Canad. J. Math. Vol. **55** (2), 2003 pp. 225–246

Short Kloosterman Sums for Polynomials over Finite Fields

William D. Banks, Asma Harcharras and Igor E. Shparlinski

Abstract. We extend to the setting of polynomials over a finite field certain estimates for short Kloosterman sums originally due to Karatsuba. Our estimates are then used to establish some uniformity of distribution results in the ring $\mathbb{F}_q[x]/M(x)$ for collections of polynomials either of the form $f^{-1}g^{-1}$ or of the form $f^{-1}g^{-1} + afg$, where f and g are polynomials coprime to M and of very small degree relative to M, and a is an arbitrary polynomial. We also give estimates for short Kloosterman sums where the summation runs over products of two irreducible polynomials of small degree. It is likely that this result can be used to give an improvement of the Brun-Titchmarsh theorem for polynomials over finite fields.

1 Introduction

Let q be a prime power, $\mathbb{F}_q$ the finite field with q elements, and $\mathcal{R}$ the polynomial ring $\mathbb{F}_q[x]$. Fix an irreducible polynomial $M \in \mathcal{R}$ of degree $\deg(M) = m > 0$, and let $\mathcal{R}_M$ denote the field $\mathcal{R}/(M)$. Put

$$\mathcal{R}_m = \{f \in \mathcal{R} \mid \deg(f) < m\}, \quad \mathcal{R}_m^* = \{f \in \mathcal{R}_m \mid f \neq 0\},$$

and observe the natural bijections

$$\mathcal{R}_m \longleftrightarrow^{\sim} \mathcal{R}_M, \quad \mathcal{R}_m^* \longleftrightarrow^{\sim} \mathcal{R}_M^\times.$$

In particular, for every $f \in \mathcal{R}_m^*$, there exists a unique element $f^* \in \mathcal{R}_m^*$ such that $ff^* \equiv 1 \pmod M$. Then f^* is the inverse of f if both polynomials are viewed as elements of $\mathcal{R}_M^\times$.

For any subset $\mathcal{E} \subset \{0, 1, \ldots, m-1\}$ and any two polynomials $f, g \in \mathcal{R}_m$, with

$$f(x) = \sum_{j=0}^{m-1} a_j x^j, \quad g(x) = \sum_{j=0}^{m-1} b_j x^j,$$

write $f \approx_{\mathcal{E}} g$ whenever $a_j = b_j$ for all $j \in \mathcal{E}$. Then $\approx_{\mathcal{E}}$ defines an equivalence relation on $\mathcal{R}_m$, and we will denote by $\mathcal{R}_m/\approx_{\mathcal{E}}$ the corresponding set of equivalence classes.

In this paper, we study the distribution in $\mathcal{R}_m/\approx_{\mathcal{E}}$ of polynomials of the form $(fg)^*$, where f and g are nonzero polynomials of small degree relative to m. We show that the polynomials $(fg)^*$ are uniformly distributed in $\mathcal{R}_m/\approx_{\mathcal{E}}$ provided that the cardinality of $\mathcal{E}$ satisfies a certain upper bound. Our main result in this direction is Theorem 6 of Section 5. As an application, our Theorem 6 implies the following result:

Received by the editors October 31, 2001; revised March 5, 2002.
AMS subject classification: 11T23, 11T06.

Theorem 1 *Let ϵ be a real number such that $0 \le \epsilon < 1/3$, and suppose that $m \gg_\epsilon 1$ and $q \gg_m 1$. Then for any polynomial $F \in \mathcal{R}_m$ and any set $\mathcal{E} \subset \{0, 1, \dots, m-1\}$ of cardinality*

$$|\mathcal{E}| \le m^{3\epsilon}(\log m)^3,$$

there exist polynomials $f, g \in \mathcal{R}_m^*$, with

$$\deg(f), \deg(g) \le m^{2/3+\epsilon} \log m,$$

such that

$$(fg)^* \approx_{\mathcal{E}} F.$$

Moreover, if ϵ is at least $1/12$, and $m \gg_\epsilon 1$, the result holds for any choice of the prime power q.

We remark that the conditions of Theorem 1 are *independent of the choice of M*; the conclusion therefore holds for *every* irreducible polynomial M of degree m.

Now for any $f \in \mathcal{R}$, let $\{f\}$ be the unique polynomial in $\mathcal{R}_m$ such that $f \equiv \{f\} \pmod M$. In this paper, we also study the distribution in $\mathcal{R}_m/\approx_{\mathcal{E}}$ of polynomials of the form $\{(fg)^* + afg\}$, where $a \in \mathcal{R}_m$, and f and g are nonzero polynomials of small degree relative to m. We show that the polynomials $\{(fg)^* + afg\}$ are uniformly distributed in $\mathcal{R}_m/\approx_{\mathcal{E}}$, assuming again that the cardinality of $\mathcal{E}$ satisfies a certain bound. Our main result in this direction is Theorem 7 of Section 5, which implies the following:

Theorem 2 *Let ϵ be a real number such that $0 \le \epsilon < 1/3$, and suppose that $m \gg_\epsilon 1$ and $q \gg_m 1$. Then for any two polynomials $F, a \in \mathcal{R}_m$ and any set $\mathcal{E} \subset \{0, 1, \dots, m-1\}$ of cardinality*

$$|\mathcal{E}| \le \frac{m^{3\epsilon}(\log m)^3}{8},$$

there exist polynomials $f, g \in \mathcal{R}_m^*$, with

$$\deg(f), \deg(g) \le m^{2/3+\epsilon} \log m,$$

such that

$$\{(fg)^* + afg\} \approx_{\mathcal{E}} F.$$

Moreover, if ϵ is at least $1/12$, and $m \gg_\epsilon 1$, the result holds for any choice of the prime power q.

The main results of this paper (Theorems 6 and 7) rely primarily on bounds for character sums of the form

$$\sum_{\substack{f,g \ne 0 \\ \deg(f) \le d \\ \deg(g) \le e}} \chi\big((fg)^* + afg\big),$$

where χ is a nontrivial additive character of $\mathcal{R}_M$. Such bounds are provided by Theorem 3 for the case $a \in \mathcal{R}_m^*$, and by Theorem 4 for the case $a = 0$ (see Section 4).

https://doi.org/10.4153/CJM-2003-010-0 Published online by Cambridge University Press

Theorems 3 and 4 are proved without the assumption that M is irreducible, and we remark that Theorems 6 and 7 can be extended (with only minor modifications) to arbitrary polynomials as well. For this reason, we do not make explicit use of the isomorphism $\mathcal{R}_M \simeq \mathcal{F}_{q^m}$, and we do not formulate Theorems 6 and 7 in terms of finite fields.

We also consider the interesting special case of sums of the form

$$\sum_{f,g\in\mathcal{P}_d} \chi\big((fg)^*\big),$$

where $\mathcal{P}_d$ denotes the set of monic irreducible polynomials of degree d that are relatively prime to M. For these sums, our techniques provide a much stronger estimate; see Theorem 5. We remark that the analogous estimate for integers has been used to improve the Brun-Titchmarsh theorem. Accordingly, we hope that our estimate can be used to improve the function field analogue of the Brun-Titchmarsh theorem as given in [3].

Our methods are essentially those of Karatsuba [5] (see also [2, 4]), which we have extended to work over the polynomial ring $\mathbb{F}_q[x]$. However, several of the underlying results have been unknown for polynomials, and we have had to establish them in the current paper (in fact, our results for polynomials exhibit some new effects that do not occur in the case of integers). Some of these fundamental results may be of independent interest and are likely to find several other applications; for example, see Lemma 2.

Finally, we remark that several uniformity of distribution results on the inverses of polynomials from small sets have recently been obtained in [1] by a different method.

The first author would like to thank Macquarie University for its hospitality. Work supported in part by NSF grant DMS-0070628 (W. Banks) and by ARC grant A69700294 (I. Shparlinski).

2 Notation

Throughout the paper, k and ℓ denote positive *integers*, while d and e are nonnegative *real numbers*.

Let q be a fixed prime power, and let $\mathbb{F}_q$ be the finite field with q elements. Put

$$\mathcal{R} = \mathbb{F}_q[x], \quad \mathcal{R}^* = \mathbb{F}_q[x] - \{0\}.$$

Given $f, g \in \mathcal{R}^*$, we write $f \sim g$ whenever $f = ag$ for some $a \in \mathbb{F}_q^\times$. Then the set of equivalence classes in $\mathcal{R}^*/\sim$ can be naturally identified with the set $\mathcal{M}$ of *monic polynomials* in $\mathcal{R}$. We denote the *greatest common divisor* of $f_1, \dots, f_k \in \mathcal{R}^*$ by $\gcd(f_1, \dots, f_k)$; by definition, it is the element $h \in \mathcal{M}$ of greatest degree such that h divides f_j, $j = 1, \dots, k$. Similarly, the *least common multiple* will be denoted by $\operatorname{lcm}[f_1, \dots, f_k]$; it is the element $h \in \mathcal{M}$ of least degree such that f_j divides h, $j = 1, \dots, k$.

