On the distribution of Jacobi sums

Qing Lu[*] Weizhe Zheng[†] Zhiyong Zheng[‡§]

Abstract

Let $\mathbf{F}_q$ be a finite field of q elements. For multiplicative characters $\chi_1, \dots, \chi_m$ of $\mathbf{F}_q^\times$, we let $J(\chi_1, \dots, \chi_m)$ 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 χ_1 and χ_2 run through all nontrivial multiplicative characters of $\mathbf{F}_q^\times$. In this paper, we show a similar property for $m \geq 2$. More generally, we show that the normalized Jacobi sum $q^{-(m-1)/2}J(\chi_1, \dots, \chi_m)$ ($\chi_1 \cdots \chi_m$ nontrivial) is asymptotically equidistributed on the unit circle, when $\chi_1, \dots, \chi_m$ run through arbitrary sets of nontrivial multiplicative characters of $\mathbf{F}_q^\times$ with two of the sets being sufficiently large. The case $m = 2$ answers a question of Shparlinski.

1 Introduction

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

$$G(\psi, \chi) = \sum_{a \in \mathbf{F}_q^\times} \psi(a)\chi(a).$$

For $m \geq 2$, $\chi_1, \dots, \chi_m \in \bar{\mathcal{X}}$, we consider the Jacobi sum

$$J(\chi_1, \dots, \chi_m) = \sum_{\substack{a_1, \dots, a_m \in \mathbf{F}_q^\times \\ a_1 + \cdots + a_m = 1}} \chi_1(a_1) \cdots \chi_m(a_m).$$

[*] 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 $\chi, \chi_1, \dots, \chi_m \in \mathcal{X}$, $\chi_1 \cdots \chi_m \neq \mathbf{1}$, where $\mathbf{1}$ denotes the trivial multiplicative character,

$$|G(\psi, \chi)| = q^{1/2}, \qquad |J(\chi_1, \dots, \chi_m)| = q^{(m-1)/2}.$$

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

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

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

$$\{q^{-1/2} G(\psi, \chi)\}_{\psi \in \Phi,\ \chi \in \mathcal{A}},$$

where ψ and χ 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

$$\{q^{-(m-1)/2} J(\chi_1, \dots, \chi_m)\}_{\chi_i \in \mathcal{A}_i,\ \chi_1 \cdots \chi_m \neq \mathbf{1}}, \tag{1.1}$$

for $m \geq 2$, where the χ_i's run through arbitrary nonempty subsets $\mathcal{A}_i \subseteq \mathcal{X}$, $i = 1, \dots, m$. 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 $\{z_1, \dots, z_N\}$ 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 $z_i = e^{2\pi i c}$. For $N = 0$ we put $D = 1$. We say that a sequence or net of such multisets $(\{z_{\alpha,1}, \dots, z_{\alpha,N_\alpha}\})_{\alpha \in I}$ is *asymptotically equidistributed* if $D = o(1)$.

For $N \geq 1$ we have $\frac{1}{N} \leq D \leq 1$. We let $D(\mathcal{A}_1, \dots, \mathcal{A}_m)$ denote the discrepancy of the multiset (1.1).

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

$$D(\mathcal{A}_1, \dots, \mathcal{A}_m) \leq 3A_1^{-1/3} q^{1/6} + \tfrac{1}{9}(A_1A_2)^{-1/2} q^{1/2}(6 + \ln q), \tag{1.2}$$

$$D(\mathcal{A}_1, \dots, \mathcal{A}_m) \leq 2A_1^{-2/7} A_2^{-1/7} q^{3/14} + \tfrac{1}{5} A_1^{-1/2} A_2^{-1/4} q^{1/2}(4 + \ln q). \tag{1.3}$$

Since $D(\mathcal{A}_1,\dots,\mathcal{A}_m)$ is symmetric in the $\mathcal{A}_i$'s, (1.2) is equivalent to

$$D(\mathcal{A}_1,\dots,\mathcal{A}_m) \le 3(\max_i \#\mathcal{A}_i)^{-1/3}q^{1/6} + \tfrac{1}{9}(\max_{i\ne j} \#\mathcal{A}_i\#\mathcal{A}_j)^{-1/2}q^{1/2}(6+\ln q).$$

Therefore, (1.1) is asymptotically equidistributed when $q\ln^2 q/\max_{i\ne j}\#\mathcal{A}_i\#\mathcal{A}_j \to 0$. We note that this condition cannot be substantially improved. In fact, for $\mathcal{A}_2,\dots,\mathcal{A}_m$ satisfying $\#\mathcal{A}_2=\cdots=\#\mathcal{A}_m=1$, there exists $\mathcal{A}_1$ satisfying $\#\mathcal{A}_1\ge(q-3)/2$ such that (1.1) is contained in a semicircle, so that $D(\mathcal{A}_1,\dots,\mathcal{A}_m)\ge\frac{1}{2}$.

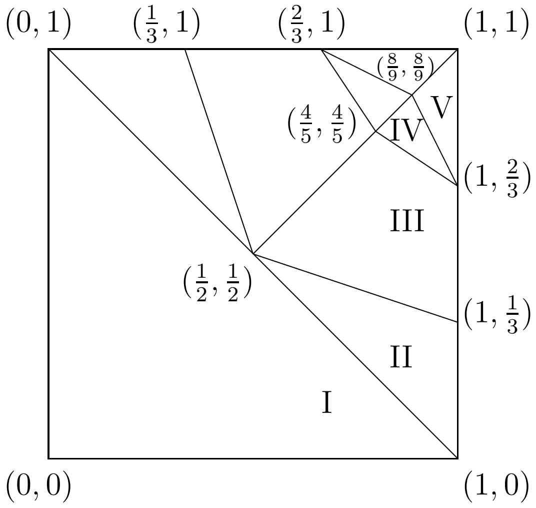
Corollary 1.3. *There exists a constant C such that for all $m\ge 2$ and for nonempty subsets $\mathcal{A}_1,\dots,\mathcal{A}_m$ of $\mathcal{X}$, we have*

$$D(\mathcal{A}_1,\dots,\mathcal{A}_m)\le Cq^{-f(\log_q\#\mathcal{A}_1,\log_q\#\mathcal{A}_2)}\ln q,$$

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

$$f(x,y)=\begin{cases}0 & x+y\le 1,\\ \frac{1}{2}x+\frac{1}{2}y-\frac{1}{2} & x+y\ge 1 \text{ and } x+3y\le 2,\\ \frac{1}{3}x-\frac{1}{6} & x+3y\ge 2 \text{ and } 2x+3y\le 4,\\ \frac{1}{2}x+\frac{1}{4}y-\frac{1}{2} & 2x+3y\ge 4 \text{ and } 2x+y\le\frac{8}{3},\\ \frac{2}{7}x+\frac{1}{7}y-\frac{3}{14} & 2x+y\ge\frac{8}{3}.\end{cases}\tag{1.4}$$

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 $f(0,0)=f(1,0)=f(\frac{1}{2},\frac{1}{2})=0$, $f(\frac{4}{5},\frac{4}{5})=\frac{1}{10}$, $f(1,\frac{1}{3})=f(1,\frac{2}{3})=f(\frac{8}{9},\frac{8}{9})=\frac{1}{6}$, $f(1,1)=\frac{3}{14}$. 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 $\mathcal{X}$. We put $D_k(\mathcal{A}_1,\dots,\mathcal{A}_m)=D(\mathcal{A}_1,\dots,\mathcal{A}_m,\mathcal{X},\dots,\mathcal{X})$ for $m,k\ge 1$ and $D_k=D(\mathcal{X},\dots,\mathcal{X})$ for $k\ge 2$, where $\mathcal{X}$ is repeated k times.

