On the distribution of Jacobi sums

Qing Lu∗ Weizhe Zheng† Zhiyong Zheng‡§

Abstract

Let \( F_q \) be a finite field of \( q \) elements. For multiplicative characters \( \chi_1, \ldots, \chi_m \) of \( F_q^\times \), we let \( J(\chi_1, \ldots, \chi_m) \) denote the Jacobi sum. Nicholas Katz and Zhiyong Zheng showed that for \( m = 2 \), the normalized Jacobi sum \( q^{-1/2}J(\chi_1, \chi_2) \) (\( \chi_1\chi_2 \) nontrivial) is asymptotically equidistributed on the unit circle as \( q \to \infty \), when \( \chi_1 \) and \( \chi_2 \) run through all nontrivial multiplicative characters of \( F_q^\times \). In this paper, we show a similar property for \( m \geq 2 \). More generally, we show that the normalized Jacobi sum \( q^{-(m-1)/2}J(\chi_1, \ldots, \chi_m) \) (\( \chi_1 \cdots \chi_m \) nontrivial) is asymptotically equidistributed on the unit circle, when \( \chi_1, \ldots, \chi_m \) run through arbitrary sets of nontrivial multiplicative characters of \( F_q^\times \) with two of the sets being sufficiently large. The case \( m = 2 \) answers a question of Shparlinski.

1 Introduction

Let \( F_q \) be a finite field of characteristic \( p \) with \( q \) elements, and let \( \mathbf{C} \) be the field of complex numbers. We let \( \Psi \) denote the set of nontrivial additive characters \( F_q \to \mathbf{C}^\times \). We let \( \mathcal{X} \) (resp. \( \mathcal{X}^\times \)) denote the set of multiplicative characters (resp. nontrivial multiplicative characters) \( F_q^\times \to \mathbf{C}^\times \). For \( \psi \in \Psi \) and \( \chi \in \mathcal{X} \), we consider the Gauss sum

\[
G(\psi, \chi) = \sum_{a \in F_q^\times} \psi(a)\chi(a).
\]

For \( m \geq 2 \), \( \chi_1, \ldots, \chi_m \in \mathcal{X} \), we consider the Jacobi sum

\[
J(\chi_1, \ldots, \chi_m) = \sum_{a_1, \ldots, a_m \in F_q^\times \atop a_1 + \cdots + a_m = 1} \chi_1(a_1) \cdots \chi_m(a_m).
\]

∗School of Mathematical Sciences, University of Chinese Academy of Sciences, Beijing 100049, China; Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing 100190, China; email: qlu@ucas.ac.cn. Partially supported by National Natural Science Foundation of China Grant 11371043.
†Morningside Center of Mathematics, Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing 100190, China; email: wzheng@math.ac.cn. Partially supported by China’s Recruitment Program of Global Experts; National Natural Science Foundation of China Grant 11321101; Hua Loo-Keng Key Laboratory of Mathematics and National Center for Mathematics and Interdisciplinary Sciences, Chinese Academy of Sciences.
‡School of Mathematics and Systems Science, Beihang University, Beijing 100191, China; email: zhengzhiyong@buaa.edu.cn. Partially supported by Program 863 Grant 2013AA013702; Program 973 Grant 2013CB834205.
§Mathematics Subject Classification 2010: 11T24 (Primary); 11K38, 14G15, 20G05 (Secondary).
It is known that for \( \chi_1, \chi_2, \ldots, \chi_m \in \mathcal{X} \), \( \chi_1 \cdots \chi_m \neq 1 \), where 1 denotes the trivial multiplicative character,

\[
|G(\psi, \chi)| = q^{1/2}, \quad |J(\chi_1, \ldots, \chi_m)| = q^{(m-1)/2}.
\]

Nicholas Katz and Zhiyong Zheng showed in [6] Theorem 1] that the normalized Gauss sums

\[
\{q^{-1/2}G(\psi, \chi)\}_{\psi \in \Psi, \chi \in \mathcal{X}}
\]

and, for \( m = 2 \), the normalized Jacobi sums

\[
\{q^{-1/2}J(\chi_1, \chi_2)\}_{\chi_1, \chi_2 \in \mathcal{X}, \chi_1 \chi_2 \neq 1}
\]

are asymptotically equidistributed in the unit circle as \( q \to \infty \). Shparlinski showed in [11] that the normalized Gauss sums

\[
\{q^{-1/2}G(\psi, \chi)\}_{\psi \in \Psi, \chi \in \mathcal{A}}
\]

where \( \psi \) and \( \chi \) run through arbitrary subsets \( \Phi \subseteq \Psi \) and \( \mathcal{A} \subseteq \mathcal{X} \) satisfying \( \#\Phi \#\mathcal{A} \geq q^{1+\epsilon} \) for a constant \( \epsilon > 0 \), are asymptotically equidistributed in the unit circle as \( q \to \infty \), and asked whether a similar property holds for \( q^{-1/2}J(\chi_1, \chi_2) \).

The goal of this paper is to study more generally equidistribution properties of the normalized Jacobi sums

\[
q^{-(m-1)/2}J(\chi_1, \ldots, \chi_m)_{\chi_1 \in \mathcal{A}_1, \ldots, \chi_m \neq 1}
\]

for \( m \geq 2 \), where the \( \chi_i \)'s run through arbitrary nonempty subsets \( \mathcal{A}_i \subseteq \mathcal{X} \), \( i = 1, \ldots, m \). We show that (1.1) is asymptotically equidistributed in the unit circle when two of the subsets are sufficiently large in the sense that \( q \ln^2 q / \max_{i \neq j} \#\mathcal{A}_i \#\mathcal{A}_j \to 0 \). The case \( m = 2 \) gives an affirmative answer to Shparlinski’s question. Moreover, we give better equidistribution estimates when some (or all) of the subsets are \( \mathcal{X} \). As in [6] and [11], we do not restrict the way how \( q \) approaches infinity. In particular, we do not fix \( p \).

To formulate our results, we need the following notion.

**Definition 1.1.** The discrepancy of a finite multiset of complex numbers \( \{z_1, \ldots, z_N\} \) on the unit circle is defined to be

\[
D = \sup_{a \leq b \leq a+1} \left| \frac{T(a, b)}{N} - (b - a) \right|,
\]

where \( T(a, b) \) is the number of \( 1 \leq i \leq N \) such that there exists \( c \in [a, b] \) satisfying \( z_i = e^{2\pi ic} \). For \( N = 0 \) we put \( D = 1 \). We say that a sequence or net of such multisets \( \{(z_{a,1}, \ldots, z_{a,N_a})\}_{a \in I} \) is asymptotically equidistributed if \( D = o(1) \).

For \( N \geq 1 \) we have \( \frac{1}{N} \leq D \leq 1 \). We let \( D(\mathcal{A}_1, \ldots, \mathcal{A}_m) \) denote the discrepancy of the multiset [11].

**Theorem 1.2.** Let \( m \geq 2 \) and let \( \mathcal{A}_1, \ldots, \mathcal{A}_m \) be nonempty subsets of \( \mathcal{X} \). Let \( A_1 = \#\mathcal{A}_1, A_2 = \#\mathcal{A}_2 \). Then

\[
D(\mathcal{A}_1, \ldots, \mathcal{A}_m) \leq 3A_1^{-1/3}q^{1/6} + \frac{1}{4}(A_1A_2)^{-1/2}q^{1/2}(6 + \ln q),
\]

(1.2)

\[
D(\mathcal{A}_1, \ldots, \mathcal{A}_m) \leq 2A_1^{-2/7}A_2^{-1/7}q^{3/14} + \frac{1}{3}A_1^{-1/2}A_2^{-1/4}q^{-1/2}(4 + \ln q).
\]

(1.3)
Since $D(A_1, \ldots, A_m)$ is symmetric in the $A_i$'s, (1.2) is equivalent to

$$D(A_1, \ldots, A_m) \leq 3(\max_i \#A_i)^{-1/3} q^{1/6} + \frac{1}{q}(\max_i \#A_i \#A_j)^{-1/2} q^{1/2} (6 + \ln q).$$

Therefore, (1.1) is asymptotically equidistributed when $q \ln^2 q/\max_{i\neq j} \#A_i \#A_j \to 0$. We note that this condition cannot be substantially improved. In fact, for $A_2, \ldots, A_m$ satisfying $\#A_2 = \cdots = \#A_m = 1$, there exists $A_1$ satisfying $\#A_1 \geq (q-3)/2$ such that (1.1) is contained in a semicircle, so that $D(A_1, \ldots, A_m) \geq \frac{1}{2}$.

