Ann. Sc. Norm. Super. Pisa Cl. Sci. (5)
Vol. XXI (2020), 931-941

Binomial exponential sums

IGOR E. SHPARLINSKI AND JOSÉ FELIPE VOLOCH

Abstract. We obtain new bounds of exponential sums modulo a prime p with binomials $ax^k + bx^n$. In particular, for $k = 1$, we improve the bound of Karatsuba (1967) from $O(n^{1/4}p^{3/4})$ to $O\left(p^{3/4} + n^{1/3}p^{2/3}\right)$ for any n, and then use it to improve the bound of Akulinichev (1965) from $O(p^{5/6})$ to $O(p^{4/5})$ for $n|(p-1)$. The result is based on a new bound on the number of solutions and of degrees of irreducible components of certain equations over finite fields.

Mathematics Subject Classification (2010): 11T06 (primary); 11T23, 14G15 (secondary).

1. Introduction

1.1. Background and motivation

For a prime p we consider the binomial exponential sums

$$S_{k,n}(a, b) = \sum_{x=0}^{p-1} \mathbf{e}_p \left(ax^k + bx^n\right)$$

(where $\mathbf{e}_p(x) = e^{2\pi i x/p}$) with positive integers k and n and arbitrary integer coefficients a and b.

There are several bounds and applications of such sums which go beyond the classical Weil bound, see [1, 5, 6, 9–12, 15] and references therein. In particular, bounds for such binomial sums played a key role in the approach and resolution in [5, 7, 12, 14] to the conjecture of Goresky and Klapper [13] and in the closely related generalised Lehmer conjecture [6]; for very recent development and generalisations see [2, 8].

A standard technique relates bounding these sums to bounding the number of solutions of certain equations over finite fields. Previous papers have used the

The first author was supported by the ARC Grants DP170100786 and DP180100201.
Received November 09, 2018; accepted in revised form April 16, 2019.
Published online December 2020.

Weil bound, see [16], when applicable as well as elementary bounds coming from Bezout's theorem, in the range where Weil's bound becomes trivial, to bound the number of solutions of these equations. Here, we obtain sharper bounds to the number of solutions of these equations.

The novelty of our approach consists of a combination of two ideas. First, we use the method of [20] (and particularly the explicit version for plane curves from [22]) that give improvements of the Weil bound for large degrees. Second, and perhaps more importantly, the equations we need to study are sometimes not irreducible and we need to bound from below the degrees of their irreducible components and consequently the number of these components. This is achieved by using ABC-type bounds for solutions of equations over *function fields* using the methods of [21]. A connection between irreducible factors and the polynomial ABC-results for $f(X) - f(Y)$ where $f(X)$ is a one-variable sparse polynomial in characteristic zero, is due to Zannier [23]. We have transposed this technique to positive characteristic for the same kind of polynomials in [19]. Here we extend this to a wider class of polynomials while sharpening the method and give applications to new bounds of binomial exponential sums $S_{k,n}(a, b)$. We expect this method to have wider applications.

1.2. Set-up and some previous results

Define

$$M_{k,n} = \max_{\substack{a,b\in\mathbb{Z}\\ \gcd(ab,p)=1}} \left|S_{k,n}(a, b)\right|.$$

In the special case $k = 1$ we set

$$M_n = M_{1,n}.$$

We also recall the bound of Karatsuba [15, Theorem 1]

$$M_n \le (n-1)^{1/4} p^{3/4}, \tag{1.1}$$

which holds for any $n \ge 1$. Furthermore, Akulinichev [1, Theorem 1] has shown that

$$M_n \le p/\sqrt{\gcd(n, p-1)}. \tag{1.2}$$

In particular combining (1.1) and (1.2) we see that if $n \mid p-1$ then

$$M_n \le p^{5/6}, \tag{1.3}$$

see [1, Corollary]. Here we improve (1.1) for an arbitrary n and then use it to improve (1.3) and obtain

$$M_n = O(p^{4/5}),$$

in the case when $n \mid p-1$; see Corollary 3.3 below.

