



On the distribution of the Rudin-Shapiro function for finite fields

Cécile Dartyge, László Mérai, Arne Winterhof

► To cite this version:

Cécile Dartyge, László Mérai, Arne Winterhof. On the distribution of the Rudin-Shapiro function for finite fields. Proceedings of the American Mathematical Society, 2021, 10.1090/proc/15668 . hal-03090416v2

HAL Id: hal-03090416

<https://hal.science/hal-03090416v2>

Submitted on 16 Mar 2021

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

On the distribution of the Rudin-Shapiro function for finite fields

CÉCILE DARTYGE¹, LÁSZLÓ MÉRAI², ARNE WINTERHOF²

¹ Institut Élie Cartan, Université de Lorraine
BP 239, 54506 Vandœuvre Cedex, France
e-mail: cecile.dartyge@univ-lorraine.fr

² Johann Radon Institute for
Computational and Applied Mathematics
Austrian Academy of Sciences
Altenbergerstr. 69, 4040 Linz, Austria
e-mail: {laszlo.merai, arne.winterhof}@oeaw.ac.at

In memory of Christian Mauduit

Abstract

Let $q = p^r$ be the power of a prime p and $(\beta_1, \dots, \beta_r)$ be an ordered basis of \mathbb{F}_q over \mathbb{F}_p . For

$$\xi = \sum_{j=1}^r x_j \beta_j \in \mathbb{F}_q \quad \text{with digits } x_j \in \mathbb{F}_p,$$

we define the Rudin-Shapiro function R on \mathbb{F}_q by

$$R(\xi) = \sum_{i=1}^{r-1} x_i x_{i+1}, \quad \xi \in \mathbb{F}_q.$$

For a non-constant polynomial $f(X) \in \mathbb{F}_q[X]$ and $c \in \mathbb{F}_p$ we study the number of solutions $\xi \in \mathbb{F}_q$ of $R(f(\xi)) = c$. If the degree d of $f(X)$ is fixed, $r \geq 6$ and $p \rightarrow \infty$, the number of solutions is asymptotically p^{r-1} for any c . The proof is based on the Hooley-Katz Theorem.

MSC 2020. 11A63, 11T23, 11T30

Keywords. finite fields, digit sums, Hooley-Katz Theorem, polynomial equations, Rudin-Shapiro function

1 Introduction

In recent years, many spectacular results have been obtained on important problems combining some arithmetic properties of the integers and some conditions on their digits in a given basis, see for example [1, 2, 8, 13–15, 17, 19, 23]. In particular, Drmota, Mauduit and Rivat [8] and Müllner [17] showed that Thue-Morse sequence and Rudin-Shapiro sequence along squares are both normal, that is, each binary pattern of the same length appears asymptotically with the same frequency.

A natural question is to study analog problems in finite fields, see for example [4, 5, 7, 9, 12, 18, 20–22]. Many of these problems can be solved for finite fields although their analogs for integers are actually out of reach.

In particular, it is conjectured but not proved yet that the subsequences of the Thue-Morse sequence and Rudin-Shapiro sequence along any polynomial of degree $d \geq 3$ are normal, see [8, Conjecture 1]. Even the weaker problem of determining the frequency of 0 and 1 in the subsequence of the Thue-Morse sequence and Rudin-Shapiro sequence along any polynomial of degree $d \geq 3$ seems to be out of reach, see [8, above Conjecture 1]. However, the analog of the latter weaker problem for the Thue-Morse sequence in the finite field setting was settled by the first author and Sárközy [5].

This paper deals with the following analog of the frequency problem for the Rudin-Shapiro sequence along polynomials.

Let $q = p^r$ be the power of a prime p and $\mathcal{B} = (\beta_1, \dots, \beta_r)$ be an ordered basis of the finite field \mathbb{F}_q over \mathbb{F}_p . Then any $\xi \in \mathbb{F}_q$ has a unique representation

$$\xi = \sum_{j=1}^r x_j \beta_j \quad \text{with } x_j \in \mathbb{F}_p, \quad j = 1, \dots, r.$$

The coefficients x_1, \dots, x_r are called the *digits* with respect to the basis \mathcal{B} .

In order to consider the finite field analogue of the Rudin-Shapiro sequence along polynomial values, we define the *Rudin-Shapiro function* $R(\xi)$ for the finite field \mathbb{F}_q with respect to the basis \mathcal{B} by

$$R(\xi) = \sum_{i=1}^{r-1} x_i x_{i+1}, \quad \xi = x_1 \beta_1 + \dots + x_r \beta_r \in \mathbb{F}_q, \quad r \geq 2.$$

For $f(X) \in \mathbb{F}_q[X]$ and $c \in \mathbb{F}_p$ we put

$$\mathcal{R}(c, f) = \{\xi \in \mathbb{F}_q : R(f(\xi)) = c\}.$$

Our goal is to prove that the size of $\mathcal{R}(c, f)$ is asymptotically the same for all c .

