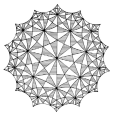
Rev. Mat. Iberoam. (Online first)
DOI 10.4171/RMI/1530



Estimates for trilinear and quadrilinear character sums

Étienne Fouvry, Igor E. Shparlinski and Ping Xi

Abstract. We obtain new bounds on some trilinear and quadrilinear character sums, which are non-trivial starting from very short ranges of the variables. An application to an apparently new problem on oscillations of characters on differences between Farey fractions is given. Other applications include a modular analogue of a multiplicative hybrid problem of Iwaniec and Sárközy (1987) and the solvability of some prime type equations with constraints.

1. Introduction and backgrounds

1.1. Set-up

Motivated by various applications to analytic number theory, estimates for character sums received a lot of attention in the past decades. In many situations, the variables are supported over some additively structured sets, such as sets of consecutive integers. But the difficulty can vary significantly since the weights might be arbitrary. This paper aims to study two kinds of multilinear character sums with arbitrary weights.

Throughout this paper, denote by p a large prime, and by χ a non-trivial multiplicative character modulo p. Take two integers a, b with $p \nmid ab$. For $K, L, M, N \geqslant 1$, we consider the trilinear character sum

$$\mathfrak{T}(\boldsymbol{\alpha}, \boldsymbol{\beta}) = \sum_{k \leqslant K} \sum_{m \leqslant M} \sum_{n \leqslant N} \alpha_m \beta_{k,n} \chi(ak + bmn) \tag{1.1}$$

and the quadrilinear sum

$$\mathfrak{Q}(\boldsymbol{\alpha}, \boldsymbol{\beta}) = \sum_{k \leqslant K} \sum_{\ell \leqslant L} \sum_{m \leqslant M} \sum_{n \leqslant N} \alpha_{\ell,m} \beta_{k,n} \chi(ak\ell + bmn), \tag{1.2}$$

where $\boldsymbol{\alpha} = (\alpha_m)$ or $(\alpha_{\ell,m})$ and $\boldsymbol{\beta} = (\beta_{k,n})$ are some complex weights. Note that one obtains (1.1) if taking $L = 1$ and $\alpha_{1,m} = \alpha_m$ in (1.2). No confusion on the definitions of $\boldsymbol{\alpha}$ arises since one is for the trilinear sum, and the other is for the quadrilinear one.

In various practical applications, one aims to obtain upper bounds, as strong as possible, for $\mathfrak{T}(\boldsymbol{\alpha}, \boldsymbol{\beta})$ and $\mathfrak{Q}(\boldsymbol{\alpha}, \boldsymbol{\beta})$ in terms of the ℓ_ρ-norms $\|\boldsymbol{\alpha}\|_\rho$ and $\|\boldsymbol{\beta}\|_\rho$ (see (1.7) below

Mathematics Subject Classification 2020: 11L40.
Keywords: character sums, trilinear forms, quadrilinear forms.

for the definition of norms). We refer to the following inequalities:

$$|\mathfrak{T}(\boldsymbol{\alpha},\boldsymbol{\beta})| \leqslant \min\{\|\boldsymbol{\alpha}\|_\infty\|\boldsymbol{\beta}\|_\infty KMN,\ \|\boldsymbol{\alpha}\|_2\|\boldsymbol{\beta}\|_2(KMN)^{1/2}\}$$

and

$$|\mathfrak{Q}(\boldsymbol{\alpha},\boldsymbol{\beta})| \leqslant \min\{\|\boldsymbol{\alpha}\|_\infty\|\boldsymbol{\beta}\|_\infty KLMN,\ \|\boldsymbol{\alpha}\|_2\|\boldsymbol{\beta}\|_2(KLMN)^{1/2}\},$$

as trivial bounds, as they follow directly from the triangle inequality and the Cauchy–Schwarz inequality. Our aim is to beat the above trivial bounds for $\boldsymbol{\alpha}, \boldsymbol{\beta}$ as general as possible and K, L, M, N as small as possible compared to p.

We would like to emphasize that weights in $\mathfrak{Q}(\boldsymbol{\alpha},\boldsymbol{\beta})$ depend on variables from different products, which makes treatments of such sums much more difficult, as the standard smoothing technique does not immediately apply.

Our bounds for $\mathfrak{T}(\boldsymbol{\alpha},\boldsymbol{\beta})$ and $\mathfrak{Q}(\boldsymbol{\alpha},\boldsymbol{\beta})$ with power-savings, as well as applications, will be given in Section 2, and we would like to give a brief outline of related results right now.

1.2. Related bilinear sums

The above studies on character sums over sumsets can be dated back to Vinogradov, see Exercise 8(c) in Chapter V of [28], on the following bilinear form:

$$\mathfrak{B}(\boldsymbol{\alpha},\boldsymbol{\beta}) = \sum_{m\in\mathcal{M}}\sum_{n\in\mathcal{N}} \alpha_m\beta_n\,\chi(m+n), \tag{1.3}$$

where χ is a non-trivial Dirichlet character modulo p and $\mathcal{M}, \mathcal{N} \subseteq [1, p]$ are arbitrary subsets with $M = \#\mathcal{M}$ and $N = \#\mathcal{N}$. A direct application of Fourier techniques yields

$$|\mathfrak{B}(\boldsymbol{\alpha},\boldsymbol{\beta})| \leqslant \|\boldsymbol{\alpha}\|_2\,\|\boldsymbol{\beta}\|_2\,p^{1/2}. \tag{1.4}$$

Although this bound is widely known, its full derivation is not easy to find in the literature, however, it can be found as a short proof of equation (1.4) in [25]. Despite a very short and elementary proof, the bound (1.4) has never been improved in full generality. However, Karatsuba [18] (see also Problem 9 in Chapter VIII of [19]) has proved, that if

$$M > p^{1/2+\eta} \quad \text{and} \quad N > p^{\eta} \tag{1.5}$$

for some $\eta > 0$, then the inequality

$$|\mathfrak{B}(\boldsymbol{\alpha},\boldsymbol{\beta})| \leqslant \|\boldsymbol{\alpha}\|_\infty\,\|\boldsymbol{\beta}\|_\infty\,MNp^{-\kappa} \tag{1.6}$$

holds with some $\kappa > 0$, depending only on η. The range (1.5) reveals the Pólya–Vinogradov threshold even when summing over arbitrary subsets. A similar phenomenon can also be found in [31]. We note that the proof of (1.6), in the range (1.5), does not seem to be in the literature, and a concise proof with an explicit upper bound, is provided in Appendix A to convince cautious readers.

It is worthwhile to point out that $\mathfrak{B}(\boldsymbol{\alpha},\boldsymbol{\beta})$ has received considerable attention in recent years due to its connection with the *Paley graph conjecture*. It is conjectured, for instance, with just constant weights $\alpha_m = \beta_n = 1$, that

$$\mathfrak{B}(\boldsymbol{\alpha},\boldsymbol{\beta}) = o(MN)$$

for all subsets $\mathcal{M}, \mathcal{N}$, with $M, N > p^\eta$ and $\eta > 0$. This is far from proven, and the classical inequalities of Vinogradov (1.4) and Karatsuba (1.6) still stand. See [9, 14] for recent progress towards this conjecture.

For structural sets, such as intervals, or sets with small doubling, or sets supported on short intervals, a large variety of bounds for $\mathfrak{B}(\boldsymbol{\alpha}, \boldsymbol{\beta})$ are known. For example, the above bounds of Vinogradov and Karatsuba have been improved by Friedlander and Iwaniec, see Theorem 3 in [12], when $\mathcal{M}$ and $\mathcal{N}$ are contained in intervals of lengths at most $\sqrt{p}$ and are of cardinalities $M, N \geqslant p^{11/24+\eta}$. Of course, the main point here is that $11/24 < 1/2$, which neither (1.4) nor (1.6) with (1.5) can achieve. The exponent $11/24$ has been reduced to $9/20$ by Bourgain, Garaev, Konyagin and Shparlinski, see Theorem 25 in [3]. Several more results of this type can be found in [2, 4, 5, 13, 21, 24, 26, 27, 29].

1.3. Related trilinear and quadrilinear sums

Before concluding this section, we also mention some recent works on various variants of $\mathfrak{B}(\boldsymbol{\alpha}, \boldsymbol{\beta})$. To proceed, we assume $\mathcal{H}, \mathcal{K}, \mathcal{M}, \mathcal{N} \subseteq [1, p]$ are arbitrary subsets. Hanson [13] has studied

$$\sum_{k \in \mathcal{K}} \sum_{m \in \mathcal{M}} \sum_{n \in \mathcal{N}} \alpha_m \beta_n \chi(k + m + n),$$

while Roche-Newton, Shparlinski and Winterhof [23] have considered

$$\sum_{k \in \mathcal{K}} \sum_{m \in \mathcal{M}} \sum_{n \in \mathcal{N}} \chi(km + mn + nk)\, \mathrm{e}\Big(\frac{a(km + mn + nk)}{p}\Big)$$

with $\gcd(a, p) = 1$. Shkredov and Shparlinski [25] have treated quadrilinear forms

$$\sum_{h \in \mathcal{H}} \sum_{k \in \mathcal{K}} \sum_{m \in \mathcal{M}} \sum_{n \in \mathcal{N}} \alpha_h \beta_{k,m,n} \chi(h + k + mn),$$
$$\sum_{h \in \mathcal{H}} \sum_{k \in \mathcal{K}} \sum_{m \in \mathcal{M}} \sum_{n \in \mathcal{N}} \alpha_h \beta_{k,m,n} \chi(h + k(m + n)).$$

See also [22], for some recent generalizations and refinements.

Our main object $\mathfrak{T}(\boldsymbol{\alpha}, \boldsymbol{\beta})$ is intimately related to the following trilinear character sum:

$$\sum_{k \leqslant K} \sum_{m \in \mathcal{M}} \sum_{n \in \mathcal{N}} \alpha_k \beta_m \gamma_n \chi(k + mn),$$

where χ is a non-trivial Dirichlet character modulo p and $\mathcal{M}, \mathcal{N} \subseteq [1, p]$ are arbitrary subsets with $M = \#\mathcal{M}$ and $N = \#\mathcal{N}$. Banks and Shparlinski (Theorem 2.2 of [1]) give the upper bound

$$KMN(p^{-1} + (KM)^{-1} + K^{-2})^{1/(2r)}(p^{1/(4r)} + N^{-1/2} p^{1/(2r)}) p^{o(1)}$$

with an arbitrary fixed integer $r \geqslant 1$, provided that the three coefficients are all bounded. Note that the above bound is non-trivial as long as

$$K > p^{1/4+\eta}, \quad KM > p^{1/2+\eta}, \quad N > p^\eta,$$

with some constant $\eta > 0$.

Our work on $\mathfrak{T}(\boldsymbol{\alpha}, \boldsymbol{\beta})$ is largely inspired by the recent work of Fouvry and Shparlinski [11] on quadrilinear character sums such as

$$\mathfrak{Q}_1(\boldsymbol{\alpha}, \boldsymbol{\beta}) = \sum_{1 \leqslant r,s,u,v \leqslant x} \sum \sum \sum \alpha_r \beta_u \chi(rs - uv),$$
$$\mathfrak{Q}_2(\boldsymbol{\gamma}) = \sum_{1 \leqslant r,s,u,v \leqslant x} \sum \sum \sum \gamma_{r,s,u} \chi(rs - uv),$$

with bounded complex weights $\boldsymbol{\alpha} = (\alpha_r)$, $\boldsymbol{\beta} = (\beta_u)$ and $\boldsymbol{\gamma} = (\gamma_{r,s,u})$. It is shown in [11], that for any fixed $\eta > 0$ and $x \geqslant p^{1/8+\eta}$, we have

$$\mathfrak{Q}_1(\boldsymbol{\alpha}, \boldsymbol{\beta}) \ll x^{4-\kappa} \quad \text{and} \quad \mathfrak{Q}_2(\boldsymbol{\gamma}) \ll x^4 \frac{\log\log p}{\log p},$$

where $\kappa > 0$ and the implied constants depend only on η (we refer to Section 1.4 for the exact definition of the symbol '$\ll$' and other standard notations).

1.4. Notation and conventions

We adopt the Landau symbol $A = O(B)$, and the Vinogradov symbol $A \ll B$, to mean $|A| \leqslant cB$ for some constant $c > 0$. We also write $a \sim A$ to indicate that $A < a \leqslant 2A$ and $A \asymp B$ to indicate $A \ll B \ll A$.

For each complex weight $\boldsymbol{\alpha} = (\alpha_m)_{m \in \mathcal{M}}$ and $\rho \geqslant 1$, we denote

$$\|\boldsymbol{\alpha}\|_\rho = \Big(\sum_{m \in \mathcal{M}} |\alpha_m|^\rho \Big)^{1/\rho} \quad \text{and} \quad \|\boldsymbol{\alpha}\|_\infty = \max_{m \in \mathcal{M}} |\alpha_m|. \tag{1.7}$$

For a finite set $\mathcal{S}$, we use $\#\mathcal{S}$ to denote its cardinality. The letter p, with or without subscripts, always denotes a prime number.

We denote by $\mathbb{F}_p$ the finite field of p elements, which we identify by $\{0, 1, \dots, p-1\}$, and in what follows, we mix the usage of $\mathbb{F}_p$ and $\{0, 1, \dots, p-1\}$. We freely alternate between the language of finite fields and the language of congruences.

We also use $\mathbb{N}$ to denote that set of positive integers.

As usual,

$$\tau(k) = \#\{d \in \mathbb{N} : d \mid k\} \tag{1.8}$$

denotes the divisor function, and we repeatedly use the classical bound $\tau(k) = k^{o(1)}$ as $k \to +\infty$ (see, for example, equation (1.81) in [15]). For an integer a, coprime to m, $\overline{a}$ denotes the multiplicative inverse of a mod m, that is, $a\overline{a} \equiv 1 \bmod m$, which should not be confused with the complex conjugate.

Given a function $f \in L^1(\mathbb{R})$, that is, with a bounded L^1-norm over $\mathbb{R}$, the Fourier transform is defined by

$$\widehat{f}(y) = \int_{\mathbb{R}} f(x)\, \mathrm{e}(-yx)\, \mathrm{d}x,$$

with $\mathrm{e}(z) = \exp(2\pi i z)$.

2. Main results

2.1. Bounds of multilinear character sums

Put

$$\mathcal{L}_1 = (|a|K + |b|MN) \quad \text{and} \quad \mathcal{L}_2 = (|a|KL + |b|MN). \tag{2.1}$$

We prove two estimates for the sums $\mathfrak{T}(\boldsymbol{\alpha}, \boldsymbol{\beta})$ given by (1.1), according to whether the weights α_m are identically 1, which we write as $\boldsymbol{\alpha} \equiv \mathbf{1}$, or arbitrary.

