M. Makhul , A. Winterhof *Res. Number Theory* (2022) 8:38
https://doi.org/10.1007/s40993-022-00335-8

Research in Number Theory

RESEARCH

Normality of the Thue–Morse function for finite fields along polynomial values

Mehdi Makhul[1*†] and Arne Winterhof[2†]

*Correspondence:
mehdi.makhul@ricam.oeaw.ac.at
†Mehdi Makhul and Arne Winterhof have contributed equally to this work.
[1]Research Institute for Symbolic Computation, Altenberger Str. 69, 4040 Linz, Austria
Full list of author information is available at the end of the article

Abstract

Let $\boldsymbol{F}_q$ be the finite field of q elements, where $q = p^r$ is a power of the prime p, and $(\beta_1, \beta_2, \ldots, \beta_r)$ be an ordered basis of $\boldsymbol{F}_q$ over $\boldsymbol{F}_p$. For

$$\xi = \sum_{i=1}^{r} x_i\beta_i, \quad x_i \in \boldsymbol{F}_p,$$

we define the Thue–Morse or sum-of-digits function $T(\xi)$ on $\boldsymbol{F}_q$ by

$$T(\xi) = \sum_{i=1}^{r} x_i.$$

For a given pattern length s with $1 \le s \le q$, a vector $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_s) \in \boldsymbol{F}_q^s$ with different coordinates $\alpha_{j_1} \ne \alpha_{j_2}$, $1 \le j_1 < j_2 \le s$, a polynomial $f(X) \in \boldsymbol{F}_q[X]$ of degree d and a vector $\mathbf{c} = (c_1, \ldots, c_s) \in \boldsymbol{F}_p^s$ we put

$$\mathcal{T}(\mathbf{c}, \boldsymbol{\alpha}, f) = \{\xi \in \boldsymbol{F}_q : T(f(\xi + \alpha_i)) = c_i,\ i = 1, \ldots, s\}.$$

In this paper we will see that under some natural conditions, the size of $\mathcal{T}(\mathbf{c}, \boldsymbol{\alpha}, f)$ is asymptotically the same for all $\mathbf{c}$ and $\boldsymbol{\alpha}$ in both cases, $p \to \infty$ and $r \to \infty$, respectively. More precisely, we have

$$\left||\mathcal{T}(\mathbf{c}, \boldsymbol{\alpha}, f)| - p^{r-s}\right| \le (d-1)q^{1/2}$$

under certain conditions on d, q and s. For monomials of large degree we improve this bound as well as we find conditions on d, q and s for which this bound is not true. In particular, if $1 \le d < p$ we have the dichotomy that the bound is valid if $s \le d$ and for $s \ge d+1$ there are vectors $\mathbf{c}$ and $\boldsymbol{\alpha}$ with $\mathcal{T}(\mathbf{c}, \boldsymbol{\alpha}, f) = \emptyset$ so that the bound fails for sufficiently large r. The case $s = 1$ was studied before by Dartyge and Sárközy.

Keywords: Finite fields, Polynomial equations, Thue–Morse function, Exponential sums, Sum of digits, Normality

Mathematics Subject Classification: 11A63, 11T06, 11T23, 11L99

1 Introduction

1.1 The problem for binary sequences

For positive integers M and s, a binary sequence (a_n) and a binary pattern

$$\mathcal{E}_s = (\varepsilon_0, \ldots, \varepsilon_{s-1}) \in \{0, 1\}^s$$

Springer

of length s we denote by $N(a_n, M, \mathcal{E}_s)$ the number of n with $0 \leq n < M$ and $(a_n, a_{n+1}, \ldots, a_{n+s-1}) = \mathcal{E}_s$. The sequence (a_n) is *normal* if for any fixed s and any pattern $\mathcal{E}_s$ of length s,

$$\lim_{M\to\infty} \frac{N(a_n, M, \mathcal{E}_s)}{M} = \frac{1}{2^s}.$$

The *Thue–Morse* or *sum-of-digits sequence* (t_n) is defined by

$$t_n = \sum_{i=0}^{\infty} n_i \bmod 2, \quad n = 0, 1, \ldots$$

if

$$n = \sum_{i=0}^{\infty} n_i 2^i, \quad n_0, n_1, \ldots \in \{0, 1\},$$

is the binary expansion of n. Recently, Drmota et al. [1] showed that the Thue–Morse sequence along squares, that is, (t_{n^2}) is normal. It is conjectured but not proved yet that the subsequence of the Thue–Morse sequence along any polynomial of degree $d \geq 3$ is normal as well, see [1, Conjecture 1]. Even the weaker problem of determining the frequency of 0 and 1 in the subsequence of the Thue–Morse sequence along any polynomial of degree $d \geq 3$ seems to be out of reach, see [1, above Conjecture 1].

However, the analog of the latter weaker problem for the Thue–Morse sequence in the finite field setting was settled by Dartyge and Sárközy [2].

1.2 The analog for finite fields

This paper deals with the following analog of the normality problem. Let $q = p^r$ be the power of a prime p and

$$\mathcal{B} = (\beta_1, \ldots, \beta_r)$$

be an ordered basis of the finite field $\boldsymbol{F}_q$ over $\boldsymbol{F}_p$. Then any $\xi \in \boldsymbol{F}_q$ has a unique representation

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

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

Dartyge and Sárközy [2] introduced the *Thue–Morse* or *sum-of-digits function* $T(\xi)$ for the finite field $\boldsymbol{F}_q$ with respect to the basis $\mathcal{B}$:

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

Note that T is a linear map from $\boldsymbol{F}_q$ to $\boldsymbol{F}_p$. Actually, we can take any non-trivial linear map

$$T(\xi) = \mathrm{Tr}(\delta\xi), \quad \delta \in \boldsymbol{F}_q^*,$$

from $\boldsymbol{F}_q$ to $\boldsymbol{F}_p$ without changing our results or proofs below, where the trace Tr is defined by (7).

For a given pattern length s with $1 \leq s \leq q$, a vector

$$\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_s) \in \boldsymbol{F}_q^s, \quad \alpha_{j_1} \neq \alpha_{j_2}, \quad 1 \leq j_1 < j_2 \leq s,$$

with different coordinates, a polynomial $f(X) \in \boldsymbol{F}_q[X]$ and a vector $\mathbf{c} = (c_1, \ldots, c_s) \in \boldsymbol{F}_p^s$ we put

$$\mathcal{T}(\mathbf{c}, \boldsymbol{\alpha}, f) = \{\xi \in \boldsymbol{F}_q : T(f(\xi + \alpha_i)) = c_i,\ i = 1, \ldots, s\}.$$

In [2] the Weil bound, see Lemma 1, was used to bound the cardinality of $\mathcal{T}(\mathbf{c}, \boldsymbol{\alpha}, f)$ for $s = 1$:

Let $f(X) \in \boldsymbol{F}_q[X]$ be a polynomial of degree d. Then for all $c \in \boldsymbol{F}_p$

$$\left||\mathcal{T}(c, f)| - p^{r-1}\right| \le (d-1)q^{1/2}, \quad \gcd(d, p) = 1, \tag{1}$$

where

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

Note that the condition $\gcd(d, p) = 1$ can be relaxed to the condition that $f(X)$ is not of the form $g(X)^p - g(X) + c$ for some $g(X) \in \boldsymbol{F}_q[X]$ and $c \in \boldsymbol{F}_q$. For example, $f(X) = X^p$ is not of the form $g(X)^p - g(X) + c$ but does not satisfy $\gcd(d, p) = 1$.

Our goal is to prove that, under some natural conditions, the size of $\mathcal{T}(\mathbf{c}, \boldsymbol{\alpha}, f)$ is asymptotically the same for all $\mathbf{c}$ and $\boldsymbol{\alpha}$.

