The Quarterly Journal of Mathematics Advance Access published January 17, 2013

The Quarterly Journal of Mathematics
Quart. J. Math. 00 (2013), 1–9; doi:10.1093/qmath/has047

THE AUTOCORRELATION OF THE MÖBIUS FUNCTION AND CHOWLA'S CONJECTURE FOR THE RATIONAL FUNCTION FIELD

by DAN CARMON† *and* ZEÉV RUDNICK‡

(*Raymond and Beverly Sackler School of Mathematical Sciences, Tel Aviv University, Tel Aviv 69978, Israel*)

[Received 23 July 2012]

Abstract

We prove a function field version of Chowla's conjecture on the autocorrelation of the Möbius function in the limit of a large finite field.

1. Introduction

There is a well-known equivalence between the Riemann hypothesis (RH) and square-root cancellation in sums of the Möbius function $\mu(n)$, namely, RH is equivalent to $\sum_{n\leq N}\mu(n) = O(N^{1/2+o(1)})$. This sum measures the correlation between $\mu(n)$ and the constant function. Recent studies have explored the correlation between $\mu(n)$ and other sequences; see [**1**, **2**, **5**]. Sarnak [**8**] showed that $\mu(n)$ does not correlate with any 'deterministic' (i.e. zero entropy) sequence, assuming an old conjecture of Chowla [**3**] on the auto-correlation of the Möbius function, which asserts that given an r-tuple of distinct integers $\alpha_1,\ldots,\alpha_r$ and $\epsilon_i \in \{1,2\}$, not all even, then

$$\lim_{N\to\infty}\frac{1}{N}\sum_{n\leq N}\mu(n+\alpha_1)^{\epsilon_1}\cdots\mu(n+\alpha_r)^{\epsilon_r} = 0. \tag{1.1}$$

Note that the number of non-zero summands here, that is, the number of $n \leq N$ for which $n+\alpha_1,\ldots,n+\alpha_r$ are all square-free, is asymptotically $c(\alpha)N$, where $c(\alpha) > 0$ if the numbers $\alpha_1,\ldots,\alpha_r$ do not contain a complete system of residues modulo p^2 for every prime p [**6**], so that (1.1) is about non-trivial cancellation in the sum.

Chowla's conjecture (1.1) seems intractable at this time, the only known case being $r = 1$ where it is equivalent with the Prime Number Theorem. Our goal in this note is to prove a function field version of Chowla's conjecture.

Let $\mathbb{F}_q$ be a finite field of q elements and $\mathbb{F}_q[x]$ be the polynomial ring over $\mathbb{F}_q$. The Möbius function of a non-zero polynomial $F \in \mathbb{F}_q[x]$ is defined to be $\mu(F) = (-1)^r$ if $F = cP_1\cdots P_r$ with $0 \neq c \in \mathbb{F}_q$ and $P_1,\ldots,P_r$ are distinct monic irreducible polynomials, and $\mu(F) = 0$ otherwise.

Let $M_n \subset \mathbb{F}_q[x]$ be the set of monic polynomials of degree n over $\mathbb{F}_q$, which is of size $\#M_n = q^n$. The number of square-free polynomials in M_n is, for $n > 1$, equal to $q^n - q^{n-1}$ [**7**, Chapter 2]. Hence, given r distinct polynomials $\alpha_1,\ldots,\alpha_r \in \mathbb{F}_q[x]$, with $\deg\alpha_j < n$, the number of $F \in M_n$ for which all of $F(x)+\alpha_j(x)$ are square-free is $q^n + O(rq^{n-1})$ as $q \to \infty$.

