Mathematika 65 (2019) 505–529 © 2019 University College London
doi:10.1112/S0025579319000032

LINEAR AND QUADRATIC UNIFORMITY OF THE MÖBIUS FUNCTION OVER $\mathbb{F}_q[t]$

PIERRE-YVES BIENVENU AND THÁI HOÀNG LÊ

Abstract. We examine correlations of the Möbius function over $\mathbb{F}_q[t]$ with linear or quadratic phases, that is, averages of the form

$$\frac{1}{q^n}\sum_{\deg f<n}\mu(f)\chi(Q(f)) \tag{1}$$

for an additive character χ over $\mathbb{F}_q$ and a polynomial $Q\in\mathbb{F}_q[x_0,\dots,x_{n-1}]$ of degree at most 2 in the coefficients $x_0,\dots,x_{n-1}$ of $f=\sum_{i<n}x_it^i$. As in the integers, it is reasonable to expect that, due to the random-like behaviour of μ, such sums should exhibit considerable cancellation. In this paper we show that the correlation (1) is bounded by $O_\epsilon(q^{(-1/4+\epsilon)n})$ for any $\epsilon>0$ if Q is linear and $O(q^{-n^c})$ for some absolute constant $c>0$ if Q is quadratic. The latter bound may be reduced to $O(q^{-c'n})$ for some $c'>0$ when $Q(f)$ is a linear form in the coefficients of f^2, that is, a Hankel quadratic form, whereas, for general quadratic forms, it relies on a bilinear version of the additive-combinatorial Bogolyubov theorem.

§1. *Introduction.* Let p be a prime and $q=p^s$ be a prime power ($s\geqslant 1$). Let $\mathbb{F}_q$ be the field over q elements and $\mathbb{F}_q[t]$ be the ring of polynomials over $\mathbb{F}_q$. The Möbius function on $\mathbb{F}_q[t]$ is defined, as its counterpart in the integers, by

$$\mu(f)=\begin{cases}(-1)^k & \text{where } k \text{ is the number of monic irreducible factors of } f\\ & \text{if } f \text{ is squarefree,}\\ 0 & \text{otherwise.}\end{cases}$$

In the integers, a folklore conjecture predicts that μ is so random-like that it does not correlate with any bounded "reasonable" or "low-complexity" function F, in the sense that

$$\sum_{n\leqslant x}\mu(n)F(n)=o(x). \tag{2}$$

For instance, linear or quadratic phases, that is, functions F defined by $n\mapsto e(\alpha n)$ or $n\mapsto e(\alpha n^2)$, should satisfy equation (2). Davenport [5] proved such a statement for linear phases and Green and Tao for general nilsequences [7, 8]. We do not attempt to define nilsequences here, but note that they include sequences formed by regular polynomials such as $F(n)=e(\alpha n^2+\beta n+\gamma)$ as

Received 10 August 2018, published online 5 March 2019.
MSC (2010): 11B30 (primary), 11T55 (secondary).

https://doi.org/10.1112/S0025579319000032 Published online by Cambridge University Press

well as "generalized polynomials" such as $F(n) = e(\lfloor n\alpha \rfloor n\beta)$. Together with Green and Tao's work [6] on the inverse theorem for the Gowers U^3 norm, this implies that $\|\mu\|_{U^3(N)} = o_{N\to+\infty}(1)$.

In this paper we examine similar correlations over $\mathbb{F}_q[t]$, that is, we aim to show that

$$\sum_{\deg f<n} \mu(f)F(f) = o(q^n)$$

for "reasonable" functions F. Quadratic and linear phases correspond to functions of the form $\chi(Q(f))$ for an additive character χ over $\mathbb{F}_q$ and a polynomial $Q \in \mathbb{F}_q[x_0, \dots, x_{n-1}]$ of degree at most 2 in the coefficients $(x_0, \dots, x_{n-1}) \in \mathbb{F}_q^n$ of $f = \sum_{i<n} x_i t^i$. Recall that the group $\widehat{\mathbb{F}_q}$ of additive characters is isomorphic to (the additive group of) $\mathbb{F}_q$. To express the isomorphism, let $\mathrm{Tr} : \mathbb{F}_q \to \mathbb{F}_p$ be the trace map. For $a \in \mathbb{F}_q$, let us denote

$$e_q(a) = \exp\left(\frac{2\pi i \,\mathrm{Tr}(a)}{p}\right).$$

Then the isomorphism $\mathbb{F}_q \to \widehat{\mathbb{F}_q}$ is given by $r \mapsto \chi_r$, where, for any $r \in \mathbb{F}_q$, the character χ_r is defined by $\chi_r(x) = e_q(rx)$.

We now state our main results.

THEOREM 1. *For any $\epsilon > 0$ and $\chi \in \widehat{\mathbb{F}_q}$, for any linear form $\ell \in \mathbb{F}_q[x_0, \dots, x_{n-1}]$, we have*

$$\sum_{\deg f<n} \mu(f)\chi(\ell(f)) \ll_{\epsilon,q} q^{(3/4+\epsilon)n} \tag{3}$$

uniformly in n and ℓ.

It suffices to prove Theorem 1 for $\chi = \chi_1$. In the integer case, Davenport [5] showed that for any $A > 0$, we have

$$\sum_{n=1}^{N} \mu(n)e(n\alpha) \ll_A N(\log N)^{-A}$$

uniformly in $\alpha \in \mathbb{R}/\mathbb{Z}$, where the implied constant is ineffective due to the possible existence of Siegel zeroes. Under the generalized Riemann hypothesis (GRH), the best result is due to Baker and Harman [1] and Montgomery and Vaughan (unpublished), who showed that, for any $\epsilon > 0$,

$$\sum_{n=1}^{N} \mu(n)e(n\alpha) \ll_\epsilon N^{3/4+\epsilon} \tag{4}$$

uniformly in $\alpha \in \mathbb{R}/\mathbb{Z}$. Our exponent $\frac{3}{4}+\epsilon$ in (3) matches the one in (4) (though it is reasonable to conjecture that in both cases the best exponent is $\frac{1}{2}+\epsilon$). However, our proof of (3) differs from that of (4) in some respects. In particular, our proof of (3) uses L-functions of *arithmetically distributed relations* introduced by Hayes [9] as opposed to Dirichlet L-functions. We remark that very recently and independently of us, Porritt [15] has proved a result similar to Theorem 1.

https://doi.org/10.1112/S0025579319000032 Published online by Cambridge University Press

Regarding quadratic polynomials, we have the following similar, but weaker, result. It depends on the polylogarithmic bilinear Bogolyubov theorem [**11**, Theorem 1.3], a quantitative improvement of a structural result in additive combinatorics, the bilinear Bogolyubov theorem from our companion paper [**3**]. We introduce this theorem in §2.3.

THEOREM 2. *Assume that $p > 2$. There exists a constant $c > 0$ such that the following holds. For any $\chi \in \widehat{\mathbb{F}_q}$, we have*

$$\frac{1}{q^n} \sum_{\deg f < n} \mu(f)\chi(Q(f)) \ll_q q^{-n^c} \tag{5}$$

uniformly in n and the quadratic polynomial Q in $\mathbb{F}_q[x_0, \dots, x_{n-1}]$.

Note that the quality of (5) is superior to Green and Tao's bound for nilsequences in [**8**], namely that if $s(n)$ is a nilsequence, then, for any $A > 0$, one has

$$\sum_{n=1}^{N} \mu(n)s(n) \ll_{s,A} N \log^{-A} N. \tag{6}$$

We have another result for quadratic phases similar to $n \mapsto e(\alpha n^2 + \beta n)$. In this case, our bound is easier to prove and gives a polynomial saving. We need some extra notation to state our result (see §2.1 for more precise definitions). On $\mathbb{F}_q[t]$, there is a natural norm $|f| = q^{\deg f}$. The completion of $\mathbb{F}_q[t]$ with respect to this norm is $\mathbb{F}_q((1/t))$, the ring of formal Laurent series in $1/t$. On $\mathbb{F}_q((1/t))$, we define the additive character $e(\alpha) = e_q((\alpha)_{-1})$, where $(\alpha)_{-1}$ denotes the coefficient of t^{-1} in α.

THEOREM 3. *There exists a constant $\epsilon > 0$ (independent of q) such that*

$$\sum_{\deg f < n} \mu(f)e(\alpha f^2 + \beta f) \ll_q q^{(1-\epsilon)n} \tag{7}$$

uniformly in n and $\alpha, \beta \in \mathbb{F}_q((1/t))$.

Note that we do not require $p > 2$ in Theorem 3, since when $p = 2$ the map $f \mapsto (\alpha f^2 + \beta f)_{-1}$ is linear and Theorem 3 follows from Theorem 1. When p is odd, the symmetric matrix of the quadratic form $f \mapsto (\alpha f^2)_{-1}$ is a *Hankel matrix*, i.e., a matrix whose (i, j)th entry depends only on $i + j$. Thus, Theorem 3 can be reformulated in terms of Hankel matrices alone. We remark that in the integers, under GRH we have bounds with polynomial savings for the sum $\sum_{n=1}^{N} \mu(n)e(\alpha n^k)$ (see [**10**, **20**]).

We point out that the motivation to tackle correlations with quadratic phases, as for the corresponding result in the integers, is the derivation of Gowers norms estimates $\|\mu\|_{U^3(\mathbb{F}_q^n)} = o(1)$, where the set of polynomials of degree less than n is identified with $\mathbb{F}_q^n$. We refrain from defining Gowers norms here and refer instead to [**19**] for a general theory, but we highlight that the bound $\|\mu\|_{U^3(\mathbb{F}_q^n)} = o(1)$ allows one to control various linear autocorrelations of μ; for instance, it

https://doi.org/10.1112/S0025579319000032 Published online by Cambridge University Press

implies that

$$\sum_{\deg f, \deg g < n} \mu(f)\mu(f+g)\mu(f+2g)\mu(f+3g) = o(q^{2n}).$$

For $p > 2$, it was shown by Green and Tao [6] that the norm $\|\cdot\|_{U^3(\mathbb{F}_p^n)}$ is controlled by correlations with quadratic polynomials[1].