1.3 Results of this paper

First we study monomials and prove the following result in Sect. 4.

Theorem 1 *Let d be any integer with $1 \le d < q$ with unique representation*

$$d = (d_0 + d_1 p + \cdots + d_{n-1}p^{n-1}) \gcd(d, q)$$

where

$$1 \le n \le r - \frac{\log(\gcd(d, q))}{\log p}, \quad 0 \le d_i < p, \quad i = 0, \ldots, n-1, \quad d_0 d_{n-1} \ne 0.$$

Let denote by

$$f_d(X) = X^d \in \boldsymbol{F}_q[X]$$

the monomial of degree d.

1. *For $n \ge 2$, assume*

$$d_m = d_{m+1} = \cdots = d_{m+k-1} = p - 1$$

for some m and k with

$$1 \le m \le m + k \le n - 1.$$

For any positive integer

$$s \le \begin{cases} (d_{m+k} + 1)(p^k - p^{k-1}), & n \ge 2 \text{ and } k \ge 1, \\ d_0, & n = 1 \text{ or } k = 0, \end{cases} \tag{2}$$

any vector $\boldsymbol{\alpha} \in \boldsymbol{F}_q^s$ with $\alpha_{j_1} \ne \alpha_{j_2}$ for $1 \le j_1 < j_2 \le s$, and any $\mathbf{c} \in \boldsymbol{F}_p^s$ we have

$$\left||\mathcal{T}(\mathbf{c}, \boldsymbol{\alpha}, f_d)| - p^{r-s}\right| \le \left(\frac{d}{\gcd(d, q)} - 1\right) q^{1/2}.$$

2. *Conversely, if*

$$(d_0 + 1)(d_1 + 1) \cdots (d_{n-1} + 1) \le p, \tag{3}$$

for any integer s with

$$q \geq s \geq (d_0+1)(d_1+1)\cdots(d_{n-1}+1), \tag{4}$$

there is a vector $\boldsymbol{\alpha} \in \boldsymbol{F}_q^s$ *with* $\alpha_{j_1} \neq \alpha_{j_2}$, $1 \leq j_1 < j_2 \leq s$, *and a vector* $\boldsymbol{c} \in \boldsymbol{F}_p^s$ *for which* $\mathcal{T}(\boldsymbol{c}, \boldsymbol{\alpha}, f_d)$ *is empty.*

3. *For any s with*

$$q \geq s > ((d_0+1)(d_1+1)\cdots(d_{n-1}+1)-1)r \tag{5}$$

and any vector $\boldsymbol{\alpha} \in \boldsymbol{F}_q^s$ *there is a vector* $\boldsymbol{c} \in \boldsymbol{F}_p^s$ *for which* $\mathcal{T}(\boldsymbol{c}, \boldsymbol{\alpha}, f_d)$ *is empty.*

For $d < p$ we have the following dichotomy:

Corollary 1 *Assume* $1 \leq d < p$.

For $s \leq d$ *we have for any vector* $\boldsymbol{\alpha} \in \boldsymbol{F}_q^s$ *with* $\alpha_{j_1} \neq \alpha_{j_2}$, $1 \leq j_1 < j_2 \leq s$, *and any* $\boldsymbol{c} \in \boldsymbol{F}_p^s$

$$\left||\mathcal{T}(\boldsymbol{c}, \boldsymbol{\alpha}, f_d)| - p^{r-s}\right| \leq (d-1)q^{1/2}.$$

For s with $q \geq s > d$ *there is a vector* $\boldsymbol{\alpha} \in \boldsymbol{F}_q^s$ *with* $\alpha_{j_1} \neq \alpha_{j_1}$, $1 \leq j_1 < j_2 \leq s$, *and a vector* $\boldsymbol{c} \in \boldsymbol{F}_p^s$ *for which* $\mathcal{T}(\boldsymbol{c}, \boldsymbol{\alpha}, f_d)$ *is empty.*

Theorem 1 provides two asymptotic formulas for $|\mathcal{T}(\mathbf{c}, \boldsymbol{\alpha}, X^d)|$ for $r \to \infty$ and $p \to \infty$, respectively.

Assume that $p, j, n, d = (d_0 + d_1 p + \cdots + d_{n-1}p^{n-1})p^j$ and s satisfying (2) are fixed. Then we have

$$\lim_{r\to\infty} \frac{|\mathcal{T}(\mathbf{c}, \boldsymbol{\alpha}, f_d)|}{p^{r-s}} = 1$$

for any vectors $\mathbf{c} \in \boldsymbol{F}_p^s$ and $\boldsymbol{\alpha} \in \boldsymbol{F}_q^s$ with $\alpha_{j_1} \neq \alpha_{j_2}$, $1 \leq j_1 < j_2 \leq s$. We may say that $T(f_d)$ is *r-normal* if (2) is satisfied.

Assume that $j = 0$ and d, r and s are fixed with $1 \leq s \leq \min\{d, \lfloor (r-1)/2 \rfloor\}$. Then we have

$$\lim_{p\to\infty} \frac{|\mathcal{T}(\mathbf{c}, \boldsymbol{\alpha}, f_d)|}{p^{r-s}} = 1$$

for any $\mathbf{c} \in \boldsymbol{F}_p^s$ and $\boldsymbol{\alpha} \in \boldsymbol{F}_q^s$ with $\alpha_{j_1} \neq \alpha_{j_2}$, $1 \leq j_1 < j_2 \leq s$. We may say that $T(f_d)$ is *p-normal* for $1 \leq s \leq \min\{d, \lfloor (r-1)/2 \rfloor\}$.

Theorem 1 is only non-trivial for small degrees. However, for very large degrees we prove the following non-trivial result in Sect. 5.

Theorem 2 *Let* $f_{q-1-d}(X) = X^{q-1-d}$ *be a monomial of degree* $q-1-d$ *with* $1 \leq d < q-1$. *Then for any* $\boldsymbol{\alpha} \in \boldsymbol{F}_q^s$ *with* $\alpha_{j_1} \neq \alpha_{j_2}$, $1 \leq j_1 < j_2 \leq s$, *and any* $\boldsymbol{c} \in \boldsymbol{F}_p^s$, *we have*

$$|| \mathcal{T}(\boldsymbol{c}, \boldsymbol{\alpha}, f_{q-1-d}) | - p^{r-s} | \leq \left(\left(\frac{d}{\gcd(d,q)} + 1 \right) s - 2 \right) q^{1/2} + s + 1.$$

Note that with the convention $0^{-1} = 0$ we have

$$\xi^{q-1-d} = \xi^{-d} \quad \text{for any } \xi \in \boldsymbol{F}_q$$

and can identify the monomial $f_{q-1-d}(X) = X^{q-1-d}$ with the rational function $f_{-d}(X) = X^{-d}$. However, the latter representation is independent of q and we can state two asymptotic formulas for $|\mathcal{T}(\mathbf{c}, \boldsymbol{\alpha}, f_{-d})|$ as well.

For any fixed d, p and s we have

$$\lim_{r\to\infty} \frac{|\mathcal{T}(\mathbf{c}, \boldsymbol{\alpha}, f_{-d})|}{p^{r-s}} = 1,$$

that is, $T(f_{-d})$ is r-normal.

For any fixed d, s and r with $1 \le s \le \lfloor (r-1)/2 \rfloor$ we have

$$\lim_{p\to\infty} \frac{|\mathcal{T}(\mathbf{c}, \boldsymbol{\alpha}, f_{-d})|}{p^{r-s}} = 1,$$

that is, $T(f_{-d})$ is p-normal for $1 \le s \le \lfloor (r-1)/2 \rfloor$.

Finally, we extend our results to arbitrary polynomials in Sect. 6.

