On the Distribution of the Rudin-Shapiro Function for Finite Fields

Arne Winterhof
(joint work with Cécile Dartyge and László Mérai)

Austrian Academy of Sciences
RICAM, Linz

Carleton Finite Fields eSeminar
June 3, 2020

Motivation

- many recent results on problems combining arithmetic properties of integers and some conditions on their digits (Bourgain, Maynard, Drmota, Mauduit, Rivat,...)
- natural to study analogs for finite fields (Porritt, Dartyge, Sárközy, Swaenepoel, ...)
- sometimes finite field analog can be solved although integer problem is out of reach
- Example: Are subsequences of Thue-Morse and Rudin-Shapiro sequence along polynomials normal?
- Yes for degree 2 by Drmota, Mauduit, Rivat / Müllner. Degree ≥ 3 open!
- Finite field analogs: Thue-Morse settled by Dartyge and Sárközy
- analog of Rudin-Shapiro settled here

Thue-Morse sequence

$n \geq 0$ integer

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

Thue-Morse (sum of digits) sequence (t_n):

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

$$t_{n+2^s} = 1 - t_n, \quad n = 0, 1, \ldots, 2^s - 1$$

$$0$$

Thue-Morse sequence

$n \geq 0$ integer

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

Thue-Morse (sum of digits) sequence (t_n):

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

$$t_{n+2^s} = 1 - t_n, \quad n = 0, 1, \ldots, 2^s - 1$$

01

Thue-Morse sequence

$n \geq 0$ integer

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

Thue-Morse (sum of digits) sequence (t_n):

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

$$t_{n+2^s} = 1 - t_n, \quad n = 0, 1, \ldots, 2^s - 1$$

0110

Thue-Morse sequence

$n \geq 0$ integer

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

Thue-Morse (sum of digits) sequence (t_n):

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

$$t_{n+2^s} = 1 - t_n, \quad n = 0, 1, \ldots, 2^s - 1$$

01101001

Thue-Morse sequence

$n \geq 0$ integer

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

Thue-Morse (sum of digits) sequence (t_n):

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

$$t_{n+2^s} = 1 - t_n, \quad n = 0, 1, \ldots, 2^s - 1$$

$$0110100110010110\ldots$$

- balanced
- no pattern 000 or 111 appears

Rudin-Shapiro sequence

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

Rudin-Shapiro sequence (r_n):

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

$$0001001000011101\ldots$$

- not 'looking random'
- many patterns, e.g., 00000 and 11111 never appear
- not 'normal'

Normal sequences

A binary sequence (s_n) is normal if for any fixed length k each pattern of length k appears asymptotically equally often.

- Almost all sequences are normal.
- However, it is difficult to find concrete examples.
- 'If you can describe a sequence, it is not 'random' anymore.'

Thue-Morse and Rudin-Shapiro sequence along squares

Thue-Morse and Rudin-Shapiro sequence are NOT normal. What about subsequences?

(t_{n^2}):

$$01101001100101101001\ldots$$

- balanced
- all pairs, triples, ... appear asymptotically equally often
- each pattern of fixed length appears asymptotically the same time (normal)

(r_{n^2}):

$$00010010000111010\ldots$$

- (r_{n^2}) is normal

Drmota, Mauduit, Rivat, 2019: (t_{n^2}) is normal

For any length $k \geq 1$ and any pattern $(b_0, \ldots, b_{k-1}) \in \{0,1\}^k$ of length k:

$$\begin{aligned} & \left|\{n = 0, \ldots, N-1 : (t_{n^2}, \ldots, t_{(n+k-1)^2}) = (b_0, \ldots, b_{k-1}\}\right| \\ = \quad & (1 + o_k(1))\frac{N}{2^k} \end{aligned}$$

Müllner, 2018: (r_{n^2}) is normal

Conjecture: For any polynomial P of degree $d \geq 2$ with $P(\mathbb{N}_0) \subseteq \mathbb{N}_0$ the sequences $(t_{P(n)})$ and $(r_{P(n)})$ are normal.

Still open even for $k = 1$!