For every $d \geq 0$, let $\mathcal{M}(d)$ be the set of monic polynomials $f \in \mathcal{M}$ of degree $\deg(f) \leq d$.

https://doi.org/10.4153/CJM-2003-010-0 Published online by Cambridge University Press

3 Preliminary Results

For every $f \in \mathcal{R}^*$ and $k \geq 1$, let $\tau_k(f)$ be the number of *ordered k-tuples* $(f_1, \ldots, f_k) \in \mathcal{M}^k$ such that $f \sim f_1 \cdots f_k$. Observe that $\tau_k(f) = \tau_k(g)$ whenever $f \sim g$.

Lemma 1 *For all $f, g \in \mathcal{R}^*$ and $k \geq 1$, we have $\tau_k(fg) \leq \tau_k(f)\tau_k(g)$. If $\gcd(f, g) = 1$, then $\tau_k(fg) = \tau_k(f)\tau_k(g)$.*

Proof For any $f \in \mathcal{R}^*$, let $\mathcal{T}_k(f) \subset \mathcal{M}^k$ be the collection of ordered k-tuples defined by

$$\mathcal{T}_k(f) = \{(f_1, \ldots, f_k) \in \mathcal{M}^k \mid f \sim f_1 \cdots f_k\}.$$

By definition, $\tau_k(f)$ is the cardinality of $\mathcal{T}_k(f)$. Consider the natural map $\mathcal{T}_k(f) \times \mathcal{T}_k(g) \to \mathcal{T}_k(fg)$ given by

$$\big((f_1, \ldots, f_k), (g_1, \ldots, g_k)\big) \mapsto (f_1 g_1, \ldots, f_k g_k).$$

It can easily be verified that this map is a *bijection* if $\gcd(f, g) = 1$, hence we obtain the second statement of the lemma.

If $p \in \mathcal{M}$ is irreducible and $\alpha \geq 0$ is any integer, one clearly has

$$\tau_k(p^\alpha) = \binom{\alpha + k - 1}{k - 1}.$$

From this it follows that $\tau_k(p^{\alpha+\beta}) \leq \tau_k(p^\alpha)\tau_k(p^\beta)$ for all $\alpha, \beta \geq 0$. Now for arbitrary $f, g \in \mathcal{R}^*$, let $p_1, \ldots, p_r \in \mathcal{M}$ be the complete set of irreducible polynomials that occur in the factorization of the product fg. Then

$$f \sim p_1^{\alpha_1} \cdots p_r^{\alpha_r}, \quad g \sim p_1^{\beta_1} \cdots p_r^{\beta_r},$$

for some uniquely determined integers $\alpha_j, \beta_j \geq 0$, $j = 1, \ldots, r$, so by our previous results, it follows that

$$\tau_k(fg) = \prod_{j=1}^{r} \tau_k(p_j^{\alpha_j+\beta_j}) \leq \prod_{j=1}^{r} \tau_k(p_j^{\alpha_j})\tau_k(p_j^{\beta_j}) = \tau_k(f)\tau_k(g).$$

This completes the proof. ∎

Lemma 2 *For all $k, \ell \geq 1$ and $d \geq 0$, we have*

$$\sum_{f \in \mathcal{M}(d)} \tau_k(f)^\ell q^{-\deg(f)} \leq \binom{\lfloor d \rfloor + k}{k}^{k^{\ell-1}}. \tag{1}$$

If $\ell = 1$, then (1) holds with equality.

https://doi.org/10.4153/CJM-2003-010-0 Published online by Cambridge University Press

Proof Let $\ell = 1$ be fixed for the moment. Since $\tau_1(f) = 1$ for all $f \in \mathcal{R}^*$, and

$$\sum_{f\in\mathcal{M}(d)} q^{-\deg(f)} = \sum_{j=0}^{\lfloor d\rfloor} \sum_{\substack{f\in\mathcal{M}\\ \deg(f)=j}} q^{-j} = \sum_{j=0}^{\lfloor d\rfloor} 1 = \lfloor d\rfloor + 1,$$

we see that (1) holds with equality for all $d \geq 0$ when $k = 1$. Proceeding inductively, we now suppose that (1) holds with equality up to $k-1$, where $k \geq 2$. Since

$$\tau_k(f) = \sum_{\substack{f_1,f_2\in\mathcal{M}\\ f\sim f_1f_2}} \tau_{k-1}(f_2),$$

we therefore have

$$\begin{aligned}
\sum_{f\in\mathcal{M}(d)} \tau_k(f)q^{-\deg(f)} &= \sum_{f\in\mathcal{M}(d)} \sum_{\substack{f_1,f_2\in\mathcal{M}\\ f\sim f_1f_2}} \tau_{k-1}(f_2)q^{-\deg(f_1f_2)}\\
&= \sum_{f_1\in\mathcal{M}(d)} q^{-\deg(f_1)} \sum_{f_2\in\mathcal{M}(d-\deg(f_1))} \tau_{k-1}(f_2)q^{-\deg(f_2)}\\
&= \sum_{f_1\in\mathcal{M}(d)} q^{-\deg(f_1)} \binom{\lfloor d\rfloor - \deg(f_1) + k - 1}{k-1}\\
&= \sum_{j=0}^{\lfloor d\rfloor} \binom{\lfloor d\rfloor - j + k - 1}{k-1} = \binom{\lfloor d\rfloor + k}{k}.
\end{aligned}$$

Hence the lemma is proved when $\ell = 1$.

Now suppose that the inequality (1) holds up to $\ell - 1$, $\ell \geq 2$, for all $k \geq 1$ and $d \geq 0$. Using Lemma 1, it follows that

$$\begin{aligned}
\sum_{f\in\mathcal{M}(d)} \tau_k(f)^\ell q^{-\deg(f)} &= \sum_{f\in\mathcal{M}(d)} \sum_{\substack{f_1,\dots,f_k\in\mathcal{M}\\ f\sim f_1\cdots f_k}} \tau_k(f_1\cdots f_k)^{\ell-1} q^{-\deg(f_1\cdots f_k)}\\
&\leq \sum_{\substack{f_1,\dots,f_k\in\mathcal{M}\\ \deg(f_1\cdots f_k)\leq d}} \prod_{j=1}^{k} \tau_k(f_j)^{\ell-1} q^{-\deg(f_j)}\\
&\leq \sum_{f_1,\dots,f_k\in\mathcal{M}(d)} \prod_{j=1}^{k} \tau_k(f_j)^{\ell-1} q^{-\deg(f_j)}\\
&= \Bigg(\sum_{f\in\mathcal{M}(d)} \tau_k(f)^{\ell-1} q^{-\deg(f)}\Bigg)^k\\
&\leq \left(\binom{\lfloor d\rfloor + k}{k}^{k^{\ell-2}}\right)^k = \binom{\lfloor d\rfloor + k}{k}^{k^{\ell-1}}.
\end{aligned}$$

https://doi.org/10.4153/CJM-2003-010-0 Published online by Cambridge University Press

This completes the proof. ∎

Using Lemma 2, we obtain the estimate

$$\sum_{f\in\mathcal{M}(d)} \tau_k(f)^\ell q^{(\alpha-1)\deg(f)} \le q^{\alpha\lfloor d\rfloor}\binom{\lfloor d\rfloor + k}{k}^{k^{\ell-1}}, \tag{2}$$

which is valid for all $k, \ell \ge 1$, $d \ge 0$, and any real number $\alpha \ge 0$. This will be used to prove the following:

Lemma 3 *For all $k \ge 1$ and $d \ge 0$, let $\mathcal{J}(k,d)$ be the number of ordered k-tuples $(f_1,\dots,f_k) \in \mathcal{M}^k$ such that*

$$\deg(f_1\cdots f_k) \le d,$$

and

$$f_1\cdots f_k \equiv 0 \pmod{\operatorname{lcm}[f_1^2,\dots,f_k^2]}.$$

Then the following estimate holds:

$$\mathcal{J}(k,d) \le q^{d/2}\binom{\lfloor d/2\rfloor + k}{k}^k \binom{\lfloor d/3\rfloor + k}{k}^{k^2}.$$