Theorem 2.1. *Let $K, M, N > 1$ and let $p > \max\{K, M, N\}$ be a large prime. Uniformly over the weights $\boldsymbol{\alpha} \equiv \mathbf{1}$, $\boldsymbol{\beta} = (\beta_{k,n})$ and integers a, b with $\gcd(ab, p) = 1$, we have*

$$|\mathfrak{T}(\boldsymbol{\alpha}, \boldsymbol{\beta})| \leqslant \|\boldsymbol{\beta}\|_\infty KMN\Delta_1\, p^{o(1)}$$

for each positive integer r, provided that $M > 4\,p^{1/(2r)}$, where

$$\Delta_1 = (1 + NK^{-1})^{1/(2r)}\,(1 + \mathcal{L}_1 MNp^{-1-1/(2r)})^{1/(2r)} \left(\frac{p^{1+1/r}}{M^4N^4}\right)^{1/(4r)},$$

with $\mathcal{L}_1$ as defined by (2.1).

Remark 2.2. Taking $N = K = 1$ in Theorem 2.1, we recover the celebrated Burgess bound for short linear character sums, which shows oscillations of non-trivial multiplicative characters modulo p, in any interval with length at least $p^{1/4+\varepsilon}$ for any $\varepsilon > 0$ and sufficiently large p. This is also known as the *Burgess threshold* (see Theorem 12.26 in [15]).

Remark 2.3. It is not easy to give a full description on the range of (K, M, N) which is equivalent to $\Delta_1 < 1$. However, when $a = b = 1$, we note that Theorem 2.1 is non-trivial if either of the following conditions holds:

- $p^{1/4+\eta} < MN \leqslant p^{1/2}$ and $N \leqslant K \leqslant p/(MN)$,
- $MN \leqslant p^{1/2+\eta} \leqslant M^2NK$ and $N \geqslant K$,

with some fixed $\eta > 0$. For example, we can take

$$K, M, N \sim p^{1/8+\eta} \tag{2.2}$$

for small $\eta > 0$. The lower bound for the values of K, M, N, given by (2.2), is the square root of the Burgess threshold.

We now use Theorem 2.1 to get a new bound, with a power saving, on the sums $\mathfrak{Q}_2(\boldsymbol{\gamma})$ from Section 1.3. Indeed, applying Theorem 2.1 with

$$(m, n, k; a, b) \leftarrow (v, u, k; 1, -1), \quad (K, M, N) \leftarrow (x^2, x, x)$$

and

$$\beta_{n,k} = \sum_{\substack{1 \leqslant r,s,u \leqslant x \\ rs = k,\, u = n}} \sum \sum \gamma_{r,s,u},$$

we find the following.

Corollary 2.4. *Let p be a large prime with $p > x^2 \geqslant 1$. Uniformly over the weights $\boldsymbol{\gamma} = (\gamma_{r,s,u})$, we have*

$$|\mathfrak{Q}_2(\boldsymbol{\gamma})| \leqslant \|\boldsymbol{\gamma}\|_\infty x^{4-2/r}(1 + x^4 p^{-1-1/(2r)})^{1/(2r)} p^{1/(4r)+1/(4r^2)+o(1)}$$

for each positive integer r.

We see that Corollary 2.4 gives a non-trivial bound for $\mathfrak{Q}_2(\boldsymbol{\gamma})$ with a power-saving as long as $x \geqslant p^{1/8+\eta}$ with some fixed $\eta > 0$. And this also recovers the above bound for $\mathfrak{Q}_1(\boldsymbol{\alpha}, \boldsymbol{\beta})$ with more general weights.

For arbitrary weights $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$, we have the following alternative bound.

Theorem 2.5. *Let $K, M, N > 1$ and let $p > \max\{K, M, N\}$ be a large prime. Uniformly over the weights $\boldsymbol{\alpha} = (\alpha_m)$, $\boldsymbol{\beta} = (\beta_{k,n})$ and integers a, b with $\gcd(ab, p) = 1$, we have*

$$|\mathfrak{T}(\boldsymbol{\alpha}, \boldsymbol{\beta})| \leqslant \|\boldsymbol{\alpha}\|_\infty \|\boldsymbol{\beta}\|_2 M(NK)^{1/2} \Delta_2 \, p^{o(1)}$$

for each integer $r \geqslant 2$, provided that $N > 4\, p^{1/r}$, where

$$\Delta_2 = (1 + KM^{-2})^{1/(4r)}(1 + \mathcal{L}_1 MNp^{-1-1/r})^{1/(2r)}\Big(\frac{p^{1+1/r}}{K(MN)^2}\Big)^{1/(4r)} + M^{-1/2},$$

with $\mathcal{L}_1$ as defined by (2.1).

Remark 2.6. Fix $a = b = 1$. Then Theorem 2.5 is non-trivial as long as

$$M > p^\eta, \quad K(MN)^2 > (1 + KM^{-2})p^{1+\eta} \quad \text{and} \quad MN(K + MN) < p$$

hold with some fixed $\eta > 0$. For example, we can take

$$K, M, N \sim p^{1/5+\eta},$$

which has to be compared with (2.2) and also with the Burgess threshold.

As an application of the above bounds for $\mathfrak{T}(\boldsymbol{\alpha}, \boldsymbol{\beta})$, one is allowed to address a modulo p version of a question of Iwaniec and Sárközy [16] about distances between product sets and squares. We present such an application in Section 2.2.

One can derive some bounds on such sums from Theorems 2.1 and 2.5 with a trivial summation over a, which plays the role of ℓ in $\mathfrak{Q}(\boldsymbol{\alpha}, \boldsymbol{\beta})$. However, we may obtain a more precise bound as follows.

Theorem 2.7. *Let $K, L, M, N > 1$ and let $p > \max\{K, L, M, N\}$ be a large prime. Uniformly over the weights $\boldsymbol{\alpha} = (\alpha_{\ell,m})$ and $\boldsymbol{\beta} = (\beta_{k,n})$, we have*

$$|\mathfrak{Q}(\boldsymbol{\alpha}, \boldsymbol{\beta})| \leqslant \|\boldsymbol{\alpha}\|_\infty \|\boldsymbol{\beta}\|_2 LM(KN)^{1/2} p^{o(1)} \cdot \Delta_3$$

for each integer $r \geqslant 2$, provided that $K, N > 4\, p^{1/r}$, where

$$\Delta_3 = (KLMN)^{-3/(4r)}\Big(\frac{M}{K} + 1\Big)^{1/(2r)}\Big(1 + \frac{\mathcal{L}_2^2}{p^{1+1/r}}\Big)^{1/(2r)} \mathcal{L}_2^{1/(2r)} p^{1/(4r)+1/(2r^2)}$$
$$+ (KN)^{-1/2} p^{1/(2r)} + (MN)^{-1/2}\, p^{1/(2r)} + (LM)^{-1/2} + p^{-1/2},$$

with $\mathcal{L}_2$ as defined by (2.1).

We now analyze when Theorem 2.7 wins over the trivial bound

$$|\mathfrak{Q}(\boldsymbol{\alpha},\boldsymbol{\beta})| \leqslant \|\boldsymbol{\alpha}\|_\infty \|\boldsymbol{\beta}\|_2 (LM)(KN)^{1/2}.$$

Corollary 2.8. *Fix $a = b = 1$. For any $\eta > 0$, there is some $\kappa > 0$, such that if*

$$\begin{cases} KL \ll MN \leqslant KLp^{1/3-\eta}, & K^5L^3N \geqslant Mp^{1+\eta}, \\ (M/K)^5(N/L)^3 \leqslant p^{1-\eta}, & (KL)^3MN \geqslant p^{1+\eta}, \\ KN \geqslant p^\eta, \quad MN \geqslant p^\eta, & LM \geqslant p^\eta, \end{cases} \tag{2.3}$$

then

$$|\mathfrak{Q}(\boldsymbol{\alpha},\boldsymbol{\beta})| \leqslant \|\boldsymbol{\alpha}\|_\infty \|\boldsymbol{\beta}\| LM(KN)^{1/2} p^{-\kappa}.$$

To see this, we write the quantity Δ_3 in an obvious manner as

$$\Delta_3 = \widetilde{\Delta}_3 + (KN)^{-1/2} p^{1/(2r)} + (MN)^{-1/2}\, p^{1/(2r)} + (LM)^{-1/2} + p^{-1/2}, \tag{2.4}$$

corresponding to five terms in its definition. By taking r sufficiently large, each of the last four terms in (2.4) is at most $p^{-\kappa}$ for some $\kappa > 0$, provided that the last three conditions in (2.3) hold. It remains to check that $\widetilde{\Delta}_3 \ll p^{-\kappa}$. We now assume $KL \ll MN$, so that $\mathcal{L}_2 = KL + MN \ll MN$. First, rising $\widetilde{\Delta}_3$ to the power $2r$ and expanding it, we obtain four terms. Each of these terms is at most $p^{-\kappa}$ as long as $KL \ll MN$ and

$$\max\Big\{(MN)^2 p^{-1/2},\ \frac{M}{K}\, p^{1/2+1/r},\ \frac{M^3N^2}{Kp^{1/2}},\ p^{1/2+1/r}\Big\} \ll (KL)^{3/2}(MN)^{1/2} p^{-2r\kappa}.$$

These lead to the remaining inequalities in (2.3), after choosing r to be large enough.

In particular, we see from Corollary 2.8 that we have a non-trivial bound on $\mathfrak{Q}(\boldsymbol{\alpha},\boldsymbol{\beta})$, provided that

$$K = L = M = N > p^{1/8+\eta}.$$

Observe that one more time the exponent $1/8$ appears as a threshold, see Remark 2.3, however, this does not seem to follow from Theorem 2.1.

2.2. Consequences and applications

Theorems 2.1 and 2.5 describe general situations, since the sequence $\boldsymbol{\beta}$ satisfies no particular hypotheses. For instance, if we choose $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$ in the landscape of multiplicative or additive characters modulo p, we obtain, as a direct consequence of Theorem 2.5, the following bound for triple character sums on short initial segments. To proceed, we use ψ to denote a non-trivial additive character of $\mathbb{F}_p$.

Corollary 2.9. *Fix a rational function P in $\mathbb{F}_p(X)$ and a rational function Q in $\mathbb{F}_p(X,Y)$. For every fixed $\eta > 0$, there exists some $\kappa > 0$ such that*

$$\sum_{k\leqslant K} \sum_{m\leqslant M} \sum_{n\leqslant N} \chi(k+mn)\,\psi(P(m)+Q(k,n)) \ll KMNp^{-\kappa}$$

and

$$\sum_{k\leqslant K} \sum_{m\leqslant M} \sum_{n\leqslant N} \chi((k+mn)P(m)Q(k,n)) \ll KMNp^{-\kappa}$$

hold uniformly for

$$p^{1/5+\eta} \leqslant K, M, N < p^{1/4-\eta}.$$

Remark 2.10. Theorem 2.7 easily leads to an obvious quadrilinear version of Corollary 2.9, but with K, L, M and N of size at least $p^{1/8+\eta}$ for any $\eta > 0$.

Furthermore, Iwaniec and Sárközy [16] have considered the following multiplicative hybrid problem with positive integers: given two arbitrary subsets $\mathcal{M}$ and $\mathcal{N}$, how close is the product mn to a square in $\mathbb{Z}$ with $(m, n) \in \mathcal{M} \times \mathcal{N}$? A special case of their general result asserts that for any $\mathcal{M}, \mathcal{N} \subseteq [N, 2N]$ with $\#\mathcal{M}, \#\mathcal{N} \gg N$, there exist $(m, n, \ell) \in \mathcal{M} \times \mathcal{N} \times \mathbb{N}$ satisfying

$$\frac{mn - \ell^2}{\ell} \ll (N/\log N)^{-1/2}.$$

Iwaniec and Sárközy [16] have also conjectured that the upper bound might be replaced by $N^{-1+o(1)}$.

Theorem 2.5 allows us to study a modular analogue of the above result of Iwaniec and Sárközy, for which the above conjectural bound $N^{-1+o(1)}$ can be realized in some particular cases. To set up, we consider subsets $\mathcal{M}, \mathcal{N} \subseteq [1, p]$, we examine the distance between mn, with $(m, n) \in \mathcal{M} \times \mathcal{N}$, and quadratic residues modulo p.

Theorem 2.11. *Fix a positive integer r, two real numbers $0 < c_0 < 1$ and $\eta > 0$. Then there exists a constant P, depending only on (r, c_0, η), such that*:

- *for every prime $p \geqslant P$,*
- *for every M and N satisfying*

$$M^4 N^2 \geqslant p^{1+1/r+\eta}, \tag{2.5}$$

- *for every subsets $\mathcal{M}, \mathcal{N} \subseteq [1, p]$ with*

$$\mathcal{M} \subseteq [M, 2M], \quad \mathcal{N} \subseteq [N, 2N], \quad \#\mathcal{M} \geqslant c_0 M, \quad \#\mathcal{N} \geqslant c_0 N, \tag{2.6}$$

there exist $m \in \mathcal{M}$, $n \in \mathcal{N}$, and some positive integer k satisfying

$$k \leqslant p^{1+1/r+\eta}(MN)^{-2} + p^{\eta},$$

such that $mn + k$ is a quadratic residue modulo p.

Actually, the proof which is given in Section 7 produces a lower bound for the cardinality of the set of triples we are interested in

$$\#\{(m, n, k) : m \in \mathcal{M},\ n \in \mathcal{N},\ k \leqslant K \text{ and } mn + k \text{ is a quadratic residue mod } p\} \gg KMN,$$

where $K \sim p^{1+1/r+\eta}(MN)^{-2}$.

To illustrate Theorem 2.11, choose $M = N \sim p^{1/5+\delta}$ (with $\delta > 0$ very small) and $\mathcal{M}$ and $\mathcal{N}$ subsets of $[N, 2N]$ such that $\#\mathcal{M}, \#\mathcal{N} \geqslant \delta N$. Then, for sufficiently large p, there exists a positive integer $k \leqslant p^{1/5}$ and $(m, n) \in \mathcal{M} \times \mathcal{N}$ such that $mn + k$ is a quadratic residue modulo p. Recall that there must exist a square of an integer between t and $t + O(\sqrt{t})$ for all $t > 1$ (namely, $\lceil \sqrt{t} \rceil^2$ is such a square) and that essentially nothing better than the upper bound $p^{1/4+o(1)}$ is proved for the distance between two consecutive quadratic residues modulo p. The above illustration shows that one can do much better if squares are replaced by quadratic residues modulo p.

