U_q \textit{ and } \mathbf{m}\in\mathcal{L}_q(\nu).$$

Proof: Since $r-\nu=3$, only the phase function modulo p^3 is pertinent. This is where we make use of (9), (16). Denoting the phase function $f_b(\mathbf{x}',j',\mathbf{m})$ *mod* p^3 by $\mathcal{Q}(=\mathcal{Q}_{\mathbf{b}}(\mathbf{x}',j',\widehat{m}))$ it follows that

$$\begin{aligned} \mathcal{Q} &:= \widehat{m}_n\cdot\{c_1\big[j'-\big(\|\mathbf{x}'\|^2+\langle 2\,\mathbf{x}'_{b_1},\mathbf{x}'\rangle\big)\big]+c_2\big[j'-\big(\|\mathbf{x}'\|^2+\langle 2\,\mathbf{x}'_{b_1},\mathbf{x}'\rangle\big)\big]^2\}+\langle\widehat{\mathbf{m}}',\mathbf{x}'\rangle \\ &= \big[\widehat{m}_n\cdot(c_1j'+c_2(j')^2)\big]+\big\langle\big(\widehat{\mathbf{m}}'-\widehat{m}_n\cdot[c_1+2c_2j']\cdot 2\,\mathbf{x}'_{b_1}\big),\mathbf{x}'\big\rangle+\widehat{m}_n\cdot\big(-c_1\|\mathbf{x}'\|^2+c_2\langle 2\,\mathbf{x}'_{b_1},\mathbf{x}'\rangle^2\big). \end{aligned} \tag{31}$$

Setting $\mathcal{Q}^*_{\mathbf{b}}(\mathbf{x}',j',\widehat{\mathbf{m}}) = \mathcal{Q}-\widehat{m}_n(c_1j'+c_2(j')^2)$, it is clear that $p\mid\mathcal{Q}^*_{\mathbf{b}}(\mathbf{x}',j',\widehat{\mathbf{m}})$ since $\mathbf{x}'\in(p)^{(n-1)}$.

Two possibilities exist for the linear in $\mathbf{x}'$ term:

(I) $\widehat{\mathbf{m}}'-\widehat{m}_n\cdot[c_1+2c_2j']\cdot 2\,\mathbf{x}'_{b_1}\neq 0\,(p)$;

(II) $\widehat{\mathbf{m}}'-\widehat{m}_n\cdot[c_1+2c_2j']\cdot 2\,\mathbf{x}'_{b_1}=0\,(p)$.

As above, only Case II poses an issue since the non zero linear term in Case I insures that $\int_{(p)^{(n-1)}}\Psi_{p^3}(\mathcal{Q}^*_{\mathbf{b}})|d\mathbf{x}'|=0$.

Case II implies $p^2\mid\mathcal{Q}^*_{\mathbf{b}}(\mathbf{x}',j',\widehat{\mathbf{m}})$ and $\widehat{m}_n\neq 0\,(p)$. So the oscillating integral reduces to an exponential sum mod p by breaking up $(p)^{(n-1)}$ into a disjoint union of cosets mod p^3:

$$\int_{(p)^{(n-1)}}\Psi_{p^3}(\mathcal{Q}^*_{\mathbf{b}})|d\mathbf{x}'| = p^{-3(n-1)}\cdot\mathcal{E}_{\mathbf{b}}(j',\widehat{\mathbf{m}}), \qquad \mathcal{E}_{\mathbf{b}}(j',\widehat{\mathbf{m}}) := \sum_{\boldsymbol{x}'\in\mathbb{F}_p^{n-1}}\Psi_p(\overline{\mathcal{Q}}^*_{\mathbf{b}}(\boldsymbol{x}',j',\widehat{\mathbf{m}}))\,.$$

Set $\widetilde{\mathcal{Q}}^*_{\mathbf{b}}(=\widetilde{\mathcal{Q}}^*_{\mathbf{b}}(\mathbf{x}')) := -c_1\|\mathbf{x}'\|^2+c_2\langle 2\,\mathbf{x}'_{b_1},\mathbf{x}'\rangle^2$ = degree 2 part of $\mathcal{Q}^*_{\mathbf{b}}(\mathbf{x}',j',\widehat{\mathbf{m}})$ *mod* p^3.