Theorem 1.4. *Let $m\ge 1$ and let $\mathcal{A}_1,\dots,\mathcal{A}_m$ be nonempty subsets of $\mathcal{X}$. Let $A_1=\#\mathcal{A}_1$. Then, for $k\ge 2$,*

$$D_k(\mathcal{A}_1,\dots,\mathcal{A}_m)\le 2q^{-\frac{k}{2(k+1)}}(1+k!q^{-1/6}\ln q),\tag{1.5}$$

$$D_k(\mathcal{A}_1,\dots,\mathcal{A}_m)\le 2A_1^{-\frac{1}{2k+3}}q^{-\frac{2k-1}{2(2k+3)}}\{1+q^{-2/7}[7^{k-1}+(2k+1)!!^{1/2}\ln q]\}.\tag{1.6}$$

For $k=1$, we have

$$D_1(\mathcal{A}_1,\dots,\mathcal{A}_m) \le 2q^{-1/4} + \tfrac{1}{6}\delta A_1^{-1}(5+\ln q)(1+2q^{-1/2}), \tag{1.7}$$

where $\delta = 0$ if $m=1$ and $\delta=1$ if $m>1$. Moreover, for $A_1 \ge q^{3/4}$, we have

$$D_1(\mathcal{A}_1,\dots,\mathcal{A}_m) \le 2A_1^{-1/5}q^{-1/10}(1+q^{-1/8}\ln q). \tag{1.8}$$

Corollary 1.5. *Let $k \ge 1$. There exists a constant C_k such that for all $m \ge 1$ (assuming $m=1$ if $k=1$) and for nonempty subsets $\mathcal{A}_1,\dots,\mathcal{A}_m$ of $\mathcal{X}$, we have*

$$D_k(\mathcal{A}_1,\dots,\mathcal{A}_m) \le C_k q^{-g_k(\log_q \#\mathcal{A}_1)},$$

where $g_k\colon [0,1] \to [\frac{k}{2(k+1)}, \frac{2k+1}{2(2k+3)}]$ is the function

$$g_k(x) = \begin{cases} \frac{k}{2(k+1)} & x \le \frac{2k+1}{2k+2}, \\ \frac{1}{2k+3}x + \frac{2k-1}{2(2k+3)} & x \ge \frac{2k+1}{2k+2}. \end{cases}$$

For $k=1$, there exists a constant C' such that for all $m \ge 1$, we have

$$D_1(\mathcal{A}_1,\dots,\mathcal{A}_m) \le C' q^{-h(\log_q \#\mathcal{A}_1)} \ln q,$$

where $h\colon [0,1] \to [0,\frac{3}{10}]$ is the function

$$h(x) = \begin{cases} x & 0 \le x \le \frac{1}{4}, \\ \frac{1}{4} & \frac{1}{4} \le x \le \frac{3}{4}, \\ \frac{1}{5}x + \frac{1}{10} & \frac{3}{4} \le x \le 1. \end{cases}$$

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 $f(1,x) \le h(x) \le g_1(x)$. Moreover, Corollary 1.5 for $k \ge 2$ improves the case $\mathcal{A}_1 = \mathcal{X}$ of Corollary 1.5 for $k-1$, since $g_{k-1}(1) = \frac{2k-1}{2(2k+1)} < \frac{k}{2(k+1)} = g_k(0) \le g_k(x)$.

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

Theorem 1.6. *For $k \ge 2$, $q \ge 3$, we have*

$$D_k \le 2q^{-\frac{k}{2(k+1)}}(1 + k!q^{-1/6}\ln q). \tag{1.9}$$

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 Zhiyong 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, $k \ge 3$.

2 A key lemma

In the rest of this paper, we fix a nontrivial additive character ψ 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

$$\mathrm{Kl}_n(a) = \sum_{\substack{a_1,\dots,a_n \in \mathbf{F}_q^\times \\ a_1 \cdots a_n = a}} \psi(a_1 + \cdots + a_n).$$

We have $\mathrm{Kl}_1(a) = \psi(a)$. The Fourier transform of $\mathrm{Kl}_n(a)$ is the n-th power of the Gauss sum $G(\chi)$:

$$G(\chi)^n = \sum_{a \in \mathbf{F}_q^\times} \mathrm{Kl}_n(a)\chi(a) \tag{2.1}$$

for all $\chi \in \bar{\mathcal{X}} = \widehat{\mathbf{F}_q^\times}$ [5, 4.0, page 47].

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

$$\left| \sum_{a \in \mathbf{F}_q^\times} \mathrm{Kl}_n(a)^k \overline{\mathrm{Kl}}_n(a)^l - Rq^{\frac{(n-1)(k+l)+2}{2}} \right| \leq \left(\left\lfloor n^{k+l-1} - \frac{R}{n} \right\rfloor + R \right) q^{\frac{(n-1)(k+l)+1}{2}}, \tag{2.2}$$

$$\left| \sum_{a \in \mathbf{F}_q^\times} \chi(a) \mathrm{Kl}_n(a)^k \overline{\mathrm{Kl}}_n(a)^l \right| \leq \left\lfloor n^{k+l-1} - \frac{R}{n} \right\rfloor q^{\frac{(n-1)(k+l)+1}{2}}. \tag{2.3}$$

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,

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

and μ_p is the group of p-th roots of unity in $\mathbf{C}$.

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

$$\mathrm{tr}(\mathrm{Fr}_a, (\mathcal{K}_n)_{\bar{a}}) = (-1)^{n-1}\mathrm{Kl}_n(a),$$

where Fr_a is the geometric Frobenius at $a \in \mathbf{G}_\mathrm{m}(\mathbf{F}_q) = \mathbf{F}_q^\times$ and $\bar{a}$ is a geometric point above a. Moreover,

$$\mathrm{tr}(\mathrm{Fr}_a, (\mathcal{K}_n^\vee)_{\bar{a}}) = (-1)^{n-1}q^{-(n-1)}\overline{\mathrm{Kl}}_n(a).$$

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 $|\mathrm{Kl}_n(a)| \leq nq^{\frac{n-1}{2}}$ 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 $R \leq$

$(k+l-1)!$ (by convention $(-1)!=1$), so that (2.2) provides a nontrivial upper bound for $\left|\sum_{a\in\mathbf{F}_q^\times}\mathrm{Kl}_n(a)^k\overline{\mathrm{Kl}}_n(a)^l\right|$ at least when n is large relative to k and l. For $k=2$, $l=1$, (2.2) recovers the bound $\left|\sum_{a\in\mathbf{F}_q^\times}\mathrm{Kl}_n(a)^2\overline{\mathrm{Kl}}_n(a)\right|\le Rq^{\frac{3n-1}{2}}+n^2q^{\frac{3n-2}{2}}$ in [6, Key Lemma 8, page 549] (in this case $R=0$ or 1, see Remark 2.4 below).

Proof of Lemma 2.1. Recall [1, Théorème 7.8] that the local monodromy of $\mathcal{K}_n$ at 0 is unipotent and tame. The local monodromy at ∞ is totally wild with Swan conductor $\mathrm{swan}_\infty(\mathcal{K}_n)=1$, so that all breaks are $1/n$ [5, Lemma 1.11].