However, Theorem 2 only yields a Gowers norm estimate when $q = p$ is a prime. To see this, fix a group isomorphism $\phi : \mathbb{F}_q \to \mathbb{F}_p^s$ and let $\phi_n : \mathbb{F}_q^n \to \mathbb{F}_p^{sn}$ be the group isomorphism it induces in dimension n. For $f \in \mathbb{F}_q^n$, write $\tilde{f} = \phi_n(f)$. Observe that not every $\mathbb{F}_p$-quadratic form $P(\tilde{f})$ can be realized as $\mathrm{Tr}(Q(f))$ for some $\mathbb{F}_q$-quadratic form $Q(f)$; this can be seen by simple counting. But controlling $\|\mu\|_{U^3(\mathbb{F}_q^n)}$ precisely requires control of correlations of μ with any $\mathbb{F}_p$-quadratic form $P(\tilde{f})$, whereas Theorem 2 only deals with $\mathbb{F}_q$-quadratic forms.

The organization of the paper is as follows. In §2 we collect necessary facts that will be used in the proofs; in particular, we introduce and motivate Hayes' theory as well as the bilinear Bogolyubov theorem (Theorem 5). In §3 we prove a character sum estimate, using standard complex analysis as well as Hayes' theory, and exploit it to infer Theorem 1 in §4. In §5 we use Vaughan's identity to reduce Theorem 2 to a problem in bilinear and quadratic algebra and prove it in §6 using Theorem 5. Finally, we derive the bound (5) for the Hankel case in §7, that is, Theorem 3.

§2. *Preliminaries.*

2.1. *Notation and basic facts.* A useful reference for the circle method in function fields, of which the basics are sketched below, is [14]. Let $\mathbb{F}_q(t)$ be the field of fractions of $\mathbb{F}_q[t]$. On $\mathbb{F}_q(t)$, we can define a norm by $|f/g| = q^{\deg f - \deg g}$ with the convention $\deg 0 = -\infty$. The completion of $\mathbb{F}_q(t)$ with respect to this norm is

$$\mathbb{F}_q\left(\left(\frac{1}{t}\right)\right) = \left\{\alpha = \sum_{i=-\infty}^{n} a_i t^i : n \in \mathbb{Z}, a_i \in \mathbb{F}_q \text{ for every } i\right\},$$

the set of formal Laurent series in $1/t$. It is easy to see that if α is as above and $a_n \neq 0$, then $|\alpha| = q^n$.

Then $\mathbb{F}_q[t] \subset \mathbb{F}_q(t) \subset \mathbb{F}_q((1/t))$, and $\mathbb{F}_q[t]$, $\mathbb{F}_q(t)$ and $\mathbb{F}_q((1/t))$ are the analogues of $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{R}$, respectively.

Let us put $\mathbb{T} = \{\alpha \in \mathbb{F}_q((1/t)) : |\alpha| < 1\}$. This is analogous to the usual torus $\mathbb{R}/\mathbb{Z}$. Let $\mathrm{Tr} : \mathbb{F}_q \to \mathbb{F}_p$ be the trace map. For $a \in \mathbb{F}_q$, let us denote

$$e_q(a) = \exp\left(\frac{2\pi i \,\mathrm{Tr}(a)}{p}\right).$$

This is an additive character on $\mathbb{F}_q$. All additive characters on $\mathbb{F}_q$ are given by $a \mapsto e_q(ra)$ for some $r \in \mathbb{F}_q$.

[1] This actually holds for $p = 2$ as well thanks to a theorem of Samorodnitsky [17].

https://doi.org/10.1112/S0025579319000032 Published online by Cambridge University Press

For $\alpha \in \mathbb{F}_q((1/t))$, we write $(\alpha)_{-1}$ to denote the coefficient of t^{-1} in α. We define $e(\alpha) = e_q((\alpha)_{-1})$. This is an additive character on $\mathbb{F}_q((1/t))$ and allows us to do Fourier analysis on $\mathbb{F}_q[t]$. It is analogous to the function $x \mapsto e^{2\pi i x}$ with a few differences. For example, $e(\alpha) = 1$ does *not* imply that $\alpha \in \mathbb{F}_q[t]$. All additive characters on $\mathbb{F}_q[t]$ are given by $f \mapsto e(f\alpha)$ for some $\alpha \in \mathbb{T}$.

We denote by M the set of all monic polynomials in $\mathbb{F}_q[t]$, A_n the set of all polynomials of degree n which are monic, G_n the set of all polynomials (not necessarily monic) of degree less than n and $\mathcal{I}$ the set of all monic, irreducible polynomials. We use the convention that $\sum_{\deg f=l}$ means $\sum_{f\in A_l}$ (that is, a sum over monic polynomials).

The von Mangoldt function on $\mathbb{F}_q[t]$ is defined by

$$\Lambda(f) = \begin{cases} \deg P & \text{if } f = P^k \text{ for some monic irreducible } P \text{ and } k \geqslant 1, \\ 0 & \text{otherwise.} \end{cases}$$

Recall that the "prime number theorem" on $\mathbb{F}_q[t]$ reads

$$\sum_{\deg f=l} \Lambda(f) = q^l.$$

2.2. *L-functions of arithmetically distributed relations.* To prove Theorem 1, we first observe that any linear form on G_n can be represented as a map $f \mapsto (\alpha f)_{-1}$ for some $\alpha \in \mathbb{T}$. Thus, Theorem 1 can be rephrased as a bound for sums of the form

$$\sum_{f\in G_n} \mu(f)e(\alpha f)$$

or, equivalently and more conveniently, of the form

$$\sum_{f\in A_n} \mu(f)e(\alpha f).$$

Now, if α is approximated by a fraction a/Q of polynomials up to a remainder $\beta = \sum_{i=-\infty}^{-l} \beta_i t^i$ for some $l \geqslant 2$, that is, $\alpha = a/Q + \beta$, then $e(\alpha f) = e(af/Q)e(\beta f)$ depends only on the residue class of f modulo Q and the coefficients of the terms of degrees at least $l-1$ of $f = \sum_{i=1}^{n} a_i t^{n-i} + t^n$. We refer to $a_1, \ldots, a_l$ as the first l coefficients of f (if $i > n$, then we define $a_i = 0$). We thus need to understand functions on A_n that only depend on the congruence class modulo a fixed modulus Q and the first l coefficients. Hence, for $l \geqslant 0$, $Q \in \mathbb{F}_q[t]$, we define an equivalence relation $R_{l,Q}$ on M as follows:

$$f \equiv g \pmod{R_{l,Q}} \text{ if } f \equiv g \pmod{Q} \text{ and the first } l \text{ coefficients of } f \text{ and } g \text{ are the same.}$$

It is an example of an *arithmetically distributed relation*, of which Hayes [9, §8] developed the theory, which we briefly review. The relevant facts can also be found in [12] or [4].

It is easy to check that $M/R_{l,Q}$ is a semigroup with respect to multiplication on $\mathbb{F}_q[t]$. The equivalence class of a polynomial $f \in \mathbb{F}_q[t]$ is invertible in $M/R_{l,Q}$ if and only if $(f, Q) = 1$.

https://doi.org/10.1112/S0025579319000032 Published online by Cambridge University Press

Put $G_{l,Q} := (M/R_{l,Q})^\times$, the set of invertible elements. This is a group of cardinality $q^l\phi(Q)$, where $\phi(Q) = \#(\mathbb{F}_q[t]/(Q))^\times$. Note that $G_{0,Q}$ is simply $(\mathbb{F}_q[t]/(Q))^\times$.

For a character λ on $G_{l,Q}$, we extend it to all of M by setting $\lambda(f) = 0$ if $(f, Q) \neq 1$. We define the L-function associated with λ as

$$L(s, \lambda) = \sum_{f \in M} \lambda(f) \frac{1}{|f|^s},$$

which converges absolutely for $\Re(s) > 1$. It is convenient to put

$$\mathcal{L}(z, \lambda) = \sum_{f \in M} \lambda(f) z^{\deg(f)} = \sum_{n=1}^{\infty} z^n \sum_{f \in A_n} \lambda(f). \tag{8}$$

Then $L(s, \lambda) = \mathcal{L}(q^{-s}, \lambda)$. We have the Euler product formula

$$\mathcal{L}(z, \lambda) = \prod_{P \in \mathcal{I}} (1 - \lambda(P) z^{\deg P})^{-1} \tag{9}$$

for $|z| < 1/q$.

In the same range of z, we also have

$$\frac{1}{\mathcal{L}(z, \lambda)} = \prod_{P} (1 - \lambda(P) z^{\deg P}) = \sum_{f \in M} \mu(f)\lambda(f) z^{\deg f} = \sum_{n=1}^{\infty} z^n \sum_{f \in A_n} \mu(f)\lambda(f). \tag{10}$$

The character constantly equal to 1 on $G_{l,Q}$ is called the *principal character*. When λ is not the principal character, $\mathcal{L}(z, \lambda)$ is a polynomial of degree $d(\lambda) < l + \deg Q$ [**9**, Lemma 8.2]. The *generalized Riemann hypothesis* states that all roots of $\mathcal{L}(z, \lambda)$ have modulus $q^{-1/2}$ or 1 for any character λ modulo an arithmetically distributed congruence relation such as $R_{l,Q}$. Weil's proof (for Dirichlet characters) was extended to these generalized characters by Rhin [**16**] (see, in particular, Ch. 2, §§4–6). In other words, we can write

$$\mathcal{L}(z, \lambda) = \prod_{i=1}^{d(\lambda)} (1 - \alpha_i z), \tag{11}$$

where $|\alpha_i| = q^{1/2}$ or 1 for $i = 1, \ldots, d(\lambda)$. In particular, $\mathcal{L}(z, \lambda)$ can be extended to an entire function and (10) remains valid when $|z| < q^{-1/2}$.

When λ is the principal character of $G_{l,Q}$, we have

$$\begin{aligned} \mathcal{L}(z, \lambda) &= \prod_{\substack{P \in \mathcal{I}, \\ (P, Q) = 1}} (1 - z^{\deg P})^{-1} \\ &= \prod_{\substack{P \in \mathcal{I}, \\ P \mid Q}} (1 - z^{\deg P}) \prod_{P \in \mathcal{I}} (1 - z^{\deg P})^{-1} \end{aligned}$$

https://doi.org/10.1112/S0025579319000032 Published online by Cambridge University Press

$$= \prod_{\substack{P\in\mathcal{I},\\ P|Q}} (1 - z^{\deg P}) \frac{1}{1-qz}.$$

Consequently, $\mathcal{L}(z,\lambda)$ can be extended to a meromorphic function and

$$\frac{1}{\mathcal{L}(z,\lambda)} = \sum_{n=1}^{\infty} z^n \sum_{f\in A_n,(f,Q)=1} \mu(f) = (1-qz) \prod_{\substack{P\in\mathcal{I},\\ P|Q}} (1 - z^{\deg P})^{-1} \tag{12}$$

for all $|z| \neq 1$.

