Absolute Irreducibility of Generalized Trinomials Defined by APN Functions of The Form $f(x) = x^i + h(x)$ over $\mathbb{F}_2^s$.

Alec Zabel-Mena[1*], Heeralal Janwa[1], Carlos Agrinsoni[2], University of Puerto Rico Río Piedras, Purdue University.

A multivariate polynomial is said to be absolutely irreducible over a field $\mathbb{F}$ provided it is irreducible over the algebraic closure of $\mathbb{F}$. In algebraic geometry, coding theory, and cryptography, the absolute irreducibility of certain algebraic curves defined by multivariate polynomials is important for determining and solving various problems such as: counting rational points using the Weil conjectures, determining error-correction capabilities, and determininig suitability for use in cryptographic systems. One can define such curves using almost perfect non-linear (APN) functions, which are a class of Boolean functions important in coding-theory and cryptography, and find their use as S-boxes in cryptographic systems.
There exist many methods for determining the absolute irreducibility of an algebraic curve over a field. One such method is testing for irreducibility for sufficiently many extensions of the base field, which is costly to implement algorithmically. One method however does not depend on testing irreducibility in multiple field extensions. All that is required is that the multivariate polynomial has square-free leading term, and that the terms be coprime. In some cases, we can omit the gcd criteria between terms by using CCZ-equivalence between APN functions.
We are interested in when certain algebraic curves defined using APN functions are absolutely irreducible over the finite field $\mathbb{F}_q$, where $q = 2^s$. We look at the curve defined by:

$$\phi_f(X, Y, Z) = \frac{f(X) + f(Y) + f(Z) + f(X + Y + Z)}{(X + Y)(Y + Z)(X + Z)}$$

as a generalized trinomial of given degree-gap, where $f(x) = x^i + h(x)$ is a trinomial APN function. We test the absolute irreducibility of $\phi_f(X, Y, Z)$ over $\mathbb{F}_q$ on the basis of the square-free criteria, the gcd criteria, and the degree-gap of $\phi_f(X, Y, Z)$. We test the absolute irreducibility of $\phi_f(X, Y, Z)$ for various $f(x) = x^i + h(x)$. For those i in which $\phi_f(X, Y, Z)$ cannot be tested on the present criteria directly, we present alternate methods for testing absolute irreducibility. In particular when $i = 24$, it is sufficient to check for irreducibility in $\mathbb{F}_{q^7}$.

Keywords: Algebraic Curve, APN Functions, Absolute Irreducibility, Generalized Trinomial, Coding-Theory, Algebraic Geometry