Proof For any $f \in \mathcal{M}$, let $\lambda_k(f)$ be the number of ordered k-tuples $(f_1,\dots,f_k) \in \mathcal{M}^k$ such that $f = f_1\cdots f_k$ and

$$f_1\cdots f_k \equiv 0 \pmod{\operatorname{lcm}[f_1^2,\dots,f_k^2]}.$$

Clearly, we have

$$\mathcal{J}(k,d) = \sum_{f\in\mathcal{M}(d)} \lambda_k(f). \tag{3}$$

If $f_j, g_j \in \mathcal{M}$ and $\gcd(f_j,g_j) = 1$ for $j = 1,\dots,k$, then

$$\operatorname{lcm}[f_1^2,\dots,f_k^2]\cdot\operatorname{lcm}[g_1^2,\dots,g_k^2] = \operatorname{lcm}[(f_1g_1)^2,\dots,(f_kg_k)^2];$$

from this it follows that λ_k is multiplicative, *i.e.*, that $\lambda_k(fg) = \lambda_k(f)\lambda_k(g)$ whenever $\gcd(f,g) = 1$. Thus, if $f \in \mathcal{M}$ and $f = p_1^{\alpha_1}\cdots p_r^{\alpha_r}$ is a factorization into positive powers of pairwise-distinct monic irreducibles, then

$$\lambda_k(f) = \lambda_k(p_1^{\alpha_1})\cdots\lambda_k(p_r^{\alpha_r}).$$

Since it is also clear that $\lambda_k(p) = 0$ for any irreducible $p \in \mathcal{M}$, every nonzero term in (3) arises from a polynomial f of the form

$$f = p_1^{\alpha_1}\cdots p_r^{\alpha_r}, \quad \alpha_1,\dots,\alpha_r \ge 2,$$

https://doi.org/10.4153/CJM-2003-010-0 Published online by Cambridge University Press

which implies that $f = g^2h^3$ for some $g, h \in \mathcal{M}$. Since $\lambda_k(f) \le \tau_k(f)$, we have

$$\mathcal{J}(k,d) \le \sum_{\substack{g,h\in\mathcal{M}\\ \deg(g^2h^3)\le d}} \lambda_k(g^2h^3) \le \sum_{\substack{g,h\in\mathcal{M}\\ \deg(g^2h^3)\le d}} \tau_k(g^2h^3).$$

By Lemma 1, it follows that

$$\mathcal{J}(k,d) \le \sum_{g\in\mathcal{M}(d/2)} \tau_k(g)^2 \sum_{h\in\mathcal{M}((d-2\deg(g))/3)} \tau_k(h)^3.$$

Applying the estimate (2) with $\ell = 3$ and $\alpha = 1$, we see that

$$\begin{aligned}\sum_{h\in\mathcal{M}((d-2\deg(g))/3)} \tau_k(h)^3 &\le q^{\lfloor (d-2\deg(g))/3\rfloor} \binom{\lfloor (d-2\deg(g))/3\rfloor + k}{k}^{k^2}\\ &\le q^{-2\deg(g)/3} q^{d/3} \binom{\lfloor d/3\rfloor + k}{k}^{k^2}.\end{aligned}$$

Applying (2) again with $\ell = 2$ and $\alpha = 1/3$, we have

$$\begin{aligned}\sum_{g\in\mathcal{M}(d/2)} \tau_k(g)^2 q^{-2\deg(g)/3} &\le q^{\lfloor d/2\rfloor/3} \binom{\lfloor d/2\rfloor + k}{k}^{k}\\ &\le q^{d/6} \binom{\lfloor d/2\rfloor + k}{k}^{k}.\end{aligned}$$

The lemma follows. ∎

4 Estimation of Character Sums

Throughout this section, we assume that $M \in \mathcal{R}$ is a fixed polynomial of degree $\deg(M) = m > 0$. Let $\mathcal{R}_M$ be the quotient ring $\mathcal{R}/(M)$, let $\mathcal{R}_M^\times$ be the multiplicative group of $\mathcal{R}_M$, and let

$$\mathcal{R}_M^* = \{f \in \mathcal{R}^* \mid \deg(f) < m \text{ and } \gcd(f, M) = 1\}.$$

We note that the canonical surjection $\mathcal{R} \to \mathcal{R}_M$ gives rise to a *bijection* $\mathcal{R}_M^* \xleftrightarrow{\sim} \mathcal{R}_M^\times$. For any $f \in \mathcal{R}$ such that $\gcd(f, M) = 1$, we denote by f^* the unique polynomial in $\mathcal{R}_M^*$ such that $ff^* \equiv 1 \pmod M$. In particular, f^* is the *inverse* of f if we regard both polynomials as elements of $\mathcal{R}_M^\times$.

For a real number d such that $0 \le d < m$, let $\mathcal{R}(d)$ [resp. $\mathcal{R}_M^*(d)$] denote the set of polynomials $f \in \mathcal{R}$ [resp. $f \in \mathcal{R}_M^*$] of degree $\deg(f) \le d$.

https://doi.org/10.4153/CJM-2003-010-0 Published online by Cambridge University Press

Lemma 4 *Suppose that $k \geq 1$, $d \geq 0$, and $(2k-1)\lfloor d \rfloor < m$. Let $\mathcal{I}(k,d)$ be the number of ordered $2k$-tuples $(f_1, \ldots, f_{2k}) \in \mathcal{R}_M^*(d)^{2k}$ such that*

$$f_1^* + \cdots + f_k^* \equiv f_{k+1}^* + \cdots + f_{2k}^* \pmod{M}. \tag{4}$$

Then

$$\mathcal{I}(k,d) \leq (q-1)^{2k} \mathcal{J}(2k, 2kd),$$

where $\mathcal{J}$ is defined as in Lemma 3.

Proof Suppose that $f_1, \ldots, f_{2k}$ are elements of $\mathcal{R}_M^*(d)$ that satisfy (4). Multiplying both sides of (4) by the product $f_1 \cdots f_{2k}$ and using the fact that $f_j f_j^* \equiv 1 \pmod{M}$, we obtain

$$g_1 + \cdots + g_k \equiv g_{k+1} + \cdots + g_{2k} \pmod{M},$$

where each g_j is defined by the relation $f_j g_j = f_1 \cdots f_{2k}$. Now since we have $\deg(g_j) \leq (2k-1)\lfloor d \rfloor < m$ for each $j = 1, \ldots, 2k$, this congruence becomes an *equality*

$$g_1 + \cdots + g_k = g_{k+1} + \cdots + g_{2k}.$$

By definition, f_j divides g_ℓ whenever $\ell \neq j$, so this equality implies that f_j divides g_j as well. Consequently

$$f_1 \cdots f_{2k} = f_j g_j \equiv 0 \pmod{f_j^2},$$

and therefore

$$f_1 \cdots f_{2k} \equiv 0 \pmod{\operatorname{lcm}[f_1^2, \ldots, f_{2k}^2]}.$$

Since $\deg(f_1 \cdots f_{2k}) \leq 2kd$, the result follows. ∎

An *additive character* of $\mathcal{R}_M$ is a homomorphism

$$\chi \colon \mathcal{R}_M \to \mathbb{C}^\times.$$

For the sake of convenience in what follows, we will also denote by χ the corresponding homomorphism $\mathcal{R} \to \mathbb{C}^\times$ which is trivial on the principal ideal (M), obtained by composing $\chi \colon \mathcal{R}_M \to \mathbb{C}^\times$ with the canonical surjection $\mathcal{R} \to \mathcal{R}_M$.

For any additive character χ of $\mathcal{R}_M$, let

$$\Omega_\chi = \{\alpha \in \mathcal{R} \mid \chi(\alpha\beta) = 1 \text{ for all } \beta \in \mathcal{R}\}.$$

Then Ω_χ is an ideal in $\mathcal{R}$; since $\mathcal{R}$ is a principal ideal domain, it follows that Ω_χ is the ideal generated by a (unique) monic polynomial $f_\chi \in \mathcal{M}$. Since $M \in \Omega_\chi$, f_χ is a divisor of M. If χ is the trivial character, then $f_\chi = 1$. On the other hand, if $f_\chi \sim M$, then χ is said to be *primitive*.

https://doi.org/10.4153/CJM-2003-010-0 Published online by Cambridge University Press

Theorem 3 *Suppose that $k, \ell \geq 1$, $d, e \geq 0$, and*

$$(2k-1)\lfloor d \rfloor < m, \quad (2\ell - 1)\lfloor e \rfloor < m.$$

Let $\mathcal{F}$ and $\mathcal{G}$ be arbitrary subsets of $\mathcal{R}_M^*(d)$ and $\mathcal{R}_M^*(e)$, respectively. Then for any primitive character χ of $\mathcal{R}_M$ and any element $a \in \mathcal{R}$, the character sum

$$\mathcal{S} = \sum_{\substack{f \in \mathcal{F} \\ g \in \mathcal{G}}} \chi\big((fg)^* + afg\big)$$

satisfies the bound $|\mathcal{S}| \leq |\mathcal{F}|\,|\mathcal{G}|\Delta$, where

$$\Delta = \big(|\mathcal{F}|^{-2k}|\mathcal{G}|^{-2\ell} q^{m+\min(d,e)+1}(q-1)^{2k+2\ell}\mathcal{J}(2k, 2kd)\mathcal{J}(2\ell, 2\ell e)\big)^{1/2k\ell},$$

and $\mathcal{J}$ is defined as in Lemma 3.