By the Grothendieck trace formula,

$$\sum_{a\in\mathbf{F}_q^\times}\mathrm{Kl}_n(a)^k\overline{\mathrm{Kl}}_n(a)^l=(-1)^{(n-1)(k+l)}q^{(n-1)l}\sum_{i=0}^{2}(-1)^i\mathrm{tr}(\mathrm{Fr}_q,H_c^i),$$

where $H_c^i=H_c^i(\mathbf{G}_{\mathrm{m},\overline{\mathbf{F}_q}},\mathcal{K}_n^{\otimes k}\otimes(\mathcal{K}_n^\vee)^{\otimes l})$. We have $H_c^0=0$ and, by Poincaré duality,

$$H_c^2\simeq H^0(\mathbf{G}_{\mathrm{m},\overline{\mathbf{F}_q}},\mathcal{K}_n^{\otimes l}\otimes(\mathcal{K}_n^\vee)^{\otimes k})^\vee(-1)$$

has dimension $h_c^2=R$. By [5, 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

$$\mathrm{tr}(\mathrm{Fr}_q,H_c^2)=Rq^{\frac{(n-1)(k-l)+2}{2}}.$$

Moreover, $(n-1)(k+l)$ is even whenever $R>0$. By Deligne's Weil II [2, Théorème 3.3.1],

$$\left|\mathrm{tr}(\mathrm{Fr}_q,H_c^1)\right|\le h_c^1q^{\frac{(n-1)(k-l)+1}{2}},$$

where $h_c^1=\dim H_c^1$. 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 ∞ 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

$$\mathrm{swan}_\infty(\mathcal{K}_n^{\otimes k}\otimes(\mathcal{K}_n^\vee)^{\otimes l})\le\lfloor(n^{k+l}-R)/n\rfloor.$$

The inequality (2.2) then follows from the Grothendieck-Ogg-Shafarevich formula [4, Théorème 7.1]

$$h_c^1=h_c^2+\mathrm{swan}_\infty(\mathcal{K}_n^{\otimes k}\otimes(\mathcal{K}_n^\vee)^{\otimes l}).$$

For (2.3), we may assume that E contains the image of χ. Let $\mathcal{L}_\chi$ be the lisse E_λ-sheaf of rank 1 on $\mathbf{G}_{\mathrm{m},\mathbf{F}_q}$ corresponding to χ. As the local monodromy at 0 of $\mathcal{K}_n^{\otimes l}\otimes(\mathcal{K}_n^\vee)^{\otimes k}\otimes\mathcal{L}_\chi^\vee$ is given by a successive extension of $\bar\chi$, we have

$$H_c^2(\mathbf{G}_{\mathrm{m},\overline{\mathbf{F}_q}},\mathcal{L}_\chi\otimes\mathcal{K}_n^{\otimes k}\otimes(\mathcal{K}_n^\vee)^{\otimes l})\simeq H^0(\mathbf{G}_{\mathrm{m},\overline{\mathbf{F}_q}},\mathcal{K}_n^{\otimes l}\otimes(\mathcal{K}_n^\vee)^{\otimes k}\otimes\mathcal{L}_\chi^\vee)^\vee(-1)=0.$$

The rest of the proof is completely similar to the proof of the first assertion. □

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 $G=\mathrm{Sp}_n$, 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 $G = \mathrm{Sp}_n$ (n even), we let V_λ denote the irreducible representation corresponding to a partition $\lambda = (\lambda_1 \geq \cdots \geq \lambda_{n/2} \geq 0)$ (where the λ_j's are integers). We have $V \simeq V_\sigma$, where $\sigma = (1, 0, \ldots, 0)$. By King's formula [7, (4.14), (4.15), (4.31)], we have

$$V_\lambda \otimes V_\sigma \simeq \bigoplus_{\lambda'} V_{\lambda'},$$

where λ' runs through σ-expansions and σ-contractions of λ. Here we say that λ' is a σ-expansion of λ, or equivalently λ is a σ-contraction of λ', 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 σ-expansion or a σ-contraction of $\lambda^{(i)}$. Moreover, by classical invariant theory [13, Section VI.7], $(V^{\otimes k})^G$ 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 $G = \mathrm{SO}_n$ (n odd), we let V_λ denote the irreducible representation of $\mathrm{O}_n = \mathrm{SO}_n \times \{\pm 1\}$ corresponding to a partition $\lambda = (\lambda_1 \geq \ldots ge\lambda_n \geq 0)$ satisfying $\lambda^T_1 + \lambda^T_2 \leq n$, where λ^T denotes the conjugate of λ. We have $V \simeq \mathrm{Res}^{\mathrm{O}_n}_{\mathrm{SO}_n} V_\sigma$ and, for $\lambda \neq \lambda'$, $\mathrm{Res}^{\mathrm{O}_n}_{\mathrm{SO}_n} V_\lambda \simeq \mathrm{Res}^{\mathrm{O}_n}_{\mathrm{SO}_n} V_{\lambda'}$ if and only if $\lambda^T_1 + \lambda'^T_1 = n$ and $\lambda^T_j = \lambda'^T_j$ for all $j > 1$. By King's formula for O_n [7, (4.14), (4.15)], we have $V_\lambda \otimes V_\sigma \simeq \bigoplus_{\lambda'} V_{\lambda'}$, where λ' runs through σ-expansions and σ-contractions of λ. Thus, for k odd (resp. even), R^k is the number of sequences of partitions $\lambda^{(0)}, \ldots, \lambda^{(k)}$, where $\lambda^{(i)} = (\lambda^{(i)}_1 \geq \cdots \geq \lambda^{(i)}_n \geq 0)$, $\lambda^{(0)} = (0, \ldots, 0)$, $\lambda^{(k)} = (1, \ldots, 1)$ (resp. $\lambda^{(k)} = (0, \ldots, 0)$), such that for each i, $\lambda^{(i+1)}$ is a σ-expansion or a σ-contraction of $\lambda^{(i)}$. Moreover, by classical invariant theory [13, Sections II.9, II.17], for k odd, $(V^{\otimes k})^G$ is spanned by the images of $\mathbf{C} \simeq \wedge^n V \subset V^{\otimes n}$ 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 $k < n$ and $R^k \leq \binom{k}{n}(k-n-1)!! \leq (k-1)!$ for $k \geq n$ (assuming $n \geq 3$). For k even, $(V^{\otimes k})^G$ 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_λ denote the irreducible representation corresponding to a partition $\lambda = (\lambda_1 \geq \lambda_2 \geq 0)$, so that $V_{0,0} = \mathbf{C}$, $V_{1,0} = V$. By Littelmann's generalized Littlewood-Richardson rule [8, 3.8], we have $V_\lambda \otimes V^{\otimes k} \simeq \bigoplus_{\lambda'} V_{\lambda'}$, where λ' satisfies one of the following

- λ' is a σ-expansion or a σ-contraction of λ; or
- $\lambda'_1 = \lambda_1 \pm 1$ and $\lambda'_2 = \lambda_2 \mp 1$; or
- $\lambda' = \lambda$ and $\lambda_1 > \lambda_2$.

Note that, for each λ, there are at most 7 possibilities for λ'. We have

$$V^{\otimes 2} \simeq V_{0,0} \oplus V_{1,0} \oplus V_{2,0} \oplus V_{1,1}, \qquad V^{\otimes 3} \simeq V_{0,0} \oplus V_{1,0}^{\oplus 4} \oplus V_{2,0}^{\oplus 3} \oplus V_{3,0} \oplus V_{1,1}^{\oplus 2} \oplus V_{2,1}^{\oplus 2},$$
$$V^{\otimes 4} \simeq V_{0,0}^{\oplus 4} \oplus V_{1,0}^{\oplus 10} \oplus V_{2,0}^{\oplus 12} \oplus V_{3,0}^{\oplus 6} \oplus V_{4,0} \oplus V_{1,1}^{\oplus 9} \oplus V_{2,1}^{\oplus 8} \oplus V_{3,1}^{\oplus 3} \oplus V_{2,2}^{\oplus 2},$$

and, for $k \geq 4$, the multiplicities appearing in the decomposition of V_λ 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

$$R^k_{G_2} \leq 12 \cdot 7^{k-5} \tag{2.4}$$

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 [10, Theorem 3.23]. It follows from this or (2.4) that $R^k \leq (k-1)!$.[1]