†E-mail: dancarmo@post.tau.ac.il

‡Corresponding author. E-mail: rudnick@post.tau.ac.il

For $r > 0$, distinct polynomials $\alpha_1, \ldots, \alpha_r \in \mathbb{F}_q[x]$, with $\deg \alpha_j < n$ and $\epsilon_i \in \{1, 2\}$, not all even, set

$$C(\alpha_1, \ldots, \alpha_r; n) := \sum_{F \in M_n} \mu(F + \alpha_1)^{\epsilon_1} \cdots \mu(F + \alpha_r)^{\epsilon_r}. \tag{1.2}$$

For $r = 1$ and $n > 1$, we have $\sum_{F \in M_n} \mu(F) = 0$ [7, Chapter 2]. For $n = 1$, we have $\mu(F) \equiv -1$ and the sum equals $(-1)^{\sum \epsilon_j} q^n$. For $n > 1$, $r > 1$, we show the following theorem.

THEOREM 1.1. *Fix $r > 1$ and assume that $n > 1$ and q is odd. Then for any choice of distinct polynomials $\alpha_1, \ldots, \alpha_r \in \mathbb{F}_q[x]$, with* $\max \deg \alpha_j < n$*, and $\epsilon_i \in \{1, 2\}$, not all even*

$$|C(\alpha_1, \ldots, \alpha_r; n)| \leq 2rnq^{n-1/2} + 3rn^2 q^{n-1}. \tag{1.3}$$

Thus, for fixed $n > 1$,

$$\lim_{q \to \infty} \frac{1}{\# M_n} \sum_{F \in M_n} \mu(F + \alpha_1)^{\epsilon_1} \cdots \mu(F + \alpha_r)^{\epsilon_r} = 0, \tag{1.4}$$

under the assumption of Theorem 1.1, giving an analogue of Chowla's conjecture (1.1).

Our starting point is Pellet's formula, see, for example, [4, Lemma 4.1], which asserts that for the polynomial ring $\mathbb{F}_q[x]$ with q odd (hence the restriction on the parity of q in Theorem 1.1), the Möbius function $\mu(F)$ can be computed in terms of the discriminant $\operatorname{disc}(F)$ of $F(x)$ as

$$\mu(F) = (-1)^{\deg F} \chi_2(\operatorname{disc}(F)), \tag{1.5}$$

where χ_2 is the quadratic character of $\mathbb{F}_q$. That will allow us to express $C(\alpha_1, \ldots, \alpha_r; n)$ as a character sum and to estimate it.

2. Reduction to a counting problem

2.1. *Character sums*

We use Pellet's formula (1.5) to write

$$C(\alpha_1, \ldots, \alpha_r; n) = (-1)^{nr} \sum_{F \in M_n} \chi_2(\operatorname{disc}(F + \alpha_1)^{\epsilon_1} \cdots \operatorname{disc}(F + \alpha_r)^{\epsilon_r}). \tag{2.1}$$

Since $\operatorname{disc}(F)$ is polynomial in the coefficients of F, (2.1) is an n-dimensional character sum; we will estimate it by trivially bounding all but one variable. We single out the constant term $t := F(0)$ of $F \in M_n$ and write $F(x) = f(x) + t$, with

$$f(x) = x^n + a_{n-1} x^{n-1} + \cdots + a_1 x, \tag{2.2}$$

and set

$$D_f(t) := \operatorname{disc}(f(x) + t), \tag{2.3}$$

which is a polynomial of degree $n - 1$ in t. Therefore, we have

$$|C(\alpha_1, \ldots, \alpha_r; n)| \le \sum_{a \in \mathbb{F}_q^{n-1}} \left| \sum_{t \in \mathbb{F}_q} \chi_2(D_{f+\alpha_1}(t)^{\epsilon_1} \cdots D_{f+\alpha_r}(t)^{\epsilon_r}) \right|. \tag{2.4}$$

We use Weil's theorem (the RH for curves over a finite field), which implies that for a polynomial $P(t) \in \mathbb{F}_q[t]$ of positive degree, which is not proportional to a square of another polynomial, we have [9, Section 2]

$$\left| \sum_{t \in \mathbb{F}_q} \chi_2(P(t)) \right| \le (\deg P - 1) q^{1/2}, \quad P(t) \ne cH^2(t). \tag{2.5}$$

