The graph structure of Chebyshev polynomials over finite fields

Claudio Qureshi

Joint work with Daniel Panario

The iteration of polynomials and rational functions over finite fields have become an active research topic. These dynamical systems have found applications in diverse areas, including cryptography, biology and physics. In cryptography, iterations of functions over finite fields were popularized by the Pollard rho algorithm for integer factorization; its variant for computing discrete logarithms is considered the most efficient method against elliptic curve cryptography based on the discrete logarithm problem. 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. Some functions over finite fields when iterated present strong symmetry properties. These symmetries allow mathematical proofs for some dynamical properties such as period and preperiod of a generic element, (average) "rho length", number of connected components, cycle lengths, etc. We are interested on these kinds of properties for Chebyshev polynomials over finite fields. Previous results for iterations of Chebyshev polynomials over finite fields have been given by Gassert (2014). We describe the functional graph of Chebyshev polynomials of any degree over a finite field of odd characteristic. Then, 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.