The proof of Theorem 2.11 can be easily generalized in many aspects. For instance, one can relax the hypothesis (2.6) about the cardinalities of $\mathcal{M}$ and $\mathcal{N}$ by choosing

$$\begin{cases} \alpha_m = \mathbf{1}_{[M,2M]\cap\mathcal{P}}(m), \\ \beta_{k,n} = \mathbf{1}_{[K,2K]\cap\mathcal{P}}(k)\cdot\mathbf{1}_{[N,2N]\cap\mathcal{P}}(n), \end{cases} \tag{2.7}$$

where $\mathcal{P}$ denotes the set of all primes, and $\mathbf{1}_S$ is the indicator function of a set S. One then deduces from Theorem 2.5 the following result by counting primes using Chebyshev's inequalities.

Corollary 2.12. *Fix $\eta > 0$. For every sufficiently large p, there exist three primes p_1, p_2 and p_3 such that*:

- $p_1, p_2, p_3 \sim p^{1/5+\eta}$,
- $p_1p_2 + p_3$ *is a quadratic non-residue modulo* p.

As we have mentioned, Corollary 2.12 follows directly from Theorem 2.5 and it can be modified in various ways, for example, one can impose different arithmetic restrictions on the primes p_1, p_2, p_3. For example, one further imposes that the three shifted primes $p_1 + 2, p_2 + 2, p_3 + 2$ have at most two prime factors. This statement is deduced from the famous work of Chen [7] about the twin prime conjecture that we write under the form of the following inequality:

$$\#\{p \leqslant x : p + 2 \text{ has at most two prime factors}\} \gg x(\log 2x)^{-2}$$

for $x \geqslant 2$. One can also appeal to Corollaire 2 in [10] to introduce a more involved definition of the coefficient $\beta_{k,n}$ (see (2.7)) leading to a new version of Corollary 2.12, where we impose on $p_1p_3 + 2$ to have at most two prime factors.

Similarly, Theorem 2.7 leads to the following result (which can also be modified along the lines mentioned in the above).

Corollary 2.13. *Fix $\eta > 0$. For every sufficiently large p, there exist four primes p_1, p_2, p_3 and p_4 such that*:

- $p_1, p_2, p_3, p_4 \sim p^{1/8+\eta}$,
- $p_1p_2 + p_3p_4$ *is a quadratic non-residue modulo* p.

Another application of Theorem 2.7 concerns sums with the divisor function (see (1.8) above)

$$S(U, V) = \sum_{u\leqslant U}\sum_{v\leqslant V} \tau(u)\,\tau(v)\,\chi(u - v).$$

These sums are two-dimensional analogues of the sum

$$S_a(U) = \sum_{u\leqslant U} \tau(u)\,\chi(u + a),$$

which has been studied in a number of works [3, 6, 17, 20]. In particular, it is shown in Theorem 27 of [3] that for any $\eta > 0$, there is some $\kappa > 0$ such that for $U > p^{1/3+\eta}$, uniformly over integers a with $\gcd(a, p) = 1$, one has

$$S_a(U) \ll Up^{-\kappa}.$$

It is easy to see that Theorem 2.7 combined with the standard completing technique (see Section 12.2 of [15]) implies the following result.

Corollary 2.14. *For any fixed $\eta > 0$, there is some $\kappa > 0$ such that for $U, V > p^{1/4+\eta}$, we have*

$$S(U, V) \ll UVp^{-\kappa}.$$

One can also use Theorem 2.7 to estimate a rich variety of other quantities, for example, sums over primes

$$W(x) = \sum_{p_1,p_2,p_3,p_4 \leqslant x} \Big(\frac{p_1}{p_3}\Big)\Big(\frac{p_2}{p_4}\Big)\chi(p_1p_2 - p_3p_4),$$

with weights given by Legendre symbols. Theorem 2.7 implies a bound on $W(x)$ with a power saving, provided $x \geqslant p^{1/8+\eta}$ for any fixed $\eta > 0$. We also note a variety of bounds on characters over various arithmetic sequences can be found in a very informative survey of Karatsuba [21].

In closing this section, we would like to state a striking application of our general bounds in Theorem 2.7 to character sums involving Farey fractions. For $R \geqslant 2$, let

$$\mathcal{F}(R) = \{r/s : \gcd(r, s) = 1,\ 0 \leqslant r \leqslant s \leqslant R\}$$

be the set of Farey fractions of order R. This can be embedded in $\mathbb{F}_p$ in a canonical way $r/s \mapsto r\overline{s} \pmod p$, where $\overline{s}$ is the multiplicative inverse of s modulo p (which is well defined for $R < p$ and, in fact, is injective for $R < p^{1/2}$).

By virtue of the multiplicativity of χ, in the form

$$\alpha_{\ell,m}\,\beta_{k,n}\,\chi(\ell\overline{m} - \overline{k}n) = (\alpha_{\ell,m}\,\overline{\chi}(m))\,(\beta_{k,n}\,\overline{\chi}(k))\,\chi(k\ell - mn).$$

we may derive the following consequence directly from Theorem 2.7.

Corollary 2.15. *Let $R \geqslant 2$ and ξ_ρ, ζ_ϱ be bounded weights supported on $\mathcal{F}(R)$. Then for any fixed $\eta > 0$, there is some $\kappa > 0$ such that for $p^{1/8+\eta} \leqslant R < p^{1/2}$, we have*

$$\sum_{\rho,\varrho \in \mathcal{F}(R)} \sum \xi_\rho \zeta_\varrho\, \chi(\rho - \varrho) \ll R^4 p^{-\kappa}.$$

Note that the use of bilinear bounds (1.5) and (1.6) would lead to a much more restrictive condition $p^{1/4+\eta} \leqslant R < p^{1/2}$ in Corollary 2.15.

3. Preliminaries

3.1. Moments of some character sums

The following result is a consequence of the Riemann hypothesis for curves over finite fields due to Weil [30]. It is a slight extension of a classical bound due to Davenport and Erdős [8], which corresponds to the case when $\mathcal{A}$ is an interval and $\boldsymbol{\gamma} = 1$. The proof of Lemma 3.1 below is identical, and it is also a part of the arguments in Appendix A.

Lemma 3.1. *Let $\mathcal{A} \subseteq \mathbb{F}_p$ be a subset of cardinality A, and χ a non-trivial multiplicative character of $\mathbb{F}_p^\times$. For each positive integer r and any complex-valued weight $\boldsymbol{\gamma} = (\gamma_a)$ with $\|\boldsymbol{\gamma}\|_\infty \leqslant 1$, we have*

$$\sum_{x\in\mathbb{F}_p}\Big|\sum_{a\in\mathcal{A}}\gamma_a\chi(x+a)\Big|^{2r} \leqslant (2r)^r(A^r p + A^{2r}p^{1/2}).$$

We also need the following version of Lemma 3.1, which again essentially repeats the argument in [8] but uses *Weil's bound* for multiplicative character sums with polynomials; see, for example, Theorem 11.23 in [15].

Lemma 3.2. *Let $\mathcal{A} \subseteq \mathbb{F}_p$ be a subset of cardinality A, and χ_1, χ_2 two non-trivial multiplicative characters of $\mathbb{F}_p^\times$. For each positive integer r and any complex-valued weight $\boldsymbol{\gamma} = (\gamma_a)$ with $\|\boldsymbol{\gamma}\|_\infty \leqslant 1$, we have*

$$\sum_{x,y\in\mathbb{F}_p}\sum\Big|\sum_{a\in\mathcal{A}}\gamma_a\chi_1(x+a)\,\chi_2(y+a)\Big|^{2r} \leqslant (2r)^r(A^r p^2 + 2rA^{2r}p).$$

Proof. Denote by S the quantity in question. Opening the power, we write

$$S \leqslant \sum_{\mathbf{a},\mathbf{b}\in\mathcal{A}^r}\sum|S(\mathbf{a},\mathbf{b};\chi_1)\,S(\mathbf{a},\mathbf{b};\chi_2)|,$$

where for $\mathbf{a} = (a_1,\dots,a_r) \in \mathcal{A}^r$, $\mathbf{b} = (b_1,\dots,b_r) \in \mathcal{A}^r$ and for each non-trivial multiplicative character χ of $\mathbb{F}_p^\times$,

$$S(\mathbf{a},\mathbf{b};\chi) = \sum_{x\in\mathbb{F}_p}\prod_{1\leqslant j\leqslant r}\chi(x+a_j)\,\overline{\chi(x+b_j)}.$$

The subsequent treatment is uniform in all non-trivial multiplicative characters χ of $\mathbb{F}_p^\times$. If the coordinates of $\mathbf{a}$ and $\mathbf{b}$ appear in pairs (with necessary permutations), we appeal to the trivial bound

$$|S(\mathbf{a},\mathbf{b};\chi)| \leqslant p.$$

Note that the number of such tuples $(\mathbf{a},\mathbf{b})$ is at most $r\binom{2r}{r}A^r \leqslant (2rA)^r$. For the remaining $\mathbf{a}$ and $\mathbf{b}$, we can apply Weil's bound for complete character sums (see Corollary 11.24 in [15]), getting

$$|S(\mathbf{a},\mathbf{b};\chi)| \leqslant 2rp^{1/2}.$$

This completes the proof of Lemma 3.2 by taking all possibilities of $\mathbf{a},\mathbf{b}$ into account. ∎

3.2. Bounds of some GCD sums

We need the following estimate.

Lemma 3.3. *Let a and b be non-zero integers. Let $A, B, K, L, M, N, U, W \geqslant 1$ with $A \ll |a|KL + |b|MN$ and $B \ll LU + MW$. Then we have*

$$\sum_{\substack{k\leqslant K\\ ak\ell_v+bm_vn=a_v,\ a\ell_vu+bm_vw=b_v,\ v=1,2\\ |a_1|\sim A,\,|b_2|\sim B,\,kw\neq nu}}\sum_{\ell_1,\ell_2\leqslant L}\sum_{m_1,m_2\leqslant M}\sum_{n\leqslant N}\sum_{u\sim U}\sum_{w\sim W}\gcd(a_1,b_1)\gcd(a_2,b_2)$$
$$\leqslant ABLM(KW+NU)\Upsilon^{o(1)}, \quad \text{with } \Upsilon = |ab|ABKLMNUW.$$

Proof. Denote by G the above quantity in question. Writing $g_1 = \gcd(a_1, b_1)$ and $g_2 = \gcd(a_2, b_2)$, we have the inequality

$$G \leqslant \sum_{g_1 \ll A,\, g_2 \ll B} g_1 g_2 \sum_{\substack{k \leqslant K \\ a k \ell_\nu + b m_\nu n \equiv a \ell_\nu u + b m_\nu w \equiv 0 \bmod g_\nu,\, \nu = 1,2 \\ |a k \ell_1 + b m_1 n| \sim A,\, |a \ell_2 u + b m_2 w| \sim B,\, kw \neq nu}} \sum_{\ell_1, \ell_2 \leqslant L} \sum_{m_1, m_2 \leqslant M} \sum_{n \leqslant N} \sum_{u \sim U} \sum_{w \sim W} 1.$$

The congruences in the summation imply

$$g_\nu \mid m_\nu w(ak\ell_\nu + bm_\nu n) - m_\nu n(a\ell_\nu u + bm_\nu w) = a\ell_\nu m_\nu (kw - nu)$$

for $\nu = 1, 2$, so that we can decompose g_ν (in a not necessarily unique way) as

$$g_\nu = d_\nu e_\nu f_\nu, \quad \text{where } d_\nu \mid a\ell_\nu,\ e_\nu \mid m_\nu,\ f_\nu \mid (kw - nu).$$

In particular, we have

$$\operatorname{lcm}[f_1, f_2] \leqslant 2(KW + NU).$$

Therefore,

$$G \leqslant \sum_{\substack{d_1 e_1 f_1 \ll A \\ d_2 e_2 f_2 \ll B \\ \operatorname{lcm}[f_1, f_2] \leqslant 2(KW + NU)}} \sum d_1 d_2 e_1 e_2 f_1 f_2 \sum_{\substack{k \leqslant K \\ \operatorname{lcm}[f_1, f_2] \mid (kw - nu) \neq 0}} \sum_{n \leqslant N} \sum_{u \sim U} \sum_{w \sim W} \sum_{\substack{\ell_1, \ell_2 \leqslant L,\, m_1, m_2 \leqslant M \\ a k \ell_1 + b m_1 n \equiv 0 \bmod d_1 e_1 f_1 \\ a \ell_2 u + b m_2 w \equiv 0 \bmod d_2 e_2 f_2 \\ \ell_\nu \equiv 0 \bmod d_\nu,\, m_\nu \equiv 0 \bmod e_\nu,\, \nu = 1,2 \\ |a k \ell_1 + b m_1 n| \sim A, \\ |a \ell_2 u + b m_2 w| \sim B}} \sum 1.$$

Making the change of variables $\ell_\nu \to d_\nu \ell_\nu$, $m_\nu \to e_\nu m_\nu$, $\nu = 1, 2$, we obtain

$$G \leqslant \sum_{\substack{d_1 e_1 f_1 \ll A \\ d_2 e_2 f_2 \ll B \\ \operatorname{lcm}[f_1, f_2] \leqslant 2(KW + NU)}} \sum d_1 d_2 e_1 e_2 f_1 f_2 \sum_{\substack{k \leqslant K \\ \operatorname{lcm}[f_1, f_2] \mid (kw - nu) \neq 0}} \sum_{k \leqslant N} \sum_{u \sim U} \sum_{w \sim W} \sum_{\substack{d_1 \ell_1, d_2 \ell_2 \leqslant L,\, e_1 m_1, e_2 m_2 \leqslant M \\ a d_1 \ell_1 k + b e_1 m_1 n \equiv 0 \bmod d_1 e_1 f_1 \\ a d_2 \ell_2 u + b e_2 m_2 w \equiv 0 \bmod d_2 e_2 f_2 \\ |a d_1 \ell_1 k + b e_1 m_1 n| \sim A, \\ |a d_2 \ell_2 u + b e_2 m_2 w| \sim B}} \sum 1.$$

Note that the congruences

$$a d_1 \ell_1 k + b e_1 m_1 n \equiv 0 \bmod d_1 e_1 f_1 \quad \text{and} \quad a d_2 \ell_2 u + b e_2 m_2 w \equiv 0 \bmod d_2 e_2 f_2$$

imply, respectively,

$$e_1 \mid a d_1 \ell_1 k, \quad d_2 \mid b e_2 m_2 w,$$

and

$$b m_1 n \equiv -a d_1 \ell_1 k / e_1 \bmod d_1 f_1, \quad a \ell_2 u \equiv -b e_2 m_2 w / d_2 \bmod e_2 f_2.$$