Theorem 3 *Let d be any integer with $1 \le d < q$ and $\gcd(d, q) = 1$. Let $f(X) \in \boldsymbol{F}_q[X]$ be any polynomial of degree d.*

1. *Denote $d_0 \equiv d \bmod p$, $1 \le d_0 < p$. For any integer s with*

$$1 \le s \le d_0,$$

any $\boldsymbol{\alpha} \in \boldsymbol{F}_q^s$ with $\alpha_{j_1} \ne \alpha_{j_2}$, $1 \le j_1 < j_2 \le s$, and any $\boldsymbol{c} \in \boldsymbol{F}_p^s$ we have

$$\big||\mathcal{T}(\boldsymbol{c}, \boldsymbol{\alpha}, f)| - p^{r-s}\big| \le (d-1)q^{1/2}.$$

2. *Conversely, if $f(X) \in \boldsymbol{F}_p[X]$ and $d < p$, then for any integer s with*

$$q \ge s \ge d+1,$$

there is $\boldsymbol{\alpha} \in \boldsymbol{F}_q^s$ with $\alpha_{j_1} \ne \alpha_{j_2}$, $1 \le j_1 < j_2 \le s$, and $\boldsymbol{c} \in \boldsymbol{F}_p^s$ for which $\mathcal{T}(\boldsymbol{c}, \boldsymbol{\alpha}, f)$ is empty.

3. *For any $f(X) \in \boldsymbol{F}_q[X]$, any s with*

$$q \ge s > dr$$

and any $\boldsymbol{\alpha} \in \boldsymbol{F}_q^s$ there is a vector $\boldsymbol{c} \in \boldsymbol{F}_p^s$ for which $\mathcal{T}(\boldsymbol{c}, \boldsymbol{\alpha}, f)$ is empty.

We give examples of degree d with $\gcd(d, p) > 1$ and $\mathcal{T}(\mathbf{c}, \boldsymbol{\alpha}, f) = \emptyset$ for any $s \ge 1$ in Sect. 7.1.

Again, for $f(X) \in \boldsymbol{F}_p[X]$ and $1 \le d < p$ we have a dichotomy.

Moreover, for any fixed d, p and s with $\gcd(d, q) = 1$ and $1 \le s \le d_0$ and any $f(X) \in \boldsymbol{F}_p[X]$ of degree d, $T(f)$ is r-normal. Note that any $f(X) \in \boldsymbol{F}_p[X]$ is an element of $\boldsymbol{F}_{p^r}[X]$ for $r = 1, 2, \ldots$

For fixed d, r and s with $1 \le s \le \min\{d, \lfloor (r-1)/2 \rfloor\}$ and any $f(X) \in \mathbf{Z}[X]$ of degree d, $T(f)$ is p-normal. Here $f(X) \in \mathbf{Z}[X]$ can be identified with an element of $\boldsymbol{F}_p[X]$ for all primes p.

We start with a section on preliminary results used in the proofs. Then we show that

$$\big||\mathcal{T}(\mathbf{c}, \boldsymbol{\alpha}, f)| - p^{r-s}\big| \le (\deg(f) - 1)q^{1/2} \tag{6}$$

under certain conditions in Sect. 3. In Sects. 4 to 6 we show that these conditions are fulfilled under the assumptions of our theorems. We finish the paper with some remarks on related work in Sect. 7.

2 Preliminary results

We start with the Weil bound, see [3, Theorem 5.38 and comments below], [4, Theorem 2E] or [5].

Lemma 1 *Let ψ be the additive canonical character of the finite field $\boldsymbol{F}_q$, and $f(X)$ be a polynomial of degree $d \geq 1$ over $\boldsymbol{F}_q$, which is not of the form $g(X)^p - g(X) + c$ for some polynomial $g(X) \in \boldsymbol{F}_q[X]$ and $c \in \boldsymbol{F}_q$. Then we have*

$$\left| \sum_{\xi \in \boldsymbol{F}_q} \psi\left(f(\xi)\right) \right| \leq (d-1)q^{1/2}.$$

We also use the analog of the Weil bound for rational functions

$$\frac{f(X)}{g(X)} \in \boldsymbol{F}_q(X)$$

of Moreno and Moreno [6, Theorem 2]. We only need the special case that $\deg(f) \leq \deg(g)$.

Lemma 2 *Let ψ be a nontrivial additive character of $\boldsymbol{F}_q$ and let $\frac{f(X)}{g(X)} \in \boldsymbol{F}_q(X)$ be a rational function over $\boldsymbol{F}_q$. Let s be the number of distinct roots of the polynomial $g(X)$ in the algebraic closure $\overline{\boldsymbol{F}_q}$ of $\boldsymbol{F}_q$. Suppose that $\frac{f(X)}{g(X)}$ is not of the form $H(X)^p - H(X)$, where $H(X)$ is a rational function over $\overline{\boldsymbol{F}_q}$. If $\deg(f) \leq \deg(g)$, then we have*

$$\left| \sum_{\xi \in \boldsymbol{F}_q, g(\xi) \neq 0} \psi\left(\frac{f(\xi)}{g(\xi)}\right) \right| \leq (\deg(g) + s - 2)\sqrt{q} + 1.$$

Note that $g(X)^p - g(X) + c$ with $g(X) \in \boldsymbol{F}_q(X)$ and $c \in \boldsymbol{F}_q$ can be written as $h(X)^p - h(X)$ for $h(X) = g(X) + \gamma \in \overline{\boldsymbol{F}_q}(X)$, where $\gamma \in \overline{\boldsymbol{F}_q}$ is a zero of the polynomial $X^p - X - c$.

Next we state Lucas' congruence, see [7] or [8, Lemma 6.3.10].

Lemma 3 *Let p be a prime. If m and n are two natural numbers with p-adic expansions*

$$m = m_{r-1}p^{r-1} + m_{r-2}p^{r-2} + \cdots + m_1 p + m_0, \quad 0 \leq m_0, \ldots, m_{r-1} < p,$$

and

$$n = n_{r-1}p^{r-1} + n_{r-2}p^{r-2} + \cdots + n_1 p + n_0, \quad 0 \leq n_0, \ldots, n_{r-1} < p,$$

then we have

$$\binom{m}{n} \equiv \prod_{j=0}^{r-1} \binom{m_j}{n_j} \mod p.$$

As a consequence of Lucas' congruence we can count the number of nonzero binomials coefficients $\binom{m}{n}$ mod p for fixed m. Indeed, by Lucas' congruence

$$\binom{m}{n} \not\equiv 0 \mod p \text{ if and only if } \binom{m_j}{n_j} \not\equiv 0 \mod p \text{ for } j = 0, \ldots, r-1,$$

or equivalently,

$$0 \leq n_j \leq m_j \quad \text{for } j = 0, \ldots, r-1.$$

Therefore, we have the following result of Fine [9, Theorem 2]:

Lemma 4 *Let p be a prime and m an integer with p-adic expansion*

$$m = m_{r-1}p^{r-1} + m_{r-2}p^{r-2} + \cdots + m_1 p + m_0, \quad 0 \leq m_0, \ldots, m_{r-1} < p.$$

Then the number of nonzero binomial coefficients $\binom{m}{n}$ mod p *with* $0 \le n \le m$ *is*

$$\prod_{j=0}^{r-1}(m_j+1).$$

3 Trace, dual basis and exponential sums

Let

$$\mathrm{Tr}(\xi) = \sum_{i=0}^{r-1} \xi^{p^i} \in \boldsymbol{F}_p \tag{7}$$

denote the (absolute) *trace* of $\xi \in \boldsymbol{F}_q$. Let $(\delta_1, \ldots, \delta_r)$ denote the (existent and unique) *dual basis* of the basis $\mathcal{B} = (\beta_1, \ldots, \beta_r)$ of $\boldsymbol{F}_q$, see for example [3], that is,

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

Then we have

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

and

$$T(\xi) = \mathrm{Tr}(\delta\xi), \quad \text{where } \delta = \sum_{i=1}^{r} \delta_i.$$

Note that

$$\delta \neq 0$$

since $\delta_1, \ldots, \delta_r$ are linearly independent. Note that we don't have to restrict ourselves to this special choice of δ and T but can deal with any non-trivial linear map

$$T(\xi) = \mathrm{Tr}(\delta\xi), \quad \delta \in \boldsymbol{F}_q^*,$$

from $\boldsymbol{F}_q$ to $\boldsymbol{F}_p$.

