Online Journal of Analytic Combinatorics
www.combinatorialpress.com/ojac

Combinatorial Press

# Dot product values over finite $p-$adic rings

Ben Lichtin*

ABSTRACT

This paper uses exponential sum methods to show that if $E \subset (\mathbb{Z}/p^r)^n \setminus (p)^{(n)}$ has a sufficiently large density and $j$ is any unit in the finite ring $\mathbb{Z}/p^r$ then there exist pairs of elements of $E$ whose dot product equals $j$. It then applies this to the problem of detecting $2-$ simplices with endpoints in $E$.

*Keywords:* point configurations, Fourier transform, exponential sum estimates, $p-$adic numbers

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

## 1. Introduction

This article studies the distribution of dot product *values* over $\mathbb{Z}_q := \mathbb{Z}/q$ on sets $E \times E \subset \mathbb{Z}_q^{2n}$ $(n \geq 2)$ which belong to the unit group $U_q := (\mathbb{Z}/q)^\times$, where $q = p^r$ *and* $r \geq 2$.

If $n \geq 2$ our main result (Theorem 1.1) finds a simple lower bound on the density $\delta_E := |E|/q^n$ of a subset $E \subset \mathbb{Z}_q^n \setminus (p)^{(n)}$, where

$$(p)^{(n)} := \{(a_1, \ldots, a_n) \in \mathbb{Z}_q^n : \quad a_i \in (p) \ \ \textit{for each } i\},$$

which is uniformly bounded from below in all $p \gg 1$ and all $r \geq 2$, and which insures that the following property is satisfied:

for each $j \in U_q$ there exist

$$\mathbf{x} = (x_1, \ldots, x_n),\ \mathbf{y} = (y_1, \ldots, y_n) \in E \text{ s.t. } \langle \mathbf{x}, \mathbf{y} \rangle := \sum_{i=1}^{n} x_i y_i = j \in \mathbb{Z}_q.$$

Defining *for each* $j \in U_q$ and $E \subset \mathbb{Z}_q^n \setminus (p)^{(n)}$

$$\beta_j(E) := |\{(\mathbf{x}, \mathbf{y}) \in E^2 : \langle \mathbf{x}, \mathbf{y} \rangle = j\}|,$$

* Corresponding author.

Received 11 Mar 2025; Revised 12 Jul 2025; Accepted 29 Dec 2025; Published Online 14 Mar 2026.
DOI: 10.61091/ojac21-03

the first observation to make is that the restriction to subsets $E$ of $\mathbb{Z}_q^n \backslash (p)^{(n)}$ is a reasonable one since any *subset* of $E$ that lies inside $(p)^{(n)}$ cannot contribute to $\beta_j(E)$ because $j \notin (p)$.

What we mean precisely by the expression "$\delta_E$ is uniformly bounded from below in all $p \gg 1$ and $r \geq 2$" is that there exist $\gamma < 0$, $P \geq 1$, and $C > 0$ (independent of $p, r$) such that

$$p \geq P \quad \textit{and} \quad \delta_E \geq C p^{\gamma} \quad \textit{implies} \quad \beta_j(E) \geq 1 \quad \textit{for all } j \in U_q \quad \textit{and } r \geq 2.$$

Our main result shows this property holds if $\gamma = -(n-1)/2$, and also gives an explicit main term for each $\beta_j(E)$. Its proof is given in Section 2.2.4 and is a simple consequence of the two estimates derived in Section 2.2.2, Section 2.2.3. The statement is as follows.

**Theorem 1.1.** *Assume $n \geq 2$ and $E \subset \mathbb{Z}_q^n \setminus (p)^{(n)}$. Then there exists a constant $C > 0$ (uniform in $p \gg 1$ and $r \geq 2$) such that*

$$p \gg 1 \quad \textit{and} \quad \delta_E \geq C\, p^{-\frac{n-1}{2}} \quad \textit{implies} \quad \beta_j(E) = \frac{|E|^2}{q} \cdot (1 + o(1)) \quad \textit{for each } j \in U_q \textit{ and } r \geq 2. \tag{1}$$

The significance of Theorem 1.1 is that our density lower bound therefore only depends upon a sufficiently large $p$ and *not* upon a choice of $r \geq 2$. This is to be contrasted with the results in [1], [8] in which the weaker density lower bound $\delta_E \gg r\, p^{-\frac{n-1}{2}}$ sufficed to insure that $\beta_j(E)$ is positive when $r \geq 1$ (for each $j$ and $n \geq 2$), but without giving the main term in (1).

An additional point to emphasize here is that our density lower bound is on a scale of $p$ and not $q$, i.e. it is a negative power of $p$ *not* $q$. This appears to be an inevitable consequence of the presence of zero divisors in $\mathbb{Z}_q^n$, that is, vectors that are zero after multiplication by some power of $p$ less than $r$.

Since our method relies upon estimates for averages of exponential sums mod $q$ of scalar products of non zero vectors, such averages are necessarily inflated because of this phenomenon (see (23), (24)ff. in Section 2.2.2). However, by being careful and using a different approach to that in [1], [8], we are able to extract some savings that result in the negative exponent of $p$ in (1).

A variant of Theorem 1.1 is the subject in Section 3. This concerns the problem of detecting points in a "2−simplex", which for our purposes here means any set of the form

$$\mathbf{\Sigma}_{\mathbf{v},j}(E) = \{(\mathbf{x}_1, \mathbf{x}_2) \in E \times E : \|\mathbf{x}_1\| = v_1\,,\ \|\mathbf{x}_2\| = v_2\,,\ \langle \mathbf{x}_1, \mathbf{x}_2 \rangle = j\}\,,$$

where $(\mathbf{v}, j) = (v_1, v_2, j) \in U_q^3$ and $\|\mathbf{x}\| = \langle \mathbf{x}, \mathbf{x} \rangle$.

It is not difficult to adapt the argument that proves Theorem 1.1 to this problem. It suffices to replace $E$ by $E_{v_1} \times E_{v_2}$ where

$$E_{v_u} := E \cap S_{v_u} := E \cap \{\mathbf{x} : \|\mathbf{x}\| = v_u\} \qquad (u = 1, 2).$$

However, an apparent obstacle exists that prevents our method from being applicable for a given $n \geq 2$ and *all* $r \geq 2$.

To see this most simply, assume that $E$ is a *random* subset of $\mathbb{Z}_q^n$, which tells us that $E$ and the $S_{\nu_u}$ are independent sets with respect to the probability measure

$$X \subset \mathbb{Z}_q^n \longrightarrow \delta_X.$$

In this event it follows that for each $u$:

$$\delta_{E_{v_u}} = \delta_E \, q^{-1} \, (1 + o(1)) \, .$$

By combining (35) and (54), we show (see Section 3) that

$$\delta_E \, q^{-1} \, (1+o(1)) \gg q^{-\frac{1}{2}} \, p^{-\frac{n-2}{2}} \quad \Longrightarrow \quad |\Sigma_{\mathbf{v},j}(E)| = \frac{|E_{v_1}| \, |E_{v_2}|}{q} \, (1+o(1)) = \frac{|E|^2}{q^3} \, (1+o(1)).$$

However, since $\delta_E \leq 1$, the hypothesis can only be satisfied when $r < n-2$ and $p \gg 1$.

More generally, our second result includes the possibility that $E$ and the $S_v$ are *not* independent.

**Theorem 1.2.** *Assume $n \geq 5$ and $r \geq 2$. Then there exists a constant $c > 0$ (uniform in $p \gg 1$, $r \geq 2$) such that for all $(\mathbf{v}, j) \in U_q^3$ :*

$$p \gg 1, r < n-2, \quad \textit{and} \quad \delta_{E_{v_1}}^{\frac{1}{2}} \, \delta_{E_{v_2}}^{\frac{1}{2}} \geq c \, q^{-\frac{1}{2}} \, p^{-\frac{(n-2)}{2}} \quad \textit{implies} \quad |\, \mathbf{\Sigma}_{\mathbf{v},j}(E) \,| = \frac{|E_{v_1}| \, |E_{v_2}|}{q} \, (1+o(1)). \tag{2}$$

In general, it is convenient to introduce a parameter $\alpha_u$, defined by setting

$$\delta_{E_{\nu_u}} := \alpha_u \, \delta_E \, \delta_{S_{\nu_u}},$$

and express the criterion of Theorem 1.2 in terms of $\alpha_1, \alpha_2$, and $|E|$ as follows.

$$p \gg 1, \;\; r < n-2, \quad \text{and} \quad \delta_E \geq c \, \frac{q^{\frac{1}{2}} \, p^{-\frac{(n-2)}{2}}}{(\alpha_1 \, \alpha_2)^{\frac{1}{2}}} \quad \textit{implies} \quad |\, \mathbf{\Sigma}_{\mathbf{v},j}(E) \,| = \frac{\alpha_1 \, \alpha_2 \, |E|^2}{q^3} \, (1+o(1)). \tag{3}$$

What this means in practice is that the parameters $\alpha_1, \alpha_2$ are implicitly constrained by the condition that any lower bound for $\delta_E$ must be at most 1, that is,

$$\alpha_1 \, \alpha_2 \gg p^{r-(n-2)}.$$

An immediate corollary of Theorem 1.2 extends the main result in [4] to detect "circular $2-$point configurations" whose vertices belong to some $E \subset \mathbb{Z}_q^n$ for all $p \gg 1$ and $n \geq 5$, provided that $2 \leq r < n-2$.

Given a set $E \subset \mathbb{Z}_q^n$ and unit $\iota$ this problem asks whether pairs of points $(\mathbf{x}_1, \mathbf{x}_2) \in E^2$ exist that satisfy simultaneously the conditions:

$$\|\mathbf{x}_1\| = \|\mathbf{x}_2\| = \iota \quad \textit{and} \quad \|\mathbf{x}_1 - \mathbf{x}_2\| = \iota.$$

Given that $2 \cdot \iota \neq \iota \, mod \, p$ when $p > 2$, such a property follows trivially from the hypotheses in (2) by setting $v_1 = v_2 = \iota$ and choosing $j = 2^{-1} \cdot \iota$, which insures that $\iota = 2\,(\iota - j)$ . Since there are $|U_q|$ possible $\iota$ there are $|U_q|$ such circular $2-$point configurations if the hypotheses in (2) hold.

Theorem 1.2 can also be interpreted in terms of the well known graph coloring problem from geometric Ramsey theory in the simplest possible case. In this context, the value

of $\|\mathbf{x}_1 - \mathbf{x}_2\|$ becomes a color for the edge of a graph whose vertex set $\{\mathbf{x}_1, \mathbf{x}_2\}$ is a subset of some $E \subset \mathbb{Z}_q^n$. Theorem 1.2 tells us that if $p$ sufficiently large then $|U_q|$ distinct monocolorings of the edge set *must exist* provided that $E$ has density at least $q^{\frac{1}{2}} p^{-\frac{n-2}{2}}$ and $r < n-2$.

It is natural to ask whether the proof of Theorem 1.2 can be extended to address analogous problems for complete graphs in $\mathbb{Z}_q^n$ with $k \geq 3$ vertices. Using very different ideas, some progress on this problem is given in [6].

Theorems 1.1 and 1.2 (as well as the theorems proved in [4]-[5]) can be thought of as a modest response to Tao's general challenge (see [7]) to extend to finite rings results in additive combinatorics involving orthogonal invariants that have been proved over finite fields, using ideas or techniques that do not typically (or immediately, or even at all) extend to finite $p-$adic rings. Although Tao's explicit interest in [ibid.] concerned the sum-product phenomenon, it does not seem unreasonable to adopt a broader understanding of his challenge to include, in addition, point configuration questions like those addressed in [op.cit.] and this article.

A basic feature of Theorem 1.1 is that it proves a result that is *uniform* in $r \geq 2$, provided only that $p$ is larger than a lower bound that does not depend upon $r$. In addition, it will be evident that there is nothing in the proof of Theorem 1.1 that would not extend straightforwardly to treat the same problem over finite subrings of the ring of integers of any finite extension of the $p-$adic field $\mathbb{Q}_p$. Filling in the details of such a discussion is an exercise best left to the reader. On the other hand, because the density lower bound in Theorem 1.1 is a power of $p$, and *not* $q$, it does not seem possible to improve Theorem 1.2 by eliminating the a priori bound for $r$.

