Math. Res. Lett. **18** (2011), *no.* 01, 155–174

THE DISTRIBUTION OF VALUES OF SHORT HYBRID EXPONENTIAL SUMS ON CURVES OVER FINITE FIELDS

Kit-Ho Mak and Alexandru Zaharescu

Abstract. Let p be a prime number, X be an absolutely irreducible affine plane curve over $\mathbb{F}_p$, and $g, f \in \mathbb{F}_p(x, y)$. We study the distribution of the values of the hybrid exponential sums

$$S_n = \sum_{\substack{P_i \in X, n < x(P_i) \leq n+H \\ y(P_i) \in \mathcal{J}}} \chi(g(P_i))\psi(f(P_i))$$

on $n \in \mathcal{I}$ for some short interval $\mathcal{I}$. We show that under some natural conditions the limiting distribution of the projections of the sum S_n, $n \in \mathcal{I}$ on any straight line through the origin is Gaussian as p tends to infinity.

1. Introduction

Many sequences that arise in number theory have Gaussian distribution. A well-known family of sequences with Gaussian distribution can be obtained by Erdös-Kac type results [4] (see also [9] for a more complete and recent account). For example, the number of distinct prime factors of an integer n [4], of $\phi(n)$ [6], of the sum $a+b$ when a and b are given in some dense set [5], of the number of points on an elliptic curve [11], of the characteristic polynomial of the Frobenius acting on Drinfeld modules [10], and of polynomials of several variables [16] are all with Gaussian distribution. Another example that falls into this type is the 2-rank of the Selmer groups of certain 2-isogenies of some families of elliptic curves [17, 18]. A well-known unpublished result of Selberg on the distribution of values of Riemann-Zeta function $\zeta(s)$ on the critical line offers another type of Gaussian distribution result. In this paper we will present another family of sequences arising naturally in number theory, which have a Gaussian distribution, but do not fall into the types mentioned above.

In [3], Davenport and Erdös studied the distribution of quadratic residues and non-residues. As a result they proved that the limiting distribution of the values of the incomplete character sum

$$S_n = \sum_{n < x \leq n+H} \chi(x), \tag{1}$$

where χ is the quadratic character modulo a large prime p, is Gaussian after a suitable normalization. More precisely, they showed that the number $N_p(\lambda)$ of integers $n \in$

Received by the editors September 25, 2010.

1991 *Mathematics Subject Classification.* Primary 11G20, 11T23, 11T24.

Key words and phrases. Gaussian distribution, exponential sums.

The second author is supported by NSF grant number DMS - 0901621.

$\{0, \ldots, p-1\}$ for which $S_n \leq \lambda H^{\frac{1}{2}}$ satisfies

$$\lim_{p\to\infty} \frac{N_p(\lambda)}{p} = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\lambda} e^{-\frac{t^2}{2}}\, dt$$

for any fixed λ, if H satisfies the growth conditions

$$H \to \infty, \frac{\log H}{\log p} \to 0$$

as p tends to infinity.

In [2], the result of Davenport and Erdös is generalized to the case of an n-dimensional sum of quadratic characters of the form

$$S_H(x_1, \ldots, x_n) = \sum_{x_1 < z_1 \leq x_1 + H} \cdots \sum_{x_n < z_n \leq x_n + H} \chi(z_1 + \ldots + z_n)\,.$$

In this paper, we will generalize the result of Davenport and Erdös in another direction by regarding the sum S_n in (1) as a special example in a more general class of incomplete hybrid exponential sums over an absolutely irreducible affine plane algebraic curve X over the finite field $\mathbb{F}_p$,

$$S_n = \sum_{\substack{P_i \in X, n < x(P_i) \leq n+H \\ y(P_i) \in \mathcal{J}}} \chi(g(P_i))\psi(f(P_i)). \tag{2}$$

Here χ is a multiplicative character of $\mathbb{F}_p$, ψ is an additive character of $\mathbb{F}_p$, $\mathcal{J}$ an interval, and $g, f \in \mathbb{F}_p(x, y)$ are rational functions. The sum (1) considered in [3] corresponds to the case when χ is the quadratic character, ψ is the trivial character, X the affine line defined by $y = 0$, and $g(x, y) = x$. In this paper, we prove that the limiting distribution of the values of most of these incomplete hybrid exponential sums is also Gaussian.

2. Statements of Main Results

Let p be a large prime, and X be an absolutely irreducible affine plane curve over $\mathbb{F}_p$, given by the equation $P(x, y) = 0$, with $\deg_y(P(x, y)) \geq 1$, where $\deg_y$ denotes the degree in y. Let χ, ψ be a *nontrivial* multiplicative character and a *nontrivial* additive character modulo p respectively, $f, g \in \mathbb{F}_p(x, y)$ be two rational functions.

Let $\mathcal{J} = [\alpha p, \beta p)$ be an interval, where $0 \leq \alpha < \beta \leq 1$. For simplicity, we assume that no two points on X with their y-coordinates in $\mathcal{J}$ have the same x-coordinates. If r denotes the number of $\mathbb{F}_p$-points on X, we let $P_1, \ldots, P_r$ be the points on X with their y-coordinates in $\mathcal{J}$, ordered by their x-coordinates in ascending order. We also let H be an integer such that $1 \leq H \leq p$, and $\mathcal{I} \subseteq [0, p-1]$ an interval. Since $\mathbb{F}_p$-points on an affine curve is uniformly distributed (see for example Meyerson [13], Fujiwara [8], or the authors [12]), we have the following estimation of r,

$$r = (\beta - \alpha)p + O(\sqrt{p}\log^2 p).$$

More generally, the number of points N on X inside the rectangle $(n, n+H] \times \mathcal{J}$ is given by

$$N = (\beta - \alpha)H + O(\sqrt{p}\log^2 p), \tag{3}$$

where $|\mathcal{I}|$ denotes the number of integers in $\mathcal{I}$.

We are interested in the distribution of the values of the hybrid exponential sums (2) for $n \in \mathcal{I}$ as p tends to infinity. It is understood that the poles of f, g are excluded from the sum.

We will show that the projections of S_n on any fixed straight line through the origin are Gaussian. More precisely, fix an angle $\theta \geq 0$ and consider the line L_θ given by the equation $y = x \tan\theta$. Let p, χ, ψ, $\mathcal{I}, \mathcal{J}$, f, g as above, we form the exponential sums S_n as in (2) for $n \in \mathcal{I}$, and study its projection u_n on L_θ, normalized by the asymptotic number of points we sum, namely $((\beta-\alpha)H)^{\frac{1}{2}}$ by (3). i.e.

$$u_n = \frac{S_n e^{-i\theta} + \overline{S_n} e^{i\theta}}{2((\beta-\alpha)H)^{\frac{1}{2}}}, \tag{4}$$

for $n \in \mathcal{I}$, and consider the sequence $\{u_n : n \in \mathcal{I}\}$ on L_θ. We will show that as H and p tends to infinity, the limiting distribution of the u_n is Gaussian. The idea is to calculate the moments

$$M_k = M_k(p, \chi, \psi, f, g, H, \mathcal{I}, \theta) = \sum_{n \in \mathcal{I}} u_n^k \tag{5}$$

for $k \in \mathbb{N}$. Our result is the following.

Theorem 2.1. *Let p, X, χ, ψ, $\mathcal{I}$, $\mathcal{J}$, H be as above. Let $g, f \in \mathbb{F}_p(x,y)$ be two rational functions. Define d_g, d_f to be the degrees of the denominators of g and f respectively. Suppose f is not of the form*

$$h^p - h + \textit{(linear terms)} + Q(x,y)P(x,y)^b$$

for any nonzero integer b, rational functions $h \in \overline{\mathbb{F}}_p(x,y), Q \in \mathbb{F}_p(x,y)$, with Q relatively prime to P, and any constant $C \in \mathbb{F}_p$ (in this paper, all the "linear terms" have coefficients in $\mathbb{F}_p$). Let $f = \frac{f_1}{f_2}$, with $f_1, f_2 \in \mathbb{F}_p[x,y]$, and f_1, f_2 have no common factors, we also assume that

1. *if f is a polynomial, then $\deg f < p$. Write $f(x,y) = r_1(x) + r_2(x,y)$, where r_1 consists of all terms which do not depend on y. We further assume that either*
   - (a) *r_2 is not of the form*
   $$\textit{(linear terms)} + Q(x,y)P(x,y)^b$$
   for any nonzero integer b, rational function Q relatively prime to P, or
   - (b) *if r_2 is of the above form, then $\deg r_1 \geq 3$.*
2. *if $\deg f_2 \geq 1$ (so that f is not a polynomial), then f_2 is not a constant multiple of the p-th power of any polynomial in $\overline{\mathbb{F}}_p[x,y]$.*

Let k be a positive integer, H, k be small compared to p (say $H, k = O(\log p)$). Then if k is odd, we have

$$M_k = O(H^{\frac{k}{2}}(d^{2k} + 2d^k d_g^k + 2d^k d_f^k)\sqrt{p}\log^{2k} p), \tag{6}$$

and if k is even,

$$M_k = \frac{1}{2^k}\binom{k}{k/2}(k/2)!\,|\mathcal{I}|\,(1 + O(k^2/H)) + O(2^{\frac{k}{2}}H^{\frac{k}{2}}(d^{2k} + 2d^k d_g^k + 2d^k d_f^k)\sqrt{p}\log^{2k} p). \tag{7}$$

The main term in (7) is

$$\frac{1}{2^k}\binom{k}{k/2}(k/2)!\,|\mathcal{I}| = 2^{-\frac{k}{2}}\cdot 1\cdot 3\cdot \ldots \cdot (k-1)\cdot |\mathcal{I}|\,.$$

As in Davenport and Erdös [3], we write

$$\mu_k = \begin{cases} 1\cdot 3\cdot \ldots \cdot (k-1), & \text{if } k \text{ is even,} \\ 0, & \text{if } k \text{ is odd.} \end{cases}$$

Then from Theorem 2.1, the next corollary follows immediately.

