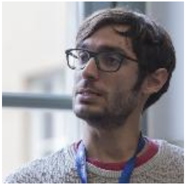
Boolean Functions and Applications (BFA) 2024, Dubrovnik, Croatia

A conjecture on permutation trinomials

Pante Stănică

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

My co-authors:



Daniele Bartoli

Mohit Pal

Work started while visiting Daniele at University of Perugia in Spring of 2024

Environment and field's flowers

- Let $q = 2^m$, $m \in \mathbb{N}$, and denote by $\mathbb{F}_q$ the finite field with q elements; $\mathbb{F}_q[X_1, \ldots, X_n]$, the ring of polynomials in n indeterminates over finite field $\mathbb{F}_q$;
- Vectorial Boolean functions $F : \mathbb{F}_q^n \to \mathbb{F}_q^n$ are fundamental building blocks in symmetric cryptography: many block ciphers employ them as components in their S-boxes.
- To counter known cipher attacks, these vectorial Boolean functions have to satisfy many criteria such as nonlinearity, avalanche features, differential uniformity, etc.
- Most such F's have to be permutations when used in applications!

Our problem

Recently, Rai and Gupta (CCDS 2023) studied permutation trinomials over finite fields of odd characteristic and proposed a conjecture.

Conjecture

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 $k = 2$.

It is the intent of our paper to prove this conjecture.

Tools from algebraic geometry I

- Field $\mathbb{F}$, $\overline{\mathbb{F}}$ be its algebraic closure, and $\mathbb{P}^m(\mathbb{F})$ (respectively, $\mathbb{A}^m(\mathbb{F})$) the m-dimensional projective (respectively, affine) space over the field $\mathbb{F}$.
- *Variety*: solutions of a system of eqs over $\mathbb{F}_q$.
- An algebraic hypersurface (def by a single eq) over a field $\mathbb{F}$ is *absolutely irreducible* if the associated polynomial is irreducible over the algebraic closure of $\mathbb{F}$.
- $\mathcal{V}$ is a variety of $\deg(\mathcal{V}) = d$ if $d = \#(\mathcal{V} \cap H)$, where $H \subseteq \mathbb{A}^r(\overline{\mathbb{F}_q})$ is a general projective subspace of dimension $r - s$; an upper bound to $\deg(\mathcal{V})$ is given by $\prod_{i=1}^{s} \deg(F_i)$; to find it precisely, not an easy matter.
- The Frobenius map $\Phi_q : x \mapsto x^q$ is an automorphism of $\mathbb{F}_{q^k}$ and generates the group $Gal(\mathbb{F}_{q^k}/\mathbb{F}_q)$ of automorphisms of $\mathbb{F}_{q^k}$ that fixes $\mathbb{F}_q$, pointwise.

General Idea and Tools I

- A crucial point in our investigation: prove the existence of suitable $\mathbb{F}_q$-rational points in algebraic surfaces $\mathcal{V}$ attached to each permutation trinomial, by showing the existence of absolutely irreducible $\mathbb{F}_q$-rational components in $\mathcal{V}$ and lower bounding the number of their $\mathbb{F}_q$-rational points.
- We need some generalizations of Lang-Weil type bounds

Theorem (Cafure–Matera, 2006)

Let $\mathcal{V} \subseteq \mathbb{A}^n(\mathbb{F}_q)$ be an absolutely irreducible variety over $\mathbb{F}_q$ of dimension $r > 0$ and degree δ. If $q > 2(r+1)\delta^2$, then

$$\left|\#(\mathcal{V}(\mathbb{A}^n(\mathbb{F}_q))) - q^r\right| \leq (\delta - 1)(\delta - 2)q^{r-1/2} + 5\delta^{13/3}q^{r-1}.$$

General Idea and Tools II

Lemma (Aubry – McGuire – Rodier, 2010)

Let $\mathcal{H}$ be a projective hypersurface and $\mathcal{X}$ a projective variety in $\mathbb{P}^n(\mathbb{F}_q)$. If $\mathcal{X} \cap \mathcal{H}$ has a non-repeated absolutely irreducible component defined over $\mathbb{F}_q$ then $\mathcal{X}$ has a non-repeated absolutely irreducible component defined over $\mathbb{F}_q$.

Theorem (Bézout 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 is

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

Our approach for $k \geq 4$ I

- Consider again the polynomial

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

which permutes $\mathbb{F}_{q^2}$ (note $GCD(q+p-1, q^2-1) = 1$) iff

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

permutes $\mu_{q+1} = \{a \in \mathbb{F}_{q^2} \ : \ a^{q+1} = 1\}$ (see Park & Lee 2001, Zieve 2009, Akbary, Ghioca & Wang 2011).
- WLOG $\alpha + 2 \neq 0$, otherwise $g_\alpha(1) = 0$, so, g_α is not PP.
- For $x \in \mu_{q+1}$, $g_\alpha(x) = \ldots = \frac{x+\alpha+x^{p-1}}{x^{p-1}+\alpha x^p + x}$.
- Known: $\mu_{q+1} \setminus \{1\} = \left\{\frac{t+i}{t-i} : t \in \mathbb{F}_q, i^q = -i\right\}$.