Proof By Hölder's inequality and the fact that $(fg)^* \equiv f^*g^* \pmod M$, we have

$$\begin{aligned} |\mathcal{S}|^\ell &\leq |\mathcal{F}|^{\ell-1} \sum_{f \in \mathcal{F}} \Big| \sum_{g \in \mathcal{G}} \chi(f^*g^* + afg)\Big|^\ell \\ &= |\mathcal{F}|^{\ell-1} \sum_{f \in \mathcal{F}} \Big| \sum_{\beta \in \mathcal{R}_M} \sum_{\delta \in \mathcal{R}(e)} \sigma_\ell(\beta, \delta)\chi(f^*\beta + af\delta)\Big|, \end{aligned}$$

where $\sigma_\ell(\beta, \delta)$ denotes the number of ordered ℓ-tuples $(g_1, \ldots, g_\ell)$ in $\mathcal{G}^\ell$ such that

$$\begin{aligned} g_1^* + \cdots + g_\ell^* &\equiv \beta \pmod M, \\ g_1 + \cdots + g_\ell &\equiv \delta \pmod M. \end{aligned}$$

Now for each $f \in \mathcal{F}$, let $\arg f$ denote the argument of the double summation inside the absolute value in the preceding inequality. Then

$$|\mathcal{S}|^\ell \leq |\mathcal{F}|^{\ell-1} \sum_{\beta \in \mathcal{R}_M} \sum_{\delta \in \mathcal{R}(e)} \sigma_\ell(\beta, \delta)\Big| \sum_{f \in \mathcal{F}} e^{-i \arg f} \chi(f^*\beta + af\delta)\Big|.$$

Raising both sides of this inequality to the power k and applying Hölder's inequality once more, we obtain

$$\begin{aligned} |\mathcal{S}|^{k\ell} \leq |\mathcal{F}|^{(\ell-1)k} &\Big(\sum_{\beta \in \mathcal{R}_M} \sum_{\delta \in \mathcal{R}(e)} \sigma_\ell(\beta, \delta)\Big)^{k-1} \\ &\times \sum_{\beta \in \mathcal{R}_M} \sum_{\delta \in \mathcal{R}(e)} \sigma_\ell(\beta, \delta)\Big| \sum_{f \in \mathcal{F}} e^{-i \arg f} \chi(f^*\beta + af\delta)\Big|^k. \end{aligned}$$

https://doi.org/10.4153/CJM-2003-010-0 Published online by Cambridge University Press

Applying Cauchy's inequality to the last part of this expression, we therefore see that

$$|\mathcal{S}|^{k\ell} \le |\mathcal{F}|^{(\ell-1)k}(\mathcal{L}_1)^{k-1}(\mathcal{L}_2)^{1/2}(\mathcal{L}_3)^{1/2}, \tag{5}$$

where

$$\mathcal{L}_1 = \sum_{\beta\in\mathcal{R}_M}\sum_{\delta\in\mathcal{R}(e)} \sigma_\ell(\beta,\delta),$$

$$\mathcal{L}_2 = \sum_{\beta\in\mathcal{R}_M}\sum_{\delta\in\mathcal{R}(e)} \sigma_\ell(\beta,\delta)^2,$$

$$\mathcal{L}_3 = \sum_{\beta\in\mathcal{R}_M}\sum_{\delta\in\mathcal{R}(e)} \Big|\sum_{f\in\mathcal{F}} e^{-i\arg f}\chi(f^*\beta + af\delta)\Big|^{2k}.$$

The first sum $\mathcal{L}_1$ is equal to the total number of ordered ℓ-tuples $(g_1,\dots,g_\ell) \in \mathcal{G}^\ell$:

$$\mathcal{L}_1 = |\mathcal{G}|^\ell. \tag{6}$$

The second sum $\mathcal{L}_2$ is equal to the number of ordered 2ℓ-tuples $(g_1,\dots,g_{2\ell}) \in \mathcal{G}^{2\ell}$ such that

$$g_1^* + \cdots + g_\ell^* \equiv g_{\ell+1}^* + \cdots + g_{2\ell}^* \pmod M,$$
$$g_1 + \cdots + g_\ell \equiv g_{\ell+1} + \cdots + g_{2\ell} \pmod M.$$

Since $(2\ell-1)\lfloor e\rfloor < m$ by hypothesis, we can use Lemma 4 to bound $\mathcal{L}_2$, and we obtain

$$\mathcal{L}_2 \le (q-1)^{2\ell}\mathcal{J}(2\ell, 2\ell e). \tag{7}$$

For the third sum $\mathcal{L}_3$, we have

$$\begin{aligned}
\mathcal{L}_3 &= \sum_{\beta\in\mathcal{R}_M}\sum_{\delta\in\mathcal{R}(e)}\sum_{f_1,\dots,f_{2k}\in\mathcal{F}} e^{-i(\arg f_1+\cdots+\arg f_k-\arg f_{k+1}-\cdots-\arg f_{2k})} \\
&\qquad \times \chi\big((f_1^*+\cdots-f_{2k}^*)\beta + a(f_1+\cdots-f_{2k})\delta\big) \\
&\le \sum_{f_1,\dots,f_{2k}\in\mathcal{F}} \Big|\sum_{\beta\in\mathcal{R}_M}\sum_{\delta\in\mathcal{R}(e)} \chi\big((f_1^*+\cdots-f_{2k}^*)\beta + a(f_1+\cdots-f_{2k})\delta\big)\Big| \\
&\le \sum_{\alpha\in\mathcal{R}_M}\sum_{\gamma\in\mathcal{R}(d)} \tilde\sigma_k(\alpha,\gamma)\Big|\sum_{\beta\in\mathcal{R}_M}\sum_{\delta\in\mathcal{R}(e)} \chi(\alpha\beta + a\gamma\delta)\Big| \\
&= \sum_{\alpha\in\mathcal{R}_M}\sum_{\gamma\in\mathcal{R}(d)} \tilde\sigma_k(\alpha,\gamma)\Big|\sum_{\beta\in\mathcal{R}_M}\chi(\alpha\beta)\sum_{\delta\in\mathcal{R}(e)}\chi(a\gamma\delta)\Big|,
\end{aligned}$$

https://doi.org/10.4153/CJM-2003-010-0 Published online by Cambridge University Press

where $\tilde{\sigma}_k(\alpha,\gamma)$ is the number of ordered $2k$-tuples $(f_1,\dots,f_{2k}) \in \mathcal{F}^{2k}$ that satisfy

$$f_1^* + \cdots + f_k^* \equiv \alpha + f_{k+1}^* + \cdots + f_{2k}^* \pmod{M}, \tag{8}$$

and

$$f_1 + \cdots + f_k \equiv \gamma + f_{k+1} + \cdots + f_{2k} \pmod{M}.$$

Now since χ is a primitive character, the sum

$$\sum_{\beta\in\mathcal{R}_M} \chi(\alpha\beta) = \begin{cases} q^m & \text{if } \alpha = 0, \\ 0 & \text{otherwise;} \end{cases} \tag{9}$$

thus

$$\mathcal{L}_3 \le q^m \sum_{\gamma\in\mathcal{R}(d)} \tilde{\sigma}_k(0,\gamma) \Big| \sum_{\delta\in\mathcal{R}(e)} \chi(a\gamma\delta)\Big| \le q^{m+e+1} \sum_{\gamma\in\mathcal{R}(d)} \tilde{\sigma}_k(0,\gamma)$$

since $|\mathcal{R}(e)| = q^{e+1}$. As the sum

$$\sum_{\gamma\in\mathcal{R}(d)} \tilde{\sigma}_k(0,\gamma)$$

counts the total number of solutions to (8) with $\alpha = 0$, and $(2k-1)\lfloor d\rfloor < m$ by hypothesis, we have by Lemma 4:

$$\mathcal{L}_3 \le q^{m+e+1}(q-1)^{2k}\mathcal{J}(2k,2kd). \tag{10}$$

Substituting the estimates (6), (7) and (10) into in (5), we obtain the bound stated in the theorem except that we now have q^{m+e+1} instead of the term $q^{m+\min(d,e)+1}$. The correct bound follows by symmetry. ∎

When M divides a, we can improve the bound stated in Theorem 3.