Our main result is the following theorem.

Theorem 1. *Let $f(X) \in \mathbb{F}_q[X]$ be of degree $d \geq 1$. For $c \in \mathbb{F}_p$ we have*

$$|\mathcal{R}(c, f)| - p^{r-1} \leq C_{d,r} p^{(3r+1)/4 - h_{r,c}},$$

where $h_{r,c}$ is defined by

$$h_{r,c} = \begin{cases} 3/4, & r \text{ even and } c \neq 0, \\ 1/2, & r \text{ odd and } c \neq 0, \\ 1/4, & r \text{ even and } c = 0, \\ 0, & r \text{ odd and } c = 0, \end{cases}$$

and $C_{d,r}$ is a constant depending only on d and r .

In particular, we have for fixed d ,

$$\lim_{p \rightarrow \infty} \frac{|\mathcal{R}(c, f)|}{p^{r-1}} = 1 \quad \text{for } c \neq 0 \text{ and } r \geq 4 \text{ or } c = 0 \text{ and } r \geq 6.$$

For $d = 1$, or more generally, for any permutation polynomial $f(X)$ of \mathbb{F}_q , it is easy to see that

$$|\mathcal{R}(c, f)| = \begin{cases} p^{r-1} - p^{\lfloor (r-1)/2 \rfloor}, & c \neq 0, \\ p^{r-1} + p^{\lfloor (r+1)/2 \rfloor} - p^{\lfloor (r-1)/2 \rfloor}, & c = 0, \end{cases} \quad r \geq 2.$$

For the convenience of the reader we will provide a very short proof in Section 2. Hence, it remains to prove Theorem 1 for $d \geq 2$.

A commonly used idea, for example in [4], to estimate the number of solutions of certain equations over finite fields is to apply the Weil bound. In some special situations the Deligne bound [6, Théorème 8.4] provides stronger results. The Weil bound has the only condition $d \geq 1$ but is too weak for our purpose. The Deligne bound needs some more intricate technical conditions which are not satisfied in our situation, see Section 6. Our main tool is a generalization of Deligne's Theorem for projective surfaces [6], the Hooley-Katz Theorem [10], see Lemma 1 in Section 3 below. The crucial steps in the proof are:

1. Identify $R(f(X))$ with a multivariate polynomial of the form

$$Q(Y_0, \dots, Y_{r-1}) = \sum_{j,k=0}^{r-1} a_{j,k} f_j(Y_j) f_k(Y_k),$$

which is done in Section 4. Note that this polynomial has coefficients in \mathbb{F}_q .

2. Estimate the dimensions of the singular loci, defined in Section 3 below, of $Q - c$ and its homogeneous part of largest degree, see Lemma 2 below.
3. We complete the proof in Section 4. After a linear variable substitution, Q is transformed to a polynomial F of the same degree as Q but with coefficients in \mathbb{F}_p . In particular, the dimensions of the singular loci are invariant under this linear transformation. Then we apply the Hooley-Katz Theorem to $F - c$.

2 The case of permutation polynomials

For a permutation polynomial $f(X)$ of \mathbb{F}_q , $|\mathcal{R}(c, f)|$ is the number $N_r(c)$ of solutions $(x_1, \dots, x_r) \in \mathbb{F}_p^r$ of the equation

$$x_1x_2 + \dots + x_{r-1}x_r = c.$$

We have

$$N_r(c) = \begin{cases} p^{r-1} - p^{\lfloor (r-1)/2 \rfloor}, & c \neq 0, \\ p^{r-1} + p^{\lfloor (r+1)/2 \rfloor} - p^{\lfloor (r-1)/2 \rfloor}, & c = 0, \end{cases} \quad r \geq 2,$$

which can be easily verified using the recursion

$$N_r(c) = pN_{r-2}(c) + (p-1)p^{r-2}, \quad r \geq 4.$$

This recursion is obtained by distinguishing the cases $x_{r-1} = 0$ and $x_{r-1} \neq 0$.

3 The Hooley-Katz Theorem

We denote by $\overline{\mathbb{F}_p}$ the algebraic closure of \mathbb{F}_p .