Thue-Morse and Rudin-Shapiro function for $\mathbb{F}_q$

p prime, $q = p^r$
$(\beta_1, \ldots, \beta_r)$ ordered basis of $\mathbb{F}_q$ over $\mathbb{F}_p$

$$\xi = x_1\beta_1 + \ldots + x_r\beta_r \in \mathbb{F}_q \quad \text{with } x_i \in \mathbb{F}_p$$

Thue-Morse function on $\mathbb{F}_q$:

$$T(\xi) = \sum_{i=1}^{r} x_i \in \mathbb{F}_p$$

Rudin-Shapiro function on $\mathbb{F}_q$:

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

Trace, dual basis and digits

$Tr : \mathbb{F}_{p^r} \to \mathbb{F}_p$,

$$Tr(\xi) = \sum_{i=0}^{r-1} \xi^{p^i}$$

$(\delta_1, \ldots, \delta_r)$ dual basis of $(\beta_1, \ldots, \beta_r)$:

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

(exists and is unique)

$$Tr(\delta_i \xi) = Tr(\delta_i \sum_{j=1}^{r} x_i \beta_i) = x_i$$

Thue-Morse function:

$$T(\xi) = \sum_{i=1}^{r} x_i = \sum_{i=1}^{r} Tr(\delta_i \xi) = Tr(\delta \xi), \quad \delta = \sum_{i=1}^{r} \delta_i \neq 0$$

Distribution of the Thue-Morse function for $\mathbb{F}_q$

$f(X) \in \mathbb{F}_q[X]$ of degree d

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

$$|\mathcal{T}(c,f)| = \sum_{\xi \in \mathbb{F}_q} \underbrace{\frac{1}{p} \sum_{a \in \mathbb{F}_p} e_p(a(T(f(\xi)) - c))}_{\substack{1, \ T(f(\xi))=c \\ 0, \ T(f(\xi))\neq c}}$$

contribution for $a = 0$: $\frac{q}{p}$

$a \neq 0$: $\psi_a(\xi) = e_p(aT(\xi)) = e_p(aTr(\delta\xi))$ is non-trivial additive character of $\mathbb{F}_q$

Dartyge, Sárközy, 2013:

$$\left||\mathcal{T}(c,f)| - \frac{q}{p}\right| \le \max_{a\neq 0}\left|\sum_{\xi\in\mathbb{F}_q}\psi_a(f(\xi))\right| \le (d-1)q^{1/2}, \quad \gcd(d,p)=1$$

by Weil's bound.

d fixed, $r \ge 3$ fixed

$$|\mathcal{T}(c,f)| = (1+o(1))p^{r-1}, \quad p\to\infty$$

Example: $\gcd(d,p)=1$ necessary

$$\begin{aligned} f(X) &= \delta^{-1}(X^p - X) \\ T(f(\xi)) &= Tr(\delta f(\xi)) = 0, \quad \xi\in\mathbb{F}_q \end{aligned}$$

$$|\mathcal{T}(0,f)| = q, \quad |\mathcal{T}(c,f)| = 0, \ c\neq 0$$

Improvement for $f(X) = X^d$ and $c \neq 0$

F be a polynomial over $\mathbb{F}_p$ in r variables. A common zero in $\overline{\mathbb{F}_p}^r$ of the polynomials

$$F, \frac{\partial F}{\partial X_1}, \ldots, \frac{\partial F}{\partial X_r}$$

is called a singular point of F.