Our approach for $k \geq 4$ II

- Note that g_α permutes μ_{q+1} if $\nexists (x, y) \in \mu_{q+1}^2$, $x \neq y$, s.t. $F_\alpha(x, y) = 0$, where $F_\alpha(X, Y)$ is given by

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

- $F_\alpha^{(1)}(X, Y) := F_\alpha(X, Y)/(X - Y)$ defines an affine curve $\mathcal{C}_\alpha$, $\mathbb{F}_{q^2}$-birationally equiv. to the affine curve $\mathcal{D}_\alpha$ defined by

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

- This 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 $\#$ of components of the two curves.

Our approach for $k \geq 4$ III

- Thus, the curve $\mathcal{D}_\alpha$ is absolutely irreducible iff $\mathcal{C}_\alpha$ is a.i.
- We aim to show that the curve $\mathcal{C}_\alpha$ is absolutely irreducible.
- By way of contradiction, let

$$\mathcal{C}_\alpha^{(1)} : X^{r_1} Y^{r_2} + \cdots = 0,$$
$$\mathcal{C}_\alpha^{(2)} : X^{p-1-r_1} Y^{p-1-r_2} + \cdots = 0$$

  be two (not necessarily irreducible) components.
- They intersect, by Bézout Theorem, in precisely

$$(r_1 + r_2)(p - 1 - r_1 + p - 1 - r_2)$$

  points counted with multiplicity. Also $\mathcal{C}_\alpha^{(1)}$ and $\mathcal{C}_\alpha^{(2)}$ must intersect at singular points of $\mathcal{C}_\alpha$.

Our approach for $k \geq 4$ IV

- Some work required to show that the only singular points of $\mathcal{C}_\alpha$ are $(1:0:0)$, $(0:1:0)$, and $(1:1:1)$ together with at most other four affine ordinary double points; also, the multiplicity of intersection of $\mathcal{C}_\alpha^{(1)}$ and $\mathcal{C}_\alpha^{(2)}$ at these points is

$$r_1(p-1-r_1)+r_2(p-1-r_2).$$

- We also show that $\mathcal{C}_\alpha^{(1)}$ and $\mathcal{C}_\alpha^{(2)}$ intersect at $(1:1:1)$, so the smallest homogeneous part in the polynomials defining these two curves must be proportional to $(Y-X)^{\frac{p-1}{2}}$. So, $r_1+r_2>\frac{p-1}{2}$ and $p-1-r_1+p-1-r_2>\frac{p-1}{2}$.

Our approach for $k \geq 4$ V

- Rearranging components, we can assume that either $r_1 = r_2$ or $r_1 = p - 1 - r_2$; In both these cases the sum of the intersection multiplicities of $\mathcal{C}_\alpha^{(1)}$ and $\mathcal{C}_\alpha^{(2)}$ is at most

$$r_1(p-1-r_1) + r_1(p-1-r_1) + \frac{p^2-1}{4} + 4.$$

- Since $\frac{p-1}{4} < r_1 < \frac{3(p-1)}{4}$ and $p \geq 11$, $\frac{p^2-1}{4} + 4 < 2r_1(p-1-r_1) < \frac{(p-1)^2}{2}$ holds.
- If $r_1 = r_2$,

$$\begin{aligned} & r_1(p-1-r_1) + r_1(p-1-r_1) + \frac{p^2-1}{4} + 4 \\ & < 2r_1(p-1-r_1) + 2r_1(p-1-r_1) \\ & < 4r_1(p-1-r_1) = \deg(\mathcal{C}_\alpha^{(1)})\deg(\mathcal{C}_\alpha^{(2)}). \end{aligned}$$

Our approach for $k \geq 4$ VI

- If $r_1 = p - 1 - r_2$,

$$
\begin{aligned}
& r_1(p-1-r_1) + r_1(p-1-r_1) + \frac{p^2-1}{4} + 4 \\
& < \frac{(p-1)^2}{2} + \frac{p^2-1}{4} + 4 \\
& < (p-1)^2 = \deg(\mathcal{C}_\alpha^{(1)}) \deg(\mathcal{C}_\alpha^{(2)}).
\end{aligned}
$$

Both these cases contradict Bézout Theorem.

Our approach for $k \geq 4$ VII

Theorem

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 (sketch)

- If $\alpha = -2$ then $g_\alpha(1) = 0$ and thus g_α is not PP;
- Let $\alpha \neq -2$. The curve $\mathcal{C}_\alpha$ is absolutely irreducible and so is $\mathcal{D}_\alpha$.