The *(affine) singular locus* $\mathcal{L}(F)$ of a polynomial F over \mathbb{F}_p in r variables is the set of common zeros in $\overline{\mathbb{F}_p}^r$ of the polynomials

$$F, \frac{\partial F}{\partial X_1}, \dots, \frac{\partial F}{\partial X_r}.$$

Our main tool is the following result, see [16, Theorem 7.1.14], which is the affine version of the Hooley-Katz Theorem [10].

Lemma 1 (Hooley-Katz). *Let F be a polynomial over \mathbb{F}_p in r variables of degree $D \geq 1$ such that the dimensions of the singular loci of F and its homogeneous part F_D of degree D satisfy*

$$\max\{\dim(\mathcal{L}(F)), \dim(\mathcal{L}(F_D)) - 1\} \leq s.$$

Then the number N of zeros of F in \mathbb{F}_p^r satisfies

$$|N - p^{r-1}| \leq C_{D,r} p^{(r+s)/2},$$

where $C_{D,r}$ is a constant depending only on D and r .

We remark, that in the statement $\dim(\mathcal{L}(F_D))$ denotes the dimension of the *affine* singular locus of the homogeneous polynomial F_D while in [16, Theorem 7.1.14] the dimension of the *projective* singular locus is considered. The difference of these dimensions is 1.

4 Proof of Theorem 1

First, we express the Rudin-Shapiro function $R(\xi)$ of \mathbb{F}_q in terms of the trace and the dual basis.

Let φ be the *Frobenius automorphism* defined by

$$\varphi(\xi) = \xi^p \quad \text{for } \xi \in \mathbb{F}_q.$$

We extend φ to the polynomial ring $\mathbb{F}_q[X_1, \dots, X_r]$ by

$$\varphi(X_i) = X_i, \quad i = 1, \dots, r.$$

Let

$$\text{Tr}(\xi) = \xi + \varphi(\xi) + \dots + \varphi^{r-1}(\xi) \in \mathbb{F}_p$$

denote the (absolute) *trace* of $\xi \in \mathbb{F}_q$. Let $(\delta_1, \dots, \delta_r)$ denote the (existent and unique) *dual basis* of the basis $\mathcal{B} = (\beta_1, \dots, \beta_r)$ of \mathbb{F}_q , see for example [11], that is,

$$\text{Tr}(\delta_i \beta_j) = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{if } i \neq j, \end{cases} \quad 1 \leq i, j \leq r. \quad (1)$$

Then we have

$$\text{Tr}(\delta_i \xi) = x_i \quad \text{for any } \xi = \sum_{j=1}^r x_j \beta_j \in \mathbb{F}_q \quad \text{with } x_j \in \mathbb{F}_p.$$

For $f(X) \in \mathbb{F}_q[X]$ we obtain that

$$\begin{aligned} R(f(\xi)) &= \sum_{i=1}^{r-1} \text{Tr}(\delta_i f(\xi)) \text{Tr}(\delta_{i+1} f(\xi)) \\ &= \sum_{i=1}^{r-1} \sum_{j,k=0}^{r-1} \varphi^j(\delta_i) \varphi^k(\delta_{i+1}) \varphi^j(f(\xi)) \varphi^k(f(\xi)). \end{aligned}$$

Write

$$\begin{aligned} &F(X_1, \dots, X_r) \\ &= \sum_{j,k=0}^{r-1} a_{j,k} f_j(\beta_1^{p^j} X_1 + \dots + \beta_r^{p^j} X_r) f_k(\beta_1^{p^k} X_1 + \dots + \beta_r^{p^k} X_r), \end{aligned} \quad (2)$$

where

$$a_{j,k} = \sum_{i=1}^{r-1} \varphi^j(\delta_i) \varphi^k(\delta_{i+1}), \quad j, k = 0, \dots, r-1, \quad (3)$$

and $f_j = \varphi^j(f) \in \mathbb{F}_q[X]$. Verify $\varphi(F) = F$, that is, $F \in \mathbb{F}_p[X_1, \dots, X_r]$ and

$$R(f(\xi)) = F(x_1, \dots, x_r) \quad \text{for } \xi = \sum_{i=1}^r x_i \beta_i, \quad x_i \in \mathbb{F}_p.$$

Theorem 1 follows from Lemma 1 and the following lemma which we prove in the next section.