Put

$$e_p(x) = \exp\left(\frac{2\pi i x}{p}\right) \quad \text{for } x \in \boldsymbol{F}_p.$$

Since

$$\sum_{a \in \boldsymbol{F}_p} e_p(ax) = \begin{cases} 0, & x \neq 0, \\ p, & x = 0, \end{cases} \quad x \in \boldsymbol{F}_p,$$

we get

$$\begin{aligned} |\mathcal{T}(\mathbf{c}, \boldsymbol{\alpha}, f)| &= \frac{1}{p^s} \sum_{\xi \in \boldsymbol{F}_q} \prod_{i=1}^{s} \sum_{a \in \boldsymbol{F}_p} e_p\left(a(T(f(\xi+\alpha_i)) - c_i)\right) \\ &= \frac{1}{p^s} \sum_{a_1,\ldots,a_s \in \boldsymbol{F}_p} \sum_{\xi \in \boldsymbol{F}_q} e_p\left(\sum_{i=1}^{s} a_i(T(f(\xi+\alpha_i)) - c_i)\right). \end{aligned}$$

Separating the term for $a_1 = \cdots = a_s = 0$ we get

$$\left| |\mathcal{T}(\mathbf{c}, \boldsymbol{\alpha}, f)| - p^{r-s} \right| \le \max_{(a_1,\ldots,a_s) \neq (0,\ldots,0)} \left| \sum_{\xi \in \boldsymbol{F}_q} \psi(F_{a_1,\ldots,a_s}(\xi)) \right|, \tag{8}$$

where

$$\psi(\xi) = e_p(\mathrm{Tr}(\xi))$$

denotes the *additive canonical character* of $\boldsymbol{F}_q$ and

$$F_{a_1,\ldots,a_s}(X) = \delta \sum_{i=1}^{s} a_i f(X+\alpha_i). \tag{9}$$

If $F_{a_1,\ldots,a_s}(X)$ is not of the form $g(X)^p - g(X) + c$ for any $(a_1,\ldots,a_s) \neq (0,\ldots,0)$, then the Weil bound, Lemma 1, can be applied and yields (6).

4 Monomials $f_d(X) = X^d$

Now we study the special case

$$f(X) = f_{dp^j}(X) = X^{dp^j} \quad \text{with} \quad \gcd(d,p) = 1 \text{ and } j = 0, 1, \ldots$$

Put $\boldsymbol{\alpha}^k = (\alpha_1^k, \ldots, \alpha_s^k)$. Since $(X+\alpha)^{dp^j} = (X^{p^j} + \alpha^{p^j})^d$ and $\xi \mapsto \xi^{p^j}$ permutes $\boldsymbol{F}_q$ we have

$$\left|\mathcal{T}(\mathbf{c}, \boldsymbol{\alpha}, f_{dp^j})\right| = \left|\mathcal{T}(\mathbf{c}, \boldsymbol{\alpha}^{p^j}, f_d)\right|$$

and we may assume $j = 0$. Since

$$\xi^q = \xi \quad \text{for all } \xi \in \boldsymbol{F}_q$$

we may restrict ourselves to the case $d < q$.

To prove the first part of Theorem 1 we have to show that (6) is applicable. By (9) with

$$f(X) = f_d(X) = X^d$$

we have

$$F_{a_1,\ldots,a_s}(X) = \delta \sum_{i=1}^{s} a_i (X+\alpha_i)^d$$

and thus

$$F'_{a_1,\ldots,a_s}(X) = \delta d \sum_{\ell=0}^{d-1} \binom{d-1}{\ell} \left(\sum_{i=1}^{s} a_i \alpha_i^\ell \right) X^{d-\ell-1}. \tag{10}$$

Assume that for some $(a_1,\ldots,a_s) \in \boldsymbol{F}_p^s \setminus \{(0,\ldots,0)\}$ we have

$$F_{a_1,\ldots,a_s}(X) = g(X)^p - g(X) + c$$

for some polynomial $g(X) \in \boldsymbol{F}_q[X]$ and some constant $c \in \boldsymbol{F}_q$. We have

$$\text{either } F_{a_1,\ldots,a_s}(X) = const \quad \text{or} \quad 1 \le \deg(F_{a_1,\ldots,a_s}) \equiv 0 \bmod p \tag{11}$$

and

$$F'_{a_1,\ldots,a_s}(X) = -g'(X).$$

Then either

$$F'_{a_1,\ldots,a_s}(X) = 0, \tag{12}$$

$$\deg(F'_{a_1,\ldots,a_s}) < \deg(g) = \frac{\deg(F_{a_1,\ldots,a_s})}{p}. \tag{13}$$

Let

$$d = d_0 + d_1 p + \cdots + d_{r-1} p^{r-1}, \quad 0 \le d_0, \ldots, d_{r-1} < p, \quad d_0 \neq 0,$$

be the p-adic expansion of d. Assume that there are $k \geq 0$ consecutive digits

$$d_m = d_{m+1} = \cdots = d_{m+k-1} = p - 1, \quad 1 \leq m \leq m + k \leq r - 1,$$

of maximal size and

$$s \leq \begin{cases} (d_{m+k} + 1)(p^k - p^{k-1}), & k \geq 1, \\ d_0, & k = 0. \end{cases}$$

Note that $\deg(F_{a_1,\dots,a_s}) \leq d - d_0$ by (11) with the convention $\deg(0) = -1$. In both cases, (12) and (13), the coefficients of $F'_{a_1,\dots,a_s}(X)$ at $X^{d-1-\ell}$ are zero for $\ell = 0, \dots, d - (d - d_0)/p - 1$. Since $\delta d \neq 0$ we get from (10)

$$\binom{d-1}{\ell} \left(\sum_{i=1}^{s} a_i \alpha_i^{\ell} \right) = 0, \quad \ell = 0, \dots, d - (d - d_0)/p - 1. \tag{14}$$

By Lucas' congruence, Lemma 3, we have

$$\binom{d-1}{\ell} \equiv \binom{d_0 - 1}{\ell} \not\equiv 0 \bmod p, \quad \ell = 0, \dots, d_0 - 1, \tag{15}$$

as well as

$$\binom{d-1}{p^m \ell} \not\equiv 0 \bmod p, \quad \ell = 0, \dots, (d_{m+k} + 1)p^k - 1, \tag{16}$$

since

$$d - 1 = e_0 + (p-1)(p^m + \cdots + p^{m+k-1}) + d_{m+k}p^{m+k} + e_1 p^{m+k+1}$$

for some

$$0 \leq e_0 < p^m, \quad 0 \leq e_1 < p^{r-k-m-1},$$

and

$$p^m \ell = \ell_0 p^m + \cdots + \ell_{k-1} p^{m+k-1} + \ell_k p^{m+k}$$

for some

$$0 \leq \ell_0, \dots, \ell_{k-1} < p, \quad 0 \leq \ell_k \leq d_{m+k},$$

and any $0 \leq \ell \leq (d_{m+k} + 1)p^k - 1$.