Our approach for $k \geq 4$ VIII

- Since $\deg(\mathcal{D}_\alpha) = p - 1$, Hasse-Weil bound implies that it has 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, $\exists\, \overline{x} \neq \overline{y} \in \mathbb{F}_q$, s.t. $g_\alpha((\overline{x}+i)/(\overline{x}-i) = g_\alpha((\overline{y}+i)/(\overline{y}-i))$, so, g_α does not permute μ_{q+1}.
- This shows that $f(X)$ is not a permutation over $\mathbb{F}_{q^2}$. $\square$

The case of $k = 3$ I

Go2Tks

- Cases $k = 2, 3$ require different methods.
- Write $f(X) = \alpha X^{pq} + \mathrm{Tr}(X^{q+p-1}) = (\alpha X^p + \mathrm{Tr}(X^{q+p-1}))^q$, where Tr is the relative trace map from $\mathbb{F}_{q^2}$ to $\mathbb{F}_q$ given by $\mathrm{Tr}(X) = X^q + X$.
- Note that f is a PP iff $\alpha X^p + \mathrm{Tr}(X^{q+p-1})$ is PP, so we assume that $f(X) = \alpha X^p + \mathrm{Tr}(X^{q+p-1}),\ \alpha \in \mathbb{F}_q^*$.
- For $k = 3$, we now consider the equation

$$\alpha X^p + \mathrm{Tr}(X^{p^3+p-1}) = \alpha X^p + X^{p^3+p-1} + X^{p^4-p^3+1} = g. \quad (1)$$

The case of $k = 3$ II

- Raising to the p^3 power (note that $\alpha^{p^3} = \alpha, X^{p^6} = X$), we get $\alpha X^{p^4} + X^{p^3+p-1} + X^{p^4-p^3+1} = g^{p^3}$, which combined with (1), renders

$$\alpha(X^{p^4} - X^p) + g - g^{p^3} = 0.$$

We use the transformation $g \mapsto h^p, \alpha \mapsto \beta^p$, obtaining

$$X^{p^3} - X - B = 0, \quad \text{where } B = \frac{h^{p^3} - h}{\beta},$$

which either has no roots or it has p^3 roots, of the form $X = -B/2 + \lambda$, with $\lambda \in \mathbb{F}_{p^3}$.

The case of $k = 3$ III

- We plug this into (1) using $B^{p^3} = -B$, $\lambda^{p^3} = \lambda$, $\gamma = \frac{\lambda}{B}$, $t := \left(\frac{h^{p^3} + h}{h^{p^3} - h}\right)^p$, $\mu = \frac{1}{\alpha + 2}$, with some effort we get

$$\gamma^{p+2} - \frac{1-4\mu}{4}\gamma^p - \frac{(1-2\mu)t}{4}\gamma^2 - \mu\gamma + (1-2\mu)t = 0. \quad (2)$$

- Goal: Need $h \notin \mathbb{F}_{p^3}$ s.t. (2) has 0 or ≥ 2 sols.
- First, we showed that $\forall \alpha$, $\exists h$ with $T^p = -T$.
- We next show that the following equation has no solution

$$\gamma^{p+2} - \frac{1-4\mu}{4}\gamma^p - \frac{T}{4}\gamma^2 - \mu\gamma + T = 0. \qquad (3)$$

- Note that $\mathbb{F}_{p^6} = \langle \mu, T \rangle_{\mathbb{F}_p}$, since $\mu \in \mathbb{F}_{p^3}$, $T \in \mathbb{F}_{p^2}$;

The case of $k = 3$ IV

- If γ exists, then $\gamma = a\mu + bT$, $a, b \in \mathbb{F}_p$ with $ab \neq 0$, since $\gamma \notin \mathbb{F}_{p^3}$; plug it into (3) (use $T^2 =: \omega \in \mathbb{F}_p$ and $T^3 \in T \cdot \mathbb{F}_p$). A bit more algebraic number theory work is required to show that the obtained eq. has no solution.

Thank you for your attention!

[Pante Stanica: http://faculty.nps.edu/pstanica]

- A. Akbary, D. Ghioca, Q. Wang, *On constructing permutations of finite fields*, Finite Fields Appl. **17**(1), 51–67 (2011).
- R. Hartshorne, Algebraic geometry, Graduate Texts in Mathematics, no. 52, Springer–Verlag, New York-Heidelberg, 1977.
- J.W.P. Hirschfeld, G. Korchmáros, F. Torres, Algebraic curves over a finite field, Princeton University Press, 2013.
- Y.H. Park, J.B. Lee, *Permutation polynomials and group permutation polynomials*, Bull. Austral. Math. Soc. **63**(1), 67–74 (2001).
- A. Rai, R. Gupta, *Further results on a class of permutation trinomials*, Cryptogr. Commun. **15**, 811–820 (2023).
- Y. Zheng, Q. Wang, W. Wei, *On Inverses of Permutation Polynomials of Small Degree Over Finite Fields*, IEEE Trans. Inf. Theory 66:2 (2020), 914–922.
- 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).