Most of the above results are based on new upper bounds on the number $T_{k,n}$ of solutions to the system of equations

$$u^k + v^k = x^k + y^k \qquad \text{and} \qquad u^n + v^n = x^n + y^n, \qquad u, v, x, y \in \mathbb{F}_p,$$

over the finite field $\mathbb{F}_p$ of p elements. As before, in the special case $k = 1$ we define

$$T_n = T_{1,n}.$$

For example, Bourgain, Cochrane, Paulhus and Pinner [5, Theorem 3] have shown that if

$$\gcd(n, p-1) = 1 \qquad \text{and} \qquad \gcd(n-1, p-1) \le \frac{9}{50} p^{16/23}$$

then

$$T_n \le 13658 p^{66/23}. \tag{1.4}$$

Cochrane and Pinner [12, Theorem 7.1] have sharpened the constant in the bound (1.4) and also extended it to $T_{k,n}$.

Here, in Section 2.2, we obtain new bounds. In particular, for $k = 1$ we improve in a wide range the trivial bound $T_n = O(np^2)$ (used in [15]). This bound is based on the investigation of irreducible factors of the polynomial

$$F_n(X, Y) = X^n + Y^n - (X + Y - 1)^n - 1 \in \mathbb{F}_p[X, Y], \tag{1.5}$$

which could be of independent interest, and also an application of some ideas and results from [20–22].

1.3. Notation

We recall that the notations $U = O(V)$, $U \ll V$ and $V \gg U$, are all equivalent to the statement that $|U| \le cV$ for some constant c, which is absolute throughout this work.

The letters k and n always denote integer numbers and the letter p always denotes a prime.

ACKNOWLEDGEMENTS. The authors are very grateful to R. Popovych for the calculations mentioned above and to the referee for the very careful reading of the manuscript and especially for the suggestion to use [10, Theorem 1.2] which has led to an improvement of our original version of Theorem 3.4.

The second author would like to thank UNSW for the hospitality during which part of this work was done.

2. Factors and zeros of some polynomials

2.1. Lower bounds on the degree of irreducible factors

We use some basic facts about the divisors on curves, which can be found in [16].

Lemma 2.1. *Let $\mathcal{X}$ be the smooth projective model of a plane curve $h(x, y) = 0$ of degree d such that the homogeneous term of degree d of h is not divisible by x or y. Then x has degree d as a function on $\mathcal{X}$.*

Proof. The poles of x and y are among the branches above the points at infinity of the plane curve $h = 0$ and these points at infinity correspond to factors $x - \alpha y$ with $\alpha \neq 0$ of the homogeneous term of degree d of h, by the hypothesis. The function $x - \alpha y$ vanishes at the corresponding branches so if x has a pole at such a branch, y also has a pole there of the same order and vice versa. So x and y have the same polar divisor D. The functions $x^i y^j$, $i + j \leq m$, belong to the Riemann-Roch space $H^0(mD)$, see [16, page 306] and the linear relations among them come from multiples of h, so a standard calculation [16, page 329] gives $\dim H^0(mD) \geq md + O(1)$. On the other hand, the Riemann-Roch theorem, see [16, Chapter IX], gives $\dim H^0(mD) = m \deg D + O(1)$ and it follows that $\deg x = \deg D \geq d$. But it is clear that $\deg x \leq d$ and this completes the proof. □

We now extend the definition of the polynomial $F_n(X, Y)$ in (1.5) to arbitrary ground fields

Lemma 2.2. *Let K be a field of positive characteristic p and let $n < p$. If $h(X, Y)$ is an irreducible polynomial factor of $F_n(X, Y) \in K[X, Y]$ of degree d, other than $X - 1$, $Y - 1$, $X + Y$, then $d \gg \min\{p/n, n\}$.*

Proof. Let $\mathcal{X}$ be a smooth model of the curve $h = 0$. The genus of $\mathcal{X}$ is at most $(d - 1)(d - 2)/2$. On $\mathcal{X}$, the functions x, y and $x + y - 1$ have at most d zeros and d poles (the latter on the line at infinity) so they are S-units for some set S of places of $\mathcal{X}$ with $\#S \leq 4d$. Consider the functions $u_1 = x^n$, $u_2 = y^n$, $u_3 = -(x+y-1)^n$, which are also S-units and satisfy the unit equation $u_1 + u_2 + u_3 = 1$.