As in the proof of Part 1 in Lemma 3 we know that

$$\textit{corank } \widetilde{\mathcal{Q}}^*_{\mathbf{b}} \textit{ mod } p^3 = \textit{corank } \overline{\mathcal{Q}}^*_{\mathbf{b}} \textit{ mod } p = 0.$$

Thus, $\;\textit{det}\ \widetilde{\mathcal{Q}}^*_{\mathbf{b}}\neq 0\,(p)\quad(p\neq 2)$. By a theorem of Dabrowski-Fisher [DF] (also see Lemma 2.9 [L]) we conclude that

$$\mathcal{E}_{\mathbf{b}}(j',\widehat{\mathbf{m}}) = O(p^{\frac{n-1}{2}}) \quad \textit{uniformly in } \mathbf{b}\,.$$

As a result, $\nu=r-3$ implies we can also use the trivial bound $O(p^{n-1})$ for the sum over $\mathbf{b}$ with fixed b_2 to conclude

$$\sum_{\{\mathbf{b}:b_1\in\mathcal{B}_{b_2}(j')\}} \mathcal{F}_{q,\mathbf{b}}\big|_{\mathcal{L}_q(r-3)}(j',\mathbf{m}) = O(p^{-\frac{3(n-1)}{2}}) \qquad \textit{uniformly in } b_2, j', \mathbf{m}.$$

Combining Lemmas 4 - 6 with those from §2.2.3, finishes the proof of Theorem 1. □

Remark 3. The estimate from [DF] also includes the case when the quadratic term in $\mathcal{E}_{\mathbf{b}}$ has corank $\kappa_{\mathbf{b}}(\widehat{\mathbf{m}}) > 0 \pmod p$. In this event we recall (see [L2] Lemma 2.10) that the bound is as follows.

$$\mathcal{E}_{\mathbf{b}}(j', \widehat{\mathbf{m}}) = O\big(p^{\frac{n-1+\kappa_{\mathbf{b}}(\widehat{\mathbf{m}})}{2}}\big)\,. \tag{32}$$

3. Proof of Theorem A

Throughout this section , we will use the following notations:

$\mathcal{M}_2(\mathbb{Z}_q) = \{2 \times 2$ *matrices with entries in* $\mathbb{Z}_q\}$;
$\delta_E = |E|/q^4 \qquad$ *(when* $E \subset \mathcal{M}_2(\mathbb{Z}_q)$*)*;
$1_E(\mathbf{x}) =$ *characteristic function of* E;
$1_j(\mathbf{x}) =$ *characteristic function of* $\{\mathbf{x} \in \mathcal{M}_2(\mathbb{Z}_q) : det\, \mathbf{x} = j\}$ *(equality in* $\mathbb{Z}_q$*)*;
for any $\mathbf{x} = (x_1, \dots, x_4), \mathbf{m} = (m_1, \dots, m_4) \in \mathbb{Z}_q^4 \quad \langle \mathbf{x}, \mathbf{m}\rangle := \sum_i x_i m_i\,;$

$$\widehat{1}_j(\mathbf{m}) = q^{-4} \sum_{\mathbf{x} \in \mathcal{M}_2(\mathbb{Z}_q)} 1_\mu(\mathbf{x}) \chi\langle \mathbf{x}, -\mathbf{m}\rangle\,.$$

The goal is to understand, for each $j \in U_q$, the function

$$\tau_j^{(2)}(E) := \big|\{(\mathbf{x}, \mathbf{y}) \in E^2 :\ det(\mathbf{x} - \mathbf{y}) = j\}\big|.$$

In order to apply the discussion in §2 to solve the additive problem for the determinant's values over $\mathbb{Z}_q$ we should replace $P(\mathbf{x})$ ($\mathbf{x} \in \mathbb{Z}_q^n$) with the function

$$\mathbf{x} = (x_{1,1}, x_{1,2}, x_{2,1}, x_{2,2}) \in \mathbb{Z}_q^4 \longrightarrow det\,(\mathbf{x}) := det\big((x_{u,v})\big)\,.$$

However, to be able to prove the bound asserted in Theorem A, we need first to change the coordinates $\mathbf{x}$ of $\mathbb{Z}_q^4$ to work with an additive quadratic form. To that end we set

$$T : \mathbf{z} := (z_1, \dots, z_4) \longrightarrow \mathbf{x}$$

where

$$x_{1,1} := \frac{z_1 + z_2}{2}\,; \quad x_{2,1} := \frac{z_3 + z_4}{2}\,; \quad x_{1,2} := \frac{z_3 - z_4}{2}\,; \quad x_{2,2} := \frac{z_1 - z_2}{2}\,. \tag{33}$$

When $p > 2$ we interpret the right sides as the products with the inverse $2^{-1} \in U_q$.

