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

Arne Winterhof (Austrian Academy of Sciences)

(joint work with Cécile Dartyge and László Mérai)

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. In particular, Drmota, Mauduit and Rivat (2019) and Müllner (2018) showed that Thue-Morse sequence and Rudin-Shapiro sequence along squares are both normal.

A natural question is to study analog problems in finite fields. 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. 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. However, the analog of the latter weaker problem for the Thue-Morse sequence in the finite field setting was settled by Dartyge and Sárközy (2013).

This talk 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 $\mathcal{B} = \{\beta_1, \ldots, \beta_r\}$ be a basis of the finite field $\mathbb{F}_q$ over $\mathbb{F}_p$. Then any $\xi \in \mathbb{F}_q$ has a unique representation

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

The coefficients $x_1, \ldots, x_r$ 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

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

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*

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

where $\beta_{r,c} \geq 0$ *is defined by*

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

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

In particular we have for fixed d,

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

Our main tool is a generalization of Deligne's Theorem for projective surfaces (1974), the Hooley-Katz Theorem (1991).