In a Concluding Remark we indicate a simple application of the uniformity in $r$ property of Theorem 1.1 to a comparable dot product problem over the ring $\mathbb{Z}_p$ of $p-$adic integers. An interesting consequence of our result is that by using only Haar measure we can say something about the presence of dot product values created by points in a subset $E \times E$ when $E$ is a closed subset of $\mathbb{Z}_p^n$. This is sketched at the end of the article. An alternative approach, for a *general* configuration problem on average, was worked out in the thesis [2], which used the full arsenal of geometric measure theoretic techniques based upon Hausdorff and Frostman measures adapted to the non archimedean metric context.

## Notations

We use throughout the particular notations below where $j \in U_q$, $\mathbf{m} = (m_1, \ldots, m_n) \in \mathbb{Z}_q^n$, $\boldsymbol{m} = (\mathbf{m}_1, \mathbf{m}_2) \in \mathbb{Z}_q^{2n}$, and $\mathbf{x} = (x_1, \ldots, x_n)$, $\mathbf{y} = (y_1, \ldots, y_n) \in \mathbb{Z}_q^n$ :

$$\langle \mathbf{x}, \mathbf{y} \rangle = \sum_{i=1}^{n} x_i y_i \,; \quad \langle \mathbf{x}, \mathbf{m} \rangle := \sum_{i} x_i m_i \,; \; \|\mathbf{x}\| := \sum_{i=1}^{n} x_i^2 \;\; (\textit{all defined in } \mathbb{Z}_q);$$

$$ord_p \, \mathbf{x} = min_i \, ord_p \, x_i := min_i \, \max \{\ell : p^\ell | x_i\};$$

$$1_j(\mathbf{x}, \mathbf{y}) = \textit{characteristic function of} \quad \{(\mathbf{x}, \mathbf{y}) \in \mathbb{Z}_q^{2n} : \langle \mathbf{x}, \mathbf{y} \rangle = j\} \,;$$

$$1_E(\mathbf{x}) = \text{characteristic function of } E \,;$$

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

$\widehat{1}_j(\boldsymbol{m}) = q^{-2n} \sum_{\mathbf{x}\in\mathbb{Z}_q^n} 1_j(\mathbf{x},\mathbf{y})\chi\langle(\mathbf{x},\mathbf{y}),-\boldsymbol{m}\rangle$; $\widehat{1}_E(\boldsymbol{m}) = q^{-n} \sum_{\mathbf{x}\in\mathbb{Z}_q^n} 1_E(\mathbf{x})\chi\langle\mathbf{x},-\mathbf{m}\rangle$;

*for any finite set* $X$, $|X|=$ *number of elements of* $X$;

$c_p = 1-p^{-1}$, $c_{p,n} = 1-p^{-rn}$, $C_{p,r,n} = c_p\, c_{p,n}\, \dfrac{1-p^{-r(n-1)}}{1-p^{-(n-1)}}$,

$\delta_E = |E|/q^n$. $\square$

## 2. Proof of Theorem 1.1

### 2.1. *Starting points*

It is clear that

$$\begin{aligned}\beta_j(E) &= \sum_{\boldsymbol{x}=(\mathbf{x}_1,\mathbf{x}_2)\in\mathbb{Z}_q^{2n}} 1_E(\mathbf{x}_1)\cdot 1_E(\mathbf{x}_2)\cdot 1_j(\boldsymbol{x})\\ &= \sum_{\boldsymbol{m}=(\mathbf{m}_1,\mathbf{m}_2)} \widehat{1}_j(\boldsymbol{m}) \sum_{\boldsymbol{x}=(\mathbf{x}_1,\mathbf{x}_2)\in\mathbb{Z}_q^{2n}} 1_E(\mathbf{x}_1)\cdot 1_E(\mathbf{x}_2)\cdot\chi\langle\boldsymbol{x},\boldsymbol{m}\rangle\\ &= q^{2n}\cdot \sum_{\boldsymbol{m}=(\mathbf{m}_1,\mathbf{m}_2)} \widehat{1}_j(\boldsymbol{m})\cdot\widehat{1}_E(-\mathbf{m}_1)\cdot\widehat{1}_E(-\mathbf{m}_2) := \mathcal{M}^* + \mathcal{E}^*,\end{aligned}$$

where

$$\begin{aligned}\mathcal{M}^* &:= q^{2n}\cdot\widehat{1}_j(\mathbf{0},\mathbf{0})\cdot\widehat{1}_E(\mathbf{0})^2\\ \mathcal{E}^* &:= q^{2n}\cdot \sum_{\boldsymbol{m}\neq(\mathbf{0},\mathbf{0})} \widehat{1}_j(\boldsymbol{m})\cdot\widehat{1}_E(-\mathbf{m}_1)\cdot\widehat{1}_E(-\mathbf{m}_2)\\ &= q^{2n}\cdot\left\{\widehat{1}_E(\mathbf{0})\cdot\sum_{\mathbf{m}_2\neq\mathbf{0}}\widehat{1}_j(\mathbf{0},\mathbf{m}_2)\cdot\widehat{1}_E(-\mathbf{m}_2) + \sum_{\mathbf{m}_1\neq\mathbf{0}}\sum_{\mathbf{m}_2}\widehat{1}_j(\boldsymbol{m})\cdot\widehat{1}_E(-\mathbf{m}_1)\cdot\widehat{1}_E(-\mathbf{m}_2)\right\}\\ &:= q^{2n}\cdot\left[\delta_E\cdot\sum_{\mathbf{m}_2\neq\mathbf{0}} I(\mathbf{m}_2) + \sum_{\mathbf{m}_1\neq\mathbf{0}}\sum_{\mathbf{m}_2} II(\boldsymbol{m})\right].\\ &:= \mathcal{E}_I^* + \mathcal{E}_{II}^*. \qquad (4)\end{aligned}$$

We think of $\mathcal{M}^*$ as an expected main term and $\mathcal{E}^*$ as an expected error term that must be shown to be strictly smaller than $\mathcal{M}^*$ provided only that $p$ and $\delta_E$ are sufficiently large in the sense given in the Introduction.

We first evaluate $\mathcal{M}^*$ when $p \neq 2$. It is clear that

$$\widehat{1}_E(\mathbf{0}) = \frac{|E|}{q^n} = \delta_E.$$

To evaluate $\widehat{1}_j(\mathbf{0},\mathbf{0})$ we note that the choice of the $\boldsymbol{x} = (\mathbf{x}_1,\mathbf{x}_2)$ coordinates on $\mathbb{Z}_q^{2n}$ is not optimal to do this since it obscures the relation to the work in [4]. It is more useful first to define

$$\mathbf{z}_1 = \mathbf{x}_1 + \mathbf{x}_2 \qquad \mathbf{z}_2 = \mathbf{x}_1 - \mathbf{x}_2\,.$$

Setting $\boldsymbol{z} = (\mathbf{z}_1, \mathbf{z}_2)$, since $p \neq 2$, it follows that

$$T(\boldsymbol{z}) = (T_1(\boldsymbol{z}), T_2(\boldsymbol{z})) = \frac{1}{2} \cdot (\mathbf{z}_1 + \mathbf{z}_2, \mathbf{z}_1 - \mathbf{z}_2) = (\mathbf{x}_1, \mathbf{x}_2), \tag{5}$$

defines a coordinate change on all of $\mathbb{Z}_q^{2n}$ such that

$$Q : \boldsymbol{z} \longrightarrow \langle (\mathbf{x}_1 \circ T)(\boldsymbol{z}), (\mathbf{x}_2 \circ T)(\boldsymbol{z}) \rangle = \frac{1}{4} \cdot (\|\mathbf{z}_1\| - \|\mathbf{z}_2\|) \ .$$

It is then clear that $1_j^*(\boldsymbol{z}) := 1_j \circ T(\boldsymbol{z})$ denotes the characteristic function of the level set $\{\mathbf{z} : Q(\mathbf{z}) = j\}$. Since $Q$ is an *additive and nondegenerate* quadratic form in $2n$ variables we deduce from [9] and a standard $p-$adic lifting argument, using Hensel's Lemma, which lifts solutions of the congruence $Q \equiv j \, mod \, p^i$ $(i = 1, 2, \ldots, r-1)$ to solutions of $Q \equiv j \, mod \, p^{i+1}$, that

$$\widehat{1}_j(\mathbf{0}, \mathbf{0}) = \widehat{1}_j^*(\mathbf{0}, \mathbf{0}) = q^{-1} \cdot \left(1 + O\left(p^{-\frac{2n-1}{2}}\right)\right) \quad \textit{uniformly in } r \geq 1 \textit{ and } j \in U_q \, . \tag{6}$$

We conclude

$$\mathcal{M}^* = \frac{|E|^2}{q} \cdot \left(1 + O(p^{-\frac{2n-1}{2}})\right). \tag{7}$$

To simplify the discussion below, it will be useful here to fix an integer $P_0$ such that

$$p \geq P_0 \implies \frac{1}{2} \leq 1 + O\left(p^{-\frac{2n-1}{2}}\right) \leq 2. \tag{8}$$

### *2.2. Bound for $\mathcal{E}^*$*

It is convenient to split the work into two parts. We first bound $\mathcal{E}_I^*$ (see (13)) whose proof only relies upon the fundamental exponential sum estimate of Weil that is used to prove (6). We then use a very different method to establish a different bound $\mathcal{E}_I^*$ in Section 2.2.2 (see (35)). We have thought it instructive to include a discussion of each method in order to highlight the relative strength of the second approach.

Of significance here, however, is that is possible to adapt the second method to bound $\mathcal{E}_{II}^*$ in Section 2.2.3. We finish the proof of Theorem 1.1 in Section 2.2.4 by showing that if $p$ is sufficiently large (uniformly in $r \geq 2$ and $j \in U_q$) and $n \geq 2$, then the expected main term $\mathcal{M}^*$ is larger than $\mathcal{E}^*$ provided that $\delta_E$ is bounded below by the product of a constant with $p^{-\frac{n-1}{2}}$ *uniformly in* $j$, $r \geq 2$, *and all* $p \gg 1$.

**Remark 2.1.** The reader might be curious about the case when $r = 1$, that is, when $\mathbb{Z}_q = \mathbb{F}_p$. The method in [1] clearly suffices for this case. So there is no need to consider this possibility in the following discussion.

