Iterating Redei Functions over Finite Fields

Daniel Panario
Carleton University, Canada
daniel@math.carleton.ca

The dynamics of iterations of polynomials and rational functions over finite fields have attracted much attention in recent years, in part due to their applications in cryptography and integer factorization methods like Pollard rho algorithm. In this talk we study the action of Redei functions over non-binary finite fields. Redei functions have been applied in several areas including pseudorandom number generators and cryptography. They are defined as $R_n(x,a) = \frac{N(x,a)}{D(x,a)}$ over $\mathbb{D}_q^a = \mathbb{P}^1(\mathbb{F}_q) \setminus \{\pm\sqrt{a}\}$, where $\mathbb{P}^1(\mathbb{F}_q) := \mathbb{F}_q \cup \{\infty\}$, $a \in \mathbb{F}_q$, and $N(x,y), D(x,y)$ are given by $(x+\sqrt{y})^n = N(x,y) + D(x,y)\sqrt{y}$. We completely characterize the functional graph of these actions.

For $x_0 \in \mathbb{F}_q$, we define the orbit of x_0 under f to be the sequence $(x_n)_n$ given by $x_n = f(x_{n-1})$, for $n \geq 1$. It is clear that there exists $c, t \geq 0$ such that $x_{c+t} = x_t$; the least such integers are the cycle length and the tail length of x_0, denoted by $c_q(x_0)$ and $t_q(x_0)$, respectively. We obtain average values for $c_q(x) = c_{n,a,q}(x)$ and $t_q(x) = t_{n,a,q}(x)$ over all $x \in \mathbb{D}_q^a$; we denote these quantities by $C(n,a,q)$ and $T(n,a,q)$. We then obtain analogous results for the number of periodic points, that is, for the number of elements $x \in \mathbb{D}_q^a$ such that $t_{n,a,q}(x) = 0$, denoted by $T_0(n,a,q)$, and for the number of cycles of $R_n(x,a)$ as a map over $\mathbb{P}^1(\mathbb{F}_q)$; this is denoted by $N(n,a,p)$.

If time allows, we give asymptotic estimates as N approaches infinity for the average value of $T_0(n,a,p)$ and $T(n,a,p)$ over all prime numbers $p \leq N$; these quantities are denoted $S_0(n,a,N)$ and $S(n,a,N)$, respectively. These latter results follow closely work by Chou and Shparlinski (2004) for iterations of exponentiations.

Joint work with Claudio Qureshi (Unicamp), and with Rodrigo Martins (UTFPR) and Claudio Qureshi (Unicamp).