Theorem 4 *Using the notation of Theorem 3, the character sum*

$$\mathcal{S} = \sum_{\substack{f\in\mathcal{F}\\ g\in\mathcal{G}}} \chi\big((fg)^*\big)$$

satisfies the bound $|\mathcal{S}| \le |\mathcal{F}|\,|\mathcal{G}|\Delta$, *where*

$$\Delta = \big(|\mathcal{F}|^{-2k}|\mathcal{G}|^{-2\ell} q^m (q-1)^{2k+2\ell}\mathcal{J}(2k,2kd)\mathcal{J}(2\ell,2\ell e)\big)^{1/2k\ell}.$$

Proof By Hölder's inequality, we have

$$|\mathcal{S}|^\ell \le |\mathcal{F}|^{\ell-1} \sum_{f\in\mathcal{F}} \Big|\sum_{g\in\mathcal{G}} \chi(f^*g^*)\Big|^\ell = |\mathcal{F}|^{\ell-1} \sum_{f\in\mathcal{F}} \Big|\sum_{\beta\in\mathcal{R}_M} \sigma_\ell(\beta)\chi(f^*\beta)\Big|,$$

https://doi.org/10.4153/CJM-2003-010-0 Published online by Cambridge University Press

where $\sigma_\ell(\beta)$ denotes the number of ordered ℓ-tuples $(g_1, \dots, g_\ell)$ in $\mathcal{G}^\ell$ such that

$$g_1^* + \cdots + g_\ell^* \equiv \beta \pmod{M}.$$

For each $f \in \mathcal{F}$, let $\arg f$ denote the argument of the summation inside the absolute value in the preceding inequality. Then

$$|\mathcal{S}|^\ell \le |\mathcal{F}|^{\ell-1} \sum_{\beta \in \mathcal{R}_M} \sigma_\ell(\beta) \Big| \sum_{f \in \mathcal{F}} e^{-i \arg f} \chi(f^* \beta) \Big|.$$

Raising both sides of this inequality to the power k and applying Hölder's inequality once more, we obtain

$$|\mathcal{S}|^{k\ell} \le |\mathcal{F}|^{(\ell-1)k} \Big(\sum_{\beta \in \mathcal{R}_M} \sigma_\ell(\beta) \Big)^{k-1} \sum_{\beta \in \mathcal{R}_M} \sigma_\ell(\beta) \Big| \sum_{f \in \mathcal{F}} e^{-i \arg f} \chi(f^* \beta) \Big|^k.$$

Applying Cauchy's inequality, we see that

$$|\mathcal{S}|^{k\ell} \le |\mathcal{F}|^{(\ell-1)k} (\mathcal{L}_1)^{k-1} (\mathcal{L}_2)^{1/2} (\mathcal{L}_3)^{1/2},$$

where

$$\mathcal{L}_1 = \sum_{\beta \in \mathcal{R}_M} \sigma_\ell(\beta),$$

$$\mathcal{L}_2 = \sum_{\beta \in \mathcal{R}_M} \sigma_\ell(\beta)^2,$$

$$\mathcal{L}_3 = \sum_{\beta \in \mathcal{R}_M} \Big| \sum_{f \in \mathcal{F}} e^{-i \arg f} \chi(f^* \beta) \Big|^{2k}.$$

The sums $\mathcal{L}_1$ and $\mathcal{L}_2$ can be estimated as in Theorem 3. For the third sum, we have

$$\begin{aligned} \mathcal{L}_3 &= \sum_{\beta \in \mathcal{R}_M} \sum_{f_1, \dots, f_{2k} \in \mathcal{F}} e^{-i(\arg f_1 + \cdots - \arg f_{2k})} \chi\big((f_1^* + \cdots - f_{2k}^*) \beta \big) \\ &\le \sum_{f_1, \dots, f_{2k} \in \mathcal{F}} \Big| \sum_{\beta \in \mathcal{R}_M} \chi\big((f_1^* + \cdots - f_{2k}^*) \beta \big) \Big| \\ &\le \sum_{\alpha \in \mathcal{R}_M} \tilde{\sigma}_k(\alpha) \Big| \sum_{\beta \in \mathcal{R}_M} \chi(\alpha \beta) \Big|, \end{aligned}$$

where $\tilde{\sigma}_k(\alpha)$ is the number of ordered $2k$-tuples $(f_1, \dots, f_{2k}) \in \mathcal{F}^{2k}$ that satisfy

$$f_1^* + \cdots + f_k^* \equiv \alpha + f_{k+1}^* + \cdots + f_{2k}^* \pmod{M}.$$

https://doi.org/10.4153/CJM-2003-010-0 Published online by Cambridge University Press

Using (9) and Lemma 4, we have

$$\mathcal{L}_3 \le q^m \bar{\sigma}_k(0) \le q^m (q-1)^{2k} \mathcal{J}(2k, 2kd).$$

The result follows. ∎

Theorem 5 *Suppose that* $(2k-1)\,d < m$. *Then for any primitive character* χ *of* $\mathcal{R}_M$, *the character sum*

$$\mathcal{S} = \sum_{f,g \in \mathcal{P}_d} \chi\big((fg)^*\big)$$

satisfies the bound

$$|\mathcal{S}| \le (k!)^{1/k^2} |\mathcal{P}_d|^{2-1/k} q^{m/2k^2}.$$

Proof From the Hölder inequality, we obtain

$$\begin{aligned} |\mathcal{S}|^k &\le |\mathcal{P}_d|^{k-1} \sum_{f \in \mathcal{P}_d} \Big| \sum_{g \in \mathcal{P}_d} \chi\big((fg)^*\big) \Big|^k \\ &= |\mathcal{P}_d|^{k-1} \sum_{f \in \mathcal{P}_d} \vartheta_f \sum_{g_1, \dots, g_k \in \mathcal{P}_d} \chi\big(f^*(g_1^* + \cdots + g_k^*)\big), \end{aligned}$$

where ϑ_f is such that $|\vartheta_f| = 1$. Denoting by $T_k(\psi)$ the number of solutions of the congruence

$$g_1^* + \cdots + g_k^* \equiv \psi \pmod{M}, \quad g_1, \dots, g_k \in \mathcal{P}_d,$$

we derive that

$$|\mathcal{S}|^k \le |\mathcal{P}_d|^{k-1} \sum_{\psi \in \mathcal{R}_M} T_k(\psi) \sum_{f \in \mathcal{P}_d} \vartheta_f \chi(\psi f^*).$$

Applying the Hölder inequality again, we have

$$|\mathcal{S}|^{2k^2} \le |\mathcal{P}_d|^{2k^2-2k} \Big(\sum_{\psi \in \mathcal{R}_M} T_k(\psi) \Big)^{2k-2} \sum_{\psi \in \mathcal{R}_M} T_k(\psi)^2 \sum_{\psi \in \mathcal{R}_M} \Big| \sum_{f \in \mathcal{P}_d} \vartheta_f \chi(\psi f^*) \Big|^{2k}.$$

Let $\mathcal{W}(k, d)$ denote the number of solutions of the congruence

$$f_1^* + \cdots + f_k^* \equiv f_{k+1}^* + \cdots + f_{2k}^* \pmod{M}, \quad f_1, \dots, f_{2k} \in \mathcal{P}_d. \tag{11}$$

Now, we have

$$\sum_{\psi \in \mathcal{R}_M} T_k(\psi) = |\mathcal{P}_d|^k \quad \text{and} \quad \sum_{\psi \in \mathcal{R}_M} T_k(\psi)^2 = \mathcal{W}(k, d).$$

https://doi.org/10.4153/CJM-2003-010-0 Published online by Cambridge University Press

Consequently

$$\begin{aligned}|\mathcal{S}|^{2k^2} &\le |\mathcal{P}_d|^{4k^2-4k}\mathcal{W}(k,d)\\ &\quad\cdot \sum_{\psi\in\mathcal{R}_M}\sum_{f_1,\dots,f_{2k}\in\mathcal{P}_d} \chi\big(\psi(f_1^*+\cdots+f_k^*-f_{k+1}^*-\cdots-f_{2k}^*)\big)\prod_{\nu=1}^{k}\vartheta_{f_\nu}\prod_{\nu=k+1}^{2k}\bar{\vartheta}_{f_\nu}\\ &\le |\mathcal{P}_d|^{4k^2-4k}\mathcal{W}(k,d)\\ &\quad\cdot \sum_{f_1,\dots,f_{2k}\in\mathcal{P}_d}\Big|\sum_{\psi\in\mathcal{R}_M}\chi\big(\psi(f_1^*+\cdots+f_k^*-f_{k+1}^*-\cdots-f_{2k}^*)\big)\Big|.\end{aligned}$$