Deligne's Theorem, 1974:
Let Q be a polynomial over $\mathbb{F}_p$ in r variables of degree $D \geq 1$ without singular points such that its homogeneous part Q_D of degree D has only the trivial singular point $(0, \ldots, 0)$. Then the number N of zeros of Q in $\mathbb{F}_p^r$ satisfies

$$\left| N - p^{r-1} \right| \leq (D-1)^r p^{(r-1)/2}.$$

The polynomial Q for the Thue-Morse function with $f(X) = X^d$

$$\xi = x_1\beta_1 + \ldots + x_r\beta_r \in \mathbb{F}_q, \quad x_i \in \mathbb{F}_p$$

$$T(\xi^d) = Tr(\delta\xi^d) = \sum_{\ell=0}^{r-1} \delta^{p^\ell} \xi^{dp^\ell}$$

$$\begin{aligned} F(X_1, \ldots, X_r) &= \sum_{\ell=0}^{r-1} \delta^{p^\ell} (\underbrace{X_1\beta_1^{p^\ell} + \ldots + X_r\beta_r^{p^\ell}}_{Y_\ell})^d \\ &= Q(Y_0, \ldots, Y_{r-1}) \end{aligned}$$

$$T((\underbrace{x_1\beta_1 + \ldots + x_r\beta_r}_{\xi})^d) = F(x_1, \ldots, x_r), \quad x_1, \ldots, x_r \in \mathbb{F}_p$$

$Q - c$ has no singular points for $c \neq 0$ and $2 \leq d < p$

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

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

$(0, \ldots, 0)$ only common zero of the partial derivatives which is only a zero of $Q - c$ if $c = 0$

Improved result

Applying Deligne's Theorem:

$$\left| |\mathcal{T}(c,f)| - \frac{q}{p} \right| \leq (d-1)^r p^{(r-1)/2}, \quad c \neq 0$$

d fixed, $r \geq 2$ fixed

$$|\mathcal{T}(c,X^d)| = (1+o(1))p^{r-1}, \quad p \to \infty, \quad c \neq 0$$

Arbitrary $f(X)$, d, r fixed, $p \to \infty$:
improvement for all but at most $(d-1)^r$ different c
(independent of p!)

Rudin-Shapiro function

$(\beta_1, \ldots, \beta_r)$ ordered basis, $(\delta_1, \ldots, \delta_r)$ its dual basis

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

$$Tr(\delta_i \xi) = x_i$$

$$R(\xi) = \sum_{i=1}^{r-1} x_i x_{i+1} = \sum_{i=1}^{r-1} Tr(\delta_i \xi)\, Tr(\delta_{i+1} \xi)$$

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

$$\left| |\mathcal{R}(c, f)| - \frac{q}{p} \right| \leq ???$$

Permutation polynomials

Let $f(X)$ be a permutation polynomial of $\mathbb{F}_q$. Then

$$\mathcal{R}(c,f) = \mathcal{R}(c,X) = \{(x_1,\ldots,x_r) \in \mathbb{F}_p^r : \sum_{i=1}^{r-1} x_i x_{i+1} = c\}.$$

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

$N_r(c)$: number of solutions $(x_1, \ldots, x_r) \in \mathbb{F}_p^r$ of the quadratic form

$$x_1x_2 + x_2x_3 + \ldots + x_{r-3}x_{r-2} + x_{r-2}x_{r-1} + x_{r-1}x_r = c.$$

The recursion

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

is obtained by distinguishing the cases $x_{r-1} = 0$ and $x_{r-1} \neq 0$. Then we get

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

Arbitrary polynomials

First try: univariate Weil bound

$$\sum_{\xi\in\mathbb{F}_q} e_p\left(a\sum_{i=1}^{r-1} Tr(\delta_i\xi^d)\,Tr(\delta_{i+1}\xi^d)\right) = \sum_{\xi\in\mathbb{F}_q}\psi_a\left(\sum_{i=1}^{r}\delta_i\,Tr(\delta_{i+1}\xi^d)\right)$$

degree too large!

second try: multivariate Weil bound

$\xi = x_1\beta_1 + \ldots + x_r\beta_r$

$$\sum_{\xi\in\mathbb{F}_q}\ldots = \sum_{(x_1,\ldots,x_r)\in\mathbb{F}_p^r}\ldots$$

Works but gives only

$$\left||\mathcal{R}(c,f)| - p^{r-1}\right| = O_d(p^{r-1/2})$$

too weak!