Corollary 2.2. *Let p, X, χ, ψ, $\mathcal{I}$, $\mathcal{J}$, H, g, f be as above. Suppose that f is not of the form*

$$\textit{(linear terms)} + Q(x,y)P(x,y)^b$$

for nonzero integer b, $Q \in \mathbb{F}_p(x,y)$ relatively prime to $P(x,y)$, and subject to the conditions

(1) *f is not a polynomial, or*
(2) *f is a polynomial, write $f(x,y) = r_1(x) + r_2(x,y)$, where r_1 consists of all terms which do not depend on y. We assume that either*
   (a) *r_2 is not of the form*

$$\textit{(linear terms)} + Q(x,y)P(x,y)^b$$

   for any nonzero integer b, rational function Q relatively prime to P, or
   (b) *if r_2 is of that form, then* $\deg r_1 \geq 3$.

Suppose in addition that H is any function of p that tends to infinity with p subjected to the following conditions:

$$1 \leq H \leq p,$$
$$\lim_{p\to\infty}\frac{\log H}{\log p} = \lim_{p\to\infty}\frac{\log d}{\log p} = \lim_{p\to\infty}\frac{\log d_g}{\log p} = \lim_{p\to\infty}\frac{\log d_f}{\log p} = 0,$$
$$\liminf_{p\to\infty}\frac{\log|\mathcal{I}|}{\log p} > \frac{1}{2}.$$

Then we have

$$\lim_{p\to\infty}\frac{2^{k/2}M_k}{|\mathcal{I}|} = \mu_k.$$

From this asymptotic behaviour of the moments, one can deduce that the distribution of our sums S_n tends to the Gaussian distribution on L_θ as p tends to infinity. We will give the argument in Section 6.

Corollary 2.3. *Suppose that the hypotheses of Corollary 2.2 are satisfied. Then for any $\lambda \geq 0$, the number $G_p(\lambda)$ of integers $n \in \mathcal{I}$ with $u_n \leq \lambda$ satisfies*

$$\lim_{p\to\infty}\frac{G_p(\lambda)}{|\mathcal{I}|} = \frac{1}{\sqrt{\pi}}\int_{-\infty}^{\lambda} e^{-t^2}\,dt.$$

Several remarks about the distribution of the sum S_n are in order.

Remark 2.4. If $\mathcal{J}$ is not chosen so that we have a one-to-one correspondence of x and y-coordinates on a curve, we may still have Gaussian distribution for the S_n. For example, if X is a hyperelliptic curve, and we choose $\mathcal{J}$ to be the whole interval $[0, p)$, then generically one x-coordinate on the curve corresponds to two y-coordinates. From Corollary 2.3, we have Gaussian distribution for $\mathcal{J}_1 = [0, p/2)$, and also for $\mathcal{J}_2 = [-p/2, 0)$. After combining the two of them we will have Gaussian distribution for the whole interval $\mathcal{J} = [-p/2, p/2)$.

Remark 2.5. Corollary 2.3 is in some sense best possible with respect to the range of $|\mathcal{I}|$, and f has to be non-linear. This is illustrated in the following examples.

Example 2.6. Let X be the diagonal defined by $x = y$, χ the quadratic character and $\psi(x) = e_p(x)$, where $e_p(x) = e^{2\pi i x/p}$. Let $g(x, y) = x, f(x, y) = xy$. All the assumptions on χ, ψ, g, f are satisfied, so we can conclude from Corollary 2.3 the Gaussian distribution of the hybrid exponential sum if $|\mathcal{I}| > p^{\frac{1}{2}}$. However, if we let $\mathcal{I} = \{1, \dots, N\}$, with $N \sim p^{\frac{1}{2}-\varepsilon}$ and $H < p^{\frac{1}{2}-\varepsilon}$, then if p is large enough, $e_p(xy) \sim 1$. Since $\chi(x)$ is real, the sum S_n will be close to a real number for any $n \in \mathcal{I}$. Thus their projections to the imaginary axis will not have Gaussian distribution.

Example 2.7. On the other hand, if X, χ, ψ is as above, and let $g(x, y) = x$, and $f(x, y) = x + y$ is linear. Let $\mathcal{I} = \{1, \dots, N\}$ with $N, H = o(p)$ but $N > p^{\frac{1}{2}}$. Then again $e_p(x + y) \sim 1$ for large p, and by the same reason as in the above paragraph, the projections of S_n to the imaginary axis will not have Gaussian distribution.

Note that our assumptions of χ and ψ being non-trivial exclude us from considering sums like (1) appeared in [3]. Our next goal is to extend our results to the cases when one of the characters χ or ψ is trivial. For trivial χ we have the following.

Theorem 2.8. *Theorem 2.1, Corollary 2.2 and Corollary 2.3 remains true if χ is trivial but all other conditions are still assumed.*

The case for trivial ψ is more difficult, but we still obtain a Gaussian distribution if we impose the necessary assumption that $g(x, y)$ is not a complete a-th power to ensure that the exponential sum is nontrivial.

Theorem 2.9. *Let p, X, χ, $\mathcal{I}$, $\mathcal{J}$, H be as in Theorem 2.1 and Corollary 2.2, and let ψ be trivial. Let a be the order of χ. Assume $g(x, y)$ is not of the form*

$$h^a + Q(x, y)P(x, y)^b$$

for any nonzero integer b, $Q \in \mathbb{F}_p(x, y)$ relatively prime to P, $h \in \overline{\mathbb{F}}_p(x, y)$, and $\deg(g)$ is small compared to p. Let k, H be positive integers which are small compared to p. Then we have the following.

(1) *If $a = 2$, and $\theta = 0$ (that is we only consider the distribution on the real line), we have*

$$M_k = O(H^{\frac{k}{2}}(d^{2k} + 2d^k d_g^k + 2d^k d_f^k)\sqrt{p}\log^{2k} p) \tag{8}$$

when k is odd, and

$$M_k = \frac{k!}{2^{\frac{k}{2}}\left(\frac{k}{2}\right)!}|\mathcal{I}|\left(1 + O(k^2/H)\right) + O(2^{\frac{k}{2}}H^k(d^{2k} - 2d^k d_g^{\frac{k}{2}} + 2d^k d_f^k)\sqrt{p}(2\log p + 1)^k) \tag{9}$$

when k is even.

(2) *If $a > 2$ is even, we have*

$$M_k = O(H^{\frac{k}{2}}(d^{2k} + 2d^k d_g^k + 2d^k d_f^k)\sqrt{p}\log^{2k} p) \tag{10}$$

when k is odd, and

$$M_k = \frac{1}{2^k}\frac{k!}{(k/2)!}|\mathcal{I}|\,(1 + O(k^{\frac{a}{2}+2}/H)) + O(H^{\frac{3k}{2}}(d^{4k} - 2d^{2k}d_g^k + 2d^{2k}d_f^{2k})\sqrt{p}\log^{2k} p) \tag{11}$$

when k is even.

(3) *If a is odd (necessarily $a > 1$ since χ is nontrivial), we have*

$$M_k = \frac{1}{2^k((\beta-\alpha)H)^{\frac{a}{2}-1}}\frac{k!}{(\frac{k}{2}+\frac{a}{2})!}(2\cos a\theta)\,|\mathcal{I}|\,(1 + O(k^{a+2}/H)) + O((H^{\frac{3k}{2}}(d^{4k} - 2d^{2k}d_g^k + 2d^{2k}d_f^{2k})\sqrt{p}\log^{2k} p). \tag{12}$$

when k is odd, and

$$M_k = \frac{1}{2^k}\frac{k!}{(k/2)!}|\mathcal{I}|\,(1 + O(k^{\frac{a}{2}+2}/H)) + O(H^{\frac{3k}{2}}(d^{4k} - 2d^{2k}d_g^k + 2d^{2k}d_f^{2k})\sqrt{p}\log^{2k} p) \tag{13}$$

when k is even.

