Explicit Formulas for Monomial Involutions Over Finite Fields

Francis Castro, Carlos Corrada, Natalia Pacheco*, Ivelisse Rubio, University of Puerto Rico, Río Piedras

Permutations of finite fields have important applications in cryptography and coding theory. Involutions are permutations that are its own inverse and are of particular interest because the implementation used for coding can also be used for decoding. We present explicit formulas for all the involutions of $\mathbb{F}_q$ that are given by monomials and for their fixed points.

Keywords: permutations, monomials, involutions, cryptography, Rèdei functions