For us, the relevant polynomial is $P(t) = D_{f+\alpha_1}(t)^{\epsilon_1} \cdots D_{f+\alpha_r}(t)^{\epsilon_r}$, which has degree $\le 2r(n-1)$. Instead of requiring that it not be proportional to a square, we impose the stronger requirement that for some i with ϵ_i odd, $D_{f+\alpha_i}(t)$ has positive degree and is square-free and that for all j such that $j \ne i$, $D_{f+\alpha_i}(t)$ and $D_{f+\alpha_j}(t)$ are coprime. We denote the set of coefficients a satisfying the stronger condition by G_n (the 'good' as, where we can apply (2.5)), and let $G_n^c = \mathbb{F}_q^{n-1} \backslash G_n$ be the complement of G_n, where we use the trivial bound q on the character sum. Thus, we deduce that we can bound

$$\begin{aligned} |C(\alpha_1, \ldots, \alpha_r; n)| &\le \sum_{a \in G_n} (2r(n-1) - 1)\sqrt{q} + \sum_{a \notin G_n} q \\ &\le (2r(n-1) - 1) q^{n-1/2} + q \# G_n^c, \end{aligned} \tag{2.6}$$

where we have used the trivial bound $\# G_n \le q^{n-1}$ for the first part of the sum. Theorem 1.1 will follow from the following proposition.

PROPOSITION 2.1. *Assume that $n > 1$ and $\max \deg \alpha_j < n$. Then*

$$\# G_n^c \le 3rn^2 q^{n-2}.$$

2.2. *Bounding $\# G_n^c$*

We can write $G_n^c \subset A_n \cup B_n$ where:

(1) $A_n = A_{n,i}$ is the set of those $a \in \mathbb{F}_q^{n-1}$ for which $D_{f+\alpha_i}(t)$ is either a constant or is not square-free, that is,

$$A_n = \{a \in \mathbb{F}_q^{n-1} : D_{f+\alpha_i}(t) \text{ is constant or } \operatorname{disc}(D_{f+\alpha_i}) = 0\}. \tag{2.7}$$

(2) $B_n = \bigcup_{j \ne i} B(j)$, where $B(j)$ are those as for which $D_{f+\alpha_i}(t)$ and $D_{f+\alpha_j}(t)$ have a common zero, which can be written as the vanishing of their resultant

$$B(j) = \{a \in \mathbb{F}_q^{n-1} : \operatorname{Res}(D_{f+\alpha_i}(t), D_{f+\alpha_j}(t)) = 0\}. \tag{2.8}$$

What is crucial is that A_n and each $B(j)$ are the zero sets of a polynomial equation in the coefficients a; this is a key property of the discriminant and the resultant.

We will need the following elementary but useful uniform upper bound on the number of zeros of polynomials (cf. [9, Section 4, Lemma 3.1]).

LEMMA 2.2. *Let $h(X_1, \dots, X_m) \in \mathbb{F}_q[X_1, \dots, X_m]$ be a non-zero polynomial of total degree at most d. Then the number of zeros of $h(X_1, \dots, X_m)$ in $\mathbb{F}_q^m$ is at most*

$$\#\{x \in \mathbb{F}_q^m : h(x) = 0\} \leq dq^{m-1}. \tag{2.9}$$

As we will see below (see Section 2.3), the equation defining A_n has total degree $3(n-1)(n-2)$ in the coefficients $a_1, \dots, a_{n-1}$, and the equation defining $B(j)$ has total degree $\leq 3(n-1)^2$. Therefore, by Lemma 2.2, if we show that the equations defining A_n, $B(j)$ are not identically zero, then we will have proved

$$\#A_n \leq 3n^2 q^{n-2} \tag{2.10}$$

and

$$\#B_n \leq 3(r-1)n^2 q^{n-2}. \tag{2.11}$$

This immediately gives Proposition 2.1.