Lemma 2. *Let $f(X) \in \mathbb{F}_q[X]$ be of degree d with $2 \leq d < p$ and $F \in \mathbb{F}_p[X_1, \dots, X_r]$ be defined by (2). Then F has degree $2d$. Moreover, for any $c \in \mathbb{F}_p$ we have*

$$\dim(\mathcal{L}(F - c)) \leq \begin{cases} r/2 - 1, & r \text{ even and } c \neq 0, \\ (r-1)/2, & r \text{ odd and } c \neq 0, \\ r/2, & r \text{ even and } c = 0, \\ (r+1)/2, & r \text{ odd and } c = 0. \end{cases}$$

Furthermore, if $F_{2d} \in \mathbb{F}_p[X_1, \dots, X_r]$ is the homogeneous part of F of degree $2d$, then

$$\dim(\mathcal{L}(F_{2d})) \leq \begin{cases} r/2, & r \text{ even}, \\ (r+1)/2, & r \text{ odd}. \end{cases}$$

5 Proof of Lemma 2

Consider the linear transformation on $\overline{\mathbb{F}_p}^r$

$$y_i = \sum_{j=1}^r \beta_j^{p^i} x_j, \quad i = 0, \dots, r-1.$$

It is invertible with inverse

$$x_k = \sum_{i=0}^{r-1} \delta_k^{p^i} y_i, \quad k = 1, \dots, r, \quad (4)$$

by (1).

Then we denote by Q the polynomial obtained from F , defined by (2), with the corresponding variable transformation,

$$F(X_1, \dots, X_r) = \sum_{j,k=0}^{r-1} a_{j,k} f_j(Y_j) f_k(Y_k) = Q(Y_0, \dots, Y_{r-1}),$$

where

$$Y_i = \sum_{j=1}^r \beta_j^{p^i} X_j, \quad i = 0, \dots, r-1. \quad (5)$$

As the degree and the dimension, see [3, Corollary 9.5.3], of singular loci are invariant under the regular transformation (5), it is enough to show the results for the polynomial Q .

We may assume that $f(X)$ is monic since otherwise we multiply the basis \mathcal{B} element-wise with the leading coefficient of $f(X)$. The degree $2d$ homogeneous part of Q is

$$Q_{2d}(Y_0, \dots, Y_{r-1}) = \sum_{j,k=0}^{r-1} a_{j,k} Y_j^d Y_k^d.$$

By the definition (3) of $a_{j,k}$ we have

$$\sum_{j=0}^{r-1} a_{j,0} \beta_1^{p^j} = \sum_{i=1}^{r-1} \delta_{i+1} \text{Tr}(\beta_1 \delta_i) = \delta_2 \neq 0.$$

Hence, $a_{j,0} \neq 0$ for some j . Since $Y_j^d Y_k^d$, $0 \leq j, k < r$, are linearly independent over \mathbb{F}_q , we get that Q_{2d} is not the zero polynomial. In particular we have

$$\deg(F) = \deg(Q) = \deg(Q_{2d}) = 2d.$$

We estimate the dimension of the singular locus $\mathcal{L}(Q - c)$. The bound for the dimension of $\mathcal{L}(Q_{2d})$ corresponds to the special case $f(X) = X^d$ and $c = 0$, that is, $Q = Q_{2d}$ in this case.

To estimate $\dim(\mathcal{L}(Q - c))$, consider the partial derivatives

$$\frac{\partial(Q - c)}{\partial Y_\ell}(Y_0, \dots, Y_{r-1}) = f'_\ell(Y_\ell) \sum_{k=0}^{r-1} (a_{k,\ell} + a_{\ell,k}) f_k(Y_k), \quad \ell = 0, \dots, r-1.$$

The condition $2 \leq d < p$ implies that $f'(X) = f'_0(X)$ is not constant and so $f'_\ell(X)$ is not constant for $\ell = 0, \dots, r-1$.

Note that

$$\mathcal{L}(Q - c) = \bigcup_{L \subseteq \{0, \dots, r-1\}} (V_L \cap C_L),$$

where V_L is the (affine) variety in $\overline{\mathbb{F}_p}^r$ of solutions of the system of equations

$$\begin{aligned} Q(Y_0, \dots, Y_{r-1}) &= c, \\ \sum_{k=0}^{r-1} (a_{k,\ell} + a_{\ell,k}) f_k(Y_k) &= 0, \quad \ell \in L, \end{aligned} \tag{6}$$

and C_L the variety of solutions of

$$\begin{aligned} Q(Y_0, \dots, Y_{r-1}) &= c, \\ f'_\ell(Y_\ell) &= 0, \quad \ell \in \{0, 1, \dots, r-1\} \setminus L. \end{aligned}$$

Hence,

$$\dim(\mathcal{L}(Q - c)) \leq \max\{\min\{\dim(V_L), \dim(C_L)\} : L \subseteq \{0, \dots, r-1\}\}, \tag{7}$$

since

$$\dim(U \cup V) = \max\{\dim(U), \dim(V)\}$$

and

$$\dim(U \cap V) \leq \min\{\dim(U), \dim(V)\},$$

see for example [3, Propositions 9.4.8 and 9.4.1].

