On the Conjecture on APN Functions and Absolute Irreducibility of Polynomials

Heeralal Janwa*

September 21, 2015

Abstract

An almost perfect nonlinear (APN) function (necessarily a polynomial function) on a finite field $\mathbb{F}$ is called exceptional APN, if it is also APN on infinitely many extensions of $\mathbb{F}$. In this article we consider the most studied case of $\mathbb{F} = \mathbb{F}_{2^n}$. A conjecture of Janwa-Wilson and McGuire-Janwa-Wilson (1993/1996), settled in 2011, was that the only monomial exceptional APN functions are the monomials x^n, where $n = 2^k + 1$ or $n = 2^{2k} - 2^k + 1$ (the Gold or the Kasami exponents, respectively). Aubry, McGuire and Rodier conjectured that the only exceptional APN function is one of the monomials just described. One of our results is that all functions of the form $f(x) = x^{2^k+1} + h(x)$ (for any odd degree $h(x) \neq 2^l + 1$) with $(k, l) = 1$), are not exceptional APN, extending substantially several recent results towards the resolution of the stated conjecture. One ingredient in deriving this result is the proof we present of our earlier conjecture on the relatively primeness of exceptional multivariate polynomials in the Gold case.

Up until now, the main tool used by most researchers in the study of exceptional APN functions, has been the method of Janwa, McGuire and Wilson [13] to prove the absolute irreducibility of multivariate polynomials. The algorithmic approach in [13] is based on intersection multiplicity theory and Bezout's theorem, and computations initiated in Janwa and Wilson [15]. Our techniques of establishing absolute irreducibility rely on repeated hyperplane intersections, linear transformations, reductions, and the known APN monomial functions. We apply the estimates of Weil, Bombieri, Deligne, Lang-Weil, Ghorpade-Lachaud on rational points on varieties over finite fields to demonstrate exceptional properties. The absolute irreducible hypersurfaces are related to hyper-plane sections of Fermat varieties, and are of independent interest. We will discuss applications of our results in the construction of algebraic geometric codes, cryptography, combinatorics, finite geometry, sequence design, and Ramanujan graphs.

*Department of Mathematics, University of Puerto Rico (UPR), Rio Piedras, Box 70377 San Juan, San Juan PR 00936-8377. Joint work with Moises Delgado.