For $G = \mathrm{SL}_n$, we let V_λ denote the representation of GL_n corresponding to a sequence $(\lambda_1 \geq \cdots \geq \lambda_n)$ (where the λ_j's are integers, possibly negative), so that $V \simeq \mathrm{Res}^{\mathrm{GL}_n}_{\mathrm{SL}_n} V_\sigma$ and $\mathrm{Res}^{\mathrm{GL}_n}_{\mathrm{SL}_n} V_\lambda \simeq \mathrm{Res}^{\mathrm{GL}_n}_{\mathrm{SL}_n} V_{\lambda'}$ if and only if λ and λ' 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 λ' runs through σ-expansions of λ and $V_\lambda \otimes V_\sigma^* \simeq \bigoplus V_{\lambda'}$ where λ' runs through σ-contractions of λ. Thus $R^{k,l} \neq 0$ if and only if $k \equiv l \pmod{n}$. In this case, $R^{k,l}$ is the number of sequences of partitions $\lambda^{(0)}, \ldots, \lambda^{(k+l)}$, where $\lambda^{(0)} = (0, \ldots, 0)$, $\lambda^{(k+l)} = (\frac{l-k}{n}, \ldots, \frac{l-k}{n})$, such that for each $0 \leq i < l$, $\lambda^{(i+1)}$ is a σ-expansion of $\lambda^{(i)}$, and for each $l \leq i < k+l$, $\lambda^{(i+1)}$ is a σ-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 σ-expansions and the number of σ-contractions of λ are both equal to $\delta(\lambda)+1$. Moreover, for any σ-expansion or σ-contraction λ' of λ, $|\delta(\lambda') - \delta(\lambda)| \leq 1$. Thus $R^{k,l} \leq \lfloor \frac{k+l}{2} \rfloor ! \lfloor \frac{k+l-1}{2} \rfloor !$. We will be particularly interested in $R^{k,1}$ and $R^{k,k}$. For $k \equiv 1 \pmod{n}$, $R^{k,1} = R^{1,k}$ 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

$$R^{k,1}_{\mathrm{SL}_n} = k!/\frac{(n+\frac{k-1}{n})!}{n!} \prod_{i=0}^{n-2} \frac{(i+\frac{k-1}{n})!}{i!}$$

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

$$R^{k,k}_{\mathrm{SL}_n} = \sum_\lambda m_\lambda^2 \leq k!,$$

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

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

Remark 2.4. Let us list the values of $R^{k,1}_G$ and $R^{k,k}_G$ for $1 \leq k \leq 3$.

- $R^{1,1}_G = 1$ in all cases.
- $R^{2,1}_G = 1$ for $G = \mathrm{SO}_3$ or G_2 and $R^{2,1}_G = 0$ otherwise.
- $R^{3,1}_G = 0$ for $G = \mu_p$ (p odd) or SL_n, $R^{3,1}_{\mu_2} = 1$, $R^{3,1}_{\mathrm{Sp}_2} = 2$, $R^{3,1}_G = 3$ for $G = \mathrm{Sp}_n$ ($n \geq 4$) or SO_n, and $R^{3,1}_{G_2} = 4$.
- $R^{2,2}_{\mu_p} = 1$, $R^{2,2}_G = 2$ for $G = \mathrm{Sp}_2$ or SL_n, $R^{2,2}_G = 3$ for $G = \mathrm{Sp}_n$ ($n \geq 4$) or SO_n, and $R^{2,2}_{G_2} = 4$.
- $R^{3,3}_{\mu_p} = 1$, $R^{3,3}_{\mathrm{Sp}_2} = 5$, $R^{3,3}_{\mathrm{SL}_n} = 6$, $R^{3,3}_{\mathrm{Sp}_4} = 14$, $R^{3,3}_G = 15$ for $G = \mathrm{Sp}_n$ ($n \geq 6$) or SO_n, and $R^{3,3}_{G_2} = 35$.

[1] The sequence $R^k_{G_2}$ ($k \geq 0$) 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 $\mathcal{A}_1, \dots, \mathcal{A}_m$ of $\mathcal{X}$, $m \geq 2$ and $n \geq 1$, we consider the incomplete n-th moment of the normalized Jacobi sums (1.1):

$$M^{(n)}(\mathcal{A}_1, \dots, \mathcal{A}_m) = \sum_{\substack{\chi_i \in \mathcal{A}_i \\ \chi_1 \cdots \chi_m \neq \mathbf{1}}} q^{-n(m-1)/2} J(\chi_1, \dots, \chi_m)^n.$$

When some of the subsets are $\mathcal{X}$, we adopt the following shorthand, similar to the notation on discrepancy. We put $M_k^{(n)}(\mathcal{A}_1, \dots, \mathcal{A}_m) = M^{(n)}(\mathcal{A}_1, \dots, \mathcal{A}_m, \mathcal{X}, \dots, \mathcal{X})$ for $m, k \geq 1$ and $M_k^{(n)} = M^{(n)}(\mathcal{X}, \dots, \mathcal{X})$ for $k \geq 2$, where $\mathcal{X}$ is repeated k times. The statements of the following theorems make use of the notation $R_{p,n}^{k,l}$ introduced in Lemma 2.1.

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

$$|M^{(n)}(\mathcal{A}_1, \dots, \mathcal{A}_m)| \leq (A_1 A_2)^{1/2} A_3 \cdots A_m [q + (n-1) A_2 q^{1/2}]^{1/2}, \tag{3.1}$$

$$|M^{(n)}(\mathcal{A}_1, \dots, \mathcal{A}_m)| \leq A_1^{1/2} A_2^{3/4} A_3 \cdots A_m [R_{p,n}^{2,2} q^2 + (n^3 + R_{p,n}^{2,2} - 1) q^{3/2}]^{1/4}. \tag{3.2}$$

Recall from Remark 2.3 that $R_{p,n}^{2,2} \leq 3$ except for $(p, n) = (2, 7)$ in which case $R_{2,7}^{2,2} = 4$.

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

$$|M_k^{(n)}(\mathcal{A}_1, \dots, \mathcal{A}_m)| \leq A_2 \cdots A_m (q-1)^k q^{-k/2} \left[A_1 \lfloor n^k - \tfrac{R_{p,n}^{k,1}}{n} \rfloor + \delta R_{p,n}^{k,1} (q^{1/2} + 1) \right] + T, \tag{3.3}$$

$$\begin{aligned} &|M_k^{(n)}(\mathcal{A}_1, \dots, \mathcal{A}_m)| \\ &\qquad \leq A_2 \cdots A_m A_1^{1/2} (q-1)^{\frac{2k+1}{2}} q^{-\frac{2k+1}{4}} \left[n^{2k+1} - 1 + R_{p,n}^{k+1,k+1} (q^{1/2} + 1) \right]^{1/2} + T, \end{aligned} \tag{3.4}$$

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 $n \geq 1$,*

$$\left| M_k^{(n)} - (q-1)^k q^{\frac{1-k}{2}} R_{p,n}^{k,1} \right| \leq (q-1)^k q^{-k/2} \left(\lfloor n^k - \tfrac{R_{p,n}^{k,1}}{n} \rfloor + R_{p,n}^{k,1} \right) + [(q-1)^k - N] q^{-n/2}, \tag{3.5}$$

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

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 $|M_2^{(n)}| \leq n^2 q + R_{p,n}^{2,1} q^{3/2}$ 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 $\bar{\mathcal{X}}$. We estimate the complete sum using Lemma 2.1.