It remains to estimate the dimensions of V_L and C_L .

Lemma 3. For $L \subseteq \{0, 1, \dots, r-1\}$ the (affine) variety V_L is of dimension at most

$$\begin{cases} r - |L| - 1, & r \text{ even and } c \neq 0, \\ r - |L|, & r \text{ even and } c = 0 \text{ or } r \text{ odd and } c \neq 0, \\ r - |L| + 1, & r \text{ odd and } c = 0. \end{cases}$$

Proof. For any $L \subset \{0, \dots, r-1\}$ we consider the variety W_L obtained by replacing $Z_j = f(Y_j)$ for $j = 0, \dots, r-1$ in the defining equations (6) of V_L . The variety W_L is the set of solutions $(\zeta_0, \dots, \zeta_{r-1}) \in \overline{\mathbb{F}_p}^r$ of the system

$$\begin{aligned} \sum_{j,k=0}^{r-1} a_{j,k} Z_j Z_k &= c \\ \sum_{k=0}^{r-1} (a_{k,\ell} + a_{\ell,k}) Z_k &= 0, \quad \ell \in L. \end{aligned} \tag{8}$$

First we show

$$\dim(V_L) \leq \dim(W_L). \tag{9}$$

Put $s = \dim(W_L)$. Since otherwise (9) is trivial we may assume $s < r$. By [3, Corollary 9.5.4] for all $\{i_1, \dots, i_{s+1}\} \subseteq \{0, \dots, r-1\}$, there exists a nonzero polynomial P in $s+1$ variables with coefficients in $\overline{\mathbb{F}_p}$ such that

$$P(\zeta_{i_1}, \dots, \zeta_{i_{s+1}}) = 0 \quad \text{for all } (\zeta_0, \dots, \zeta_{r-1}) \in W_L$$

and thus

$$P(f_{i_1}(\eta_{i_1}), \dots, f_{i_{s+1}}(\eta_{i_{s+1}})) = 0 \quad \text{for all } (\eta_0, \dots, \eta_{r-1}) \in V_L.$$

Since the polynomial $F(Y_{i_1}, \dots, Y_{i_{s+1}}) = P(f_{i_1}(Y_{i_1}), \dots, f_{i_{s+1}}(Y_{i_{s+1}}))$ is obviously not the zero polynomial we deduce $\dim(V_L) \leq s$ by [3, Corollary 9.5.4]. It remains to show

$$\dim(W_L) \leq \begin{cases} r - |L| - 1, & r \text{ even and } c \neq 0, \\ r - |L|, & r \text{ even and } c = 0 \text{ or } r \text{ odd and } c \neq 0, \\ r - |L| + 1, & r \text{ odd and } c = 0. \end{cases}$$

Let \widetilde{W}_L be the $\overline{\mathbb{F}_p}$ -linear space of solutions of the system of linear equations

$$\sum_{k=0}^{r-1} (a_{k,\ell} + a_{\ell,k}) Z_k = 0, \quad \ell \in L.$$

First we compute $\dim(\widetilde{W}_{\{0,1,\dots,r-1\}})$, that is, we determine $(\zeta_0, \dots, \zeta_{r-1}) \in \overline{\mathbb{F}_p}^r$ satisfying

$$\sum_{k=0}^{r-1} (a_{\ell,k} + a_{k,\ell}) \zeta_k = 0, \quad \ell = 0, \dots, r-1,$$

and thus

$$\sum_{k=0}^{r-1} \sum_{\ell=0}^{r-1} \beta_m^{p^\ell} (a_{\ell,k} + a_{k,\ell}) \zeta_k = 0, \quad m = 1, \dots, r.$$

Since

$$\begin{aligned} \sum_{\ell=0}^{r-1} \beta_m^{p^\ell} (a_{\ell,k} + a_{k,\ell}) &= \sum_{i=1}^{r-1} \left(\delta_{i+1}^{p^k} \text{Tr}(\beta_m \delta_i) + \delta_i^{p^k} \text{Tr}(\beta_m \delta_{i+1}) \right) \\ &= \begin{cases} \delta_2^{p^k}, & m = 1, \\ \delta_{m-1}^{p^k} + \delta_{m+1}^{p^k}, & m = 2, \dots, r-1, \\ \delta_{r-1}^{p^k}, & m = r, \end{cases} \end{aligned}$$

for $k = 0, \dots, r-1$, we get

$$\begin{aligned} \sum_{k=0}^{r-1} \delta_2^{p^k} \zeta_k &= 0, \\ \sum_{k=0}^{r-1} \left(\delta_{m-1}^{p^k} + \delta_{m+1}^{p^k} \right) \zeta_k &= 0, \quad m = 2, \dots, r-1, \\ \sum_{k=0}^{r-1} \delta_{r-1}^{p^k} \zeta_k &= 0. \end{aligned} \tag{10}$$

