

POLYNOMIAL GAUSS SUMS

STEPHEN D. COHEN, MICHAEL DEWAR, JOHN B. FRIEDLANDER, DANIEL PANARIO,
AND IGOR E. SHPARLINSKI

(Communicated by Wen-Ching Winnie Li)

ABSTRACT. A recent bound for exponential sums by Friedlander, Hansen and Shparlinski is extended to twisted exponential sums with general polynomial arguments. As a by-product a new result about perfect powers in certain products of polynomials is established.

1. INTRODUCTION

Denote by \mathbb{Z}_t the residue ring modulo t and by \mathcal{U}_t its group of units, that is, the collection of residue classes which are relatively prime to t . A sequence $\mathcal{Z} = (z_1, \dots, z_T)$ of T elements from \mathbb{Z}_t is called \mathcal{K} -invariant if $\mathcal{K} \subseteq \mathcal{U}_t$ is such that the sequence kz_1, \dots, kz_T , taken modulo t , is a permutation of the original sequence z_1, \dots, z_T for each $k \in \mathcal{K}$.

For a prime p and an integer a , define the additive character

$$\psi(z) = \exp(2\piiaz/p)$$

of \mathbb{F}_p . We also use $\chi(z)$ to denote a multiplicative character of \mathbb{F}_p^* , extended to the whole field \mathbb{F}_p by setting $\chi(0) = 0$. As usual χ is said to be of order s if s is the smallest positive integer for which $\chi^s = \chi_0$, the trivial multiplicative character. (We refer to [5] for an exhaustive description of multiplicative and additive characters, and other important notions of the theory of finite fields.)

Let ϑ be an integer of multiplicative order $t \geq 1$ modulo p . Given two polynomials $f(X), g(X) \in \mathbb{F}_p[X]$ and additive and multiplicative characters ψ and χ over \mathbb{F}_p , we define the twisted exponential sum

$$(1) \quad S_{\mathcal{Z}}(\chi, \psi; f, g) = \sum_{z_s \in \mathcal{Z}} \chi(f(\vartheta^{z_s})) \psi(g(\vartheta^{z_s}))$$

Received by the editors October 20, 2003.

2000 *Mathematics Subject Classification*. Primary 11L07, 11T23; Secondary 11B50, 11K31.

The second author was supported in part by an NSERC Undergraduate Student Research Award.

The third author was supported in part by NSERC grant A5123 and a Killam Research Fellowship.

The fourth author was supported in part by NSERC grant 238757.

The fifth author was supported in part by ARC grant A69700294.

over a \mathcal{K} -invariant set \mathcal{Z} for some set \mathcal{K} . (Of course, this sum also depends on ϑ but perhaps the notation is already sufficiently complicated.)

In the special case that $f(X) = g(X) = X$, if ϑ is a primitive root and $\mathcal{Z} = \mathcal{U}_p$, this is simply the Gauss sum. Further, when $g(X) = X$ and $f(X) = 1$, such sums have been estimated in [2, 3]. Here that method is modified to yield bounds for the more general sums $S_{\mathcal{Z}}(\chi, \psi; f, g)$. We remark that when the additive character influences the sum in a nontrivial way, then these sums can be treated in exactly the same way as the sums from [2, 3]. However, in the other case, that is, when either ψ is trivial or $g(X)$ is constant, one needs to use some new arguments to establish the applicability of the Weil bound. We anticipate that the ensuing result (Lemma 1) may have some other applications.

2. PRELIMINARIES

We start with the following statement which may be of independent interest.

Lemma 1. *Let $s > 1$ be an integer with $\gcd(s, p) = 1$. Also, for some $m \geq 1$, let $\{k_1, \dots, k_m\}$ be a set of m distinct positive integers with $\gcd(k_j, p) = 1$ for each $j \leq m$ and let $\{d_1, \dots, d_m\}$ be a further set of positive integers. Suppose that $f(X) \in \mathbb{F}_p[X]$ is a polynomial indivisible by X . We define*

$$F(X) = \prod_{j=1}^m f(X^{k_j})^{d_j}.$$

If $F(X)$ is an s -th power of a polynomial in $\mathbb{F}_p[X]$, then there is a factorisation $s = s_0 d_0$ and a polynomial $f_0(X) \in \mathbb{F}_p[X]$ such that $f(X) = f_0(X)^{s_0}$ and d_0 divides d_j for each $j \leq m$.

Proof. The proof proceeds by induction on s . First it is established for s prime, and then, using induction, for s composite.