**Corollary 1.3.** There exists a constant $C$ such that for all $m \geq 2$ and for nonempty subsets $A_1, \ldots, A_m$ of $X$, we have

$$D(A_1, \ldots, A_m) \leq C q^{-f(\log_q \#A_1, \log_q \#A_2)} \ln q,$$

where $f: [0,1] \times [0,1] \to [0, \frac{3}{14}]$ is the function satisfying $f(x,y) = f(y,x)$ and such that for $x \geq y$,

$$f(x,y) = \begin{cases} 
0 & x + y \leq 1, \\
\frac{1}{3}x + \frac{1}{3}y - \frac{1}{2} & x + y \geq 1 \text{ and } x + 3y \leq 2, \\
\frac{1}{3}x - \frac{1}{6} & x + 3y \geq 2 \text{ and } 2x + 3y \leq 4, \\
\frac{1}{3}x + \frac{1}{3}y - \frac{1}{2} & 2x + 3y \geq 4 \text{ and } 2x + y \leq \frac{8}{3}, \\
\frac{1}{3}y - \frac{1}{11} & 2x + y \geq \frac{8}{3}.
\end{cases}$$

Note that the function $f(x,y)$ is nondecreasing with respect to both $x$ and $y$, continuous, and is linear on each piece of the following partition of $[0,1] \times [0,1]$

with $f(0,0) = f(1,0) = f(\frac{1}{3}, \frac{1}{3}) = 0$, $f(\frac{1}{3}, \frac{1}{3}) = \frac{1}{10}$, $f(1, \frac{1}{3}) = f(1, \frac{2}{3}) = f(\frac{1}{2}, \frac{1}{3}) = f(\frac{1}{2}, \frac{1}{2}) = \frac{1}{5}$, $f(1,1) = \frac{2}{14}$. The pieces marked with I, II, III, IV, V correspond to the five cases of (1.4).

Next we give better upper bounds for the discrepancy when some of the subsets are actually $X$. We put $D_k(A_1, \ldots, A_m) = D(A_1, \ldots, A_m, X', \ldots, X')$ for $m, k \geq 1$ and $D_k = D(X, \ldots, X)$ for $k \geq 2$, where $X'$ is repeated $k$ times.

**Theorem 1.4.** Let $m \geq 1$ and let $A_1, \ldots, A_m$ be nonempty subsets of $X$. Let $A_1 = \#A_1$. Then, for $k \geq 2$,

$$\begin{align*}
D_k(A_1, \ldots, A_m) &\leq 2q^{-\frac{k}{2k+1}} (1 + k!q^{-1/6} \ln q), \\
D_k(A_1, \ldots, A_m) &\leq 2A_1 \frac{(2k+1)!}{k!} \ln q \{ 1 + q^{-2/7} [r^{k-1} + (2k + 1)!!/2 \ln q] \}.
\end{align*}$$
For $k = 1$, we have
\begin{equation}
(1.7) \quad D_1(\mathcal{A}_1, \ldots, \mathcal{A}_m) \leq 2q^{-1/4} + \frac{k}{6}A_1^{-1}(5 + \ln q)(1 + 2q^{-1/2}),
\end{equation}
where $\delta = 0$ if $m = 1$ and $\delta = 1$ if $m > 1$. Moreover, for $A_1 \geq q^{3/4}$, we have
\begin{equation}
(1.8) \quad D_1(\mathcal{A}_1, \ldots, \mathcal{A}_m) \leq 2A_1^{-1/5}q^{-1/10}(1 + q^{-1/8} \ln q).
\end{equation}

**Corollary 1.5.** Let $k \geq 1$. There exists a constant $C_k$ such that for all $m \geq 1$ (assuming $m = 1$ if $k = 1$) and for nonempty subsets $\mathcal{A}_1, \ldots, \mathcal{A}_m$ of $\mathcal{X}$, we have
\[ D_k(\mathcal{A}_1, \ldots, \mathcal{A}_m) \leq C_kq^{-g_k(\log_q \# \mathcal{A}_1)}, \]
where $g_k : [0, 1] \to \left[\frac{k}{2(k+1)}, \frac{2k+1}{2(2k+3)}\right]$ is the function
\[ g_k(x) = \begin{cases} 
\frac{k}{2(k+1)} & x \leq \frac{2k+1}{2k+2}, \\
\frac{1}{2k+3}x + \frac{2k-1}{2(2k+3)} & x \geq \frac{2k+1}{2k+2}.
\end{cases} \]

For $k = 1$, there exists a constant $C'$ such that for all $m \geq 1$, we have
\[ D_1(\mathcal{A}_1, \ldots, \mathcal{A}_m) \leq C'q^{-h(\log_q \# \mathcal{A}_1)} \ln q, \]
where $h : [0, 1] \to [0, \frac{3}{10}]$ is the function
\[ h(x) = \begin{cases} 
x & 0 \leq x \leq \frac{1}{5}, \\
\frac{1}{4}x + \frac{1}{10} & \frac{1}{5} \leq x \leq \frac{3}{10}, \\
\frac{3}{10} & \frac{3}{10} \leq x \leq 1.
\end{cases} \]

Note that the functions $g_k(x)$ and $h(x)$ are nondecreasing, continuous and piecewise-linear. Corollary 1.5 for $k = 1$ improves the case $\mathcal{A}_1 = \mathcal{X}$ of Corollary 1.3, since $f(1, x) \leq h(x) \leq g_1(x)$. Moreover, Corollary 1.5 for $k \geq 2$ improves the case $\mathcal{A}_1 = \mathcal{X}$ of Corollary 1.5 for $k - 1$, since $g_{k-1}(1) = \frac{2k-1}{2k+1} < \frac{2k}{2(k+1)} = g_k(0) \leq g_k(x)$.

When all of the subsets are $\mathcal{X}$, we have the following extension of (1.5).

**Theorem 1.6.** For $k \geq 2$, $q \geq 3$, we have
\begin{equation}
(1.9) \quad D_k \leq 2q^{-\frac{k}{k+1}}(1 + k!q^{-1/6} \ln q).
\end{equation}

This improves the case $m = 1$, $\mathcal{A}_1 = \mathcal{X}$ of Corollary 1.5 for $k - 1$. For $k = 2$, we recover the result $D_2 = O(q^{-1/3})$ of Katz and Zhongyang Zheng [6, Theorem 1].

To prove the above theorems, we use the Erdős-Turán inequality together with estimates of moments of Jacobi sums. Our method of estimating moments of Jacobi sums is based on the theory of Kloosterman sheaves as in [6], but we need estimates for higher tensor powers of Kloosterman sheaves, which we give in Section 2. We give estimates for moments of Jacobi sums in Section 3. In Section 4, we prove the upper bounds for the discrepancy and give a lower bound for $D_k$, $k \geq 3$. 

4
2 A key lemma

In the rest of this paper, we fix a nontrivial additive character \( \psi \) on \( \mathbf{F}_q \) and omit it from the notation. For \( n \geq 1 \) and \( a \in \mathbf{F}_q^\times \), we consider the Kloosterman sum

\[
K_{l,n}(a) = \sum_{a_1, \ldots, a_n \in \mathbf{F}_q^\times, a_1 \cdots a_n = a} \psi(a_1 + \cdots + a_n).
\]

We have \( K_{1,n}(a) = \psi(a) \). The Fourier transform of \( K_{l,n}(a) \) is the \( n \)-th power of the Gauss sum \( G(\chi) \):

\[
G(\chi)^n = \sum_{a \in \mathbf{F}_q^\times} K_{l,n}(a) \chi(a)
\]

for all \( \chi \in \widehat{\mathbf{F}_q^\times} \) \([5] 4.0, page 47\).

**Lemma 2.1.** Let \( n \geq 1 \), \( k,l \geq 0 \). Let \( \chi \) be a nontrivial multiplicative character of \( \mathbf{F}_q^\times \). Then

\[
\left| \sum_{a \in \mathbf{F}_q^\times} K_{l,n}(a)^k \mathbf{R}_{l,n}(a)^l - R q^{(n-1)(k+l)+1} \right| \leq \left( \left| n^{k+l-1} - \frac{R}{n} \right| + R \right) q^{(n-1)(k+l)+1},
\]

\[
\left| \sum_{a \in \mathbf{F}_q^\times} \chi(a) K_{l,n}(a)^k \mathbf{R}_{l,n}(a)^l \right| \leq \left| n^{k+l-1} - \frac{R}{n} \right| q^{(n-1)(k+l)+1}.
\]

Here \( R = R_{p,n}^{k,l} \) is the dimension of \( (V^\otimes l) \otimes (V^* \otimes k)^G \), where \( V \) is the standard complex representation of \( G \) of dimension \( n \),

\[
G = \begin{cases}
\mu_p & n = 1, \\
\text{Sp}_n & n \text{ even}, \\
\text{SL}_n & p, n \geq 3 \text{ odd}, \\
\text{SO}_n & p = 2, \ n \neq 1, 7 \text{ odd}, \\
G_2 & p = 2, \ n = 7,
\end{cases}
\]

and \( \mu_p \) is the group of \( p \)-th roots of unity in \( \mathbb{C} \).