For even r this implies

$$\sum_{k=0}^{r-1} \delta_m^{p^k} \zeta_k = 0, \quad m = 1, \dots, r,$$

and since the transformation (4) is regular we get $\zeta_k = 0$ for all k and thus $\dim(\widetilde{W}_{\{0, \dots, r-1\}}) = 0$.

For odd r , (10) implies

$$\sum_{k=0}^{r-1} \delta_m^{p^k} \zeta_k = \begin{cases} 0, & m \text{ even}, \\ (-1)^{(m-1)/2} \lambda, & m \text{ odd}, \end{cases} \quad m = 1, \dots, r,$$

where $\sum_{k=0}^{r-1} \delta_1^{p^k} \zeta_k = \lambda$ for some $\lambda \in \overline{\mathbb{F}_p}$. We get $\dim(\widetilde{W}_{\{0, \dots, r-1\}}) = 1$.

Now for any proper subset L of $\{0, \dots, r-1\}$ the variety is defined by deleting $j = r - |L|$ equations from the definition of $\widetilde{W}_{\{0, \dots, r-1\}}$. That is, its dimension is increased by at most $r - |L|$. The vector space \widetilde{W}_L is of dimension t with $t \leq r - |L|$ for even r and $t \leq \min\{r, r - |L| + 1\}$ for odd r .

Let (u_1, \dots, u_t) be basis of \widetilde{W}_L so that each $z = (\zeta_0, \dots, \zeta_{r-1}) \in \widetilde{W}_L$ is of the form $z = \sum_{i=1}^t \lambda_i u_i$ with $\lambda_1, \dots, \lambda_t \in \overline{\mathbb{F}_p}$. If we write each $u_i = (\mu_{0,i}, \dots, \mu_{r-1,i})$ for $i = 1, \dots, t$, then the coordinates of z satisfy

$$\zeta_k = \lambda_1 \mu_{k,1} + \dots + \lambda_t \mu_{k,t} \quad \text{for } 0 \leq k \leq r-1.$$

After the linear variable substitution

$$Z_k = \sum_{i=1}^t \mu_{ki} L_i$$

the first equation of (8) becomes

$$\sum_{j,k=0}^{r-1} a_{j,k} \left(\sum_{i=1}^t \mu_{j,i} L_i \right) \left(\sum_{i=1}^t \mu_{k,i} L_i \right) = c.$$

The left hand side is a quadratic form in L_1, \dots, L_t . If this form is identically zero, then $W_L = \emptyset$ if $c \neq 0$ and $W_L = \widetilde{W}_L$ if $c = 0$. If the form is not identically zero, then the variables L_1, \dots, L_t are algebraically dependent and we get $\dim(W_L) \leq \dim(\widetilde{W}_L) - 1$ by [3, Corollary 9.5.4]. \square

It is easy to see that

$$\dim(C_L) \leq |L| \quad (11)$$

by removing the equation $Q(Y_0, \dots, Y_{r-1}) = 0$ and having the same argument as in the proof of Lemma 3, this time substituting $Z_j = f'_j(Y_j)$ for $j = 0, \dots, r-1$ and applying [3, Corollary 9.5.4].

Combining (7), Lemma 3 and (11) we get

$$\dim(\mathcal{L}(Q - c)) \leq \begin{cases} r/2 - 1, & r \text{ even and } c \neq 0, \\ (r-1)/2, & r \text{ odd and } c \neq 0, \\ r/2, & r \text{ even and } c = 0, \\ (r+1)/2, & r \text{ odd and } c = 0. \end{cases}$$

6 Final remarks

Some cases with singular locus $\mathcal{L}(Q_{2d})$ of positive dimension

Unfortunately, we cannot apply the Deligne bound to obtain a better result if the singular locus $\mathcal{L}(Q_{2d})$ has positive dimension.

It is clear from the proof of Lemma 3 that for odd r the singular locus of Q_{2d} is of dimension at least 1. For some special choices of the dual basis, $\mathcal{L}(Q_{2d})$ has also positive dimension for any $r \geq 4$.