It is then clear that up to the unit factor 4^{-1} we have that

$$Det(\mathbf{z}) := det \circ T(\mathbf{z}) = 4^{-1} \cdot \big[\big(z_1^2 - z_2^2\big) - \big(z_3^2 - z_4^2\big)\big] = 4^{-1} \cdot D(\mathbf{z})$$

is now an additive form to which Lemmas 1 - 4 immediately apply. Moreover, defining, for any $\eta \in U_q$ and subset $F \subset \mathbb{Z}_q^4$

$$\Theta_\eta^{(2)}(F) = \big|\{(\mathbf{z}, \mathbf{w}) \in F \times F \subset \mathbb{Z}_q^8 : D(\mathbf{z} - \mathbf{w}) = \eta\}\big| \tag{34}$$

and setting $j = 4^{-1}\eta$, the fact that T is a bijection between $F := T^{-1}E$ and E now implies that

$$\tau_j^{(2)}(E) = \Theta_\eta^{(2)}(F)\,.$$

Applying Theorem 1 to the right side is possible because D is an additive form in $\mathbf{z}$, which insures that the estimate from Lemma 4 can be used. In particular, the reader can check the fact that the proof of Lemma 2.0.9 in [CIP] applies to the form D because the precise coefficients of the z_i^2 monomials in the expression for D are immaterial to the validity of the exponential sum (over $\mathbb{F}_p$) estimate. As a result, we conclude :

(35)

$$p \gg 1 \ \text{ and } \ \delta_E \gg p^{-3/2} \quad \text{implies} \quad \tau_j^{(2)}(E) = \frac{|E|^2}{q} \cdot (1 + o(1)) \quad \text{uniformly in } j \text{ and } r \geq 2\,. \qquad \square$$

Remarks.

1) It is also evident that the same argument applies if $\mathbf{x}+\mathbf{y}$ replaces $\mathbf{x}-\mathbf{y}$, or, for that matter, any other linear form in $\mathbf{x},\mathbf{y}$ whose coefficients belong to U_q. Thus, for all $r \geq 2$ and $j \in U_q$:

$$\begin{aligned} \left|\{(\mathbf{x},\mathbf{y}) \in E^2 : \ det(\mathbf{x}+\mathbf{y}) = j\}\right. &= \sum_{\mathbf{x},\mathbf{y}} 1_E(\mathbf{x}) \cdot 1_E(\mathbf{y}) \cdot 1_j(\mathbf{x}+\mathbf{y}) \\ &= \frac{|E|^2}{q} \cdot (1+o(1)) \quad \textit{if } \delta_E \gg p^{-3/2} \ \textit{ and } \quad p \gg 1. \end{aligned}$$

2) It would be quite interesting to extend Theorem A to treat the additive representation of $n \times n$ determinant values for $n > 2$. Since the methods worked out in [CIP] only apply to degree 2 pure monomials, it is necessary to use Katz' bound [K] instead. To that end, it seems reasonable to believe that the following assertion should hold.

Conjecture: For any $n \geq 3$ there exists a positive $\beta = \beta(n) < 1$ that is uniform in $r \geq 2$ and $j \in U_q$ such that for any subset $E \subset \mathcal{M}_n(\mathbb{Z}_q)$:

$$\tau_j^{(n)}(E) := |\{(\mathbf{x},\mathbf{y}) \in E^2 : det\,(\mathbf{x}-\mathbf{y}) = j\}| = \frac{|E|^2}{q} \cdot (1+o(1)) \quad \textit{if } p \gg_n 1 \textit{ and } \delta_E \gg_n p^{-\beta}.$$

In order to prove this it is necessary to understand the range of values possible for the coranks $\kappa_{\mathbf{b}}$ appearing in (26). When $n = 2$ it is elementary to do this. But when $n \geq 3$ it requires some rather elaborate calculations to do so.

To illustrate the general procedure, §4 works out the argument where it is feasible to do so by hand, that is, when $n = 2$ and *without the use of Gaussian sum or Salié bounds*. As such, the argument dispenses with the coordinate transformation and additive form D from §3 and confines itself to applying the procedure sketched in §2 to the four variable function $\mathbf{x} \to det(\mathbf{x})$. The result is as follows.