Note that

$$\begin{aligned} d - \frac{d - d_0}{p} - 1 &\geq (d-1)\left(1 - \frac{1}{p}\right) \geq ((d_{m+k} + 1)p^k - 1)\left(1 - \frac{1}{p}\right) p^m \\ &\geq ((d_{m+k} + 1)(p^k - p^{k-1}) - 1)p^m, \quad k \geq 1. \end{aligned}$$

Combining (14) with (15) and (16), respectively, we get

$$\sum_{i=1}^{s} a_i \alpha_i^{\ell} = 0, \quad \ell = 0, \dots d_0 - 1, \tag{17}$$

and

$$\sum_{i=1}^{s} a_i \alpha_i^{p^m \ell}, \quad \ell = 0, \dots, (d_{m+k} + 1)(p^k - p^{k-1}) - 1, \quad k \geq 1, \tag{18}$$

respectively.

Hence, if $s \leq d_0$ ($n = 1$ or $k = 0$) or $s \leq (d_{m+k} + 1)(p^k - p^{k-1})$ ($n \geq 2$ and $k \geq 1$), the $s \times s$ coefficient matrix of the equations for $\ell = 0, \dots, s - 1$ of (17) or (18), respectively, is an invertible Vandermonde matrix and we get

$$a_i = 0, \quad i = 1, \dots, s,$$

contradicting $(a_1, \ldots, a_s) \in \boldsymbol{F}_p^s \setminus \{(0, \ldots, 0)\}$. For the second case we used that $\xi \mapsto \xi^{p^m}$ permutes $\boldsymbol{F}_q$ and the $\alpha_i^{p^m}$, $i = 1, \ldots, s$, are pairwise distinct.

Proof of the second part of Theorem 1: now assume $d < p^n$ for some n with $1 \le n \le r$, that is, $d_n = \cdots = d_{r-1} = 0$, and assume (3) and (4). Let D be the number of binomial coefficients $\binom{d}{\ell}$, $\ell = 1, \ldots, d$, which are nonzero modulo p. By Lemma 4 we have

$$D = (d_0 + 1) \cdots (d_{n-1} + 1) - 1.$$

For any $\alpha \in \boldsymbol{F}_q$ the polynomial

$$(X + \alpha)^d - \alpha^d = \sum_{\ell=0}^{d-1} \binom{d}{\ell} \alpha^\ell X^{d-\ell}$$

is in the vector space generated by the monomials $X^{d-\ell}$ with nonzero $\binom{d}{\ell}$ mod p, $\ell = 0, \ldots, d-1$, of dimension D. For $D < s \le q$ and any $(\alpha_1, \ldots, \alpha_s) \in \boldsymbol{F}_q^s$ there is a nontrivial linear combination

$$\sum_{i=1}^{s} \rho_i \left((X + \alpha_i)^d - \alpha_i^d \right) = 0$$

of the zero polynomial with $(\rho_1, \ldots, \rho_s) \in \boldsymbol{F}_q^s \setminus \{(0, \ldots, 0)\}$. If $D < s \le p$ and we take $\alpha_i \in \boldsymbol{F}_p$, $i = 1, \ldots, s$, then we may assume $\rho_i = a_i \in \boldsymbol{F}_p$ and

$$\sum_{i=1}^{s} a_i \mathrm{Tr} \left(\delta \left((\xi + \alpha_i)^d - \alpha_i^d \right) \right) = 0 \quad \text{for all } \xi \in \boldsymbol{F}_q.$$

Taking $(a_1, \ldots, a_s) \in \boldsymbol{F}_p^s \setminus \{(0, \ldots, 0)\}$ from the previous step, the vector space of solutions $(c_1, \ldots, c_s) \in \boldsymbol{F}_p^s$ of the equation

$$a_1 c_1 + \cdots + a_s c_s = 0$$

is of dimension $s - 1$. More precisely, the mapping

$$\varphi : \boldsymbol{F}_p^s \to \boldsymbol{F}_p, \quad \varphi(_1, \ldots, c_s) = a_1 c_1 + \cdots + a_s c_s$$

is surjective since $(a_1, \ldots, a_s)$ is not the zero vector. By the rank-nullity theorem its kernel is of dimension $s - 1$.

That is, not all $\mathbf{c} = (c_1, \ldots, c_s) \in \boldsymbol{F}_p^s$ are attained as

$$\mathbf{c} = \left(\mathrm{Tr} \left(\delta \left((\xi + \alpha_i)^d - \alpha_i^d \right) \right) \right)_{i=1}^{s}$$

for any $\xi \in \boldsymbol{F}_q$, namely those $\mathbf{c}$ which are not in the kernel of φ. We can extend this argument to $s > p$ by extending $(a_1, \ldots, a_p) \in \boldsymbol{F}_p^p \setminus \{(0, \ldots, 0)\}$ to $(a_1, \ldots, a_p, 0, \ldots, 0) \in \boldsymbol{F}_p^s \setminus \{(0, \ldots, 0)\}$.

Proof of the third part of Theorem 1: now we drop the condition (3) but then s has to satisfy the stronger condition (5) instead of (4). We extend the definition of the trace to polynomials $f(X) \in \boldsymbol{F}_{p^r}[X]$,

$$\mathrm{Tr}(f(X)) = \sum_{j=0}^{r-1} f(X)^{p^j}.$$

For each $\alpha \in \boldsymbol{F}_q$ we have

$$\mathrm{Tr}(\delta((X + \alpha)^d - \alpha^d)) = \sum_{\ell=0}^{d-1} \binom{d}{\ell} \mathrm{Tr}(\delta \alpha^\ell X^{d-\ell}),$$

since the trace is $\boldsymbol{F}_p$-linear, and thus it lies in the $\boldsymbol{F}_p$-linear space generated by the polynomials $\mathrm{Tr}(\beta_i X^{d-\ell})$ with nonzero $\binom{d}{\ell}$ modulo p, $i=1,\ldots,r$, $\ell=1,\ldots,d$, of dimension at most Dr, where $\{\beta_1,\ldots,\beta_r\}$ is a basis of $\boldsymbol{F}_q$ over $\boldsymbol{F}_p$. Now let $s > Dr$, then for any $\boldsymbol{\alpha}=(\alpha_1,\ldots\alpha_s)\in\boldsymbol{F}_q^s$ consider the set of polynomials

$$\left\{\mathrm{Tr}(\delta((X+\alpha_i)^d-\alpha_i^d)) : i=1,\ldots,s\right\}.$$

Since $s > Dr$ there is a nontrivial $\boldsymbol{F}_p$-linear combination

$$\sum_{i=1}^{s} a_i \mathrm{Tr}(\delta((X+\alpha_i)^d-\alpha_i^d)) = 0$$

of the zero polynomial. Now consider the linear subspace of solutions $(c_1,\ldots,c_s)\in\boldsymbol{F}_p^s$ of the equation $a_1c_1+\cdots+a_sc_s=0$ which is of dimension $s-1$. Let $\mathbf{c}\in\boldsymbol{F}_p^s$ be a point which does not lie in this linear subspace, then $\mathbf{c}$ is not attained as $\mathbf{c}=(\mathrm{Tr}(\delta((\xi+\alpha_i)^d-\alpha_i^d)))_{i=1}^s$ for any $\xi\in\boldsymbol{F}_q$.