2.2.1. Bound for $\mathcal{E}_I^*$ (see (13)). We first apply Cauchy-Schwarz and Plancherel's Theorem to the sum over $\mathbf{m}_2 \neq \mathbf{0}$ which implies

$$\mathcal{E}_I^* \leq q^n \cdot |E| \cdot \delta_E^{1/2} \cdot \left( \sum_{\mathbf{m}_2 \neq \mathbf{0}} |\widehat{1}_j(\mathbf{0}, \mathbf{m}_2)|^2 \right)^{1/2}$$

$$=q^n\cdot|E|\cdot\delta_E^{1/2}\cdot\left[\sum_{\mathbf{m}_2\neq\mathbf{0}}\widehat{1}_j(\mathbf{0},\mathbf{m}_2)\cdot\widehat{1}_j(\mathbf{0},-\mathbf{m}_2)\right]^{1/2}. \tag{9}$$

Second, we note that the definition of each Fourier transform in (9) implies

$$\sum_{\mathbf{m}_2\neq\mathbf{0}}\widehat{1}_j(\mathbf{0},\mathbf{m}_2)\cdot\widehat{1}_j(\mathbf{0},-\mathbf{m}_2)=q^{-4n}\cdot\sum_{\mathbf{m}_2\neq\mathbf{0}}\left[\sum_{\mathbf{y}}\sigma_j(\mathbf{y})\,\chi\langle\mathbf{y},-\mathbf{m}_2\rangle\right]\cdot\left[\sum_{\mathbf{y}'}\sigma'_j(\mathbf{y}')\,\chi\langle\mathbf{y}',\mathbf{m}_2\rangle\right], \tag{10}$$

where

$$\sigma_j(\mathbf{y}):=\sum_{\mathbf{x}}1_j(\mathbf{x},\mathbf{y})\quad\text{ and }\quad\sigma'_j(\mathbf{y}')=\sum_{\mathbf{x}'}1_j(\mathbf{x}',\mathbf{y}').$$

As a result, since $\sigma_j(\mathbf{y})=\sigma'_j(\mathbf{y})$ and the function

$$(\mathbf{y},\mathbf{y}')\longrightarrow\sum_{\mathbf{m}_2\neq\mathbf{0}}\chi\langle\mathbf{y}'-\mathbf{y},\mathbf{m}_2\rangle\ \ \textit{equals}\ \ (\mathbf{y},\mathbf{y}')\longrightarrow q^n\cdot1_{\{\mathbf{y}=\mathbf{y}'\}}(\mathbf{y},\mathbf{y}')-1\,,$$

it follows that

$$\begin{aligned}\sum_{\mathbf{m}_2\neq\mathbf{0}}\widehat{1}_j(\mathbf{0},\mathbf{m}_2)\cdot\widehat{1}_j(\mathbf{0},-\mathbf{m}_2)&=q^{-4n}\cdot\sum_{\mathbf{y},\mathbf{y}'}\sigma_j(\mathbf{y})\sigma'_j(\mathbf{y}')\left(\sum_{\mathbf{m}_2}\chi\langle\mathbf{y}'-\mathbf{y},\mathbf{m}_2\rangle-1\right)\\&=q^{-4n}\cdot\left\{q^n\cdot\sum_{\mathbf{y}}\sigma_j^2(\mathbf{y})-\left(\sum_{\mathbf{y}}\sigma_j(\mathbf{y})\right)\cdot\left(\sum_{\mathbf{y}'}\sigma'_j(\mathbf{y}')\right)\right\}\\&=q^{-3n}\cdot\sum_{\mathbf{y}}\sigma_j^2(\mathbf{y})-q^{-4n}\cdot\left(\sum_{\mathbf{x},\mathbf{y}}1_j(\mathbf{x},\mathbf{y})\right)^2.\end{aligned} \tag{11}$$

Since $j\in U_q$, the sums over $\mathbf{y},\mathbf{y}'$ are actually concentrated on $\mathbb{Z}_q^n\setminus(p)^{(n)}$. As a result, for each fixed $\mathbf{y},\mathbf{y}'\in\mathbb{Z}_q^n\setminus(p)^{(n)}$:

$$\sigma_j(\mathbf{y})=\sigma'_j(\mathbf{y}')=q^{n-1}\,,$$

which implies

$$q^{-3n}\cdot\sum_{\mathbf{y}}\sigma_j^2(\mathbf{y})\leq q^{-3n}\cdot q^{2(n-1)}\cdot|\{\mathbf{y}\in\mathbb{Z}_q^n\setminus(p)^{(n)}|=q^{-2}\,(1-p^{-n})<q^{-2}\,.$$

Moreover, (6) implies

$$\sum_{\mathbf{x},\mathbf{y}}1_j(\mathbf{x},\mathbf{y})=q^{2n-1}\cdot\left(1+O(p^{-\frac{2n-1}{2}})\right)\quad\textit{uniformly in } r\geq1\textit{ and } j\in U_q.$$

Combining these estimates, and using the facts that the sum over $\mathbf{m}_2$ is nonnegative, and for $p\gg1$

$$\left(1+O(p^{-\frac{2n-1}{2}})\right)^2=1+O(p^{-\frac{2n-1}{2}})\,,$$

we conclude that

$$0 \leq \sum_{\mathbf{m}_2 \neq \mathbf{0}} \widehat{1}_j(\mathbf{0}, \mathbf{m}_2) \cdot \widehat{1}_j(\mathbf{0}, -\mathbf{m}_2) < |q^{-2} - q^{-2}(1 + O(p^{-\frac{2n-1}{2}})| = q^{-2} \cdot O(p^{-\frac{2n-1}{2}}) \,. \quad (12)$$

As a result, (9) now implies that there exists $P_I'$ and a constant $c_I'$ uniform in $r \geq 2$, $j$, and $p \geq P_I'$ such that

$$p \geq P_I' \implies \mathcal{E}_I^* \leq c_I' \cdot q^n \cdot |E| \cdot \delta_E^{1/2} \cdot \left(q^{-2} \cdot p^{-n+\frac{1}{2}}\right)^{1/2} = c_I' \cdot p^{-\frac{n}{2}+\frac{1}{4}} \cdot q^{\frac{n}{2}-1} \cdot |E|^{\frac{3}{2}} \,. \quad (13)$$

2.2.2. A better bound for $\mathcal{E}_I^*$ for any $r \geq 2$ and $n \geq 2$ (see (35)). We start again with (9) but use a different idea to bound the rightmost factor where, implicitly, $r \geq 2$ is always assumed.

Setting $\boldsymbol{z} = (\mathbf{z}_1, \mathbf{z}_2)$ and $\boldsymbol{z}' = (\mathbf{z}_1', \mathbf{z}_2')$, and using the definition, it is clear that for each $\mathbf{m}_2 \neq \mathbf{0}$

$$\begin{aligned} |\widehat{1}_j(\mathbf{0}, \mathbf{m}_2)|^2 &= q^{-4n} \cdot \left(\sum_{\boldsymbol{z}} 1_j(\boldsymbol{z}) \chi\langle \mathbf{z}_2, -\mathbf{m}_2\rangle\right) \cdot \left(\sum_{\boldsymbol{z}'} 1_j(\boldsymbol{z}') \chi\langle \mathbf{z}_2', \mathbf{m}_2\rangle\right) \\ &= q^{-4n} \cdot \left(\sum_{\boldsymbol{z}, \boldsymbol{z}'} 1_j(\boldsymbol{z}) \cdot 1_j(\boldsymbol{z}') \cdot \chi\langle \mathbf{z}_2, -\mathbf{m}_2\rangle \cdot \chi\langle \mathbf{z}_2', \mathbf{m}_2\rangle\right) \,. \end{aligned} \quad (14)$$

In which case, by exchanging the order of summation with $\mathbf{m}_2$ we see that

$$\sum_{\mathbf{m}_2 \neq \mathbf{0}} |\widehat{1}_j(\mathbf{0}, \mathbf{m}_2)|^2 = q^{-4n} \cdot \left(\sum_{\boldsymbol{z}, \boldsymbol{z}'} 1_j(\boldsymbol{z}) \cdot 1_j(\boldsymbol{z}') \cdot \sum_{\mathbf{m}_2 \neq \mathbf{0}} \chi\langle \mathbf{z}_2, -\mathbf{m}_2\rangle \cdot \chi\langle \mathbf{z}_2', \mathbf{m}_2\rangle\right) . \quad (15)$$

We first note that since $j \in U_q$ it follows that $\boldsymbol{z}, \boldsymbol{z}' \notin (p)^{(2n)}$. For each $\mathbf{z}_1$ resp. $\mathbf{z}_1' \notin (p)^{(n)}$ set $\mathfrak{1}(\mathbf{z}_1)$ resp. $\mathfrak{1}(\mathbf{z}_1')$ *to denote a fixed vector, depending upon* $\mathbf{z}_1$ *resp.* $\mathbf{z}_1'$, *in*

$$\{\mathbf{z}_2 : 1_j(\mathbf{z}_1, \mathbf{z}_2) = 1\} \quad \text{resp.} \quad \{\mathbf{z}_2' : 1_j(\mathbf{z}_1', \mathbf{z}_2') = 1\} \,,$$

and set

$$\mathcal{K}(\mathbf{z}_1) = \{\mathbf{z}_2 : \langle \mathbf{z}_1, \mathbf{z}_2\rangle = 0\} \quad \text{resp.} \quad \mathcal{K}(\mathbf{z}_1') = \{\mathbf{z}_2' : \langle \mathbf{z}_1', \mathbf{z}_2'\rangle = 0\}.$$

It then follows that

$$\begin{aligned} &rhs(15) \\ &= \sum_{\mathbf{z}_1, \mathbf{z}_1'} \sum_{\substack{\mathbf{w}_1 \in \mathcal{K}(\mathbf{z}_1) \\ \mathbf{w}_1' \in \mathcal{K}(\mathbf{z}_1')}} \sum_{\mathbf{m}_2 \neq \mathbf{0}} \chi\langle \mathfrak{1}(\mathbf{z}_1), -\mathbf{m}_2\rangle \cdot \chi\langle \mathfrak{1}(\mathbf{z}_1'), \mathbf{m}_2\rangle \cdot \chi\langle \mathbf{w}_1, -\mathbf{m}_2\rangle \cdot \chi\langle \mathbf{w}_1', \mathbf{m}_2\rangle \\ &= \sum_{\mathbf{z}_1, \mathbf{z}_1'} \sum_{\mathbf{m}_2 \neq \mathbf{0}} \chi\langle \mathfrak{1}(\mathbf{z}_1), -\mathbf{m}_2\rangle \cdot \chi\langle \mathfrak{1}(\mathbf{z}_1'), \mathbf{m}_2\rangle \sum_{\substack{\mathbf{w}_1 \in \mathcal{K}(\mathbf{z}_1) \\ \mathbf{w}_1' \in \mathcal{K}(\mathbf{z}_1')}} \chi\langle \mathbf{w}_1, -\mathbf{m}_2\rangle \cdot \chi\langle \mathbf{w}_1', \mathbf{m}_2\rangle \,. \end{aligned} \quad (16)$$

We now must understand the behavior of the functions

$$\mathbf{v} \neq \mathbf{0} \longrightarrow \sum_{\mathbf{w} \in \mathcal{K}(\mathbf{z})} \chi\langle \mathbf{w}, \mathbf{v}\rangle \quad \textit{when } \mathbf{z} \in \{\mathbf{z}_1, \mathbf{z}_1'\} \quad \textit{and} \quad \mathbf{v} \in \{\pm \mathbf{m}_2\}. \quad (17)$$

To do this we use the fact that if $\mathbf{w} \in \mathcal{K}(\mathbf{z}) \longrightarrow \chi\langle \mathbf{w}, \mathbf{v}\rangle$ is a trivial resp. nontrivial homomorphism of the additive group $\mathcal{K}(\mathbf{z})$ then

$$\textit{the exponential sum in (17) equals } q^{n-1} \quad \textit{resp.} \quad 0\,. \tag{18}$$

To decide which possibility can occur it suffices to reduce the $2 \times n$ matrix

$$\mathcal{L} := \begin{pmatrix} \mathbf{z} \\ \mathbf{v} \end{pmatrix} = \begin{pmatrix} z_1 & z_2 & \cdots & z_n \\ v_1 & v_2 & \cdots & v_n \end{pmatrix},$$

to row echelon form. By a permutation of indices we may assume $z_1 \in U_q$, in which event $\mathcal{L}$ is row equivalent to

$$\mathcal{L}' = \begin{pmatrix} z_1 & z_2 & \cdots & z_n \\ 0 & v_2 - v_1\, z_1^{-1}\, z_2 & \cdots & v_n - v_1\, z_1^{-1}\, z_n \end{pmatrix},$$

where the inverse in $\mathbb{Z}_q$ of $z_1$ is denoted $z_1^{-1}$, and

$$\mathcal{K}(\mathbf{z}) = \left\{ \left( -[\sum_{j=2}^{n}\, w_j \cdot\, z_1^{-1}\, z_j],\, w_2, \ldots, w_n \right) : (w_2, \ldots, w_n) \in \mathbb{Z}_q^{n-1} \right\}.$$

So, if $v_1 \neq 0$ and $\langle \mathbf{z}\rangle := \{\tau\, \mathbf{z} : \tau \in \mathbb{Z}_q\}$ then

$$\mathbf{v} \in \langle \mathbf{z}\rangle \iff \mathbf{w} \in \mathcal{K}(\mathbf{z}) \to \chi\langle \mathbf{w}, \mathbf{v}\rangle \quad \textit{is identically } 1. \tag{19}$$

