A Conjecture on Permutation Trinomials

Daniele Bartoli
Department of Mathematics and Computer Science
University of Perugia
Perugia, Italy
daniele.bartoli@unipg.it

Mohit Pal
Department of Informatics
University of Bergen
Bergen, Norway
mohit.pal@uib.no

Pantelimon Stănică
Applied Mathematics Department
Naval Postgraduate School
Monterey, CA 93943, USA
pstanica@nps.edu

Abstract

In this note we use a connection with algebraic curves to show the validity of a conjecture of [A. Rai, R. Gupta, *Further results on a class of permutation trinomials*, Cryptogr. Commun. (2023)], if the dimension of the underlying field is greater than 8.

Keywords: Finite fields, permutations, trinomial, algebraic curves

1 Introduction

Let $\mathbb{F}_q$ be the finite field with $q = p^k$ elements, where p is a prime number and k is a positive integer. We denote by $\mathbb{F}_q^*$ the multiplicative group of nonzero elements of $\mathbb{F}_q$ and by $\mathbb{F}_q[X]$ the ring of polynomials in indeterminate X over finite field $\mathbb{F}_q$. Let f be a function from the finite field $\mathbb{F}_q$ to itself. It is well-known, due to Lagrange's interpolation formula, that f can be uniquely expressed as a polynomial $f \in \mathbb{F}_q[X]/(X^q - X)$. A polynomial $f \in \mathbb{F}_q[X]$ is called a permutation polynomial (PP) if the induced mapping $c \mapsto f(c)$ permutes the elements of $\mathbb{F}_q$. The general study of permutation polynomials started with Hermite [5] who considered the case of prime fields whereas permutation polynomials of arbitrary finite fields were first studied by Dickson [3]. The simplest kind of permutation polynomials are monomials. A monomial X^n permutes $\mathbb{F}_q$ if and only if $\gcd(n, q-1) = 1$. However, the classification of binomials and trinomials is more difficult. For a brief survey of permutation binomials and trinomials, we refer to [7] and the references therein.

Recently, Rai and Gupta [9] studied permutation trinomials over finite fields of odd characteristic and proposed the following conjecture.

Conjecture 1. Let $q = p^k$, where $p > 7$ is a prime. Then, for $\alpha \in \mathbb{F}_q^*$ and $k > 1$, the trinomial

$$f(X) = X^{q(p-1)+1} + \alpha X^{pq} + X^{q+p-1}$$

is a permutation polynomial over $\mathbb{F}_{q^2}$ if and only if $\alpha = -1$ and $k = 2$.

In this note we shall use algebraic curves methods to show that the above conjecture is true for $k \geq 4$. The note is organised as follows. In Section 2, we recall some definitions and results that will be used in the subsequent sections. In Section 3, we shall give the sketch of the proof of the conjecture for $k \geq 4$.

2 Preliminaries on algebraic curves

In this section, we shall first recall some basic facts on curves/surfaces over (finite) fields. For more details, we refer to [4, 6], or the reader's favorite algebraic geometry book. As customary, for a field $\mathbb{F}$, we denote by $\overline{\mathbb{F}}$ its algebraic closure. We denote, by $\mathbb{P}^m(\mathbb{F})$ (respectively, $\mathbb{A}^m(\mathbb{F})$) the m-dimensional projective (respectively, affine) space over the field $\mathbb{F}$. Solutions of polynomial equations (systems) form what we call algebraic hypersurfaces (varieties). An algebraic hypersurface defined over a field $\mathbb{F}$ is called absolutely irreducible if the associated polynomial is irreducible over every algebraic extension of $\mathbb{F}$. An absolutely irreducible $\mathbb{F}$-rational component of a hypersurface defined by a polynomial f is an absolutely irreducible hypersurface, associated to a factor of f defined over $\mathbb{F}$. In two dimensions, $\mathcal{C}$ is an affine curve over a field $\mathbb{F}$ if it is the zero set of a polynomial $f(X, Y) \in \mathbb{F}[X, Y]$. The polynomial f is the defining polynomial of $\mathcal{C}$.

Given a curve $\mathcal{C} : f(X, Y) = 0$, with $f(X, Y) \in \mathbb{F}[X, Y]$, the set of $\mathbb{F}$-rational points of $\mathcal{C}$ in $\mathbb{A}^2(\mathbb{F})$ is the the set of points $(x_0, y_0) \in \mathbb{A}^2(\mathbb{F})$ such that $f(x_0, y_0) = 0$. This definitions extends to curves defined in $\mathbb{P}^2(\mathbb{F})$.