The u_i are functions on $\mathcal{X}$ so $(u_1{:}u_2{:}u_3)$ defines a morphism $\mathcal{X} \to \mathbb{P}^2$ of degree at most dn. If $dn \geq p$, the desired result follows immediately. If $dn < p$, then [21, Theorem 4] holds with the same proof in characteristic $p > 0$ (as the morphism has classical orders by [20, Corollary 1.8]). Also $\deg u_1 = nd$ by Lemma 2.1 since h satisfies the hypothesis being a factor of $F_n(X, Y)/((X - 1)(Y - 1))$, so we get

$$nd \leq \deg u_1 \leq 3(d(d - 3) + 4d) \ll d^2$$

giving the result, provided u_1, u_2, u_3 are linearly independent over K.

If $au_1 + bu_2 + cu_3 = 0$ and $abc \neq 0$, then we consider the unit equation $-au_1/bu_2 - cu_3/bu_2 = 1$. We claim that the degree of $-au_1/bu_2$ is nd. This follows if we show that the degree of x/y is d. Now, x has d zeros counted with multiplicity, so the same will be true for x/y unless y vanishes at one of the zeros of x. This does not happen because $F_n(X, Y)$ does not vanish at the origin for n even and $F_n(X, Y)/(X + Y)$ does not vanish at the origin for n odd. So the same argument as before gives the inequality of the theorem.

If $c = 0$ then u_1/u_2 is constant so x/y is constant, say $y = \alpha x$. The equation $F_n(x, \alpha x) = 0$ has to be satisfied identically, which means by looking at the linear term that $\alpha = -1$, that is, $x + y = 0$ and the constant term forces n to be odd. If $a = 0$, a similar argument gives $x = 1$ and if $b = 0$ then $y = 1$. □

We now treat the more general polynomials

$$F_{k,n}(X, Y) = (X^n + Y^n - 1)^{k/r} - (X^k + Y^k - 1)^{n/r} \in \mathbb{F}_p[X, Y], \tag{2.1}$$

where k and n are distinct integers and $r = \gcd(k, n)$. They reduce to F_n when $k = 1$.

Unfortunately, the result that we obtain below about the components of the polynomials (2.1) is weaker than the corresponding statement for F_n. One reason is that Lemma 2.1 does not apply for $k > 1$.

Lemma 2.3. *Let K be a field of positive characteristic p and let $1 \le k, n < p$ be distinct integers and let $r = \gcd(k, n)$. If $h(X, Y)$ is an irreducible polynomial factor of $F_{k,n}(X, Y) \in K[X, Y]$ of degree d, other than a factor of $X^r - 1$, $Y^r - 1$ or $X^r + Y^r$, then*

$$d \ge \max\left\{\min\left\{p/k, \sqrt{k/3} - r\right\}, \min\left\{p/n, \sqrt{n/3} - r\right\}\right\}.$$

Proof. We proceed as in Lemma 2.2 and consider the curve $\mathcal{X}$. We define $u_1 = x^n, u_2 = y^n, u_3 = 1 - x^n - y^n$ so that they satisfy the unit equation $u_1 + u_2 + u_3 = 1$. Again, the poles of u_1, u_2, u_3 are among the at most d points at infinity of $\mathcal{X}$ with multiplicity at most n and that u_1 (respectively u_2) have zeros at the at most d zeros of x (respectively y). As for u_3, note that $u_3^{k/r} = (x^k + y^k - 1)^{n/r}$, which shows that each zero of u_3 has multiplicity divisible by n/r, as $\gcd(k/r, n/r) = 1$. Since u_3 has degree at most dn, it follows that u_3 has at most dr distinct zeros. Hence u_1, u_2, u_3 are S-units for a set S with $\#S \le (r + 3)d$. If $dn < p$ we can apply the unit equation bound, provided u_1, u_2, u_3 are linearly independent over K, to get $\deg u_1 \le 3(d(d - 3) + \#S) \le 3(d^2 + rd)$. If u_1 is not constant, then $\deg u_1 \ge n$ and we get $d \ge \sqrt{n/3} - r$. If u_1 is constant, then x is constant and it can be shown that h is a factor of $X^r - 1$, which was excluded.

If $au_1 + bu_2 + cu_3 = 0$ and $abc \ne 0$, then we consider the unit equation $-au_1/bu_2 - cu_3/bu_2 = 1$ and conclude as before if u_1/u_2 is not constant. We note that $abc = 0$ means some quotient of two of u_1, u_2, u_3 is constant. These possibilities are ruled out since they lead to h being a factor of $X^r - 1$, $Y^r - 1$ or $X^r + Y^r$. So we get $d \ge \min\{p/n, \sqrt{n/3} - r\}$.