Assume first that s is prime. Without loss of generality we can suppose that the standard decomposition of $f(X)$ in terms of distinct polynomials, irreducible over $\mathbb{F}_p[X]$, can be expressed as

$$f(X) = \prod_{i=1}^r f_i(X)^{t_i}, \quad 1 \leq t_i < s, \quad i = 1, \dots, r,$$

and also that $1 \leq d_j < s$, $j = 1, \dots, m$. Since the k_1, \dots, k_m are distinct, we can also suppose that $k_1 > \dots > k_m$. Moreover, let e_i be the order of the irreducible polynomial $f_i(X)$, $1 \leq i \leq r$. Because polynomials $f_i(X)$ are irreducible, this is also the order of each of the roots of f_i , $1 \leq i \leq r$. We can suppose the latter are ordered so that $e_1 \geq \dots \geq e_r$.

Evidently, the order of any root (or irreducible factor) of $f_i(X^{k_j})$, $1 \leq i \leq r$, $1 \leq j \leq m$, is a divisor of $k_j e_i$ (that is itself divisible by e_i). Certainly it does not exceed $k_j e_i$. Now, the result of Butler [1] implies, for example, that the polynomial $f_1(X^{k_1})$ has at least one irreducible factor of order $k_1 e_1 / l$ for each divisor l of k_1 relatively prime to e_1 . Take $l = 1$ to deduce the existence of an irreducible factor $g(X)$ of $f_1(X^{k_1})$ of order precisely $k_1 e_1 > k_j e_i$, $i \geq 1$, $j > 1$. Further, $f_1(X^{k_1}), \dots, f_r(X^{k_1})$ are pairwise relatively prime (since f_1, \dots, f_r are). It follows that the irreducible polynomial $g(X)$ is not a factor of any polynomial $f_i(X^{k_j})$

except $f_1(X^{k_1})$. Accordingly, g appears in the product F with precise multiplicity $t_1 d_1$, and this is indivisible by s . The result for s prime follows.

Now suppose s is composite. Let s_0 be the maximal divisor of s such that $f(X) = f_0(X)^{s_0}$, $f_0(X) \in \mathbb{F}_p[X]$. We can assume $s_0 \neq s$ (otherwise the result is trivial). Further, if $s_0 > 1$, we can use induction applied to f_0 with s replaced by s/s_0 to obtain the result. Hence we can suppose $s_0 = 1$.

Next, suppose $d_0 = \gcd(d_1, \dots, d_m, s) > 1$. If $d_0 = s$, then again the result is trivial. Further, if $1 < d_0 < s$, we replace s by s/d_0 and each d_i by d_i/d_0 . Apply induction to conclude that F cannot be an s -th power.

Consequently, we may suppose $s_0 = d_0 = 1$. Now take any prime divisor l of s and set $w = s/l$. Thus $1 < w < s$ (since s is composite). Trivially, $f(X) = g(X)^u$ for some polynomial $g(X) \in \mathbb{F}_p[X]$ and an integer $u|w$, only if $u = 1$, and $\gcd(d_1, \dots, d_m, w) = 1$ (since the corresponding assertions hold for s instead of w). By induction, with s replaced by w , F cannot be a w -th power and therefore cannot be an s -th power. □

We now recall Lemma 2 from [2].

Lemma 2. *Suppose that $\mathcal{K} \subseteq \mathcal{U}_t$ is a set of cardinality $|\mathcal{K}| = K$. Then, for any fixed $\delta > 0$ and any integer $h \geq t^\delta$ there exists an integer $r \in \mathcal{U}_t$ such that the congruence*

$$rk \equiv y \pmod{t}, \quad k \in \mathcal{K}, \quad 0 \leq y \leq h - 1,$$

has

$$L_r(h) \gg \frac{Kh}{t}$$

solutions, where the implied constant depends on δ .

We also need the Weil bound for character sums (see Theorem 3 of Chapter 6 of [4]).

Lemma 3. *Let $F(X)$ be a non-zero rational function over \mathbb{F}_p of degree m and let $G(X)$ be polynomial over \mathbb{F}_p of degree n . Let χ be a multiplicative character of \mathbb{F}_p^* of order $s \geq 1$ and let ψ be an additive character of \mathbb{F}_p . Assume that at least one of the following holds:*

- either χ is non-trivial and F is not an s -th power of a rational function over the algebraic closure of \mathbb{F}_p ;
- or ψ is non-trivial and G is not constant modulo p .