Indeed, the condition is clearly sufficient. The fact that it is also necessary is seen as follows. If for each $u \geq 2$ we choose $w_u$ to be a non zero divisor and set

$$\mathbf{w}_u := w_u \cdot (-\, z_1^{-1}\, z_u, 0, \ldots, 0, 1, 0, \ldots, 0) \in \mathcal{K}(\mathbf{z}) \quad \textit{(where the } u^{th} \textit{ entry equals } 1\textit{)},$$

then for each $u \geq 2$

$$\begin{aligned} \chi\langle \mathbf{w}_u, \mathbf{v}\rangle = 1 &\iff 0 = \langle \mathbf{w}_u, \mathbf{v}\rangle = w_u \cdot \left(v_u - v_1\; z_1^{-1}\, z_u\right) \\ &\implies z_1\, \mathbf{v} = v_1\, \mathbf{z} \implies \mathbf{v} = (z_1^{-1}\, v_1)\, \mathbf{z} \in \langle \mathbf{z}\rangle\,. \end{aligned}$$

In addition, since $ord_p\, \mathbf{z} = 0$, we also observe that if $\nu := ord_p\, \mathbf{v}$, then

$$z_1\, \mathbf{v} = v_1\, \mathbf{z} \implies \nu = ord_p\, v_1 \;\; \textit{and} \;\; \hat{\mathbf{v}} := p^{-\nu}\mathbf{v} = (z_1^{-1}\, p^{-\nu}\, v_1)\, \mathbf{z} \in \langle \mathbf{z}\rangle \cap \left(\mathbb{Z}_q^n \setminus (p)^{(n)}\right). \tag{20}$$

Moreover, if $v_1 = 0$ then it is equally clear that $\mathbf{v} \neq \mathbf{0}$ cannot belong to $\langle \mathbf{z}\rangle$, and

$$\mathbf{v} \neq \mathbf{0} \implies \sum_{\mathbf{w} \in \mathcal{K}(\mathbf{z})} \chi\langle \mathbf{w}, \mathbf{v}\rangle = \sum_{\widetilde{\mathbf{w}} = (0, w_2, \ldots, w_n) \in \mathbb{Z}_q^{n-1}} \chi\langle \widetilde{\mathbf{w}}, \mathbf{v}\rangle = 0\,, \tag{21}$$

since, in this event, the map $\mathbf{w} \in \mathcal{K}(\mathbf{z}) \longrightarrow \chi\langle \mathbf{w}, \mathbf{v}\rangle = \chi\langle \widetilde{\mathbf{w}}, \mathbf{v}\rangle$ is a nontrivial homomorphism (i.e., not identically equal to 1) on the additive group $\mathcal{K}(\mathbf{z})$.

This tells us that the rightmost sum in (16) can only be nonzero when $\mathbf{m}_2 \in \langle \mathbf{z}_1\rangle \cap \langle \mathbf{z}_1'\rangle$, in which event, (18) then implies this product equals $q^{2(n-1)}$. In other words :

$$rhs(15) = q^{-2n-2} \sum_{\mathbf{m}_2 \neq \mathbf{0}} \sum_{\mathbf{z}_1, \mathbf{z}_1' \notin (p)^{(n)}} \chi\langle \mathbf{1}(\mathbf{z}_1), -\mathbf{m}_2\rangle \cdot \chi\langle \mathbf{1}'(\mathbf{z}_1'), \mathbf{m}_2\rangle \cdot 1_{\langle \mathbf{z}_1\rangle \cap \langle \mathbf{z}_1'\rangle}(\mathbf{m}_2). \tag{22}$$

We next split up the innermost sum into that part over which $\mathbf{z}_1 = \mathbf{z}_1'$ and $\mathbf{z}_1 \neq \mathbf{z}_1'$ and bound each part separately.

*If* $\mathbf{z}_1 = \mathbf{z}_1'$ then we can evidently choose $\zeta(\mathbf{z}_1) = \zeta'(\mathbf{z}_1')$ and write each $\mathbf{m}_2 = p^\nu\,\widehat{\mathbf{m}}$ where $\widehat{\mathbf{m}} \in \mathbb{Z}^n_{p^{r-\nu}}$ and $ord_p\,\widehat{\mathbf{m}} = 0$, in which case, by thinking of $\mathbb{Z}^n_{p^{r-\nu}}$ as being embedded in $\mathbb{Z}^n_q$ as the vectors each of whose coefficients of a power of $p$ *larger than* $r-\nu-1$ *equals* $\mathbf{0}$, we have:

$$\sum_{\mathbf{m}_2\neq\mathbf{0}}\sum_{\mathbf{z}_1=\mathbf{z}_1'\notin(p)^{(n)}}\chi\langle\boldsymbol{\imath}(\mathbf{z}_1),-\mathbf{m}_2\rangle\cdot\chi\langle\boldsymbol{\imath}'(\mathbf{z}_1'),\mathbf{m}_2\rangle\cdot 1_{\langle\mathbf{z}_1\rangle}(\mathbf{m}_2)=\sum_{\nu=0}^{r-1}\sum_{\widehat{\mathbf{m}}}\sum_{\mathbf{z}\notin(p)^{(n)}}1_{\langle\mathbf{z}\rangle}(p^\nu\,\widehat{\mathbf{m}}).\quad(23)$$

Denoting the units in $\mathbb{Z}_{p^{r-\nu}}$ by $U_{r-\nu}$, we then note that

$$p^\nu\,\widehat{\mathbf{m}}\in\langle\mathbf{z}\rangle\iff \textit{there exists } \eta\in U_{r-\nu}\ \textit{ such that }\ \widehat{\mathbf{m}}=\eta\,\mathbf{z}\ mod\,p^{r-\nu}.\qquad(24)$$

However, from this congruence one cannot infer that any of the coefficients of $p^{r-\nu}, p^{r-\nu+1}$, $\ldots, p^{r-1}$ of the $p-$adic expansion of $\mathbf{z}$ must also equal $\mathbf{0}$. So, any such $\mathbf{z}$ is only determined uniquely mod $p^{r-\nu}$.

Setting $\eta' = \eta^{-1} \in U_{r-\nu}$ it follows that this property is equivalent to

$$\mathbf{z}=\eta'\,\widehat{\mathbf{m}}\ mod\,p^{r-\nu}\,.$$

Since for fixed $\mathbf{m}$, $\eta'$, and a fixed representative $\tilde{\mathbf{z}}_0$ mod $p^{r-\nu}$ of $\eta'\,\widehat{\mathbf{m}}$ in $\mathbb{Z}^n_q$ there exist $p^{\nu n}$ other vectors $\tilde{\mathbf{z}}\in\mathbb{Z}^n_q$ such that

$$\{\tilde{\mathbf{z}}_0+p^{r-\nu}\tilde{\mathbf{z}}\}=\{\mathbf{z}\notin(p)^{(n)}\,mod\,q:\mathbf{z}=\eta'\widehat{\mathbf{m}}\ mod\,p^{r-\nu}\}\,,$$

it follows that if $\mathbf{z}_1' = \mathbf{z}_1$ then:

$$\begin{aligned}rhs(23)=\sum_{\nu=0}^{r-1}|U_{r-\nu}|\,p^{\nu n}\,c_{p,n}&=c_p\,c_{p,n}\,q\sum_{\nu=0}^{r-1}p^{\nu(n-1)}\\&=c_p\,c_{p,n}\,q\,p^{(r-1)(n-1)}\,(1-p^{-r(n-1)})\,(1-p^{-(n-1)})^{-1}\\&=[c_p\,c_{p,n}(1-p^{-r(n-1)})\,(1-p^{-(n-1)})^{-1}]\,q^n\,p^{-(n-1)}\\&=C_{p,r,n}\,q^n\,p^{-(n-1)}\,.\end{aligned}\qquad(25)$$

*If* $\mathbf{z}_1 \neq \mathbf{z}_1'$ it follows that if $\nu = ord_p\,\mathbf{m}_2$ then there exist $\eta_0 = \eta_0(\nu), \mu_0 = \mu_0(\nu) \in U_{r-\nu}$ such that (as equations in $\mathbb{Z}^n_q$)

$$\begin{aligned}\mathbf{m}_2\in\langle\mathbf{z}_1\rangle\cap\langle\mathbf{z}_1'\rangle\ &\Longrightarrow\mathbf{m}_2=p^\nu\,\widehat{\mathbf{m}}:=(p^\nu\,\eta_0)\cdot\mathbf{z}_1=(p^\nu\,\mu_0)\cdot\mathbf{z}_1'\\&\Longrightarrow\mathbf{z}_1'=\eta_0\,\mu_0^{-1}\,\mathbf{z}_1\ mod\,p^{r-\nu}.\end{aligned}\qquad(26)$$

Setting

$$\xi:=\eta_0\,\mu_0^{-1}\in U_{r-\nu}\,,$$

it is clear that in (26), the set of possible $\eta_0, \mu_0$ *consists of all units in* $U_{r-\nu}$ since $\mathbf{z}_1, \mathbf{z}_1'$ are independent elements of $\mathbb{Z}^n_q \setminus (p)^{(n)}$. As a result, the set of all possible $\xi$ *also equals* $U_{r-\nu}$ and (26) says the following:

$$\mathbf{m}_2\in\langle\mathbf{z}_1\rangle\cap\langle\mathbf{z}_1'\rangle\ \textit{and}\ \ \mathbf{m}_2:=p^\nu\,\eta_0\,\mathbf{z}_1=p^\nu\,\mu_0\,\mathbf{z}_1'\implies\mathbf{z}_1'=\xi\,\mathbf{z}_1\ mod\,p^{r-\nu}.\qquad(27)$$

In other words

$$\begin{aligned}&\mathbf{m}_2 \in \langle \mathbf{z}_1 \rangle \cap \langle \mathbf{z}_1' \rangle \\ &\implies \chi\langle \boldsymbol{\imath}(\mathbf{z}_1), -\mathbf{m}_2\rangle \cdot \chi\langle \boldsymbol{\imath}'(\mathbf{z}_1'), \mathbf{m}_2\rangle = \chi\left(p^{\nu}\,\mu_0\, j\,(1-\xi)\right)\; 1_{\{\mathbf{z}_1' = \xi\,\mathbf{z}_1(p^{r-\nu})\}}\,(\mathbf{z}_1, \mathbf{z}_1'). \end{aligned} \tag{28}$$

Setting, for each $\nu$ and $\xi \in U_{r-\nu}$,

$$N(\nu, \xi) := \sum_{\mathbf{z}_1, \mathbf{z}_1' \notin (p)^{(n)}} 1_{\{\mathbf{z}_1' = \xi\,\mathbf{z}_1(p^{r-\nu})\}}\,(\mathbf{z}_1, \mathbf{z}_1')\,,$$

it is elementary to see that

$$N(\nu, \xi) = c_{p,n}\, q^n\, p^{\nu n} \quad \textit{uniformly in } \xi \in U_{r-\nu}. \tag{29}$$

We now evaluate the contribution from those $\mathbf{z}_1 \neq \mathbf{z}_1'$ in (22) as follows:

$$\begin{aligned}&\sum_{\mathbf{m}_2 \neq \mathbf{0}} \sum_{\mathbf{z}_1 \neq \mathbf{z}_1' \notin (p)^{(n)}} \chi\langle \boldsymbol{\imath}(\mathbf{z}_1), -\mathbf{m}_2\rangle \cdot \chi\langle \boldsymbol{\imath}'(\mathbf{z}_1'), \mathbf{m}_2\rangle \cdot 1_{\langle \mathbf{z}_1\rangle \cap \langle \mathbf{z}_1'\rangle}(\mathbf{m}_2) \\ &\quad = \sum_{0 \le \nu \le r-1} \sum_{\mu, \xi \in U_{r-\nu}} \chi\left(p^{\nu}\, j\, \mu\,(1-\xi)\right)\; N(\nu, \xi) \\ &\quad = \sum_{0 \le \nu \le r-1} \sum_{\mu \in U_{r-\nu}} \chi\left(p^{\nu}\, j\, \mu\right)\; E_{\nu}(\mu) \end{aligned} \tag{30}$$

where

$$\begin{aligned} E_{\nu}(\mu) &= \sum_{\xi \in U_{r-\nu}} \chi(-p^{\nu}\, j\, \mu\, \xi)\, N(\nu, \xi) \\ &= c_{p,n}\, q^n\, p^{\nu n} \sum_{\xi \in U_{r-\nu}} \chi(-p^{\nu}\, j\, \mu\, \xi) \\ &= c_{p,n}\, q^n\, p^{\nu n} \sum_{\kappa \in U_{r-\nu}} \chi(p^{\nu}\, j\, \kappa)\,, \end{aligned} \tag{31}$$

where the last line is due to the fact that for each fixed $\mu$, $\{\mu\,\xi : \xi \in U_{r-\nu}\} = U_{r-\nu}$.

