"An introduction to iterating functions over finite sets"

By Daniel Panario, Carleton University

Abstract:

Let f be a function defined over a finite set X. For any $x_0 \in X$, consider successive compositions of f with itself:

$$ x_0, f(x_0), f(f(x_0)), f(f(f(x_0))), \ldots.$$

When this is done for every element of X, a natural underlying graph, called the ``functional graph'' of f, emerges. This graph has as vertices the elements of X, and it has an edge from a to b, $a,b \in X$, if $f(a)=b$.

We give examples showing the structure of functional graphs for special functions, such as quadratic polynomials and Chebyshev functions over finite fields. Combinatorially, 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.

Finally, using analytic combinatorics, we briefly comment on the behaviour of random mappings over finite sets and their relation to applications in cryptography.