Then

$$\left| \sum_{x \in \mathbb{Z}_p} \chi(F(x))\psi(G(x)) \right| \leq (m + n - 1)p^{1/2}.$$

3. MAIN RESULTS

The following bound¹ is our main result. It provides a direct generalization of Lemma 4 from [2].

Theorem 4. *Let $\mathcal{Z} = (z_1, \dots, z_T)$ be a \mathcal{K} -invariant sequence of elements of \mathbb{Z}_t with respect to the set $\mathcal{K} \subseteq \mathcal{U}_t$ of cardinality $K = |\mathcal{K}|$ and let N be the number of*

¹At the risk of stating the obvious we mention that, by an expression such as $N^{1/2\nu}$, we mean $N^{1/(2\nu)}$ and not $N^{\nu/2}$.

solutions of the congruence $z_\ell \equiv z_r \pmod{t}$, $1 \leq \ell, r \leq T$. Let $f(X)$ and $g(X)$ be two polynomials over \mathbb{F}_p each of degree at most D . Assume that at least one of the following holds:

- either the multiplicative character χ is non-trivial of order s and f is not an s -th power of a rational function over the algebraic closure of \mathbb{F}_p ;
- or ψ is non-trivial and g is not constant modulo p .

If $t \geq p^{1/2+\varepsilon}$, then for any integer $\nu \geq 1$ the bound

$$|S_{\mathcal{Z}}(\chi, \psi; f, g)| \ll D^{1/2\nu} N^{1/2\nu} T^{1-1/\nu} K^{-1/2(\nu+1)} t^{1/2\nu} p^{1/4(\nu+1)}$$

holds, where the implied constant depends on ε and ν .

Proof. Fix some $\varepsilon > 0$ and put

$$h = \left\lceil tK^{-\nu/(\nu+1)}p^{-1/2(\nu+1)} \right\rceil.$$

In this case

$$h \geq t^{1/(\nu+1)}p^{-1/2(\nu+1)} \geq p^{\varepsilon/(\nu+1)},$$

thus Lemma 2 applies.

We select r as in Lemma 2. Let \mathcal{L} denote the subset of \mathcal{K} which satisfies the corresponding congruence and let $L = |\mathcal{L}|$.

Define $Q(x)$ as the number of elements $z \in \mathcal{Z}$ with $z \equiv x \pmod{t}$. Note that

$$\sum_{x \in \mathbb{Z}_t} Q(x) = T$$

and

$$\sum_{x \in \mathbb{Z}_t} Q(x)^2 = N.$$

We also have $Q(kx) = Q(x)$ for any $k \in \mathcal{K}$ since repetitions in \mathcal{Z} are preserved under the permutation of \mathcal{Z} generated by multiplication by $k \in \mathcal{K}$. Therefore

$$\begin{aligned} S_{\mathcal{Z}}(\chi, \psi; f, g) &= \sum_{z_s \in \mathcal{Z}} \chi(f(\vartheta^{z_s})) \psi(g(\vartheta^{z_s})) \\ &= \sum_{x \in \mathbb{Z}_t} Q(x) \chi(f(\vartheta^x)) \psi(g(\vartheta^x)) \\ &= \frac{1}{L} \sum_{k \in \mathcal{L}} \sum_{x \in \mathbb{Z}_t} Q(kx) \chi(f(\vartheta^{kx})) \psi(g(\vartheta^{kx})) \\ &= \frac{1}{L} \sum_{k \in \mathcal{L}} \sum_{x \in \mathbb{Z}_t} Q(x) \chi(f(\vartheta^{kx})) \psi(g(\vartheta^{kx})) \\ &= \frac{1}{L} \sum_{x \in \mathbb{Z}_t} Q(x) \sum_{k \in \mathcal{L}} \chi(f(\vartheta^{kx})) \psi(g(\vartheta^{kx})). \end{aligned}$$

