The Dynamics of Iterating Functions over Finite Fields

Daniel Panario
Carleton University, Canada

Abstract. When we iterate functions over finite structures, there is an underlying natural functional graph. For a function f over a finite field $\mathbb{F}_q$, this graph has q nodes and a directed edge from vertex a to vertex b if and only if $f(a) = b$. It is well known, combinatorially, that functional graphs are sets of connected components, components are directed cycles of nodes, and each of these nodes is the root of a directed tree from leaves to its root.

The study of iterations of functions over a finite field and their corresponding functional graphs is a growing area of research, in part due to their applications in cryptography and integer factorization methods like Pollard rho algorithm. Periodicity and permutational properties (including the cycle decomposition) of the function can be explained by its functional graph.

Some functions over finite fields when iterated present strong symmetry properties. These symmetries allow mathematical proofs of some dynamical properties such as period and preperiod of a generic element, (average) "rho length" (number of iterations until we cycle back), number of connected components, cycle lengths, etc.

We survey the main problems addressed in this area so far and some of the recent results. We briefly comment on cryptographical applications and heuristics where one treats functions as random mappings, and give results for random mappings. Then we focus on iterations of concrete (that is, not taken at random) functions. We exemplify by completely describing the functional graph of Chebyshev polynomials over a finite field. We use our structural results to obtain estimates for the average rho length, average number of connected components and the expected value for the period and preperiod of iterating Chebyshev polynomials over finite fields.

Based on joint works with Rodrigo Martins (UTFPR, Brazil), Claudio Qureshi (Unicamp, Brazil) and Lucas Reis (UFMG, Brazil).