In order to show that a polynomial $h \in \mathbb{F}_q[X_1, \dots, X_m]$ is not identically zero, we may instead consider it as a polynomial defined over $\bar{\mathbb{F}}_q$, the algebraic closure of $\mathbb{F}_q$. In this context, we can investigate the zero set $Z_h = \{a \in \bar{\mathbb{F}}_q^m : h(a) = 0\}$, which is a subvariety of the affine space $\mathbb{A}^m$. The polynomial h is not identically zero if and only if $Z \neq \mathbb{A}^m$. This shall be our main tool in the following sections.

2.3. *Resultant and discriminant formulas*

The discriminant $\operatorname{disc}(F)$ of a polynomial $F(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$, $a_n \neq 0$, is given in term of its roots $r_1, \dots, r_n$ in the algebraic closure $\bar{\mathbb{F}}_q$ as $\operatorname{disc} F = a_n^{2n-2} \prod_{i<j}(r_i - r_j)^2$, and is a homogeneous polynomial with integer coefficients in $a_0, \dots, a_n$, with degree of homogeneity $2n-2$, has total degree $2n-2$, and has degree $n-1$ as a polynomial in a_0. Moreover, if a_i is regarded as having degree i, then $\operatorname{disc}(F)$ is homogeneous of degree $n(n-1)$, that is, for every monomial $c_r \prod_i a_i^{r_i}$ in $\operatorname{disc}(F)$,

$$\sum_i i r_i = n(n-1). \tag{2.12}$$

The resultant of two polynomials $F(x) = a_n x^n + \cdots$, $G = b_m x^m + \cdots$, of degrees n and m, is

$$\operatorname{Res}(F, G) = a_n^m b_m^n \prod_{F(\rho)=0} \prod_{G(\eta)=0} (\rho - \eta). \tag{2.13}$$

It is a homogeneous polynomial of degree $m+n$ in the coefficients of F and G, in fact it is homogeneous of degree m in $a_0, \dots, a_n$ and of degree n in $b_0, \dots, b_m$. Moreover, if a_i, b_i are regarded as having degree i, then $\operatorname{Res}(F, G)$ is homogeneous of degree mn. We have

$$\operatorname{Res}(F, G) = a_n^m \prod_{F(\rho)=0} G(\rho) = (-1)^{mn} b_m^n \prod_{G(\eta)=0} F(\eta). \tag{2.14}$$

Furthermore, the discriminant of a polynomial $F(x) = a_n x^n + \cdots + a_0$ of degree n may be computed in terms of the resultant as

$$\operatorname{disc} F = (-1)^{n(n-1)/2} a_n^{n-\deg(F')-2} \operatorname{Res}(F, F'). \tag{2.15}$$

We apply this to compute the discriminant of $D_f(t) = \operatorname{disc}(f(x)+t)$, $f(x) = x^n + a_{n-1}x^{n_1} + \cdots + a_1 x$. The discriminant $\operatorname{disc}(D_f(t))$ is a polynomial in the coefficients $a_1, \dots, a_{n-1}$ of $f(x)$. We claim that the total degree of $\operatorname{disc} D_f(t)$ is $3(n-1)(n-2)$. Indeed, $D_f(t) = \sum_{j=0}^{n-1} b_j t^j$ is a polynomial of degree $n-1$ in t, and since it is homogeneous of degree $2(n-1)$ in $t, a_1, \dots, a_{n-1}$ we find that b_j are polynomials of total degree $2(n-1) - j$ in the a_js. Now $\operatorname{disc} D_f(t) = \sum c_r \prod_j b_j^{r_j}$ has total degree $2(n-1) - 2 = 2(n-2)$ in the b_js, that is, $\sum r_j = 2(n-2)$, and by (2.12), $\sum_j j r_j = (n-1)(n-2)$. Thus, the total degree of $\operatorname{disc} D_f(t)$ in $a_1, \dots, a_{n-1}$ is

$$\begin{aligned}\sum_j r_j \deg b_j &= \sum r_j (2(n-1) - j) = 2(n-1) \sum r_j - \sum j r_j \\ &= 2(n-1) \cdot 2(n-2) - (n-1)(n-2) = 3(n-1)(n-2),\end{aligned}$$

as claimed.