2.3. *The bilinear Bogolyubov theorem.* When proving Theorem 2, we will suppose for a contradiction that

$$\sum_{f\in G_n} \mu(f + t^n)\chi(Q(f)) \geqslant \epsilon q^n.$$

Let M be the $n \times n$ symmetric matrix corresponding to Q and k an integer. For any $a \in G_{k+1}$, consider the map $L_a : G_{n-k} \to G_n$ that maps f to af. We also write L_a to denote its $n \times (n-k)$ coordinate matrix in the canonical basis (i.e., the basis of monomials). For any $(a,b) \in G_{k+1}^2$, let $M_{a,b} = L_a^T M L_b + L_b^T M L_a$; it is a symmetric $(n-k) \times (n-k)$ matrix.

After exploiting Vaughan's identity in Section 5.2, we will find that for some $n \ll k \leqslant n$, M has the property that the set of pairs

$$P_h := \{(a,b) \in G_{k+1} \times G_{k+1} | \text{rk } M_{a,b} \leqslant h\}$$

is large; that is, it contains at least δq^{2k+2} pairs for some parameters δ and h (depending on ϵ and n). We will want to convert this information about the ranks of many $M_{a,b}$ into one on the rank of M itself. However, we need these pairs to have some special structure in order to extract some information; in particular, it would be extremely convenient if the set

$$\{(t^i, t^j) \mid (i,j) \in \{0,\dots,k\}^2\} \tag{13}$$

could be in P_h, because M_{t^i,t^j} is then simply a submatrix of M. Unfortunately, its large size alone does not force P_h to contain such a nice structure, but, to boost our chances, we are ready to do some additive smoothing, that is, adjoining to our set P elements such as $(a_1 - a_2, b)$ whenever (a_1, b) and (a_2, b) are in P; and the same on the second coordinate. The rank remains controlled under this operation, because rk $M_{a_1-a_2,b} =$ rk $(M_{a_1,b} - M_{a_2,b}) \leqslant 2h$. Now our companion paper [3] shows that additive smoothing does indeed produce useful structures. Here is the result we get [3, Corollary 4].

PROPOSITION 4. *For any δ, there exists a constant $c(\delta)$ such that the following holds. If $|P_h| \geqslant \delta q^{2k+2}$, then there exist $\mathbb{F}_p$-subspaces W_1, W_2 of the*

https://doi.org/10.1112/S0025579319000032 Published online by Cambridge University Press

$\mathbb{F}_p$-vector space G_{k+1} of codimensions r_1, r_2 and $\mathbb{F}_p$-bilinear forms $Q_1, \dots, Q_r$ on $W_1 \times W_2$ such that $P_{64h} = \{(a,b) \in G_{k+1}^2 | \mathrm{rk}\, M_{a,b} \leqslant 64h\}$ contains the set

$$\{(x,y) \in W_1 \times W_2 \mid Q_1(x,y) = \cdots = Q_r(x,y) = 0\}$$

and $\max(r, r_1, r_2) \leqslant c(\delta)$.

We call this statement a bilinear Bogolyubov theorem, by analogy with the original (linear) Bogolyubov theorem. We found that we can take $c(\delta)$ to be $O(\exp(\exp(\exp(\log^{O(1)} 1/\delta))))$, where the implied constants may depend on q, but, unfortunately, because δ will be as small as, say, n^{-5}, this bound for $c(\delta)$ is too large. By analogy with Sanders' bound for the linear Bogolyubov theorem [**18**], it is reasonable to imagine [**3**, Conjecture 3] that the linear and bilinear codimensions r, r_1, r_2 could be taken as small as polylogarithmic in δ^{-1}. In [**3**], we show that indeed we can take r and one of r_1 and r_2 to be polylogarithmic in δ^{-1}. Recently, Hosseini and Lovett [**11**, Theorem 1.3] lowered $c(\delta)$ to $\log^{O(1)} \delta^{-1}$, at the cost of replacing 64 in Proposition 4 by a larger constant.

THEOREM 5 (Polylogarithmic bilinear Bogolyubov). *For any δ, if $|P_h| \geqslant \delta q^{2k+2}$, then there exist $\mathbb{F}_p$-subspaces W_1, W_2 of the $\mathbb{F}_p$-vector space G_{k+1} of codimensions r_1, r_2 and $\mathbb{F}_p$-bilinear forms $Q_1, \dots, Q_r$ on $W_1 \times W_2$ such that $P_{2^9 h} = \{(a,b) \in G_{k+1}^2 | \mathrm{rk}\, M_{a,b} \leqslant 2^9 h\}$ contains the set*

$$\{(x,y) \in W_1 \times W_2 \mid Q_1(x,y) = \cdots = Q_r(x,y) = 0\} \tag{14}$$

and $\max(r, r_1, r_2) \leqslant O(\log^{80} \delta^{-1})$.

Applied with $\delta = q^{-n^c}$, this means that the codimensions should be $O(n^{O(c)})$.

The reason why sets of the form (14) are so desirable for us is the following lemma.

LEMMA 6. *Let W be an $\mathbb{F}_p$-vector space of dimension n and $Q_1, \dots, Q_r$ be quadratic forms on W. If $n \geqslant 2r(r+1)$, then the set of isotropic vectors*

$$X = \{x \in W \mid Q_1(x) = \cdots = Q_r(x) = 0\} \tag{15}$$

contains at least $(1 - p^{-1/2}) p^{n-2r(r+1)}$ elements.

More compactly, we can write $|X| \gg p^{n-O(r^2)}$. We now prove Lemma 6. We introduce the averaging notation $\mathbb{E}_{x \in W} = (1/|W|) \sum_{x \in W}$.

Proof. The density $|X|/|W|$ of isotropic vectors is given by

$$\mathbb{E}_{x \in W} \mathbb{E}_{t_1, \dots, t_r \in \mathbb{F}_p} \omega^{\sum_i t_i Q_i(x)} = \mathbb{E}_{t_1, \dots, t_r} \mathbb{E}_{x \in W} \omega^{\sum_i t_i Q_i(x)}, \tag{16}$$

https://doi.org/10.1112/S0025579319000032 Published online by Cambridge University Press

where $\omega = e^{2\pi i/p}$. Let $m \leqslant n$ be a parameter to be determined later (in terms of r). Now, if a quadratic form Q on $W \times W$ has rank at least m, we can see that

$$|\mathbb{E}_{x\in W}\omega^{Q(x)}| \leqslant p^{-m/2}$$

by squaring this expectation (see Lemma 13). Thus, if, for any nonzero $(t_1, \dots, t_r)$, the rank of $\sum_i t_i Q_i$ is at least m, we see from equation (16) that the density of isotropic vectors is at least $p^{-r} - p^{-m/2}$. Otherwise, there exists a form Q_i such that $Q_i = \sum_{j\neq i} t_j Q_j + R$ with rk $R < m$; without loss of generality, suppose that $i = r$. Let W' be the kernel of R, a subspace of codimension less than m. Then the set

$$X' = \{x \in W' | Q_1(x) = \cdots = Q_{r-1}(x) = 0\} \tag{17}$$

is a subset X and we will now count isotropic vectors in X'. Thus, incurring a dimension loss of at most m, we reduce the number of quadratic forms by 1. We iterate this process until we get a family of quadratic forms for which any nontrivial linear combination has rank at least m (or an empty family). At that point, this is a family of at most r forms on a space of dimension at least $n - rm$. Thus, it must have at least

$$p^{n-r(m+1)} - p^{n-rm-m/2}$$

isotropic vectors. Taking $m = 2r + 1$, we obtain the result. □

We will use this lemma in §6 to obtain sets of the form (13) inside $P_{2^9 h}$.

2.4. *Divisor bounds.* We list some facts regarding the divisor function in $\mathbb{F}_q[t]$ which we will need in the sequel. Let $\tau(f)$ denote the number of monic divisors of $f \in \mathbb{F}_q[t]$. We first have the following result.

LEMMA 7 [**13**, Lemma 8]. *If* $\deg f = n > 1$, *then*

$$\tau(f) \leqslant \exp\left(O_q\left(\frac{n}{\log n}\right)\right).$$

Consequently, the number of monic irreducible factors of f *is* $O_q(n/\log n)$.

The next result is a bound for the second moment of τ.

LEMMA 8. *We have*

$$\mathbb{E}_{\deg d=n}\tau(d)^2 \leqslant 4n^3.$$

Proof. We observe that for any irreducible P and any integer k, we have $\tau(P^k)^2 = (k+1)^2$.

Thus, the Dirichlet series $D = \sum_{n=0}^{+\infty}\sum_{f\in A_n}(\tau(f)^2/|f|^s)$ of the function τ^2 can be written as an Euler product as

$$D = \prod_P \sum_{k=0}^{+\infty}(k+1)^2|P|^{-ks}. \tag{18}$$

https://doi.org/10.1112/S0025579319000032 Published online by Cambridge University Press

Next we note the following relations between formal power series:

$$\sum_{k=0}^{+\infty}(k+1)^2x^k = \sum_{k=0}^{+\infty}(k+2)(k+1)x^k - \sum_{k=0}^{+\infty}(k+1)x^k$$
$$= 2(1-x)^{-3} - (1-x)^{-2} = \frac{1+x}{(1-x)^3},$$

so finally

$$\sum_{k=0}^{+\infty}(k+1)^2x^k = \frac{1-x^2}{(1-x)^4}. \tag{19}$$

Combining equations (18) and (19) yields

$$D = \prod_P \frac{1-|P|^{-2s}}{(1-|P|^{-s})^4}.$$

We can then express this Euler product in terms of the zeta function of $\mathbb{F}_q[t]$. Letting $u = q^{-s}$, we obtain

$$D = \zeta(s)^4/\zeta(2s) = (1-q^{1-2s})(1-q^{1-s})^{-4} = (1-qu^2)(1-qu)^{-4}.$$

This is a power series $S(u)$ in u and $S(u) = \sum_n a_n u^n = \sum_n (S^{(n)}(0)/n!)u^n$, where $a_n = \sum_{\deg d=n}\tau(d)^2$. Now, for $n \geqslant 3$, deriving n times using Leibniz' formula, we find that

$$S^{(n)}(u) = (1-qu^2)q^n(4\times\cdots\times(n+3))(1-qu)^{-4-n}$$
$$-2qunq^{n-1}(4\times\cdots\times(n+2))(1-qu)^{-3-n}$$
$$-2q\binom{n}{2}q^{n-2}(4\times\cdots\times(n+1))(1-qu)^{-2-n}.$$

Evaluating in $u=0$ gives

$$\frac{S^{(n)}(0)}{q^n n!} = (n+3)(n+2)(n+1)/6 - q^{-1}n(n+1)^2/6 \leqslant 4n^3,$$

where the left-hand side is exactly $\mathbb{E}_{\deg d=n}\tau(d)^2$. □

§3. *Character sum estimates.* In this section we prove the following result.