It then follows that

$$G \leqslant \sum_{\substack{d_1 e_1 f_1 \ll A \\ d_2 e_2 f_2 \ll B \\ \operatorname{lcm}[f_1, f_2] \leqslant 2(KW + NU)}} \sum d_1 d_2 e_1 e_2 f_1 f_2 \sum_{\substack{k \leqslant K \\ \operatorname{lcm}[f_1, f_2] \mid (kw - nu) \neq 0}} \sum_{n \leqslant N} \sum_{u \sim U} \sum_{w \sim W} \sum_{\substack{d_1 \ell_1, d_2 \ell_2 \leqslant L,\, e_1 m_1, e_2 m_2 \leqslant M \\ e_1 \mid a d_1 \ell_1 k,\, b m_1 n \equiv -a d_1 \ell_1 k / e_1 \bmod d_1 f_1 \\ d_2 \mid b e_2 m_2 w,\, a \ell_2 u \equiv -b e_2 m_2 w / d_2 \bmod e_2 f_2 \\ |a d_1 \ell_1 k + b e_1 m_1 n| \sim A, \\ |a d_2 \ell_2 u + b e_2 m_2 w| \sim B}} \sum 1$$

$$\leqslant \sum_{\substack{d_1 f_1 \ll A\\ e_2 f_2 \ll B\\ \mathrm{lcm}[f_1,f_2]\leqslant 2(KW+NU)}}\sum d_1 e_2 f_1 f_2 \sup_{\delta\in\mathbb{Z}} \sum_{k\leqslant K}\sum_{w\sim W}\sum_{\substack{d_2\ll B/(e_2 f_2)\\ e_1\ll A/(d_1 f_1)}}\sum d_2 e_1$$
$$\times \sum_{n\leqslant N}\sum_{u\sim U} \sum_{\substack{d_1\ell_1, d_2\ell_2\leqslant L,\ e_1 m_1, e_2 m_2\leqslant M\\ e_1 \mid ad_1\ell_1 k,\ bm_1 n\equiv -ad_1\ell_1 k/e_1 \bmod d_1 f_1\\ d_2\mid be_2 m_2 w,\ a\ell_2 u\equiv -be_2 m_2 w/d_2 \bmod e_2 f_2\\ |ad_1\ell_1 k/e_1 + bm_1 n|\sim A/e_1,\\ |a\ell_2 u + be_2 m_2 w/d_2|\sim B/d_2}}\sum\sum\sum\sum 1.$$

To proceed, we group the variables m_1, n, and ℓ_2, u, separately, so that we need to count the number of tuples (r, s) with

$$|ad_1\ell_1 k/e_1 + br| \sim A/e_1, \quad |as + be_2 m_2 w/d_2| \sim B/d_2$$

and

$$br \equiv -d_1\ell_1 k/e_1 \bmod d_1 f_1, \quad as \equiv -e_2 m_2 w/d_2 \bmod e_2 f_2.$$

It is clear that the number T of such tuples (r, s) satisfies

$$T \ll \Big(1 + \frac{A\gcd(b, d_1 f_1)}{bd_1 e_1 f_1}\Big)\Big(1 + \frac{B\gcd(a, e_2 f_2)}{ad_2 e_2 f_2}\Big) \ll \frac{AB}{d_1 d_2 e_1 e_2 f_1 f_2}.$$

This leads us to

$$G \ll AB \sum_{\substack{d_1 f_1\ll A\\ e_2 f_2\ll B\\ \mathrm{lcm}[f_1,f_2]\leqslant 2(KW+NU)}}\sum \sup_{\delta\in\mathbb{Z}} \sum_{k\leqslant K}\sum_{w\sim W}\sum_{\substack{d_2\ll B/(e_2 f_2)\\ e_1\ll A/(d_1 f_1)}}\sum\sum_{\substack{\ell_1\leqslant L/d_1, m_2\leqslant M/e_2\\ d_2\mid be_2 m_2 w,\ e_1\mid ad_1\ell_1 k}}\sum 1.$$

In what follows, we would like to sum over d_2, e_1 firstly, and then ℓ_1, m_2, so that

$$G \leqslant ABLM\Upsilon^{o(1)} \sum_{\substack{d_1 f_1\ll A\\ e_2 f_2\ll B\\ \mathrm{lcm}[f_1,f_2]\leqslant 2(KW+NU)}}\sum \frac{1}{d_1 e_2} \sup_{\delta\in\mathbb{Z}} \sum_{k\leqslant K}\sum_{w\sim W}\sum_{kw\equiv\delta \bmod \mathrm{lcm}[f_1,f_2]} 1.$$

Again, by grouping variables, we arrive at

$$\begin{aligned} G &\leqslant ABLM\Upsilon^{o(1)} \sum_{\substack{d_1 f_1\ll A\\ e_2 f_2\ll B\\ \mathrm{lcm}[f_1,f_2]\leqslant 2(KW+NU)}}\sum \frac{1}{d_1 e_2}\Big(\frac{KW}{\mathrm{lcm}[f_1, f_2]} + 1\Big)\\ &\leqslant ABLM\Upsilon^{o(1)} \sum_{d_1\ll A}\frac{1}{d_1}\sum_{e_1\ll A}\frac{1}{e_2}\sum_{f\ll KW+NU}\Big(\frac{KW}{f} + 1\Big)\\ &\leqslant ABLM(KW + NU)\,\Upsilon^{o(1)}, \end{aligned}$$

where we have used the bound on the divisor function to count the number of pairs (f_1, f_2) with $\mathrm{lcm}[f_1, f_2] = f$. This completes the proof of the lemma. ∎

4. Proof of Theorem 2.1

4.1. Preparations

Throughout this section, we assume that $\boldsymbol{\alpha}$ is identically 1 on its support. Suppose without loss of generality that $\|\boldsymbol{\beta}\|_\infty \leqslant 1$ and M is a positive integer. Following an approach of Friedlander and Iwaniec [12], we define the function $w \in L^1(\mathbb{R})$ as

$$w(x) = \begin{cases} \min\{x, 1, M+1-x\} & \text{for } x \in [0, M+1], \\ 0 & \text{otherwise.} \end{cases}$$

The integration by parts implies

$$\widehat{w}(\xi) \ll \min\{M, |\xi|^{-1}, |\xi|^{-2}\}. \tag{4.1}$$

4.2. Amplification

The above function w allows us to run the summation over m to the whole set $\mathbb{Z}$. That is,

$$\mathfrak{T}(\boldsymbol{\alpha}, \boldsymbol{\beta}) = \sum_{k \leqslant K} \sum_{m \in \mathbb{Z}} \sum_{n \leqslant N} w(m)\, \beta_{k,n}\, \chi(ak + bmn).$$

Furthermore, for all integers u, v, we have

$$\mathfrak{T}(\boldsymbol{\alpha}, \boldsymbol{\beta}) = \sum_{k \leqslant K} \sum_{m \in \mathbb{Z}} \sum_{n \leqslant N} w(m + uv)\, \beta_{k,n}\, \chi(ak + b(m+uv)n).$$

We choose two real positive parameters U and V with

$$U, V \geqslant 1, \quad UV = \frac{1}{4} M. \tag{4.2}$$

By Fourier inversion and summing over integers u and v with $u \sim U$, $v \sim V$, we have the amplified expression

$$\mathfrak{T}(\boldsymbol{\alpha}, \boldsymbol{\beta}) \ll \frac{1}{UV} \sum_{k \leqslant K} \sum_{m \leqslant M} \sum_{n \leqslant N} \sum_{u \sim U} \int_{\mathbb{R}} |\widehat{w}(\xi)| \Big| \sum_{v \sim V} \mathrm{e}(uv\xi) \chi(\overline{un}(ak + bmn) + bv) \Big| \, \mathrm{d}\xi.$$

Making the change of variable $\xi \to \xi/u$ and replacing UV with M, in view of (4.1), it follows that

$$\begin{aligned} \mathfrak{T}(\boldsymbol{\alpha}, \boldsymbol{\beta}) &\ll \frac{1}{M} \sum_{k \leqslant K} \sum_{m \leqslant M} \sum_{n \leqslant N} \sum_{u \sim U} \int_{\mathbb{R}} \Big| \widehat{w}\Big(\frac{\xi}{u}\Big) \Big| \\ &\quad \times \Big| \sum_{v \sim V} \mathrm{e}(v\xi)\, \chi(\overline{un}(ak + bmn) + bv) \Big| \frac{\mathrm{d}\xi}{u} \\ &\ll \frac{1}{M} \int_{\mathbb{R}} \min\Big\{ \frac{M}{U}, \frac{1}{|\xi|}, \frac{U}{|\xi|^2} \Big\} \\ &\quad \times \sum_{k \leqslant K} \sum_{m \leqslant M} \sum_{n \leqslant N} \sum_{u \sim U} \Big| \sum_{v \sim V} \mathrm{e}(v\xi)\, \chi(\overline{un}(ak + bmn) + bv) \Big| \, \mathrm{d}\xi. \end{aligned} \tag{4.3}$$

This yields

$$\mathfrak{T}(\boldsymbol{\alpha},\boldsymbol{\beta}) \ll \frac{\log M}{M} \sum_{k\leqslant K} \sum_{m\leqslant M} \sum_{n\leqslant N} \sum_{u\sim U} \Big| \sum_{v\sim V} \mathrm{e}(v\xi)\, \chi(\overline{un}(ak+bmn)+bv)\Big|$$

for some $\xi \in \mathbb{R}$ (for which the multiple sum in (4.3) achieves its largest possible value).

We may further restrict our summation to triples (k,m,n) such that $p \nmid (ak+bmn)$ up to an error term at most

$$p^{o(1)} \sum_{\substack{k\leqslant K\\ ak+b\ell\equiv 0 \bmod p}} \sum_{\ell\leqslant MN} 1 \leqslant \Big(\frac{MN}{p}+1\Big) Kp^{o(1)}.$$

Therefore,

$$\begin{aligned}\mathfrak{T}(\boldsymbol{\alpha},\boldsymbol{\beta}) \ll \frac{\log M}{M} \sum_{\substack{k\leqslant K\\ p\nmid (ak+bmn)}} \sum_{m\leqslant M} \sum_{n\leqslant N} \sum_{u\sim U} \Big| \sum_{v\sim V} \mathrm{e}(v\xi)\chi(\overline{un}(ak+bmn)+bv)\Big|\\ + \Big(\frac{MN}{p}+1\Big) Kp^{o(1)}.\end{aligned}$$

4.3. Regrouping, counting and Weil's bound

Put

$$\varrho(x) = \sum_{\substack{m\leqslant M\\ ak+bmn\equiv unx\not\equiv 0 \bmod p}} \sum_{n\leqslant N} \sum_{k\leqslant K} \sum_{u\sim U} 1$$

for $x \bmod p$. We now have

$$\mathfrak{T}(\boldsymbol{\alpha},\boldsymbol{\beta}) \ll \frac{\log M}{M} \sum_{x \bmod p} \varrho(x) \Big| \sum_{v\sim V} \mathrm{e}(v\xi)\chi(x+bv)\Big| + \Big(\frac{MN}{p}+1\Big) Kp^{o(1)}.$$

Applying the Hölder inequality with $r \geqslant 1$, we obtain

$$\mathfrak{T}(\boldsymbol{\alpha},\boldsymbol{\beta}) \ll \frac{\log M}{M} \mathcal{J}_1^{1-1/r} (\mathcal{J}_2 \cdot \mathcal{J}_3)^{1/(2r)} + \Big(\frac{MN}{p}+1\Big) Kp^{o(1)}, \tag{4.4}$$

with

$$\mathcal{J}_j = \sum_{x \bmod p} \varrho(x)^j, \quad j=1,2, \qquad \mathcal{J}_3 = \sum_{x \bmod p} \Big| \sum_{v\sim V} \mathrm{e}(v\xi)\chi(x+bv)\Big|^{2r}.$$

Trivially we have

$$\mathcal{J}_1 \ll KMNU. \tag{4.5}$$

Regarding $\mathcal{J}_2$, we refer to the following lemma.

Lemma 4.1. *With the above notation, we have*

$$\mathcal{I}_2 \leqslant KMU(K+N)\Big(1+\frac{(|a|K+|b|MN)UN}{p}\Big)p^{o(1)}. \tag{4.6}$$

Proof. It is easy to see that $\mathcal{I}_2$ is the number of 8–tuples

$$(k,\tilde{k},m,\tilde{m},n,\tilde{n},u,\tilde{u}) \in \mathbb{N}^8$$

satisfying the conditions

$$\begin{aligned} &k,\tilde{k} \leqslant K, \quad m,\tilde{m} \leqslant M, \quad n,\tilde{n} \leqslant N, \quad u,\tilde{u} \sim U,\\ &(ak+bmn)\tilde{n}\tilde{u} \equiv (a\tilde{k}+b\tilde{m}\tilde{n})nu \not\equiv 0 \pmod{p}, \end{aligned}$$

which is bounded by the number of 9–tuples

$$(k,\tilde{k},m,\tilde{m},n,\tilde{n},u,\tilde{u},t) \in \mathbb{N}^8 \times \mathbb{Z},$$

satisfying

$$\begin{aligned} &k,\tilde{k} \leqslant K, \quad m,\tilde{m} \leqslant M, \quad n,\tilde{n} \leqslant N, \quad u,\tilde{u} \sim U, \quad |t| \leqslant T,\\ &(ak+bmn)\tilde{n}\tilde{u} = (a\tilde{k}+b\tilde{m}\tilde{n})nu + tp, \quad (ak+bmn)(a\tilde{k}+b\tilde{m}\tilde{n}) \neq 0, \end{aligned} \tag{4.7}$$

with

$$T = 1 + (|a|K+|b|MN)NU/p. \tag{4.8}$$

Note that $\tilde{n} \mid a\tilde{k}un + tp$ and $a\tilde{k}un \not\equiv 0 \pmod{p}$. Hence, $a\tilde{k}un + tp \neq 0$ for any $t \in \mathbb{Z}$, and thus, for given $\tilde{k}$, n, t and u, which we can fix in $O(KNTU)$ ways, the number of $\tilde{n}$ satisfying (4.7) is at most $p^{o(1)}$. After $\tilde{k}$, $\tilde{m}$, n, $\tilde{n}$, t and u are fixed, there are at most $(K/N+1)p^{o(1)}$ possibilities for the tuple $(m,\tilde{u},k)$. This is due to the observations that $\tilde{u} \mid (a\tilde{k}+b\tilde{m}\tilde{n})un + tp \neq 0$ and the number of solutions (m,k) to

$$ak + bmn = \frac{(a\tilde{k}+b\tilde{m}\tilde{n})un + tp}{\tilde{u}\tilde{n}},$$

with $m \leqslant M, k \leqslant K$, is at most $O(1+K/N)$ since k falls in a prescribed arithmetic progression modulo $n \sim N$, which is already fixed.