Two applications of the Hölder inequality yield

$$\begin{aligned}
 & |S_{\mathcal{Z}}(\chi, \psi; f, g)|^{2\nu} \\
 & \leq L^{-2\nu} \left(\sum_{x \in \mathbb{Z}_t} Q(x) \left| \sum_{k \in \mathcal{L}} \chi(f(\vartheta^{kx})) \psi(g(\vartheta^{kx})) \right| \right)^{2\nu} \\
 & = L^{-2\nu} \left(\sum_{x \in \mathbb{Z}_t} (Q(x)^2)^{1/2\nu} Q(x)^{(\nu-1)/\nu} \left| \sum_{k \in \mathcal{L}} \chi(f(\vartheta^{kx})) \psi(g(\vartheta^{kx})) \right| \right)^{2\nu} \\
 & \leq L^{-2\nu} \sum_{x \in \mathbb{Z}_t} Q(x)^2 \left(\sum_{x \in \mathbb{Z}_t} Q(x) \right)^{2\nu-2} \sum_{x \in \mathbb{Z}_t} \left| \sum_{k \in \mathcal{L}} \chi(f(\vartheta^{kx})) \psi(g(\vartheta^{kx})) \right|^{2\nu} \\
 & = L^{-2\nu} NT^{2\nu-2} \sum_{x \in \mathbb{Z}_t} \left| \sum_{k \in \mathcal{L}} \chi(f(\vartheta^{kx})) \psi(g(\vartheta^{kx})) \right|^{2\nu}.
 \end{aligned}$$

Let $d = (p - 1)/t$. Then for each power ϑ^x , $x \in \mathbb{Z}_t$, there exist precisely d values of $z \in \mathcal{U}_p$ such that $\vartheta^x \equiv z^d \pmod{p}$. Therefore,

$$\begin{aligned}
 & \sum_{x \in \mathbb{Z}_t} \left| \sum_{k \in \mathcal{L}} \chi(f(\vartheta^{kx})) \psi(g(\vartheta^{kx})) \right|^{2\nu} \\
 & = d^{-1} \sum_{z \in \mathcal{U}_p} \left| \sum_{k \in \mathcal{L}} \chi(f(z^{dk})) \psi(g(z^{dk})) \right|^{2\nu} \\
 & \leq d^{-1} \sum_{z \in \mathbb{Z}_p} \left| \sum_{k \in \mathcal{L}} \chi(f(z^{dk})) \psi(g(z^{dk})) \right|^{2\nu} \\
 & \leq d^{-1} \sum_{j_1, \dots, j_\nu \in \mathcal{L}} \sum_{k_1, \dots, k_\nu \in \mathcal{L}} \\
 & \quad \times \sum_{z \in \mathbb{Z}_p} \chi \left(\prod_{i=1}^\nu \frac{f(z^{dj_i})}{f(z^{dk_i})} \right) \psi \left(\sum_{i=1}^\nu (g(z^{dj_i}) - g(z^{dk_i})) \right) \\
 & \leq d^{-1} \sum_{j_1, \dots, j_\nu \in \mathcal{L}} \sum_{k_1, \dots, k_\nu \in \mathcal{L}} \\
 & \quad \times \sum_{z \in \mathbb{Z}_p} \chi \left(\prod_{i=1}^\nu \frac{f(z^{drj_i})}{f(z^{drk_i})} \right) \psi \left(\sum_{i=1}^\nu (g(z^{drj_i}) - g(z^{drk_i})) \right),
 \end{aligned}$$

because $\gcd(r, t) = 1$.

We need to bound the inner sum. For those configurations where each of the integers $(k_1, \dots, k_\nu, j_1, \dots, j_\nu)$ occurs at least twice, we shall use the trivial bound. This gives a contribution of $O(L^\nu p)$.

The generic situation, where the above does not occur, trivially happens in at most $L^{2\nu}$ ways, and for each of these terms we wish to apply Lemma 3. In the case where we assume the additive character acts non-trivially that bound automatically applies due to our assumptions about ψ and g , since in particular we know that (k_1, \dots, k_ν) is not a permutation of (j_1, \dots, j_ν) .

In the remaining case the multiplicative character acts non-trivially, due to our assumptions about χ and f . Here, because we know that at least one of the integers k_i, j_i occurs with multiplicity one in the configuration, it follows from Lemma 1 that Lemma 3 applies.

Thus, in either case, each such term gives a contribution of $O(Ddh p^{1/2})$. Hence

$$\begin{aligned} |S_{\mathcal{Z}}(\chi, \psi; f, g)|^{2\nu} &\ll L^{-2\nu} d^{-1} N T^{2\nu-2} \left(L^\nu p + L^{2\nu} D d h p^{1/2} \right) \\ &\ll N T^{2\nu-2} \left(L^{-\nu} t + D h p^{1/2} \right). \end{aligned}$$

Therefore $S_{\mathcal{Z}}(\chi, \psi; f, g) \ll N^{1/2\nu} T^{1-1/\nu} \left(L^{-1/2} t^{1/2\nu} + h^{1/2\nu} D^{1/2\nu} p^{1/4\nu} \right)$. Basic manipulations and Lemma 2 yield the desired result. \square