The analogue to Corollary 2.2 for trivial ψ is the following.

Corollary 2.10. *Let*

$$\mu_k = \begin{cases} 1\cdot 3\cdot \ldots \cdot (k-1), & \text{if } k \text{ is even,} \\ 0, & \text{if } k \text{ is odd.} \end{cases}$$

If ψ is trivial, and keeping the other assumptions in Theorem 2.9 and Corollary 2.2, then if we take the limit as p tends to infinity with χ being a series of quadratic characters modulo p, and we only consider the moments on the real line, then

$$\lim_{p\to\infty}\frac{M_k}{|\mathcal{I}|} = \mu_k.$$

If on the other hand, we take the limit with χ being restricted to characters of order $a > 2$, then the same conclusion as in Corollary 2.2 holds. That is,

$$\lim_{p\to\infty}\frac{2^{k/2}M_k}{|\mathcal{I}|} = \mu_k.$$

Finally, we get the analogue to Corollary 2.3, which shows that we still have Gaussian distribution when ψ is trivial.

Corollary 2.11. *Assumptions as in Corollary 2.10. For any $\lambda \geq 0$, let $G_p(\lambda)$ be the number of integers $n \in \mathcal{I}$ with $u_n \leq \lambda$. If p tends to infinity, with χ a quadratic character modulo p and we only consider the distribution on the real line, then*

$$\lim_{p\to\infty}\frac{G_p(\lambda)}{|\mathcal{I}|} = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{\lambda} e^{-\frac{t^2}{2}}\,dt.$$

On the other hand, if we restrict the χ to be characters of order $a > 2$, then the same conclusion as Corollary 2.3 holds. That is,

$$\lim_{p\to\infty} \frac{G_p(\lambda)}{|\mathcal{I}|} = \frac{1}{\sqrt{\pi}} \int_{-\infty}^{\lambda} e^{-t^2}\, dt.$$

Therefore, we have Gaussian distributions in all the above cases, but when we take the limit through a series of quadratic character modulo p, we get a Gaussian distribution with different parameters compared to all other cases.

Remark 2.12. If the order of χ is $a = 2$, then we only have Gaussian distribution on the real line, but not when S_n is projected to other lines. The reason is simple: since χ is quadratic, our S_n is real for any n in this case, and we certainly do not have Gaussian distribution if we project S_n to the imaginary axis.

Remark 2.13. Although we get the same results for odd and even a, we note that when a is odd, our estimation shows that we just barely obtain the Gaussian distribution. In fact, the main term (12) for the case a and k both odd is of order $|\mathcal{I}|/H$, which just barely tends to zero after dividing by $|\mathcal{I}|$, thanks to the assumption that H tends to infinity with p.

Remark 2.14. We can get back the result from Davenport-Erdös [3] if we take X to be the straight line $y = 0$, χ being the quadratic character modulo p, ψ trivial, and $g(x) = x$. Note that this is exactly the case when we get different parameters for the Gaussian distribution.

3. Some preliminaries

To prove Theorem 2.1, the first thing we need is an estimation for the incomplete hybrid exponential sums over an affine space curve $Y \subseteq \mathbb{A}^m$, which need not be irreducible nor reduced. The sum is defined as follows.

$$S_{\mathcal{J}_1,\dots,\mathcal{J}_m} = \sum_{\mathbf{x}\in Y\cap(\mathcal{J}_1\times\dots\times\mathcal{J}_m)} \chi(\tilde{g}(\mathbf{x}))\psi(\tilde{f}(\mathbf{x})),$$

where $\mathbf{x} = (x_1, \dots, x_m)$ and $\mathcal{J}_i \subseteq [0, p-1]$ are intervals, $\tilde{g}, \tilde{f} \in \mathbb{F}_p(x_1, \dots, x_m)$ are rational functions, and ψ is a nontrivial character.

Lemma 3.1. *Let p be a large prime, D be the degree of Y, $d_{\tilde{g}}, d_{\tilde{f}}$ the degrees of the denominators of $\tilde{g}, \tilde{f}$ respectively. Let a be the order of χ. Unless there are rational functions $\tilde{g}_1, \tilde{f}_1 \in \overline{\mathbb{F}}_p(x_1, \dots, x_m)$ such that $\tilde{g} - {\tilde{g}_1}^a$ vanishes identically and $\tilde{f} - {\tilde{f}_1}^p + \tilde{f}_1$ is linear on some irreducible component of Y simultaneously, we have*

$$|S_{\mathcal{J}_1,\dots,\mathcal{J}_m}| \le ((D^2 - 3D + 2Dd_{\tilde{g}} + 2Dd_{\tilde{f}})\sqrt{p} + D^2 + O(D))(2\log p + 1)^m.$$

Proof. The work of Perel'muter [14] deals with the case when $S_{\mathcal{J}_1,\dots,\mathcal{J}_m}$ is complete, i.e. if all $\mathcal{J}_i = [0, p-1]$. He showed that unless $\tilde{g} - {\tilde{g}_1}^a$ and $\tilde{f} - f_1^p + f_1$ vanishes identically on some irreducible component of Y simultaneously, the complete sum satisfies

$$\left|S_{[0,p-1]^m}\right| \le (D^2 - 3D + 2Dd_{\tilde{g}} + 2Dd_{\tilde{f}})\sqrt{p} + D^2 + O(D). \tag{14}$$

His work uses the idea of Bombieri-Weil type estimate of an exponential sum along an algebraic curve [1, 15]. Note that compared to [14] we have an extra $O(D)$ term

because we are considering an affine curve, thereby missing at most $O(D)$ terms in the sum, each of those having absolute value at most 1.

We then express our incomplete sum $S_{\mathcal{J}_1,\ldots,\mathcal{J}_m}$ in terms of complete sums of the same type. Recall the orthogonal relation

$$\frac{1}{p}\sum_{t \bmod p} \psi(ty) = \begin{cases} 1, & \text{if } y = 0, \\ 0, & \text{otherwise,} \end{cases} \tag{15}$$

we see that

$$\begin{aligned} S_{\mathcal{J}_1,\ldots,\mathcal{J}_m} &= \sum_{\mathbf{x}\in Y} \chi(\tilde{g}(\mathbf{x}))\psi(\tilde{f}(\mathbf{x})) \prod_{i=1}^{m} \left(\sum_{m_i\in\mathcal{J}_i} \frac{1}{p} \sum_{t_i \bmod p} \psi(t_i(m_i - x_i)) \right) \\ &= \frac{1}{p^m} \prod_{i=1}^{m} \sum_{t_i \bmod p} \left(\sum_{m_i\in\mathcal{J}_i} \psi(t_i m_i) \right) \\ &\quad \times \sum_{\mathbf{x}\in Y} \chi(\tilde{g}(\mathbf{x}))\psi(\tilde{f}(\mathbf{x}) - t_1x_1 - \ldots - t_mx_m). \end{aligned} \tag{16}$$

From the assumption in our lemma, we see that the inner sum satisfies the assumption in [14], and so can be estimated by (14). To estimate the outer sum, first we need the estimation

$$\left| \sum_{t \bmod p} \left(\sum_{m\in\mathcal{J}} \psi(tm) \right) \right| \le 2p\log p + |\mathcal{J}|\,. \tag{17}$$

To see this, note that any nontrivial additive character ψ modulo p is of the form $\psi(x) = e_p(kx) = e^{2\pi ikx/p}$ $(x \in \mathbb{F}_p)$ for some k with $(k,p) = 1$. Let $\mathcal{J} \cap \mathbb{Z} = \{l, l+1, \ldots, l+h-1\}$, where $h = |\mathcal{J}|$, then

$$\sum_{m\in\mathcal{J}} \psi(tm) = \sum_{m\in\mathcal{J}} e_p(ktm) = \begin{cases} h & \text{if } t = 0, \\ \left(e^{\frac{-2\pi itkl}{p}}\right) \frac{1-e^{-2\pi itkh/p}}{1-e^{-2\pi itk/p}} & \text{if } t \neq 0. \end{cases}$$

Hence if $t \neq 0$,

$$\left| \sum_{m\in\mathcal{J}} \psi(tm) \right| \le \frac{2}{\left|1 - e^{-2\pi itk/p}\right|}.$$

If $\|\cdot\|$ denotes the distance to the nearest integer, then

$$\left|1 - e^{-2\pi itk/p}\right| = 2\left|\sin\left(\pi tk/p\right)\right| \ge \left\| \frac{kt}{p} \right\|$$

for p large enough. We obtain the estimate

$$\left| \sum_{m\in\mathcal{J}} \psi(tm) \right| \le 2\left(\left\| \frac{kt}{p} \right\| \right)^{-1}.$$