Taking all possibilities into account, we find the contributions from $ak + bmn \neq 0$ to $\mathcal{I}_2$ are at most

$$KNTU \cdot M \cdot \Big(1+\frac{K}{N}\Big)p^{o(1)} \leqslant KMTU(K+N)p^{o(1)}.$$

Now Lemma 4.1 follows by recalling the choice of T in (4.8). ∎

To bound $\mathcal{I}_3$, we apply Lemma 3.1 with $\mathcal{A} = \{bv : v \sim V\}$, getting

$$\mathcal{I}_3 \ll V^{2r}p^{1/2} + V^r p \tag{4.9}$$

as a consequence of Weil's bound for complete character sums over finite fields (see Theorem 11.23 in [15]).

4.4. Concluding the proof of Theorem 2.1

To balance the two terms in (4.9), we choose

$$V = p^{1/(2r)} \quad \text{and} \quad U = \frac{1}{4} Mp^{-1/(2r)}$$

in view of (4.2), so that (4.5) and (4.6) become

$$\mathcal{J}_1 \ll KM^2Np^{-1/(2r)} \quad \text{and} \quad \mathcal{J}_2 \leqslant KM^2p^{-1/(2r)}(K+N)(1+\mathcal{L}_1MNp^{-1-1/(2r)})p^{o(1)},$$

respectively, where $\mathcal{L}_1$ is defined by (2.1), while (4.9) becomes

$$\mathcal{J}_3 \ll p^{3/2}.$$

Now Theorem 2.1 follows by combining the inequality (4.4) and the above estimates for $\mathcal{J}_1$, $\mathcal{J}_2$ and $\mathcal{J}_3$.

5. Proof of Theorem 2.5

5.1. Cauchy–Schwarz inequality and amplification

We note that the auxiliary parameters T, U and V from Section 4 have different meaning henceforth. This time it is convenient to assume that $\|\boldsymbol{\alpha}\|_\infty \leqslant 1$. By the Cauchy–Schwarz inequality, we have

$$|\mathfrak{T}(\boldsymbol{\alpha}, \boldsymbol{\beta})|^2 \leqslant \|\boldsymbol{\beta}\|_2^2 T, \tag{5.1}$$

where

$$T = \sum_{k \leqslant K} \sum_{n \in \mathbb{Z}} W\Big(\frac{n}{N}\Big) \Big| \sum_{m \leqslant M} \alpha_m \chi(ak + bmn)\Big|^2,$$

with any fixed real-valued smooth function $W \in \mathcal{C}_c^\infty([-2, 2])$, which majorizes the characteristic function of the unit interval $[0, 1]$.

Squaring out, changing the order of summation and estimating the contribution from the diagonal terms with $m_1 = m_2$, we obtain

$$T \ll T_1 + KMN, \tag{5.2}$$

with

$$T_1 = \sum_{k \leqslant K} \sum_{\substack{m_1, m_2 \leqslant M \\ m_1 \neq m_2}} \sum_{n \in \mathbb{Z}} W\Big(\frac{n}{N}\Big) \alpha_{m_1} \overline{\alpha}_{m_2} \chi(ak + bm_1n) \overline{\chi}(ak + bm_2n).$$

For any integers u and v, we may write

$$T_1 = \sum_{k \leqslant K} \sum_{\substack{m_1, m_2 \leqslant M \\ m_1 \neq m_2}} \sum_{n \in \mathbb{Z}} W\Big(\frac{n+uv}{N}\Big) \alpha_{m_1} \overline{\alpha}_{m_2} \chi(ak + bm_1(n+uv)) \overline{\chi}(ak + bm_2(n+uv)).$$

By Fourier inversion and summing over $u \sim U$ and $v \sim V$, for some positive parameters U and V with

$$U, V \geqslant 1, \quad UV = \frac{1}{4} N, \tag{5.3}$$

it follows that

$$T_1 \ll \frac{1}{N} \sum_{k \leqslant K} \sum_{\substack{m_1, m_2 \leqslant M \\ m_1 \neq m_2}} \sum_{|n| \leqslant 2N} \sum_{u \sim U} \int_{\mathbb{R}} |\widehat{W}(\xi)| \times \Big| \sum_{v \sim V} \mathrm{e}\Big(\frac{uv\xi}{N}\Big) \chi(\overline{m_1 u}(ak + bm_1 n) + bv)\, \overline{\chi}(\overline{m_2 u}(ak + bm_2 n) + bv) \Big| \, \mathrm{d}\xi.$$

In view of

$$\widehat{W}(\xi) \ll (1 + |\xi|)^{-2},$$

implied by the smoothness of $W(x)$ via partial integration, and making the change of variable $\xi \to \xi/u$, after simple transformations, we obtain

$$T_1 \ll \frac{1}{NU} \int_{\mathbb{R}} \Big(1 + \frac{|\xi|}{U}\Big)^{-2} \sum_{k \leqslant K} \sum_{\substack{m_1, m_2 \leqslant M \\ m_1 \neq m_2}} \sum_{|n| \leqslant 2N} \sum_{u \sim U} \times \Big| \sum_{v \sim V} \mathrm{e}\Big(\frac{v\xi}{N}\Big) \chi(\overline{m_1 u}(ak + bm_1 n) + bv)\, \overline{\chi}(\overline{m_2 u}(ak + bm_2 n) + bv) \Big| \, \mathrm{d}\xi.$$

Again, as in the proof of Theorem 2.1, this implies

$$T_1 \ll \frac{1}{N} \sum_{k \leqslant K} \sum_{\substack{m_1, m_2 \leqslant M \\ m_1 \neq m_2}} \sum_{|n| \leqslant 2N} \sum_{u \sim U} \times \Big| \sum_{v \sim V} \mathrm{e}(v\xi) \chi(\overline{m_1 u}(ak + bm_1 n) + bv)\, \overline{\chi}(\overline{m_2 u}(ak + bm_2 n) + bv) \Big| \tag{5.4}$$

for some $\xi \in \mathbb{R}$.

5.2. Regrouping, counting and Weil's bound

Put

$$\varrho(x_1, x_2) = \sum_{|n| \leqslant 2N} \sum_{k \leqslant K} \sum_{m_1, m_2 \leqslant M} \sum_{u \sim U} \sum_{\substack{ak + bm_1 n \equiv u m_1 x_1 \not\equiv 0 \bmod p \\ ak + bm_1 n \equiv u m_2 x_2 \not\equiv 0 \bmod p \\ m_1 \neq m_2}} 1$$

for $x_1, x_2 \bmod p$. We now have

$$T_1 \ll \frac{1}{N} \sum_{x_1, x_2 \bmod p} \sum \varrho(x_1, x_2) \Big| \sum_{v \sim V} \mathrm{e}(v\xi) \chi(x_1 + bv)\, \overline{\chi}(x_2 + bv) \Big| + (1 + MN/p) KM p^{o(1)},$$

where the last term comes from those k, m_1, m_2, n, with $p \mid (ak + bm_1 n)(ak + bm_2 n)$ in (5.4) .

Applying the Hölder inequality with $r \geqslant 1$, similarly to (4.4), we find

$$T_1 \ll \frac{1}{N} \mathcal{J}_1^{1-1/r} (\mathcal{J}_2 \cdot \mathcal{J}_3)^{1/(2r)} + (1 + MN/p) KM p^{o(1)}, \tag{5.5}$$

with

$$\mathcal{J}_j = \sum_{x_1, x_2 \bmod p} \sum \varrho(x_1, x_2)^j, \quad j = 1, 2,$$

and

$$\mathcal{J}_3 = \sum_{x_1, x_2 \bmod p} \sum \Big| \sum_{v \sim V} \mathrm{e}(v\xi) \chi(x_1 + bv)\, \overline{\chi}(x_2 + bv) \Big|^{2r}.$$

Note that

$$\mathcal{J}_1 \ll KM^2 NU. \tag{5.6}$$

We appeal to the following lemma in bounding $\mathcal{J}_2$.

Lemma 5.1. *With the above notation, we have*

$$\mathcal{J}_2 \leqslant KNU(K + M^2) \Big(1 + \frac{(|a|K + |b|MN)MU}{p}\Big)^2 p^{o(1)}. \tag{5.7}$$

Proof. We observe that $\mathcal{J}_2$ is bounded by the number of 10-tuples

$$(k, \tilde{k}, m_1, \tilde{m}_1, m_2, \tilde{n}_2, n, \tilde{n}, u, \tilde{u}) \in \mathbb{N}^{10}$$

satisfying

$$\begin{gathered} k, \tilde{k} \leqslant K, \quad m_1, \tilde{m}_1, m_2, \tilde{m}_2 \leqslant M, \quad n, \tilde{n} \in [-2N, 2N], \quad u, \tilde{u} \sim U, \\ (ak + bm_1 n)\tilde{m}_1 \tilde{u} \equiv (a\tilde{k} + b\tilde{m}_1 \tilde{n}) m_1 u \not\equiv 0 \bmod p, \\ (ak + bm_2 n)\tilde{m}_2 \tilde{u} \equiv (a\tilde{k} + b\tilde{m}_2 \tilde{n}) m_2 u \not\equiv 0 \bmod p, \\ m_1 \neq m_2, \quad \tilde{m}_1 \neq \tilde{m}_2. \end{gathered}$$

We now rewrite the above congruences as equations:

$$(ak + bm_1 n)\tilde{m}_1 \tilde{u} = (a\tilde{k} + b\tilde{m}_1 \tilde{n}) m_1 u + t_1 p \neq 0, \tag{5.8a}$$

$$(ak + bm_2 n)\tilde{m}_2 \tilde{u} = (a\tilde{k} + b\tilde{m}_2 \tilde{n}) m_2 u + t_2 p \neq 0, \tag{5.8b}$$

where $0 \leqslant |t_1|, |t_2| \leqslant T$, with

$$T = 1 + (|a|K + 2|b|MN)MU/p. \tag{5.9}$$

It follows from (5.8a) that

$$\tilde{m}_1 \mid a\tilde{k} m_1 u + t_1 p \neq 0 \quad \text{and} \quad \tilde{u} \mid (\tilde{m}_1 \tilde{n} + a\tilde{k}) m_1 u + t_1 p \neq 0,$$

which produces at most $p^{o(1)}$ tuples of $(\tilde{m}_1, \tilde{u})$ for given $\tilde{n}, \tilde{k}, m_1, u, t_1$.

After fixing $\tilde{m}_1, \tilde{u}, \tilde{n}, \tilde{k}, m_1, u$ and t_1, we obtain the equation

$$ak + bm_1 n = \frac{(a\tilde{k} + b\tilde{m}_1\tilde{n})m_1 u + t_1 p}{\tilde{m}_1\tilde{u}} \tag{5.10}$$

in k and n, thanks to (5.8a). We further fix m_2 and t_2. We see from (5.8b) that $\tilde{m}_2 \mid a\tilde{k}m_2 u + t_2 p \neq 0$, by which there are at most $p^{o(1)}$ values of $\tilde{m}_2$ for given $\tilde{k}, m_2, u, t_2$. As before, using (5.8b), we obtain the equation

$$ak + bm_2 n = \frac{(a\tilde{k} + b\tilde{m}_2\tilde{n})m_2 u + t_2 p}{\tilde{m}_2\tilde{u}} \tag{5.11}$$

in k and n. It then follows from (5.10) and (5.11) that k is uniquely defined modulo m_1 and modulo m_2, so that the number of such positive integers k is at most

$$\frac{K}{\operatorname{lcm}[m_1, m_2]} + 1 = \frac{\gcd(m_1, m_2)}{m_1 m_2} K + 1.$$

Now n is uniquely determined after k is fixed. Collecting all above arguments, we find

$$\mathcal{J}_2 \leqslant KNUT^2 p^{o(1)} \sum_{m_1, m_2 \leqslant M} \sum \Big(\frac{\gcd(m_1, m_2)}{m_1 m_2} K + 1 \Big) \leqslant KNUT^2 (K + M^2) p^{o(1)}.$$

Lemma 5.1 now follows immediately by recalling the choice of T in (5.9). ∎

Using Lemma 3.2 with the special choice $\mathcal{A} = \{bv : v \sim V\}$ therein, we find

$$\mathcal{J}_3 \ll V^{2r} p + V^r p^2. \tag{5.12}$$

5.3. Concluding the proof of Theorem 2.5

We now choose

$$V = p^{1/r} \quad \text{and} \quad U = \frac{1}{4} N p^{-1/r}$$

subject to the constraint in (5.3), so that the above bounds for $\mathcal{J}_1$ and $\mathcal{J}_2$ in (5.6) and (5.7) become

$$\mathcal{J}_1 \ll K(MN)^2 p^{-1/r} \quad \text{and} \quad \mathcal{J}_2 \leqslant KN^2 p^{-1/r} (K + M^2)(1 + \mathcal{L}_1 MN p^{-1-1/r})^2 p^{o(1)},$$

respectively, while the bound for $\mathcal{J}_3$ in (5.12) becomes $\mathcal{J}_3 \ll p^3$. Substituting these estimates to (5.5), we arrive at

$$\begin{aligned} T_1 \leqslant \frac{1}{N} (KM^2 N^2)^{1-1/(2r)} (1 + KM^{-2})^{1/(2r)} (1 + \mathcal{L}_1 MN p^{-1-1/r})^{1/r} \\ \times p^{1/(2r)+1/(2r^2)+o(1)} + (1 + MN/p) KM p^{o(1)}. \end{aligned}$$

From this and inequalities (5.1) and (5.2) Theorem 2.5 follows.