Arguing similarly, one sees that the resultant $\operatorname{Res}(D_f(t), D_{f+\alpha}(t))$ has total degree $3(n-1)^2$ in the coefficients $a_1, \dots, a_{n-1}$.

Assume $\gcd(q, n) = 1$. Then $f'(t) = nx^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots$ has degree $n-1$ and by (2.14) and (2.15) we find

$$D_f(t) = \operatorname{disc}_x(f(x)+t) = (-1)^{n(n-1)/2} n^n \prod_{f'(\rho)=0} (t + f(\rho)) \tag{2.16}$$

has degree $n-1$, with roots $-f(\rho)$ as ρ runs over the $n-1$ roots of $f'(x)$.

In the case where $\gcd(q, n) > 1$, $f'(t) = -a_{n-1}x^{n-2} + \cdots$ has degree $n-2$ provided that $a_{n-1} \neq 0$, in which case by (2.14) and (2.15) we have

$$D_f(t) = \operatorname{disc}_x(f(x)+t) = (-1)^{n(n-1)/2} a_{n-1}^n \prod_{f'(\rho)=0} (t + f(\rho)), \tag{2.17}$$

which has degree $n-2$ and again has roots $-f(\rho)$ as ρ runs over the $n-2$ roots of $f'(x)$.

3. Non-vanishing of the resultant

PROPOSITION 3.1. *Given a non-zero polynomial $\alpha \in \mathbb{F}_q[x]$, with $\deg \alpha < n$, then $a \mapsto \operatorname{Res}(D_f(t), D_{f+\alpha}(t))$ is not the zero polynomial, that is, the polynomial function*

$$R(a) := \operatorname{Res}_t(D_f(t), D_{f+\alpha}(t)) \in \mathbb{Z}[\vec{a}] \tag{3.1}$$

is not identically zero.

Applying this to $\alpha = \alpha_j - \alpha_i$ for each $j \neq i$ will show that (2.11) holds.

Proof. Write $\alpha(x) = A_{n-1}x^{n-1} + \cdots + A_0 \in \mathbb{F}_q[x]$ with $\deg \alpha < n$.

Let p be the characteristic of $\mathbb{F}_q$. Assume first that $p \nmid n$. Then, by (2.14) and (2.16), we find

$$\operatorname{Res}(D_f, D_{f+\alpha}) = n^{2n(n-1)} \prod_{\substack{f'(\rho_1)=0 \\ f'(\rho_2)+\alpha'(\rho_2)=0}} (f(\rho_2) + \alpha(\rho_2) - f(\rho_1)). \tag{3.2}$$

If $p \mid n$, but $a_{n-1} \neq 0$ and $a_{n-1} + A_{n-1} \neq 0$, then by (2.14) and (2.17), we find

$$\operatorname{Res}(D_f, D_{f+\alpha}) = a_{n-1}^{n(n-2)} (a_{n-1} + A_{n-1})^{n(n-2)} \times \prod_{\substack{f'(\rho_1)=0 \\ f'(\rho_2)+\alpha'(\rho_2)=0}} (f(\rho_2) + \alpha(\rho_2) - f(\rho_1)). \tag{3.3}$$

Note that when $a_{n-1} = 0$ or $a_{n-1} + A_{n-1} = 0$, the resultant $\operatorname{Res}(D_f, D_{f+\alpha})$ is given by different polynomials than in the above case. However, this might affect at most $2q^{n-2}$ 'bad' $\vec{a}$s, which is a negligible amount, and the conclusion of (2.11) remains valid.