We then sum the above over all t modulo p. We choose the set of representatives with $0 \le |t| \le (p-1)/2$, noting that for $t \neq 0$, $(k,p) = 1$, $\left\| \frac{kt}{p} \right\|$ is a reordering of $\left\| \frac{t}{p} \right\|$,

but in our set of representatives, $\left\|\frac{t}{p}\right\| = \frac{|t|}{p}$. Now (17) follows from the elementary inequality

$$1 + \frac{1}{2} + \cdots + \frac{1}{\frac{p-1}{2}} \leq \log p.$$

Finally, putting (14) and (17) into (16), we get

$$\begin{aligned} |S_{\mathcal{J}_1,\ldots,\mathcal{J}_m}| &\leq \frac{1}{p^m}\prod_{i=1}^{m}(2p\log p + |\mathcal{J}_i|)((D^2 - 3D + 2Dd_{\tilde{g}} + 2Dd_{\tilde{f}})\sqrt{p} + D^2 + O(D)) \\ &\leq ((D^2 - 3D + 2Dd_{\tilde{g}} + 2Dd_{\tilde{f}})\sqrt{p} + D^2 + O(D))(2\log p + 1)^m. \end{aligned}$$

□

Remark 3.2. If we assume that $\tilde{g} - \tilde{g_1}^a$ is not identically zero on X, then the above lemma still hold even when ψ is the trivial character. In fact, the same proof hold by using any arbitrarily chosen nontrivial ψ for (15). This remark will be useful when we prove Theorem 2.9 for sums with trivial ψ.

Remark 3.3. If $\tilde{g} - \tilde{g_1}^a$ vanishes identically and $\tilde{f} - \tilde{f_1}^p + \tilde{f_1}$ is linear on some irreducible component of Y simultaneously, the resulting hybrid sum may be large in some interval $\mathcal{J}_i$.

For example, let Y be the elliptic curve defined by the equation $y^2 - x^3 - ax - b = 0$, $\mathcal{J} = [0, p/2)$ and χ the quadratic character of $\mathbb{F}_p$. Suppose now $g(x,y) = x^2$ and $f(x,y) = x^p - x$, so that $\chi(g(x,y)) = 1$ and $\psi(f(x,y)) = 1$ for any $\mathbb{F}_p$-point (x,y). Then each term in the hybrid sum is 1, and hence if $|\mathcal{I}| > p^{\frac{1}{2}}$, we will have

$$S_{\mathcal{I},\mathcal{J}} = \frac{1}{2}|\mathcal{I}| + O(\sqrt{p}),$$

which is much bigger than the bound suggested in Lemma 3.1 when p is large.

The following strange looking lemma prove that certain rational functions are not of the form disallowed by Lemma 3.1. This will be of vital importance for our later calculations.

Lemma 3.4. *Let p be a large prime, $f \in \mathbb{F}_p(x,y)$ be a rational function in two variables, $f = f_1/f_2$, $f_1, f_2 \in \mathbb{F}_p[x,y]$, f_1, f_2 has no common factors. Suppose that $f \neq h^p - h +$ (linear terms) for any rational function $h \in \overline{\mathbb{F}}_p(x,y)$, and subject to the following conditions:*

1. *If f is a polynomial, then* $\deg f < p$. *Write $f(x,y) = r_1(x) + r_2(x,y)$, where r_1 consists of all terms which do not depend on y. We further assume that either r_2 is not linear, or if r_2 is linear, then* $\deg r_1 \geq 3$.
2. *If* $\deg f_2 \geq 1$ *(so that f is not a polynomial), then f_2 is not a constant multiple of the p-th power of any polynomial in $\mathbb{F}_p[x,y]$.*

Let H, j_1, j_2 be positive integers so that both H and $j_1 + j_2$ are small compared to p. Let $1 \leq h_1, \ldots, h_{j_1+j_2} \leq H$ be integers, which may or may not be distinct. Let $y_1, \ldots, y_{j_1+j_2}$ be indeterminates, which again may or may not be the same. Suppose that y_i, y_j stand for the same indeterminate if and only if $h_i = h_j$. Define

$$F(x, y_1, \ldots, y_{j_1+j_2}) = \sum_{j=1}^{j_1} f(x + h_j, y_j) - \sum_{j=j_1+1}^{j_1+j_2} f(x + h_j, y_j).$$

If $F = \tilde{h}^p - \tilde{h} +$ (linear terms) for some rational function $\tilde{h} \in \overline{\mathbb{F}}_p(x, y_1, \ldots, y_{j_1+j_2})$, then we have $j_1 = j_2$ and $F(x, y_1, \ldots, y_{j_1+j_2})$ is the zero polynomial.

Proof. First we collect the terms in F that coincide (i.e. with equal h_j's) and reordering the y_j's if necessary, we get

$$F = m_1 f(x + u_1, y_1) + \ldots + m_r f(x + u_r, y_r), \tag{18}$$

where $m_1, \ldots, m_r \in \mathbb{Z}$, $u_1, \ldots, u_r \in \mathbb{F}_p$ are distinct, $1 \leq u_i \leq H$, and $y_1, \ldots, y_r$ are distinct indeterminate. It suffices to show that $m_1, \ldots, m_r$ are all zero.

Suppose not all the m_j's are zero, then by removing the m_j's that are zero, we may assume that $m_j \neq 0$ for any j in (18). By assumption, $F = \tilde{h}^p - \tilde{h} +$ (linear terms) for some rational function $\tilde{h}$.

First, if f is a polynomial, then F and hence h are polynomials. From (18) and the assumption that $\deg f < p$, we see that $\deg F < p$. However, if $\tilde{h}$ is non-constant, then $F = \tilde{h}^p - \tilde{h} +$ (linear terms) has degree greater than or equal to p, which is impossible. So $\tilde{h}$ is a constant, and so $F -$ (linear terms) $= \tilde{h}^p - \tilde{h} \in \mathbb{F}_p$. This implies F is linear. We claim that this is also impossible unless F is zero.

To prove the claim, we let $f(x, y) = r_1(x) + r_2(x, y)$, where r_1 consists of all the terms that do not depend on y. From (18), we see that

$$F = (m_1 r_1(x + u_1) + \ldots + m_r r_1(x + u_r)) + (m_1 r_2(x, y_1) + \ldots + m_r r_2(x + u_r, y_r))$$

is linear. This clearly implies that

$$\begin{aligned} R_1(x) &= m_1 r_1(x + u_1) + \ldots + m_r r_1(x + u_r), \\ R_2(x, y_1, \ldots, y_r) &= m_1 r_2(x, y_1) + \ldots + m_r r_2(x + u_r, y_r) \end{aligned}$$

are both linear. From the expression for R_2 it is immediate that r_2 is linear, and the conditions that $H, j_1 + j_2$ is small compared to p and $\deg f < p$ ensure that $\deg r_1 \leq 2$ (or otherwise the coefficient of $x^{\deg r_1 - 1}$ in $R_1(x)$ does not vanish and so it cannot be linear). This contradicts to our assumption imposed on r_1 and r_2.

On the other hand, if $\deg f_2 \geq 1$, then let $F = F_1/F_2, \tilde{h} = h_1/h_2$ be in lowest form (the numerator has no common factors with the denominator). It is easy to see that $\deg h_2 \geq 1$. By clearing the denominator in (18) and compare with $F = h^p - h +$ (linear terms), we get

$$\frac{F_1}{f_2(x + u_1, y_1) \ldots f_2(x + u_r, y_r)} = \frac{h_1^p - h_1 h_2^{p-1} - h_2^p(\text{linear terms})}{h_2^p}.$$

Both sides are clearly in its lowest form. Hence $f_2(x + u_1, y_1) \ldots f_2(x + u_r, y_r) = h_2^p$, which implies each of the $f_2(x + u_j, y_j)$ is a constant multiple of a complete p-th power (here the fact that $j_1 + j_2$ is small compared to p is critical, so that the factors of f_2 that involves only x cannot stack together and become a p-th power if they are not originally a p-th power). This is a contradiction to our assumption when $\deg f_2 \geq 1$. □

4. Computation of the moments M_k

Recall that S_n is defined by (2), u_n by (4) and the moments M_k by (5). Our calculation of M_k starts with

$$M_k = \frac{1}{2^k((\beta-\alpha)H)^{\frac{k}{2}}} \sum_{n\in\mathcal{I}} \sum_{j=0}^{k} \binom{k}{j} e^{-ji\theta+(k-j)i\theta} S_n^j \overline{S_n}^{k-j} \tag{19}$$

$$= \frac{1}{2^k((\beta-\alpha)H)^{\frac{k}{2}}} \sum_{j=0}^{k} \binom{k}{j} e^{(k-2j)i\theta} S(j,k-j),$$

where

$$S(j_1,j_2) = \sum_{n\in\mathcal{I}} S_n^{j_1} \overline{S_n}^{j_2}. \tag{20}$$

The diagonal sum $S(j,j)$ behave differently from the non-diagonal ones, and we treat them separately.