Namely, if

$$\sum_{i=1}^{r-1} \delta_i \delta_{i+1} = 0, \quad (12)$$

the coefficients $a_{j,j}$, $j = 0, \dots, r-1$, defined by (3) vanish. Then each $(\eta_0, \dots, \eta_{r-1}) \in \overline{\mathbb{F}_p}^r$ with only one non-zero coordinate is a singular point of Q_{2d} .

Now we construct such a dual basis. Let α be a defining element of \mathbb{F}_q over \mathbb{F}_p , that is, $\mathbb{F}_q = \mathbb{F}_p(\alpha)$. Then, for sufficiently large p with respect to r ,

$(\delta_1, \dots, \delta_r)$ defined by

$$\begin{aligned}\delta_{2i+1} &= \alpha^{r-1-i}, \quad i = 0, 1, \dots, \lfloor r/2 \rfloor - 1, \\ \delta_{2i+2} &= \alpha^i, \quad i = 0, 1, \dots, \lfloor (r-1)/2 \rfloor - 1, \\ \delta_r &= - \begin{cases} (r/2 - 1)(\alpha^{r/2-1} + \alpha^{r/2-2}), & r \text{ even}, \\ \frac{r-1}{2}\alpha^{(r+1)/2} + \frac{r-3}{2}\alpha^{(r-1)/2}, & r \text{ odd}, \end{cases} \quad r \geq 4,\end{aligned}$$

is a basis of \mathbb{F}_q over \mathbb{F}_p , since $\alpha^{\lfloor (r-1)/2 \rfloor}$ appears only in δ_r , satisfying (12).

The Thue-Morse function of \mathbb{F}_q for monomials

The *Thue-Morse function* T for \mathbb{F}_q with respect to the basis \mathcal{B} is

$$T(\xi) = \sum_{i=1}^r x_i, \quad \xi = x_1\beta_1 + \dots + x_r\beta_r \in \mathbb{F}_q,$$

where $x_1, \dots, x_r \in \mathbb{F}_p$. For $f(X) \in \mathbb{F}_q[X]$ of degree $d \geq 1$ and $c \in \mathbb{F}_p$ we put

$$\mathcal{T}(c, f) = \{\xi \in \mathbb{F}_q : T(f(\xi)) = c\}.$$

The first author and Sárközy [5, Theorem 1.2] proved

$$|\mathcal{T}(c, f)| - p^{r-1} \leq (d-1)p^{r/2}, \quad \gcd(d, p) = 1.$$

For monomials $f(X) = X^d$, $c \neq 0$, fixed $d \geq 2$ and fixed r , the Hooley-Katz Theorem provides the improvement

$$|\mathcal{T}(c, X^d)| - p^{r-1} \leq C_{d,r}p^{(r-1)/2}, \quad c \neq 0.$$

In particular, we get

$$\lim_{p \rightarrow \infty} \frac{|\mathcal{T}(c, X^d)|}{p^{r-1}} = 1, \quad c \neq 0,$$

also for $r = 2$.

The crucial step is to show that the singular locus of

$$Q(Y_0, \dots, Y_{r-1}) = \sum_{\ell=0}^{r-1} \delta^{p^\ell} Y_\ell^d - c$$

is of dimension -1 , where we used the same notation as before and

$$\delta = \sum_{i=1}^r \delta_i \neq 0,$$

since $\delta_1, \dots, \delta_r$ are linearly independent. Now the partial derivatives are

$$\frac{\partial Q}{\partial Y_\ell} = \delta^{p^\ell} d Y_\ell^{d-1}, \quad \ell = 0, \dots, r-1.$$

We may assume $d < p$. Then the only common zero of all partial derivatives is $(0, \dots, 0)$. However, $(0, \dots, 0)$ is not a zero of Q for $c \neq 0$.

The Hooley-Katz Theorem can also be applied for general $f(X) \in \mathbb{F}_q[X]$ of degree $d \geq 2$ but would give an improvement of [5, Theorem 1.2] only for $c \in \mathbb{F}_p \setminus \mathcal{C}$ where \mathcal{C} is a subset of \mathbb{F}_p with at most $(d-1)^r$ elements, where d and r are fixed and p is sufficiently large. The polynomial Q for a general f becomes

$$Q(Y_0, \dots, Y_{r-1}) = \sum_{\ell=0}^{r-1} \delta^{p^\ell} f_\ell(Y_\ell) - c,$$

with $f_\ell = \varphi^\ell(f)$ as in Section 4.