6. Proof of Theorem 2.7

6.1. Preliminary transformations

Assume $\|\boldsymbol{\alpha}\|_\infty \leqslant 1$ and $\gcd(a,b) = 1$ without loss of generality. By periodicity, we also assume that $1 \leqslant |a|, |b| < p/2$. By the Cauchy–Schwarz inequality, we have

$$|\mathfrak{Q}(\boldsymbol{\alpha},\boldsymbol{\beta})|^2 \leqslant \|\boldsymbol{\beta}\|_2^2\, Q, \tag{6.1}$$

where

$$Q = \sum_{k,n\in\mathbb{Z}} \Phi\Big(\frac{k}{K}\Big)\Phi\Big(\frac{n}{N}\Big)\Big|\sum_{\ell\leqslant L}\sum_{m\leqslant M}\alpha_{\ell,m}\,\chi(ak\ell+bmn)\Big|^2,$$

for any smooth function Φ which dominates the characteristic function of $[-1,1]$ and is supported only inside the interval $[-2,2]$. Squaring out and switching the order of summation, we get

$$Q \leqslant |Q_1| + KLMN(LM/p+1)p^{o(1)} \tag{6.2}$$

with

$$Q_1 = \sum_{\substack{\ell_1,\ell_2\leqslant L,\ m_1,m_2\leqslant M\\ \ell_1m_2\not\equiv\ell_2m_1 \bmod p}}\sum_{k,n\in\mathbb{Z}} \Phi\Big(\frac{k}{K}\Big)\Phi\Big(\frac{n}{N}\Big)\alpha_{\ell_1,m_1}\,\overline{\alpha}_{\ell_2,m_2} \times \chi(ak\ell_1+bm_1n)\,\overline{\chi}(ak\ell_2+bm_2n),$$

where the second term in (6.2) comes from the contribution from $\ell_1m_2 \equiv \ell_2m_1 \bmod p$. The trivial bound for Q_1 is

$$Q_1 \ll KL^2M^2N, \tag{6.3}$$

and, by (6.1), we obtain a non-trivial bound of $\mathfrak{Q}(\boldsymbol{\alpha},\boldsymbol{\beta})$ as soon as we improve (6.3). For all integers u, v and w, using that $\mathbb{Z}$ is invariant under shifts by integers, we can write

$$Q_1 = \sum_{\substack{\ell_1,\ell_2\leqslant L,\ m_1,m_2\leqslant M\\ \ell_1m_2\not\equiv\ell_2m_1 \bmod p}}\sum_{k,n\in\mathbb{Z}} \Phi\Big(\frac{k+uv}{K}\Big)\Phi\Big(\frac{n+wv}{N}\Big)\alpha_{\ell_1,m_1}\,\overline{\alpha}_{\ell_2,m_2} \times \chi(a(k+uv)\ell_1+bm_1(n+wv))\,\overline{\chi}(a(k+uv)\ell_2+bm_2(n+wv)).$$

By Fourier inversion and summing over $u\sim U, v\sim V, w\sim W$, with

$$U,V,W \geqslant 1, \quad UV = \frac{1}{4}K \quad\text{and}\quad WV = \frac{1}{4}N, \tag{6.4}$$

it follows that

$$\begin{aligned} Q_1 \ll \frac{1}{UVW}\sum_{|k|\leqslant 2K}\sum_{|n|\leqslant 2N}\sum_{\substack{\ell_1,\ell_2\leqslant L,\ m_1,m_2\leqslant M\\ \ell_1m_2\not\equiv\ell_2m_1 \bmod p}}\sum_{u\sim U}\sum_{w\sim W}\iint_{\mathbb{R}^2}|\widehat{\Phi}(\xi)\,\widehat{\Phi}(\eta)| \\ \times\Big|\sum_{v\sim V}\mathrm{e}\Big(\frac{uv\xi}{K}+\frac{wv\eta}{N}\Big)\chi\big(\overline{(a\ell_1u+bm_1w)}(ak\ell_1+bm_1n)+v\big) \\ \times\overline{\chi}\big(\overline{(a\ell_2u+bm_2w)}(ak\ell_2+bm_2n)+v\big)\Big|\,\mathrm{d}\xi\,\mathrm{d}\eta+\mathsf{Err}_1, \end{aligned} \tag{6.5}$$

where

- the variables of summation satisfy the extra condition

$$p \nmid (a\ell_1 u + bm_1 w)(a\ell_2 u + bm_2 w)(ak\ell_1 + bm_1 n)(ak\ell_2 + bm_2 n), \tag{6.6}$$

- and the term Err_1 corresponds to the error induced by the terms

$$p \mid (a\ell_1 u + bm_1 w)(a\ell_2 u + bm_2 w)(ak\ell_1 + bm_1 n)(ak\ell_2 + bm_2 n).$$

As a typical possibility, the number of tuples (ℓ_1, u, m_1, w) satisfying $p \mid (a\ell_1 u + bm_1 w)$ is at most $LU(1 + MW/p)p^{o(1)}$. Taking all the remaining possibilities into account, we find

$$\mathsf{Err}_1 \leqslant \frac{KL^2MNUV}{UVW}\Big(1 + \frac{MW}{p}\Big)p^{o(1)} \leqslant KL^2M\Big(V + \frac{MN}{p}\Big)p^{o(1)}. \tag{6.7}$$

Combining (6.7) with the inequality $\widehat{\Phi}(\xi) \ll (1 + |\xi|)^{-2}$, and with the change of variables $(\xi, \eta) \to (\xi/u, \eta/w)$ in (6.5), we obtain

$$\begin{aligned} Q_1 \ll \frac{1}{U^2VW^2} \iint_{\mathbb{R}^2} \Big(1 + \frac{|\xi|}{U}\Big)^{-2}\Big(1 + \frac{|\eta|}{W}\Big)^{-2} \sum_{|k|\leqslant 2K} \sum_{|n|\leqslant 2N} \sum_{\substack{\ell_1,\ell_2\leqslant L,\ m_1,m_2\leqslant M\\ \ell_1m_2\not\equiv \ell_2m_1 \bmod p}}\sum\sum\sum\sum \\ \times \sum_{u\sim U}\sum_{w\sim W}\Big|\sum_{v\sim V} \mathrm{e}\Big(\frac{v\xi}{K} + \frac{v\eta}{N}\Big)\chi\big(\overline{(a\ell_1 u + bm_1 w)}(ak\ell_1 + bm_1 n) + v\big) \\ \times \overline{\chi}\big(\overline{(a\ell_2 u + bm_2 w)}(ak\ell_2 + bm_2 n) + v\big)\Big| \mathrm{d}\xi\, \mathrm{d}\eta + \mathsf{Err}_1. \end{aligned}$$

This implies

$$\begin{aligned} Q_1 \ll \frac{1}{UVW} \sum_{|k|\leqslant 2K} \sum_{|n|\leqslant 2N} \sum_{\substack{\ell_1,\ell_2\leqslant L,\ m_1,m_2\leqslant M\\ \ell_1m_2\not\equiv \ell_2m_1 \bmod p}}\sum\sum\sum\sum \\ \times \sum_{u\sim U}\sum_{w\sim W}\Big|\sum_{v\sim V} \mathrm{e}(v\xi)\chi\big(\overline{(a\ell_1 u + bm_1 w)}(ak\ell_1 + bm_1 n) + v\big) \\ \times \overline{\chi}\big(\overline{(a\ell_2 u + bm_2 w)}(ak\ell_2 + bm_2 n) + v\big)\Big| + \mathsf{Err}_1 \end{aligned}$$

for some $\xi \in \mathbb{R}$, where Err_1 satisfies (6.7). We now pull out the gcd of ak and bn for latter purpose. To this end, we put

$$d = \gcd(ak, bn), \quad d_1 = \frac{d}{\gcd(a,d)}, \quad d_2 = \frac{d}{\gcd(b,d)},$$
$$a^* = \frac{a}{\gcd(a,d)} \quad \text{and} \quad b^* = \frac{b}{\gcd(b,d)}.$$

We observe that $p \nmid d$, $\gcd(a,d) = \gcd(a,n)$, $\gcd(b,d) = \gcd(b,k)$, and $d \leqslant D$ with

$$D = \min\{|a|K, |b|N\} \ (< p^2).$$

Note that $d \mid ak$ implies $d_1 \mid k$, and similarly, $d \mid bn$ implies $d_2 \mid n$. Hence, we have the relations $d_1 \mid k$, $d_2 \mid n$, $ad_1 = a^* d$ and $bd_2 = b^* d$. Therefore, changing the variables

$$k \mapsto d_1 k, \quad n \mapsto d_2 n, \tag{6.8}$$

we obtain the inequality

$$Q_1 \ll \frac{1}{UVW} \sum_{\substack{d \leqslant D \\ p \nmid d}} Q_1(d) + \mathsf{Err}_1 \tag{6.9}$$

with

$$\begin{aligned} Q_1(d) = \sum_{\substack{|k| \leqslant 2K/d_1 \\ \gcd(a^*k, b^*n)=1}} \sum_{|n| \leqslant 2N/d_2} \sum\sum_{\substack{\ell_1, \ell_2 \leqslant L, \\ \ell_1 m_2 \not\equiv \ell_2 m_1 \bmod p}} \sum\sum_{m_1, m_2 \leqslant M} \\ \times \sum_{u \sim U} \sum_{w \sim W} \Bigg| \sum_{v \sim V} \mathrm{e}(v\xi)\, \chi\big(\overline{(a\ell_1 u + bm_1 w)}(ad_1 k\ell_1 + bd_2 m_1 n) + v\big) \\ \times \bar{\chi}(\overline{(a\ell_2 u + bm_2 w)}(ad_1 k\ell_2 + bd_2 m_2 n) + v)\Bigg|. \end{aligned}$$

Writing $ad_1 k\ell_1 + bd_2 m_1 n = d(a^* k\ell_1 + b^* m_1 n)$, we now continue as

$$\begin{aligned} Q_1(d) = \sum_{\substack{|k| \leqslant 2K/d_1 \\ \gcd(a^*k, b^*n)=1}} \sum_{|n| \leqslant 2N/d_2} \sum\sum_{\substack{\ell_1, \ell_2 \leqslant L, \\ \ell_1 m_2 \not\equiv \ell_2 m_1 \bmod p}} \sum\sum_{m_1, m_2 \leqslant M} \\ \times \sum_{u \sim U} \sum_{w \sim W} \Bigg| \sum_{v \sim V} \mathrm{e}(v\xi) \chi(d\,\overline{(a\ell_1 u + bm_1 w)}(a^* k\ell_1 + b^* m_1 n) + v) \\ \times \bar{\chi}(d\,\overline{(a\ell_2 u + bm_2 w)}(a^* k\ell_2 + b^* m_2 n) + v)\Bigg|, \end{aligned}$$

which can be also interpreted as

$$\begin{aligned} Q_1(d) = \sum_{\substack{|k| \leqslant 2K/d_1 \\ \gcd(a^*k, b^*n)=1}} \sum_{|n| \leqslant 2N/d_2} \sum\sum_{\substack{\ell_1, \ell_2 \leqslant L, \\ \ell_1 m_2 \not\equiv \ell_2 m_1 \bmod p}} \sum\sum_{m_1, m_2 \leqslant M} \\ \times \sum_{\substack{u \sim \gcd(a,d)U \\ \gcd(a,d) \mid u}} \sum_{\substack{w \sim \gcd(b,d)W \\ \gcd(b,d) \mid w}} \Bigg| \sum_{v \sim V} \mathrm{e}(v\xi) \chi(d\,\overline{(a^*\ell_1 u + b^* m_1 w)}(a^* k\ell_1 + b^* m_1 n) + v) \\ \times \bar{\chi}(d\,\overline{(a^*\ell_2 u + b^* m_2 w)}(a^* k\ell_2 + b^* m_2 n) + v)\Bigg|. \end{aligned}$$

Here we have used the formulas $a^* = a/\gcd(a,d)$, $b^* = b/\gcd(b,d)$. Of course, the variables of summation continue to satisfy (6.6) with necessary changes of variables as in (6.8). We further impose a restriction that $kw \gcd(b,d) \neq nu \gcd(a,d)$, which introduces an additional error $\mathsf{Err}_2(d)$ with

$$\sum_{d \leqslant D} \mathsf{Err}_2(d) \leqslant KL^2 M^2 VW p^{o(1)}.$$

Next for $x_1, x_2 \in \mathbb{F}_p^*$, and for

$$1 \leqslant A \ll \mathcal{L}_2/d, \quad 1 \leqslant B \ll |a|LU + |b|MW \ll \mathcal{L}_2/V, \quad 1 \leqslant C \leqslant K/d_1,$$

we put

$$\varrho(x_1, x_2) = \sum_{|k|\sim C} \sum_{|n|\leqslant 2N/d_2} \sum_{\ell_1,\ell_2\leqslant L} \sum\sum_{m_1,m_2\leqslant M} \sum_{u\sim U} \sum_{w\sim W} 1, \tag{6.10}$$
$$\begin{gathered} a^*k\ell_1+b^*m_1n\equiv(a\ell_1u+bm_1w)x_1 \bmod p \\ a^*k\ell_2+b^*m_2n\equiv(a\ell_2u+bm_2w)x_2 \bmod p \\ \ell_1m_2\not\equiv\ell_2m_1 \bmod p, \quad kw\gcd(b,d)\neq nu\gcd(a,d), \quad \gcd(a^*k,b^*n)=1 \\ |a^*k\ell_1+b^*m_1n|\sim A,\ |a\ell_2u+bm_2w|\sim B \end{gathered}$$

where the condition (6.6) continues to apply to the variables of summation with necessary changes of variables as in (6.8). We now have

$$Q_1(d) \leqslant p^{o(1)} \sup_{\substack{1\leqslant A\ll\mathcal{L}_2/d\\ 1\leqslant B\ll\mathcal{L}_2/V\\ 1\leqslant C\leqslant K/d_1}} \sum_{x_1,x_2\in\mathbb{F}_p^*} \varrho(x_1,x_2)\Big|\sum_{v\sim V} \mathrm{e}(v\xi)\chi(dx_1+v)\overline{\chi}(dx_2+v)\Big| + \mathsf{Err}_2(d).$$

Applying the Hölder inequality with a positive integer $r \geqslant 2$, we find

$$Q_1(d) \leqslant Q_2(d)\, p^{o(1)} + \mathsf{Err}_2(d), \tag{6.11}$$

where

$$Q_2(d) = \sup_{\substack{1\leqslant A\ll\mathcal{L}_2/d\\ 1\leqslant B\ll\mathcal{L}_2/V\\ 1\leqslant C\leqslant K/d_1}} \Sigma_1^{1-1/r}\,(\Sigma_2\cdot\Sigma_3)^{1/(2r)} \tag{6.12}$$

with

$$\Sigma_j = \Sigma_j(A,B,C) = \sum_{x_1,x_2\in\mathbb{F}_p^*}\sum \varrho(x_1,x_2;A,B,C)^j, \quad \text{for } j=1,2,$$

and

$$\Sigma_3 = \sum_{x_1,x_2\in\mathbb{F}_p}\sum \Big|\sum_{v\sim V} \mathrm{e}(v\xi)\chi(x_1+v)\overline{\chi}(x_2+v)\Big|^{2r}.$$

Trivially, we have

$$\Sigma_1 \ll CL^2M^2NUWd_2^{-1}. \tag{6.13}$$

Furthermore, using Lemma 3.2, we have the inequality

$$\Sigma_3 \ll V^{2r}p + V^r p^2. \tag{6.14}$$

Next we estimate Σ_2.

6.2. Bounding Σ_2

This following bound is the core of our method.