Applying (9), we see that

$$|\mathcal{S}|^{2k^2} \le |\mathcal{P}_d|^{4k^2-4k}q^n\mathcal{W}(k,d)^2.$$

To estimate $\mathcal{W}(k,d)$, we remark that (11) is equivalent to the congruence

$$\sum_{\nu=1}^{k}\prod_{\substack{i=1\\ i\ne\nu}}^{2k} f_i \equiv \sum_{\nu=k+1}^{2k}\prod_{\substack{i=1\\ i\ne\nu}}^{2k} f_i \pmod{M}.$$

Since the degrees of the polynomials on the both sides of this congruence are at most $(2k-1)d < n$, this congruence yields an equality over $\mathbb{F}_q[X]$:

$$\sum_{\nu=1}^{k}\prod_{\substack{i=1\\ i\ne\nu}}^{2k} f_i = \sum_{\nu=k+1}^{2k}\prod_{\substack{i=1\\ i\ne\nu}}^{2k} f_i.$$

Hence,

$$f_1^*+\cdots+f_k^* = f_{k+1}^*+\cdots+f_{2k}^*.$$

Recalling that the polynomials $f_1,\dots,f_{2k}$ are irreducible and comparing the denominators of the expressions on both sides of this equation, we see that equality is possible if and only if

$$\{f_1,\dots,f_k\} = \{f_{k+1},\dots,f_{2k}\}.$$

Therefore

$$\mathcal{W}(k,d) \le k!\,|\mathcal{P}_d|^k,$$

and the result follows. ∎

5 Results on Uniform Distribution

Throughout this section, let $M \in \mathcal{R}$ be a fixed *irreducible* polynomial of degree $\deg(M) = m > 0$. Put

$$\mathcal{R}_m = \{f \in \mathcal{R} \mid \deg(f) < m\}, \quad \mathcal{R}_m^* = \{f \in \mathcal{R}_m \mid f \ne 0\},$$

https://doi.org/10.4153/CJM-2003-010-0 Published online by Cambridge University Press

and for any real number d with $0 \le d < m$, let

$$\mathcal{R}^*(d) = \{f \in \mathcal{R}^* \mid \deg(f) \le d\}.$$

Note that $\mathcal{R}_m^* = \mathcal{R}_M^*$ and $\mathcal{R}^*(d) = \mathcal{R}_M^*(d)$ in our previous notation, since $\gcd(f, M) = 1$ for all $f \in \mathcal{R}_m^*$. As in the previous section, for each $f \in \mathcal{R}_m^*$, let f^* be the unique polynomial in $\mathcal{R}_m^*$ such that $ff^* \equiv 1 \pmod{M}$. Then f^* is an inverse for f in the multiplicative group $\mathcal{R}_M^\times$.

Since M is irreducible, $\mathcal{R}_M = \mathcal{R}/(M)$ is a *field*; consequently, an additive character χ of $\mathcal{R}_M$ is primitive if and only if it is nontrivial.

Lemma 5 *Let k and d be positive integers such that*

$$d = \left\lfloor \frac{m}{2k - \delta} \right\rfloor,$$

where $0 < \delta < 1$. Then for every nontrivial character χ of $\mathcal{R}_M$, the character sum

$$\mathcal{S} = \sum_{f,g \in \mathcal{R}^*(d)} \chi\big((fg)^*\big)$$

satisfies the bound $|\mathcal{S}| \le |\mathcal{R}^*(d)|^2 \exp(\Delta)$, where

$$\Delta = -\frac{\delta m \log q}{2k^2(2k - \delta)} + \frac{\log q}{k} + 12k \log m.$$

Proof Set $e = d$, $\ell = k$, and $\mathcal{F} = \mathcal{G} = \mathcal{R}^*(d)$. Since

$$(2k - 1)d \le \frac{(2k - 1)}{(2k - \delta)} m < m,$$

we see that all of the conditions of Theorem 4 hold; thus

$$|\mathcal{S}| \le |\mathcal{R}^*(d)|^2 \Delta',$$

where

$$(\Delta')^{2k^2} = |\mathcal{R}^*(d)|^{-4k} q^m (q - 1)^{4k} \mathcal{J}(2k, 2kd)^2.$$

Since $|\mathcal{R}^*(d)| = q^{d+1} - 1$, we have by Lemma 3:

$$\begin{aligned}
(\Delta')^{2k^2} &= q^m \left(\frac{q - 1}{q^{d+1} - 1} \right)^{4k} \mathcal{J}(2k, 2kd)^2 \\
&\le q^{m - 4kd} \mathcal{J}(2k, 2kd)^2 \\
&\le q^{m - 2kd} \binom{kd + 2k}{2k}^{4k} \binom{\lfloor 2kd/3 \rfloor + 2k}{2k}^{8k^2}.
\end{aligned}$$

https://doi.org/10.4153/CJM-2003-010-0 Published online by Cambridge University Press

First, we estimate

$$m - 2kd < m - 2k\Big(\frac{m}{2k-\delta} - 1\Big) = 2k - \frac{\delta m}{2k-\delta}.$$

Next, since $k \ge 1$, we have $kd \le (2k-1)d < m$, hence $kd + 1 \le m$. Consequently,

$$\binom{kd+2k}{2k} \le (kd+1)^{2k} \le m^{2k}.$$

Similarly,

$$\binom{\lfloor 2kd/3 \rfloor + 2k}{2k} \le m^{2k},$$

and the result follows. ∎

Recall that for a set $\mathcal{E}$ of nonnegative integers and two polynomials

$$f(x) = \sum_{j\ge 0} a_j x^j, \quad g(x) = \sum_{j\ge 0} b_j x^j,$$

we write $f \approx_{\mathcal{E}} g$ to indicate that $a_j = b_j$ for all $j \in \mathcal{E}$. Then $\approx_{\mathcal{E}}$ defines an equivalence relation on $\mathcal{R}$.

Theorem 6 *Let k and d be positive integers such that*

$$d = \Big\lfloor \frac{m}{2k-\delta} \Big\rfloor,$$

where $0 < \delta < 1$. Fix an arbitrary subset $\mathcal{E} \subset \{0, 1, \dots, m-1\}$ of cardinality $|\mathcal{E}| = n$ and a polynomial $F \in \mathcal{R}$, and let $\mathcal{N}$ be the number of ordered pairs (f, g) in $\mathcal{R}^*(d)^2$ such that $(fg)^* \approx_{\mathcal{E}} F$. Then

$$\Big|\mathcal{N} - \frac{|\mathcal{R}^*(d)|^2}{q^n}\Big| < |\mathcal{R}^*(d)|^2 \exp(\Delta),$$

where Δ is defined as in Lemma 5. In particular, if

$$n \le \frac{\delta m}{2k^2(2k-\delta)} - \frac{1}{k} - \frac{12k\log m}{\log q},$$

then

$$0 < \mathcal{N} < 2\frac{|\mathcal{R}^*(d)|^2}{q^n}.$$

https://doi.org/10.4153/CJM-2003-010-0 Published online by Cambridge University Press

Proof Without loss of generality, we can assume that $\deg(F) < m$. Let $\mathcal{X}_{\mathcal{E}}$ be the set of polynomials in $\mathcal{R}_m$ whose coefficients vanish on $\mathcal{E}$; that is,

$$\mathcal{X}_{\mathcal{E}} = \Big\{ f \in \mathcal{R}_m \;\Big|\; f(x) = \sum_{j \notin \mathcal{E}} a_j x^j \Big\}.$$

Note that $\mathcal{X}_{\mathcal{E}}$ is an additive subgroup of $\mathcal{R}$: $\mathcal{X}_{\mathcal{E}} + \mathcal{X}_{\mathcal{E}} = \mathcal{X}_{\mathcal{E}}$. Let $\mathcal{Q}$ be the number of representations of the form

$$F = (fg)^* + \phi - \psi,$$

where $f, g \in \mathcal{R}^*(d)$ and $\phi, \psi \in \mathcal{X}_{\mathcal{E}}$. Since $(fg)^* \approx_{\mathcal{E}} F$ if and only if $F - (fg)^*$ lies in $\mathcal{X}_{\mathcal{E}}$, and $|\mathcal{X}_{\mathcal{E}}| = q^{m-n}$, we have

$$\mathcal{Q} = q^{m-n}\mathcal{N}.$$

Now

$$\begin{aligned}
\mathcal{Q} &= \sum_{f,g \in \mathcal{R}^*(d)} \sum_{\phi,\psi \in \mathcal{X}_{\mathcal{E}}} \frac{1}{q^m} \sum_{\chi} \chi\big((fg)^* - F - \phi + \psi\big), \\
&= \frac{1}{q^m} \sum_{\chi} \overline{\chi(F)} \sum_{\phi,\psi \in \mathcal{X}_{\mathcal{E}}} \chi(\psi - \phi) \sum_{f,g \in \mathcal{R}^*(d)} \chi\big((fg)^*\big) \\
&= \frac{1}{q^m} \sum_{\chi} \overline{\chi(F)} \Big| \sum_{\phi \in \mathcal{X}_{\mathcal{E}}} \chi(\phi) \Big|^2 \sum_{f,g \in \mathcal{R}^*(d)} \chi\big((fg)^*\big) \\
&= |\mathcal{R}^*(d)|^2 q^{m-2n} + \frac{1}{q^m} \sum_{\chi \neq 1} \overline{\chi(F)} \Big| \sum_{\phi \in \mathcal{X}_{\mathcal{E}}} \chi(\phi) \Big|^2 \sum_{f,g \in \mathcal{R}^*(d)} \chi\big((fg)^*\big).
\end{aligned}$$