Finally, reversing the roles of n and k gives the inequality $d \ge \min\{p/k, \sqrt{k/3} - r\}$ and completes the proof. □

2.2. Upper bounds on the number of zeros of some equations

We now derive bounds on

$$N_{k,n} = \#\left\{(x, y) \in \mathbb{F}_p^2 : \ F_{k,n}(x, y) = 0\right\},$$

where $F_{k,n}(X, Y) \in \mathbb{F}_p[X, Y]$ is the polynomial defined by (2.1).

We start with a bound on

$$N_n = N_{1,n}$$

which is based on Lemma 2.2.

Theorem 2.4. *We have*

$$N_n \ll p + n^{4/3} p^{2/3}.$$

Proof. Clearly there are

$$N_n^{(0)} \ll p, \tag{2.2}$$

points on the on linear factors $X - 1, Y - 1, X + Y$ of F_n.

Each of the remaining factors is of degree

$$d \gg \min\{p/n, n\}$$

by Lemma 2.2. Hence the number J of such irreducible factors is

$$J \ll \frac{\deg F_n}{\min\{p/n, n\}} \ll \max\{1, n^2/p\}.$$

The contribution to N_n from each irreducible factor $h \mid F_n$ of degree $d < p^{1/4}$ is $O(p)$ by the Weil bound (see [16]). Hence the total contribution $N_n^{(1)}$ from such factors can be estimated as

$$N_n^{(1)} \ll Jp \ll \max\{1, n^2/p\}p \ll \max\{p, n^2\}. \tag{2.3}$$

Each irreducible factor $h \mid F_n$ of degree $\deg h = d \geq p^{1/4}$ contributes $O\left(d^{4/3} p^{2/3}\right)$ by [22, Theorem (i)] and, in total they contribute

$$\begin{aligned} N_n^{(2)} &\ll \sum_{\substack{h \mid F_n, \text{irred} \\ \deg h \geq p^{1/4}}} (\deg h)^{4/3} p^{2/3} \leq \left(\sum_{\substack{h \mid F_n, \text{irred} \\ \deg h \geq p^{1/4}}} \deg h \right)^{4/3} p^{2/3} \\ &\leq n^{4/3} p^{2/3}, \end{aligned} \tag{2.4}$$

using the convexity of the function $z \mapsto z^{4/3}$.

Combining (2.2), (2.3) and (2.4) we obtain

$$N_n \leq N_n^{(0)} + N_n^{(1)} + N_n^{(2)} \ll p + n^2 + n^{4/3} p^{2/3}.$$

Since $n^2 \leq n^{4/3} p^{2/3}$ for $n \leq p$, the result follows. $\square$

Corollary 2.5. *We have*

$$T_n \ll p^2 + n^{4/3} p^{5/3}.$$

Proof. Eliminating u we obtain that T_n is equal to the number of solutions to the equation $x^n + y^n = v^n + (x + y - v)^n$. For $v = 0$ there are at most np values for $(x, y) \in \mathbb{F}_p^2$. If $v \neq 0$, then replacing $x \mapsto xv$, $y \mapsto yv$, we obtain $x^n + y^n = 1 + (x+y-1)^n$. Hence, by Theorem 2.4, we have $T_n \le np + pN_n \ll np + p^2 + n^{4/3} p^{5/3}$. Since $n \le p$, the result follows. □

For an arbitrary k our bound on $N_{k,n}$ is based on Lemma 2.3.

Theorem 2.6. *Let $1 \le k, n < p$ be distinct integers and let $r = \gcd(k, n)$ and assume that $r \le 0.5\sqrt{n}$. Then we have*

$$N_{k,n} \ll k\sqrt{n}p/r + (kn/r)^{4/3} p^{2/3}.$$

Proof. Let $s = \gcd(k, n, p-1) = \gcd(r, p-1)$. Clearly there are

$$N_{k,n}^{(0)} \ll sp \tag{2.5}$$

$\mathbb{F}_p$-rational points on the factors $X^r - 1$, $Y^r - 1$ or $X^r + Y^r$ of $F_{k,n}$.