Lemma 6.1. *With the above notation, we have*

$$\Sigma_2 \leqslant (M/C+1)^2\Big(1+\frac{\mathcal{L}_2^2}{dpV}\Big)^2(ABLM)^{1+o(1)}(CW\gcd(b,d)+NU\gcd(a,d)/d_2)$$

for all $1 \leqslant A \ll \mathcal{L}_2/d$, $1 \leqslant B \ll \mathcal{L}_2/V$ *and* $1 \leqslant C \leqslant K/d_1$.

Proof. Let $U_1 = \gcd(a,d)U$ and $W_1 = \gcd(b,d)W$. We operate the changes of variables

$$u \mapsto \frac{u}{\gcd(a,d)}, \quad w \mapsto \frac{w}{\gcd(b,d)} \tag{6.15}$$

in the definition (6.10) of $\rho(x_1,x_2)$. Note that Σ_2 is bounded by the number of tuples with length 16

$$(k,\tilde{k},\ell_1,\tilde{\ell}_1,\ell_2,\tilde{\ell}_2,m_1,\tilde{m}_1,m_2,\tilde{m}_2,n,\tilde{n},u,\tilde{u},w,\tilde{w})$$

satisfying

$$\begin{aligned}
&|k|,|\tilde{k}| \sim C, \quad \ell_1,\tilde{\ell}_1,\ell_2,\tilde{\ell}_2 \leqslant L, \quad m_1,\tilde{m}_1,m_2,\tilde{m}_2 \leqslant M, \quad |n|,|\tilde{n}| \leqslant 2N/d_2,\\
&u,\tilde{u} \sim U_1, \quad w,\tilde{w} \sim W_1, \quad kw \neq nu, \quad \tilde{k}\tilde{w} \neq \tilde{n}\tilde{u},\\
&\gcd(a^*k,b^*n) = \gcd(a^*\tilde{k},b^*\tilde{n}) = 1, \quad |a^*k\ell_1 + b^*m_1n| \sim A,\\
&|a^*\tilde{k}\tilde{\ell}_1 + b^*\tilde{m}_1\tilde{n}| \sim A, \quad |a^*\ell_2u + b^*m_2w| \sim B, \quad |a^*\tilde{\ell}_2\tilde{u} + b^*\tilde{m}_2\tilde{w}| \sim B,\\
&\ell_1m_2 \not\equiv \ell_2m_1 \bmod p, \quad \tilde{\ell}_1\tilde{m}_2 \not\equiv \tilde{\ell}_2\tilde{m}_1 \bmod p,
\end{aligned}$$

with the additional non-divisibility conditions

$$p \nmid (a^*\ell_1u + b^*m_1w)(a^*\ell_2u + b^*m_2w)(a^*k\ell_1 + b^*m_1n)(a^*k\ell_2 + b^*m_2n), \tag{6.16}$$

and

$$p \nmid (a^*\tilde{\ell}_1\tilde{u} + b^*\tilde{m}_1\tilde{w})(a^*\tilde{\ell}_2\tilde{u} + b^*\tilde{m}_2\tilde{w})(a^*\tilde{k}\tilde{\ell}_1 + b^*\tilde{m}_1\tilde{n})(a^*\tilde{k}\tilde{\ell}_2 + b^*\tilde{m}_2\tilde{n}), \tag{6.17}$$

and also such that

$$(a^*k\ell_1+b^*m_1n)(a^*\tilde{\ell}_1\tilde{u}+b^*\tilde{m}_1\tilde{w}) = (a^*\tilde{k}\tilde{\ell}_1+b^*\tilde{m}_1\tilde{n})(a^*\ell_1u+b^*m_1w) + z_1p, \tag{6.18}$$

and

$$(a^*k\ell_2+b^*m_2n)(a^*\tilde{\ell}_2\tilde{u}+b^*\tilde{m}_2\tilde{w}) = (a^*\tilde{k}\tilde{\ell}_2+b^*\tilde{m}_2\tilde{n})(a^*\ell_2u+b^*m_2w) + z_2p, \tag{6.19}$$

with some $0 \leqslant |z_1|, |z_2| \leqslant Z$, where

$$Z = 1 + 4(|a|KL + |b|MN)(|a|LU + |b|MW)/(dp),$$

so by hypothesis we have the inequality

$$Z \ll 1 + \frac{\mathcal{L}_2^2}{dpV}. \tag{6.20}$$

Note that the conditions (6.16) and (6.17) are resulted by (6.6) with changes of variables as in (6.8) and (6.15).

We now fix $k, \ell_1, \ell_2, m_1, m_2, n, u, w$, and put

$$a_j = a^* k\ell_j + b^* m_j n, \quad b_j = a^* \ell_j u + b^* m_j w$$

for $j = 1, 2$. Note that

$$|a_1| \sim A, \quad |a_2| \leqslant 2\mathcal{L}_2/d, \quad |b_1| \leqslant \mathcal{L}_2/V, \quad |b_2| \sim B,$$

with $a_1 a_2 b_1 b_2 \neq 0$. Given z_1, z_2 with $0 \leqslant |z_1|, |z_2| \leqslant Z$ as above, we now look at the equations

$$a_1 x_1 = b_1 y_1 + z_1 p, \quad a_2 x_2 = b_2 y_2 + z_2 p \tag{6.21}$$

in $x_1, x_2, y_1, y_2 \in \mathbb{Z}$ with $|x_1| \leqslant \mathcal{L}_2/V$, $|x_2| \sim B$, $|y_1| \sim A$ and $|y_2| \leqslant 2\mathcal{L}_2/d$. It is clear that the number of such tuples (x_1, x_2, y_1, y_2) satisfying (6.21) is bounded, up to an absolute constant, by

$$\Big(\frac{A \gcd(a_1, b_1)}{a_1} + 1\Big)\Big(\frac{B \gcd(a_2, b_2)}{b_2} + 1\Big) \ll \gcd(a_1, b_1) \gcd(a_2, b_2). \tag{6.22}$$

We claim that, for given $k, \ell_1, \ell_2, m_1, m_2, n, u, w, z_1, z_2$ as above, the number $\mathcal{N}$ of tuples $(\tilde{k}, \tilde{\ell}_1, \tilde{\ell}_2, \tilde{m}_1, \tilde{m}_2, \tilde{n}, \tilde{u}, \tilde{w})$ satisfying the above-mentioned conditions satisfies

$$\mathcal{N} \ll (M/C + 1)^2. \tag{6.23}$$

Hence

$$\Sigma_2 \ll \Big(\frac{M}{C} + 1\Big)^2 Z^2 \sum_{|k| \sim C} \sum_{\ell_1, \ell_2 \leqslant L} \sum_{m_1, m_2 \leqslant M} \sum_{|n| \leqslant 2N/d_2} \sum_{u \sim U_1} \sum_{w \sim W_1} \gcd(a_1, b_1) \gcd(a_2, b_2)$$
$$\substack{a^* k\ell_1 + b^* m_1 n = a_1,\ a^* \ell_1 u + b^* m_1 w = b_1 \\ a^* k\ell_2 + b^* m_2 n = a_2,\ a^* \ell_2 u + b^* m_2 w = b_2 \\ |a_1| \sim A,\ |b_2| \sim B,\ kw \neq nu}$$

in view of (6.22). Then the desired bound for Σ_2 follows from (6.20) and Lemma 3.3.

It suffices to prove (6.23), and keep in mind that $k, \ell_1, \ell_2, m_1, m_2, n, u, w, z_1, z_2$ are all fixed. We now fix one of such tuples (x_1, x_2, y_1, y_2), satisfying (6.21). Then (6.18) and (6.19) lead us to consider the system of four equations

$$\begin{cases} a^* \tilde{\ell}_1 \tilde{u} + b^* \tilde{m}_1 \tilde{w} = x_1, \\ a^* \tilde{k} \tilde{\ell}_1 + b^* \tilde{m}_1 \tilde{n} = y_1, \\ a^* \tilde{\ell}_2 \tilde{u} + b^* \tilde{m}_2 \tilde{w} = x_2, \\ a^* \tilde{k} \tilde{\ell}_2 + b^* \tilde{m}_2 \tilde{n} = y_2, \end{cases} \tag{6.24}$$

in $\tilde{k}, \tilde{\ell}_1, \tilde{\ell}_2, \tilde{m}_1, \tilde{m}_2, \tilde{n}, \tilde{u}, \tilde{w} \in \mathbb{Z}$. Recalling the restriction $\tilde{\ell}_1 \tilde{m}_2 \not\equiv \tilde{\ell}_2 \tilde{m}_1 \bmod p$, it suffices to consider the solutions satisfying $\tilde{\ell}_1 \tilde{m}_2 \neq \tilde{\ell}_2 \tilde{m}_1$.

We now fix integers $\mathfrak{l}_1, \mathfrak{l}_2, \mathfrak{m}_1$ and $\mathfrak{m}_2$ satisfying

$$\mathfrak{l}_1, \mathfrak{l}_2 \leqslant L, \quad \mathfrak{m}_1, \mathfrak{m}_2 \leqslant M, \quad \mathfrak{l}_1 \mathfrak{m}_2 \neq \mathfrak{l}_2 \mathfrak{m}_1. \tag{6.25}$$

such that the two equations

$$a^* \tilde{k} \mathfrak{l}_1 + b^* \mathfrak{m}_1 \tilde{n} = y_1, \quad a^* \tilde{k} \mathfrak{l}_2 + b^* \mathfrak{m}_2 \tilde{n} = y_2 \tag{6.26}$$

are solvable in $\tilde{k}, \tilde{n}$ with $\gcd(\tilde{k}, \tilde{n}) = 1$, given the above $\mathfrak{l}_1, \mathfrak{l}_2, \mathfrak{m}_1, \mathfrak{m}_2$. Note that the system (6.26) has at most one solution $(\tilde{k}, \tilde{n})$ because its determinant does not vanish. Suppose that a solution to (6.26) does exist. Then by (6.25) all solutions to the second equation in (6.24) are of the shape

$$\tilde{\ell}_1 = \mathfrak{l}_1 - s_1 b^* \tilde{n}, \quad \tilde{m}_1 = \mathfrak{m}_1 + s_1 a^* \tilde{k}, \quad 0 \leqslant |s_1| \ll M/|\tilde{k}| \ll M/C,$$

and all solutions to the fourth equation in (6.24) are of the shape

$$\tilde{\ell}_2 = \mathfrak{l}_2 - s_2 b^* \tilde{n}, \quad \tilde{m}_2 = \mathfrak{m}_2 + s_2 a^* \tilde{k}, \quad 0 \leqslant |s_2| \ll M/|\tilde{k}| \ll M/C.$$

After determining $\tilde{\ell}_1, \tilde{\ell}_2, \tilde{m}_1, \tilde{m}_2$ with $\tilde{\ell}_1 \tilde{m}_2 \neq \tilde{\ell}_2 \tilde{m}_1$, we may find at most one tuple $(\tilde{u}, \tilde{w})$ satisfying the first and third equations in (6.24) simultaneously.

We have proved (6.23) so far, and thus completed the proof of Lemma 6.1. ∎

Subsequently, by Lemma 6.1, for all $1 \leqslant A \ll \mathcal{L}_2/d$, $1 \leqslant B \ll |a|LU + |b|MW \ll \mathcal{L}_2/V$ and $1 \leqslant C \leqslant K/d_1$, we have the bound

$$\begin{aligned} \Sigma_2 &\leqslant (M/C+1)^2\Big(1+\frac{\mathcal{L}_2^2}{dpV}\Big)^2 \\ &\quad \times \frac{(\mathcal{L}_2^2 LM)^{1+o(1)}}{dV}(CW\gcd(b,d) + NU\gcd(a,d)/d_2). \end{aligned} \tag{6.27}$$

6.3. Concluding the proof of Theorem 2.7

We substitute the bounds (6.13), (6.14) and (6.27) into (6.12) and note that

$$d_1 d_2 = \frac{d^2}{\gcd(a,d)\gcd(b,d)} = \frac{d^2}{\gcd(ab,d)}$$

since we have assumed $\gcd(a,b) = 1$. Hence, we derive

$$\begin{aligned} Q_2(d) &\leqslant p^{o(1)} \sup_{C \leqslant K/d_1} (CL^2M^2NUWd_2^{-1})^{1-1/r}(M/C+1)^{1/r}\Big(1+\frac{\mathcal{L}_2^2}{dpV}\Big)^{1/r} \\ &\quad \times \Big(\frac{\mathcal{L}_2^2 LM}{dV}\Big)^{1/(2r)}(CW\gcd(b,d) + NU\gcd(a,d)/d_2)^{1/(2r)}(V^{2r}p + V^r p^2)^{1/(2r)}. \end{aligned}$$

It is easy to see that in the last expression, after expanding, C appears only in positive powers, and therefore the supremum is attained at $C = K/d_1$. Hence,

$$\begin{aligned} Q_2(d) &\leqslant p^{o(1)}(KL^2M^2NUW/d^2)^{1-1/r}(d_1M/K+1)^{1/r}\Big(1+\frac{\mathcal{L}_2^2}{dpV}\Big)^{1/r} \\ &\quad \times \Big(\frac{\mathcal{L}_2^2 LM}{dV}\Big)^{1/(2r)}\gcd(ab,d)^{1-1/r}(KW\gcd(b,d)/d_1 \\ &\quad + NU\gcd(a,d)/d_2)^{1/(2r)}(V^{2r}p + V^r p^2)^{1/(2r)} \\ &\leqslant p^{o(1)}(KL^2M^2NUW/d^2)^{1-1/r}(d_1M/K+1)^{1/r}\Big(1+\frac{\mathcal{L}_2^2}{dpV}\Big)^{1/r} \\ &\quad \times \Big(\frac{\mathcal{L}_2^2 KLMN}{d^2V^2}\Big)^{1/(2r)}\gcd(ab,d)^{1-1/(2r)}(V^{2r}p + V^r p^2)^{1/(2r)}. \end{aligned}$$

We also note that

$$d^{-2+2/r} \cdot d_1^{1/r} \cdot d^{-1/r} \cdot \gcd(ab, d)^{1-1/(2r)} \leqslant d^{-2+2/r} \gcd(ab, d)^{1-1/(2r)} \leqslant d^{-1} \gcd(ab, d)^{1-1/(2r)}$$

for $r \geqslant 2$. Recalling (6.7), (6.9) and (6.11) and then summing over $d \leqslant D$, we obtain

$$\begin{aligned} Q_1 &\ll \frac{p^{o(1)}}{UVW} \sum_{d \leqslant D} (Q_2(d) + \mathsf{Err}_2(d)) + \mathsf{Err}_1 \\ &\leqslant p^{o(1)} (KL^2M^2N)^{1-1/r} (UVW)^{-1/r} (M/K+1)^{1/r} \Big(1 + \frac{\mathcal{L}_2^2}{pV}\Big)^{1/r} \\ &\quad \times (\mathcal{L}_2^2 KLMNp)^{1/(2r)} (1 + V^{-1/2} p^{1/(2r)}) \\ &\quad + KL^2M^2U^{-1}p^{o(1)} + KL^2M\Big(V + \frac{MN}{p}\Big)p^{o(1)}. \end{aligned}$$

Taking

$$V = p^{1/r}, \qquad U = \frac{1}{4} K p^{-1/r}, \qquad W = \frac{1}{4} N p^{-1/r},$$

so that the assumption (6.4) is satisfied, we derive that

$$\begin{aligned} Q_1 &\leqslant (KL^2M^2N)^{1-1/r} (KN)^{-1/r} (M/K+1)^{1/r} \Big(1 + \frac{\mathcal{L}_2^2}{p^{1+1/r}}\Big)^{1/r} (\mathcal{L}_2^2 KLMN)^{1/(2r)} \\ &\quad \times p^{1/(2r)+1/r^2+o(1)} + (LM)^2 p^{1/r+o(1)} + KL^2M\Big(p^{1/r} + \frac{MN}{p}\Big)p^{o(1)} \\ &\leqslant (KLMN)^{2-3/(2r)} (KN)^{-1} (M/K+1)^{1/r} \Big(1 + \frac{\mathcal{L}_2^2}{p^{1+1/r}}\Big)^{1/r} \mathcal{L}_2^{1/r} p^{1/(2r)+1/r^2+o(1)} \\ &\quad + (LM)^2 p^{1/r+o(1)} + KL^2M\Big(p^{1/r} + \frac{MN}{p}\Big)p^{o(1)}. \end{aligned}$$

It remains to recall (6.1) and (6.2) to conclude the proof of Theorem 2.7.