Given two affine plane curves $\mathcal{C}$ and $\mathcal{C}'$, a *rational map* $\phi : \mathcal{C} \to \mathcal{C}'$ is defined by

$$(x, y) \mapsto \left(\frac{f(x, y)}{h(x, y)}, \frac{g(x, y)}{h(x, y)} \right),$$

for some $f, g, h \in \mathbb{F}[X, Y]$, $\mathbb{F}$ any field, satisfying that h does not vanish on $\mathcal{C}$. We say that $\mathcal{C}$ and $\mathcal{C}'$ are *birationally equivalent* if there are rational maps $\phi_1 : \mathcal{C} \to \mathcal{C}'$ and $\phi_2 : \mathcal{C}' \to \mathcal{C}$ such that $\phi_1 \circ \phi_2$ and $\phi_2 \circ \phi_1$ are the identity maps on $\mathcal{C}'$ and $\mathcal{C}$. A birational equivalence does not preserve the set of $\mathbb{F}'$-rational points, if $\mathbb{F}' \subsetneq \mathbb{F}$, nor the degree of the curves, but preserves the absolute irreducibility and the number of absolutely irreducible components.

We now recall Bézout's Theorem [6, Theorem 3.13], which will be used in the proof of the conjecture.

Theorem 2 (Bézout's Theorem)**.** *Let $\mathcal{C}_1, \mathcal{C}_2$ be two projective plane curves of degrees d_1, respectively, d_2. If $\mathcal{C}_1$ and $\mathcal{C}_2$ do not have a common component, then the sum of*

multiplicities of their common points (on the algebraic closure of $\mathbb{F}$) is

$$\sum_{P \in \mathcal{C}_1 \cap \mathcal{C}_2} m\left(P, \mathcal{C}_1 \cap \mathcal{C}_2\right) = d_1 d_2.$$

A crucial point in our arguments will be the celebrated Hasse-Weil theorem. Here, we propose a slightly modified version that is more suitable for our purposes.

Theorem 3 (Aubry-Perret bound)**.** [2, Corollary 2.5] *Let $\mathcal{C} \subset \mathbb{P}^2(\mathbb{F}_q)$ be an absolutely irreducible curve of degree d. Then its number of $\mathbb{F}_q$-rational points $\mathcal{C}(\mathbb{F}_q)$ satisfies*

$$q + 1 - (d-1)(d-2)\sqrt{q} \leq \#\mathcal{C}(\mathbb{F}_q) \leq q + 1 + (d-1)(d-2)\sqrt{q}. \tag{1}$$

3 The sketch of the proof of the conjecture

We only briefly treat here the sufficiency for $k \geq 4$. Consider the polynomial

$$f(X) = X^{(p-1)q+1} + \alpha X^{pq} + X^{q+p-1} \in \mathbb{F}_{q^2}[X],$$

where $\alpha \in \mathbb{F}_q^*$ and $q = p^k$, $k > 1$ and p is an odd prime. It is well known [8, 10, 1] that $f(X) = X^{q+p-1}(X^{(q-1)(p-2)} + \alpha X^{(q-1)(p-1)} + 1)$ permutes $\mathbb{F}_{q^2}$ if and only if $\gcd(q + p - 1, q^2 - 1) = 1$ and

$$g_\alpha(X) = X^{q+p-1}(X^{p-2} + \alpha X^{p-1} + 1)^{q-1}$$

permutes $\mu_{q+1} := \{a \in \mathbb{F}_{q^2} \mid a^{q+1} = 1\}$. We can restrict our investigation to those α such that $\alpha + 2 \neq 0$, otherwise $g_\alpha(1) = 0$, and so, it cannot be a permutation on μ_{q+1}. Notice that for any $x \in \mu_{q+1}$,

$$\begin{aligned} g_\alpha(x) &= x^{p-2}\frac{(x^{p-2} + \alpha x^{p-1} + 1)^q}{x^{p-2} + \alpha x^{p-1} + 1} \\ &= x^{p-2}\frac{(1/x)^{p-2} + \alpha (1/x)^{p-1} + 1}{x^{p-2} + \alpha x^{p-1} + 1} \\ &= \frac{x + \alpha + x^{p-1}}{x^{p-1} + \alpha x^p + x}. \end{aligned}$$

We shall need below the well known fact that

$$\mu_{q+1} \setminus \{1\} = \left\{ \frac{t+i}{t-i} \mid t \in \mathbb{F}_q, i^q = -i \right\}.$$

Consider

$$\begin{aligned} F_\alpha(X,Y) &:= (X + \alpha + X^{p-1})(Y^{p-1} + \alpha Y^p + Y) - (Y + \alpha + Y^{p-1})(X^{p-1} + \alpha X^p + X) \\ &= \alpha(X^{p-1}Y^p - X^p Y^{p-1} + XY^p - X^p Y + \alpha(Y-X)^p + Y^{p-1} - X^{p-1} + Y - X). \end{aligned}$$

It is readily seen that g_α permutes μ_{q+1} if and only if there exist no pairs $(x, y) \in \mu_{q+1}^2$, $x \neq y$, such that $F_\alpha(x, y) = 0$. The polynomial $F_\alpha^{(1)}(X, Y) := F_\alpha(X, Y)/(X - Y)$ defines

a curve $\mathcal{C}_\alpha$ in $\mathbb{A}^2(\mathbb{F}_{q^2})$ that is $\mathbb{F}_{q^2}$-birationally equivalent to the curve $\mathcal{D}_\alpha \subset \mathbb{A}^2(\mathbb{F}_q)$ defined by

$$G_\alpha(X,Y) := \frac{(X-i)(Y-i)}{2i(Y-X)} F_\alpha\left(\frac{X+i}{X-i}, \frac{Y+i}{Y-i}\right).$$