5 Rational functions $f_{-d}(X)=X^{-d}$

Let $f_{q-d-1}(X)=X^{q-1-d}$ be a monomial of degree $q-d-1$, where $1\le d<q-1$. With the convention $0^{-1}=0$ we can identify $f_{q-d-1}(X)$ with the rational function $f_{-d}(X)=X^{-d}$. Let $\gcd(d,q)=p^j$. Since

$$(X+\alpha)^{-p^j}=(X^{p^j}+\alpha^{p^j})^{-1}$$

and $\xi\mapsto\xi^{p^j}$ permutes $\boldsymbol{F}_q$ we have

$$\left|\mathcal{T}(\mathbf{c},\boldsymbol{\alpha},f_{-dp^j})\right|=\left|\mathcal{T}(\mathbf{c},\boldsymbol{\alpha}^{p^j},f_{-d})\right|$$

and may restrict ourselves to the case $\gcd(d,q)=1$, that is,

$$d=d_0+t_1p,\quad \text{where } 1\le d_0<p.$$

We first show that there is no nonzero s-tuple

$$(a_1,\ldots,a_s)\in\boldsymbol{F}_p^s\setminus\{(0,\ldots,0)\}$$

such that

$$F_{a_1,\ldots,a_s}(X)=\sum_{i=1}^{s}a_i(X+\alpha_i)^{-d}=H(X)^p-H(X)$$

for any rational function $H(X)\in\overline{\boldsymbol{F}_p}(X)$. We have

$$F_{a_1,\ldots,a_s}(X)=\frac{f(X)}{g(X)},$$

where

$$f(X)=\delta\sum_{j=1}^{s}a_j\prod_{i\neq j}(X+\alpha_i)^d$$

and

$$g(X)=\prod_{i=1}^{s}(X+\alpha_i)^d.$$

Suppose to the contrary that there exists a rational function

$$H(X)=\frac{u(X)}{v(X)}\in\overline{\boldsymbol{F}_p}(X)\quad\text{with }\gcd(u,v)=1\quad\text{and}\quad v(X)\text{ is monic}$$

satisfying

$$F_{a_1,\dots,a_s}(X) = H(X)^p - H(X).$$

Therefore, we have

$$\frac{f(X)}{g(X)} = \frac{u(X)^p}{v(X)^p} - \frac{u(X)}{v(X)}. \tag{19}$$

Clearing denominators we obtain

$$f(X)v(X)^p = (u(X)^p - u(X)v(X)^{p-1})g(X)$$

and thus $v(X)^p$ divides $g(X)$, hence

$$v(X) = \prod_{i=1}^{s}(X+\alpha_i)^{e_i} \quad \text{for some } 0 \le e_i \le t_1, \quad i = 1, \dots, s.$$

Now by taking derivatives of both sides of (19) and clearing denominators we get

$$(f'(X)g(X) - f(X)g'(X))v(X)^2 = (u(X)v'(X) - u'(X)v(X))g(X)^2. \tag{20}$$

Without loss of generality we may assume $a_1 \neq 0$, thus

$$f(-\alpha_1) = \delta a_1 \prod_{i=2}^{s}(\alpha_i - \alpha_1)^d \neq 0$$

and

$$X + \alpha_1 \text{ does not divide } f(X).$$

Moreover, $(X+\alpha_1)^{d-1}$ and $(X+\alpha_1)^d$ are the largest powers dividing $g'(X)$ and $g(X)$, respectively, that is,

$$(X+\alpha_1)^{d-1+2e_1}$$

is the largest power of $(X+\alpha_1)$ dividing the left hand side of (20). Observing that $g(X)^2$ and thus the right hand side of (20) is divisible by

$$(X+\alpha_1)^{2d}$$

we get

$$d - 1 + 2e_1 \ge 2d$$

and thus

$$e_1 \ge \frac{d+1}{2} > \frac{t_1 p}{2} \ge t_1,$$

which is a contradiction.

We showed that the conditions of Lemma 2 are satisfied and Theorem 2 follows from (8) and Lemma 2 since

$$\left|\sum_{\xi \in \mathbf{F}_q} \psi(F_{a_1,\dots,a_s}(\xi))\right| \le \left|\sum_{\xi \in \mathbf{F}_q \setminus -\boldsymbol{\alpha}} \psi(F_{a_1,\dots,a_s}(\xi))\right| + s,$$

where $-\boldsymbol{\alpha} = \{-\alpha_1, \dots, -\alpha_s\}$.

6 Arbitrary polynomials

In this section we prove Theorem 3.

Let

$$f(X)=\sum_{j=0}^{d}\gamma_j X^j \in \boldsymbol{F}_q[X], \quad \gamma_d \neq 0,$$

be a polynomial of degree

$$d=d_0+t_1p, \quad 1\le d_0<p, \quad 0\le t_1<q/p.$$

Proof of the first part: we have to show that (6) is applicable, that is, the polynomial $F_{a_1,\dots,a_s}(X)$ defined by (9) is not of the form $g(X)^p-g(X)+c$ for any $(a_1,\dots,a_s)\neq(0,\dots,0)$.

Suppose the contrary that there exists an s-tuple

$$(a_1,\dots,a_s)\in \boldsymbol{F}_p^s\setminus\{(0,\dots,0)\}$$

such that the polynomial

$$F_{a_1,\dots,a_s}(X)=\delta\sum_{\ell=0}^{d}\left(\sum_{j=\ell}^{d}\sum_{i=1}^{s}a_i\gamma_j\binom{j}{\ell}\alpha_i^{j-\ell}\right)X^\ell$$

can be written as

$$g(X)^p-g(X)+c \quad \text{for some } g(X)\in \boldsymbol{F}_q[X] \quad \text{and} \quad c\in \boldsymbol{F}_q.$$

We have either

$$F_{a_1,\dots,a_s}(X)=0$$

or

$$\deg(F_{a_1,\dots,a_s})\equiv 0 \bmod p.$$

Hence,

$$\deg(F_{a_1,\dots,a_s})\le d-d_0,$$

where we used the convention $\deg(0)=-1$. We conclude that the coefficients δR_ℓ of $F_{a_1,\dots,a_s}(X)$ at X^ℓ vanish for $\ell=d-d_0+1,\dots,d$. Since $\delta\neq 0$ we have

$$R_\ell=\sum_{j=\ell}^{d}\sum_{i=1}^{s}a_i\gamma_j\binom{j}{\ell}\alpha_i^{j-\ell}=0, \quad \ell=(d-d_0)+1,\dots,d. \tag{21}$$

Note that by Lucas' congruence, Lemma 3,

$$\binom{d}{r}\equiv\binom{d_0}{r}\not\equiv 0 \bmod p, \quad r=0,\dots,d_0. \tag{22}$$

Define T_ℓ, $\ell=0,\dots d_0-1$, recursively by

$$T_0=R_d$$

and

$$T_\ell=R_{d-\ell}-\gamma_d^{-1}\sum_{r=0}^{\ell-1}\gamma_{d-\ell+r}\binom{r+d-\ell}{d-\ell}\binom{d}{r}^{-1}T_r, \tag{23}$$

for $\ell=1,\dots,d_0-1$. Next we show that

$$T_\ell=\gamma_d\binom{d}{\ell}\sum_{i=1}^{s}a_i\alpha_i^\ell=0, \quad \ell=0,\dots,d_0-1. \tag{24}$$

For $\ell = 0$ the formula follows from (21) and for $\ell = 1, \dots, d_0 - 1$ from (23) we get by induction

$$T_\ell = R_{d-\ell} - \sum_{r=0}^{\ell-1} \gamma_{d-\ell+r} \binom{r+d-\ell}{d-\ell} \sum_{i=1}^{s} a_i \alpha_i^r$$

and from (21)

$$T_\ell = \gamma_d \binom{d}{\ell} \sum_{i=1}^{s} a_i \alpha_i^\ell.$$

Moreover, we get

$$T_\ell = 0, \quad \ell = 0, \dots, d_0 - 1,$$

from (21), (23) again by induction.