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

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

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

Proof of Theorem 3.1. We may assume $A_1 \geq A_2$. Let $M^{(n)} = M^{(n)}(\mathcal{A}_1, \dots, \mathcal{A}_m)$. By the facts recalled above,

$$|M^{(n)}| = \left| \sum_{\substack{\chi_i\in\mathcal{A}_i\\ \chi_1\cdots\chi_m\neq\mathbf{1}}} \left[q^{-(m+1)/2}G(\chi_1)\cdots G(\chi_m)\overline{G(\chi_1\cdots\chi_m)}\right]^n \right| \leq \left|\sum_{\substack{\chi_i\in\mathcal{A}_i\\ \chi_1\cdots\chi_m=\mathbf{1}}}\right| + \left|\sum_{\chi_i\in\mathcal{A}_i}\right|$$
$$\leq A_2\cdots A_m q^{-n/2} + W \leq (A_1A_2)^{1/2}A_3\cdots A_m q^{-n/2} + W,$$

where

$$W = \sum_{\chi_1\in\mathcal{A}_1}\left|\sum_{\chi_i\in\mathcal{A}_i,\ i=2,\dots,m}[q^{-m/2}G(\chi_2)\cdots G(\chi_m)\overline{G(\chi_1\cdots\chi_m)}]^n\right|.$$

By the Cauchy-Schwarz inequality,

$$W^2 \leq A_1\sum_{\chi_1\in\mathcal{A}_1}\left|\sum_{\chi_i\in\mathcal{A}_i,\ i=2,\dots,m}\left[q^{-m/2}G(\chi_2)\cdots G(\chi_m)\overline{G(\chi_1\cdots\chi_m)}\right]^n\right|^2$$
$$\leq A_1\sum_{\chi_1\in\bar{\mathcal{X}}}\left|\sum_{\chi_i\in\mathcal{A}_i,\ i=2,\dots,m}\right|^2$$
$$= A_1\sum_{\chi_1\in\bar{\mathcal{X}}}\sum_{\chi_i,\chi_i'\in\mathcal{A}_i,\ i=2,\dots,m}\left[q^{-m}G(\chi_2)\cdots G(\chi_m)\overline{G(\chi_1\chi_2\cdots\chi_m)}\overline{G(\chi_2')\cdots G(\chi_m')\overline{G(\chi_1\chi_2'\cdots\chi_m')}}\right]^n$$
$$\leq A_1\sum_{\chi_i,\chi_i'\in\mathcal{A}_i,\ i=2,\dots,m} q^{-n}\left|\sum_{\chi_1\in\bar{\mathcal{X}}}\overline{G(\chi_1\chi_2\cdots\chi_m)}^n G(\chi_1\chi_2'\cdots\chi_m')^n\right| =: X$$

By (2.1),

$$\sum_{\chi_1\in\bar{\mathcal{X}}}\overline{G(\chi_1\chi_2\cdots\chi_m)}^n G(\chi_1\chi_2'\cdots\chi_m')^n = \sum_{a,b\in\mathbf{F}_q^\times}\sum_{\chi_1\in\bar{\mathcal{X}}}\overline{\mathrm{Kl}}_n(a)\mathrm{Kl}_n(b)\overline{\chi_1\cdots\chi_m}(a)\chi_1'\cdots\chi_m'(b)$$
$$= (q-1)\sum_{a\in\mathbf{F}_q^\times}\mathrm{Kl}_n(a)\overline{\mathrm{Kl}}_n(a)\overline{\chi_2\cdots\chi_m}\chi_2'\cdots\chi_m'(a).$$

For $\chi_2\cdots\chi_m = \chi_2'\cdots\chi_m'$, we have

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

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

$$X = A_1\sum_{\substack{\chi_i,\chi_i'\in\mathcal{A}_i,\ i=2,\dots,m\\ \chi_2\cdots\chi_m=\chi_2'\cdots\chi_m'}} + A_1\sum_{\substack{\chi_i,\chi_i'\in\mathcal{A}_i,\ i=2,\dots,m\\ \chi_2\cdots\chi_m\neq\chi_2'\cdots\chi_m'}}$$
$$\leq A_1A_2(A_3\cdots A_m)^2(q-2+q^{-n}) + A_1(A_2\cdots A_m)^2(q-1)(n-1)q^{-1/2}$$
$$= A_1A_2(A_3\cdots A_m)^2[q-2+q^{-n}+(n-1)A_2(q-1)q^{-1/2}].$$

Thus

$$|M^{(n)}| \leq (A_1A_2)^{1/2}A_3\cdots A_m\{q^{-n/2} + [q-2+q^{-n}+(n-1)A_2(q-1)q^{-1/2}]^{1/2}\}.$$

For (3.1), it suffices to show

$$q-2+q^{-n}+(n-1)A_2(q-1)q^{-1/2} \leq \left\{[q+(n-1)A_2q^{1/2}]^{1/2} - q^{-n/2}\right\}^2,$$

namely

$$2q^{-n/2}[q+(n-1)A_2q^{1/2}]^{1/2} \le (n-1)A_2q^{-1/2}+2,$$

which is clear by taking squares.

It remains to show (3.2) for $n \ge 2$. We have

$$X = A_1 \sum_{\substack{\chi_2'\in\mathcal{A}_2 \\ \chi_i,\chi_i'\in\mathcal{A}_i,\ i=3,\dots,m}} Y,$$

where

$$Y = \sum_{\chi_2\in\mathcal{A}_2} \frac{q-1}{q^n}\left|\sum_{a\in\mathbf{F}_q^\times} \mathrm{Kl}_n(a)\overline{\mathrm{Kl}}_n(a)\overline{\chi_2\cdots\chi_m}\chi_2'\cdots\chi_m'(a)\right|.$$

To obtain (3.2), we apply the Cauchy-Schwarz inequality again:

$$\begin{aligned}
Y^2 &\le A_2\left(\frac{q-1}{q^n}\right)^2 \sum_{\chi_2\in\mathcal{A}_2}\left|\sum_{a\in\mathbf{F}_q^\times}\right|^2 \le A_2\left(\frac{q-1}{q^n}\right)^2 \sum_{\chi_2\in\bar{\mathcal{X}}}\left|\sum_{a\in\mathbf{F}_q^\times}\right|^2 \\
&= A_2\left(\frac{q-1}{q^n}\right)^2 \sum_{a,b\in\mathbf{F}_q^\times}\sum_{\chi_2\in\bar{\mathcal{X}}} |\mathrm{Kl}_n(a)\mathrm{Kl}_n(b)|^2\overline{\chi_2\cdots\chi_m}\chi_2'\cdots\chi_m'(ab^{-1}) \\
&= A_2\frac{(q-1)^3}{q^{2n}}\sum_{a\in\mathbf{F}_q^\times}\mathrm{Kl}_n(a)^2\overline{\mathrm{Kl}}_n(a)^2.
\end{aligned}$$

Thus, by (2.2), we have

$$\begin{aligned}
Y^2 &\le A_2(q-1)^3[R^{2,2}q^{-1}+(n^3+R^{2,2}-1)q^{-3/2}] \\
&= A_2[R^{2,2}q^2+(n^3+R^{2,2}-1)q^{3/2}](1-\tfrac{1}{q})^3,
\end{aligned}$$

so that

$$X \le A_1A_2(A_3\cdots A_m)^2A_2^{1/2}[R^{2,2}q^2+(n^3+R^{2,2}-1)q^{3/2}]^{1/2}(1-\tfrac{1}{q})^{3/2}.$$

Therefore,

$$\begin{aligned}
|M^{(n)}| &\le (A_1A_2)^{1/2}A_3\cdots A_m\left\{q^{-n/2}+(1-\tfrac{1}{q})^{3/4}A_2^{1/4}[R^{2,2}q^2+(n^3+R^{2,2}-1)q^{3/2}]^{1/4}\right\} \\
&\le (A_1A_2)^{1/2}A_3\cdots A_mA_2^{1/4}[R^{2,2}q^2+(n^3+R^{2,2}-1)q^{3/2}]^{1/4}.
\end{aligned}$$