Third try: Deligne's Theorem

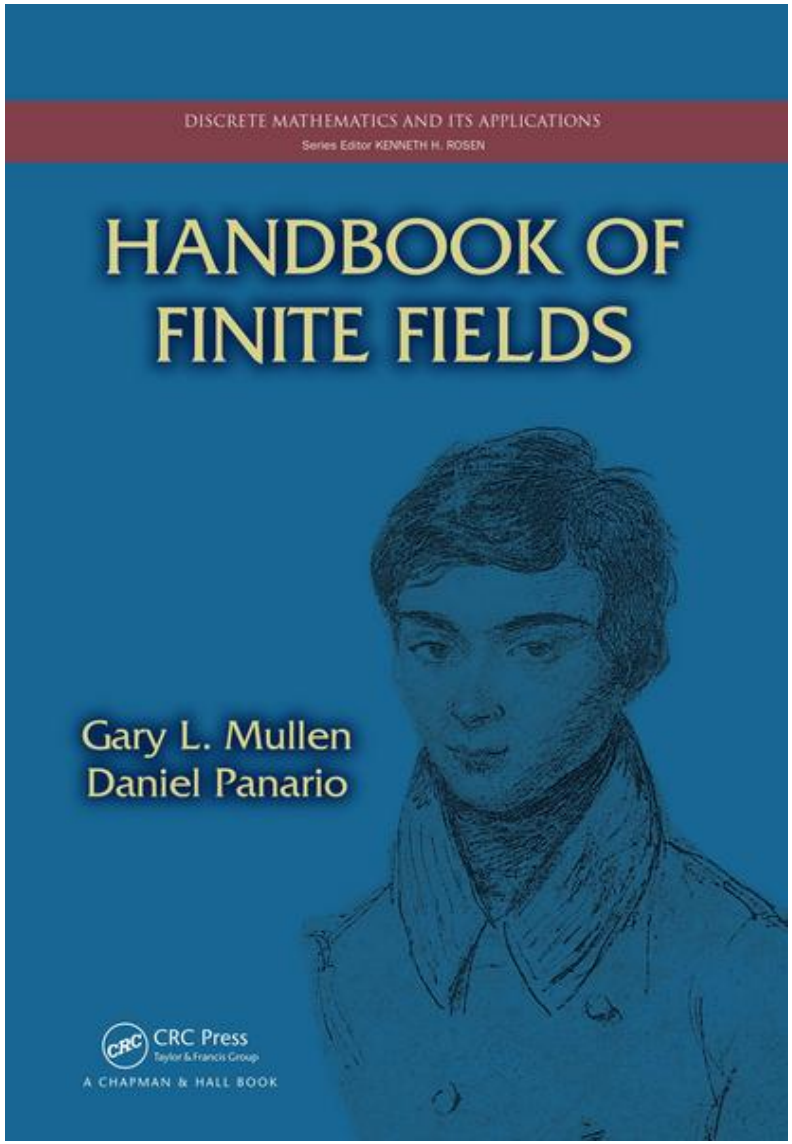
Problem: Our polynomial has singular points in general,

- for odd r always,
- for even r at least for some special choices of the basis $\{\beta_1, \ldots, \beta_r\}$.

What now?

What now?

Daqing Wan: Equation over finite fields, Chapter 7,



The Hooley-Katz Theorem, 1991

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

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

Let Q be a polynomial over $\mathbb{F}_p$ in r variables of degree $D \geq 1$ such that the dimensions of the singular loci of Q and its homogeneous part Q_D of degree D satisfy

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

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

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

$s = -1$: Deligne

The main result

Theorem

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

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

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,

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

Dimension

1. generalization of dimension of vector spaces over $\overline{\mathbb{F}_p}$
2. point, line, plane, ... are of dimension $0, 1, 2 \ldots$
3. $\dim(\emptyset) = -1$
4. $1 \leq |\mathcal{L}| < \infty$: $\dim(\mathcal{L}) = 0$
5. $\dim(U \cup V) = \max\{\dim(U), \dim(V)\}$
6. $\dim(U \cap V) \leq \min\{\dim(U), \dim(V)\}$
7. $V = \{\underline{x} \in \overline{\mathbb{F}_p}^r : f_i(\underline{x}) = 0,\ i = 1, \ldots, r\}$ for some polynomials f_i $I \subset \{1, \ldots, r\}$:

$$\dim(\{\underline{x} \in \overline{\mathbb{F}_p}^r : f_i(\underline{x}) = 0,\ i \in I\}) \leq \dim(V) - r + |I|$$

Deleting k equations increases the dimension by at most k.