By (24) and (22) we get since $\gamma_d \neq 0$,

$$\sum_{i=1}^{s} a_i \alpha_i^\ell = 0, \quad \ell = 0, \dots, d_0 - 1.$$

Thus for $s \le d_0$, the $(s \times s)$-coefficient matrix

$$\left(\alpha_i^\ell\right)_{i=1,\dots,s,\ell=0,1,\dots,s-1}$$

of the system of the first s equations is a regular Vandermonde matrix and we get $(a_1, \dots, a_s) = (0, \dots, 0)$, which is a contradiction.

For the second part of Theorem 3 we assume $f(X) \in \boldsymbol{F}_p[X]$ and notice that for any $\alpha \in \boldsymbol{F}_q$ the element $f(X+\alpha) - f(\alpha)$ is in the vector space generated by the monomials X^i, $i = 1, \dots, d$, of dimension d.

If $d < s \le p$, we can choose any $\boldsymbol{\alpha} \in \boldsymbol{F}_p^s$. Then

$$f(X+\alpha_i) - f(\alpha_i), \quad i = 1, \dots, s,$$

are linearly dependent over $\boldsymbol{F}_p$ as well as

$$\mathrm{Tr}(\delta(f(X+\alpha_i) - f(\alpha_i))), \quad i = 1, \dots, s,$$

that is,

$$\sum_{i=1}^{s} a_i \mathrm{Tr}(\delta(f(X+\alpha_i) - f(\alpha_i))) = 0$$

for some $(a_1, \dots, a_s) \in \boldsymbol{F}_p^s \setminus \{(0, \dots, 0)\}$ and the result follows since not all $(c_1, \dots, c_s) \in \boldsymbol{F}_p^s$ satisfy $a_1 c_1 + \dots + a_s c_s = 0$.

If $d < p$ and $s > p$, we can choose $(a_1, \dots, a_p) \in \boldsymbol{F}_p^p \setminus \{(0, \dots, 0)\}$ as in the case $s = p$ and extend it to $(a_1, \dots, a_p, a_{p+1}, \dots, a_s) \in \boldsymbol{F}_p^s \setminus \{(0, \dots, 0)\}$ with $a_{p+1} = \dots = a_s = 0$.

Proof of the third part of Theorem 3: recall that $\{\beta_1, \dots, \beta_r\}$ is a basis of $\boldsymbol{F}_q$ over $\boldsymbol{F}_p$. Each $\delta(f(X+\alpha) - f(\alpha))$ lies in the $\boldsymbol{F}_p$-vector space generated by

$$\delta \beta_j X^i, \quad j = 1, \dots, r, \quad i = 1, \dots, d,$$

of dimension dr. The dimension of the vector space generated by

$$\mathrm{Tr}(\delta \beta_j X^i) \quad j = 1, \dots, r, \quad i = 1, \dots, d,$$

is at most dr. If $q \ge s > dr$, there is a nontrivial linear combination

$$\sum_{i=1}^{s} a_i \mathrm{Tr}(\delta(f(X+\alpha_i) - f(\alpha_i))) = 0$$

for any $\boldsymbol{\alpha} \in \boldsymbol{F}_q^s$ and the result follows.

7 Final remarks

7.1 Examples for $\gcd(d, p) > 1$ and $\mathcal{T}(\mathbf{c}, \alpha, f) = \emptyset$

Now we provide an example that if we drop the condition on s in part 1 of Theorem 3, the restriction $\gcd(d, q) = 1$, that is $d_0 \geq 1$, is needed.

Choose any $f(X)$ of the form

$$f(X) = \delta^{-1}(g(X)^p - g(X) + c) \quad \text{for some } g(X) \in \boldsymbol{F}_q[X] \quad \text{and} \quad c \in \boldsymbol{F}_q.$$

Then we obtain

$$\begin{aligned} T(f(\xi + \alpha_1)) &= \mathrm{Tr}(\delta f(\xi + \alpha_1)) \\ &= \mathrm{Tr}(g(\xi + \alpha_1)^p - g(\xi + \alpha_1) + c) = \mathrm{Tr}(c) \end{aligned}$$

for all $\xi \in \boldsymbol{F}_q$, that is, any vector $(c_1, \ldots, c_r) \in \boldsymbol{F}_p^r$ with $c_1 \neq \mathrm{Tr}(c)$ is not attained as $(T(f(\xi + \alpha_i)))_{i=1}^s$.

We conclude that for polynomials of degree d with $\gcd(d, p) > 1$, the bound of Theorem 3 may not hold for all s. However, by Theorem 1, for monomials the restriction $\gcd(d, p) = 1$ is not needed.

7.2 Missing digits and subsets

For subsets $\mathcal{D}$ of $\boldsymbol{F}_p$, the closely related problem of estimating the number of $\xi \in \boldsymbol{F}_q$ with

$$f(\xi) \in \{d_1\beta_1 + \cdots + d_r\beta_r : d_1, \ldots, d_r \in \mathcal{D}\}$$

was studied in [10–12], that is, $f(\xi)$ 'misses' the digits in $\boldsymbol{F}_p \setminus \mathcal{D}$. It is straightforward to extend these results combining our approach with certain bounds on character sums to estimate the number of $\xi \in \boldsymbol{F}_q$ with

$$f(\xi + \alpha_i) \in \{d_1\beta_1 + \cdots + d_r\beta_r : d_1, \ldots, d_r \in \mathcal{D}\}, \quad i = 1, \ldots, s.$$

For example, for $\mathcal{D} = \{0, \ldots, t-1\}$ we can use the bound on exponential sums of [13].

Instead of restricting the set of digits we may restrict the set of ξ. That is, for a subset $\mathcal{S}$ of $\boldsymbol{F}_q$ we are interested in the number of solutions $\xi \in \mathcal{S}$ of

$$(T(f(\xi + \alpha_1)), \ldots, T(f(\xi + \alpha_s))) = \mathbf{c}$$

for any fixed $\mathbf{c} \in \boldsymbol{F}_p^s$. Typical choices of $\mathcal{S}$ are 'boxes' [13,14] and 'consecutive' elements [15].

7.3 Optimality and prescribed digits

Swaenepoel [16] improved the bound (1) of [2] in the case when the polynomial $f(X)$ has degree 2 or is a monomial. In particular, for $s = 1$ and $d = 2$ the improved bound of [16] is optimal. She also generalized (1) to several polynomials with $\boldsymbol{F}_p$-linearly independent leading coefficients [16, Theorem 1.5].

Moreover, in [17] Swaenepoel studied the number of solutions $\xi \in \boldsymbol{F}_q$ for which some of the digits of $f(\xi)$ are prescribed, that is, for given $\mathcal{I} \subset \{1, \ldots, r\}$ and given $c_i \in \boldsymbol{F}_p$, $i \in \mathcal{I}$, the number of $\xi \in \boldsymbol{F}_q$ with

$$\mathrm{Tr}(\delta_i f(\xi)) = c_i, \quad i \in \mathcal{I}.$$

7.4 Related work on pseudorandom number generators

Some of the ideas of the proofs in this paper are based on earlier work on nonlinear, in particular, inversive pseudorandom number generators, see [18–20].

More precisely, in [20] the q-periodic sequence (η_n) over $\boldsymbol{F}_q$ defined by

$$\eta_{n_1+n_2p+\cdots+n_rp^{r-1}} = f(n_1\beta_1+\cdots+n_r\beta_r), \quad 0 \le n_1,\ldots,n_r < p,$$

passes the *s-dimensional lattice test* if s polynomials of the form

$$f(X+\alpha_j) - f(\alpha_j), \quad j = 1,\ldots,s,$$

are $\boldsymbol{F}_q$-linearly independent. However, in the proofs of this paper we need that they are linearly independent (resp. dependent) over $\boldsymbol{F}_p$.

To prove Theorem 2 for $d < p$, the method of [19] can be easily adjusted using [19, Lemma 2]. However, for $d \ge p$ we had to use a different approach since [19, Lemma 2] is not applicable in this case.