Theorem 2.
(36)

$$p \gg 1 \ \textit{ and } \ \delta_E \gg p^{-1} \quad \textit{implies} \quad \tau_j^{(2)}(E) = \tfrac{|E|^2}{q} \cdot (1+o(1)) \quad \textit{uniformly in } j \textit{ and } r \geq 2\,.$$

4. Proof of Theorem 2

The reader will easily check that the argument used to prove Lemma 1 for $P(\mathbf{x}) = \|\mathbf{x}\|$ on $\mathbb{Z}_q^n$ applies directly to $det(\mathbf{x})$ on $\mathbb{Z}_q^4$. As such, notations introduced in §2.2.1 are used here with the understanding that n is now replaced throughout by 4. In particular, note that the index set $\mathcal{B} := \mathcal{B}_{det}$ now has $O(p^4)$ pairs $\mathbf{b} = (b_1, b_2)$ and, for any fixed b_2,

$$\left|\{b_1 : (b_1, b_2) \in \mathcal{B}_{det}\}\right| = O(p^3). \tag{37}$$

At a fixed point $\mathbf{x}_{b_1} = (\xi_{1,1}, \xi_{1,2}, \xi_{2,1}, \xi_{2,2})$ at which $det\,\mathbf{x}_{b_1} = j_{b_2}$, where $j_{b_2} \in U_q$, we may assume by permuting indices if needed, that $\xi_{1,1} \in U_q$.

Setting $\mathbf{x}'_{b_1} = (\xi_{1,1}, \xi_{1,2}, \xi_{2,1})$ we first write out the analogue of $\Delta\varphi_{\mathbf{b}}(\mathbf{x}', j')$ on $[\mathbf{x}'_{b_1}]_1 \times [j_{b_2}]_1$ where $\mathbf{x}' = (x_{1,1}, x_{1,2}, x_{2,1}) \in (p)^3$ and $j' \in (p)$ denote p-adic coordinates on $[\mathbf{x}'_{b_1}]_1 \times [j_{b_2}]_1$ centered at $(\mathbf{x}'_{b_1}, j_{b_2})$.

Since $x_{1,1} \in (p)$ it follows that

$$u := x_{1,1} + \xi_{1,1} \quad \textit{is a unit on } (p)\,.$$

An elementary calculation also left to the reader now shows the following:

$$\begin{aligned} & (x_{1,1} + \xi_{1,1}, x_{1,2} + \xi_{1,2}, x_{2,1} + \xi_{2,1}, x_{2,2} + \xi_{2,2}) \in \{det - j = 0\} \cap [\mathbf{x}_{b_1}]_1 \times [j_{b_2}]_1 \\ \text{iff} \quad & j = j_{b_2} + j' \quad \text{and} \quad x_{2,2} = u^{-1} \cdot \big(j' + L_\xi(\mathbf{x}') + Q(\mathbf{x}')\big)\,, \\ \text{where} \quad & L_\xi := -\xi_{2,2}x_{1,1} + \xi_{2,1}x_{1,2} + \xi_{1,2}x_3\,, \ \ Q(\mathbf{x}') := x_{1,2}x_{2,1}\,. \end{aligned}$$

In other words, as an equation on $[\mathbf{x}'_{b_1}]_1 \times [j_{b_2}]_1$ we have

$$x_{2,2} = \Delta\varphi_{\mathbf{b}}(\mathbf{x}', j') := u^{-1} \cdot \big(j' + L_\xi(\mathbf{x}') + Q(\mathbf{x}')\big)\,. \tag{38}$$

The next step is to introduce $\mathbf{m} := (\mathbf{m}', m_{2,2}) = (m_{1,1}, m_{1,2}, m_{2,1}, m_{2,2}) \in \mathbb{Z}_q^4$ and set (see (16))

$$f_{\mathbf{b}}(\mathbf{x}', j', \mathbf{m}) := m_{2,2} \cdot \Delta\varphi_{\mathbf{b}}(\mathbf{x}', j') + \langle \mathbf{x}', \mathbf{m}' \rangle = m_{2,2} \cdot u^{-1}\big[j' + L_\xi(\mathbf{x}') + Q(\mathbf{x}')\big] + \langle \mathbf{x}', \mathbf{m}' \rangle.$$

For fixed j' we next compute the Hessian matrix of $f_{\mathbf{b}}(\mathbf{x}', j', \mathbf{m})$

$$\mathcal{H}_{\mathbf{b}}(\mathbf{x}', j', \mathbf{m}) = \big(\partial^2 f_{\mathbf{b}}(\mathbf{x}', j', \mathbf{m}) / \partial x_{u_1,v_1} \partial x_{u_2,v_2}\big) \tag{39}$$

as a function of $\mathbf{x}', j', \mathbf{m}$. A straightforward calculation, also left to the reader, shows the following.

