Recent Developments on Permutation Trinomials

Xiang-dong Hou

Department of Mathematics and Statistics
University of South Florida

The Third Workshop on Boolean Functions and Their Applications
Loen, Norway, June 20, 2018

outline

- Introduction
- Recent results in characteristic 2
- A new proof
- Outline of the new proof

- Introduction
- Recent results in characteristic 2
- A new proof
- Outline of the new proof

permutation trinomails

Let $\mathbb{F}_q$ denote the finite field with q elements. A polynomial $f \in \mathbb{F}_q[X]$ is called a *permutation polynomial* (PP) of $\mathbb{F}_q$ if it induces a permutation of $\mathbb{F}_q$.

Permutation monomials are easy to describe: X^n is a PP of $\mathbb{F}_q$ if and only if $\gcd(n, q-1) = 1$.

permutation trinomails

Let $\mathbb{F}_q$ denote the finite field with q elements. A polynomial $f \in \mathbb{F}_q[X]$ is called a *permutation polynomial* (PP) of $\mathbb{F}_q$ if it induces a permutation of $\mathbb{F}_q$.

Permutation monomials are easy to describe: X^n is a PP of $\mathbb{F}_q$ if and only if $\gcd(n, q-1) = 1$.

What about permutation binomials and trinomials?

Let $\mathbb{F}_q$ denote the finite field with q elements. A polynomial $f \in \mathbb{F}_q[X]$ is called a *permutation polynomial* (PP) of $\mathbb{F}_q$ if it induces a permutation of $\mathbb{F}_q$.

Permutation monomials are easy to describe: X^n is a PP of $\mathbb{F}_q$ if and only if $\gcd(n, q-1) = 1$.

What about permutation binomials and trinomials?

Difficult. Perhaps a general description is impossible.

we are interested in ...

People are interested in PPs of the form

$$f(X) = X + aX^{s_1(q-1)+1} + bX^{s_2(q-1)+1} \in \mathbb{F}_{q^2}[X], \tag{1}$$

where $1 \le s_1, s_2 \le q$ and $s_1 \ne s_2$.

we are interested in ...

People are interested in PPs of the form

$$f(X) = X + aX^{s_1(q-1)+1} + bX^{s_2(q-1)+1} \in \mathbb{F}_{q^2}[X], \tag{1}$$

where $1 \le s_1, s_2 \le q$ and $s_1 \ne s_2$.

Why? A number of reasons:

- Simplicity: It appears that PPs of the form (1) can be characterized by concise conditions on the parameters.
- Challenge: Proofs are usually difficult and require sophisticated tools and heavy computations.
- Mystery: Seemingly out-of-control expressions suddenly factor nicely. Sufficient conditions turn out to be necessary, and vice versa.
- There is something special about $\mathbb{F}_{q^2}$: The subgroup μ_{q+1} of order $q+1$ of $\mathbb{F}_{p^2}^*$ is bijectively mapped to the projective line $\mathbb{F}_q \cup \{\infty\}$ by a degree one rational function.

no assumptions on a and b

There are many interesting results on PPs of the form

$$f(X) = X + aX^{s_1(q-1)+1} + bX^{s_2(q-1)+1} \in \mathbb{F}_{q^2}[X]$$

with additional assumptions on a and b.

In this talk, we make no assumptions on a and b. With given s_1 and s_2, the goal is to determine the conditions on a, b and q that are necessary and sufficient for f to be a PP of $\mathbb{F}_{q^2}$.

the case $(s_1, s_2) = (1, 2)$, q odd

Theorem (H 2014)

Let $f = aX + bX^q + X^{2q-1} \in \mathbb{F}_{q^2}[X]$, where q is odd. Then f is a PP of $\mathbb{F}_{q^2}$ if and only if one of the following is satisfied.

(i) $a = b = 0$, $q \equiv 1, 3 \pmod 6$.

(ii) $(-a)^{\frac{q+1}{2}} = -1$ *or* 3, $b = 0$.

(iii) $ab \neq 0$, $a = b^{1-q}$, $1 - \frac{4a}{b^2}$ *is a square of* $\mathbb{F}_q^*$.

(iv) $ab(a - b^{1-q}) \neq 0$, $1 - \frac{4a}{b^2}$ *is a square of* $\mathbb{F}_q^*$, $b^2 - a^2 b^{q-1} - 3a = 0$.

the case $(s_1, s_2) = (1, 2)$, q even

Theorem (H 2014)

Let $f = aX + bX^q + X^{2q-1} \in \mathbb{F}_{q^2}[X]$, *where* q *is even. Then* f *is a PP of* $\mathbb{F}_{q^2}$ *if and only if one of the following is satisfied.*

(i) $a = b = 0$, $q = 2^{2k}$.