THEOREM 9. *Let $l \geqslant 0$, $Q \in \mathbb{F}_q[t]$, $\deg Q = m \geqslant 0$ and λ be a character of $G_{l,Q}$. Then, for any d and $\epsilon > 0$, we have*

$$\left|\sum_{f\in A_d}\mu(f)\lambda(f)\right| \ll_{\epsilon,q} q^{((1/2)+\epsilon)d+\epsilon(m+l)}. \tag{20}$$

Proof. First we assume that λ is not principal. We will prove the following more precise bound:

$$\left|\sum_{f\in A_d}\mu(f)\lambda(f)\right| \leqslant q^{(d/2)+(d\log\log(m+l)/\log(m+l))+O_q((m+l)/\log^2(m+l))}. \tag{21}$$

Our method is a generalization of the proof of [2, Theorem 2].

https://doi.org/10.1112/S0025579319000032 Published online by Cambridge University Press

Like [2], we deduce (21) from an estimate for $\log \mathcal{L}(z, \lambda)$ near the circle $|z| = q^{-1/2}$, which is in turn deduced from an estimate for $\mathcal{L}'(z, \lambda)/\mathcal{L}(z, \lambda)$.

By taking the logarithmic derivatives of (9) and (11), we have two different expressions for $\mathcal{L}'(z, \lambda)/\mathcal{L}(z, \lambda)$. On the one hand, we have

$$\frac{\mathcal{L}'(z, \lambda)}{\mathcal{L}(z, \lambda)} = \sum_{l=1}^{\infty} a_l z^{l-1},$$

where

$$a_l = -\sum_{i=1}^{d(\lambda)} \alpha_i^l \tag{22}$$

according to (11).

On the other hand, according to (9), we have

$$a_l = \sum_{\deg f = l} \Lambda(f)\lambda(f). \tag{23}$$

From (22), we have

$$|a_l| \leqslant d(\lambda) q^{l/2} \tag{24}$$

and, from (23), we have

$$|a_l| \leqslant \sum_{\deg f = l} \Lambda(f) = q^l. \tag{25}$$

Put $L = \lfloor 2 \log_q d(\lambda) \rfloor$. For $l > L$, we use the bound (24) and, for $l \leqslant L$, we use the bound (25). Therefore, for any z, we have

$$\left| \frac{\mathcal{L}'(z, \lambda)}{\mathcal{L}(z, \lambda)} \right| \leqslant \sum_{l=1}^{L} q^l |z|^{l-1} + \sum_{l=L+1}^{\infty} d(\lambda) q^{l/2} |z|^{l-1}. \tag{26}$$

Let $0 < \epsilon < 1/4$ be chosen later, $R = q^{-1/2-\epsilon}$ and w be arbitrary on the circle $|w| = R$. Integrating (26) along the line from 0 to w, and noting that $\mathcal{L}(0, \lambda) = 1$, we have

$$|\log \mathcal{L}(w, \lambda)| \leqslant \sum_{l=1}^{L} \frac{(Rq)^l}{l} + \sum_{l=L+1}^{\infty} d(\lambda) \frac{(Rq^{1/2})^l}{l}. \tag{27}$$

The second sum in (27) can be bounded by

$$\frac{d(\lambda)}{L} \sum_{l=L+1}^{\infty} (Rq^{1/2})^l \leqslant \frac{d(\lambda)}{L} R^L q^{L/2} \frac{1}{1 - Rq^{1/2}} \ll \frac{d(\lambda)^2 R^L}{L} \frac{1}{1 - Rq^{1/2}}. \tag{28}$$

As for the first sum in (27), we bound it crudely by

$$\sum_{l=1}^{L} (Rq)^l \leqslant (Rq)^L \sum_{k=0}^{\infty} (Rq)^{-k} \leqslant \frac{d(\lambda)^2 R^L}{1 - (qR)^{-1}} \ll_q d(\lambda)^2 R^L, \tag{29}$$

https://doi.org/10.1112/S0025579319000032 Published online by Cambridge University Press

since $qR \geqslant q^{1/4}$. By combining (28) and (29), we have

$$|\log \mathcal{L}(w,\lambda)| \ll_q d(\lambda)^2 R^L \left(1 + \frac{1}{L(1-Rq^{1/2})}\right).$$

Hence,

$$\left|\frac{1}{\mathcal{L}(w,\lambda)}\right| \leqslant \exp\left(O_q\left(d(\lambda)^2 R^L \left(1 + \frac{1}{L(1-Rq^{1/2})}\right)\right)\right). \tag{30}$$

Let C_R be the circle $|w| = R = q^{-1/2-\epsilon}$. From (10), we see that

$$\begin{aligned}\left|\sum_{f\in A_d} \lambda(f)\mu(f)\right| &= \left|\frac{1}{2\pi i}\int_{C_R} \frac{1}{\mathcal{L}(w,\chi)} w^{-d-1}\,dw\right| \\ &\leqslant \max_{C_R}\left|\frac{1}{\mathcal{L}(w,\lambda)}\right| R^{-d} \\ &\leqslant q^{d(1/2+\epsilon)+O_q(d(\lambda)^{1-2\epsilon}(1+1/\epsilon\log d(\lambda)))}. \end{aligned} \tag{31}$$

We now make the choice $\epsilon = (\log\log d(\lambda)/\log d(\lambda))$. Recalling that $d(\lambda) \leqslant l + m - 1$, (21) follows. The bound (21) is stronger than (20) when $\log\log(l+m)/\log(l+m)$ is greater than the ϵ in (20). For the finitely many exceptional pairs (m,l), (20) follows from (31) (with the same ϵ).

We now consider the case where λ is principal. From (12), on the circle $|z| = q^{-1/2}$, we have

$$\begin{aligned}\left|\frac{1}{\mathcal{L}(z,\lambda)}\right| &= |1-qz| \prod_{P\in\mathcal{I}, P|Q} |1-z^{\deg P}|^{-1} \\ &\ll \prod_{P\in\mathcal{I}, P|Q} (1-q^{-\deg P/2})^{-1} \\ &\leqslant \prod_{P\in\mathcal{I}, P|Q} (1-q^{-1/2})^{-1} \\ &= (1-q^{-1/2})^{-k} \leqslant q^{O_q(m/\log m)}, \end{aligned} \tag{32}$$

where k is the number of monic irreducible factors of Q and (32) follows from Lemma 7. Integrating $z^{-d-1}(1/\mathcal{L}(z,\lambda))$ along the circle $|z| = q^{-1/2}$ and using (32), we see that

$$\sum_{f\in A_n,(f,Q)=1} \mu(f) \ll q^{d/2+O_q(m/\log m)}, \tag{33}$$

from which (20) follows. □

We remark that (12) readily gives a formula for $\sum_{f\in A_n,(f,Q)=1}\mu(f)$, but it is not immediate to derive (33) from this formula.

§4. *Exponential sum estimates.* We say that a function $F : M \to \mathbb{C}$ is $R_{l,Q}$-periodic if it is constant on each equivalence class of $R_{l,Q}$. In other words, F is $R_{l,Q}$-periodic if $F(f)$ depends only on the residue class of f modulo Q and the

https://doi.org/10.1112/S0025579319000032 Published online by Cambridge University Press

first l coefficients of f. We say that F is 1-bounded if $|F(f)| \leqslant 1$ for any $f \in M$. First we show that μ is orthogonal to $R_{l,Q}$-periodic functions by adapting the argument of [7, Proposition 3.2].

PROPOSITION 10. *Suppose that* $\deg Q = m$. *For any* $R_{l,Q}$*-periodic and 1-bounded function* $F : M \to \mathbb{C}$ *and* $\epsilon > 0$, *we have*

$$\sum_{f \in A_n} F(f)\mu(f) \ll_{\epsilon,q} q^{(1/2+\epsilon)(n+m+l)},$$

where the bound is uniform in F.

Proof. We first consider the case where $F(f) = 0$ whenever $(f, Q) \neq 1$. This means that F is a function on $G_{l,Q}$. Let $K = |G_{l,Q}| = q^l \phi(Q) \leqslant q^{l+m}$ and $\lambda_1, \ldots, \lambda_K$ be the characters of $G_{l,Q}$. Define the Fourier coefficients of F by

$$\widehat{F}(\lambda) = \mathbb{E}_{f \in G_{l,Q}} F(f)\overline{\lambda(f)}$$

for any character λ of $G_{l,Q}$. Then $F(f) = \sum_{i=1}^{K} \widehat{F}(\lambda_i)\lambda_i(f)$. Plancherel's formula implies that

$$\sum_{i=1}^{K} |\widehat{F}(\lambda_i)|^2 = \mathbb{E}_{f \in G_{l,Q}} |F(f)|^2 \leqslant 1. \tag{34}$$

We have

$$\begin{aligned}
\left| \sum_{f \in A_n} F(f)\mu(f) \right| &= \left| \sum_{i=1}^{K} \widehat{F}(\lambda_i) \sum_{f \in A_n} \lambda_i(f)\mu(f) \right| \\
&\ll_{\epsilon,q} q^{n/2+\epsilon(n+l+m)} \sum_{i=1}^{K} |\widehat{F}(\lambda_i)| \qquad (35) \\
&\leqslant q^{n/2+\epsilon(n+l+m)} K^{1/2} \qquad (36) \\
&\leqslant q^{n/2+(l+m)/2+\epsilon(n+l+m)}.
\end{aligned}$$

Here (35) follows from Theorem 9 and (36) follows from the Cauchy–Schwarz inequality and (34).

