Rédei functions that are involutions

Juliane Capaverde

Universidade Federal do Rio Grande do Sul

Abstract

Permutations of finite fields have been extensively studied over the past decades, mainly because of their use in cryptography and coding theory. An involution is a permutation that is its own inverse, and since in most applications both the permutation and its inverse must be implemented, the use of involutions is advantageous, particularly in environments with limited resources. In this talk we focus on a well studied family of permutation polynomials called Rédei functions. We determine when Rédei involutions with a certain number of fixed points exist, and also give explicit formulas for all Rédei involutions in terms of their number of fixed points.

This is joint work with Ariane Masuda (The City University of New York) and Virgínia Rodrigues (Universidade Federal do Rio Grande do Sul).