It is a standard fact (see [3], pg. 56) that there is considerable cancellation in the character sums as follows:

$$\sum_{\kappa \in U_{r-\nu}} \chi(p^{\nu}\, j\, \kappa) = \begin{cases} -1 & \text{if } \nu = r-1, \\ 0 & \text{if } \nu \le r-2. \end{cases} \tag{32}$$

Combining (30), (31) with (32) amounts to evaluating (30) at $r = n-1$. Then, combining this with (25), now tells us the following:

$$\begin{aligned} rhs(15) &= q^{-2n-2} \cdot \{C_{p,r,n}\, q^n\, p^{-(n-1)} + c_{p,n}\, q^{2n}\, p^{-n}\} \\ &= q^{-2}\, p^{-n} \cdot O(1) \quad \textit{uniformly in } r \ge 2 \textit{ and } p \gg 1. \end{aligned} \tag{33}$$

As a result we have now shown

$$\sum_{\mathbf{m}_2 \neq \mathbf{0}} |\widehat{1}_j(\mathbf{0}, \mathbf{m}_2)|^2 = q^{-2}\, p^{-n}\, O(1)\,. \tag{34}$$

Going back to the original error bound in (9) we conclude that there exists constants $P_I, C_I$ such that for all $r \geq 2$

$$p \geq P_I \implies \mathcal{E}_I^* \leq C_I\, q^n\, |E|\, \delta_E^{\frac{1}{2}}\, q^{-1}\, p^{-\frac{n}{2}} = C_I\, q^{\frac{n}{2}-1} p^{-\frac{n}{2}}\, |E|^{\frac{3}{2}}. \tag{35}$$

In this way we see some improvement in the upper bound from (13), having eliminated the $p^{1/4}$ factor.

2.2.3. Bound for $\mathcal{E}_{II}^*$ (see (50)). The method is similar to that in Section 2.2.2, but the estimate we get (see (50)) is rather different in form to the bound in (35). The reason for this seems to be due to the fact that the behavior of the factor in the summation over $\mathbf{x}_2$ in (44) depends upon $ord_p\,(1-\xi)$, i.e., it is evidently *not uniform* in the variable $\xi$.

As a result, it will suffice to emphasize in this section the details that differ from those in the preceding section (see Remark 2.2 in particular).

Defining (see (4)) for each $\mathbf{m}_1 \neq \mathbf{0}$

$$\mathcal{F}(\mathbf{m}_1) = \sum_{\mathbf{m}_2 \in \mathbb{Z}_q^n} \widehat{1}_E(\mathbf{m}_2)\, \widehat{1}_j(\mathbf{m}_1, \mathbf{m}_2), \tag{36}$$

an application of Cauchy-Schwarz and Plancherel's Theorem, as with $\mathcal{E}_I^*$, first tells us that

$$\begin{aligned} \mathcal{E}_{II}^* \leq & q^{2n} \cdot \left( \sum_{\mathbf{m}_1 \neq \mathbf{0}} |\widehat{1}_E(\mathbf{m}_1)|^2 \right)^{1/2} \cdot \left( \sum_{\mathbf{m}_1 \neq \mathbf{0}} |\mathcal{F}(\mathbf{m}_1)|^2 \right)^{1/2} \\ \leq & q^{2n} \cdot \delta_E^{1/2} \cdot \left( \sum_{\mathbf{m}_1 \neq \mathbf{0}} \mathcal{F}(\mathbf{m}_1) \cdot \overline{\mathcal{F}(\mathbf{m}_1)} \right)^{1/2}. \end{aligned} \tag{37}$$

The second step is to rewrite, for each $\mathbf{m}_1 \neq \mathbf{0}$, the factors in the sum (37) using the Fourier transform definition. This gives the following, in which we have set $\boldsymbol{z} := (\mathbf{z}_1, \mathbf{z}_2), \boldsymbol{z}' := (\mathbf{z}_1', \mathbf{z}_2')$, and used the fact that $\overline{\mathcal{F}(\mathbf{m}_1)} = \sum_{\mathbf{m}_2'} \widehat{1}_E(-\mathbf{m}_2')\, \widehat{1}_j(-\mathbf{m}_1, -\mathbf{m}_2')$:

$$\begin{aligned} F(\mathbf{m}_1) \cdot \overline{\mathcal{F}(\mathbf{m}_1)} = & q^{-6n} \cdot \sum_{\mathbf{m}_2, \mathbf{m}_2'} \left\{ \left( \sum_{\mathbf{x}_2} 1_E(\mathbf{x}_2)\, \chi\langle \mathbf{x}_2, -\mathbf{m}_2 \rangle \right) \cdot \left( \sum_{\mathbf{x}_2'} 1_E(\mathbf{x}_2')\, \chi\langle \mathbf{x}_2', \mathbf{m}_2' \rangle \right) \right. \\ & \left. \cdot \left( \sum_{\boldsymbol{z}} 1_j(\boldsymbol{z})\, \chi\langle \boldsymbol{z}, -(\mathbf{m}_1, \mathbf{m}_2) \rangle \right) \cdot \left( \sum_{\boldsymbol{z}'} 1_j(\boldsymbol{z}')\, \chi\langle \boldsymbol{z}', (\mathbf{m}_1, \mathbf{m}_2') \rangle \right) \right\}. \end{aligned} \tag{38}$$

In the third step we interchange the sums over $\mathbf{m}_2, \mathbf{m}_2'$ with those over $\mathbf{x}_2, \boldsymbol{z}, \mathbf{x}_2', \boldsymbol{z}'$. This then gives:

$$\begin{aligned} \mathcal{F}(\mathbf{m}_1) \cdot \overline{\mathcal{F}(\mathbf{m}_1)} = & q^{-6n} \cdot \left\{ \sum_{\mathbf{x}_2, \boldsymbol{z}} 1_E(\mathbf{x}_2)\, 1_j(\boldsymbol{z})\, \chi\langle \mathbf{z}_1, -\mathbf{m}_1 \rangle \cdot \left( \sum_{\mathbf{m}_2} \chi\langle \mathbf{x}_2 + \mathbf{z}_2, -\mathbf{m}_2 \rangle \right) \right. \\ & \left. \cdot \sum_{\mathbf{x}_2', \boldsymbol{z}'} 1_E(\mathbf{x}_2')\, 1_j(\boldsymbol{z}')\, \chi\langle \mathbf{z}_1', \mathbf{m}_1 \rangle \cdot \left( \sum_{\mathbf{m}_2'} \chi\langle \mathbf{x}_2' + \mathbf{z}_2', \mathbf{m}_2' \rangle \right) \right. . \end{aligned} \tag{39}$$

Since the sums over $\mathbf{m}_2, \mathbf{m}_2'$ are *complete* exponential sums over $\mathbb{Z}_q^n$, it now follows that

$$\sum_{\mathbf{m}_2} \chi\langle \mathbf{x}_2 + \mathbf{z}_2, -\mathbf{m}_2\rangle = q^n \cdot 1_{\{\mathbf{x}_2+\mathbf{z}_2=\mathbf{0}\}}(\mathbf{x}_2, \mathbf{z}_2),$$

and

$$\sum_{\mathbf{m}_2'} \chi\langle \mathbf{x}_2' + \mathbf{z}_2', \mathbf{m}_2'\rangle = q^n \cdot 1_{\{\mathbf{x}_2'+\mathbf{z}_2'=\mathbf{0}\}}(\mathbf{x}_2', \mathbf{z}_2')\,.$$

Substituting the right sides into (39) and simplifying a bit then shows:

$$\mathcal{F}(\mathbf{m}_1) \cdot \overline{\mathcal{F}(\mathbf{m}_1)} = q^{-4n} \cdot II(\mathbf{m}_1) \cdot II'(\mathbf{m}_1), \tag{40}$$

where

$$II(\mathbf{m}_1) := \sum_{\mathbf{x}_2,\mathbf{z}_1} 1_E(\mathbf{x}_2)\, 1_j(\mathbf{z}_1, -\mathbf{x}_2)\, \chi\langle \mathbf{z}_1, -\mathbf{m}_1\rangle,$$

and

$$II'(\mathbf{m}_1) := \sum_{\mathbf{x}_2',\mathbf{z}_1'} 1_E(\mathbf{x}_2')\, 1_j(\mathbf{z}_1', -\mathbf{x}_2')\, \chi\langle \mathbf{z}_1', \mathbf{m}_1\rangle\,.$$

We can now compare these expressions with those in (14) since the right sides can be rewritten as follows

$$\sum_{\mathbf{x}_2,\mathbf{z}_1} 1_E(\mathbf{x}_2)\, 1_j(\mathbf{z}_1, -\mathbf{x}_2)\, \chi\langle \mathbf{z}_1, -\mathbf{m}_1\rangle = \sum_{\mathbf{x}_2} 1_E(\mathbf{x}_2) \cdot \left( \sum_{\mathbf{z}_1} 1_j(\mathbf{z}_1, -\mathbf{x}_2)\, \chi\langle \mathbf{z}_1, -\mathbf{m}_1\rangle \right)$$

$$\sum_{\mathbf{x}_2',\mathbf{z}_1'} 1_E(\mathbf{x}_2')\, 1_j(\mathbf{z}_1', -\mathbf{x}_2')\, \chi\langle \mathbf{z}_1', \mathbf{m}_1\rangle = \sum_{\mathbf{x}_2'} 1_E(\mathbf{x}_2') \cdot \left( \sum_{\mathbf{z}_1'} 1_j(\mathbf{z}_1', -\mathbf{x}_2')\, \chi\langle \mathbf{z}_1', \mathbf{m}_1\rangle \right)\,.$$

Adapting the idea from Section 2.2.2, for each $\mathbf{x}_2, \mathbf{x}_2'$, we note that the sums over $\mathbf{z}_1, \mathbf{z}_1'$ are, by definition, concentrated on the following two affine subspaces of $\mathbb{Z}_q^n$, *which can only be nonempty when* $\mathbf{x}_2, \mathbf{x}_2' \notin (p)^{(n)}$ *since* $j \in U_q$ :

$$\begin{aligned}
\mathcal{H}_j(\mathbf{x}_2) :=& \{\mathbf{z}_1 : \langle \mathbf{z}_1, -\mathbf{x}_2\rangle = j\} = \widetilde{\mathbf{z}}_1(\mathbf{x}_2) + \mathcal{K}(\mathbf{x}_2);\\
\mathcal{H}_j'(\mathbf{x}_2') :=& \{\mathbf{z}_1' : \langle \mathbf{z}_1', -\mathbf{x}_2'\rangle = j\} = \widetilde{\mathbf{z}}_1'(\mathbf{x}_2') + \mathcal{K}(\mathbf{x}_2')\,,
\end{aligned}$$

where $\mathcal{K}(\mathbf{x}_2)$ resp. $\mathcal{K}(\mathbf{x}_2')$ denotes the linear subspaces on which $\mathbf{z}_1 \to \langle \mathbf{z}_1, -\mathbf{x}_2\rangle$ resp. $\mathbf{z}_1' \to \langle \mathbf{z}_1', -\mathbf{x}_2'\rangle$ *vanishes*, and $\widetilde{\mathbf{z}}_1(\mathbf{x}_2)$ resp. $\widetilde{\mathbf{z}}_1'(\mathbf{x}_2')$ denotes a particular solution of

$$\langle \mathbf{z}_1, -\mathbf{x}_2\rangle = j \quad \textit{resp.} \quad \langle \mathbf{z}_1', -\mathbf{x}_2'\rangle = j\,.$$

Exactly as in (19), (21)

$$\boldsymbol{x} \in \{\mathbf{x}_2, \mathbf{x}_2'\} \implies \sum_{\mathbf{w}\in\mathcal{K}(\boldsymbol{x})} \chi\langle \mathbf{w}, \mathbf{v}\rangle = \begin{cases} q^{n-1} & \textit{if } \mathbf{v} \in \langle \boldsymbol{x}\rangle \\ 0 & \textit{if not.} \end{cases} \tag{41}$$