(ii) $ab \neq 0$, $a = b^{1-q}$, $\mathrm{Tr}_{q/2}(b^{-1-q}) = 0$.

(iii) $ab(a - b^{1-q}) \neq 0$, $\frac{a}{b^2} \in \mathbb{F}_q$, $\mathrm{Tr}_{q/2}(\frac{a}{b^2}) = 0$, $b^2 + a^2 b^{q-1} + a = 0$.

the case $(s_1, s_2) = (q, 2)$, q even

Tu, Zeng, Li, and Helleseth considered the case $(s_1, s_2) = (q, 2)$ with even q. Let

$$f(X) = X + aX^{q(q-1)+1} + bX^{2(q-1)+1} \in \mathbb{F}_{q^2}[X], \tag{2}$$

where q is even and $a, b \in \mathbb{F}_{q^2}^*$.

Theorem (Tu, Zeng, Li, Helleseth 2018)

Let q be even. The polynomial f in (2) is a PP of $\mathbb{F}_{q^2}$ if

$$b(1 + a^{q+1} + b^{q+1}) + a^{2q} = 0$$

and

$$\begin{cases} \mathrm{Tr}_{q/2}\Big(1 + \dfrac{1}{a^{q+1}}\Big) = 0 & \text{if } b^{q+1} = 1, \\ \mathrm{Tr}_{q/2}\Big(\dfrac{b^{q+1}}{a^{q+1}}\Big) = 0 & \text{if } b^{q+1} \neq 1, \end{cases}$$

the method on T-Z-L-H's proof

Reduction of the original problem to low degree polynomial equations on the unit circle $\mu_{q+1} = \{x \in \mathbb{F}_{q^2} : x^{q+1} = 1\}$, and a careful analysis of the solutions of such equations.

conjectured by Tu, Zeng, Li, Helleseth, proved by Bartoli

Theorem (Tu, Zeng, Li, Helleseth 2018)

Let q be even. The polynomial f in (2) is a PP of $\mathbb{F}_{q^2}$ if

$$b(1 + a^{q+1} + b^{q+1}) + a^{2q} = 0 \tag{3}$$

and

$$\begin{cases} \mathrm{Tr}_{q/2}\left(1 + \dfrac{1}{a^{q+1}}\right) = 0 & \text{if } b^{q+1} = 1, \\ \mathrm{Tr}_{q/2}\left(\dfrac{b^{q+1}}{a^{q+1}}\right) = 0 & \text{if } b^{q+1} \neq 1, \end{cases} \tag{4}$$

Conjecture (Tu, Zeng, Li, Helleseth 2018)

The conditions in (3) and (4) are also necessary for f to be a PP of $\mathbb{F}_{q^2}$.

Theorem (Bartoli 2018)

The above conjecture is true.

the method of Bartoli's proof

- If $f(X) = X + aX^{q(q-1)+1} + bX^{2(q-1)+1}$ is a PP of $\mathbb{F}_{q^2}$, there is an associated rational function $F(X) \in \mathbb{F}_q(X)$ of degree 3 which permutes $\mathbb{F}_q$.
- The Hasse-Weil bound implies that when q is not too small, the numerator of $(F(X) - F(Y))/(X - Y)$ does not have absolutely irreducible factors in $\mathbb{F}_q[X, Y]$.
- Using MAGMA, necessary and sufficient conditions are found for the numerator of $(F(X) - F(Y))/(X - Y)$ not to have absolutely irreducible factors in $\mathbb{F}_q[X, Y]$; the conditions are equivalent to (3) and (4).
- Recently, P. Yuan found a computer-free proof for Bartoli's result.

- Introduction
- Recent results in characteristic 2
- A new proof
- Outline of the new proof

a new proof

Recently, we found a new proof for the results of Tu, Zeng, Li, Helleseth, and Bartoli.

- We also use the Hasse-Weil bound, but in a different way.
- We prove the necessity and sufficiency of the conditions (3) and (4) at the same time.
- The method also appears to be working for odd characteristics (work in progress).