4.1. The sum $S(j,j)$.

For $j \geq 0$ we have

$$S(j,j) = \sum_{n\in\mathcal{I}} |S_n|^{2j},$$

and clearly $S(0,0) = |\mathcal{I}| + O(1)$. An estimate for $S(j,j)$ when j is positive is given by the following lemma.

Lemma 4.1. *Let p be a large prime, and X be an irreducible affine plane curve of degree $d > 1$ over $\mathbb{F}_p$ defined by the equation $P(x,y) = 0$, χ, ψ be a nontrivial multiplicative character and a nontrivial additive character modulo p respectively, $f, g \in \mathbb{F}_p(x,y)$ be two rational functions. Define d_g, d_f be the degree of the denominator of g and f respectively. Suppose f satisfies the same conditions as in Theorem 2.1.*

Let $\mathcal{I} \subseteq [0, p-1]$ an interval and $\mathcal{J} = [\alpha p, \beta p)$ an interval, where $0 \leq \alpha < \beta \leq 1$, such that no two points on X with their y-coordinates in $\mathcal{J}$ have the same x-coordinates. Let H, j be small compared to p, then we have

$$S(j,j) = j!H^j |\mathcal{I}| (\beta-\alpha)^{2j}(1+O(j^2/H)) + O(H^{2j}(d^{4j} - 2d^{2j}d_g^j + 2d^{2j}d_f^{2j})\sqrt{p}\log^{2j} p).$$

Proof. We have

$$|S_n|^{2j} = \sum_{\substack{n<x(P_{i_1})\le n+H \\ y(P_{i_1})\in\mathcal{J}}} \cdots \sum_{\substack{n<x(P_{i_{2j}})\le n+H \\ y(P_{i_{2j}})\in\mathcal{J}}} \prod_{l=1}^{j} \chi(g(P_{i_l}))\psi(f(P_{i_l})) \tag{21}$$

$$\prod_{l=j+1}^{2j} \bar{\chi}(g(P_{i_l}))\bar{\psi}(f(P_{i_l}))$$

$$= \sum_{\substack{n<x(P_{i_1})\le n+H \\ y(P_{i_1})\in\mathcal{J}}} \cdots \sum_{\substack{n<x(P_{i_{2j}})\le n+H \\ y(P_{i_{2j}})\in\mathcal{J}}} \chi\left(\frac{g(P_{i_1})\dots g(P_{i_j})}{g(P_{i_{j+1}})\dots g(P_{i_{2j}})}\right)$$

$$\times \psi\left(\sum_{l=1}^{j} f(P_{i_l}) - \sum_{l=j+1}^{2j} f(P_{i_l})\right).$$

The main difficulty here is that the contents inside the two characters are not rational functions, and so Lemma 3.1 is not directly applicable. We proceed by transforming the sum into a hybrid sum on another curve, so that we can apply Lemma 3.1.

If X be an absolutely irreducible affine plane curve defined by $P(x,y)=0$, and $\mathcal{U}=\{u_1,\dots,u_m\}$ be a subset of $\{1,\dots,p\}$. Similar to [12], to each pair $(X,\mathcal{U})$, we define the x-shifted curve of X by $\mathcal{U}$, $X_{\mathcal{U}}$, to be the curve defined by the family of equations

$$\begin{aligned} P(x+u_1,y_1)&=0\\ P(x+u_2,y_2)&=0\\ &\vdots\\ P(x+u_m,y_m)&=0 \end{aligned}$$

in $\mathbb{A}_p^{m+1}$, the affine $(m+1)$-space over $\mathbb{F}_p$. It is easy to see that $X_{\mathcal{U}}$ is indeed a curve. (Note that the definition here is a little bit different from that of [12].) From the definition of $C_{\mathcal{U}}$ it is immediate that a point $(x,y_1,\dots,y_m)$ of $X_{\mathcal{U}}$ correspond to an m-tuple $(Q_1,\dots,Q_m)$ of distinct points in X with $x(Q_i)=x+u_i$.

Now fix a $(2j)$-tuple $\mathbf{h}=(h_1,\dots,h_{2j})$, with $1\le h_i\le H$, and set $\mathcal{U}_{\mathbf{h}}=\{u_1,\dots,u_m\}$ be the set of all h_i without multiplicity. By our assumption on $\mathcal{J}$, $P_{i_{l_1}}=P_{i_{l_2}}$ if and only if $h_{l_1}=h_{l_2}$. Thus we can view the $(2j)$-tuple $(P_{i_1},\dots,P_{i_{2j}})$ appeared in the above sum (21) as a point on $X_{\mathcal{U}}$ with x-coordinates equal to n, and this correspondence is one-to-one. So using (21), and change the order of summation, we get

$$S(j,j) = \sum_{h_1=1}^{H} \cdots \sum_{h_{2j}=1}^{H} \sum_{\substack{x\in\mathcal{I},y_1,\dots,y_{2j}\in\mathcal{J} \\ (x,y_1,\dots,y_{2j})\in X_{\mathcal{U}_{\mathbf{h}}}}} \chi\left(\frac{g(x+h_1,y_1)\dots g(x+h_j,y_j)}{g(x+h_{j+1},y_{j+1})\dots g(x+h_{2j},y_{2j})}\right)$$

$$\times \psi\left(\sum_{l=1}^{j} f(x+h_l,y_l) - \sum_{l=j+1}^{2j} f(x+h_l,y_l)\right),$$

where y_i and y_j stand for the same indeterminate if and only if $h_i = h_j$. Since

$$\tilde{g}_{\mathbf{h}}(x, y_1, \dots, y_{2j}) = \frac{g(x+h_1, y_1) \dots g(x+h_j, y_j)}{g(x+h_{j+1}, y_{j+1}) \dots g(x+h_{2j}, y_{2j})}$$

and

$$\tilde{f}_{\mathbf{h}}(x, y_1, \dots, y_{2j}) = \sum_{l=1}^{j} f(x+h_l, y_l) - \sum_{l=j+1}^{2j} f(x+h_l, y_l)$$

are rational functions, we can now apply Lemma 3.1 whenever the assumptions in that lemma are satisfied. We first calculate

$$D = \deg X_{\mathcal{U}_{\mathbf{h}}} \le d^{2j},$$
$$\deg(\text{denominator of } \tilde{g}_{\mathbf{h}}) \le d_g^j,$$
$$\deg(\text{denominator of } \tilde{f}_{\mathbf{h}}) \le d_f^{2j}.$$

To estimate the number of $(2j)$-tuples $\mathbf{h} = (h_1, \dots, h_{2j}$ that does not satisfy the assumption of Lemma 3.1 is to estimate the number of such tuples with $\tilde{g}_{\mathbf{h}}$ being an (ord χ)-th power and $\tilde{f}_{\mathbf{h}}$ is of the form $h^p - h +$ (linear terms). From Lemma 3.4, we must have $\tilde{f}_{\mathbf{h}} = 0$, and so $(h_1, \dots, h_j)$ and $(h_{j+1}, \dots, h_{2j})$ only differs by a permutation. Since there are $j(j-1)/2$ possible pairs from a j-tuple, there are a total $O(j^2 H^{j-1})$ j-tuples that have at least two equal components, and for $(h_1, \dots, h_j)$ with distinct components, there are exactly $j!$ possible permutations. Thus, the number of terms that we cannot use Lemma 3.1 to estimate is $j!H^j(1 + O(j^2/H))$. By the fact that $\mathbb{F}_p$-points are uniformly distributed on an affine curve (see Corollary 2.7 in [12]), each of the terms with distinct components contribute

$$|\mathcal{I}|\,(\beta - \alpha)^j + O(2^j d^{2j} \sqrt{p} \log^j p)$$

to the sum (except when we hit a pole of $g(x, y)$, and their contribution can be absorbed in the error term above), and is less for the terms with at least two components equal. Hence, the sum of all terms that we cannot apply Lemma 3.1 is

$$j!H^j\,|\mathcal{I}|\,(\beta - \alpha)^j(1 + O(j^2/H)) + O(2^j d^{2j} \sqrt{p} \log^j p).$$

For the other terms, we use Lemma 3.1, and the contribution of these terms to the sum is

$$O(H^{2j}(d^{4j} - 2d^{2j}d_g^j + 2d^{2j}d_f^{2j})\sqrt{p}(2\log p + 1)^{2j}).$$