When $\mathbf{v} = \pm\mathbf{m}_1$ we apply this for any $\mathbf{x}_2, \mathbf{x}_2'$ and conclude:

$$\sum_{\mathbf{z}_1} 1_j(\mathbf{z}_1, -\mathbf{x}_2)\, \chi\langle \mathbf{z}_1, -\mathbf{m}_1\rangle = q^{n-1} \cdot \chi\langle \widetilde{\mathbf{z}}_1(\mathbf{x}_2), -\mathbf{m}_1\rangle \cdot 1_{\langle \mathbf{x}_2\rangle}(\mathbf{m}_1)\,,$$

$$\sum_{\mathbf{z}_1'} 1_j(\mathbf{z}_1', -\mathbf{x}_2')\,\chi\langle \mathbf{z}_1', \mathbf{m}_1\rangle = q^{n-1}\cdot \chi\langle \widetilde{\mathbf{z}}_1'(\mathbf{x}_2'), \mathbf{m}_1\rangle \cdot 1_{\langle \mathbf{x}_2'\rangle}(\mathbf{m}_1)\,. \tag{42}$$

Given that $\nu := ord_p\,\mathbf{m}_1 \in [0, r-1]$ we follow the same method from Section 2.2.2 by using the fact that $ord_p\,\mathbf{x}_2 = ord_p\,\mathbf{x}_2' = 0$. Thus, there exist units $\eta = \eta(\mathbf{m}_1, \mathbf{x}_2)$, $\mu = \mu(\mathbf{m}_1, \mathbf{x}_2') \in U_{r-\nu}$ and $\widehat{\mathbf{m}}_1 \in \mathbb{Z}_{r-\nu}^n$ with $ord_p\,\widehat{\mathbf{m}}_1 = 0$ such that

(i) $\mathbf{m}_1 \in \langle \mathbf{x}_2\rangle \cap \langle \mathbf{x}_2'\rangle \iff$
$\widehat{\mathbf{m}}_1 = \eta\,\mathbf{x}_2 \ mod\, p^{r-\nu}$; $\widehat{\mathbf{m}}_1 = \mu\,\mathbf{x}_2' \ mod\, p^{r-\nu}$; $\mathbf{x}_2' = \mu\,\eta^{-1}\mathbf{x}_2 \ mod\, p^{r-\nu}$;

(ii) $\chi\langle \widetilde{\mathbf{z}}_1(\mathbf{x}_2), -\mathbf{m}_1\rangle = \chi\left(-p^\nu\,\eta\,j\right)$ *and* $\chi\langle \widetilde{\mathbf{z}}_1'(\mathbf{x}_2'), \mathbf{m}_1\rangle = \chi\left(p^\nu\,\mu\,j\right)$ .

Defining next

$$\xi = \eta\,\mu^{-1} \in U_{r-\nu}\,,$$

it will also be convenient (see Remark 2.3 below) to think of $\xi$ as a unit in $U_q$ as well by setting

$$\widehat{\xi} = \xi_0 + p\xi_1 + \cdots + p^{r-\nu-1}\xi_{r-\nu-1} + (p^{r-\nu}0 + \cdots + p^{r-1}0). \tag{43}$$

Such a unit of $U_q$ can be thought of as the "canonical lift" of $\xi$ to $U_q$.

We then combine (40) with (i), (ii) and the other preliminary remarks, to understand more precisely the sum over $\mathbf{m}_1 \neq \mathbf{0}$ in (37). Arguing as in Section 2.2.2, we have the following:

$$\begin{aligned}\sum_{\mathbf{m}_1\neq\mathbf{0}} \mathcal{F}(\mathbf{m}_1)\cdot\overline{\mathcal{F}(\mathbf{m}_1)} &= q^{-4n}\cdot \sum_{\mathbf{m}_1\neq\mathbf{0}} \left\{ \sum_{\mathbf{x}_2,\mathbf{x}_2'} 1_E(\mathbf{x}_2)\,1_E(\mathbf{x}_2') \left(\sum_{\mathbf{z}_1} 1_j(\mathbf{z}_1, -\mathbf{x}_2)\chi\langle \mathbf{z}_1, -\mathbf{m}_1\rangle\right)\right. \\ &\qquad \left.\cdot \left(\sum_{\mathbf{z}_1'} 1_j(\mathbf{z}_1', -\mathbf{x}_2')\chi\langle \mathbf{z}_1', \mathbf{m}_1\rangle\right)\right\} \qquad (44)\\ &= q^{-2n-2}\cdot \sum_{\nu=0}^{r-1} \sum_{\eta,\mu\in U_{r-\nu}} \left\{ \sum_{\substack{\mathbf{x}_2,\mathbf{x}_2'\notin(p)^{(n)}\\ \mathbf{x}_2'=\mu\eta^{-1}\mathbf{x}_2\,(p^{r-\nu})}} 1_E(\mathbf{x}_2)\,1_E(\mathbf{x}_2')\chi\left(p^\nu\,j\,(\mu-\eta)\right)\right\} \\ &= q^{-2n-2}\cdot \sum_{\nu=0}^{r-1} \sum_{\mu,\xi\in U_{r-\nu}} \left\{ \sum_{\substack{\mathbf{x}_2,\mathbf{x}_2'\notin(p)^{(n)}\\ \mathbf{x}_2'=\xi\mathbf{x}_2\,(p^{r-\nu})}} 1_E(\mathbf{x}_2)\,1_E(\mathbf{x}_2')\,\chi\left(p^\nu\,\mu\,j\,(1-\xi)\right)\right\} \\ &= q^{-2n-2}\cdot \sum_{\nu=0}^{r-1} \sum_{\xi\in U_{r-\nu}} N_E(\nu,\xi)\,\mathcal{E}(\nu,\xi)\,. \qquad (45)\end{aligned}$$

where

$$N_E(\nu,\xi) = \sum_{\substack{\mathbf{x}_2,\mathbf{x}_2'\notin(p)^{(n)}\\ \mathbf{x}_2'=\xi\mathbf{x}_2\,(p^{r-\nu})}} 1_E(\mathbf{x}_2)\,1_E(\mathbf{x}_2') \quad \text{and} \quad \mathcal{E}(\nu,\xi) := \sum_{\mu\in U_{r-\nu}} \chi\left(p^\nu\,j\,\mu\,(1-\xi)\right)\,.$$

Unlike the argument in Section 2.2.2, there is no uniform in $\xi$ bound for the double sum over $\mathbf{x}_2, \mathbf{x}_2'$.

To overcome this issue, we must first sum over $\mu$ for each fixed $\xi$. To do this, we first set, for any $\xi \in U_{r-\nu}$,

$$\rho(\xi) = 1 - \xi \in \mathbb{Z}_{p^{r-\nu}}\,; \quad \kappa = ord_p\,\rho(\xi)\,; \quad \rho(\xi) = p^{\kappa}\,\widehat{\rho}(\xi) \qquad where \quad \widehat{\rho}(\xi) \in U_{r-\nu-\kappa}\,,$$

where it is understood that $\kappa \le r-\nu$ with equality iff $\xi = 1$. We then break up the sum over $\xi$ according to the value of $\kappa$. It then follows that

$$\sum_{\mathbf{m}_1 \neq \mathbf{0}} \mathcal{F}(\mathbf{m}_1) \cdot \overline{\mathcal{F}(\mathbf{m}_1)} = q^{-2n-2} \sum_{0 \le \nu \le r-1} \sum_{\kappa \le r-\nu} \sum_{\substack{\xi \in U_{r-\nu} \\ ord_p\,\rho(\xi) = \kappa}} N_E(\nu,\xi)\,\mathcal{E}(\nu,\kappa,\xi) \tag{46}$$

where

$$\mathcal{E}(\nu,\kappa,\xi) = \sum_{\mu \in U_{r-\nu}} \chi\left(p^{\nu+\kappa}\, j\, \mu\, \widehat{\rho}(\xi)\right)\,.$$

It is now evident that the character sum evaluations in (32) apply to each $\mathcal{E}(\nu,\kappa,\xi)$. In particular, for given $\nu$ there is a nonzero contribution only when $\kappa \in \{r-\nu-1, r-\nu\}$, in which event it follows that

$$(44) = q^{-2n-2} \sum_{0 \le \nu \le r-1} (A(\nu) + B(\nu))$$

where

$$\begin{aligned} A(\nu) =& \sum_{\substack{\xi \in U_{r-\nu} \\ \xi = 1 + p^{r-\nu-1}\hat{\rho}_{r-\nu-1}(\xi) \\ \hat{\rho}_{r-\nu-1}(\xi) \in U_1}} N_E(\nu,\xi) \sum_{\mu \in U_{r-\nu}} \chi\left(p^{r-1}\, j\, \mu\, \widehat{\rho}_{r-\nu-1}(\xi)\right) \\ =& (-q\,p^{-\nu-1}) \sum_{\substack{\xi \in U_{r-\nu} \\ \xi = 1 + p^{r-\nu-1}\hat{\rho}_{r-\nu-1}(\xi) \\ \hat{\rho}_{r-\nu-1}(\xi) \in U_1}} N_E(\nu,\xi) \quad (\textstyle\sum_{\mu \in U_{r-\nu}}(\cdot)\ is\ uniform\ in\ \xi), \\ B(\nu) =& |U_{r-\nu}| \sum_{\substack{\mathbf{x}_2, \mathbf{x}_2' \notin (p)^{(n)} \\ \mathbf{x}_2' = \mathbf{x}_2\,(p^{r-\nu})}} 1_E(\mathbf{x}_2)\, 1_E(\mathbf{x}_2') \le c_p\, q\, p^{\nu(n-1)}\, |E|\,. \end{aligned}$$

For $\nu \ge 1$ we denote the coset mod $p^{r-\nu}$ of any vector $\mathbf{z} \in \mathbb{Z}_q^n$ by

$$[\mathbf{z}]_{r-\nu} = \{\mathbf{y} \in \mathbb{Z}_q^n : \mathbf{y} = \mathbf{z}\,(p^{r-\nu})\}\,.$$

Then, for each $\mathbf{x}_2 \notin (p)^{(n)}$ and $\hat{\xi} \in U_q$, the canonical lift of $\xi \in U_{r-\nu}$ (see (43)), it follows that

$$\begin{aligned} \sum_{\substack{\xi \in U_{r-\nu} \\ \xi = 1 + p^{r-\nu-1}\hat{\rho}_{r-\nu-1}(\xi) \\ \hat{\rho}_{r-\nu-1}(\xi) \in U_1}} N_E(\nu,\xi) :=& \sum_{\mathbf{x}_2 \notin (p)^{(n)}} 1_E(\mathbf{x}_2) \left( \sum_{\substack{\xi \in U_{r-\nu} \\ \xi = 1 + p^{r-\nu-1}\hat{\rho}_{r-\nu-1}(\xi) \\ \hat{\rho}_{r-\nu-1}(\xi) \in U_1}} \sum_{\mathbf{z} \in [\hat{\xi}\,\mathbf{x}_2]_{r-\nu}} 1_E(\mathbf{z}) \right) \\ \le& c_p\, p^{n\nu+1}\, |E| \quad (since\ |U_1| = p-1). \end{aligned} \tag{47}$$

This extends trivially to the case $\nu = 0$ since in that event each congruence $\mathbf{x}_2' = \xi\,\mathbf{x}_2\,(p^r)$ has but one solution. From this it is easy to verify that

$$\sum_{0\le\nu\le r-1} B(\nu) \le c_p\, q\, |E| \sum_{\nu=0}^{r-1} p^{\nu(n-1)} = q^n\, p^{-(n-1)}\, |E|\, O(1)$$

$$\left| \sum_{0\le\nu\le r-1} A(\nu) \right| \le \sum_{0\le\nu\le r-1} |A(\nu)| \le q\, p^{-1}\, |E| \sum_{\nu=0}^{r-1} p^{\nu(n-1)} = q^n\, p^{-n}\, |E|\, O(1)\,. \tag{48}$$

As a result, we have shown the existence of a constant $C_{II}$ which is uniform in $p \gg 1$ and $r \ge 2$ such that

$$\left( \sum_{\mathbf{m}_1 \neq \mathbf{0}} \mathcal{F}(\mathbf{m}_1) \cdot \overline{\mathcal{F}(\mathbf{m}_1)} \right)^{1/2} \le C_{II}\, q^{-\frac{n}{2}-1}\, p^{-\frac{n-1}{2}}\, |E|^{\frac{1}{2}}\,, \tag{49}$$

from which (37) now implies:

*There exist constants $P_{II}$ and $C_{II}$ such that for all $r \ge 2$ and $j$:*

$$p \ge P_{II} \implies \mathcal{E}^*_{II} \le C_{II}\, q^{n-1}\, p^{-\frac{n-1}{2}}\, |E|\,. \tag{50}$$

**Remark 2.2.** The fact that this argument gives the factor $|E|$ in (50), *not* $|E|^{3/2}$ (as in (13)), is crucial for the proof of Theorem 1.1

**Remark 2.3.** One could only hope to improve upon this if one knew something more precise about the function

$$\xi \longrightarrow \left| \{\mathbf{x}' \in E : \mathbf{x}' = \xi \mathbf{x}\,(p^{r-\nu}) \text{ for some } \mathbf{x} \in E\} \right|.$$

To that end, and with a sharpening in mind (see Section 3) whenever $E$ is replaced by

$$E_v := E \cap S_v \qquad \text{for some } v \in U_q\,,$$

which will be used in Section 3, it is useful to point out here how (50) can be improved in that event.