Since $r \le 0.5\sqrt{n}$, each of the remaining factors is of degree

$$d \gg \min\{p/n, \sqrt{n/3} - r\} \gg \min\{p/n, \sqrt{n}\}$$

by Lemma 2.3. Hence, the number J of such irreducible factors is

$$J \ll \frac{\deg F_{k,n}}{\min\{p/n, \sqrt{n}\}} \ll \max\{k\sqrt{n}/r, kn^2/(pr)\}.$$

The contribution to $N_{k,n}$ from each irreducible factor $h \mid F_{k,n}$ of degree $d < p^{1/4}$ is $O(p)$ by the Weil bound (see [16]). Hence, similarly to (2.3), the total contribution $N_{k,n}^{(1)}$ from such factors can be estimated as

$$N_{k,n}^{(1)} \ll Jp \ll \max\{k\sqrt{n}/r, kn^2/(pr)\}p \ll \max\{k\sqrt{n}p/r, kn^2/r\}. \tag{2.6}$$

As in the proof of Theorem 2.4, we now use that each irreducible factor $h \mid F_{k,n}$ of degree $\deg h = d \ge p^{1/4}$ contributes $O\left(d^{4/3} p^{2/3}\right)$ by [22, Theorem (i)] and, in total they contribute similarly as in the bound (2.4), using that the degree of Fk, n is kn/r.

$$N_{k,n}^{(2)} \ll (kn/r)^{4/3} p^{2/3}, \tag{2.7}$$

using the convexity of the function $z \mapsto z^{4/3}$.

Combining (2.5), (2.6) and (2.7) we obtain

$$N_{k,n} \le N_{k,n}^{(0)} + N_{k,n}^{(1)} + N_{k,n}^{(2)} \ll sp + k\sqrt{n}p/r + kn^2/r + (kn/r)^{4/3} p^{2/3}.$$

Since $r \ll \min\{k, \sqrt{n}\}$ we have

$$s \le r \ll \sqrt{n} \ll k\sqrt{n}/r$$

and also $n \le p$ we have

$$kn^2/r \le n^2 \le n^{4/3}p^{2/3} \le (kn/r)^{4/3}p^{2/3}.$$

The result now follows. □

Corollary 2.7. *Let* $1 \le k, n < p$ *be distinct integers and let*

$$r = \gcd(k, n) \qquad \textit{and} \qquad s = \gcd(r, p-1).$$

Assume that $r \le 0.5\sqrt{n}$, *then we have*

$$T_{k,n} \ll k\sqrt{n}sp^2/r + (kn/r)^{4/3}sp^{5/3}.$$

Proof. Eliminating u we obtain that $T_{k,n} \le sR_{k,n}$ where $R_{k,n}$ is the number of solutions to the equation

$$(x^n + y^n - v^n)^{k/r} = (x^k + y^k - v^k)^{n/r}$$

(as for any fixed v, x, y the power u^r is uniquely defined and so u either $u = 0$ or can take at most $s = \gcd(r, p-1)$ values).

For $v = 0$ there are at most knp/r values for $(x, y) \in \mathbb{F}_p^2$. If $v \ne 0$, then replacing $x \mapsto xv$, $y \mapsto yv$, we obtain $(x^n + y^n - 1)^{k/r} = (x^k + y^k - 1)^{n/r}$. Hence, by Theorem 2.6, we have

$$\begin{aligned} T_{k,n} &\le sR_{k,n} \le s\left(knp/r + k\sqrt{n}p^2/r + (kn/r)^{4/3}p^{5/3}\right) \\ &\ll sknp/r + k\sqrt{n}sp^2/r + (kn/r)^{4/3}sp^{5/3}. \end{aligned}$$

Since $r \le k$ and $n \le p$, we obtain

$$T_{k,n} \ll k\sqrt{n}sp^2/r + (kn/r)^{4/3}sp^{5/3} \tag{2.8}$$

and the result follows. □

Using the trivial bound $s \le r$ we can simplify Corollary 2.7 as

$$T_{k,n} \ll k\sqrt{n}p^2 + (kn)^{4/3}r^{-1/3}p^{5/3}.$$

Furthermore, let d be the largest divisor of r with $\gcd(d, p-1) = 1$. If we set

$$k^* = k/d, \qquad n^* = n/d, \qquad r^* = r/d$$

then $r^* = \gcd(k^*, n^*)$ and $\gcd(r^*, p-1) = \gcd(r, p-1) = s$. Since $\gcd(d, p-1) = 1$, we clearly have $T_{k,n} = T_{k^*,n^*}$. Thus, using (2.8) with (k^*, n^*, r^*) in place of (k, n, r) we obtain