Next we consider the general case where $F(f)$ is not necessarily 0 when $(f, Q) \neq 1$. If f is square-free, $(f, Q) = D$, we can write $f = Dg$, where g is square-free and $(g, Q) = 1$. Hence,

$$\begin{aligned}
\sum_{f \in A_n} F(f)\mu(f) &= \sum_{\substack{D \in M, D|Q, \\ D \text{ square-free}}} \sum_{\substack{\deg g = n - \deg D, \\ g \text{ square-free}}} F(Dg)\mu(Dg)1_{(g,Q)=1} \\
&= \sum_{D \in M, D|Q} \mu(D) \sum_{\substack{\deg g = n - \deg D, \\ g \text{ square-free}}} F(Dg)\mu(g)1_{(g,Q)=1}. \qquad (37)
\end{aligned}$$

https://doi.org/10.1112/S0025579319000032 Published online by Cambridge University Press

Now the function $g \mapsto F(Dg)\mu(g)1_{(g,Q)=1}$ is $R_{l,Q}$-periodic and vanishes on elements of M that are not coprime to Q. By the above, we infer that

$$\sum_{\substack{\deg g = n - \deg D, \\ g \text{ square-free}}} F(Dg)\mu(g)1_{(g,Q)=1} \ll_{\epsilon,q} q^{(n-\deg D)/2+(l+m)/2+\epsilon(n+m+l)}$$

for any $\epsilon > 0$. Furthermore, still for any $\epsilon > 0$, we observe that

$$\sum_{D|Q} q^{-(\deg D)/2} \leqslant \tau(Q) \ll_{\epsilon,q} |Q|^{\epsilon} = q^{\epsilon m}$$

by Lemma 7. This completes the proof. □

We will now use Proposition 10 and the ideas outlined at the beginning of §2.2 to prove the following exponential sum estimate.

THEOREM 11. *Given any $\epsilon > 0$, for all $\alpha \in \mathbb{T}$ and n, we have*

$$\sum_{f \in A_n} \mu(f)e(\alpha f) \ll_{\epsilon,q} q^{(3/4+\epsilon)n} \tag{38}$$

and

$$\sum_{f \in G_n} \mu(f)e(\alpha f) \ll_{\epsilon,q} q^{(3/4+\epsilon)n}. \tag{39}$$

The first bound implies the second bound, because

$$\sum_{f \in G_n} \mu(f)e(\alpha f) = \sum_{c \in \mathbb{F}_q^*} \sum_{k=0}^{n-1} \sum_{f \in A_k} \mu(f)e(\alpha c f),$$

so we only need to prove the bound (38). It is easy to see that any linear form on G_n can be written as $f \mapsto (\alpha f)_{-1}$ (i.e., the coefficient of t^{-1} in αf) for some $\alpha \in \mathbb{T}$. Thus, Theorem 1 follows from Theorem 11.

Proof. By Dirichlet's approximation theorem, we can find $a, g \in \mathbb{F}_q[t]$, $g \neq 0, \deg g \leqslant \lfloor n/2 \rfloor$ such that $|\alpha - a/g| < 1/q^{\lfloor n/2 \rfloor}|g|$. Put $\beta = \alpha - a/g$. Then

$$\sum_{f \in A_n} \mu(f)e(\alpha f) = \sum_{f \in A_n} \mu(f)e\left(\frac{af}{g}\right)e(\beta f).$$

Since $|\beta| < q^{-\lfloor n/2 \rfloor - \deg g}$, we see that $e(\beta f)$ depends only on the first $n - \lfloor n/2 \rfloor - \deg g$ coefficients of f. Also, $e(af/g)$ depends only on the residue class of f modulo g. Applying Proposition 10 to $(l, Q) = (n - \lfloor n/2 \rfloor - \deg g, g)$, for any $\epsilon > 0$, we have

$$\begin{aligned}\sum_{f \in A_n} \mu(f)e\left(\frac{af}{g}\right)e(\beta f) &\ll_{\epsilon,q} q^{((1+\epsilon)/2)(n+n-\lfloor n/2 \rfloor - \deg g + \deg g)} \\ &= q^{((1+\epsilon)/2)(2n-\lfloor n/2 \rfloor)} \ll_{\epsilon,q} q^{(3/4+\epsilon)n},\end{aligned}$$

as desired. □

https://doi.org/10.1112/S0025579319000032 Published online by Cambridge University Press

As we show next, this implies that if a function is determined by the values of a few linear forms, it does not correlate with the Möbius function.

COROLLARY 12. *Let $c > 0$ be a constant. Let $F : \mathbb{F}_q^r \to \mathbb{C}$ be 1-bounded and suppose that $r \leqslant cn$. Let $\ell_1, \dots, \ell_r$ be linear forms on G_n. Then, for any $\epsilon > 0$,*

$$\sum_{f \in G_n} \mu(f + t^n) F(\ell_1(f), \dots, \ell_r(f)) \ll_{\epsilon,q} q^{(3/4+c+\epsilon)n}.$$

Obviously, this is interesting only if $c < 1/4$.

Proof. Theorem 11 immediately implies that for any linear form ℓ on G_n, we have

$$\sum_{f \in G_n} \mu(f + t^n) e_q(\ell(f)) \ll_{\epsilon,q} q^{(3/4+\epsilon)n}. \tag{40}$$

For any $\mathbf{a} = (a_1, \dots, a_r) \in \mathbb{F}_q^r$, let $V_{\mathbf{a}} \leqslant G_n$ be the affine subspace defined by the equations $\ell_i(f) = a_i$ for $i \in [r]$. Then one can write

$$\sum_{f \in G_n} \mu(f + t^n) F(\ell_1(f), \dots, \ell_r(f)) = \sum_{\mathbf{a} \in \mathbb{F}_q^r} F(\mathbf{a}) \sum_{f \in V_{\mathbf{a}}} \mu(f + t^n). \tag{41}$$

Now we observe that

$$1_{V_{\mathbf{a}}}(f) = \mathbb{E}_{\boldsymbol{\chi} = (\chi_1, \dots, \chi_r) \in \widehat{\mathbb{F}_q}^r} \prod_{i \in [r]} \chi_i(\ell_i(f) - a_i),$$

so that

$$\sum_{f \in V_{\mathbf{a}}} \mu(f + t^n) = \mathbb{E}_{\boldsymbol{\chi} \in \widehat{\mathbb{F}_q}^r} \prod_{i \in [r]} \chi_i(-a_i) \sum_{f \in G_n} \mu(f + t^n) \prod_{i \in [r]} \chi_i(\ell_i(f))$$

and, by the triangle inequality,

$$\left| \sum_{f \in V_{\mathbf{a}}} \mu(f + t^n) \right| \leqslant \max_{\boldsymbol{\chi} \in \widehat{\mathbb{F}_q}^r} \left| \sum_{f \in G_n} \mu(f + t^n) \prod_{i \in [r]} \chi_i(\ell_i(f)) \right|.$$

Recall from §2.1 that each χ_i is of the form $\chi_i(x) = e_q(t_i x)$, so that

$$\prod_{i \in [r]} \chi_i(\ell_i(f)) = e_q\left(\sum_{i=1}^r t_i \ell_i(f) \right).$$

We then apply (40) to the linear form $\ell = \sum_{i \in [r]} t_i \ell_i$. This shows that

$$\left| \sum_{f \in V_{\mathbf{a}}} \mu(f + t^n) \right| \ll q^{(3/4+\epsilon)n}.$$

Inserting this bound in equation (41) and using the fact that $|F| \leqslant 1$, this gives the desired result. □

§5. *Quadratic phases and Vaughan's identity.* From now on, we suppose that the field $\mathbb{F}_q$ we work with has characteristic $p > 2$. Recall that $q = p^s$ and $s \geqslant 1$.

https://doi.org/10.1112/S0025579319000032 Published online by Cambridge University Press

5.1. *Quadratic phases.* We call a *quadratic form* on $\mathbb{F}_q^n$ a homogenous polynomial of degree 2, that is, a map of the form $F(x) = x^T Mx$, where M is a symmetric matrix. The corresponding (symmetric) bilinear form is the map

$$B(x, y) = x^T My.$$

The *rank* of F is the rank of the matrix M. It equals the codimension of the space K of vectors x such that the linear form B_x defined by $B_x(y) = B(x, y)$ satisfies $B_x = 0$. A *quadratic polynomial* is a polynomial of degree 2, that is, a quadratic form plus a linear form. A *quadratic phase* is a map of the form $\Phi(x) = \chi(P(x))$ for a quadratic polynomial P and an additive character χ. Its *rank* is the rank of the corresponding quadratic form. Thanks to the following standard lemma, quadratic phases can be classified, depending on their rank, into major arcs and minor arcs, by analogy with the circle method.

LEMMA 13 (Gauss sums). *Let $\Phi(x) = \chi(P(x))$ be a quadratic phase of rank at least r. Then*

$$|\mathbb{E}_{x\in\mathbb{F}_q^n}\Phi(x)| \leqslant q^{-r/2}.$$

Thus, quadratic phases of low rank correspond to major arcs, while the ones of high rank correspond to minor arcs.

Proof. We use the standard technique called Weyl differencing, consisting of squaring the expectation to duplicate the variable. We have

$$\begin{aligned}|\mathbb{E}_{x\in\mathbb{F}_q^n}\Phi(x)|^2 &= \mathbb{E}_{x,h}\Phi(x+h)\overline{\Phi(x)}\\ &= \mathbb{E}_{x,h}\chi(P(x+h)-P(x))\\ &= \mathbb{E}_h\chi(P(h))\mathbb{E}_x\chi(2B_h(x)),\end{aligned}$$

where all variables range over $\mathbb{F}_q^n$. Now, if $h \notin K$, the form $2B_h$ is a nonzero linear form (remember that the characteristic p is not 2), whence $\mathbb{E}_{x\in\mathbb{F}_q^n}\chi(2B_h(x)) = \mathbb{E}_{x\in\mathbb{F}_q}\chi(x) = 0$. This implies that

$$|\mathbb{E}_{x\in\mathbb{F}_q^n}\Phi(x)|^2 \leqslant \mathbb{E}_{h\in\mathbb{F}_q^n}1_{h\in K} = q^{-r}$$

and the claim follows. □

We now start the proof of Theorem 2. Let P be a quadratic polynomial on $\mathbb{F}_q^n$ and $\Phi = \chi \circ P$ be a quadratic phase. We want to bound the sum

$$\sum_{f\in G_n}\mu(f+t^n)\Phi(f) = \sum_{f\in A_n}\mu(f)\Phi(f),$$

where, by abuse of notation, if $f \in A_n$, we write $\Phi(f)$ for $\Phi(f-t^n)$. The general strategy is the following. We first observe that when Φ is a quadratic phase of rank at most cn with $c < 1/4$, then Corollary 12 concludes: indeed, a quadratic form of rank r depends on r linear forms only, so a quadratic polynomial of rank r depends on $r+1$ linear forms at most. So, we will show that in order for μ to correlate with a quadratic phase Φ, the corresponding quadratic form needs to be of small rank (major arcs). This would imply that μ cannot correlate with a quadratic phase at all.

https://doi.org/10.1112/S0025579319000032 Published online by Cambridge University Press

5.2. *Exploitation of Vaughan's identity.* We will show the following result.