We first note that (see (47)) for any $1 \le \nu \le r-1$ and $\xi \in U_{r-\nu}$ such that $1 - \xi = p^{r-\nu-1}\,\widehat{\rho}(\xi)$ with $\widehat{\rho}(\xi) \in U_1$ :

$$\begin{aligned} &\mathbf{x}_2' = \xi\,\mathbf{x}_2\,(p^{r-\nu}) \ \text{ and } \ 1_{E_v}(\mathbf{x}_2') = 1_{E_v}(\mathbf{x}_2) = 1 \\ &\implies \mathbf{x}_2' \in [\hat{\xi}\,\mathbf{x}_2]_{r-\nu} = \{\hat{\xi}\,\mathbf{x}_2 + p^{r-\nu}\mathbf{y} : \mathbf{y} = \mathbf{y}_0 + p\,\mathbf{y}_1 + \cdots + p^{\nu-1}\mathbf{y}_{\nu-1} \in \mathbb{Z}_{p^\nu}^n\} \\ &\implies v(1-\hat{\xi}^2) = p^{r-\nu}\left(2\,\hat{\xi}\,\langle \mathbf{x}_2, \mathbf{y}\rangle + p^{r-\nu}\|\mathbf{y}\|\right) \qquad (\textit{an equation in } \mathbb{Z}_q)\,. \end{aligned} \tag{51}$$

As a result, if $\mathbf{x}_2' = \hat{\xi}\,\mathbf{x}_2 + p^{r-\nu}\mathbf{y}$ satisfies $1_{E_v}(\mathbf{x}_2') = 1$ then $p^{r-\nu} | v(1-\hat{\xi}^2)$ in $\mathbb{Z}_q$.

On the other hand, since $\xi \neq 1\,(p^{r-\nu})$ it follows that

$$\hat{\xi}^2 = (1 - p^{r-\nu-1}\hat{\rho}(\xi))^2 = 1 - 2\hat{\rho}(\xi)\,p^{r-\nu-1}\ (p^{r-\nu}) \neq 1\ (p^{r-\nu}).$$

In other words, it is *not* possible that

$$v(1-\hat{\xi}^2) = 0\,(p^{r-\nu}).$$

This now tells us that whenever $E$ is replaced by $E_v$ in (36) then

$$(44) = q^{-2n-2} \sum_{0\le\nu\le r-1} (A(\nu)+B(\nu)) = \sum_{0\le\nu\le r-1} B(\nu)\,,$$

that is, only each $B(\nu)$, when $\xi = 1\,(p^{r-\nu})$ can effectively contribute.

From this we now conclude that any $\mathbf{y}$ appearing in (51) *must then satisfy the congruence*

$$0 = 2\,\langle \mathbf{x}_2, \mathbf{y}\rangle + p^{r-\nu}\|\mathbf{y}\|\ (p^\nu). \tag{52}$$

This condition determines a non singular hypersurface in $\mathbb{Z}_{p^\nu}^n$ since the linear part is not identically zero, given that $\mathbf{x}_2 \notin (p)^{(n)}$.

Applying the standard method, via Hensel's Lemma, of lifting solutions mod $p$ to solutions mod $p^\nu$, which is possible because the linear part $\mathbf{y} \to \langle \mathbf{x}_2, \mathbf{y}\rangle$ is non zero mod $p$, it follows that

$$|\{\mathbf{y} \in \mathbb{Z}_{p^\nu}^n : (52) \text{ holds } \}| = O(p^{\nu(n-1)}). \tag{53}$$

As a result, for any $v \in U_q$, when we replace $E$ by $E_v$ in the definition (36) of $\mathcal{F}(\mathbf{m}_1)$, (47) - (49) can then be improved as follows:

$$\sum_{0\le\nu\le r-1} B(\nu) \le c_p\, q\, |E_v|\, \sum_{\nu=0}^{r-1} p^{\nu(n-2)} = q^{n-1}\, p^{-(n-2)}\, |E_v|\, O(1)$$

$$\left(\sum_{\mathbf{m}_1\neq\mathbf{0}} \mathcal{F}(\mathbf{m}_1)\cdot\overline{\mathcal{F}(\mathbf{m}_1)}\right)^{1/2} \le C_{II}\, q^{-\frac{n}{2}-\frac{3}{2}}\, p^{-\frac{n-2}{2}}\, |E_v|^{\frac{1}{2}} \ \textit{(when } E = E_v \textit{ in (36))}\,. \tag{54}$$

2.2.4. Finishing the proof of Theorem 1.1 . The proof of Theorem 1.1 is now very easy.

We must compare the bound for $\mathcal{E}_I^*$ in (35) with that for $\mathcal{E}_{II}^*$ from (50) when $p$ is sufficiently large and $r \ge 2$. To that end, we first observe :

$$C_{II}\, q^{n-1}\, p^{-\frac{n-1}{2}}\, |E| < C_I\, q^{\frac{n}{2}-1} p^{-\frac{n}{2}}\, |E|^{\frac{3}{2}} \quad \textit{iff} \quad \delta_E \ge p\left(\frac{C_{II}}{C_I}\right)^2. \tag{55}$$

Since $\delta_E \le 1$ this cannot occur for $p$ sufficiently large. So it suffices to understand under what conditions is it the case that

$$\mathcal{M}^* > 2\, C_{II}\, q^{n-1}\, p^{-\frac{n-1}{2}}\, |E| \ge 2\,\mathcal{E}_{II}^* \ge \mathcal{E}_I^* + \mathcal{E}_{II}^* = \mathcal{E}^*.$$

It is clear that this occurs if

$$\delta_E > 2\, C_{II}\, p^{-\frac{n-1}{2}}.$$

This now completes the proof of the assertion:

$$\exists\ C > 0 \quad s.t. \quad p \gg 1 \quad \textit{and} \quad \delta_E \ge C\, p^{-\frac{n-1}{2}} \implies \mathcal{M}^* > \mathcal{E}^* \quad \textit{if} \quad n, r \ge 2. \tag{56}$$

## 3. Proof of Theorem 1.2

Recalling the definition of $\mathbf{\Sigma}_{\mathbf{v},j}(E)$ from the Introduction, it is clear that

$$\sigma_{\mathbf{v},j}(E) := |\,\mathbf{\Sigma}_{\mathbf{v},j}(E)\,| = \sum_{\boldsymbol{x}=(\mathbf{x}_1,\mathbf{x}_2)\in\mathbb{Z}_q^{2n}} 1_{E,v_1}(\mathbf{x}_1)\cdot 1_{E,v_2}(\mathbf{x}_2)\cdot 1_j(\boldsymbol{x})\,, \tag{57}$$

where for each $u$

$$1_{E,v_u}(\mathbf{x}_u) = 1_E(\mathbf{x}_u)\cdot 1_{S_{v_u}}(\mathbf{x}_u),$$

is the characteristic function of $E_{v_u} := E\cap S_{v_u}$.

Applying Fourier inversion as in Section 2.2.1, it follows that

$$\begin{aligned}\sigma_{\mathbf{v},j}(E) =& \sum_{\boldsymbol{m}=(\mathbf{m}_1,\mathbf{m}_2)} \widehat{1}_j(\boldsymbol{m}) \sum_{\boldsymbol{x}=(\mathbf{x}_1,\mathbf{x}_2)\in\mathbb{Z}_q^{2n}} 1_{E,v_1}(\mathbf{x}_1)\cdot 1_{E,v_2}(\mathbf{x}_2)\cdot \chi\langle \boldsymbol{x},\boldsymbol{m}\rangle \\ =& q^{2n}\cdot \sum_{\boldsymbol{m}=(\mathbf{m}_1,\mathbf{m}_2)} \widehat{1}_j(\boldsymbol{m})\cdot \widehat{1}_{E,v_1}(-\mathbf{m}_1)\cdot \widehat{1}_{E,v_2}(-\mathbf{m}_2) := \mathcal{M}^*_{\mathbf{v},j} + \mathcal{E}^*_{\mathbf{v},j},\end{aligned} \tag{58}$$

where (see (7))

$$\begin{aligned}\mathcal{M}^*_{\mathbf{v},j} :=& q^{2n}\cdot \widehat{1}_j(\mathbf{0},\mathbf{0})\cdot \widehat{1}_{E,v_1}(\mathbf{0})\cdot \widehat{1}_{E,v_2}(\mathbf{0}) = \frac{|E_{v_1}|\cdot|E_{v_2}|}{q}\cdot\Big(1+O(p^{-\frac{2n-1}{2}})\Big) \\ \mathcal{E}^*_{\mathbf{v},j} :=& q^{2n}\cdot \sum_{\boldsymbol{m}\neq(\mathbf{0},\mathbf{0})} \widehat{1}_j(\boldsymbol{m})\cdot \widehat{1}_{E,v_1}(-\mathbf{m}_1)\cdot \widehat{1}_{E,v_2}(-\mathbf{m}_2) \\ =& q^{2n}\cdot\Big\{\widehat{1}_{E,v_1}(\mathbf{0})\cdot \sum_{\mathbf{m}_2\neq\mathbf{0}} \widehat{1}_j(\mathbf{0},\mathbf{m}_2)\cdot \widehat{1}_{E,v_2}(-\mathbf{m}_2) \\ &\quad + \sum_{\mathbf{m}_1\neq\mathbf{0}}\sum_{\mathbf{m}_2} \widehat{1}_j(\boldsymbol{m})\cdot \widehat{1}_{E,v_1}(-\mathbf{m}_1)\cdot \widehat{1}_{E,v_2}(-\mathbf{m}_2)\Big\} \\ :=& q^{2n}\cdot\Big[\delta_{E_{v_1}}\cdot \sum_{\mathbf{m}_2\neq\mathbf{0}} I_{v_2,j}(\mathbf{m}_2) + \sum_{\mathbf{m}_1\neq\mathbf{0}}\sum_{\mathbf{m}_2} II_{\mathbf{v},j}(\boldsymbol{m})\Big]. \\ :=& \mathcal{E}^*_I + \mathcal{E}^*_{II}.\end{aligned} \tag{59}$$

The extension of (35) to bound $\mathcal{E}^*_I$ is straightforward. It suffices to replace $\widehat{1}_E(\mathbf{m}_2)$ in the applications of Cauchy-Schwarz and Plancherel in (9) by $\widehat{1}_{E,v_2}$, in which event the factor $\delta_E^{1/2}$ should change to $\delta_{E_{v_2}}^{1/2}$. Furthermore, the definitions of $P_I, c_I$ in Remark 1 remain unchanged.