Let \( E \subset \mathbb{C} \) be a number field containing the \( p \)-th roots of unity and let \( \lambda \) be a finite place of \( E \) not dividing \( p \). Recall from Deligne \([11] \) Théorème 7.8 that the Kloosterman sheaf \( \mathcal{K}_n \) is a lisse \( E_\lambda \)-sheaf on \( \mathbf{G}_{m,F_q} \) of rank \( n \) and weight \( n - 1 \) satisfying

\[
\text{tr}(\text{Fr}_a, (\mathcal{K}_n)_a) = (-1)^{n-1} K_{l,n}(a),
\]

where \( \text{Fr}_a \) is the geometric Frobenius at \( a \in \mathbf{G}_{m}(\mathbf{F}_q) = \mathbf{F}_q^\times \) and \( \breve{a} \) is a geometric point above \( a \). Moreover,

\[
\text{tr}(\text{Fr}_a, (\mathcal{K}_n^\vee)_a) = (-1)^{n-1} q^{-(n-1)} \mathbf{R}_{l,n}(a).
\]

The group \( G \) in the lemma is the Zariski closure of the geometric monodromy group of \( \mathcal{K}_n \) as computed by Katz \([5] \) Theorem 11.1].

Deligne’s bound \( |K_{l,n}(a)| \leq n q^{\frac{n-1}{2}} \) implies that the left hand side of (2.3) is bounded by \( n^{k+l}(q - 1)q^{\frac{(n-1)(k+l)}{2}} \). Thus (2.3) is nontrivial. We will see in Remark 2.3 that \( R \leq \)
Recall [1, Théorème 7.8] that the local monodromy of the above lemma. We have $\mathbb{R}$ We gather some formulas and bounds for the constant $(n K_{\text{swan}})$ unipotent and tame. The local monodromy at $\infty$ of this sheaf are at most 1. By the Grothendieck trace formula, the inequality (2.2) then follows from the Grothendieck-Ogg-Shafarevich formula [4, Corollary 11.3], the arithmetic fundamental group of $\mathcal{K}_n(\frac{n-1}{2})$ (well-defined up to adjoining $q^{\frac{n-1}{2}}$ to $E$) coincides with $G$. Thus $$\text{tr}(\text{Fr}_q, H^2_c) = Rq^{\frac{(n-1)(k-l)-1}{2}}.$$ Moreover, $(n-1)(k+l)$ is even whenever $R > 0$. By Deligne’s Weil II [2, Théorème 3.3.1], $$\left|\text{tr}(\text{Fr}_q, H^1_c)\right| \leq h^1_c q^{\frac{(n-1)(k-l)+1}{2}},$$ where $h^1_c = \dim H^1_c$. The sheaf $\mathcal{K}_n^\otimes k \otimes (\mathcal{K}_n^\vee)^\otimes l$ has rank $n^{k+l}$ and is tame at 0. All breaks at $\infty$ of this sheaf are at most 1/n by [5, Lemma 1.3] and at least $R$ breaks are 0. It follows that the Swan conductor $$\text{swan}_{\infty}(\mathcal{K}_n^\otimes k \otimes (\mathcal{K}_n^\vee)^\otimes l) \leq \left\lfloor \frac{(n^{k+l} - R)}{n} \right\rfloor.$$ The inequality (2.2) then follows from the Grothendieck-Ogg-Shafarevich formula [4, Théorème 7.1] $$h^1_c = h^2_c + \text{swan}_{\infty}(\mathcal{K}_n^\otimes k \otimes (\mathcal{K}_n^\vee)^\otimes l).$$ For (2.3), we may assume that $E$ contains the image of $\chi$. Let $\mathcal{L}_\chi$ be the lisse $E_\chi$-sheaf of rank 1 on $\mathbb{G}_{m,F_q}$ corresponding to $\chi$. As the local monodromy at 0 of $\mathcal{K}_n^\otimes k \otimes (\mathcal{K}_n^\vee)^\otimes l \otimes \mathcal{L}_\chi$ is given by a successive extension of $\bar{\chi}$, we have $$H^2_c(\mathbb{G}_{m,F_q}, \mathcal{L}_\chi \otimes \mathcal{K}_n^\otimes k \otimes (\mathcal{K}_n^\vee)^\otimes l) \simeq H^0(\mathbb{G}_{m,F_q}, \mathcal{L}_\chi \otimes \mathcal{K}_n^\otimes k \otimes (\mathcal{K}_n^\vee)^\otimes l \otimes \mathcal{L}_\chi^\vee)^\otimes (-1) = 0.$$ The rest of the proof is completely similar to the proof of the first assertion. \hfill \Box

**Remark 2.2.** We gather some formulas and bounds for the constant $R = R^{k,l} = R_{G}^{k,l}$ in the above lemma. We have $R^{k,l} = R^{l,k}$. For $G = \text{Sp}_n$, $\text{SO}_n$, or $G_2$, $V^* \simeq V$ so that $R^{k,l}$ depends only on $k+l$ (and $G$). In this case, we put $R^{k+l} = R^{k,l}$.

For $G = \mu_p$, $R^{k,l} = 1$ if $k \equiv l \pmod{p}$ and $R^{k,l} = 0$ otherwise.
For $G = \text{Sp}_n$ ($n$ even), we let $V_\lambda$ denote the irreducible representation corresponding to a partition $\lambda = (\lambda_1 \geq \cdots \geq \lambda_n) \geq 0$ (where the $\lambda_j$’s are integers). We have $V \simeq V_\sigma$, where $\sigma = (1, 0, \ldots, 0)$. By King’s formula \[ (4.14), (4.15), (4.31) \], we have
\[
V_\lambda \otimes V_\sigma \simeq \bigoplus_{\lambda'} V_{\lambda'},
\]
where $\lambda'$ runs through $\sigma$-expansions and $\sigma$-contractions of $\lambda$. Here we say that $\lambda'$ is a $\sigma$-expansion of $\lambda$, or equivalently $\lambda$ is a $\sigma$-contraction of $\lambda'$, if there exists $j$ satisfying $\lambda'_j = \lambda_j + 1$ and $\lambda'_j = \lambda_j$ for all $j' \neq j$. Thus $R^k$ is the number of sequences of partitions $\lambda^{(0)}, \ldots, \lambda^{(k)}$ with $\lambda^{(0)} = \lambda^{(k)} = (0, \ldots, 0)$, such that for each $0 \leq i < k$, $\lambda^{(i+1)}$ is a $\sigma$-expansion or a $\sigma$-contraction of $\lambda^{(i)}$. Moreover, by classical invariant theory \[13\] Section VI.7], $(\bigotimes V)^G$ is spanned by the invariants given by partitions of $\{1, \ldots, k\}$ into pairs, so that $R^k \leq (k - 1)!!$, and equality holds if and only if $k \leq n$ and $k$ even. Here we adopt the convention that $(-1)!! = 1$. For $k$ odd, $R^k = 0$.

For $G = \text{SO}_n$ ($n$ odd), we let $V_\lambda'$ denote the irreducible representation of $O_n = \text{SO}_n \times \{\pm 1\}$ corresponding to a partition $\lambda = (\lambda_1 \geq \cdots \geq \lambda_n \geq 0)$ satisfying $\lambda_1 + \lambda_2 \leq n$, where $\lambda^T$ denotes the conjugate of $\lambda$. We have $V \simeq \text{Res}^0_{\text{SO}_n} V_\sigma$ and, for $\lambda \neq \lambda'$, $\text{Res}^0_{\text{SO}_n} V_\lambda \simeq \text{Res}^0_{\text{SO}_n} V_{\lambda'}$ if and only if $\lambda_1 + \lambda_2 = n$ and $\lambda_1 + \lambda_2 = \lambda'_1 + \lambda'_2$ for all $j > 1$. By King’s formula for $O_n$ \[4\] (4.14), (4.15)], we have $V_\lambda \otimes V_\sigma \simeq \bigoplus_{\lambda'} V_{\lambda'}$, where $\lambda'$ runs through $\sigma$-expansions and $\sigma$-contractions of $\lambda$. Thus, for $k$ odd (resp. even), $R^k$ is the number of sequences of partitions $\lambda^{(0)}, \ldots, \lambda^{(k)}$, where $\lambda^{(i)} = (\lambda_1^{(i)} \geq \cdots \geq \lambda_n^{(i)} \geq 0)$, $\lambda^{(0)} = (0, \ldots, 0)$, $\lambda^{(k)} = (1, \ldots, 1)$ (resp. $\lambda^{(k)} = (0, \ldots, 0)$), such that for each $i$, $\lambda^{(i+1)}$ is a $\sigma$-expansion or a $\sigma$-contraction of $\lambda^{(i)}$.

Moreover, by classical invariant theory \[13\] Sections II.9, II.17], for $k$ odd, $(\bigotimes V)^G$ is spanned by the images of $C \simeq \bigwedge^n V \subset V^\otimes n$ under the expansion operators $V^\otimes n \to V^\otimes k$ given by an injection $\{1, \ldots, n\} \hookrightarrow \{1, \ldots, k\}$ and a partition of the complement into pairs, so that $R^k = 0$ for $k \leq n$ and $R^k \leq (k - 1)!! \leq (k - 1)!$ for $k > n$ (assuming $n \geq 3$). For $k$ even, $(\bigotimes V)^G$ is spanned by the invariants given by partitions of $\{1, \ldots, k\}$ into pairs, so that $R^k \leq (k - 1)!!$, and equality holds if and only if $k \leq 2n$.