PROPOSITION 14. *Let $\delta > 0$. Suppose that $|\sum_{f\in A_n}\mu(f)\Phi(f)| \geqslant \delta q^n$. Then at least one of the following two statements holds.*

(1) *There exists $k \leqslant n/9$ such that for at least one polynomial d of degree k, the quadratic polynomial on G_{n-k} defined by*

$$w \mapsto P(dw)$$

has rank at most $O(\log(n/\delta))$.

(2) *There exists $k \in [n/18, 17n/18]$ such that for at least $(\delta/n)^{O(1)}q^{2k}$ pairs of polynomials d, d' of degree k, the quadratic polynomial on G_{n-k} defined by*

$$w \mapsto P(d'w) - P(dw)$$

has rank at most $O(\log(n/\delta))$.

Before proving this proposition, we underline that for any $d \in G_{k+1}$, we see the map $w \mapsto dw$ as a linear map from G_{n-k} to G_n, which allows one to see $w \mapsto P(dw)$ as a quadratic polynomial.

We now start proving the proposition. The first tool we need is Vaughan's identity, which reads

$$\mu(f) = -\sum_{\substack{ab|f\\ \deg a\leqslant u,\deg b\leqslant v}}\mu(a)\mu(b) + \sum_{\substack{ab|f\\ \deg a>u,\deg b>v}}\mu(a)\mu(b),$$

where the sum is over monic polynomials a and b, and $u = v = n/18$ (though in general they can be chosen arbitrarily). We shall adopt the notational convention that $N = q^n, U = q^u$ and so on. Moreover, for $f \in \mathbb{F}_q[t]$, recall the notation $|f| = q^{\deg f}$. Vaughan's identity implies that

$$\sum_{f\in A_n}\mu(f)\Phi(f) = -T_1 + T_2, \tag{42}$$

where

$$T_1 = \sum_{|d|\leqslant UV} a_d \sum_{w\in A_{n-\deg d}}\Phi(dw) \tag{43}$$

and

$$T_2 = \sum_{V\leqslant|d|\leqslant N/U} b_d \sum_{w\in A_{n-\deg d}}\mu(w)\Phi(dw) \tag{44}$$

are called type I and type II sums, respectively. The sums over d are over monic polynomials. The coefficients a_d are unimportant and all we need to know is that $\max(|a_d|, |b_d|) \leqslant \tau(d)$. In the type I sum, we have made the change of variables $d = ab, w = f/d$, while in the other one we wrote $w = fb, d = f/w$. The splitting into two sums yields the following dichotomy, which we will use to prove Proposition 14.

https://doi.org/10.1112/S0025579319000032 Published online by Cambridge University Press

PROPOSITION 15. *Make the same hypothesis as in Proposition 14. Then either there exists $k \leqslant n/9$ so that*

$$\mathbb{E}_{d\in A_k}|\mathbb{E}_{w\in A_{n-k}}\Phi(dw)|^2 \geqslant \delta^2/(16n^5) \tag{45}$$

or there is a $k \in [n/18, 17n/18]$ such that

$$\mathbb{E}_{w,w'\in A_{n-k}}\mathbb{E}_{d,d'\in A_k}\Phi(dw)\overline{\Phi(dw')\Phi(d'w)}\Phi(d'w') \geqslant \delta^4/(256n^{10}). \tag{46}$$

Proof. If $|\sum_{f\in A_n}\mu(f)\Phi(f)| \geqslant \delta N$, the decomposition (42) implies that either $|T_1| \geqslant \delta N/2$ or $|T_2| \geqslant \delta N/2$. Suppose first that $|T_1| \geqslant \delta N/2$. On the other hand, using the triangle inequality and equation (43), we bound T_1 by

$$\begin{aligned}|T_1| &\leqslant \sum_{k\leqslant u+v}\sum_{d\in A_k}\tau(d)\frac{N}{|d|}|\mathbb{E}_{w\in A_{n-k}}\Phi(dw)| \\ &\leqslant n\max_{k\leqslant u+v}\frac{N}{K}\sum_{d\in A_k}\tau(d)|\mathbb{E}_{w\in A_{n-k}}\Phi(dw)|.\end{aligned}$$

Fix a $k \leqslant u+v = n/9$ that realizes the maximum in the line above. The Cauchy–Schwarz inequality then yields

$$|T_1|^2/N^2 \leqslant n^2\,(\mathbb{E}_{d\in A_k}\tau^2(d))(\mathbb{E}_{d\in A_k}|\mathbb{E}_{w\in A_{n-k}}\Phi(dw)|^2).$$

Now Lemma 8 ensures that

$$\mathbb{E}_{d\in A_k}\tau^2(d) \leqslant 4k^3 \leqslant 4n^3,$$

so we can affirm that

$$\delta^2N^2/4 \leqslant |T_1|^2 \leqslant 4n^5N^2\mathbb{E}_{d\in A_k}|\mathbb{E}_{w\in A_{n-k}}\Phi(dw)|^2.$$

This means that

$$\mathbb{E}_{d\in A_k}|\mathbb{E}_{w\in A_{n-k}}\Phi(dw)|^2 \geqslant \delta^2/(16n^5),$$

which proves equation (45).

Let us now suppose that $|T_2| \geqslant \delta N/2$. Using the triangle inequality and equation (44), we have

$$\begin{aligned}|T_2| &\leqslant \sum_{V\leqslant|d|\leqslant N/U}\tau(d)\left|\sum_{w\in A_{n-k}}\mu(w)\Phi(dw)\right| \\ &\leqslant nN\max_{v\leqslant k\leqslant n-u}\mathbb{E}_{d\in A_k}\tau(d)|\mathbb{E}_{w\in A_{n-k}}\mu(w)\Phi(dw)|.\end{aligned}$$

We again fix a k (this time $k \in [n/18, 17n/18]$) that realizes the maximum and apply the Cauchy–Schwarz inequality together with Lemma 8, obtaining

$$|T_2|^2/N^2 \leqslant 4n^5\,\mathbb{E}_{d\in A_k}\mathbb{E}_{w,w'\in A_{n-k}}\mu(w)\mu(w')\Phi(dw)\overline{\Phi(dw')}.$$

https://doi.org/10.1112/S0025579319000032 Published online by Cambridge University Press

This implies that

$$\mathbb{E}_{w,w'\in A_{n-k}}\,\mu(w)\mu(w')\mathbb{E}_{d\in A_k}\Phi(dw)\overline{\Phi(dw')}\geqslant \delta^2/(16n^5)$$

and again we apply Cauchy–Schwarz to eliminate μ, which yields

$$\mathbb{E}_{w,w'\in A_{n-k}}\mathbb{E}_{d,d'\in A_k}\Phi(dw)\overline{\Phi(dw')\Phi(d'w)}\Phi(d'w')\geqslant \delta^4/(256n^{10}).$$

This is the content of clause (46), so the proof of Proposition 15 is complete. □

We now derive Proposition 14 using Proposition 15. Suppose first that equation (45) holds, so there is $k\leqslant n/9$ such that

$$\mathbb{E}_{d\in A_k}|\mathbb{E}_{w\in A_{n-k}}\Phi(dw)|^2\geqslant \delta', \tag{47}$$

where $\delta'=\delta^2/(16n^5)$. Equation (47) implies that there exists $d\in A_k$ such that

$$|\mathbb{E}_{w\in A_{n-k}}\Phi(dw)|^2\geqslant\delta'.$$

Fix such a $d\in A_k$. Lemma 13 then implies that the quadratic polynomial $w\mapsto P(dw)$ has rank at most $\log_q(\delta'^{-1})=O(\log(n/\delta))$. This corresponds exactly to the first statement of Proposition 14.

Suppose instead that equation (46) holds. Then we have $k\in[n/18,17n/18]$ such that

$$\mathbb{E}_{w,w'\in A_{n-k}}\mathbb{E}_{d,d'\in A_k}\Phi(dw)\overline{\Phi(dw')\Phi(d'w)}\Phi(d'w')\geqslant\delta',$$

where $\delta'=\delta^4/(256n^{10})$. The triangle inequality ensures that

$$\mathbb{E}_{d,d'\in A_k}|\mathbb{E}_{w\in A_{n-k}}\chi(P(dw)-P(d'w))|\geqslant\delta'.$$

In particular, for a proportion of at least $\delta'/2$ pairs of monic polynomials d,d' of degree k, we have

$$\begin{aligned}&|\mathbb{E}_{w\in G_{n-k}}\chi(P(d(w+t^{n-k}))-P(d'(w+t^{n-k})))|\\&\quad=|\mathbb{E}_{w\in A_{n-k}}\chi(P(dw)-P(d'w))|\geqslant\delta'/2.\end{aligned}$$

Observe that for $w\in G_{n-k}$, the rank of $w\mapsto P(d(w+t^{n-k}))-P(d'(w+t^{n-k}))$ is the same as that of $w\mapsto P(dw)-P(d'w)$. Lemma 13 implies that the rank of $w\mapsto P(dw)-P(d'w)$ is at most $-2\log_q(\delta'/2)=O(\log(n/\delta))$. This is precisely the second part of Proposition 14. So, in every case, Proposition 14 holds.

https://doi.org/10.1112/S0025579319000032 Published online by Cambridge University Press

§6. *Using the polylogarithmic bilinear Bogolyubov theorem.* Let $c > 0$ be a constant to be determined later and let $\delta = q^{-n^c}$. To prove Theorem 2, it suffices to show that $|\sum_{f\in A_n}\mu(f)\Phi(f)| < \delta q^n$ for n large enough. (The bound for $\sum_{f\in G_n}$ simply follows from summing the bounds for $\sum_{f\in A_k}$ for $k = 1, \dots, n-1$.) For the sake of contradiction, suppose instead that there exists an unbounded set Z of integers n such that

$$\left|\sum_{f\in A_n}\mu(f)\Phi(f)\right| \geqslant \delta q^n \tag{48}$$

whenever $n \in Z$. We then apply Proposition 14. Suppose that the first statement holds. Write $P(f) = B(f, f)$ for some bilinear form $B(x, y)$ on $\mathbb{F}_q^n \times \mathbb{F}_q^n$ (we may omit the linear part of P as it modifies the rank by at most 1). Then we know that the form $R_d : w \mapsto P(dw)$ on G_{n-k} has rank at most $O(n^c)$ for at least one d of some degree $0 \leqslant k \leqslant n/9$. Now the rank of the quadratic form R_d is simply the rank of the bilinear form B restricted to the subspace $dG_{n-k} \subset G_n$ of codimension k. Thus, the rank of R_d is at least rk $B - 2k$, which implies that rk $B \leqslant 2n/9 + O(n^c)$. If $n \in Z$ is large enough (remember that Z is unbounded), this is less than $c'n$ for some $c' < 1/4$. Then Corollary 12 brings the desired contradiction.