A singular point $(\eta_0, \dots, \eta_{r-1}) \in \overline{\mathbb{F}_p}^r$ satisfies

$$f'_\ell(\eta_\ell) = 0 \quad \text{for } \ell = 0, \dots, r-1. \quad (13)$$

This singular point has to be also a zero of Q , that is,

$$c = \sum_{i=0}^{r-1} \delta^{p^i} f_i(\eta_i).$$

For all other $c \in \mathbb{F}_p$ there are no singular points. Since (13) has at most $(d-1)^r$ solutions in $\overline{\mathbb{F}_p}^r$ we have $|\mathcal{C}| \leq (d-1)^r$.

Acknowledgments

The second and third author are partially supported by the Austrian Science Fund FWF, Projects P 31762 and P 30405, respectively.

The authors wish to thank Igor Shparlinski for pointing to Deligne's bound for projective surfaces and related theorems.

We wish to thank the anonymous referees for very useful comments.

References

- [1] Jean Bourgain. Prescribing the binary digits of primes. *Israel J. Math.*, 194(2):935–955, 2013.
- [2] Jean Bourgain. Prescribing the binary digits of primes, II. *Israel J. Math.*, 206(1):165–182, 2013.
- [3] David A. Cox, John Little, and Donal O'Shea. *Ideals, varieties, and algorithms*. Undergraduate Texts in Mathematics. Springer, Cham, fourth edition, 2015. An introduction to computational algebraic geometry and commutative algebra.
- [4] Cécile Dartyge, Christian Mauduit, and András Sárközy. Polynomial values and generators with missing digits in finite fields. *Funct. Approx. Comment. Math.*, 52(1):65–74, 2015.

- [5] Cécile Dartyge and András Sárközy. The sum of digits functions in finite fields. *Proc. Amer. Math. Soc.*, 141(12):4119–4124, 2013.
- [6] Pierre Deligne. La conjecture de Weil. I. *Inst. Hautes Études Sci. Publ. Math.*, 43:273–307, 1974.
- [7] Rainer Dietmann, Christian Elsholtz, and Igor E. Shparlinski. Prescribing the binary digits of squarefree numbers and quadratic residues. *Trans. Amer. Math. Soc.*, 369(12):8369–8388, 2017.
- [8] Michael Drmota, Christian Mauduit, and Joël Rivat. Normality along squares. *J. Eur. Math. Soc. (JEMS)*, 21(2):507–548, 2019.
- [9] Mikhail R. Gabdullin. On the squares in the set of elements of a finite field with constraints on the coefficients of its basis expansion. *Mat. Zametki*, 100(6):807–824, 2016.
- [10] Christopher Hooley. On the number of points on a complete intersection over a finite field. *J. Number Theory*, 38(3):338–358, 1991. With an appendix by Nicholas M. Katz.
- [11] Rudolf Lidl and Harald Niederreiter. *Finite fields*, volume 20 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, second edition, 1997.
- [12] Sam Mattheus. Trace of products in finite fields from a combinatorial point of view. *SIAM J. Discrete Math.*, 33(4):2126–2139, 2019.
- [13] Christian Mauduit and Joël Rivat. La somme des chiffres des carrés. *Acta Math.*, 203(1):107–148, 2010.
- [14] Christian Mauduit and Joël Rivat. Sur un problème de Gelfond : la somme des chiffres des nombres premiers. *Ann. of Math. (2)*, 171(3):1591–1646, 2010.
- [15] James Maynard. Primes with restricted digits. *Invent. Math.*, 217(1):127–218, 2019.
- [16] Gary L. Mullen and Daniel Panario, editors. *Handbook of finite fields*. Discrete Mathematics and its Applications (Boca Raton). CRC Press, Boca Raton, FL, 2013.
- [17] Clemens Müllner. The Rudin-Shapiro sequence and similar sequences are normal along squares. *Canad. J. Math.*, 70(5):1096–1129, 2018.
- [18] Sam Porritt. Irreducible polynomials over a finite field with restricted coefficients. *Canad. Math. Bull.*, 62(2):429–439, 2019.
- [19] Zhimin Sun and Arne Winterhof. On the maximum order complexity of subsequences of the Thue-Morse and Rudin-Shapiro sequence along squares. *Int. J. Comput. Math. Comput. Syst. Theory*, 4(1):30–36, 2019.

- [20] Cathy Swaenepoel. On the sum of digits of special sequences in finite fields. *Monatsh. Math.*, 187(4):705–728, 2018.
- [21] Cathy Swaenepoel. Prescribing digits in finite fields. *J. Number Theory*, 189:97–114, 2018.
- [22] Cathy Swaenepoel. Trace of products in finite fields. *Finite Fields Appl.*, 51:93–129, 2018.
- [23] Cathy Swaenepoel. Prime numbers with a positive proportion of preassigned digits. *Proc. Lond. Math. Soc. (3)*, 121(1):83–151, 2020.