Combining the above two estimations, we finally get

$$S(j,j) = j!H^j\,|\mathcal{I}|\,(\beta-\alpha)^j(1+O(j^2/H)) + O(2^j H^{2j}(d^{4j} - 2d^{2j}d_g^j + 2d^{2j}d_f^{2j})\sqrt{p}\log^{2j} p).$$

This finishes the proof of our lemma. □

4.2. The sum $S(j_1, j_2)$ for $j_1 \neq j_2$. As in the previous subsection, fix a $(j_1 + j_2)$-tuple $\mathbf{h} = (h_1, \dots, h_{j_1+j_2})$, with $1 \le h_i \le H$, and set $\mathcal{U}_{\mathbf{h}} = \{u_1, \dots, u_m\}$ be the set of all h_i without multiplicity. We have

$$S(j_1, j_2) = \sum_{h_1=1}^{H} \cdots \sum_{h_{j_1+j_2}=1}^{H} \sum_{\substack{x \in \mathcal{I}, y_1, \dots, y_{j_1+j_2} \in \mathcal{J} \\ (x, y_1, \dots, y_{j_1+j_2}) \in X_{\mathcal{U}_{\mathbf{h}}}}} \chi(\tilde{g}(x, y_1, \dots, y_{j_1+j_2})) \times \psi(\tilde{f}(x, y_1, \dots, y_{j_1+j_2})), \tag{22}$$

where

$$\tilde{g}_{\mathbf{h}}(x, y_1, \dots, y_{j_1+j_2}) = \frac{g(x+h_1, y_1)\dots g(x+h_{j_1}, y_{j_1})}{g(x+h_{j_1+1}, y_{j_1+1})\dots g(x+h_{j_1+j_2}, y_{j_1+j_2})}$$

and

$$\tilde{f}_{\mathbf{h}}(x, y_1, \dots, y_{j_1+j_2}) = \sum_{l=1}^{j_1} f(x+h_l, y_l) - \sum_{l=j_1+1}^{j_1+j_2} f(x+h_l, y_l).$$

Here again y_i and y_j stand for the same indeterminate if and only if $h_i = h_j$. We also have

$$\begin{aligned} D = \deg X_{\mathcal{U}_{\mathbf{h}}} &\le d^{j_1+j_2}, \\ \deg(\text{denominator of } \tilde{g}_{\mathbf{h}}) &\le d_g^{j_2}, \\ \deg(\text{denominator of } \tilde{f}_{\mathbf{h}}) &\le d_f^{j_1+j_2}. \end{aligned}$$

Unlike the case for $S(j,j)$, here by Lemma 3.4 we see that every term in our sum satisfy the assumption in Lemma 3.1. Therefore, we easily get the following lemma.

Lemma 4.2. *Assumptions as in Lemma 4.1. We have*

$$S(j_1, j_2) = O(H^{j_1+j_2}(d^{2j_1+2j_2} + 2d^{j_1+j_2}d_g^{j_2} + 2d^{j_1+j_2}d_f^{j_1+j_2})\sqrt{p}\log^{2j_1+2j_2} p).$$

5. The proof of Theorem 2.1

Now we have all the ingredients we need to calculate the moments M_k. First suppose k is an odd positive integer. Then $j \neq k-j$ for any integer j, so we can bound M_k by using Lemma 4.2 in the formula (19). We get

$$\begin{aligned} M_k &= O\left(\frac{1}{2^k((\beta-\alpha)H)^{\frac{k}{2}}}\sum_{j=0}^{k}\binom{k}{j}H^k(d^{2k} + 2d^k d_g^{k-j} + 2d^k d_f^k)\sqrt{p}\log^{2k} p\right) \\ &= O(H^{\frac{k}{2}}(d^{2k} + 2d^k d_g^k + 2d^k d_f^k)\sqrt{p}\log^{2k} p). \end{aligned}$$

This proves (6).

Next, if k is even, we use Lemma 4.1 for $S(k/2, k/2)$ and Lemma 4.2 for other terms. We obtain

$$\begin{aligned} M_k &= \frac{1}{2^k((\beta-\alpha)H)^{\frac{k}{2}}}\binom{k}{k/2}S(\frac{k}{2}, \frac{k}{2}) + O(2^{\frac{k}{2}}H^{\frac{k}{2}}(d^{2k} + 2d^k d_g^k + 2d^k d_f^k)\sqrt{p}\log^{2k} p) \\ &= \frac{1}{2^k}\binom{k}{k/2}(k/2)!\,|\mathcal{I}|\,(1 + O(k^2/H)) \\ &\quad + O(2^{\frac{k}{2}}H^{\frac{k}{2}}(d^{2k} + 2d^k d_g^k + 2d^k d_f^k)\sqrt{p}\log^{2k} p). \end{aligned}$$

This proves (7) and hence finished the proof of Theorem 2.1.

6. Proof of Corollary 2.3

From Corollary 2.2, we obtain the limit

$$\lim_{p\to\infty} \frac{2^{k/2} M_k}{|\mathcal{I}|} = \mu_k,$$

where

$$\mu_k = \begin{cases} 1 \cdot 3 \cdot \ldots \cdot (k-1), & \text{if } k \text{ is even,} \\ 0, & \text{if } k \text{ is odd.} \end{cases}$$

From the definition of M_k, this is

$$\lim_{p\to\infty} \frac{1}{|\mathcal{I}|} \sum_{n\in\mathcal{I}} (\sqrt{2}u_n)^k = \mu_k. \tag{23}$$

Let $N_p(s)$ be the number of integers $n \in \mathcal{I}$ such that $u_n \le s$. Then $N_p(s)$ is a monotonic increasing step-function of s, with discontinuities at $s = s_1, s_2, \ldots, s_h$, say. Note that $N_p(s) = 0$ if $s < -H$, and $N_p(s) = |\mathcal{I}|$ if $s \ge H$. Collecting together the values of $n \in \mathcal{I}$ for which $u_n = s_i$ in (23), we get (set $N_p(s_0) = 0$ by convention)

$$\lim_{p\to\infty} \frac{1}{|\mathcal{I}|} \sum_{i=1}^{h} (\sqrt{2}s_i)^k (N_p(s_i) - N_p(s_{i-1})) = \mu_k.$$

The left hand side of the above equation can be written as a Riemann-Stieltjes integral

$$\text{LHS} = \int_{-\infty}^{\infty} (\sqrt{2}t)^k \, d\phi_p(t),$$

where

$$\phi_p(t) = \frac{1}{|\mathcal{I}|} N_p(s).$$

Set

$$\phi(t) = \frac{1}{\sqrt{\pi}} \int_{-\infty}^{t} e^{-u^2} \, du,$$

then we have

$$\begin{aligned} \int_{-\infty}^{\infty} (\sqrt{2}t)^k \, d\phi(t) &= \frac{1}{\sqrt{\pi}} \int_{-\infty}^{\infty} (\sqrt{2}t)^k e^{-t^2} \, dt \\ &= \frac{1}{\sqrt{\pi}} 2^{\frac{k}{2}} (1 + (-1)^k) \Gamma((1+k)/2) \\ &= \mu_k. \end{aligned}$$

Thus

$$\lim_{p\to\infty} \int_{-\infty}^{\infty} (\sqrt{2}t)^k \, d\phi_p(t) = \int_{-\infty}^{\infty} (\sqrt{2}t)^k \, d\phi(t) \tag{24}$$

for any k. Essentially by the uniqueness of the moment problem with bounded support in probability theory (see for example [7]), one can deduce from (24) that

$$\lim_{p\to\infty} \phi_p(t) = \phi(t).$$

This finishes the proof of Corollary 2.3.

7. The case for χ trivial

The case when χ is the trivial character is easy to settle. Our Theorem 2.1 do not make any assumptions on $g(x)$, hence it is easy to see that the theorem still hold when χ is the trivial character, if other conditions in the theorem is still assumed. Indeed, given the exponential sum

$$S_n = \sum_{\substack{n<x(P_i)\leq n+H \\ y(P_i)\in\mathcal{J}}} \psi(f(P_i)),$$

we can form another hybrid sum

$$S'_n = \sum_{\substack{n<x(P_i)\leq n+H \\ y(P_i)\in\mathcal{J}}} \chi(g(P_i))\psi(f(P_i)),$$

with χ being the quadratic character, and $g(x,y) = x^2$. Then S_n and S'_n have the same values unless there is a P_i with zero x-coordinate, and the number of such P_i is at most $\deg(X)$, which is much smaller than the error term in Theorem 2.1. Now we apply the theorem to S'_n, and get the same conclusion for S_n. Since the corollaries to Theorem 2.1 does not make use of the properties of characters, they will continue to hold once Theorem 2.1 is correct. In particular, we have Gaussian distribution for the limiting distribution of the values of S_n also when χ is trivial. This finishes the proof of Theorem 2.8.