For $G = G_2$, we let $V_\lambda$ denote the irreducible representation corresponding to a partition $\lambda = (\lambda_1 \geq \lambda_2 \geq 0)$, so that $V_{0,0} = C$, $V_{1,0} = V$. By Littlewood-Richardson’s generalized Littlewood-Richardson rule \[8\] 3.8], we have $V_\lambda \otimes V^\otimes k \simeq \bigoplus_{\lambda'} V_{\lambda'}$, where $\lambda'$ satisfies one of the following

$\bullet$ $\lambda'$ is a $\sigma$-expansion or a $\sigma$-contraction of $\lambda$;

$\bullet$ $\lambda'_1 = \lambda_1 \pm 1$ and $\lambda_2' = \lambda_2 \mp 1$; or

$\bullet$ $\lambda' = \lambda$ and $\lambda_1 > \lambda_2$.

Note that, for each $\lambda$, there are at most 7 possibilities for $\lambda'$. We have
\[
V^\otimes 2 \simeq V_{0,0} \oplus V_{1,0} \oplus V_{2,0} \oplus V_{1,1}, \quad V^\otimes 3 \simeq V_{0,0} \oplus V_{1,0} \oplus V_{2,0} \oplus V_{3,0} \oplus V_{1,1} \oplus V_{2,1},
\]
\[
V^\otimes 4 \simeq V_{0,0} \oplus V_{1,0} \oplus V_{2,0} \oplus V_{3,0} \oplus V_{4,0} \oplus V_{2,1} \oplus V_{3,1} \oplus V_{2,2},
\]
and, for $k \geq 4$, the multiplicities appearing in the decomposition of $V^\otimes k$ are at most $12 \cdot 7^{k−4}$. Since $R^k_{G_2}$ is the multiplicity of $V_{1,0}$ in $V^\otimes (k−1)$, we have

\[ (2.4) \]
\[ R^k_{G_2} \leq 12 \cdot 7^{k−5} \]
for \( k \geq 5 \). Moreover, \((V^\otimes k)^G\) is spanned by invariants given by partitions of \( \{1, \ldots, k\} \) into subsets of cardinality 2, 3, or 4 by \cite[Theorem 3.23]{11}. It follows from this or \cite[(2.4)]{22} that \( R^k \leq (k - 1)! \).

For \( G = \text{SL}_n \), we let \( V_\lambda \) denote the representation of \( \text{GL}_n \) corresponding to a sequence \((\lambda_1 \geq \cdots \geq \lambda_n)\) (where the \( \lambda_j \)'s are integers, possibly negative), so that \( V \simeq \text{Res}_{\text{SL}_n}^{\text{GL}_n} V_\sigma \) and \( \text{Res}_{\text{SL}_n}^{\text{GL}_n} V_\lambda \simeq \text{Res}_{\text{SL}_n}^{\text{GL}_n} V_\lambda \) if and only if \( \lambda \) and \( \lambda' \) are congruent modulo \((1, \ldots, 1)\). By the Littlewood-Richardson rule (or Petri’s formula), \( V_\lambda \otimes V_\sigma \simeq \bigoplus V_\lambda' \) where \( \lambda' \) runs through \( \sigma \)-expansions of \( \lambda \) and \( V_\lambda \otimes V_\sigma' \simeq \bigoplus V_\lambda' \) where \( \lambda' \) runs through \( \sigma \)-contractions of \( \lambda \). Thus \( R^k \neq 0 \) if and only if \( k \equiv l \pmod{n} \). In this case, \( R^k \) is the number of sequences of partitions \( \lambda^{(0)}, \ldots, \lambda^{(k+1)} \), where \( \lambda^{(0)} = (0, \ldots, 0) \), \( \lambda^{(k+1)} = (\frac{\lambda - k}{n}, \ldots, \frac{\lambda - k}{n}) \), such that for each \( 0 \leq i < l \), \( \lambda^{(i)} \) is a \( \sigma \)-expansion of \( \lambda^{(i+1)} \), and for each \( l \leq i < k + l \), \( \lambda^{(i+1)} \) is a \( \sigma \)-contraction of \( \lambda^{(i)} \). We let \( \delta(\lambda) \) denote the number of \( 1 \leq j < n \) such that \( \lambda_j + 1 \neq \lambda_j \). We have \( 0 \leq \delta(\lambda) \leq n - 1 \). The number of \( \sigma \)-expansions and the number of \( \sigma \)-contractions of \( \lambda \) are both equal to \( \delta(\lambda) + 1 \). Moreover, for any \( \sigma \)-expansion or \( \sigma \)-contraction \( \lambda' \) of \( \lambda \), \( |\delta(\lambda') - \delta(\lambda)| \leq 1 \). Thus \( R^k \leq \binom{n}{\frac{k+1}{2}}! \binom{k+1}{l}! \). We will be particularly interested in \( R^k_1 \) and \( R^k_2 \). For \( k \equiv 1 \pmod{n} \), \( R^k_2 = R^k_1 \) is the number of standard Young tableaux on the Young diagram corresponding to \((\frac{k-1}{n} + 1, \frac{k-1}{n}, \ldots, \frac{k-1}{n})\), so

\[
R^k_{1, \text{SL}_n} = k! \frac{(n + \frac{k-1}{n})!}{n!} \prod_{i=0}^{n-2} \frac{(i + \frac{k-1}{n})!}{i!}
\]

by the hook length formula. For any \( k \), \( R^k_2 \) is the dimension of \( \text{End}(V^\otimes k)^G \) and we have

\[
R^k_{1, \text{SL}_n} = \sum_\lambda m^2_\lambda \leq k!,
\]

where equality holds if and only if \( k \leq n \). Here \( \lambda \) runs over partitions \( \lambda = (\lambda_1 \geq \cdots \geq \lambda_n \geq 0) \) satisfying \( \sum \lambda_i = k \), and \( m_\lambda \) is the multiplicity of \( V_\lambda \) in \( V^\otimes k \), namely the number of standard Young tableaux on the Young diagram corresponding to \( \lambda \).

**Remark 2.3.** By the preceding remark, we have \( R^k_2 \leq (k + l - 1)! \) in all cases. Moreover, for \( G \neq G_2 \), \( R^k_2 \leq (2k - 1)!! \).

**Remark 2.4.** Let us list the values of \( R^k_1 \) and \( R^k_2 \) for \( 1 \leq k \leq 3 \).

- \( R^1_1 = 1 \) in all cases.
- \( R^2_1 = 1 \) for \( G = \text{SO}_3 \) or \( G_2 \) and \( R^2_2 = 0 \) otherwise.
- \( R^3_1 = 0 \) for \( G = \mu_p \) (\( p \) odd) or \( \text{SL}_n \), \( R^3_2 = 1 \), \( R^3_3 = 1 \), \( R^3_4 = 2 \), \( R^3_5 = 3 \) for \( G = \text{Sp}_n \) (\( n \geq 4 \)) or \( \text{SO}_n \), and \( R^3_6 = 4 \).
- \( R^2_1 = 1 \), \( R^2_2 = 2 \) for \( G = \text{Sp}_2 \) or \( \text{SL}_n \), \( R^2_3 = 3 \) for \( G = \text{Sp}_n \) (\( n \geq 4 \)) or \( \text{SO}_n \), and \( R^2_4 = 4 \).
- \( R^3_1 = 1 \), \( R^3_2 = 5 \), \( R^3_3 = 6 \), \( R^3_4 = 14 \), \( R^3_5 = 15 \) for \( G = \text{Sp}_n \) (\( n \geq 6 \)) or \( \text{SO}_n \), and \( R^3_6 = 35 \).

\footnote{The sequence \( R^k_2 \) (\( k \geq 0 \)) is sequence A059710 in the On-Line Encyclopedia of Integer Sequences. The first terms are 1, 0, 1, 1, 4, 10, 35, 120, 455.}
3 Moments of Jacobi sums

For subsets $\mathcal{A}_1, \ldots, \mathcal{A}_m$ of $\mathcal{X}$, $m \geq 2$ and $n \geq 1$, we consider the incomplete $n$-th moment of the normalized Jacobi sums (\ref{eq:moment}):

$$M^{(n)}(\mathcal{A}_1, \ldots, \mathcal{A}_m) = \sum_{\chi \in \mathcal{A}_1} q^{-n(n-1)/2} J(\chi_1, \ldots, \chi_m)^n.$$  

When some of the subsets are empty, we adopt the following shorthand, similar to the notation on discrepancy. We put $M^{(n)}_l(\mathcal{A}_1, \ldots, \mathcal{A}_m) = M^{(n)}(\mathcal{A}_1, \ldots, \mathcal{A}_m, \mathcal{X}, \ldots, \mathcal{X})$ for $m, k \geq 1$ and $M^{(n)}_k = M^{(n)}(\mathcal{X}, \ldots, \mathcal{X})$ for $k \geq 2$, where $\mathcal{X}$ is repeated $k$ times. The statements of the following theorems make use of the notation $R^{(n)}_{p,n}$ introduced in Lemma \ref{lem:ramanujan}.