7. Proof of Theorem 2.11

Let $p > \max\{K, M, N\}$. Consider the trilinear sum of Legendre symbols

$$\mathfrak{S} = \sum_{k \leqslant K} \sum_{m \in \mathcal{M}} \sum_{n \in \mathcal{N}} \Big(\frac{k + mn}{p}\Big),$$

with

$$K = \lfloor p^{1+1/r+\eta} (MN)^{-2} + p^{\eta} \rfloor. \tag{7.1}$$

Suppose that the values of $k + mn$, for all given k, m, n in the above ranges, are always quadratic non-residues or zero modulo p. Then we see from (2.6) that $\mathfrak{S}$ satisfies the trivial bound

$$|\mathfrak{S}| \geqslant c_0^2 KMN + O((MN/p + 1)Kp^{o(1)}),$$

where the error term accounts for the cases with $k + mn \equiv 0 \pmod p$.

Therefore, Theorem 2.11 is proved as soon as we have the bound

$$\mathfrak{S} = o(KMN) \tag{7.2}$$

under the hypotheses (2.5) and p tending to infinity.

We first consider the case $(MN)^2 > p^{1+1/r}$, for which we see from (7.1) that $K \asymp p^{\eta}$. Now (7.2) is an immediate consequence of Karatsuba presented already in (1.6) and (1.5). We henceforth assume that $(MN)^2 \leqslant p^{1+1/r}$. Applying Theorem 2.5 with the choice

$$a = b = 1, \quad \alpha_m = \mathbf{1}_{\mathcal{M}}(m) \quad \text{and} \quad \beta_{k,n} = \mathbf{1}_{[1,K]}(k) \cdot \mathbf{1}_{\mathcal{N}}(n),$$

we deduce that (7.2) is proved as soon as one has the following three inequalities:

$$M \geqslant K^{1/2}, \quad K(MN)^2 \geqslant p^{1+1/r+\eta/2}, \quad M \geqslant p^{\eta/4}.$$

The choice (7.1) guarantees the above three conditions provided that

$$M \geqslant p^{\eta/4} \quad \text{and} \quad M^4N^2 > p^{1+1/r+\eta}.$$

The restriction $M \geqslant p^{\eta/4}$ can also be dropped, since otherwise we should have $N^2 > p^{1+1/r}$, and we may instead appeal to Karatsuba by noting that $K \geqslant p^{\eta}$ thanks to the choice (7.1). This completes the proof of Theorem 2.11.

A. Karatsuba's bound for double character sums

Recall that

$$\mathfrak{B}(\boldsymbol{\alpha}, \boldsymbol{\beta}) = \sum_{m \in \mathcal{M}} \sum_{n \in \mathcal{N}} \alpha_m \beta_n \chi(m+n)$$

as in (1.3) We now give a proof of (1.6) in the range of (1.5). More precisely, we have the following explicit estimate for $\mathfrak{B}(\boldsymbol{\alpha}, \boldsymbol{\beta})$.

Theorem A.1. *Let χ be a non-trivial character of $\mathbb{F}_p^{\times}$ and $\mathcal{M}, \mathcal{N} \subseteq \mathbb{F}_p$ two arbitrary subsets with cardinalities M, N, respectively. For each positive integer r, we have*

$$\mathfrak{B}(\boldsymbol{\alpha}, \boldsymbol{\beta}) \ll \|\boldsymbol{\alpha}\|_1^{1-1/r} \|\boldsymbol{\alpha}\|_2^{1/r} \|\boldsymbol{\beta}\|_{\infty} (Np^{1/(4r)} + N^{1/2} p^{1/(2r)}),$$

where the implicit constant depends only on r.

Remark A.2. Theorem A.1 implies that

$$\mathfrak{B}(\boldsymbol{\alpha}, \boldsymbol{\beta}) \ll \|\boldsymbol{\alpha}\|_{\infty} \|\boldsymbol{\beta}\|_{\infty} MN(M^{-1/(2r)} p^{1/(4r)} + M^{-1/(2r)} N^{-1/2} p^{1/(2r)}).$$

This readily implies (1.6) for

$$M > p^{1/2+\eta} \quad \text{and} \quad N > p^{\eta}$$

by taking $r > 1/\eta$.

The proof is quite short. From the Hölder inequality, it follows that

$$|\mathfrak{B}(\boldsymbol{\alpha}, \boldsymbol{\beta})| \leqslant \sum_{m \in \mathcal{M}} |\alpha_m| \Big| \sum_{n \in \mathcal{N}} \beta_n \chi(m+n) \Big| \leqslant \|\boldsymbol{\alpha}\|_1^{1-1/r} \|\boldsymbol{\alpha}\|_2^{1/r} W^{1/(2r)},$$

where

$$W = \sum_{m \in \mathcal{M}} \Big| \sum_{n \in \mathcal{N}} \beta_n \chi(m+n) \Big|^{2r}.$$

The ingredient here is that one enlarges the sum over m to $\mathbb{F}_p$, and ignores the structure of $\mathcal{M}$, so that

$$W \leqslant \sum_{m \in \mathbb{F}_p} \Big| \sum_{n \in \mathcal{N}} \beta_n \chi(m+n) \Big|^{2r}.$$

Now Theorem A.1 follows immediately from Lemma 3.1.

Funding. During the preparation of this work I. S. was supported in part by the Australian Research Council Grants DP230100530 and DP230100534, and P. X. was supported in part by the National Natural Science Foundation of China (no. 12025106).

References

[1] Banks, W. and Shparlinski, I. E.: Congruences with intervals and arbitrary sets. *Arch. Math. (Basel)* **114** (2020), no. 5, 527–539. Zbl 1483.11260 MR 4088555

[2] Bourgain, J., Garaev, M. Z., Konyagin, S. V. and Shparlinski, I. E.: On the hidden shifted power problem. *SIAM J. Comput.* **41** (2012), no. 6, 1524–1557. Zbl 1311.11111 MR 3023803

[3] Bourgain, J., Garaev, M. Z., Konyagin, S. V. and Shparlinski, I. E.: On congruences with products of variables from short intervals and applications. *Proc. Steklov Inst. Math.* **280** (2013), 61–90. (Translated from *Tr. Mat. Inst. Steklova* **280** (2013), 67–96.) Zbl 1301.11041 MR 3241837

[4] Bourgain, J., Konyagin, S. V. and Shparlinski, I. E.: Character sums and deterministic polynomial root finding in finite fields. *Math. Comp.* **84** (2015), no. 296, 2969–2977. Zbl 1400.11153 MR 3378857

[5] Chang, M.-C.: On a question of Davenport and Lewis and new character sum bounds in finite fields. *Duke Math. J.* **145** (2008), no. 3, 409–442. Zbl 1241.11137 MR 2462111

[6] Chang, M.-C.: Character sums in finite fields. In *Finite fields: Theory and applications*, pp. 83–98,. Contemp. Math. 518, American Mathematical Society, Providence, RI, 2010. Zbl 1227.11121 MR 2648541

[7] Chen, J. R.: On the representation of a larger even integer as the sum of a prime and the product of at most two primes. *Sci. Sinica* **16** (1973), 157–176. Zbl 0319.10056 MR 434997

[8] Davenport, H. and Erdős, P.: The distribution of quadratic and higher residues. *Publ. Math. Debrecen* **2** (1952), 252–265. Zbl 0050.04302 MR 55368

[9] Di Benedetto, D., Solymosi, J. and White, E. P.: On the directions determined by a Cartesian product in an affine Galois plane. *Combinatorica* **41** (2021), no. 6, 755–763. Zbl 1499.51005 MR 4357429

[10] Fouvry, É.: Répartition des suites dans les progressions arithmétiques. *Acta Arith.* **41** (1982), no. 4, 359–382. Zbl 0469.10028 MR 677549

[11] Fouvry, É. and Shparlinski, I. E.: On character sums with determinants. *Sci. China Math.* **66** (2023), no. 12, 2693–2714. Zbl 1542.11071 MR 4670144

[12] Friedlander, J. and Iwaniec, H.: Estimates for character sums. *Proc. Amer. Math. Soc.* **119** (1993), no. 2, 365–372. Zbl 0782.11022 MR 1152276

[13] Hanson, B.: Estimates for character sums with various convolutions. *Acta Arith.* **179** (2017), no. 2, 133–146. Zbl 1391.11095 MR 3670200

[14] Hanson, B. and Petridis, G.: Refined estimates concerning sumsets contained in the roots of unity. *Proc. Lond. Math. Soc. (3)* **122** (2021), no. 3, 353–358. Zbl 1497.11029 MR 4230057

[15] Iwaniec, H. and Kowalski, E.: *Analytic number theory*. Amer. Math. Soc. Colloq. Publ. 53, American Mathematical Society, Providence, RI, 2004. Zbl 1059.11001 MR 2061214

[16] Iwaniec, H. and Sárközy, A.: On a multiplicative hybrid problem. *J. Number Theory* **26** (1987), no. 1, 89–95. Zbl 0607.10030 MR 883536

[17] Karatsuba, A. A.: A certain arithmetic sum. *Soviet Math. Dokl.* **12** (1971), 1172–1174. (Translated from *Dokl. Akad. Nauk SSSR* **199** (1971), 770–772.) Zbl 0227.10036 MR 291102

[18] Karatsuba, A. A.: Distribution of values of Dirichlet characters on additive sequences. *Soviet Math. Dokl.* **44** (1992), 145–148. (Translated from *Dokl. Akad. Nauk SSSR* **319** (1991), no. 3, 543–545.) Zbl 0772.11028 MR 1148968

[19] Karatsuba, A. A.: *Basic analytic number theory*. Springer, Berlin, 1993. Zbl 0767.11001 MR 1215269

[20] Karatsuba, A. A.: Weighted character sums. *Izv. Math.* **64** (2000), no. 2, 249–263. (Translated from *Izv. Ross. Akad. Nauk Ser. Mat.* **64** (2000), no. 2, 29–42.) Zbl 0963.11046 MR 1770671

[21] Karatsuba, A. A.: Arithmetic problems in the theory of Dirichlet characters. *Russian Math. Surveys* **63** (2008), no. 4, 641–690. (Translated from *Uspekhi Mat. Nauk* **63** (2008), no. 4, 43–92.) Zbl 1230.11099 MR 2483199

[22] Koh, D., Mirzaei, M., Pham, T. and Shen, C.-Y.: Exponential sum estimates over prime fields. *Int. J. Number Theory* **16** (2020), no. 2, 291–308. Zbl 1484.11041 MR 4077423

[23] Roche-Newton, O., Shparlinski, I. E. and Winterhof, A.: Analogues of the Balog–Wooley decomposition for subsets of finite fields and character sums with convolutions. *Ann. Comb.* **23** (2019), no. 1, 183–205. Zbl 1473.11033 MR 3921343

[24] Schoen, T. and Shkredov, I. D.: Character sums estimates and an application to a problem of Balog. *Indiana Univ. Math. J.* **71** (2022), no. 3, 953–964. Zbl 1528.11075 MR 4448574

[25] Shkredov, I. D. and Shparlinski, I. E.: On some multiple character sums. *Mathematika* **63** (2017), no. 2, 553–560. Zbl 1427.11078 MR 3706596

[26] Shkredov, I. D. and Shparlinski, I. E.: Double character sums over intervals and arbitrary sets. *Proc. Steklov Math. Inst.* **303** (2018), 239–258. (Translated from *Tr. Mat. Inst. Steklova* **303** (2018), 258–278.) Zbl 1459.11166 MR 3918867

[27] Shkredov, I. D. and Volostnov, A. S.: Sums of multiplicative characters with additive convolutions. *Proc. Steklov Math. Inst.* **296** (2017), 256–269. (Translated from *Tr. Mat. Inst. Steklova* **303** (2018), 265–279.) Zbl 1371.11127 MR 3640789

[28] Vinogradov, I. M.: *Elements of number theory*. Dover Publications, New York, 1954. Zbl 0057.28201 MR 62138

[29] Volostnov, A. S.: On double sums with multiplicative characters. *Math. Notes* **104** (2018), 197–203. (Translated from *Mat. Zametki* **104** (2018), no. 2, 174–182.) Zbl 1444.11163 MR 3833493

[30] Weil, A.: *Sur les courbes algébriques et les variétés qui s'en déduisent*. Hermann & Cie, Paris, 1948. Zbl 0036.16001 MR 27151

[31] Xi, P.: Bilinear forms with trace functions over arbitrary sets and applications to Sato–Tate. *Sci. China Math.* **66** (2023), no. 12, 2819–2834. Zbl 1544.11101 MR 4670153

Received May 13, 2024; revised October 7, 2024.

Étienne Fouvry
Département de Mathématiques, Université Paris-Saclay
91405 Orsay Cedex, France;
etienne.fouvry@universite-paris-saclay.fr

Igor E. Shparlinski
School of Mathematics and Statistics, University of New South Wales
Sydney, NSW 2052, Australia;
igor.shparlinski@unsw.edu.au

Ping Xi
School of Mathematics and Statistics, Xi'an Jiaotong University
710049 Xi'an, P. R. China;
ping.xi@xjtu.edu.cn