Here we used the inequality $(1-\frac{1}{q})^{3/4} \le 1-\frac{3}{4q}$. □

Proof of Theorem 3.2. We have

$$\begin{aligned}
&|M_k^{(n)}(\mathcal{A}_1,\dots,\mathcal{A}_m)| \\
&= \left|\sum_{\substack{\chi_i\in\mathcal{A}_i,\ \rho_j\in\mathcal{X} \\ \chi_1\cdots\chi_m\rho_1\cdots\rho_k\neq\mathbf{1}}}\left[q^{-(m+k+1)/2}G(\chi_1)\cdots G(\chi_m)G(\rho_1)\cdots G(\rho_k)\overline{G(\chi_1\cdots\chi_m\rho_1\cdots\rho_k)}\right]^n\right| \\
&\le \left|\sum_{\substack{\chi_i\in\mathcal{A}_i,\ \rho_j\in\bar{\mathcal{X}} \\ \chi_1\cdots\chi_m\rho_1\cdots\rho_k=\mathbf{1}\text{ or }\exists j,\rho_j=\mathbf{1}}}\right| + \left|\sum_{\chi_i\in\mathcal{A}_i,\ \rho_j\in\bar{\mathcal{X}}}\right| \\
&\le (k+1)A_1\cdots A_m(q-1)^{k-1}q^{-n/2}+X,
\end{aligned}$$

where

$$X = \sum_{\chi_i\in\mathcal{A}_i} q^{-n(k+1)/2}\left|\sum_{\rho_j\in\bar{\mathcal{X}}} G(\rho_1)^n\cdots G(\rho_k)^n\overline{G(\chi_1\cdots\chi_m\rho_1\cdots\rho_k)}^n\right|.$$

By (2.1),

$$\sum_{\rho_j\in\bar{\mathcal{X}}} G(\rho_1)^n\cdots G(\rho_k)^n\overline{G(\chi_1\cdots\chi_m\rho_1\cdots\rho_k)}^n = (q-1)^k\sum_{a\in\mathbf{F}_q^\times}\mathrm{Kl}_n(a)^k\overline{\mathrm{Kl}}_n(a)\overline{\chi_1\cdots\chi_m}(a).$$

Thus, by Lemma 2.1, we have

$$\begin{aligned} X &= \sum_{\substack{\chi_i\in\mathcal{A}_i\\ \chi_1\cdots\chi_m\neq\mathbf{1}}} + \sum_{\substack{\chi_i\in\mathcal{A}_i\\ \chi_1\cdots\chi_m=\mathbf{1}}}\\ &\le (q-1)^kq^{-k/2}\left\{\sum_{\substack{\chi_i\in\mathcal{A}_i\\ \chi_1\cdots\chi_m\neq\mathbf{1}}}\lfloor n^k-\tfrac{R^{k,1}}{n}\rfloor + \sum_{\substack{\chi_i\in\mathcal{A}_i\\ \chi_1\cdots\chi_m=\mathbf{1}}}\left[R^{k,1}q^{1/2}+(\lfloor n^k-\tfrac{R^{k,1}}{n}\rfloor+R^{k,1})\right]\right\}\\ &\le (q-1)^kq^{-k/2}\left[A_1\cdots A_m\lfloor n^k-\tfrac{R^{k,1}}{n}\rfloor+\delta A_2\cdots A_mR^{k,1}(q^{1/2}+1)\right].\end{aligned}$$

It remains to show (3.4). We have

$$X = \sum_{\chi_i\in\mathcal{A}_i,\ i=2,\ldots,m} Y,$$

where

$$Y = \sum_{\chi_1\in\mathcal{A}_1}\frac{(q-1)^k}{q^{n(k+1)/2}}\left|\sum_{a\in\mathbf{F}_q^\times}\mathrm{Kl}_n(a)^k\overline{\mathrm{Kl}}_n(a)\overline{\chi_1\cdots\chi_m}(a)\right|.$$

By the Cauchy-Schwarz inequality,

$$\begin{aligned} Y^2 &\le A_1\frac{(q-1)^{2k}}{q^{n(k+1)}}\sum_{\chi_1\in\mathcal{A}_1}\left|\sum_{a\in\mathbf{F}_q^\times}\right|^2 \le A_1\frac{(q-1)^{2k}}{q^{n(k+1)}}\sum_{\chi_1\in\bar{\mathcal{X}}}\left|\sum_{a\in\mathbf{F}_q^\times}\right|^2\\ &= A_1\frac{(q-1)^{2k}}{q^{n(k+1)}}\sum_{a,b\in\mathbf{F}_q^\times}\sum_{\chi_1\in\bar{\mathcal{X}}}\mathrm{Kl}_n(a)^k\overline{\mathrm{Kl}}_n(a)\overline{\mathrm{Kl}_n(b)^k\overline{\mathrm{Kl}}_n(b)}\,\overline{\chi_1\cdots\chi_m}(ab^{-1})\\ &= A_1\frac{(q-1)^{2k+1}}{q^{n(k+1)}}\sum_{a\in\mathbf{F}_q^\times}\mathrm{Kl}_n(a)^{k+1}\overline{\mathrm{Kl}}_n(a)^{k+1}.\end{aligned}$$

Thus, by (2.2),

$$\begin{aligned} Y^2 &\le A_1\frac{(q-1)^{2k+1}}{q^{(k+1)}}(R^{k+1,k+1}q+(n^{2k+1}-1+R^{k+1,k+1})q^{1/2})\\ &\le A_1\frac{(q-1)^{2k+1}}{q^{\frac{2k+1}{2}}}[n^{2k+1}-1+R^{k+1,k+1}(q^{1/2}+1)].\end{aligned}$$

Therefore,

$$X \le A_1^{1/2}A_2\cdots A_m(q-1)^{\frac{2k+1}{2}}q^{-\frac{2k+1}{4}}[n^{2k+1}-1+R^{k+1,k+1}(q^{1/2}+1)]^{1/2}.$$

□

Proof of Theorem 3.3. This is similar to the proof of (3.3). We have

$$\left| M_k^{(n)} - \sum_{\rho_j \in \bar{\mathcal{X}}} \right| \leq \left| \sum_{\substack{\rho_j \in \bar{\mathcal{X}} \\ \rho_1 \cdots \rho_k = \mathbf{1} \text{ or } \exists j, \rho_j = \mathbf{1}}} \right| \leq [(q-1)^k - N] q^{-n/2}.$$

By (2.1),

$$\sum_{\rho_j \in \bar{\mathcal{X}}} G(\rho_1)^n \cdots G(\rho_k)^n \overline{G(\rho_1 \cdots \rho_k)}^n = (q-1)^k \sum_{a \in \mathbf{F}_q^\times} \mathrm{Kl}_n(a)^k \overline{\mathrm{Kl}}_n(a).$$

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 $\rho_1 \cdots \rho_j = \mathbf{1}$:

$$N = \sum_{i=1}^{\lceil k/2 \rceil} \binom{k-i}{i-1} (q-2)^i (q-3)^{k+1-2i}.$$

4 Bounds for the discrepancy

The Erdős-Turán inequality [3, 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, 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, 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 1.2. Let $D = D(\mathcal{A}_1, \ldots, \mathcal{A}_m)$. 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 (1.2), we may assume $3 A_1^{-1/3} q^{1/6} < 1$, namely $A_1 > 3^3 q^{1/2}$. As $A_1 < q$, this implies $A_1 > 3^6$. By Lemma 4.1, for any integer $K \geq 1$, we have

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

Thus, by (3.1) and the inequality $(a+b)^{1/2} \leq a^{1/2} + b^{1/2}$ for $a, b \geq 0$, we have

$$\begin{aligned} D &\leq \frac{1}{K+1} + c \frac{A_1^{1/2}}{A_1 - 1} A_2^{-1/2} \left[\sum_{n=1}^{K} n^{-1} q^{1/2} + \sum_{n=2}^{K} n^{-1/2} A_2^{1/2} q^{1/4} \right] \\ &\leq \frac{1}{K+1} + c (A_1 A_2)^{-1/2} \left[(1 + \ln K) q^{1/2} + 2(K^{1/2} - 1) A_2^{1/2} q^{1/4} \right] \frac{A_1}{A_1 - 1}, \end{aligned}$$

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 $K = \lfloor A_1^{1/3} q^{-1/6} \rfloor$. Then $K \geq 3$. We have $1 + \ln K \leq \frac{1}{6}(6 + \ln q)$. Thus,

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

which implies (1.2).

