A New Absolute Irreducibility Criterion for Multivariate Polynomials over Finite Fields: Its Complexity and Applications

Carlos Agrinsoni*, Heeralal Janwa[1], Moises Delgado[2], University of Puerto Rico Rio Piedras, University of Puerto Rico Cayey

One of the key problems in algebraic geometry and its applications in coding theory, cryptography, and other disciplines is to determine whether the variety defined by a set of polynomials is absolutely irreducible, i.e., it remains irreducible in the algebraic closure of the defining field. The famous Eisenstein criterion for irreducibility works only over the defining fields. One important place one needs this is when one wants to apply the Riemann-Roch theorem. Another important application is the Weil conjectures and their applications to find bounds on the number of rational points and exponential sums. In our case, we consider the hypersurfaces defined by a multivariate polynomial. We present a new absolute irreducibility criterion for multivariate polynomials over finite fields. There are only a handful of criteria for absolute irreducibility known so far. We will also give a complexity analysis. Also, we will apply our algorithm to show absolute irreducibly of a large class of polynomials. Particular applications will be to a class of Trinomials.

Keywords: multivariate polynomial, factorization, absolutely irreducible polynomials, hypersurfaces, finite fields, algebraic geometric codes.