By Lemma 5, we have

$$\begin{aligned}
\big|\mathcal{Q} - |\mathcal{R}^*(d)|^2 q^{m-2n}\big| &\le \frac{1}{q^m} \sum_{\chi \neq 1} \Big| \sum_{\phi \in \mathcal{X}_{\mathcal{E}}} \chi(\phi) \Big|^2 \Big| \sum_{f,g \in \mathcal{R}^*(d)} \chi\big((fg)^*\big) \Big| \\
&\le \frac{|\mathcal{R}^*(d)|^2 \exp(\Delta)}{q^m} \sum_{\chi \neq 1} \Big| \sum_{\phi \in \mathcal{X}_{\mathcal{E}}} \chi(\phi) \Big|^2.
\end{aligned}$$

Using the estimate

$$\sum_{\chi \neq 1} \Big| \sum_{\phi \in \mathcal{X}_{\mathcal{E}}} \chi(\phi) \Big|^2 = -q^{2m-2n} + \sum_{\chi} \sum_{\phi,\psi \in \mathcal{X}_{\mathcal{E}}} \chi(\psi - \phi) = q^{2m-n} - q^{2m-2n},$$

we have

$$\big|\mathcal{Q} - |\mathcal{R}^*(d)|^2 q^{m-2n}\big| < |\mathcal{R}^*(d)|^2 q^{m-n} \exp(\Delta).$$

https://doi.org/10.4153/CJM-2003-010-0 Published online by Cambridge University Press

The result follows. ∎

Using Theorem 6, we can now give a proof of Theorem 1 as stated in the introduction.

Proof Put $\lambda = (1/2)^{1/7} < 1$, and consider the collection $\mathcal{D}$ of integers d in the interval

$$\lambda m^{2/3+\epsilon} \log m \le d \le m^{2/3+\epsilon} \log m.$$

For every $d \in \mathcal{D}$, we have

$$\frac{m^{1/3-\epsilon}}{\log m} \le \frac{m}{d} \le \frac{m^{1/3-\epsilon}}{\lambda \log m}.$$

If $m \gg_\epsilon 1$, the closed interval $[m^{1/3-\epsilon}/\log m, m^{1/3-\epsilon}/(\lambda \log m)]$ has length

$$(\lambda^{-1} - 1)\frac{m^{1/3-\epsilon}}{\log m} > 2 + (1 - \lambda).$$

On the other hand, if d and $d+1$ both lie in $\mathcal{D}$, then

$$\frac{m}{d} - \frac{m}{d+1} < \frac{m}{d^2} \le \frac{1}{\lambda^2 m^{1/3+2\epsilon} (\log m)^2} < (1 - \lambda)$$

provided that $m \gg_\epsilon 1$. Consequently, for some $d \in \mathcal{D}$, there exists an integer k such that m/d lies in the open interval $\big(2k - 1, 2k - 1 + (1 - \lambda)\big)$. Let k and d be fixed with these properties, and set $\delta = 2k - m/d$. Then we have $\lambda < \delta < 1$, and

$$k = \frac{m}{2d} + \frac{\delta}{2} > 0,$$

hence all of the conditions of Theorem 6 are satisfied. Applying the theorem, we see that $\mathcal{N} > 0$ provided that

$$|\mathcal{E}| \le \frac{\delta m}{2k^2(2k - \delta)} - \frac{1}{k} - \frac{12k \log m}{\log q}. \tag{12}$$

Now for all $m \gg_\epsilon 1$, we have

$$k < \frac{m}{2d} + \frac{1}{2} \le \frac{m^{1/3-\epsilon}}{2\lambda \log m} + \frac{1}{2} < \frac{m^{1/3-\epsilon}}{2\lambda^2 \log m},$$

thus

$$\frac{\delta m}{2k^2(2k - \delta)} > \frac{\lambda m}{2k^2(m/d)} = \frac{\lambda d}{2k^2} > \frac{\lambda^2 m^{2/3+\epsilon} \log m}{2\big(m^{1/3-\epsilon}/(2\lambda^2 \log m)\big)^2};$$

that is,

$$\frac{\delta m}{2k^2(2k - \delta)} > 2\lambda^6 m^{3\epsilon} (\log m)^3.$$

https://doi.org/10.4153/CJM-2003-010-0 Published online by Cambridge University Press

Since $-1/k \geq -1$, and

$$-\frac{12k\log m}{\log q} > -\frac{6m^{1/3-\epsilon}}{\lambda^2 \log q},$$

it follows that the right side of (12) is bounded below by

$$2\lambda^6 m^{3\epsilon}(\log m)^3 - \frac{6m^{1/3-\epsilon}}{\lambda^2 \log q} - 1,$$

and this is bounded below by

$$2\lambda^7 m^{3\epsilon}(\log m)^3 = m^{3\epsilon}(\log m)^3$$

provided that

$$\log q > \frac{6m^{1/3-\epsilon}}{(\lambda - \lambda^2)m^{3\epsilon}(\log m)^3 - \lambda^2}.$$

The theorem follows. ∎

For the rest of this section, we study the distribution in $\mathcal{R}_M$ of polynomials of the form $(fg)^* + afg$, where a is a fixed element of $\mathcal{R}$, and f and g run through the sets $\mathcal{R}^*(d)$ and $\mathcal{R}^*(e)$, respectively.

Lemma 6 *Let k, ℓ, d and e be positive integers such that*

$$d = \left\lfloor \frac{m}{2k-\delta} \right\rfloor, \quad e = \left\lfloor \frac{m}{2\ell - \gamma} \right\rfloor,$$

where $0 < \delta, \gamma < 1$. Suppose that $d \leq e$. Then for every nontrivial character χ of $\mathcal{R}_M$ and any polynomial $a \in \mathcal{R}$, the character sum

$$\mathcal{S} = \sum_{\substack{f \in \mathcal{R}^*(d) \\ g \in \mathcal{R}^*(e)}} \chi\big((fg)^* + afg\big)$$

satisfies the bound $|\mathcal{S}| \leq |\mathcal{R}^*(d)|\,|\mathcal{R}^*(e)| \exp(\Delta)$, where

$$\Delta = \Big(-\frac{\delta m}{4k-2\delta} - \frac{\gamma m}{4\ell - 2\gamma} + k + \ell + d + 1\Big)\frac{\log q}{2k\ell} + \frac{(6k^3 + 6\ell^3)\log m}{k\ell}.$$

Proof Set $\mathcal{F} = \mathcal{R}^*(d)$ and $\mathcal{G} = \mathcal{R}^*(e)$. Since

$$(2k-1)d \leq \frac{(2k-1)}{(2k-\delta)}m < m, \quad (2\ell - 1)e \leq \frac{(2\ell - 1)}{(2\ell - \gamma)}m < m,$$

all of the conditions of Theorem 3 hold; thus

$$|\mathcal{S}| \leq |\mathcal{R}^*(d)|\,|\mathcal{R}^*(e)|\Delta',$$

https://doi.org/10.4153/CJM-2003-010-0 Published online by Cambridge University Press

where

$$(\Delta')^{2k\ell} = |\mathcal{R}^*(d)|^{-2k}|\mathcal{R}^*(e)|^{-2\ell}q^{m+d+1}(q-1)^{2k+2\ell}\mathcal{J}(2k,2kd)\mathcal{J}(2\ell,2\ell e).$$

The lemma now follows as in the proof of Lemma 5. ∎

For any $f \in \mathcal{R}$, we denote by $\{f\}$ the unique element of $\mathcal{R}_m$ such that $f \equiv \{f\} \pmod M$.