4. APPLICATIONS

There are many examples of specific sequences \mathcal{Z} to which Theorem 4 applies. We provide bounds for the same sequences considered in [2]. In particular, for an integer $n \geq 2$ and $\lambda \in \mathcal{U}_t$ of multiplicative order T modulo t , we define

$$\begin{aligned} S_n(\chi, \psi; f, g) &= \sum_{x \in \mathbb{Z}_t} \chi \left(f \left(\vartheta^{x^n} \right) \right) \psi \left(g \left(\vartheta^{x^n} \right) \right), \\ S_n^*(\chi, \psi; f, g) &= \sum_{x \in \mathcal{U}_t} \chi \left(f \left(\vartheta^{x^n} \right) \right) \psi \left(g \left(\vartheta^{x^n} \right) \right), \\ U_\lambda(\chi, \psi; f, g) &= \sum_{x=1}^T \chi \left(f \left(\vartheta^{\lambda^x} \right) \right) \psi \left(g \left(\vartheta^{\lambda^x} \right) \right). \end{aligned}$$

For these sequences one now derives from Theorem 4 complete analogues of Theorems 6, 7 and 8 of [2] which for the sake of completeness we now formulate in the following form.

Theorem 5. *Let $f(X)$ and $g(X)$ be two polynomials over \mathbb{F}_p each of degree at most D . Assume that at least one of the following holds:*

- *either the multiplicative character χ is non-trivial of order s and f is not an s -th power of a rational function over the algebraic closure of \mathbb{F}_p ;*
- *or ψ is non-trivial and g is not constant modulo p .*

Let $n \geq 2$ and let $\lambda \in \mathcal{U}_t$ be of multiplicative order T modulo t . Then for any integer $\nu \geq 1$, the following bounds hold:

$$\begin{aligned} S_n(\chi, \psi; f, g) &\ll t^{3/4} p^{1/8+\varepsilon}, \\ S_n^*(\chi, \psi; f, g) &\ll \begin{cases} t^{3/4} p^{1/8+\varepsilon}, & \text{if } n = 2 \text{ or } t \text{ is cube-free,} \\ t^{1-\alpha(n)} p^{\alpha(n)/2+\varepsilon}, & \text{otherwise,} \end{cases} \\ U_\lambda(\chi, \psi; f, g) &\ll T^{1-(2\nu+1)/2\nu(\nu+1)} t^{1/2\nu} p^{1/4(\nu+1)}, \end{aligned}$$

where $\alpha(n)$ is given by

$$\alpha(n) = \frac{\lceil n/2 \rceil - 1}{n \lceil n/2 \rceil + 1}$$

and the implied constant depends on ε and ν .

REFERENCES

- [1] M. C. R. Butler, ‘The irreducible factors of $f(x^m)$ over a finite field’, *J. London Math. Soc.*, **30** (1955), 480–482. MR0071463 (17,130d)
- [2] J. B. Friedlander, J. Hansen, and I. E. Shparlinski, ‘On character sums with exponential functions’, *Mathematika*, **47** (2000), 75–85. MR1924489 (2003g:11089)
- [3] J. B. Friedlander, S. V. Konyagin and I. E. Shparlinski, ‘Some doubly exponential sums over \mathbb{Z}_m ’, *Acta Arith.*, **105** (2002), 349–370. MR1932568 (2004c:11147)
- [4] W. C. W. Li, *Number Theory with Applications*, World Scientific Publishing Co., Singapore, 1996. MR1390759 (98b:11001)
- [5] R. Lidl and H. Niederreiter, *Finite Fields*, Cambridge University Press, Cambridge, 1997. MR1429394 (97i:11115)

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF GLASGOW, GLASGOW G12 8QW, SCOTLAND,
UNITED KINGDOM

E-mail address: `sdc@maths.gla.ac.uk`

SCHOOL OF MATHEMATICS AND STATISTICS, CARLETON UNIVERSITY, OTTAWA, ONTARIO,
CANADA K1S 5B6

E-mail address: `mdewar@magma.ca`

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF TORONTO, TORONTO, ONTARIO, CANADA M5S
3G3

E-mail address: `frdlndr@math.toronto.edu`

SCHOOL OF MATHEMATICS AND STATISTICS, CARLETON UNIVERSITY, OTTAWA, ONTARIO,
CANADA K1S 5B6

E-mail address: `daniel@math.carleton.ca`

DEPARTMENT OF COMPUTING, MACQUARIE UNIVERSITY, SYDNEY, NSW 2109, AUSTRALIA

E-mail address: `igor@ics.mq.edu.au`