$$\begin{aligned} & \mathcal{H}_{\mathbf{b}}(\mathbf{x}', j', \mathbf{m}) \qquad (40) \\ & := m_{2,2} \cdot \begin{pmatrix} 2u^{-3}\big[j' + \xi_{1,1}\xi_{2,2} + \xi_{2,1}x_{1,2} + \xi_{1,2}x_{2,1} + Q(\mathbf{x}')\big] & -u^{-2}(x_{2,1} + \xi_{2,1}) & -u^{-2}(x_{1,2} + \xi_{1,2}) \\ -u^{-2}(x_{2,1} + \xi_{2,1}) & 0 & u^{-1} \\ -u^{-2}(x_{1,2} + \xi_{1,2}) & u^{-1} & 0 \end{pmatrix}. \end{aligned}$$

In light of the discussion in §2.2.3, 2.2.4, which depends upon the principal of Stationary Phase over p-adic rings, the important issue to resolve concerns the corank of the matrix $\mathcal{H}_{\mathbf{b}}(\mathbf{0}', j', \mathbf{m})$ *mod* p. Since $j' \equiv 0$ *mod* p, it suffices to understand

$$\mathcal{H}_{\mathbf{b}}(\mathbf{0}', 0, \mathbf{m}) := m_{2,2} \cdot \begin{pmatrix} 2\,\xi_{1,1}^{-2}\,\xi_{2,2} & -\,\xi_{1,1}^{-2}\,\xi_{2,1} & -\,\xi_{1,1}^{-2}\,\xi_{1,2} \\ -\,\xi_{1,1}^{-2}\,\xi_{2,1} & 0 & \xi_{1,1}^{-1} \\ -\,\xi_{1,1}^{-2}\,\xi_{1,2} & \xi_{1,1}^{-1} & 0 \end{pmatrix} \ mod\, p \tag{41}$$

at any point at which the gradient $\nabla_{\mathbf{x}'} f_{\mathbf{b}}(\mathbf{0}', 0, \mathbf{m}) = \mathbf{0}$ *mod* p. Since $\xi_{1,1} \neq 0$ *mod* p, this property cannot occur if $m_{2,2} = 0$ *mod* p, so we may assume $m_{2,2} \neq 0$ *mod* p.

A calculation now shows that

$$det\big(\mathcal{H}_{\mathbf{b}}(\mathbf{0}', 0, \mathbf{m})\big) \ mod\, p = 2 \cdot \ m_{2,2} \cdot \xi_{1,1}^{-3}\,\big[\xi_{1,2}\xi_{2,1} - \xi_{1,1}^{3}\,\xi_{2,2}\big] \ mod\, p\,.$$

Setting

$$\kappa_{\mathbf{b}}(\mathbf{m}) := \textit{corank } \mathcal{H}_{\mathbf{b}}(\mathbf{0}', 0, \mathbf{m}) \textit{ mod } p \ \textit{ for any } \mathbf{m} \textit{ such that } m_{2,2} \neq 0 \textit{ mod } p \,,$$

we see that

either (42) $(i)\ \kappa_{\mathbf{b}}(\mathbf{m}) = 0$

or $(ii)\ \kappa_{\mathbf{b}}(\mathbf{m}) > 0 \ \textit{ and } \ \xi_{1,1}\,\xi_{2,2} - \xi_{1,2}\,\xi_{2,1} = j_{b_2} \textit{ mod } p \ \textit{ and } \ \xi_{1,2}\,\xi_{2,1} = \xi_{1,1}^{3}\,\xi_{2,2} \textit{ mod } p\,.$

This now allows us to refine (37) as follows.

Lemma 7. *For each b_2:*
1) $\left|\{(b_1 : \mathbf{b} = (b_1, b_2)) \in \mathcal{B}_{det} \ \textit{ and } \ \kappa_{\mathbf{b}}(\mathbf{m}) = 0\}\right| \ = O(p^3)\,.$
2) $\left|\{(b_1 : \mathbf{b} = (b_1, b_2)) \in \mathcal{B}_{det} \ \textit{ and } \ \kappa_{\mathbf{b}}(\mathbf{m}) > 0\}\right| \ = O(p^2)\,.$
3) If $\kappa_{\mathbf{b}}(\mathbf{m}) > 0$, then $\kappa_{\mathbf{b}}(\mathbf{m}) = 1$.