The above equation is obtained considering the birationality

$$(X,Y) \mapsto \left(\frac{X+i}{X-i}, \frac{Y+i}{Y-i}\right)$$

applied to the curve $F_\alpha(X,Y) = 0$ and then removing from it the image of component $(X-Y) = 0$ (this is not a component of $\mathcal{C}_\alpha$). Such a birationality does not preserve the $\mathbb{F}_q$-rationality of points nor of components of the two curves in general, but sends $(x,y) \in \mu_{q+1}^2$ in $\mathcal{C}_\alpha$ into $(\overline{x},\overline{y}) \in \mathbb{F}_q^2$ in $\mathcal{D}_\alpha$ and viceversa and preserves the number of components of the two curves. Thus, the curve $\mathcal{D}_\alpha$ is absolutely irreducible if and only if so is $\mathcal{C}_\alpha$. In the full paper, we show that the curve $\mathcal{C}_\alpha$ is absolutely irreducible (we are skipping the proof here due to page limit, but it will be part of the full paper).

Theorem 4. *Let $\alpha \in \mathbb{F}_q^*$ and $q = p^k$, $k \geq 4$, $p > 7$ prime. Then the trinomial*

$$f(X) = X^{q(p-1)+1} + \alpha X^{pq} + X^{q+p-1}$$

is not a permutation polynomial over $\mathbb{F}_{q^2}$.

Proof. As already observed if $\alpha = -2$ then $g_\alpha(1) = 0$ and thus g_α does not permute μ_{q+1}.

Suppose now $\alpha \neq -2$. To demonstrate the absolute irreducibility of the curve $\mathcal{C}_\alpha$, we can analyze the set of singular points and the multiplicity of the intersection of two putative components of $\mathcal{C}_\alpha$ at these points. A contradiction is then obtained using Bézout's Theorem. Since $\mathcal{C}_\alpha$ is absolutely irreducible and so is $\mathcal{D}_\alpha$. Since $\mathcal{D}_\alpha$ is defined over $\mathbb{F}_q$ and of degree $p-1$, Hasse-Weil bound (see Equation (1)) tells us that it possesses at least

$$p^k + 1 - (p-2)(p-3)p^{k/2}$$

$\mathbb{F}_q$-rational points in $\mathbb{P}^2(\mathbb{F}_q)$ and at most $2(p-1)$ of them belong to the line at infinity or to $X - Y = 0$. Since $k \geq 4$,

$$p^k + 1 - (p-2)(p-3)p^{k/2} - 2(p-1) > 0.$$

Thus there exists a pair $(\overline{x},\overline{y}) \in \mathbb{F}_q^2$, $\overline{x} \neq \overline{y}$, such that $g_\alpha((\overline{x}+i)/(\overline{x}-i) = g_\alpha((\overline{y}+i)/(\overline{y}-i))$ and therefore g_α does not permute μ_{q+1}. This shows that $f(X)$ is not a permutation over $\mathbb{F}_{q^2}$. □

Acknowledgements

This paper was being written during an enjoyable visit of the third-named author P.S. to the University of Perugia. He thanks the host D.B. for the invitation and the excellent working conditions.

References

[1] A. Akbary, D. Ghioca, Q. Wang, *On constructing permutations of finite fields*, Finite Fields Appl. **17**(1), 51–67 (2011).

[2] Y. Aubry, M. Perret, *A Weil theorem for singular curves*, in: Arithmetic, geometry and coding theory (eds. R. Pellikaan, M. Perret, S. G. Vladut), De Gruyter Proceedings in Mathematics, de Gruyter, Berlin, 1–7 (1996).

[3] L.E. Dickson, *The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group*, Ann. Math. **11**, 65–120 (1896).

[4] R. Hartshorne, Algebraic geometry, Graduate Texts in Mathematics, no. 52, Springer–Verlag, New York-Heidelberg, 1977.

[5] C. Hermite, *Sur les fonctions de sept lettres*, C.R. Acad. Sci. Paris **57** (1863), 750–757.

[6] J.W.P. Hirschfeld, G. Korchmáros, F. Torres, Algebraic curves over a finite field, Princeton University Press, 2013.

[7] X. Hou, *A survey of permutation binomials and trinomials over finite fields,* in: Proceedings of the 11th International Conference on Finite Fields and Their Applications, Contemp. Math., Magdeburg, Germany, July 2013, 632 AMS 177–191 (2015).

[8] Y.H. Park, J.B. Lee, *Permutation polynomials and group permutation polynomials*, Bull. Austral. Math. Soc. **63**(1), 67–74 (2001).

[9] A. Rai, R. Gupta, *Further results on a class of permutation trinomials*, Cryptogr. Commun. **15**, 811–820 (2023).

[10] M.E. Zieve, *On some permutation polynomials over* $\mathbb{F}_q$ *of the form* $x^r h(x^{(q-1)/d})$, Proc. Amer. Math. Soc. **137**(7), 2209–2216 (2009).