An observation

Recall that $f = X(1 + aX^{q(q-1)} + bX^{2(q-1)}) \in \mathbb{F}_{q^2}[X]$, where $a, b \in \mathbb{F}_{q^2}^*$. Let $\beta \in \mathbb{F}_{q^2}$ be such that $\beta^4 = b$. Then

$$f(\beta X) = \beta X(1 + a\beta^{1-q}X^{q(1-q)} + \beta^{2(q+1)}X^{2(q-1)}),$$

where $\beta^{2(q+1)} \in \mathbb{F}_q^*$. Thus we may assume that $b \in \mathbb{F}_q^*$ in $f(X)$.

Under the assumption that $b \in \mathbb{F}_q^*$, conditions (3) and (4) become slightly simpler:

Theorem

Let q be even and $f(X) = X + aX^{q(q-1)+1} + bX^{2(q-1)+1}$, where $a \in \mathbb{F}_{q^2}^*$ and $b \in \mathbb{F}_q^*$. Then f is a PP of $\mathbb{F}_{q^2}$ if and only if

(i) $b = 1$, $a \in \mathbb{F}_q^*$ *and* $\mathrm{Tr}_{q/2}(1 + a^{-1}) = 0$, *or*

(ii) $b \neq 1$, $\mathrm{Tr}_{q/2}(b/(b+1)) = 0$ *and* $a^2 = b(b+1)$.

- Introduction
- Recent results in characteristic 2
- A new proof
- Outline of the new proof

a folklore

Theorem (Park and Lee 2001, Wang 2007, Zieve 2009)

Let d and r be positive integers with $d \mid q-1$. Let $f = X^r f_1(X^{(q-1)/d})$, where $f_1 \in \mathbb{F}_q[X]$. Then f is a PP of $\mathbb{F}_q$ if and only if

(i) $\gcd(r, (q-1)/d) = 1$ *and*

(ii) $X^r f_1(X)^{(q-1)/d}$ *permutes* $\mu_d = \{x \in \mathbb{F}_q : x^d = 1\}$.

reformulation of the question

Let $\mu_{q+1} = \{x \in \mathbb{F}_{q^2}^* : x^{q+1} = 1\}$.

- f is a PP of $\mathbb{F}_{q^2}$ iff $h(X) = X(1 + aX^q + bX^2)^{q-1}$ permutes μ_{q+1}.
- For $x \in \mu_{q+1}$ with $1 + ax^q + bx^2 \neq 0$, i.e., $bx^3 + x + a \neq 0$, we have $h(x) = g(x)$, where
$$g(X) = \frac{a^q X^3 + X^2 + b}{bX^3 + X + a} \in \mathbb{F}_{q^2}(X)$$
- Let $z \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ be such that $\mathrm{Tr}_{q^2/q}(z) = 1$; hence $z^2 + z + k = 0$, where $k = z^{q+1}$. The rational function $\phi(X) = (X + z^q)/(X + z)$ maps $\mathbb{F}_q \cup \{\infty\}$ to μ_{q+1} bijectively with $\phi(\infty) = 1$.

Combining the above facts gives

Proposition

f is a PP of $\mathbb{F}_{q^2}$ if and only if

(i) *$bX^3 + X + a$ has no root in μ_{q+1}, and*

(ii) *for each $y \in \mathbb{F}_q$, there is a unique $x \in \mathbb{F}_q$ such that*
$$g\left(\frac{x + z^q}{x + z}\right) = (1 + a + b)^{q-1} \frac{y + z^q}{y + z}. \tag{5}$$

a cubic equation in x

Write the equation

$$g\left(\frac{x+z^q}{x+z}\right) = (1+a+b)^{q-1}\frac{y+z^q}{y+z}$$

as

$$x^3 + A_2(y)x^2 + A_1(y)x + A_0(y) = 0, \tag{6}$$

where $A_i(Y) \in \mathbb{F}_q(Y)$ and they depends on a, b, z. Further write (6) as

$$x'^3 + B_1(y)x' + B_0(y) = 0, \tag{7}$$

where $x' = x + A_2(y)$ and $B_i(y) \in \mathbb{F}_q(Y)$ and $B_i(Y)$ depends on a, b, z. Then use the following

Lemma (Williams, 1975)

Let $\alpha, \beta \in \mathbb{F}_{2^n}$, $\beta \neq 0$. The polynomial $X^3 + \alpha X + \beta$ has exactly one root in $\mathbb{F}_{2^n}$ if and only if $\text{Tr}_{2^n/2}(1 + \alpha^3\beta^{-2}) = 1$.