Proof of (2): If $\kappa_{\mathbf{b}} > 0$ occurs, then it follows that $\xi_{1,2}\,\xi_{2,1} \neq 0 \textit{ mod } p$ must hold. Indeed, if this were not the case then necessarily $j_{b_2} = 0 \textit{ mod } p$. As a result, we see that $\xi_{2,2} = \xi_{2,2}(\xi_{1,1}, j_{b_2})$ and $\xi_{2,1} = \xi_{2,1}(\xi_{1,1}, \xi_{1,2}, j_{b_2}) \neq 0$.

In other words, if $\kappa_{\mathbf{b}}(\mathbf{m}) > 0$ and $m_{2,2} \neq 0 \textit{ mod } p$ then $\xi_{1,1}$ and $\xi_{1,2}$ are independent and $\xi_{2,1}, \xi_{2,2}$ are dependent variables on the locus

$$\{\xi_{1,1}\xi_{2,2} - \xi_{1,2}\xi_{2,1} = j_{b_2}\} \cap \{\mathcal{H}_{\mathbf{b}}(\mathbf{0}, 0, \mathbf{m}) = 0\}\,.$$

This implies the bound asserted in (2).

Part 3 is clear from the fact that the second and third rows of $\mathcal{H}_{\mathbf{b}}(\mathbf{0}, 0, \mathbf{m})$ are non zero and independent mod p. □

We now use this to bound each $\widehat{1}_{j_{b_2}+j'}(\mathbf{m})$ by starting with a suitable refinement of (17) that takes into account the existence of two different possible values for $\kappa_{\mathbf{b}}(\mathbf{m})$ when $\nu(\mathbf{m}) < r - 1$. To that end, we first define for each b_2 and $j' \in (p)$:

$$(43)\ \mathcal{F}_q^{(\kappa)}(j_{b_2} + j', \mathbf{m}) \ = \sum_{\substack{\mathbf{b}=(b_1,b_2)\in\mathcal{B}_{det} \\ b_1 \in \mathcal{B}_{b_2}(j') \\ \kappa_{\mathbf{b}}(\mathbf{m})=\kappa}} \Psi_q(\langle \mathbf{x}_{b_1}, \mathbf{m}\rangle) \cdot \int_{(p)^3} \Psi_q\big(f_{\mathbf{b}}(\mathbf{x}', j_{b_2} + j', \mathbf{m})\big)|d\mathbf{x}'|$$

$$:= \sum_{\substack{\mathbf{b}=(b_1,b_2)\in\mathcal{B}_{det} \\ b_1 \in \mathcal{B}_{b_2}(j') \\ \kappa_{\mathbf{b}}(\mathbf{m})=\kappa}} \Psi_q(\langle \mathbf{x}_{b_1}, \mathbf{m}\rangle) \cdot \mathcal{F}_{q,\mathbf{b}}(j_{b_2} + j', \mathbf{m})\,.$$

and note that

$$\widehat{1}_{j_{b_2}+j'}(\mathbf{m}) = q^{-1} \cdot \Big[\mathcal{F}_q^{(0)}(j_{b_2} + j', \mathbf{m}) + \mathcal{F}_q^{(1)}(j_{b_2} + j', \mathbf{m})\Big]. \tag{44}$$

Once we know this, by setting $n = 4$, defining $\Delta\varphi_{\mathbf{b}}(\mathbf{x}', j')$ by (38), and restricting to $\mathbf{m}$ with $\nu(\mathbf{m}) < r - 1$, it is clear that all the assertions in Lemmas 3 - 6 can be proved for the summand $\mathcal{F}_q^{(0)}(j_{b_2}+j',\mathbf{m})$ without any particularly significant change to the proofs sketched in §2.2.3-2.2.4. In this way we see immediately that

(45)
$\mathcal{F}_q^{(0)}(j_{b_2}+j',\mathbf{m}) = O(p^{-3/2})$ *uniformly in* $j_{b_2} \in U_q$, $j' \in (p)$, *and* $\mathbf{m}$ *s.t.* $0 \leq \nu(\mathbf{m}) < r-1$.

To bound the other summand in (44) for any $\nu(\mathbf{m}) < r-1$ we need to combine the estimates from Remarks 1 and 3 with Part 2 of Lemma 7.