$$\begin{aligned} T_{k,n} &\ll k^*\sqrt{n^*}sp^2/r^* + (k^*n^*/r^*)^{4/3}sp^{5/3} \\ &= k\sqrt{nr^*}sp^2/(r^{3/2}) + (knr^*/r^2)^{4/3}sp^{5/3}, \end{aligned}$$

provided that $r^* \le 0.5\sqrt{n}$. Clearly that if r is squarefree that $r^* = s$ in which case we obtain yet another modification of Corollary 2.7

$$T_{k,n} \ll k\sqrt{n}s^{3/2}p^2r^{-3/2} + (kn)^{4/3}s^{7/3}p^{5/3}r^{-8/3}.$$

3. Exponential sums with binomials

3.1. Preparations

The following relation between $M_{k,n}$ and $T_{k,n}$ has appeared implicitly in several previous works. It is essentially based on the equality of the sums

$$S_{k,n}(a, b) = S_{k,n}\left(az, bz^n\right), \qquad z \in \mathbb{F}_p^*,$$

and the identity

$$\sum_{\lambda,\mu\in\mathbb{F}_p} \left|S_{k,n}(\lambda, \mu)\right|^4 = p^2T_n,$$

which follows from the orthogonality of exponential functions.

Here we present it in a form which is a special case of [10, Theorem 1.2].

Lemma 3.1. *Let $1 \le k, n < p$ be distinct integers. Then we have*

$$M_{k,n}^4 \le pT_{k,n}.$$

3.2. Bounds of exponential sums

Combining Corollary 2.5 with Lemma 3.1 (used with $k = 1$), we immediately obtain:

Theorem 3.2. *For $1 \le n < p$, we have*

$$M_n \ll p^{3/4} + n^{1/3}p^{2/3}.$$

Using the bound (1.2) for $n > p^{2/5}$ and Theorem 3.2 otherwise, we obtain

Corollary 3.3. *For any $n \mid p-1$, we have*

$$M_n \ll p^{4/5}.$$

Similarly, combining Corollary 2.7 with Lemma 3.1 we derive:

Theorem 3.4. *Let* $1 \le k, n < p$ *be distinct integers and let*

$$r = \gcd(k,n) \qquad \text{and} \qquad s = \gcd(r, p-1).$$

Assume that $r \le 0.5\sqrt{n}$*, then we have*

$$M_{k,n} \ll k^{1/4}n^{1/8}s^{1/4}p^{3/4}/r^{1/4} + (kn/r)^{1/3}s^{1/4}p^{2/3}.$$

Again, using the trivial bound $s \le r$ we derive from Theorem 3.4 that

$$M_{k,n} \ll k^{1/4}n^{1/8}p^{3/4} + (kn)^{1/3}r^{-1/12}p^{2/3}.$$

4. Comments

We note that in Lemma 2.3 regardless of whether $k < n$ or $k > n$ both lower bounds can be of use. However in other results, such as Theorems 2.6 and 3.4, without loss of generality we can assume that $k < n$.

A computer calculation for primes $p \le 67$ using Magma [4] verified that, except for $n = (p+1)/2$, the polynomials F_n, $2 \le n < p$, have a unique irreducible factor in addition to the trivial factors explicitly given in Lemma 2.2. For $n = (p+1)/2$, on the other hand, F_n factors completely into quadratic polynomials in addition to the trivial factors. R. Popovych has extended the calculation using Maple up to $p < 200$. There are two special cases where we can prove that the factorisation of F_n is as these calculations suggest, for all p. Namely, we can show that indeed $F_{(p+1)/2}$ factors completely into quadratic polynomials in addition to the trivial factors, while we can show, using the results of [3], that $F_{(p-1)/2}$ has a unique irreducible factor in addition to the trivial factors.

The polynomials $F_{k,n}$, $2 \le k < n < p \le 29$, however, all have a unique irreducible factor in addition to the trivial cyclotomic factors explicitly given in Lemma 2.3.

We also remark that our approach applies to binomial Laurent polynomials, that is, when one of k and n is negative.

Finally, we expect that our method can give new results fo exponential sums with trinomials and other sparse polynomials and Laurent polynomials, see [17,18].