Theorem 3.1. Let $m \geq 2$ and let $\mathcal{A}_1, \ldots, \mathcal{A}_m$ be subsets of $\mathcal{X}$. Let $A_i = \#\mathcal{A}_i$, $i = 1, \ldots, m$. Then, for $n \geq 1$,

\begin{align}
|M^{(n)}(\mathcal{A}_1, \ldots, \mathcal{A}_m)| &\leq (A_1 A_2 A_3 \cdots A_m [q + (n-1) A_2 q^{1/2}])^{1/2}, \\
|M^{(n)}_l(\mathcal{A}_1, \ldots, \mathcal{A}_m)| &\leq A_1^{1/2} A_2^{3/4} A_3 \cdots A_m [R^{(n)}_{p,n} q^{2} + n^3 + R^{(n)}_{p,n} - 1] q^{3/2} \\
|M^{(n)}_k| &\leq A_2 \cdots A_m A_1^{1/2} (q-1)^{2k+1} q^{-2k+1} \left[n^{2k+1} - 1 + R^{k+1}_{p,n} (q^{1/2} + 1)\right]^{1/2} + T,
\end{align}

where $\delta = 0$ for $m = 1$ and $\delta = 1$ for $m \neq 1$, and

$$T = (k+1) A_1 \cdots A_m (q-1)^{k-1} q^{-n/2}.$$  

Theorem 3.2. Let $k, m \geq 1$ and let $\mathcal{A}_1, \ldots, \mathcal{A}_m$ be nonempty subsets of $\mathcal{X}$. Let $A_i = \#\mathcal{A}_i$, $i = 1, \ldots, m$. Then, for $n \geq 1$,

\begin{align}
|M^{(n)}_k| &\leq A_2 \cdots A_m A_1^{1/2} (q-1)^{2k+1} q^{-2k+1} \left[n^{2k+1} - 1 + R^{k+1}_{p,n} (q^{1/2} + 1)\right]^{1/2} + T,
\end{align}

where $\delta = 0$ for $m = 1$ and $\delta = 1$ for $m \neq 1$, and

$$T = (k+1) A_1 \cdots A_m (q-1)^{k-1} q^{-n/2}.$$  

Theorem 3.3. Let $k \geq 2$. Then, for $n \geq 1$,

\begin{align}
|M^{(n)}_k| &\leq (q-1)^{k-1} q^{k-2} R^{k,1}_{p,n} \left[\left(n^{k} - \frac{R^{k,1}_{p,n}}{n}\right) + R^{k,1}_{p,n}\right] + [(q-1)^k - N] q^{-n/2},
\end{align}

where $N \geq (q-2)^{k-1} (q-1) - k$ is the number of $k$-tuples $(\rho_1, \ldots, \rho_k)$, $\rho_i \in \mathcal{X}$ such that $\rho_1 \cdots \rho_k \neq 1$.

For $k = 2$ and $n \geq 2$, we have $(q-1)^2 q^{-1} n^2 + (3q-5) q^{-n/2} \leq n^2 q$, hence Theorem 3.3 implies the bound $|M^{(n)}_2| \leq n^2 q + R^{2,1}_{p,n} q^{3/2}$ of Katz and Zhiyong Zheng [6, Theorem 3].

As in Shparlinski [11], one strategy followed in the proofs consists of applying the Cauchy-Schwarz inequality and extending the sum over $\mathcal{X}$. We estimate the complete sum using Lemma \ref{lem:ramanujan}.

Let us recall two simple facts that will be used in the proofs. The Jacobi sums and Gauss sums are related by the formula

$$J(\chi_1, \ldots, \chi_m) = G(\chi_1) \cdots G(\chi_m) G(\chi_1 \cdots \chi_m)^{-1} = q^{-1} G(\chi_1) \cdots G(\chi_m) G(\chi_1 \cdots \chi_m),$$

for $\chi_1, \ldots, \chi_m \in \mathcal{X}$ satisfying $\chi_1 \cdots \chi_m \neq 1$. Moreover, $G(1) = -1$.  


Proof of Theorem 3.1. We may assume $A_1 \geq A_2$. Let $M^{(n)} = M^{(n)}(A_1, \ldots, A_m)$. By the facts recalled above,

$$|M^{(n)}| \leq \sum_{\chi_1 \in A_1} \left| q^{-\frac{n+1}{2}} G(\chi_1) \cdots G(\chi_m) \overline{G(\chi_1 \cdots \chi_m)} \right|^n \leq \sum_{\chi_i \in A_i} \left| G(\chi_1) \cdots G(\chi_m) \overline{G(\chi_1 \cdots \chi_m)} \right|^n$$

$$\leq A_2 \cdots A_m q^{-n/2} + W \leq (A_1 A_2)^{1/2} A_3 \cdots A_m q^{-n/2} + W,$$

where

$$W = \sum_{\chi_1 \in A_1} \sum_{\chi_i \in A_i, i=2,\ldots,m} \left| q^{-m/2} G(\chi_2) \cdots G(\chi_m) \overline{G(\chi_1 \cdots \chi_m)} \right|^n.$$

By the Cauchy-Schwarz inequality,

$$W^2 \leq A_1 \sum_{\chi_1 \in A_1} \sum_{\chi_i \in A_i, i=2,\ldots,m} \left| q^{-m/2} G(\chi_2) \cdots G(\chi_m) \overline{G(\chi_1 \cdots \chi_m)} \right|^2$$

$$\leq A_1 \sum_{\chi_1 \in \mathcal{X}} \sum_{\chi_i \in A_i, i=2,\ldots,m} \left| q^{-m/2} G(\chi_2) \cdots G(\chi_m) \overline{G(\chi_1 \chi_2 \cdots \chi_m)} \right|^n$$

$$= A_1 \sum_{\chi_1 \in \mathcal{X}} \sum_{\chi_i \in A_i, i=2,\ldots,m} \left| q^{-m/2} G(\chi_2) \cdots G(\chi_m) \overline{G(\chi_1 \chi_2 \cdots \chi_m)} \right|^n G(\chi_1 \chi_2 \cdots \chi_m)$$

$$\leq A_1 \sum_{\chi_1, \chi_2, \ldots \in A_i, i=2,\ldots,m} q^{-n} \left| \sum_{\chi_1 \in \mathcal{X}} G(\chi_1 \chi_2 \cdots \chi_m) \right|^n \left| G(\chi_1 \chi_2 \cdots \chi_m) \right|^n =: X.$$

By (2.1),

$$\sum_{\chi_1 \in \mathcal{X}} G(\chi_1 \chi_2 \cdots \chi_m) G(\chi_1 \chi_2 \cdots \chi_m) = \sum_{a \in \mathcal{F}_q} \sum_{\chi_1} \text{Kl}_n(a) \overline{\text{Kl}_n(b)} \chi_1 \cdots \chi_m(a) \chi_1 \cdots \chi_m(b)$$

$$= (q-1) \sum_{a \in \mathcal{F}_q} \text{Kl}_n(a) \overline{\text{Kl}_n(a)} \chi_2 \cdots \chi_m \chi_1 \cdots \chi_m(a).$$

For $\chi_2 \cdots \chi_m = \chi'_2 \cdots \chi'_m$, we have

$$\sum_{\chi_1 \in \mathcal{X}} G(\chi_1 \chi_2 \cdots \chi_m) G(\chi_1 \chi'_2 \cdots \chi'_m)^n = (q-2) q^n + 1.$$

Thus, by (2.3) (where $R^{1,1} = 1$), we have

$$X = A_1 \sum_{\chi_1, \chi_2, \ldots \in A_i, i=2,\ldots,m} + A_1 \sum_{\chi_1, \chi_2, \ldots \in A_i, i=2,\ldots,m} \text{Kl}_n(a) \chi_1 \cdots \chi_m(a) \chi_1 \cdots \chi_m(b)$$

$$\leq A_1 A_2 (A_3 \cdots A_m)^2 (q - 2 + q^{-n}) + A_1 (A_2 \cdots A_m)^2 (q - 1)(n - 1) q^{-1/2}$$

$$= A_1 A_2 (A_3 \cdots A_m)^2 [q - 2 + q^{-n} + (n - 1) A_2(q - 1) q^{-1/2}].$$

Thus

$$|M^{(n)}| \leq (A_1 A_2)^{1/2} A_3 \cdots A_m \{q^{-n/2} + [q - 2 + q^{-n} + (n - 1) A_2(q - 1) q^{-1/2}]^{1/2}\}.$$

For (3.1), it suffices to show

$$q - 2 + q^{-n} + (n - 1) A_2(q - 1) q^{-1/2} \leq \left\{ q + (n - 1) A_2 q^{1/2} \right\}^{1/2} - q^{-n/2},$$

10
namely
\[2q^{-n/2}[q + (n - 1)A_2q^{1/2}]^{1/2} \leq (n - 1)A_2q^{-1/2} + 2,\]
which is clear by taking squares.