The first step treats the possibility that $\nu(\mathbf{m}) \leq r-4$ and $r \geq 2$. Using (26) gives :

$$\begin{aligned} \widehat{1}_{j_{b_2}+j'}(\mathbf{m}) &= q^{-1} \cdot \sum_{\substack{\mathbf{b}=(b_1,b_2)\in\mathcal{B}_{det} \\ b_1\in\mathcal{B}_{b_2}(j') \\ \kappa_{\mathbf{b}}(\mathbf{m})=1}} \Psi_q(\langle \mathbf{x}_{b_1},\mathbf{m}\rangle) \cdot \mathcal{F}_{q,\mathbf{b}}(j_{b_2}+j',\mathbf{m}) \\ &= O\big(q^{-1}\cdot p^2 \cdot p^{-4}\big) = O(q^{-1}\cdot p^{-2}). \end{aligned} \tag{46}$$

This is uniform in $j_{b_2}+j' \in U_q$, all $\mathbf{m}$ with $\nu(\mathbf{m}) \leq r-4$, and $r \geq 2$.

The second step assumes $\nu(\mathbf{m}) = r-2$. Here, for fixed $\mathbf{m}$ the needed observation is that the bound from Lemma 5 does not change since the number of pertinent b_1 is $O(1)$ *not* $O(p^2)$ (see (30)ff.). As a result we have

$$\begin{aligned} \widehat{1}_{j_{b_2}+j'}(\mathbf{m})\big|_{\nu(\mathbf{m})=r-2} &= q^{-1} \cdot \sum_{\substack{\mathbf{b}=(b_1,b_2)\in\mathcal{B}_{det} \\ b_1\in\mathcal{B}_{b_2}(j') \\ \kappa_{\mathbf{b}}(\mathbf{m})=1}} \Psi_q(\langle \mathbf{x}_{b_1},\mathbf{m}\rangle) \cdot \mathcal{F}_{q,\mathbf{b}}(j_{b_2}+j',\mathbf{m}) \\ &= O\big(q^{-1}\cdot p^{-3}\big). \end{aligned} \tag{47}$$

The third step assumes $\nu(\mathbf{m}) = r-3$. Here we must use the bound from Remark 3. However now the number of a priori pertinent b_1 is again $O(p^2)$. As a result we have

$$\begin{aligned} \widehat{1}_{j_{b_2}+j'}(\mathbf{m})\big|_{\nu(\mathbf{m})=r-3} &= q^{-1} \cdot \sum_{\substack{\mathbf{b}=(b_1,b_2)\in\mathcal{B}_{det} \\ b_1\in\mathcal{B}_{b_2}(j') \\ \kappa_{\mathbf{b}}(\mathbf{m})=1}} \Psi_q(\langle \mathbf{x}_{b_1},\mathbf{m}\rangle) \cdot \mathcal{F}_{q,\mathbf{b}}(j_{b_2}+j',\mathbf{m}) \\ &= O\big(q^{-1}\cdot p^2 \cdot p^{-9+2}\big) = O(q^{-1}\cdot p^{-5}). \end{aligned} \tag{48}$$

These bounds are all uniform in $j_{b_2}+j' \in U_q$, $\mathbf{m}$ with $\nu(\mathbf{m}) < r-1$, and $r \geq 2$.

There is, however, a basic difference when the stationary phase method is inapplicable, that is, when $\nu(\mathbf{m}) = r-1$. The more general estimate (29), due to Katz, applies to the exponential sum over the $\mathbb{F}_p$-points of the hypersurface $\{\overline{det} = \bar{j}_{b_2}\}$. This is slightly poorer than $3/2$ since the value of n in (29) equals 4 in this case.

As a result, when we sum over the reductions mod p of *all* the points $\mathbf{x}_{b_1}$, *that is, without distinguishing between the corank values*, we can only affirm :

(49)
for any $\mathbf{m}$ *with* $\nu(\mathbf{m}) = r-1$: $\quad p^{-3} \displaystyle\sum_{\{\mathbf{x}_{b_1}:\overline{det}\,(\mathbf{x}_{b_1})=\bar{j}_{b_2}\}} \Psi_p\big(\langle \mathbf{x}_{b_1},\widehat{\mathbf{m}}\rangle\big) = O(p^{-3+2}) = O(p^{-1}).$

As a result, we have the following estimate:

$$\widehat{1}_{j_{b_2}+j'}(\mathbf{m})\big|_{\nu(\mathbf{m})=r-1} = q^{-1}\cdot\sum_{\kappa=0}^{1}\mathcal{F}_q^{(\kappa)}(j_{b_2}+j',\mathbf{m})\big|_{\nu(\mathbf{m})=r-1} = O(q^{-1}\cdot p^{-1}). \tag{50}$$

Putting together the proofs of (45) - (47) with (49), (50) finishes the proof of the following.