Theorem 7 *Let k, ℓ, d and e be positive integers such that*

$$d = \left\lfloor \frac{m}{2k-\delta} \right\rfloor, \quad e = \left\lfloor \frac{m}{2\ell-\gamma} \right\rfloor,$$

where $0 < \delta, \gamma < 1$. Suppose that $d \le e$. Fix a subset $\mathcal{E} \subset \{0,1,\dots,m-1\}$ of cardinality $|\mathcal{E}| = n$ and two polynomials $F, a \in \mathcal{R}$, and let $\mathcal{N}$ be the number of ordered pairs (f,g), with $f \in \mathcal{R}^*(d)$ and $g \in \mathcal{R}^*(e)$, such that $\{(fg)^* + afg\} \approx_{\mathcal{E}} F$. Then

$$\left| \mathcal{N} - \frac{|\mathcal{R}^*(d)|\,|\mathcal{R}^*(e)|}{q^n} \right| < |\mathcal{R}^*(d)|\,|\mathcal{R}^*(e)| \exp(\Delta),$$

where Δ is defined as in Lemma 6. In particular, if

$$n \le \frac{\delta m}{4k\ell(2k-\delta)} + \frac{\gamma m}{4k\ell(2\ell-\gamma)} - \frac{k+\ell+d+1}{2k\ell} - \frac{(6k^3+6\ell^3)\log m}{k\ell \log q},$$

then

$$0 < \mathcal{N} < 2 \cdot \frac{|\mathcal{R}^*(d)|\,|\mathcal{R}^*(e)|}{q^n}.$$

Proof Using Lemma 6, the proof is very similar to the proof of Theorem 6; details are left to the reader. ∎

Using Theorem 7, we can now give a proof of Theorem 2.

Proof Put $\lambda = (1/2)^{1/9} < 1$, and consider the collection $\mathcal{D}$ of pairs of integers (d,e) such that

$$\lambda m^{2/3+\epsilon}\log m \le \frac{2d}{\lambda} \le e \le m^{2/3+\epsilon}\log m.$$

For all such pairs, we have

$$\frac{2m^{1/3-\epsilon}}{\lambda \log m} \le \frac{m}{d} \le \frac{2m^{1/3-\epsilon}}{\lambda^2 \log m}, \quad \frac{m^{1/3-\epsilon}}{\log m} \le \frac{m}{e} \le \frac{m^{1/3-\epsilon}}{\lambda \log m}.$$

https://doi.org/10.4153/CJM-2003-010-0 Published online by Cambridge University Press

If $m \gg_\epsilon 1$, the closed intervals $[2m^{1/3-\epsilon}/(\lambda \log m), 2m^{1/3-\epsilon}/(\lambda^2 \log m)]$ and $[m^{1/3-\epsilon}/\log m, m^{1/3-\epsilon}/(\lambda \log m)]$ have lengths greater than $2 + (1 - \lambda)$. On the other hand, if (d, e) and $(d + 1, e + 1)$ lie in $\mathcal{D}$, then

$$\frac{m}{d} - \frac{m}{d+1} < \frac{m}{d^2} \leq \frac{4}{\lambda^4 m^{1/3+2\epsilon} (\log m)^2} < (1 - \lambda),$$
$$\frac{m}{e} - \frac{m}{e+1} < \frac{m}{e^2} \leq \frac{1}{\lambda^2 m^{1/3+2\epsilon} (\log m)^2} < (1 - \lambda),$$

provided that $m \gg_\epsilon 1$. Consequently, for some $(d, e) \in \mathcal{D}$, there exist integers k and ℓ such that m/d lies in the open interval $\big(2k - 1, 2k - 1 + (1 - \lambda)\big)$, and m/e lies in the open interval $\big(2\ell - 1, 2\ell - 1 + (1 - \lambda)\big)$. Let k, ℓ, d and e be fixed with these properties, and set $\delta = 2k - m/d$, $\gamma = 2\ell - m/e$. Then $\lambda < \delta, \gamma < 1$, and

$$k = \frac{m}{2d} + \frac{\delta}{2} > 0, \quad \ell > \frac{m}{2e} + \frac{\gamma}{2} > 0,$$

thus all of the conditions of Theorem 7 are satisfied. Applying the theorem, we see that $\mathcal{N} > 0$ if $|\mathcal{E}|$ is less than or equal to

$$\frac{\delta m}{4k\ell(2k - \delta)} + \frac{\gamma m}{4k\ell(2\ell - \gamma)} - \frac{k + \ell + d + 1}{2k\ell} - \frac{(6k^3 + 6\ell^3) \log m}{k\ell \log q}.$$

Since

$$\frac{\gamma m}{(2\ell - \gamma)} = \gamma e > \lambda e \geq 2d,$$

it follows that $\mathcal{N} > 0$ provided that

$$|\mathcal{E}| \leq \frac{\delta m}{4k\ell(2k - \delta)} - \frac{k + \ell + 1}{2k\ell} - \frac{(6k^3 + 6\ell^3) \log m}{k\ell \log q}. \tag{13}$$

Now for $m \gg_\epsilon 1$, we have

$$k < \frac{m}{2d} + \frac{1}{2} \leq \frac{m^{1/3-\epsilon}}{\lambda^2 \log m} + \frac{1}{2} < \frac{m^{1/3-\epsilon}}{\lambda^3 \log m},$$

and

$$\ell < \frac{m}{2e} + \frac{1}{2} \leq \frac{m^{1/3-\epsilon}}{2\lambda \log m} + \frac{1}{2} < \frac{m^{1/3-\epsilon}}{2\lambda^2 \log m}.$$

Consequently,

$$\frac{\delta m}{4k\ell(2k - \delta)} = \frac{\delta d}{4k\ell} > \frac{(\lambda^3 m^{2/3+\epsilon} \log m)/2}{4\big(m^{1/3-\epsilon}/(\lambda^3 \log m)\big)\big(m^{1/3-\epsilon}/(2\lambda^2 \log m)\big)},$$

that is,

$$\frac{\delta m}{2k^2(2k - \delta)} > \frac{\lambda^8 m^{3\epsilon} (\log m)^3}{4}.$$

https://doi.org/10.4153/CJM-2003-010-0 Published online by Cambridge University Press

We also have

$$-\frac{k+\ell+1}{2k\ell} > -\frac{3}{2}.$$

Finally, since

$$k\ell > \frac{m}{2d}\cdot\frac{m}{2e} \geq \frac{m^2}{(\lambda m^{2/3+\epsilon}\log m)(2m^{2/3+\epsilon}\log m)} = \frac{m^{2/3-2\epsilon}}{2\lambda(\log m)^2},$$

it follows that

$$-\frac{(6k^3+6\ell^3)\log m}{k\ell\log q} > -\Big(\frac{3}{\lambda^{10}}+\frac{3}{8\lambda^7}\Big)\frac{m^{1/3-\epsilon}}{\log q} > -\frac{8m^{1/3-\epsilon}}{\log q}.$$

Thus the right side of (13) is bounded below by

$$\frac{\lambda^8 m^{3\epsilon}(\log m)^3}{4} - \frac{8m^{1/3-\epsilon}}{\log q} - \frac{3}{2},$$

and this is bounded below by

$$\frac{\lambda^9 m^{3\epsilon}(\log m)^3}{4} = \frac{m^{3\epsilon}(\log m)^3}{8}$$

provided that

$$\log q > \frac{32m^{1/3-\epsilon}}{(\lambda^8-\lambda^9)m^{3\epsilon}(\log m)^3 - 6}.$$

The theorem follows. ∎

References

[1] W. Banks and I. E. Shparlinski, *Distribution of inverses in polynomial rings*. Indag. Math. **12**(2001), 303–315.

[2] J. Friedlander and H. Iwaniec, *The Brun-Titchmarsh theorem*. Analytic Number Theory, Lond. Math. Soc. Lecture Note Series **247**(1997), 363–372.

[3] C.-N. Hsu, *The Brun-Titchmarsh theorem in function fields*. J. Number Theory **79**(1999), 67–82.

[4] A. A. Karatsuba, *Fractional parts of functions of a special form*. Izv. Akad. Nauk Ser. Mat., Transl. as Russian Acad. Sci. Izv. Math. (4) **55**(1995), 61–80.

[5] ———, *Analogues of Kloosterman sums*. (Russian), Izv. Ross. Akad. Nauk Ser. Mat. (5) **59**(1995), 93–102.

Department of Mathematics
University of Missouri
Columbia, Missouri 65211
USA
e-mail: bbanks@math.missouri.edu
harchars@math.missouri.edu

Department of Computing
Macquarie University
Sydney, NSW 2109
Australia
e-mail: igor@ics.mq.edu.au

https://doi.org/10.4153/CJM-2003-010-0 Published online by Cambridge University Press