1126-12-308 **Daniel Panario*** (daniel@math.carleton.ca). *Iterating Rédei Functions over Finite Fields.*

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. We study the action of Rédei functions over nonbinary finite fields. Rédei 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 studying the cycle length and tail length of its orbits, as well as the number of periodic points, and the number of cycles of $R_n(x,a)$ as a map over $\mathbb{P}^1(\mathbb{F}_q)$.

Based on joint works with Claudio Qureshi (Unicamp) and Rodrigo Martins (UTFPR). (Received January 16, 2017)