We then know that

$$p\geq P_I \implies \mathcal{E}^*_I \leq C_I\, q^n\,|E_{v_1}|\,\delta_{E_{v_2}}^{\frac{1}{2}}\,q^{-1}\,p^{-\frac{n}{2}} = C_I\, q^{\frac{n}{2}-1}p^{-\frac{n}{2}}\,|E_{v_1}||E_{v_2}|^{\frac{1}{2}} := \mathcal{B}^*_I\,. \tag{60}$$

Moreover, unlike the situation in Section 2.2.1, where the choice is made to fix $\mathbf{m}_1=\mathbf{0}$ and leads to a bound that is independent of this choice, in this section there are actually two possible choices to be made of that index $\iota$ for which $\mathbf{m}_\iota=\mathbf{0}$. In other words, there is a second possible bound as follows:

$$p\geq P_I \implies \mathcal{E}^*_I \leq C'_I\, q^n\,|E_{v_2}|\,\delta_{E_{v_1}}^{\frac{1}{2}}\,q^{-1}\,p^{-\frac{n}{2}} = C'_I\, q^{\frac{n}{2}-1}p^{-\frac{n}{2}}\,|E_{v_2}||E_{v_1}|^{\frac{1}{2}} := \widetilde{\mathcal{B}}^*_I\,. \tag{61}$$

The extension of (50) to bound $\mathcal{E}^*_{II}$, given that one has decided to fix $\mathbf{m}_1 = 0$ to define $\mathcal{E}^*_I$, is also straightforward and similarly achieved by replacing $\widehat{1}_E(\mathbf{m}_1)$ resp. $\widehat{1}_E(\mathbf{m}_2)$ wherever either function appears in the discussion of Section 2.2.3 by $\widehat{1}_{E,v_1}(\mathbf{m}_1)$ resp. $\widehat{1}_{E,v_2}(\mathbf{m}_2)$. Applying the bounds (54) from Remark 2.3, we conclude as follows:

There exist $P_{II}$ and $C_{II}$ uniform in $r \geq 2$ and $\mathbf{v}, j$ such that :

$$p \geq P_{II} \implies \mathcal{E}^*_{II} \leq C_{II}\, q^{n-\frac{3}{2}}\, p^{-\frac{n-2}{2}}\, |E_{v_1}|^{\frac{1}{2}}\, |E_{v_2}|^{\frac{1}{2}} := \mathcal{B}^*_{II}\,. \tag{62}$$

Note that this bound is actually *independent* of the choice to fix $\mathbf{m}_1 = \mathbf{0}$ in the definition of $\mathcal{E}^*_I$. That is, *exactly the same estimate holds* if we had chosen to define $\mathcal{E}^*_I$ by setting $\mathbf{m}_2 = \mathbf{0}$. The main point here is that *the exponent of each* $|E_{v_u}|$ *in* $\mathcal{B}^*_{II}$ *equals* $1/2$ *and is independent of the choice made to define* $\mathcal{E}^*_I$.

As a result, the single choice to make concerns whether $\mathcal{B}^*_I$ is *at least* resp. *at most* $\widetilde{\mathcal{B}}^*_I$. This is evidently equivalent to

$$(a)\ \delta_{E_{v_1}} \geq \delta_{E_{v_2}} \quad \text{resp.} \quad (b)\ \delta_{E_{v_1}} \leq \delta_{E_{v_2}}.$$

If (a) occurs, then $\widetilde{\mathcal{B}}^*_I$ is better (i.e. smaller) than $\mathcal{B}^*_I$, so we should next compare $\widetilde{\mathcal{B}}^*_I$ to $\mathcal{B}^*_{II}$. To that end we note that

$$\mathcal{B}^*_{II} \leq \widetilde{\mathcal{B}}^*_I \quad \textit{iff} \quad C_{II}\, q^{n-\frac{3}{2}}\, p^{-\frac{n-2}{2}}\, |E_{v_1}|^{\frac{1}{2}}\, |E_{v_2}|^{\frac{1}{2}} \leq C'_I\, q^{\frac{n}{2}-1} p^{-\frac{n}{2}}\, |E_{v_2}||E_{v_1}|^{\frac{1}{2}}\,.$$

But since this inequality would require

$$q^{-\frac{1}{2}}\,(1+o(1)) = \delta^{\frac{1}{2}}_{S_{v_2}} \geq \delta^{\frac{1}{2}}_{E_{v_2}} \gg q^{-\frac{1}{2}}\, p,$$

it *cannot* occur for $p \gg 1$.

As a result :

$$\textit{for } p \textit{ sufficiently large it is not possible that} \quad \mathcal{B}^*_{II} \leq \widetilde{\mathcal{B}}^*_I.$$

So, we may assume $\mathcal{B}^*_{II} > \widetilde{\mathcal{B}}^*_I$ whenever $p \gg 1$, in which event, it is now elementary to verify the following:

$$p \gg 1\,, \quad n, r \geq 2\,, \quad \textit{and} \quad \delta^{\frac{1}{2}}_{E_{v_1}}\, \delta^{\frac{1}{2}}_{E_{v_2}} > 2\, C_{II}\, q^{-\frac{1}{2}}\, p^{-\frac{n-2}{2}} \quad \textit{implies} \quad \mathcal{M}^*_{\mathbf{v},j} > 2\,\mathcal{B}^*_{II} > \mathcal{E}^*_{\mathbf{v},j}\,. \tag{63}$$

The lower bound in (63) however, *must also be compatible* with an a priori upper bound

$$q^{-1}\,(1+o(1)) \geq \delta^{\frac{1}{2}}_{S_{v_1}}\, \delta^{\frac{1}{2}}_{S_{v_2}} \geq \delta^{\frac{1}{2}}_{E_{v_1}}\, \delta^{\frac{1}{2}}_{E_{v_2}} > 2\, C_{II}\, q^{-\frac{1}{2}}\, p^{-\frac{n-2}{2}}\,.$$

The two inequalities are evidently compatible *if*

$$1 + o(1) > 2C_{II}\, p^{\frac{r-(n-2)}{2}} \quad \textit{that is, if} \quad r < n-2 \quad \textit{when} \quad p \gg 1. \tag{64}$$

In other words, if $\delta_{E_{v_1}} \geq \delta_{E_{v_2}}$, $n \geq 2$, and $r < n-2$, we conclude that if $p \gg 1$ then

$$q^{-2}(1+o(1))^2 \geq \delta_{E_{v_1}}\, \delta_{E_{v_2}} > 4\, C^2_{II}\, q^{-1}\, p^{2-n} \quad \textit{implies} \quad \sigma_{\mathbf{v},j}(E) = \frac{|E_{v_1}|\,|E_{v_2}|}{q}\,(1+o(1)). \tag{65}$$

If, however, $\delta_{E_{v_1}} \leq \delta_{E_{v_2}}$, then it is clear that it suffices to interchange $v_1$ with $v_2$ as subscripts in (63) and use the same argument as above to conclude that $\mathcal{M}^*_{\mathbf{v},j} > \mathcal{E}^*_{\mathbf{v},j}$ whenever $p \gg 1$ and $r < n-2$. We leave these details for the reader to verify.

The union $\Omega$ of the two sets of permissible densities is independent of $\mathbf{v}, j$ and satisfies the property that if $E$ is any set for which $(\delta_{E_{v_1}}, \delta_{E_{v_2}}) \in \Omega$, then $\mathcal{M}^*_{\mathbf{v},j} > \mathcal{E}^*_{\mathbf{v},j}$ and

$$\sigma_{\mathbf{v},j}(E) = \frac{|E_{v_1}|\,|E_{\mathbf{v}_2}|}{q}\cdot(1+o(1)) \quad \textit{uniformly in } p \gg 1 \textit{ whenever } 2 \leq r < n-2 \textit{ and } n \geq 5. \quad \square$$

## 4. Concluding remarks

It is natural to want to apply our methods to detect the presence of particular dot product values between $n-$vectors over the ring of $p-$adic integers $\mathcal{Z}_p$ when $n \geq 2$. We also continue to use the notation $(p)^{(n)}$ to denote the $n-$fold product of the maximal ideal $(p)$ in $\mathcal{Z}_p$.

Starting with a subset $\mathcal{E} \subset \mathcal{Z}_p^n \setminus (p)^{(n)}$ and denoting by $E_r$ the projection (or truncation by $p^r$) of $\mathcal{E}$ to $\mathbb{Z}_q^n$, we impose the hypotheses:

(i) $p \gg 1$ *and* $\delta_{E_r} \gg p^{-\frac{n-1}{2}}$ *for all* $r \geq 1$;

(ii) $\mathcal{E} = \varprojlim_r E_r$.

Note that condition (i) is a purely Haar measure theoretic condition since the density of $E_r \subset \mathbb{Z}_q^n$ equals the normalized Haar measure of $E_r$. Condition (ii) says that $\mathcal{E}$ equals the intersection of its family of approximating "tubular" neighborhoods $\mathcal{T}_r(\mathcal{E})$ of width $p^{-rn}$:

$$\mathcal{T}_r(\mathcal{E}) := \{\mathbf{z} \in \mathcal{Z}_p^n : max_{\mathbf{x}\in\mathcal{E}}\ \|\mathbf{z}-\mathbf{x}\| \leq p^{-rn}\}.$$

**Remark 4.1.** Note that this property does *not* hold if $\mathcal{E} = \mathbb{Z}^n$.

Theorem 1.1 tells us that if the two hypotheses are satisfied, for example, if $\mathcal{E}$ is a closed subset (in the $p-$adic metric topology), and if, in addition, $\delta_{E_r} \gg p^{-\frac{n-1}{2}}$ for each $r$, then for any unit $\mathbf{j} \in \mathcal{Z}_p$

$$\beta_{j_r}(E_r) \neq \emptyset \qquad (\textit{where } j_r \in \mathbb{Z}_q \textit{ denotes the reduction mod } q \textit{ of } \mathbf{j})\,.$$

Denoting by $(\mathbf{x}_r, \mathbf{y}_r)$ a point in $E_r \times E_r$ for which $\langle \mathbf{x}_r, \mathbf{y}_r\rangle = j_r$ the resulting sequence of points $\{(\mathbf{x}_r, \mathbf{y}_r)\}_r$ is a Cauchy sequence in $\mathcal{Z}_p^n \times \mathcal{Z}_p^n$. By the hypothesis (ii), the unique limit point $(\mathbf{x}, \mathbf{y})$ of this sequence belongs to $\mathcal{E} \times \mathcal{E}$. Moreover, since $\mathbf{j} = lim_r\, j_r$ it follows that

$$\langle \mathbf{x}, \mathbf{y}\rangle = \mathbf{j}\,.$$

In other words, for any unit $\mathbf{j}$ we have shown that if the hypotheses (i), (ii) are satisfied by a set $\mathcal{E} \subset \mathcal{Z}_p^n \setminus (p)^{(n)}$ then $\{(\mathbf{x}, \mathbf{y}) \in \mathcal{E} \times \mathcal{E} : \langle \mathbf{x}, \mathbf{y}\rangle = \mathbf{j}\} \neq \emptyset\,.$

## References

[1] D. Covert, A. Iosevich, and J. Pakianathan. Geometric configurations in the ring of integers modulo $p^\ell$. *Indiana University Mathematics Journal*, 61:1949–1967, 2012.

[2] D. Ethier. *Sum-Product Estimates and Finite Point Configurations Over P-Adic Fields*. PhD thesis, University of Rochester, 2017.

[3] J. I. Igusa. *Lectures on Forms of Higher Degree*. Tata Institute of Fundamental Research, 1978. TATA Institute Lectures.

[4] B. Lichtin. Distance and sum-product problems over p-adic rings. *Proceedings of the London Mathematical Society*, 118:1450–1470, 2019. https://doi.org/10.1112/plms.12219.

[5] B. Lichtin. Averages of point configuration problems over finite $p$-adic rings. *Proceedings of the American Mathematical Society*, 149:2825–2839, 2021. https://doi.org/10.1090/proc/15449.

[6] B. Lichtin. $k$-simplices over finite $p$-adic rings. (submitted).

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

[8] N. Van The and L. A. Vinh. Dot-product sets and simplices over finite rings. *Journal of Fourier Analysis and Applications*, 28:38, 2022. https://doi.org/10.1007/s00041-022-09933-7.

[9] A. Weil. Numbers of solutions of equations in finite fields. *Bulletin of the American Mathematical Society*, 55:497–508, 1949.

Ben Lichtin
49 Boardman St., Rochester, NY 14607, USA
E-mail lichtin@frontier.com