To show (1.3), we may assume $A_1 \geq A_2$ and $2A_1^{-2/7} A_2^{-1/7} q^{3/14} < 1$. Thus $2A_1^{-3/7} q^{3/14} < 1$, namely $A_1 > 2^{7/3} q^{1/2}$. As $A_1 < q$, this implies $A_1 > 2^{14/3} > 25$. By Lemma 4.1, (3.2), and the case $n = 1$ of (3.1), for any integer $K \geq 1$,

$$\begin{aligned} D &\leq \frac{1}{K+1} + c\frac{A_1^{1/2}}{A_1 - 1} A_2^{-1/4} \left\{ \left[1 + \sum_{\substack{n=2 \\ n \neq 7}}^{K} \frac{3^{1/4}}{n} + \frac{4^{1/4}}{7} \right] q^{1/2} + \sum_{n=2}^{K} \frac{(n^3+3)^{1/4}}{n} q^{3/8} \right\} \\ &\leq \frac{1}{K+1} + cA_1^{-1/2} A_2^{-1/4} \left\{ \left[1 + 3^{1/4}(\ln K - \tfrac{1}{7}) + \tfrac{4^{1/4}}{7}\right] q^{1/2} + \tfrac{4}{3}(K-1)^{3/4} q^{3/8} \right\} \frac{A_1}{A_1 - 1}, \end{aligned}$$

Here we used the inequality

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

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

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

so that

$$D \leq \left[(1 + \tfrac{4}{3}c)A_1^{-2/7} A_2^{-1/7} q^{3/14} + \tfrac{3^{5/4}}{14} c A_1^{-1/2} A_2^{-1/4} q^{1/2}(4 + \ln q)\right](1 - A_1^{-1})^{-1},$$

which implies (1.3). □

Proof of Theorems 1.4 and 1.6. Let $D = D_k(\mathcal{A}_1, \ldots, \mathcal{A}_m)$. The cardinality N of the multiset satisfies $N \geq A_1 \cdots A_m (q-2)^{k-1}(q-3)$. Let $\epsilon = (1 - \frac{2}{q})^{k-1}(1 - \frac{3}{q})$.

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 (3.5), for any integer $K \geq 1$,

$$\begin{aligned} D &\leq \frac{1}{K+1} + c\epsilon^{-1} \sum_{n=1}^{K} n^{-1} \left[n^k q^{-k/2} + \delta R_{p,n}^{k,1}(q^{1/2}+1) A_1^{-1} q^{-k/2} + (k+1) q^{-1-n/2} \right] \\ &\leq \frac{1}{K+1} + \epsilon^{-1}\frac{c}{k}[(K+1)^k - 1] q^{-k/2} \\ &\quad + \epsilon^{-1} c \left[(1 + q^{-1/2})\delta(1 + R' \ln K) q^{(1-k)/2} A_1^{-1} + \tfrac{1}{1 - q^{-1/2}}(k+1) q^{-3/2} \right], \end{aligned}$$

where $R' = \max_{n \geq 2} R_{p,n}^{k,1} \leq k!$ (Remark 2.3) and we used the fact that $R_{p,1}^{k,1} \leq 1$ for $n = 1$. For $k \geq 2$, to show (1.5) and (1.9), we may assume $4q^{-\frac{k}{2(k+1)} - \frac{1}{6}} \ln q < 1$. This implies $q^{2/3} > q^{\frac{k}{2(k+1)} + \frac{1}{6}} > 4 \ln q$, so that $q > 70$. Let $K = \lfloor q^{\frac{k}{2(k+1)}} \rfloor - 1$. Then $K + 2 > q^{\frac{k}{2(k+1)}} \geq q^{2/5} > 5$. We have

$$\frac{1}{K+1} = \frac{K+2}{K+1}\frac{1}{K+2} \leq \frac{1}{1 - q^{-2/5}} q^{-\frac{k}{2(k+1)}}, \qquad (K+1)^k q^{-k/2} \leq q^{-\frac{k}{2(k+1)}}.$$

For the error terms, we have

$$(1+R'\ln K)q^{(1-k)/2} \le \tfrac{1}{2}k!(1+\ln q)q^{-\frac{k}{2(k+1)}-\frac{1}{6}},$$
$$\tfrac{c}{1-q^{-1/2}}q^{-3/2} < q^{-\frac{k}{2(k+1)}-1}.$$

Therefore,

$$D \le q^{-\frac{k}{2(k+1)}}\left[\left(\frac{1}{1-q^{-2/5}}+\frac{c}{k}\right)+\tfrac{c}{2}k!q^{-1/6}(1+\ln q)(1+q^{-1/2})+(k+1)q^{-1}\right]\epsilon^{-1},$$

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 $K=\lfloor c^{-1/2}q^{1/4}\rfloor$. Then $K\ge 2$. We have

$$1+\ln K \le 1-\tfrac{1}{2}\ln c+\tfrac{1}{4}\ln q < \tfrac{1}{4}(5+\ln q),$$

so that

$$\begin{aligned}D &\le c^{1/2}q^{-1/4}+\frac{1}{1-3q^{-1}}c^{1/2}q^{-1/4}+c\tfrac{1+q^{-1/2}}{1-3q^{-1}}\delta\tfrac{1}{4}(5+\ln q)A_1^{-1}+4cq^{-3/2}\\ &\le \left[\left(1+\frac{1}{1-3q^{-1}}\right)c^{1/2}+4cq^{-5/4}\right]q^{-1/4}+\tfrac{c}{4}\delta A_1^{-1}(5+\ln q)(1+2q^{-1/2}),\end{aligned}$$

which implies (1.7).

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

$$\begin{aligned}D &\le \frac{1}{K+1}+c\sum_{n=1}^{K}n^{-1}\left\{\left[n^{k+\frac{1}{2}}+(R_{p,n}^{k+1,k+1})^{1/2}q^{1/4}(1+q^{-1/2})^{1/2}\right]A_1^{-1/2}q^{\frac{1}{4}-\frac{k}{2}}+(k+1)q^{-1-\frac{n}{2}}\right\}\epsilon^{-1}\\ &\le \frac{1}{K+1}+\epsilon^{-1}\frac{c}{k+\frac{1}{2}}[(K+1)^{k+\frac{1}{2}}-1]A_1^{-1/2}q^{\frac{1}{4}-\frac{k}{2}}\\ &\quad+\epsilon^{-1}c(1+q^{-1/2})^{1/2}\left\{1+R''^{1/2}[\ln(K+\tfrac{1}{2})-\ln\tfrac{3}{2}-\tfrac{1}{7}]+\tfrac{1}{7}(R_{2,7}^{k+1,k+1})^{1/2}\right\}A_1^{-1/2}q^{(1-k)/2}\\ &\quad+\epsilon^{-1}\tfrac{c}{(1-q^{-1/2})}(k+1)q^{-3/2},\end{aligned}$$

where $R''=\max_n R_{p,n}^{k+1,k+1}=(2k+1)!!$, the maximum running over all $n\ge 2$ such that $(p,n)\ne(2,7)$, and we used the fact that $R_{p,1}^{k+1,k+1}=1$ for $n=1$. For $k\ge 2$, we have $R_{2,7}^{k+1,k+1}\le 12\cdot 7^{2k-3}$ by (2.4). To show (1.6), we may assume