8. The case for ψ trivial

The case when ψ is the trivial character is a little bit more subtle, since Lemma 3.4 is not applicable. We return to the calculation of the moments M_k in (19), and investigate the sum $S(j_1,j_2)$ in (20). If ψ is trivial, then (22) becomes

$$S(j_1,j_2) = \sum_{h_1=1}^{H} \cdots \sum_{h_{j_1+j_2}=1}^{H} \sum_{\substack{x\in\mathcal{I},y_1,\ldots,y_{j_1+j_2}\in\mathcal{J} \\ (x,y_1,\ldots,y_{j_1+j_2})\in X_{\mathcal{U}_{\mathbf{h}}}}} \chi(\tilde{g}(x,y_1,\ldots,y_{j_1+j_2})),$$

where

$$\tilde{g}_{\mathbf{h}}(x,y_1,\ldots,y_{j_1+j_2}) = \frac{g(x+h_1,y_1)\ldots g(x+h_{j_1},y_{j_1})}{g(x+h_{j_1+1},y_{j_1+1})\ldots g(x+h_{j_1+j_2},y_{j_1+j_2})}.$$

We recall that y_i and y_j stand for the same indeterminate if and only if $h_i = h_j$.

Let a be the order of χ. We can apply Lemma 3.1 if $\tilde{g}$ is not a complete a-th power thanks to the assumptions in Theorem 2.9 and Remark 3.2. From the assumption we made to g, and that H, $\deg(g)$ are small compared to p, we see that products and quotients of $g(x+h_i,y_i)$ with distinct y_i's cannot be a complete a-th power (even when g does not depend on y) in any irreducible component of the x-shifted curve $X_{\mathcal{U}_{\mathbf{h}}}$. Hence, if the $g(x+h_i,y_i)$'s stack together and become a complete a-th power, it must come from a terms with the same h_i, or the same h_i appears in both the numerator and denominator of $\tilde{g}$.

Suppose first that $j_1 - j_2$ is not a multiple of a, then from the above discussion we see that $\tilde{g}$ can never be a complete a-th power. Hence we can use Lemma 3.1 to

obtain the estimate

$$S(j_1,j_2)=O(H^{j_1+j_2}(d^{2j_1+2j_2}+2d^{j_1+j_2}d_g^{j_2}+2d^{j_1+j_2}d_f^{j_1+j_2})\sqrt{p}\log^{2j_1+2j_2}p) \tag{25}$$

for those terms.

If $j_1-j_2=ma$ for some integer m, then we may obtain an a-th power by having the same h_i in the numerators and denominators, and group the remaining terms into $|m|$ blocks, each block consists of a terms with the same h_i. Note that for $a=2$ these two ways are the same since $\chi(g(x+h_i,y_i))$ agrees with its reciprocal. Fixing j_1 and j_2, it is easy to count the total number of such terms that make $\tilde{g}$ a complete a-th power. Letting $j=\min\{j_1,j_2\}$, this number is

$$j!\frac{(|m|\,a)!}{(a!)^{|m|}\,|m|!}H^{j+|m|}(1+O(j^2/H))$$

when $a>2$, and is

$$\frac{(j_1+j_2)!}{2^{\frac{j_1+j_2}{2}}\left(\frac{j_1+j_2}{2}\right)!}H^{\frac{j_1+j_2}{2}}(1+O((j_1+j_2)^2/H))$$

for $a=2$. Now each of the terms contribute at most

$$|\mathcal{I}|\,(\beta-\alpha)^{j+|m|}+O(2^{j+|m|}d^{2(j+|m|)}\sqrt{p}\log^{j+|m|}p)$$

to the sum for $a>2$, and

$$|\mathcal{I}|\,(\beta-\alpha)^{\frac{j_1+j_2}{2}}+O(2^{\frac{j_1+j_2}{2}}d^{j_1+j_2}\sqrt{p}\log^{\frac{j_1+j_2}{2}}p)$$

to the sum for $a=2$. Hence, the sum of all terms that we cannot apply Lemma 3.1 is

$$j!\frac{(|m|\,a)!}{(a!)^{|m|}\,|m|!}H^{j+|m|}\,|\mathcal{I}|\,(\beta-\alpha)^{j+|m|}(1+O(j^2/H))+O(2^{j+|m|}d^{2(j+|m|)}\sqrt{p}\log^{j+|m|}p)$$

for $a>2$, and is

$$\frac{(j_1+j_2)!}{2^{\frac{j_1+j_2}{2}}\left(\frac{j_1+j_2}{2}\right)!}H^{\frac{j_1+j_2}{2}}\,|\mathcal{I}|\,(\beta-\alpha)^{\frac{j_1+j_2}{2}}(1+O((j_1+j_2)^2/H))$$
$$+O(2^{\frac{j_1+j_2}{2}}d^{j_1+j_2}\sqrt{p}\log^{\frac{j_1+j_2}{2}}p)$$

for $a=2$.

For the other terms, we use Lemma 3.1, and the contribution of these terms to the sum is

$$O(H^{2(j+|m|)}(d^{4(j+|m|)}-2d^{2(j+|m|)}d_g^{j+|m|}+2d^{2(j+|m|)}d_f^{2(j+|m|)})\sqrt{p}(2\log p+1)^{2(j+|m|)})$$

for $a>2$, and

$$O(H^{j_1+j_2}(d^{2(j_1+j_2)}-2d^{j_1+j_2}d_g^{\frac{j_1+j_2}{2}}+2d^{j_1+j_2}d_f^{j_1+j_2})\sqrt{p}(2\log p+1)^{j_1+j_2})$$

for $a=2$.

Combining the above estimations, we finally get

$$S(j_1,j_2)=j!\frac{(|m|\,a)!}{(a!)^{|m|}\,|m|!}H^{j+|m|}\,|\mathcal{I}|\,(\beta-\alpha)^{j+|m|}(1+O(j^2/H))+O(2^{j+|m|}H^{2(j+|m|)} \tag{26}$$
$$\times(d^{4(j+|m|)}-2d^{2(j+|m|)}d_g^{j+|m|}+2d^{2(j+|m|)}d_f^{2(j+|m|)})\sqrt{p}\log^{2(j+|m|)}p),$$

for $j_1 - j_2 = ma$, $j = \min\{j_1, j_2\}$ and $a > 2$, and

$$S(j_1, j_2) = \frac{(j_1+j_2)!}{2^{\frac{j_1+j_2}{2}}\left(\frac{j_1+j_2}{2}\right)!} H^{\frac{j_1+j_2}{2}} |\mathcal{I}| (\beta-\alpha)^{\frac{j_1+j_2}{2}} (1 + O((j_1+j_2)^2/H)) + O(2^{\frac{j_1+j_2}{2}} H^{j_1+j_2} (d^{2(j_1+j_2)} - 2d^{j_1+j_2} d_g^{\frac{j_1+j_2}{2}} + 2d^{j_1+j_2} d_f^{j_1+j_2}) \times \sqrt{p}(2\log p + 1)^{j_1+j_2})$$

for $j_1 = j_2 = ma$, $a = 2$. Note that $S(j_1, j_2)$ only depend on $j_1 + j_2$ but not the particular j_1, j_2.

With the estimations for $S(j_1, j_2)$ in hand, we are ready to calculate the moments. From (19) we have

$$M_k = \frac{1}{2^k((\beta-\alpha)H)^{\frac{k}{2}}} \sum_{j=0}^{k} \binom{k}{j} e^{(k-2j)i\theta} S(j, k-j).$$

There are 2 cases according to the parity of a.

8.1. The case when a is even. First suppose a is even. Then if k is odd, we have $j - (k-j) = 2j - k$ is also odd, and thus it can never be a multiple of a. Every term in the above sum can then be estimated using (25). We have

$$\begin{aligned} M_k &= O\left(\frac{1}{2^k((\beta-\alpha)H)^{\frac{k}{2}}} \sum_{j=0}^{k} \binom{k}{j} H^k (d^{2k} + 2d^k d_g^{k-j} + 2d^k d_f^k) \sqrt{p} \log^{2k} p \right) \\ &= O(H^{\frac{k}{2}} (d^{2k} + 2d^k d_g^k + 2d^k d_f^k) \sqrt{p} \log^{2k} p). \end{aligned}$$

This proves (8) and (10) in Theorem 2.9.