In both cases above, the 'bad' $\vec{a}$s are those for which there are $\rho_1, \rho_2 \in \bar{\mathbb{F}}_q$ such that

$$f'(\rho_1) = 0, \quad f'(\rho_2) = -\alpha'(\rho_2), \quad f(\rho_2) - f(\rho_1) = -\alpha(\rho_2). \tag{3.4}$$

This is a *linear* system of equations for $\vec{a} \in \mathbb{A}^{n-1}$, which has the form

$$M(\rho)a = b(\rho), \quad \rho = (\rho_1, \rho_2), \tag{3.5}$$

for a suitable $3 \times (n-1)$ matrix $M(\rho)$ and vector $b(\rho) \in \mathbb{A}^3$. Thus, over $\bar{\mathbb{F}}_q$, the solutions of $R(\vec{a}) = 0$ are precisely those $\vec{a} \in \bar{\mathbb{F}}_q^{n-1}$ which satisfy the system (3.5) for some $\rho \in \bar{\mathbb{F}}_q^2$.

We consider the affine variety (possibly reducible) defined by these equations

$$Z = \{(\rho, a) \in \mathbb{A}^2 \times \mathbb{A}^{n-1} : M(\rho)a = b(\rho)\} \subset \mathbb{A}^2 \times \mathbb{A}^{n-1}. \tag{3.6}$$

Let $\phi : Z \to \mathbb{A}^{n-1}$ be the restriction to Z of the projection $\mathbb{A}^2 \times \mathbb{A}^{n-1} \to \mathbb{A}^{n-1}$ and $\pi : Z \to \mathbb{A}^2$ be the restriction to Z of the projection $\mathbb{A}^2 \times \mathbb{A}^{n-1} \to \mathbb{A}^2$.

$$\begin{tikzcd} & Z \subset \mathbb{A}^2 \times \mathbb{A}^{n-1} \arrow[dl, "\pi"'] \arrow[dr, "\phi"] & \\ \mathbb{A}^2 & & \mathbb{A}^{n-1} \end{tikzcd} \tag{3.7}$$

From the above, the solution set of $R(\vec{a}) = 0$ is precisely $\phi(Z)$.

We will show that Z has dimension $n-2$, and hence the dimension of $\{R = 0\} = \phi(Z)$ cannot exceed $n-2$ and hence is not all of $\mathbb{A}^{n-1}$. Thus, R is not the zero polynomial, proving Proposition 3.1.

To do so, we study the dimensions of the fibres $\pi^{-1}(\rho)$, which are affine linear subspaces. We first assume that $n > 3$. In this case, we will show that $\pi(Z)$ is dense in $\mathbb{A}^2$ and generically, that is, if $\rho_1 \neq \rho_2$, the fibres $\pi^{-1}(\rho)$ have dimension $n-4$. Moreover, there are at most $\deg \alpha$ non-generic fibres, each of dimension $n-2$. This will show that $\dim Z = n-2$.

We rewrite the system (3.5) as

$$\begin{aligned} \cdots + 3a_3\rho_1^2 + 2a_2\rho_1 + a_1 &= -n\rho_1^{n-1}, \\ \cdots + 3a_3\rho_2^2 + 2a_2\rho_2 + a_1 &= -\alpha'(\rho_2) - n\rho_2^{n-1}, \\ \cdots + a_3(\rho_2^3 - \rho_1^3) + a_2(\rho_2^2 - \rho_1^2) + a_1(\rho_2 - \rho_1) &= -\alpha(\rho_2) - (\rho_2^n - \rho_1^n). \end{aligned} \tag{3.8}$$

To find the rank of the matrix $M(\rho)$, we compute that

$$\det \begin{pmatrix} 3\rho_1^2 & 2\rho_1 & 1 \\ 3\rho_2^2 & 2\rho_2 & 1 \\ \rho_2^3 - \rho_1^3 & \rho_2^2 - \rho_1^2 & \rho_2 - \rho_1 \end{pmatrix} = (\rho_1 - \rho_2)^4, \tag{3.9}$$

and thus $M(\rho)$ has full rank 3 unless $\rho_1 = \rho_2$, and so the generic fibres $\pi^{-1}(\rho)$ have dimension $n - 1 - 3 = n - 4$.