Finally, in the proof of [18, Theorem 4] we showed that polynomials of the form $F_{a_1,\ldots,a_s}(X)$ can only be identical 0 if $a_1 = \cdots = a_s = 0$. However, in the proof of Theorem 3 we had to show that $F_{a_1,\ldots,a_s}(X)$ is not of the form $g(X)^p - g(X) + c$ and we had to modify the idea of [18].

7.5 Rudin–Shapiro function

The *Rudin–Shapiro sequence* (r_n) is defined by

$$r_n = \sum_{i=0}^{\infty} n_i n_{i+1}, \quad n = 0, 1, \ldots$$

if

$$n = \sum_{i=0}^{\infty} n_i 2^i, \quad n_0, n_1, \ldots \in \{0, 1\}.$$

Müllner showed that the Rudin–Shapiro sequence along squares (r_{n^2}) is normal [21].

The *Rudin–Shapiro function* $R(\xi)$ for the finite field $\boldsymbol{F}_q$ with respect to the ordered basis $(\beta_1,\ldots,\beta_r)$ is defined as

$$R(\xi) = \sum_{i=1}^{r-1} x_i x_{i+1}, \quad \xi = x_1\beta_1 + x_2\beta_2 + \cdots + x_r\beta_r, \quad x_1,\ldots,x_r \in \boldsymbol{F}_p.$$

For $f(X) \in \boldsymbol{F}_q[X]$ and $c \in \boldsymbol{F}_p$ let

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

It seems to be not possible to use character sums to estimate the size of $\mathcal{R}(c,f)$. However, in [22] the Hooley–Katz Theorem, see [23, Theorem 7.1.14] or [24] was used to show that if $d = \deg(f) \ge 1$,

$$\left|\mathcal{R}(c,f) - p^{r-1}\right| \le C_{r,d}\, p^{\frac{3r+1}{4}},$$

where $C_{r,d}$ is a constant depending only on r and d. In particular, we have for fixed d and $r \ge 6$,

$$\lim_{p\to\infty} \frac{|\mathcal{R}(c,f)|}{p^{r-1}} = 1,$$

that is, $R(f)$ is p-normal for $s = 1$ and $r \ge 6$.

However, we are not aware of a result on the r-normality of $R(f)$.

Acknowledgements
The authors are partially supported by the Austrian Science Fund FWF Project P 30405. They wish to thank the anonymous referee for very useful suggestions.

Funding Open access funding provided by Johannes Kepler University Linz.

Author details
[1]Research Institute for Symbolic Computation, Altenberger Str. 69, 4040 Linz, Austria, [1]Johann Radon Institute for Computational and Applied Mathematics, Austrian Academy of Sciences, Altenberger Str. 69, 4040 Linz, Austria.

Received: 5 October 2021 Accepted: 1 May 2022 Published online: 12 June 2022

References

1. Drmota, M., Mauduit, C., Rivat, J.: Normality along squares. J. Eur. Math. Soc. **21**(2), 507–548 (2019). https://doi.org/10.4171/JEMS/843
2. Dartyge, C., Sárközy, A.: The sum of digits function in finite fields. Proc. Am. Math. Soc. **141**(12), 4119–4124 (2013). https://doi.org/10.1090/S0002-9939-2013-11801-0
3. Lidl, R., Niederreiter, H.: Introduction to Finite Fields and Their Applications, p. 407. Cambridge University Press, Cambridge (1986)
4. Schmidt, W.M.: Equations over Finite Fields. An Elementary Approach. Lecture Notes in Mathematics, vol. 536, p. 276. Springer, Berlin (1976)
5. Weil, A.: On some exponential sums. Proc. Natl Acad. Sci. USA **34**, 204–207 (1948). https://doi.org/10.1073/pnas.34.5.204
6. Moreno, C.J., Moreno, O.: Exponential sums and Goppa codes. I. Proc. Am. Math. Soc. **111**(2), 523–531 (1991). https://doi.org/10.2307/2048345
7. Lucas, E.: Theorie des Fonctions Numeriques Simplement Periodiques. Am. J. Math. **1**(2), 184–196 (1878). https://doi.org/10.2307/2369308
8. Niederreiter, H., Winterhof, A.: Applied Number Theory, p. 442. Springer, Berlin (2015). https://doi.org/10.1007/978-3-319-22321-6
9. Fine, N.J.: Binomial coefficients modulo a prime. Am. Math. Mon. **54**, 589–592 (1947). https://doi.org/10.2307/2304500
10. Dartyge, C., Mauduit, C., Sárközy, A.: Polynomial values and generators with missing digits in finite fields. Funct. Approx. Comment. Math. **52**(1), 65–74 (2015). https://doi.org/10.7169/facm/2015.52.1.5
11. Dietmann, R., Elsholtz, C., Shparlinski, I.E.: Prescribing the binary digits of squarefree numbers and quadratic residues. Trans. Am. Math. Soc. **369**(12), 8369–8388 (2017). https://doi.org/10.1090/tran/6903
12. Gabdullin, M.R.: 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). https://doi.org/10.4213/mzm11091
13. Konyagin, S.V.: Estimates for character sums in finite fields. Mat. Zametki **88**(4), 529–542 (2010). https://doi.org/10.1134/S0001434610090221
14. Davenport, H., Lewis, D.J.: Character sums and primitive roots in finite fields. Rend. Circ. Mat. Palermo **2**(12), 129–136 (1963). https://doi.org/10.1007/BF02843959
15. Winterhof, A.: Incomplete additive character sums and applications. In: Finite Fields and Applications (Augsburg, 1999), pp. 462–474. Springer, Berlin (2001)
16. Swaenepoel, C.: On the sum of digits of special sequences in finite fields. Mon. Math. **187**(4), 705–728 (2018). https://doi.org/10.1007/s00605-017-1148-5
17. Swaenepoel, C.: Prescribing digits in finite fields. J. Number Theory **189**, 97–114 (2018). https://doi.org/10.1016/j.jnt.2017.11.012
18. Meidl, W., Winterhof, A.: On the linear complexity profile of explicit nonlinear pseudorandom numbers. Inf. Process. Lett. **85**(1), 13–18 (2003). https://doi.org/10.1016/S0020-0190(02)00335-6
19. Niederreiter, H., Winterhof, A.: Incomplete exponential sums over finite fields and their applications to new inversive pseudorandom number generators. Acta Arith. **93**(4), 387–399 (2000). https://doi.org/10.4064/aa-93-4-387-399
20. Niederreiter, H., Winterhof, A.: On the lattice structure of pseudorandom numbers generated over arbitrary finite fields. Appl. Algebra Eng. Commun. Comput. **12**(3), 265–272 (2001). https://doi.org/10.1007/s002000100074
21. Müllner, C.: The Rudin–Shapiro sequence and similar sequences are normal along squares. Can. J. Math. **70**(5), 1096–1129 (2018). https://doi.org/10.4153/CJM-2017-053-1
22. Dartyge, C., Mérai, L., Winterhof, A.: On the distribution of the Rudin–Shapiro function for finite fields. Proc. Am. Math. Soc. **149**(12), 5013–5023 (2021). https://doi.org/10.1090/proc/15668
23. Mullen, G.L. (ed.): Handbook of Finite Fields. Discrete Mathematics and Its Applications (Boca Raton), p. 1033. CRC Press, Boca Raton (2013). https://doi.org/10.1201/b15006
24. Hooley, C.: On the number of points on a complete intersection over a finite field. J. Number Theory **38**(3), 338–358 (1991). https://doi.org/10.1016/0022-314X(91)90023-5 (**With an Appendix by Nicholas M. Katz**)

Publisher's Note