If k is even, then the case for $a = 2$ is different from the others. If $a = 2$, we have

$$\begin{aligned} M_k &= \frac{1}{2^k((\beta-\alpha)H)^{\frac{k}{2}}} \sum_{j=0}^{k} \binom{k}{j} e^{(k-2j)i\theta} S(j, k-j) \\ &= \frac{1}{2^k((\beta-\alpha)H)^{\frac{k}{2}}} \sum_{j=0}^{k} \binom{k}{j} e^{(k-2j)i\theta} \frac{k!}{2^{\frac{k}{2}}\left(\frac{k}{2}\right)!} H^{\frac{k}{2}} |\mathcal{I}| (\beta-\alpha)^{\frac{k}{2}} (1 + O(k^2/H)) \\ &\quad + O(2^{\frac{k}{2}} H^k (d^{2k} - 2d^k d_g^{\frac{k}{2}} + 2d^k d_f^k) \sqrt{p} (2\log p + 1)^k) \\ &= \frac{1}{2^k} \frac{k!}{2^{\frac{k}{2}}\left(\frac{k}{2}\right)!} |\mathcal{I}| \left(\sum_{j=0}^{k} \binom{k}{j} e^{(k-2j)i\theta} \right) (1 + O(k^2/H)) \\ &\quad + O(2^{\frac{k}{2}} H^k (d^{2k} - 2d^k d_g^{\frac{k}{2}} + 2d^k d_f^k) \sqrt{p} (2\log p + 1)^k) \end{aligned}$$

In general we are unable to handle the sum $\sum_{j=0}^{k} \binom{k}{j} e^{(k-2j)i\theta}$, and we do not have Gaussian distribution for general θ. See Remark 2.12 for details.

For $\theta = 0$, the above calculation of M_k becomes

$$M_k = \frac{k!}{2^{\frac{k}{2}}\left(\frac{k}{2}\right)!} |\mathcal{I}| (1 + O(k^2/H)) + O(2^{\frac{k}{2}} H^k (d^{2k} - 2d^k d_g^{\frac{k}{2}} + 2d^k d_f^k) \sqrt{p} (2\log p + 1)^k).$$

This is (9) in Theorem 2.9.

If $a > 2$ (still even), then it is easy to see that $2j - k$ is a multiple of a if and only if $j = k/2 + m(a/2)$ for $m = -[k/a], -[k/a]+1, \dots, [k/a]$, where $[x]$ denotes the greatest integer function. Note that for those j, we have $2j - k = ma$. By estimating the terms corresponding to above j using (26), and all other terms using (25), we have

$$\begin{aligned} M_k &= \frac{1}{2^k((\beta-\alpha)H)^{\frac{k}{2}}} \sum_{m=-[\frac{k}{a}]}^{[\frac{k}{a}]} \frac{k!}{(\frac{k}{2}+\frac{a|m|}{2})!} \frac{(|m|\,a)!}{(a!)^{|m|}} |\mathcal{I}| \,(H(\beta-\alpha))^{(\frac{k}{2}-a\frac{|m|}{2})+|m|} \\ &\qquad \times (1+O(k^2/H)) + O(H^{\frac{3k}{2}}(d^{4k} - 2d^{2k}d_g^k + 2d^{2k}d_f^{2k})\sqrt{p}\log^{2k} p) \\ &= \frac{1}{2^k}\frac{k!}{(k/2)!}\,|\mathcal{I}|\,(1+O(k^{\frac{a}{2}+2}/H)) + O(H^{\frac{3k}{2}}(d^{4k} - 2d^{2k}d_g^k + 2d^{2k}d_f^{2k})\sqrt{p}\log^{2k} p). \end{aligned}$$

This is (11).

8.2. The case when a is odd. Let a be an odd integer, $a > 1$. Again there are two cases according to the parity of k. First assume k is even, then $2j - k$ is even, and since a is odd, $2j - k$ will be a multiple of a if and only if it is a multiple of $2a$. Therefore, the result here is the same as the case where the order of χ is $2a$. We have

$$\begin{aligned} M_k = \frac{1}{2^k}\frac{k!}{(k/2)!}\,|\mathcal{I}|\,(1+O(k^{\frac{a}{2}+2}/H)) \\ + O(H^{\frac{3k}{2}}(d^{4k} - 2d^{2k}d_g^k + 2d^{2k}d_f^{2k})\sqrt{p}\log^{2k} p). \end{aligned}$$

This gives (13).

Now if k is odd, then if $2j - k = ma$, m must be odd. Similar to the calculation in the case a even and $a > 2$, we see that the main terms of M_k correspond to $j = \frac{k}{2} + \frac{a}{2}$ and $j = \frac{k}{2} - \frac{a}{2}$. We have

$$\begin{aligned} M_k &= \frac{1}{2^k((\beta-\alpha)H)^{\frac{k}{2}}}\binom{k}{\frac{k}{2}-\frac{a}{2}}(e^{ia\theta}+e^{-ia\theta})\left(\frac{k}{2}-\frac{a}{2}\right)!H^{\frac{k}{2}-\frac{a}{2}+1}\,|\mathcal{I}|\,(\beta-\alpha)^{\frac{k}{2}-\frac{a}{2}+1} \\ &\qquad \times (1+O(k^{a+2}/H)) + O((H^{\frac{3k}{2}}(d^{4k} - 2d^{2k}d_g^k + 2d^{2k}d_f^{2k})\sqrt{p}\log^{2k} p) \\ &= \frac{1}{2^k((\beta-\alpha)H)^{\frac{a}{2}-1}}\frac{k!}{(\frac{k}{2}+\frac{a}{2})!}(2\cos a\theta)\,|\mathcal{I}|\,(1+O(k^{a+2}/H)) \\ &\qquad + O((H^{\frac{3k}{2}}(d^{4k} - 2d^{2k}d_g^k + 2d^{2k}d_f^{2k})\sqrt{p}\log^{2k} p). \end{aligned}$$

This proves (12) and finishes the proof of Theorem 2.9.

References

[1] E. Bombieri, *On Exponential Sums in Finite Fields*, Amer. J. Math. **88** (1966), no. 1, 71–105.

[2] O.-Y. Chan, G. Choi, and A. Zaharescu, *A multidimensional version of a result of Davenport-Erdős*, J. Integer Seq. **6** (2003), no. 2, Article 03.2.6, 9 pp. (electronic).

[3] H. Davenport and P. Erdös, *The distribution of quadratic and higher residues*, Publ. Math. Debrecen **2** (1952) 252–265.

[4] P. Erdös and M. Kac, *The Gaussian law of errors in the theory of additive number theoretic functions*, Amer. J. Math. **62** (1940) 738–742.

[5] P. Erdös, H. Maier, and A. Sárközy, *On the distribution of the number of prime factors of sums $a + b$*, Trans. Amer. Math. Soc. **302** (1987), no. 1, 269–280.

[6] P. Erdős and C. Pomerance, *On the normal number of prime factors of $\phi(n)$*, Rocky Mountain J. Math. **15** (1985), no. 2, 343–352. Number theory (Winnipeg, Man., 1983).
[7] W. Feller, An Introduction to Probability Theory and Its Applications, Vol. 2, Wiley, 2nd edition (1971).
[8] M. Fujiwara, *Distribution of rational points on varieties over finite fields*, Mathematika **35** (1988), no. 2, 155–171.
[9] A. Granville and K. Soundararajan, *Sieving and the Erdős-Kac theorem*, in Equidistribution in number theory, an introduction, Vol. 237 of *NATO Sci. Ser. II Math. Phys. Chem.*, 15–27, Springer, Dordrecht (2007).
[10] W. Kuo and Y.-R. Liu, *Gaussian laws on Drinfeld modules*, Int. J. Number Theory **5** (2009), no. 7, 1179–1203.
[11] Y.-R. Liu, *Prime analogues of the Erdős-Kac theorem for elliptic curves*, J. Number Theory **119** (2006), no. 2, 155–170.
[12] K.-H. Mak and A. Zaharescu, *Poisson type phenomena for points on hyperelliptic curves modulo p*. Submitted.
[13] G. Myerson, *The distribution of rational points on varieties defined over a finite field*, Mathematika **28** (1981), no. 2, 153–159 (1982).
[14] G. I. Perel'muter, *Estimation of a sum along an algebraic curve*, Mat. Zametki **5** (1969) 373–380.
[15] A. Weil, *On some exponential sums*, Proc. Nat. Acad. Sci. U. S. A. **34** (1948) 204–207.
[16] M. Xiong, *The Erdős-Kac theorem for polynomials of several variables*, Proc. Amer. Math. Soc. **137** (2009), no. 8, 2601–2608.
[17] M. Xiong and A. Zaharescu, *Distribution of Selmer groups of quadratic twists of a family of elliptic curves*, Adv. Math. **219** (2008), no. 2, 523–553.
[18] ———, *Selmer groups and Tate-Shafarevich groups for the congruent number problem*, Comment. Math. Helv. **84** (2009), no. 1, 21–56.

Department of Mathematics, University of Illinois at Urbana-Champaign, 273 Altgeld Hall, MC-382, 1409 W. Green Street, Urbana, Illinois 61801, USA
E-mail address: mak4@illinois.edu

Department of Mathematics, University of Illinois at Urbana-Champaign, 273 Altgeld Hall, MC-382, 1409 W. Green Street, Urbana, Illinois 61801, USA
E-mail address: zaharesc@math.uiuc.edu