Lemma 8.

$$\widehat{1}_j(\mathbf{m}) = O(q^{-1}\cdot p^{-1}) \quad \textit{uniformly in } j\in U_q,\ r\geq 2,\ \mathbf{m}\neq\mathbf{0}, \textit{ and } p\gg 1. \tag{51}$$

It is now easy to modify the proof of (6) and complete the

Proof of Theorem 2. We proceed as in the beginning of §2, keeping in mind what 1_j denotes here. We first write out $\tau_j^{(2)}(E)$ as

$$\tau_j^{(2)}(E) = \sum_{\mathbf{x},\mathbf{y}} 1_E(\mathbf{x})\cdot 1_E(\mathbf{y})\cdot 1_j(\mathbf{x}-\mathbf{y})\,,$$

and apply Fourier inversion to 1_j. This gives after some simplification

$$\begin{aligned}\tau_j^{(2)}(E) &= q^{2n}\cdot\sum_{\mathbf{m}\in\mathbb{Z}_q^4}\widehat{1}_E(\mathbf{m})\cdot\widehat{1}_E(-\mathbf{m})\cdot\widehat{1}_j(\mathbf{m}) = q^{2n}\cdot\left\{\widehat{1}_E^2(\mathbf{0})\cdot\widehat{1}_j(\mathbf{0})+\sum_{\mathbf{m}\neq\mathbf{0}}|\widehat{1}_E(\mathbf{m})|^2\cdot\widehat{1}_j(\mathbf{m})\right\}\\ &:= \mathcal{M}+\mathcal{E}.\end{aligned}$$

As with $P=\|\cdot\|$, we know that

$$\widehat{1}_j(\mathbf{0}) = \big|\{\mathbf{x}\in\mathbb{Z}_q^4 : det\,\mathbf{x}=j\}\big|/q^4 = q^{-1}\cdot(1+o(1))\,,$$

so that

$$\mathcal{M} = \frac{|E|^2}{q}\cdot(1+o(1)).$$

Bounding $\mathcal{E}$ uses (51) to give

$$\mathcal{E} \ll q^{2n}\cdot\delta_E\cdot(q^{-1}\cdot p^{-1}) = q^n\cdot|E|\cdot(q^{-1}\cdot p^{-1})$$

where the implied constant is uniform in $r\geq 2$ and $p\gg 1$. It then follows immediately that

$$p\gg 1 \quad \textit{and} \quad \delta_E\gg p^{-1} \quad \textit{implies} \quad \mathcal{M}>\mathcal{E}\,.$$

Thus,

$$p\gg 1 \quad \textit{and} \quad \delta_E\gg p^{-1} \quad \textit{implies} \quad \tau_j^{(2)}(E) = \frac{|E|^2}{q}\cdot(1+o(1)) \textit{ uniformly in } r\geq 2 \textit{ and } j\in U_q. \quad \square$$

References

[CIP] D. Covert, A. Iosevich, and J. Pakianathan *Geometric configurations in the ring of integers modulo p^ℓ* Indiana. Math. J., 61 (2012) 1949–1967.

[DF] R. Dabrowski and B. Fisher *A stationary phase formula for exponential sums over $\mathbb{Z}/p^m\mathbb{Z}$ and applications to $GL(3)-$Kloosterman sums.* Acta. Arith., 80 (1997) 1–48.

[D] Y. Demiroglu *Unit-graphs and special unit-digraphs on matrix rings.* Forum Math. 30 (2018) 1397–1412.

[IR] A. Iosevich and M. Rudnev *Erdös Distance Problem in Vector Spaces over Finite Fields*. Trans. A.M.S., 359 (2007) 6127–6142.

[K] N. Katz *Estimates for "singular" exponential sums*. IMRN, 16 (1999) 875–899.

[L] B. Lichtin *Distance and Sum-Product Problems over p-adic Rings.* Proc. London Math. Soc. 118 (2019) 1450–1470.

[L2] B. Lichtin *On a question of Heath-Brown: Good estimates on average for higher degree Kloosterman sums*. Forum Math., 15 (2003) 329–375.

[S] H. Salié *Über die Kloostermanschen summen $S(u,v;q)$*. Math. Z., 34 (1932) 91–109.

[T] T. Tao *The sum-product phenomenon in arbitrary rings*. Contributions to Discrete Mathematics, 4 (2009) 59–82.

Email address: `lichtin@frontier.com`