Rédei permutations with cycles of length 1 and $k$

Juliane Capaverde (Universidade Federal do Rio Grande do Sul), Ariane Masuda* (NYC College of Technology), Virgínia Rodrigues (Universidade Federal do Rio Grande do Sul)

Let $\mathbb{F}_q$ be a finite field of order $q$. The functional graph associated to a mapping $f : \mathbb{F}_q \to \mathbb{F}_q$ is the directed graph on $q$ vertices labelled by the elements of $\mathbb{F}_q$ where there is an edge from a vertex $u$ to a vertex $v$ if and only if $f(u) = v$. For a nonbinary field $\mathbb{F}_q$, $a \in \mathbb{F}_q^*$ and a positive integer $n$, the Rédei function $R_n(x, a)$ can be defined as $R_n(x, a) = \sqrt{a}(x + \sqrt{a})^n + (x - \sqrt{a})^n$. Rédei functions have been used in several applications such as Cryptography and Coding Theory as well as in the generation of pseudorandom numbers and Pell equations. In this talk we will present results on Rédei permutations that decompose in cycles of length 1 and $k$ where $k \geq 2$ is an integer. In particular, we will describe all Rédei functions that are involutions.

Keywords: Rédei functions, involutions, finite fields, functional graphs, graph isomorphism.