It remains to show (3.2) for \( n \geq 2 \). We have
\[
X = A_1 \sum \chi_i \chi_i' \in A_i, \ i = 3, \ldots, m
\]
where
\[
Y = \sum_{\chi, \chi' \in A_2} \frac{q - 1}{q^n} \left| \sum_{a \in F_q} K_{\alpha}(a) \overline{K_{\beta}(a)} \chi_2 \cdots \chi_m \chi_2' \cdots \chi_m'(a) \right|.
\]
To obtain (3.2), we apply the Cauchy-Schwarz inequality again:
\[
Y^2 \leq A_2 \left( \frac{q - 1}{q^n} \right)^2 \sum_{\chi' \in A_2} \left( \sum_{a \in F_q} |K_{\alpha}(a)K_{\beta}(b)|^2 \chi_2 \cdots \chi_m \chi_2' \cdots \chi_m'(ab^{-1}) \right)^2
\]
\[
= A_2 \left( \frac{q - 1}{q^n} \right)^2 \sum_{a, b \in F_q} \sum_{\chi' \in A_2} |K_{\alpha}(a)K_{\beta}(b)|^2 \chi_2 \cdots \chi_m \chi_2' \cdots \chi_m'(ab^{-1})
\]
\[
= A_2 \left( \frac{q - 1}{q^n} \right)^2 \sum_{a \in F_q} K_{\alpha}(a)^2 K_{\beta}(a)^2.
\]
Thus, by (2.2), we have
\[
Y^2 \leq A_2(q - 1)^3[R^{2.2}q^{-1} + (n^3 + R^{2.2} - 1)q^{-3/2}] + A_2[R^{2.2}q^2 + (n^3 + R^{2.2} - 1)q^{3/2}](1 - \frac{1}{q})^3,
\]
so that
\[
X \leq A_1 A_2 (A_3 \cdots A_m)^2 A_2^{1/2}[R^{2.2}q^2 + (n^3 + R^{2.2} - 1)q^{3/2}]^{1/2}(1 - \frac{1}{q})^{3/2}.
\]
Therefore,
\[
|M^{(n)}| \leq (A_1 A_2)^{1/2} A_3 \cdots A_m \left\{ q^{-n/2} + (1 - \frac{1}{q})^{3/4} A_2^{1/4}[R^{2.2}q^2 + (n^3 + R^{2.2} - 1)q^{3/2}]^{1/4} \right\}
\]
\[
\leq (A_1 A_2)^{1/2} A_3 \cdots A_m A_2^{1/4}[R^{2.2}q^2 + (n^3 + R^{2.2} - 1)q^{3/2}]^{1/4}.
\]
Here we used the inequality \((1 - \frac{1}{q})^{3/4} \leq 1 - \frac{3}{4q}\).

**Proof of Theorem 3.2**  We have
\[
|M^{(n)}(A_1, \ldots, A_m)|
\]
\[
= \left| \sum_{\chi_i \in A_i, \ \rho_j \in \mathcal{X}} [q^{-(m+k+1)/2}G(\chi_1) \cdots G(\chi_m)G(\rho_1) \cdots G(\rho_k)\overline{G(\chi_1 \cdots \chi_m \rho_1 \cdots \rho_k)}]^n \right|
\]
\[
\leq \left| \sum_{\chi_i \in A_i, \ \rho_j \in \mathcal{X}} [q^{-n/2} + X] \right| + \left| \sum_{\chi_i \in A_i, \ \rho_j \in \mathcal{X}} [q^{-n/2}] \right|
\]
\[
\leq (k + 1)A_1 \cdots A_m (q - 1)^{k-1}q^{-n/2} + X,
\]

\[ \]
where
\[ X = \sum_{\chi_1 \in A_1} q^{-n(k+1)/2} \left| \sum_{\rho_j \in \mathcal{X}} G(\rho_1)^n \cdots G(\rho_k)^n \overline{G(\chi_1 \cdots \chi_m \rho_1 \cdots \rho_k)} \right|. \]

By (2.2),
\[ \sum_{\rho_j \in \mathcal{X}} G(\rho_1)^n \cdots G(\rho_k)^n \overline{G(\chi_1 \cdots \chi_m \rho_1 \cdots \rho_k)} = (q - 1)^k \sum_{\alpha \in F_q} K_l(a)^k \overline{K_l(a)} \chi_1 \cdots \chi_m(a). \]

Thus, by Lemma 2.1, we have
\[
X = \sum_{\chi_1 \in A_1} + \sum_{\chi_1 \cdots \chi_m = 1} \sum_{\chi_1 \cdots \chi_m \neq 1} (q - 1)^k q^{-k/2} \left\{ \sum_{\chi_1 \in A_1} \left| n\chi_1 - \frac{R^{k,1}}{n} \right| + \sum_{\chi_1 \in A_1} \left[ R^{k,1}q^{1/2} + \left( \left| n\chi_1 - \frac{R^{k,1}}{n} \right| + R^{k,1} \right) \right] \right\} \\
\leq (q - 1)^k q^{-k/2} \left[ A_1 \cdots A_m [n\chi_1 - \frac{R^{k,1}}{n}] + \delta A_2 \cdots A_m R^{k,1} (q^{1/2} + 1) \right].
\]

It remains to show (3.4). We have
\[
X = \sum_{\chi_1 \in A_1, i=2,\ldots,m} Y,
\]
where
\[
Y = \sum_{\chi_1 \in A_1} (q - 1)^k q^{n(k+1)/2} \sum_{\alpha \in F_q} K_l(a)^k \overline{K_l(a)} \chi_1 \cdots \chi_m(a).
\]

By the Cauchy-Schwarz inequality,
\[
Y^2 \leq A_1 (q - 1)^{2k} q^{n(k+1)} \sum_{\chi_1 \in A_1} \sum_{\alpha \in F_q} \left| K_l(a)^k \overline{K_l(a)} \chi_1 \cdots \chi_m(ab^{-1}) \right|^2 \\
= A_1 (q - 1)^{2k} q^{n(k+1)} \sum_{a, b \in F_q} \sum_{\chi_1 \in A_1} K_l(a)^k \overline{K_l(a)} K_l(b)^k \overline{K_l(b)} \chi_1 \cdots \chi_m(a^{-1}b^{-1}) \\
= A_1 (q - 1)^{2k+1} q^{n(k+1)} \sum_{a \in F_q} K_l(a)^{k+1} \overline{K_l(a)}^{k+1}.
\]

Thus, by (2.2),
\[
Y^2 \leq A_1 (q - 1)^{2k+1} q^{n(k+1)} (R^{k+1,k+1}q + (n^{2k+1} - 1 + R^{k+1,k+1})q^{1/2}) \\
\leq A_1 \frac{(q - 1)^{2k+1}}{q^{2k+1}} [n^{2k+1} - 1 + R^{k+1,k+1} (q^{1/2} + 1)].
\]

Therefore,
\[
X \leq A_1^{1/2} A_2 \cdots A_m (q - 1)^{2k} q^{2k+1} (n^{2k+1} - 1 + R^{k+1,k+1} (q^{1/2} + 1))^{1/2}.
\]

\[ \square \]
Proof of Theorem 3.3. This is similar to the proof of (3.3). We have

\[ | M_k^{(n)} - \sum_{\rho_j \in R} | \leq \sum_{\rho_1 \cdots \rho_k = 1 \text{ or } \exists j, \rho_j = 1} \leq [(q - 1)^k - N]q^{-n/2}. \]

By (2.1),

\[ \sum_{\rho_j \in R} G(\rho_1)^n \cdots G(\rho_k)^n G(\rho_1 \cdots \rho_k)^n = (q - 1)^k \sum_{a \in F_q} K_n(a)^k K_n(a). \]

It then suffices to apply (2.2).

In Theorem 3.3 an explicit formula for \( N \) can be given by considering the number \( i \) of indices \( 0 \leq j < k \) such that the partial product \( \rho_1 \cdots \rho_j = 1 \):

\[ N = \sum_{i=1}^{[k/2]} \binom{k - i}{i - 1} (q - 2)^i (q - 3)^{k - 1 - 2i}. \]

4 Bound for the discrepancy

The Erdős-Turán inequality \([3, \text{Theorem III}]\) is a quantitative version of Weyl’s criterion on equidistribution. We will use the following form of the inequality, due to Rivat and Tenenbaum \([9, \text{Corollaire 1.3}]\).

Lemma 4.1. Let \( z_1, \ldots, z_N \) be complex numbers on the unit circle. Then, for any integer \( K \geq 0 \), the discrepancy \( D \) (Definition 1.1) satisfies

\[ D \leq \frac{1}{K + 1} + c \sum_{n=1}^{K} \frac{1}{nN} \left| \sum_{i=1}^{N} z_i^n \right|, \]

where \( c = 0.653 \).

It is shown in \([9, \text{Theorem 1}]\) that if \( c’ \) is a constant such that the lemma holds with \( c \) replaced by \( c’ \), then \( c’ \geq \frac{2}{\pi} > 0.636 \).