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

This implies $q^{11/14}\ge A_1^{\frac{1}{2k+3}}q^{\frac{2k-1}{2(2k+3)}+\frac{2}{7}}>2(7+\sqrt{15}\ln q)$, so that $q>150$. Let $K=\lfloor A_1^{\frac{1}{2k+3}}q^{\frac{2k-1}{2(2k+3)}}\rfloor-1$. Then $K+2>A_1^{\frac{1}{2k+3}}q^{\frac{2k-1}{2(2k+3)}}\ge q^{\frac{2k-1}{2(2k+3)}}\ge q^{3/14}>2$. We have

$$\frac{1}{K+1}=\frac{K+2}{K+1}\frac{1}{K+2}\le\frac{1}{1-(K+2)^{-1}}A_1^{-\frac{1}{2k+3}}q^{-\frac{2k-1}{2(2k+3)}},$$
$$(K+1)^{k+\frac{1}{2}}A_1^{-1/2}q^{\frac{1}{4}-\frac{k}{2}}\le A_1^{-\frac{1}{2k+3}}q^{-\frac{2k-1}{2(2k+3)}}.$$

For the error terms, we have

$$1+R''^{1/2}[\ln(K+\tfrac{1}{2})-\ln\tfrac{3}{2}-\tfrac{1}{7}]\le\tfrac{1}{2}(2k+1)!!^{1/2}\ln q,$$
$$A_1^{-1/2}q^{(1-k)/2}\le A_1^{-\frac{1}{2k+3}}q^{-\frac{2k-1}{2(2k+3)}-\frac{2}{7}},$$
$$q^{-3/2}<q^{-\frac{2k+1}{2(2k+3)}-1}\le A_1^{-\frac{1}{2k+3}}q^{-\frac{2k-1}{2(2k+3)}-1}.$$

Therefore,

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

which implies (1.6). For $k = 1$, we have $R'' = 3$ and $R_{2,7}^{2,2} = 4$ (Remark 2.4). For $A_1 \ge q^{3/4}$, to show (1.8), we may assume $2A_1^{-\frac{1}{5}} q^{-\frac{1}{10}-\frac{1}{8}} \ln q < 1$. This implies $q^{17/40} \ge A_1^{\frac{1}{5}} q^{\frac{1}{10}+\frac{1}{8}} > 2 \ln q$, so that $q > 300$. Let $K = \lfloor A_1^{1/5} q^{1/10} \rfloor - 1$. Then $K + 2 > A_1^{1/5} q^{1/10} \ge q^{1/4} > 4$. We have

$$\begin{aligned} D &\le \frac{K+2}{K+1} \frac{1}{K+2} + \frac{1}{1-3q^{-1}} \cdot \frac{2}{3} c (K+1)^{3/2} A_1^{-1/2} q^{-1/4} \\ &\quad + \left\{ 1 + \sqrt{3} [\ln(K + \tfrac{1}{2}) - \ln \tfrac{3}{2} - \tfrac{1}{7}] + \tfrac{2}{7} \right\} A_1^{-1/2} + 2q^{-3/2} \\ &\le A_1^{-1/5} q^{-1/10} \left[\left(\frac{1}{1-q^{-1/4}} + \frac{1}{1-3q^{-1}} \cdot \frac{2}{3} c \right) + \tfrac{3}{10} \sqrt{3} q^{-1/8} (1 + \ln q) + 2q^{-6/5} \right], \end{aligned}$$

which implies (1.8). □

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

$$f_0(x,y) = \max \left\{ 0, \min\{ \tfrac{1}{2}x + \tfrac{1}{2}y - \tfrac{1}{2}, \tfrac{1}{3}x - \tfrac{1}{6} \}, \min\{ \tfrac{1}{2}x + \tfrac{1}{4}y - \tfrac{1}{2}, \tfrac{2}{7}x + \tfrac{1}{7}y - \tfrac{3}{14} \} \right\}.$$

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

$$f(x,y) = \max\{ f_0(x,y), f_0(y,x) \}.$$

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

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

$$g_k(x) = \max \left\{ \tfrac{k}{2(k+1)}, \tfrac{1}{2k+3} x + \tfrac{2k-1}{2(2k+3)} \right\}.$$

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

$$h(x) = \begin{cases} \min\{x, \frac{1}{4}\} & x \le \frac{3}{4}, \\ \frac{1}{5}x + \frac{1}{10} & x \ge \frac{3}{4}. \end{cases}$$

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

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

$$D_k \ge \left(\frac{2}{\pi^2} \sum_{n=1}^{\infty} \frac{|M_k^{(n)}|^2}{N^2 n^2} \right)^{1/2}.$$

For $k \geq 3$, we have $R^{k,1}_{p,k-1} \geq k-1$ for $n = k-1$. Thus, by Theorem 3.5, we have

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

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

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

For $k = p = 2$, we have $R^{2,1}_{2,3} = 1$ 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

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

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

[1] P. Deligne, *Application de la formule des traces aux sommes trigonométriques*, Cohomologie étale, Lecture Notes in Mathematics, vol. 569, Springer-Verlag, Berlin, 1977. Séminaire de Géométrie Algébrique du Bois-Marie SGA $4\frac{1}{2}$, pp. 168–232. ↑5, 6

[2] ______, *La conjecture de Weil. II*, Inst. Hautes Études Sci. Publ. Math. **52** (1980), 137–252 (French). MR601520 (83c:14017) ↑6

[3] P. Erdös and P. Turán, *On a problem in the theory of uniform distribution. I, II*, Nederl. Akad. Wetensch., Proc. **51** (1948), 1146–1154, 1262–1269 = Indagationes Math. **10**, 370–378, 406–413. MR0027895 (10,372c), MR0027896 (10,372d) ↑13

[4] A. Grothendieck, *Formule d'Euler-Poincaré en cohomologie étale*, Cohomologie l-adique et fonctions L, Lecture Notes in Mathematics, vol. 589, Springer-Verlag, Berlin, 1977. Séminaire de Géometrie Algébrique du Bois-Marie 1965–1966 (SGA 5), pp. 372–406. Exposé X, rédigé par I. Bucur. ↑6

[5] N. M. Katz, *Gauss sums, Kloosterman sums, and monodromy groups*, Annals of Mathematics Studies, vol. 116, Princeton University Press, Princeton, NJ, 1988. MR955052 (91a:11028) ↑5, 6

[6] N. M. Katz and Z. Zheng, *On the uniform distribution of Gauss sums and Jacobi sums*, Analytic number theory, Vol. 2 (Allerton Park, IL, 1995), Progr. Math., vol. 139, Birkhäuser Boston, Boston, MA, 1996, pp. 537–558. MR1409377 (97e:11089) ↑2, 4, 6, 9

[7] R. C. King, *Modification rules and products of irreducible representations of the unitary, orthogonal, and symplectic groups*, J. Mathematical Phys. **12** (1971), 1588–1598. MR0287816 (44 #5019) ↑7

[8] P. Littelmann, *A generalization of the Littlewood-Richardson rule*, J. Algebra **130** (1990), no. 2, 328–368, DOI 10.1016/0021-8693(90)90086-4. MR1051307 (91f:22023) ↑7

[9] J. Rivat and G. Tenenbaum, *Constantes d'Erdős-Turán*, Ramanujan J. **9** (2005), no. 1-2, 111–121, DOI 10.1007/s11139-005-0829-1 (French, with English and French summaries). MR2166382 (2006g:11158) ↑13

[10] G. W. Schwarz, *Invariant theory of G_2 and* Spin_7, Comment. Math. Helv. **63** (1988), no. 4, 624–663, DOI 10.1007/BF02566782. MR966953 (89k:14080) ↑8

[11] I. E. Shparlinski, *On the distribution of arguments of Gauss sums*, Kodai Math. J. **32** (2009), no. 1, 172–177, DOI 10.2996/kmj/1238594554. MR2518562 (2010b:11104) ↑2, 9

[12] F. E. Su, *A LeVeque-type lower bound for discrepancy*, Monte Carlo and quasi-Monte Carlo methods 1998 (Claremont, CA), Springer, Berlin, 2000, pp. 448–458. MR1849870 (2002f:11098) ↑16

[13] H. Weyl, *The classical groups*, Princeton Landmarks in Mathematics, Princeton University Press, Princeton, NJ, 1997. Their invariants and representations; Fifteenth printing; Princeton Paperbacks. MR1488158 (98k:01049) ↑7