References

[1] N. M. AKULINICHEV, *Estimates for rational trigonometric sums of a special type*, Doklady Acad. Sci. USSR, **161** (1965), 743–745 (in Russian).

[2] B. ALSULMI, T. COCHRANE, M. MOSSINGHOFF, V. PIGNO, C. PINNER, C. RICHARDSON and I. THOMPSON, *A generalization of the Goresky–Klapper conjecture, Part I*, SIAM J. Discrete Math. **32** (2018), 2973–3002.

[3] H. BORGES, G. COOK and M. COUTINHO, *Plane sections of Fermat surfaces over finite fields*, Finite Fields Appl. **52** (2018), 156–173.

[4] W. BOSMA, J. CANNON and C. PLAYOUST, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), 235–265.
[5] J. BOURGAIN, T. COCHRANE, J. PAULHUS and C. PINNER, *Decimations of ℓ-sequences and permutations of even residues* mod p, SIAM J. Discrete Math. **23** (2009), 842–857.
[6] J. BOURGAIN, T. COCHRANE, J. PAULHUS and C. PINNER, *On the parity of k-th powers modulo p. A generalization of a problem of Lehmer*, Acta. Arith. **147** (2011), 173–203.
[7] T. COCHRANE and S. V. KONYAGIN, *Proof of the Goresky-Klapper conjecture on decimations of ℓ-sequences*, SIAM J. Discrete Math. **25** (2011), 1812–1831.
[8] T. COCHRANE, M. MOSSINGHOFF, C. PINNER and C. RICHARDSON, *A generalization of the Goresky–Klapper conjecture, Part II*, Exp. Math., to appear.
[9] T. COCHRANE and C. PINNER, *Stepanov's method applied to binomial exponential sums*, Quart. J. Math. **54** (2003), 243–255.
[10] T. COCHRANE and C. PINNER, *An improved Mordell type bound for exponential sums*, Proc. Amer. Math. Soc. **133** (2005), 313–320.
[11] T. COCHRANE and C. PINNER, *Bounds on fewnomial exponential sums over $\mathbb{Z}_p$*, Math. Proc. Camb. Philos. Soc. **149** (2010), 217–227.
[12] T. COCHRANE and C. PINNER, *Explicit bounds on monomial and binomial exponential sums*, Quart. J. Math. **62** (2011), 323–349.
[13] M. GORESKY and A. KLAPPER, *Arithmetic crosscorrelations of feedback with carry shift register sequences*, IEEE Trans. Inform.Theory **43** (1997), 1342–1346.
[14] M. GORESKY, A. KLAPPER, R. MURTY and I. SHPARLINSKI, *On decimations of ℓ-sequences*, SIAM J. Discrete Math. **18** (2004), 130–140.
[15] A. A. KARATSUBA, *Estimates of complete trigonometric sums*, Mathem. Notes (Translated from Matem. Zametki) **1** (1967), 133–139 (in Russian).
[16] D. LORENZINI, "An Invitation to Arithmetic Geometry", Amer. Math. Soc., 1996.
[17] S. MACOURT, *Bounds on exponential sums with quadrinomials*, J. Number Theory **193** (2018), 118–127.
[18] S. MACOURT, I. D. SHKREDOV and I. E. SHPARLINSKI, *Multiplicative energy of shifted subgroups and bounds on exponential sums with trinomials in finite fields*, Canad. J. Math. **70** (2018), 1319–1338.
[19] I. SHPARLINSKI and J. F. VOLOCH, *Value sets of sparse polynomials*, Canad. Math. Bull. **63** (2020), 187–196.
[20] K. O. STÖHR and J. F. VOLOCH, *Weierstrass points and curves over finite fields*, Proc. London Math. Soc. **52** (1986), 1–19.
[21] J. F. VOLOCH, *Diagonal equations over function fields*, Bol. Soc. Bras. Mat. **16** (1985), 29–39.
[22] J. F. VOLOCH, *On the number of values taken by a polynomial over a finite field*, Acta Arith. **52** (1989), 197–201.
[23] U. ZANNIER, *On the number of terms of a composite polynomial*, Acta Arith. **127** (2007), 157–168.

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

School of Mathematics and Statistics
University of Canterbury
Private Bag 4800
Christchurch 8140, New Zealand
felipe.voloch@canterbury.ac.nz