Proof of Theorem 4.2 Let \( D = D(A_1, \ldots, A_m) \). The cardinality \( N \) of the multiset (1.1) satisfies \( N \geq (A_1 - 1)A_2 \cdots A_m \).

Since \( D \leq 1 \) by definition, to show (4.2), we may assume \( 3A_1^{-1/3}q^{1/6} < 1 \), namely \( A_1 > 3^3q^{1/2} \). As \( A_1 < q \), this implies \( A_1 > 3^6 \). By Lemma 4.1, for any integer \( K \geq 1 \), we have

\[ D \leq \frac{1}{K + 1} + \frac{c}{(A_1 - 1)A_2 \cdots A_m} \sum_{n=1}^{K} M(n). \]

Thus, by (3.4) and the inequality \((a + b)^{1/2} \leq a^{1/2} + b^{1/2}\) for \( a, b \geq 0 \), we have

\[ D \leq \frac{1}{K + 1} + \frac{A_1^{1/2}}{A_1 - 1} A_2^{-1/2} \left[ \sum_{n=1}^{K} n^{-1}q^{1/2} + \sum_{n=2}^{K} n^{-1/2} A_2^{1/2} q^{1/4} \right] \]

\[ \leq \frac{1}{K + 1} + c\left( A_1 A_2 \right)^{-1/2} \left[ (1 + \ln K)q^{1/2} + 2(K^{1/2} - 1)A_2^{1/2} q^{1/4} \right] \frac{A_1}{A_1 - 1}, \]

13
We choose $K$ to optimize the bound for $D$. In this optimization, we ignore $\ln K$ as it is less sensitive to the choice of $K$. Also, we do not attempt to optimize the coefficients. Thus we take $K = \lfloor A_1^{-1/2} q^{-1/6} \rfloor$. Then $K \geq 3$. We have $1 + \ln K \leq \frac{1}{6}(6 + \ln q)$. Thus,

$$D \leq \left[ (1 + 2c) A_1^{-1/3} q^{1/6} + \frac{c}{6} (A_1 A_2)^{-1/2} q^{1/2}(6 + \ln q) \right] (1 - A_1^{-1})^{-1},$$

which implies (1.2).

To show (1.3), we may assume $A_1 \geq A_2$ and $2 A_1^{-2/7} A_2^{-1/7} q^{3/14} < 1$. Thus $2 A_1^{-3/7} q^{3/14} < 1$, namely $A_1 > 2^{7/3} q^{1/2}$. As $A_1 < q$, this implies $A_1 > 2^{4/3} > 25$. By Lemma (3.2), and the case $n = 1$ of (3.1), for any integer $K \geq 1$,

$$D \leq \frac{1}{K + 1} + c A_1^{-1/2} A_2^{-1/4} \left\{ \left[ 1 + \frac{3}{4} \left( \sum_{n=2}^{K} \frac{3^n}{n} + 4 \frac{4^{1/4}}{7} \right) \right] q^{1/2} + \sum_{n=2}^{K} \frac{(n^3 + 3)^{1/4}}{n} q^{3/8} \right\} A_1 A_2^{-1/4},$$

Here we used the inequality

$$\left( \frac{n^3 + 3}{4} \frac{1}{n} \right)^{1/4} \leq (n - 1)^{-1/4}$$

for $n \geq 2$. Let $K = \lfloor A_1^{2/7} A_2^{-1/7} q^{-3/14} \rfloor$. Then $K \geq 2$. We have

$$1 + 3^{1/4} (\ln K - \frac{1}{2}) + \frac{4^{1/4}}{7} \leq 1 + 3^{1/4} (\frac{3}{14} \ln q - \frac{1}{2}) + \frac{4^{1/4}}{7} < \frac{5\ln q}{14}(4 + \ln q),$$

so that

$$D \leq \left[ (1 + \frac{4}{3} c) A_1^{-2/7} A_2^{-1/7} q^{3/14} + \frac{4}{14} c A_1^{-1/2} A_2^{-1/4} q^{1/2}(4 + \ln q) \right] (1 - A_1^{-1})^{-1},$$

which implies (1.3). □

Proof of Theorems 1.4 and 1.6. Let $D = D_k(A_1, \ldots, A_m)$. The cardinality $N$ of the multiset satisfies $N \geq A_1 \cdots A_m (q - 2)^{k-1}(q - 3)$. Let $\epsilon = (1 - \frac{2}{q})^{k-1}(1 - \frac{2}{q})$.

To give a uniform treatment of the cases $m = 0$ and $m \geq 1$, we adopt the convention $A_1 = \delta = 1$ for $m = 0$. By Lemma (2.1 (3.3), and (3.3), for any integer $K \geq 1$,

$$D \leq \frac{1}{K + 1} + c \epsilon^{-1} \sum_{n=1}^{K} n^{-1} \left[ n^k q^{-k/2} + \delta R_{p,n}^{k,1} q^{1/2} + 1 \right] A_1^{-1} q^{-k/2} + (k + 1) q^{-1-n/2} \right]\right\} A_1^{-1} q^{-k/2} + (k + 1) q^{-1-n/2}$$

$$\leq \frac{1}{K + 1} + c \epsilon^{-1} \left[ (K + 1)^k - 1 \right] q^{-k/2} + \epsilon^{-1} \left[ (1 + q^{-1/2}) \delta (1 + R') \ln q \right] q^{(1-k)/2} A_1^{-1} + \frac{1}{1 - q^{1/2}} (k + 1) q^{-3/2} \right]\right\},$$

where $R' = \max_{n \geq 2} R_{p,n}^{k,1} \leq k!$ (Remark (2.3) and we used the fact that $R_{p,n}^{k,1} \leq 1$ for $n = 1$.

For $k \geq 2$, to show (1.5) and (1.9), we may assume $4q^{-\frac{k}{2(\ln q + 1)}} \ln q < 1$. This implies $q^{2/3} > q^{\frac{k}{2(\ln q + 1)}} > 4 \ln q$, so that $q > 70$. Let $K = \lfloor q^{\frac{k}{2(\ln q + 1)}} \rfloor$. Then $K + 2 > q^{\frac{k}{2(\ln q + 1)}} \geq q^{2/5} > 5$. We have

$$\frac{1}{K + 1} = \frac{K + 2}{K + 1} \frac{1}{K + 2} \leq \frac{1}{1 - q^{-2/5}} q^{-\frac{k}{2(\ln q + 1)}} = \frac{1}{1 - q^{-2/5}} q^{-\frac{k}{2(\ln q + 1)}}.$$
For the error terms, we have

\[(1 + R' \ln K)q^{1-k)/2} \leq \frac{1}{2}k!(1 + \ln q)q^{-\frac{k}{2(2k+3)} - \frac{1}{5}},\]

so that

\[\frac{c}{1 - q^{-1/2}}q^{-3/2} < q^{-\frac{k}{2(2k+3)} - 1}.\]

Therefore,

\[D \leq q^{-\frac{k}{2(2k+3)}} \left[ \left( \frac{1}{1 - q^{-2/3}} + \frac{c}{k} \right) + \frac{c}{2}k!q^{-1/6}(1 + \ln q)(1 + q^{-1/2}) + (k + 1)q^{-1} \right] \epsilon^{-1},\]

which implies (1.5) and (1.9). For \(k = 1\), \(R' = 1\). To show (1.7), we may assume \(2q^{-1/4} < 1\), namely \(q > 16\). Let \(K = |c^{-1/2}q^{1/4}|\). Then \(K \geq 2\). We have

\[1 + \ln K \leq 1 - \frac{1}{2} \ln c + \frac{1}{4} \ln q < \frac{1}{4}(5 + \ln q),\]

so that

\[D \leq c^{1/2}q^{-1/4} + \frac{1}{1 - 3q^{-1}}c^{1/2}q^{-1/4} + c^{1+q^{-1/2}}q^{-1/2}(5 + \ln q)A_1^{-1} + 4cq^{-3/2}\]

\[\leq \left[ \left( 1 + \frac{1}{1 - 3q^{-1}} \right) c^{1/2} + 4cq^{-5/4} \right] q^{-1/4} + \frac{c}{2}A_1^{-1}(5 + \ln q)(1 + 2q^{-1/2}),\]

which implies (1.7).