(See for example Cox, Little, O'Shea, 2015.)

The polynomial Q for the Rudin-Shapiro function (and monomials)

$$Q(Y_0, \ldots, Y_{r-1}) = \sum_{k,\ell=0}^{r-1} a_{k,\ell} Y_k^d Y_\ell^d$$

with

$$a_{k,\ell} = \sum_{i=1}^{r-1} \delta_i^{p^k} \delta_{i+1}^{p^\ell}$$

$$\frac{\partial Q}{\partial Y_\ell} = d Y_\ell^{d-1} \sum_{k=0}^{r-1} (a_{k,\ell} + a_{\ell,k}) Y_k^d, \quad \ell = 0, \ldots, r-1.$$

We may restrict ourselves to $2 \le d < p$.

Singular points with only nonzero coordinates

Common zeros $(\eta_0, \ldots, \eta_{r-1}) \in \overline{\mathbb{F}_p}^r$ of

$$\sum_{k=0}^{r-1} (a_{k,\ell} + a_{\ell,k}) Y_k^d, \quad \ell = 0, \ldots, r-1.$$

After some calculations: $\zeta_m = \sum_{k=0}^{r-1} \delta_m^{p^k} \eta_k^d$

$$\begin{aligned} \zeta_2 &= 0, \\ \zeta_{m-1} + \zeta_{m+1} &= 0, \quad m = 2, \ldots, r-1, \\ \zeta_{r-1} &= 0. \end{aligned}$$

Even r

$$\zeta_m = \sum_{k=0}^{r-1} \delta_m^{p^k} \eta_k^d = 0, \quad m = 1, \ldots, r$$

regular coordinate transformation of $(\eta_0^d, \ldots, \eta_{r-1}^d)$:

$$\eta_k^d = \eta_k = 0, \quad k = 0, 1, \ldots, r-1.$$

Odd r

$$\zeta_m = \sum_{k=0}^{r-1} \delta_m^{p^k} \eta_k^d = \begin{cases} 0, & m \text{ even}, \\ (-1)^{(m-1)/2}\lambda, & m \text{ odd}, \end{cases} \qquad m = 1, \ldots, r,$$

for any $\lambda \in \overline{\mathbb{F}_p}$.

$$\eta_k^d = \lambda \sum_{\substack{m=1 \\ m \text{ odd}}}^{r} \beta_m^{p^k} (-1)^{(m-1)/2}, \quad k = 0, \ldots, r-1.$$

dimension 1!

A dirty trick

$L \subset \{0, \ldots, r-1\}$
Assume that $(\eta_0, \ldots, \eta_{r-1})$ is a singular point with $\eta_\ell \neq 0$ iff $\ell \in L$, that is, it is a solution of

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

obtained from the above case by deleting $r - |L|$ equations, that is, of dimension at most $r - |L|\{+1\}$ depending if r is even or odd.
On the other hand

$$\{(\eta_0, \ldots, \eta_{r-1}) : \eta_\ell = 0, \quad \ell \notin L\}$$

is of dimension $|L|$.
Note that we still have to check if $Q(\eta_0, \ldots, \eta_{r-1}) = c$.

Bound on the dimension of the singular locus

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

- easy to generalize to any polynomial $f(X)$
- homogeneous part Q_{2d} of Q of degree $2d$ corresponds to $f(X) = X^d$ and $c = 0$

Recall Hooley-Katz:
Let Q be a polynomial over $\mathbb{F}_p$ in r variables of degree $D \geq 1$ such that the dimensions of the singular loci of Q and its homogeneous part Q_D of degree D satisfy

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

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

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

The main result

Theorem

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

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

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.

Thank you for your attention!