an (essentially equivalent) condition

f is a PP (essentially) if and only if for each $y \in \mathbb{F}_q$ with $B_0(y) \neq 0$, there are precisely two $x \in \mathbb{F}_q$ such that

$$x^2 + x = k + 1 + \frac{B_1(y)^3}{B_0(y)^2},$$

where $k = z^{q+1}$. (Note that $\mathrm{Tr}_{q/2}(k) = 1$ since $z^2 + z + k = 0$ and $z \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$.)

an algebraic curve arises

Consider the Artin-Scherier curve

$$X^2 + X = k + 1 + \frac{B_1(Y)^3}{B_0(Y)^2},$$

Clearing the denominator gives

$$F(X,Y) = 0,$$

where

$$F(X,Y) = Q(Y)(X^2 + X + k + 1) + P(Y) \in \mathbb{F}_q[X,Y], \tag{8}$$

$P, Q \in \mathbb{F}_q[Y]$ and $\gcd(P,Q) = 1$.

the Hasse-Weil bound

Assume that f is a PP of $\mathbb{F}_{q^2}$. Then for every $y \in \mathbb{F}_q$ with $B_0(y) \neq 0$, there are precisely two $x \in \mathbb{F}_q$ such that $F(x, y) = 0$. Let

$$V_{\mathbb{F}_q^2}(F) = \{(x, y) \in \mathbb{F}_q^2 : F(x, y) = 0\}.$$

- $|V_{\mathbb{F}_q^2}(F)| \geq 2(q-2)$ zeros in $\mathbb{F}_q$.
- By the Hasse-Weil bound, for $q \geq 2^6$, $F(X, Y)$ is not irreducible over $\overline{\mathbb{F}}_q$, i.e, $F = G_1G_2$, where $G_1, G_2 \in \overline{\mathbb{F}}_q[X, Y]$ and $\deg_X G_i = 1$.
- We claim that $G_1, G_2 \in \mathbb{F}_q[X, Y]$. Otherwise, choose $\sigma \in \mathrm{Aut}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ such that $\sigma G_1 \neq G_1$. Then $\sigma G_1 = G_2$ and hence

  $$V_{\mathbb{F}_q^2}(F) \subset V_{\mathbb{F}_q^2}(G_1) \cap V_{\mathbb{F}_q^2}(\sigma G_1).$$

  By Bézout's theorem,

  $$|V_{\mathbb{F}_q^2}(F)| \leq |V_{\mathbb{F}_q^2}(G_1) \cap V_{\mathbb{F}_q^2}(\sigma G_1)| \leq (\deg G_1)^2 \leq 9,$$

  which is a contradiction.

conclusion: a factorization

Hence $F = G_1 G_2$, where $G_1, G_2 \in \mathbb{F}_q[X, Y]$ and $\deg_X G_i = 1$.

Conclusion

f is a PP of $\mathbb{F}_{q^2}$ (essentially) if and only if

$$X^2 + X + k + 1 + \frac{B_1(Y)^3}{B_0(Y)^2} = \Big(X + \frac{D}{B_0(Y)}\Big)\Big(X + 1 + \frac{D}{B_0(Y)}\Big) \tag{9}$$

for some $D \in \mathbb{F}_q[Y]$.

Comparing the coefficients in the above factorization gives several equations in a, b, k. These equations plus some additional computation give the necessary and sufficient conditions in the main theorem.

Theorem

Let q be even and $f(X) = X + aX^{q(q-1)+1} + bX^{2(q-1)+1}$, where $a \in \mathbb{F}_{q^2}^*$ and $b \in \mathbb{F}_q^*$. Then f is a PP of $\mathbb{F}_{q^2}$ if and only if

(i) $b = 1$, $a \in \mathbb{F}_q^*$ *and* $\mathrm{Tr}_{q/2}(1 + a^{-1}) = 0$, *or*

(ii) $b \neq 1$, $\mathrm{Tr}_{q/2}(b/(b+1)) = 0$ *and* $a^2 = b(b+1)$.

references

- D. Bartoli, *On a conjecture about a class of permutation trinomials*, Finite Fields Appl. **52** (2018), 30 – 50.
- X. Hou, *Determination of a type of permutation trinomials over finite fields, II*, Finite Fields Appl. **35** (2015), 16 – 35.
- X. Hou, *On a class of permutation trinomials in characteristic* 2, arXiv:1804.02376.
- Z. Tu, X. Zeng, C. Li, T. Helleseth, *A class of new permutation trinomials*, Finite Fields Appl. **50** (2018), 178 – 195.

Thank You!