In the non-generic case $\rho_1 = \rho_2$, the matrix has rank 1 and we need $\alpha'(\rho_2) = 0 = \alpha(\rho_2)$, which constrains us to have at most finitely many fibres (the number bounded by $\deg \alpha/2$), each of which has dimension $n - 1 - 1 = n - 2$.

Finally, the cases $n = 2, 3$ are handled similarly, except that the image of the map $\pi : Z \to \mathbb{A}^2$ is no longer dense, due to algebraic conditions constraining ρ_1, ρ_2. We omit the (tedious) details. $\square$

4. Non-vanishing of the discriminant

We wish to show that the condition for being in A_n is not always satisfied. Without loss of generality, we can assume $\alpha_i = 0$. We first study a couple of small degree cases.

For $n = 2$, $\mathrm{disc}(x^2 + ax + t) = a^2 - 4t$ is linear and hence has no repeated roots (recall q is odd), hence A_n is empty. When $n = 3$, we have

$$D_f(t) = \mathrm{disc}_x(x^3 + ax^2 + bx + t) = (a^2b^2 - 4b^3) + (18ab - 4a^3)t - 27t^2. \tag{4.1}$$

If $3 \mid q$, then $D_f(t) = (a^2b^2 - 4b^3) - 4a^3t$ has degree 1 for $a \neq 0$; if $3 \nmid q$, then $D(t)$ has degree 2 and we compute that

$$\mathrm{disc}_t\ \mathrm{disc}_x(x^3 + ax^2 + bx + t) = -16(a^2 - 3b)^3, \tag{4.2}$$

which is clearly not identically zero. So we may assume $n \geq 4$.

4.1.

Similarly to our approach in the previous section, it suffices to show that outside a set of $\vec{a}$s of codimension at least 1 in the parameter space $\mathbb{A}^{n-1}$, $D_f(t)$ is of positive degree, and is square-free, that is, with non-zero discriminant.

We conclude from (2.16) and (2.17) that if $n \geq 4$ and $\vec{a}$ is in the 'bad' set (but $a_{n-1} \neq 0$ if $\gcd(n, q) \neq 1$), then at least one of the following occurs:

(1) There is some $\rho \in \bar{\mathbb{F}}_q$ for which $f'(x)$ has a double zero at $x = \rho$, that is, there is some $\rho \in \bar{\mathbb{F}}_q$ for which

$$f'(\rho) = 0, \quad f''(\rho) = 0. \tag{4.3}$$

(2) There are two distinct $\rho_1 \neq \rho_2$ so that $f(\rho_1) = f(\rho_2)$ and so that $f'(x)$ vanishes at both $x = \rho_1$ and $x = \rho_2$, that is,

$$f'(\rho_1) = 0, \quad f'(\rho_2) = 0, \quad f(\rho_1) = f(\rho_2). \tag{4.4}$$

We want to show that the set of $\vec{a} \in \bar{\mathbb{F}}_q^{n-1}$, which solves at least one of (4.3) and (4.4), has dimension at most $n - 2$.

4.2.