It remains to show (1.6) and (1.8). By Lemma 2.1 and (3.4), for any integer \(K \geq 1\),

\[D \leq \frac{1}{K + 1} + c \sum_{n=1}^{K} n^{-1} \left\{ \left[ n^{k+\frac{1}{2}} + (R_{p,n}^{k+1,k+1})^{1/2}q^{1/4}(1 + q^{-1/2})^{1/2} \right] A_1^{-1/2}q^{\frac{1}{2}} + (k + 1)q^{-1/2} \right\} \epsilon^{-1}\]

\[\leq \frac{1}{K + 1} + \epsilon^{-1} c \left[ \left( K + 1 \right)^{k+\frac{1}{2}} - 1 \right] A_1^{-1/2}q^{\frac{1}{2}} \]

\[+ \epsilon^{-1} c \left( 1 + q^{-1/2} \right)^{1/2} \left\{ 1 + R'' \left[ \ln \left( K + \frac{1}{2} \right) - \ln \frac{3}{2} - \frac{1}{4} \right] + \frac{1}{4}(R_{27}^{k+1,k+1})^{1/2} \right\} A_1^{-1/2}q^{(1-k)/2}\]

\[+ \epsilon^{-1} \frac{c}{1 - q^{-2/3}} (k + 1)q^{-3/2},\]

where \(R'' = \max_n R_{p,n}^{k+1,k+1} = (2k + 1)!!\), the maximum running over all \(n \geq 2\) such that \((p, n) \neq (2, 7)\), and we used the fact that \(R_{p,1}^{k+1,k+1} = 1\) for \(n = 1\). For \(k \geq 2\), we have \(R_{27}^{k+1,k+1} \leq 12 \cdot 7^{2k-3}\) by (2.3). To show (1.6), we may assume

\[2A_1^{-1/2}q^{-\frac{2k-1}{2(2k+3)} - \frac{2}{5}} (7 + \sqrt{15}\ln q) < 1.\]

This implies \(q^{11/14} \geq A_1^{-1/2}q^{-\frac{2k-1}{2(2k+3)} - \frac{2}{5}} > 2(7 + \sqrt{15}\ln q)\), so that \(q > 150\). Let \(K = \left[ A_1^{-1/2}q^{-\frac{2k-1}{2(2k+3)}} \right] - 1\). Then \(K + 2 > A_1^{-1/2}q^{-\frac{2k-1}{2(2k+3)} - \frac{1}{4}} \geq q^{-\frac{2k-1}{2(2k+3)}} \geq q^{3/14} > 2\). We have

\[\frac{1}{K + 1} = \frac{1}{K + 1} \left[ \frac{1}{K + 1} + 2 \right] \leq \frac{1}{1 - (K + 2)^{-1}} A_1^{-1/2} q^{\frac{2k-1}{2(2k+3)}},\]

\[(K + 1)^{k+\frac{1}{2}} A_1^{-1/2} q^{\frac{1}{2}} \leq A_1^{-1/2} q^{\frac{1}{2}} A_1^{-1/2} q^{\frac{1}{2}} \leq A_1^{-1/2} q^{-\frac{2k-1}{2(2k+3)}}.\]

For the error terms, we have

\[1 + R'' \left[ \ln \left( K + \frac{1}{2} \right) - \ln \frac{3}{2} - \frac{1}{4} \right] \leq \frac{1}{2}(2k + 1)!!^{1/2} \ln q,\]

\[A_1^{-1/2} q^{(1-k)/2} \leq A_1^{-1/2} q^{-\frac{2k-1}{2(2k+3)} - \frac{2}{5}},\]

\[q^{-3/2} < q^{-\frac{2k-1}{2(2k+3)} - 1} \leq A_1^{-1/2} q^{-\frac{2k-1}{2(2k+3)} - 1}.\]
Therefore,

\[
D \leq A_1^{-\frac{1}{2k+1}} q^{-\frac{2k-1}{2k+3}} \left[ \left( \frac{1}{1 - (K + 2)^{-1}} + \frac{c}{k + \frac{1}{2}} \right) + \frac{1}{2} q^{-2/7} \left( 7^{k-1} + (2k + 1)!^{1/2} \ln q \right) + (k + 1)q^{-1} \right] e^{-1},
\]

which implies (1.6). For \( k = 1 \), we have \( R'' = 3 \) and \( R''_{2,7} = 4 \) (Remark 2.4). For \( A_1 \geq q^{3/4} \), to show (1.8), we may assume \( 2A_1^{-1/2} q^{3/4} + \frac{1}{q} \ln q < 1 \). This implies \( q^{17/40} \geq A_1^{-1/2} q^{3/4} + \frac{1}{q} \ln q > 2 \ln q \), so that \( q > 300 \). Let \( K = [A_1^{1/5} q^{1/10}] - 1 \). Then \( K + 2 > A_1^{1/5} q^{1/10} \geq q^{1/4} > 4 \). We have

\[
D \leq K + 2 \frac{1}{K + 1} + \frac{1}{K + 2} + \frac{2}{3} c(K + 1)^{3/2} A_1^{-1/2} q^{-1/4}
\]

\[
+ \left\{ 1 + 3 \left[ \ln(K + \frac{1}{2}) - \ln \frac{3}{2} - \frac{1}{4} \right] + \frac{3}{2} \right\} A_1^{-1/2} + 2q^{-3/2}
\]

\[
\leq A_1^{-1/5} q^{-1/10} \left[ \left( \frac{1}{1 - q^{-1/4}} + \frac{1}{1 - 3q^{-1}} \cdot \frac{2}{3} c \right) + \frac{3}{10} \sqrt{3q^{-1/8}(1 + \ln q)} + 2q^{-6/5} \right],
\]

which implies (1.8).

\[ \square \]

**Proof of Corollary 1.3.** Let \( x = \log_q |\mathcal{A}_1| \) and \( y = \log_q |\mathcal{A}_2| \). Combining the inequalities \( D \leq 1 \), (1.2), and (1.3), we get that there exists a constant \( C \) such that \( D \leq C q^{-f_0(x,y)} \ln q \), where

\[
f_0(x, y) = \max \left\{ 0, \min \left\{ \frac{1}{2} x + \frac{1}{2} y - \frac{1}{2} \right\}, \min \left\{ \frac{1}{2} x + \frac{1}{2} y - \frac{1}{3} \right\}, \min \left\{ \frac{1}{2} x + \frac{1}{2} y - \frac{1}{2}, \frac{1}{2} x + \frac{1}{2} y - \frac{3}{14} \right\} \right\}.
\]

By symmetry, \( D \leq C q^{-f_0(y,x)} \ln q \), so that \( D \leq C q^{-f(x,y)} \ln q \), where

\[
f(x, y) = \max \left\{ f_0(x, y), f_0(y, x) \right\}.
\]

It is easy to check that \( f(x, y) \) is as described in the corollary.

\[ \square \]

**Proof of Corollary 1.5.** Let \( x = \log_q |\mathcal{A}_1| \). For \( k \geq 2 \), by the inequalities (1.5) and (1.6), there exists a constant \( C_k \) such that \( D \leq C_k q^{-g_k(x)} \), where

\[
g_k(x) = \max \left\{ \frac{k}{2(k+1)}, \frac{2k-1}{2k+3} x + \frac{2k-1}{2k+3} \right\}.
\]

For \( k = 1 \), by the inequalities (1.7) and (1.8), there exists a constant \( C' \) such that \( D \leq C' q^{-h(x)} \ln q \), where

\[
h(x) = \begin{cases} 
\min \{ x, \frac{1}{4} \} & x \leq \frac{3}{4}, \\
\frac{1}{2} x + \frac{1}{10} & x \geq \frac{3}{4}.
\end{cases}
\]

The case \( k = m = 1 \) can be proven similarly, taking into account of the fact that \( \delta = 0 \) in this case.

\[ \square \]

**Remark 4.2.** Our estimates of the moments \( M_k^{(n)} \) also provide a lower bound for the discrepancy \( D_k \) for \( k \geq 3 \) or \( p = 2 \). By a general result on the discrepancy of probability measures [12, Theorem 1], we have

\[
D_k \geq \left( \frac{2}{\pi^2} \sum_{n=1}^{\infty} \left| \frac{M_k^{(n)} 2}{N^2 n^2} \right|^{1/2} \right)^{1/2}.
\]
For $k \geq 3$, we have $R_{p,k-1}^{k,1} \geq k - 1$ for $n = k - 1$. Thus, by Theorem 3.3, we have

$$|M_{k}^{(k-1)}| \geq Nq^{k-1}(k - 1) - (q - 1)^k q^{-k/2}[(k - 1)^k - 1 + k!].$$

Therefore, for $q \geq 4$, we have

$$D_k \geq \frac{\sqrt{2}}{\pi} q^{-1/4} \left[1 - 2q^{-1/2}(k - 1)^{k-1} \left(\frac{q-1}{q-3}\right)^k\right].$$

For $k = p = 2$, we have $R_{2,3}^{2,1} = 1$ for $n = 3$. Thus, by Theorem 3.3, we have

$$|M_{2}^{(3)}| \geq (q - 2)(q - 3)q^{-1/2} - 9(q - 1)^2 q^{-1}.$$

Therefore, for $q = 2^f \geq 4$, we have

$$D_2 \geq \frac{\sqrt{2}}{3\pi} q^{-1/2} \left[1 - 9q^{-1/2} \left(\frac{q-1}{q-3}\right)^2\right].$$

Acknowledgements

We thank Ming Fang, Ofer Gabber, and Nicholas Katz for useful discussions. Part of this work was done during visits of the first named and the second named authors to l’Institut des Hautes Études Scientifiques. He thanks the institute for hospitality and support. We thank the referee for helpful comments.

References