Now let us suppose that the second case of Proposition 14 holds. Let $n/18 \leqslant k \leqslant 17n/18$ be the parameter returned by this proposition. Then the set

$$Y = \{(d, d') \in A_k^2 \mid w \mapsto P(dw) - P(d'w) \text{ has rank at most } O(n^c)\}$$

has size at least $q^{2k+2-O(n^c)}$. Note that, for $d, d' \in G_{k+1}$,

$$P(dw) - P(d'w) = B((d - d')w, (d + d')w)$$

is a quadratic polynomial in $w \in G_{n-k}$. For $a, b \in G_{k+1}$, let $B_{a,b}$ be the symmetric bilinear form on $\mathbb{F}_q^{n-k} \times \mathbb{F}_q^{n-k}$ (identified with $G_{n-k} \times G_{n-k}$) defined by $B_{a,b}(x, y) = (B(ax, by) + B(ay, bx))/2$. Thus, we have a set

$$X = \{(a, b) \in G_{k+1} \times G_{k+1} \mid \text{rk } B_{a,b} \leqslant O(n^c)\}$$

of density at least $\eta = q^{-O(n^c)}$ in $G_{k+1} \times G_{k+1}$. As discussed in §2.3, we would like to replace the large set X by a more structured set, namely the zero set of a (not too large) family of bilinear forms, at the cost of slightly worsening the bounds on the rank. Theorem 5, an application of the bilinear Bogolyubov theorem from [**11**], precisely implies that

$$X' = \{(a, b) \in G_{k+1} \times G_{k+1} \mid \text{rk } B_{a,b} \leqslant O(n^c)\}$$

contains a set of the form

$$Y = \{(a, b) \in W_1 \times W_2 \mid F_1(a, b) = \cdots = F_r(a, b) = 0\},$$

https://doi.org/10.1112/S0025579319000032 Published online by Cambridge University Press

where W_1, W_2 are $\mathbb{F}_p$-subspaces of G_{k+1} (itself seen as an $\mathbb{F}_p$-vector space of dimension $s(k+1) = O(k)$) and $\max(\operatorname{codim} W_1, \operatorname{codim} W_2, r) = O(\log^{80} \eta^{-1}) = O(n^{80c})$.

Now take $\epsilon = 1/10$ and consider a set of indices

$$I = \{0 = i_1 < i_2 < \cdots < i_m = \lfloor k - \epsilon k \rfloor\} \subset [0, k - \epsilon k]$$

such that $i_{j+1} - i_j < (n-k)/2$ for any j and $m = O(1)$. Such a set exists, because $n - k \geqslant n/18 \geqslant k/18$. Consider $W = W_1 \cap W_2 \cap G_{\epsilon k}$, an $\mathbb{F}_p$-vector space of dimension at least $\epsilon sk - O(n^{80c})$. Consider the $\mathbb{F}_p$-quadratic forms on W given by $F_l^{i,j}(w) = F_l(t^i w, t^j w)$ for any $l \in [r]$ and $i, j \in I$, where the map $w \mapsto t^i w$ is identified with the corresponding $\mathbb{F}_p$-linear map between the vectors of coefficients. This is still a family of at most $O(n^{80c})$ bilinear forms. Thus, we can find at least $\Omega(p^{\epsilon sk - O(n^{160c})})$ common isotropic vectors in W to these forms, thanks to Lemma 6. We take c sufficiently small such that the exponent of n in the last equation is less than 1 ($c = 1/161$ is good enough). Then, if k (and thus n) is large enough, there is definitely at least one nonzero polynomial w of degree at most ϵk such that $F_l(t^i w, t^j w) = 0$ for all $i, j \in I$ and $l \in [r]$. Consequently, $\operatorname{rk} B_{t^i w, t^j w} \leqslant \kappa = O(n^c)$ for all $i, j \in I$.

Consider the (symmetric) matrix M of the $\mathbb{F}_q$-bilinear form B restricted to the space of the multiples of w, written in the basis $(wt^i)_{0 \leqslant i < n - \deg w}$. We call the matrix element $B(wt^i, wt^j)$ the *cell* (i, j) of M. The rank of B differs from the rank of M by at most $2\epsilon n$, so it suffices to bound the rank of M.

Now let us examine the (symmetric) matrix $N_{i,j}$ of the quadratic form $B_{t^i w, t^j w}$ in the canonical basis of G_{n-k}.

Observe that the map $u \mapsto t^i w u$, seen as an $\mathbb{F}_q$-linear map (between vectors of coefficients), transforms an element t^j of the canonical basis of G_{n-k} into a basis element $t^{i+j} w$. That means that its matrix in the canonical basis of G_{n-k} and the basis $(wt^i)_{0 \leqslant i < n - \deg w}$ is an $(n - \deg w) \times (n-k)$ matrix, which we can write by block as

$$L_{t^i w} = \begin{pmatrix} 0 \\ I_{n-k} \\ 0 \end{pmatrix},$$

where the central block is an identity block and the other blocks are 0 blocks.

A submatrix of a matrix consisting of consecutive rows and columns is called a *block*. Next we observe that

$$2N_{i,j} = L_{t^i w}^T M L_{t^j w} + L_{t^j w}^T M L_{t^i w},$$

which makes it easy to see that $N_{i,j}$ is the symmetric part of the $(n-k) \times (n-k)$ block of M whose top-left corner is the (i, j) cell of M. Write $M_{i,j}$ for this block.

We remark that if $i = j$, this block is a diagonal block of a symmetric matrix and hence a symmetric matrix, so it must have small rank itself. Hence, the matrix M contains a number of large diagonal blocks $M_{i,i}$ which have small

https://doi.org/10.1112/S0025579319000032 Published online by Cambridge University Press

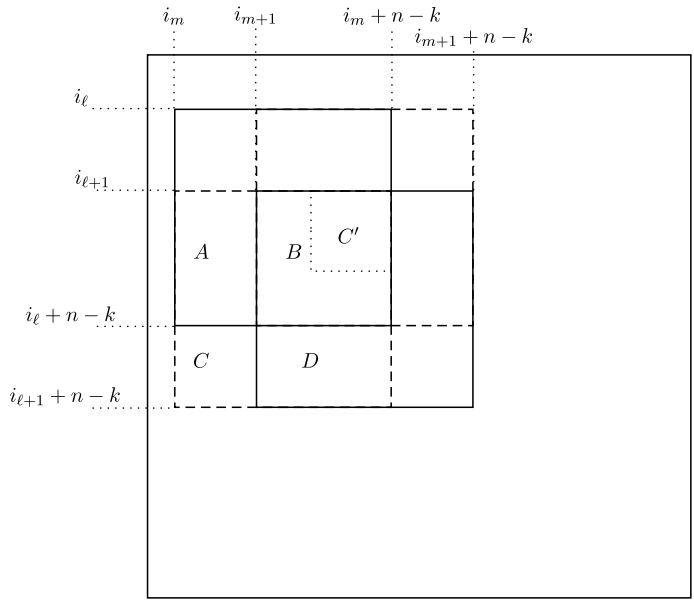


Figure 1: Covering M by submatrices and moving away from the diagonal.

rank. To bound the rank of M, it suffices to bound the ranks of all submatrices $M_{i,j}$ for $(i, j) \in I^2$. Indeed, the matrix M being covered by these submatrices, we have the bound

$$\operatorname{rk} M \leqslant \sum_{(i,j)\in I^2} \operatorname{rk} M_{i,j} \leqslant |I|^2 \max_{(i,j)\in I^2} \operatorname{rk} M_{i,j}.$$

The cardinality $|I|$ being bounded, bounding the ranks of these blocks suffices to bound rk M. We now prove by induction on $\ell - m$ that M_{i_ℓ, i_m} has small rank, namely at most $5^{\ell-m}\kappa$. Because $M_{i_\ell,i_m} = M_{i_m,i_\ell}^T$, it suffices to prove it in the case $\ell \geqslant m$. When $\ell - m = 0$, as we have already seen, the corresponding block is diagonal and of rank at most κ. We now suppose that for some $\ell \geqslant m$ we already know that rk $M_{i_\ell,i_m} \leqslant 5^{\ell-m}\kappa$ and we inspect $M_{i_{\ell+1},i_m}$. The reader can follow the proof in Figure 1.

In Figure 1, the dotted $(n-k)\times(n-k)$ block $M_{i_{\ell+1},i_m} = E$ is made of the four blocks A, B, C, D and it is known to have a symmetric part of small rank. On the other hand, A, B and D are already known to have rank at most $5^{\ell-m}\kappa$, because they are submatrices of M_{i_ℓ,i_m} and $M_{i_{\ell+1},i_{m+1}}$, respectively. Now the symmetric part $E + E^T$ admits as bottom-left square block of the size of C the matrix $C + C'^T$, where C' is the top-right block of B (here it is crucial that $i_{\ell+1} - i_\ell < (n-k)/2$). As a submatrix of a matrix of small rank, $C + C'^T$ must have small rank. But C' has small rank itself as a submatrix of B, whence it follows that $C = (C + C'^T) - C'^T$ has small rank, namely a rank of at most $2 \cdot 5^{\ell-m}\kappa$.

https://doi.org/10.1112/S0025579319000032 Published online by Cambridge University Press

Hence,

$$\operatorname{rk} M_{i_{\ell+1},i_m} = \operatorname{rk} E \leqslant \operatorname{rk} A + \operatorname{rk} B + \operatorname{rk} C + \operatorname{rk} D \leqslant 5^{\ell+1-m}\kappa.$$

This completes the induction proof and implies that $\operatorname{rk} M = O(\kappa) = O(n^c)$.