We first look at f for which (4.3) happens. This gives a pair of equations for $\vec{a} \in \bar{\mathbb{F}}_q^{n-1}$:

$$\begin{aligned} \cdots + 2\rho a_2 + a_1 &= -n\rho^{n-1}, \\ \cdots + 2a_2 + 0 &= -n(n-1)\rho^{n-2}. \end{aligned} \tag{4.5}$$

Defining

$$W = \{(\rho, \vec{a}) \in \mathbb{A}^1 \times \mathbb{A}^{n-1} : (4.3) \text{ holds}\}, \tag{4.6}$$

we have a fibration of W over the ρ line $\mathbb{A}^1$ and a map $\phi : W \to \mathbb{A}^{n-1}$, the restriction of the projection $\mathbb{A}^1 \times \mathbb{A}^{n-1} \to \mathbb{A}^{n-1}$,

$$\begin{tikzcd} & W \subset \mathbb{A}^1 \times \mathbb{A}^{n-1} \arrow[dl, "\pi"'] \arrow[dr, "\phi"] & \\ \mathbb{A}^1 & & \mathbb{A}^{n-1} \end{tikzcd} \tag{4.7}$$

and the solutions of (4.3) are precisely $\phi(W)$.

The system (4.5) is non-singular (rank 2) and hence $\pi : W \to \mathbb{A}^1$ is surjective and for each ρ the dimension of the solution set is $n - 1 - 2 = n - 3$. We find that $\dim W = n - 2$ and hence $\dim \phi(W) \leq n - 2$.

4.3.

Next we consider the system (4.4) which given $\rho_1 \neq \rho_2$ is a linear system for $\vec{a} \in \bar{\mathbb{F}}_q^{n-1}$ of the form

$$\begin{aligned} \cdots + 3\rho_1^2 a_3 + 2\rho_1 a_2 + a_1 &= -n\rho_1^{n-1}, \\ \cdots + 3\rho_2^2 a_3 + 2\rho_2 a_2 + a_1 &= -n\rho_2^{n-1}, \\ \cdots + (\rho_2^3 - \rho_1^3)a_3 + (\rho_2^2 - \rho_1^2)a_2 + (\rho_2 - \rho_1)a_1 &= -\rho_2^n + \rho_1^n. \end{aligned} \tag{4.8}$$

This system shares the matrix part of (3.8), and hence has rank 3 for every $\rho_1 \neq \rho_2$. Thus, the arguments of the previous section show that

$$\{\vec{a} \in \mathbb{A}^{n-1} : \exists \rho_1 \neq \rho_2 \text{ s.t. (4.4) holds}\} \tag{4.9}$$

is of dimension at most $n-2$. This shows that (2.10) holds, thus concluding the proof of Proposition 2.1.

Funding

The research leading to these results has received funding from the European Research Council under the European Union's Seventh Framework Programme (FP7/2007-2013)/ERC grant agreement no. 320755.

References

1. J. Bourgain, P. Sarnak and T. Ziegler, *Disjointness of Möbius from horocycle flows*, preprint, 2011, arXiv:1110.0992v1.

2. F. Cellarosi and Ya. G. Sinai, The Möbius function and statistical mechanics, *Bull. Math. Sci.* **1** (2011), 245–275.

3. S. Chowla, *The Riemann Hypothesis and Hilbert's Tenth Problem*, Gordon & Breach, NY, 1965.

4. K. Conrad, Irreducible values of polynomials: a non-analogy, *Number Fields and Function Fields: Two Parallel Worlds*, Progress in Mathematics 239, Birkhäuser, Basel, 2005, 71–85.

5. B. Green and T. Tao, The Möbius function is strongly orthogonal to nilsequences, *Ann. of Math.* (2) **175** (2012), 541–566.

6. L. Mirsky, Note on an asymptotic formula connected with r-free integers, *Quart. J. Math. Oxford Ser.* **18** (1947), 178–182.

7. M. Rosen, *Number Theory in Function Fields*, Graduate Texts in Mathematics 210, Springer, New York, 2002.

8. P. Sarnak, *Three lectures on Möbius randomness*, 2011, http://www.math.ias.edu/files/wam/2011/PSMobius.pdf.

9. W. M. Schmidt, *Equations over Finite Fields: An Elementary Approach*, 2nd edn, Kendrick Press, Heber City, UT, 2004.