Finally, as already noted, the rank of B is at most the rank of M plus $2\epsilon n$. In particular, given that $2\epsilon = 1/5$, it is surely less than $c'n$ for some $c' < n/4$ if $n \in Z$ is large enough. Again invoking Corollary 12, we obtain the desired contradiction with the hypothesis (48). This concludes the proof of Theorem 2.

§7. *The Hankel case.* We prove Theorem 3 and again we assume that $p > 2$. If $\alpha = \sum_{j=-\infty}^{m} a_j t^j$, then the matrix of the quadratic form $f \mapsto (\alpha f^2)_{-1}$ in the canonical basis of G_n is

$$M = M(\alpha) = \begin{pmatrix} a_{-1} & a_{-2} & \cdots & a_{-n} \\ a_{-2} & \iddots & \iddots & a_{-n-1} \\ \vdots & \iddots & \iddots & \vdots \\ a_{-n} & \alpha_{-n-1} & \cdots & a_{-2n+1} \end{pmatrix}.$$

We will follow the same strategy as in §§5.2 and 6 with $\Phi(f) = e(\alpha f^2 + \beta f)$. Suppose for a contradiction that, for arbitrarily large n, we have

$$\left| \sum_{f \in G_n} \mu(f)\Phi(f) \right| > \delta q^n \tag{49}$$

with $\delta = q^{-\epsilon' n}$ for some $\epsilon' > 0$ to be decided later. We apply Proposition 14. We discard the first case of that proposition, because in that case the reasoning of §6 goes through without Theorem 5. The parameter $\delta' = (\delta/n)^{O(1)}$ is still at least $q^{-\epsilon n}$ for some $\epsilon = O(\epsilon')$ if n is large enough. Thus, we find a $k \in [n/18, 17n/18]$ such that for at least $q^{(2-\epsilon)(k+1)}$ pairs of polynomials (d, d') of degree k, the quadratic phase on G_{n-k} defined by

$$w \mapsto e(\alpha(d^2 - d'^2)w^2)$$

has rank at most $O(\epsilon n)$. Write $d - d' = a$ and $d + d' = b$. We infer that for at least $q^{(2-\epsilon)(k+1)}$ pairs of polynomials a, b of degree at most k, the quadratic phase

$$w \mapsto e(\alpha a b w^2)$$

has rank at most $c\epsilon n$ for some constant $c = O(1)$.

With the notation of the previous section, the symmetric matrix of that form is

$$M_{a,b} = L_a^T M(\alpha) L_b = L_b^T M(\alpha) L_a = M(\alpha ab).$$

Thus, compared to the general case, $M_{a,b}$ is a product involving M and not a sum of two products, which makes it much easier to analyse. As in the proof of

https://doi.org/10.1112/S0025579319000032 Published online by Cambridge University Press

Theorem 2, we will show that M has low rank by covering it by submatrices of low rank.

By Markov's inequality, there exists a set $X \subset G_{k+1}$ of size $q^{(1-\epsilon)(k+1)}/2$ such that for any $a \in X$, the set

$$B_a := \{b \in G_{k+1} \mid \text{rk } M_{a,b} \leqslant c\epsilon n\}$$

has size at least $q^{(1-\epsilon)(k+1)}/2$.

Let $\eta = 2\epsilon$. For any $i \in \{0, \dots, k - \eta k\}$ and $a \in X$, by the pigeonhole principle, there exist two distinct $b \neq b'$ in B_a such that $f = b' - b = \sum_{m=i}^{i+\eta k} c_m t^m$ for some coefficients c_m. Moreover, we have rk $M_{a,f} \leqslant 2c\epsilon n$. Write $f = f_{a,i}$ to emphasize the dependence. Fix $(i, j) \in \{0, \dots, k - 2\eta k\}^2$. Again the pigeonhole principle implies that there exist $a \neq a' \in X$ such that $g = a - a' \in \text{span}(t^j, \dots, t^{j+2\eta k})$ and $f_{a,i} = f_{a',i}$. If f is this common value, we have rk $M_{g,f} = O(\epsilon n)$. Observe that for such a pair (g, f), we have

$$L_g = \begin{pmatrix} 0 \\ C_g \\ 0 \end{pmatrix},$$

where the central block is an $(n - k + 2\eta k) \times (n - k)$ matrix of rank $n - k$ and the other blocks are 0 blocks. The same holds for L_f with a central block C_f. So, if N is the $(n - k + 2\eta k) \times (n - k + 2\eta k)$ block of M whose top-left cell is (j, i), then $M_{g,f} = C_g^T N C_f$, so that rk $M_{g,f} \geqslant$ rk $N - 4\eta k$. As a result, rk $N = O(\epsilon n)$.

Covering M by a bounded number of blocks of size $(n - k + 2\eta k) \times (n - k + 2\eta k)$, we find that rk $M = O(\epsilon n)$. By taking ϵ small enough, the bound $O(\epsilon n)$ is constrained to be smaller than, say, $n/5$, for n large enough. Thus, if ϵ is small enough (that is, if ϵ' is small enough), we get a contradiction between the hypothesis (49) and Corollary 12. Theorem 3 follows.

It is possible to give an alternative proof of Theorem 3 using the more traditional language of Diophantine properties of α and β. We have opted for the present proof, since it shows parallels between the general case and the special case.

Acknowledgements. The authors would like to thank Ben Green for the suggestion to prove and use a bilinear Bogolyubov theorem, Terence Tao for helpful conversations and Trevor Wooley for suggesting the Hankel case. We are also grateful to Sam Porritt for drawing our attention to [**15**], in which results similar to our linear case are proved, and for useful discussions which led to an improvement of an earlier version of Theorem 1. The first author is thankful to his supervisor Julia Wolf for guidance. We thank the referee for a careful reading and very useful comments which helped to improve the presentation of the paper.

Part of this work was carried out while the first author was staying at the Simons Institute for the Theory of Computing and supported by a travel grant of the University of Bristol Alumni Foundation. He also benefited from the

https://doi.org/10.1112/S0025579319000032 Published online by Cambridge University Press

hospitality of the University of Mississippi. The second author was supported by National Science Foundation Grant DMS-1702296 and a Ralph E. Powe Junior Faculty Enhancement Award from Oak Ridge Associated Universities.

References

1. R. C. Baker and G. Harman, Exponential sums formed with the Möbius function. *J. Lond. Math. Soc.* (2) **43**(2) (1991), 193–198.
2. A. Bhowmick, T. H. Lê and Y.-R. Liu, A note on character sums in finite fields. *Finite Fields Appl.* **46** (2017), 247–254.
3. P.-Y. Bienvenu and T. H. Lê, A bilinear Bogolyubov theorem. *European J. Combin.* **77** (2019), 102–113.
4. M. Car, Distribution des polynômes irréductibles dans $\mathbb{F}_q[T]$. *Acta Arith.* **88**(2) (1999), 141–153.
5. H. Davenport, On some infinite series involving arithmetical functions. *Q. J. Math.* **8** (1937), 8–13.
6. B. Green and T. Tao, An inverse theorem for the Gowers $U^3(G)$ norm. *Proc. Edinb. Math. Soc.* (2) **51**(1) (2008), 73–153.
7. B. Green and T. Tao, Quadratic uniformity of the Möbius function. *Ann. Inst. Fourier (Grenoble)* **58**(6) (2008), 1863–1935.
8. B. Green and T. Tao, The Möbius function is strongly orthogonal to nilsequences. *Ann. of Math.* (2) **175**(2) (2012), 541–566.
9. D. R. Hayes, The distribution of irreducibles in $GF[q, x]$. *Trans. Amer. Math. Soc.* **117** (1965), 101–127.
10. X. He and B. Huang, Exponential sums involving the Möbius function. *Acta Arith.* **175**(3) (2016), 201–209.
11. K. Hosseini and S. Lovett, A bilinear Bogolyubov–Ruzsa lemma with poly-logarithmic bounds. *Preprint*, 2018, arXiv:1808:049651.
12. C.-N. Hsu, The distribution of irreducible polynomials in $\mathbb{F}_q[t]$. *J. Number Theory* **61** (1996), 85–96.
13. T. H. Lê, Green–Tao theorem in function fields. *Acta Arith.* **147** (2011), 129–152.
14. Y.-R. Liu and T. D. Wooley, Waring's problem in function fields. *J. reine angew. Math.* **638** (2010), 1–67.
15. S. Porritt, A note on exponential-Möbius sums over $\mathbb{F}_q[t]$. *Finite Fields Appl.* **51** (2018), 298–305.
16. G. Rhin, Répartition modulo 1 dans un corps de séries formelles sur un corps fini. *Dissertationes Math. (Rozprawy Mat.)* **95** (1972), 75 pp.
17. A. Samorodnitsky, Low-degree tests at large distances. In *STOC'07—Proc. 39th Annu. ACM Symp. Theory of Computing*, ACM (New York, 2007), 506–515.
18. T. Sanders, On the Bogolyubov–Ruzsa lemma. *Anal. PDE* **5**(3) (2012), 627–655.
19. T. Tao and T. Ziegler, The inverse conjecture for the Gowers norm over finite fields via the correspondence principle. *Anal. PDE* **3**(1) (2010), 1–20.
20. T. Zhan and J.-Y. Liu, Exponential sums involving the Möbius function. *Indag. Math. (N.S.)* **7**(2) (1996), 271–278.

Pierre-Yves Bienvenu,
Institut Camille-Jordan, Université Lyon 1,
43 boulevard du 11 novembre 1918,
69622 Villeurbanne cedex,
France
E-mail: pbienvenu@math.univ-lyon1.fr

Thái Hoàng Lê,
Department of Mathematics,
The University of Mississippi,
University, MS 38677,
U.S.A.
E-mail: leth@olemiss.edu

https://doi.org/10.1112/S0025579319000032 Published online by Cambridge University Press