New Permutation Binomials and Trinomials over Finite Fields

Xiang-dong Hou

Department of Mathematics and Statistics
University of South Florida

Fq11, Magdeburg, Germany, July 22-26, 2013
1. Permutation polynomials over finite fields
2. Main results
3. Background and connections
4. Sketch of proof: Theorem 1
5. Sketch of proof: Theorem 2
6. What’s next?
1. Permutation polynomials over finite fields

1. Permutation polynomials over finite fields
Every function from $F_q$ to $F_q$ can be represented by a polynomial $f \in F_q[x]$.

$f \in F_q[x]$ is called a permutation polynomial (PP) of $F_q$ if the mapping $x \mapsto f(x)$ is a permutation of $F_q$.

PPs in simple algebraic forms are interesting. Such PPs are sometimes the result of the mysterious interplay between the algebraic and combinatorial structures of the finite field.

Permutation binomials and trinomials are particularly interesting.
$f$ is a PP of $\mathbb{F}_q$ if and only if one of the following holds
Criteria

\[ f \text{ is a PP of } \mathbb{F}_q \text{ if and only if one of the following holds} \]

\[
\sum_{x \in \mathbb{F}_q} f(x)^s = \begin{cases} 
0 & \text{if } 1 \leq s \leq q - 2, \\
-1 & \text{if } s = q - 1. 
\end{cases}
\]
Criteria

\( f \) is a PP of \( \mathbb{F}_q \) if and only if one of the following holds

\[
\sum_{x \in \mathbb{F}_q} f(x)^s = \begin{cases} 
0 & \text{if } 1 \leq s \leq q - 2, \\
-1 & \text{if } s = q - 1.
\end{cases}
\]

\[
\sum_{x \in \mathbb{F}_q} \zeta_p^{\text{Tr}_{q/p}(af(x))} = 0 \text{ for all } a \in \mathbb{F}_q^*,
\]

where \( p = \text{char} \mathbb{F}_q, \zeta_p = e^{2\pi i/p}. \)
f is a PP of $\mathbb{F}_q$ if and only if one of the following holds

\[ \sum_{x \in \mathbb{F}_q} f(x)^s = \begin{cases} 
0 & \text{if } 1 \leq s \leq q - 2, \\
-1 & \text{if } s = q - 1.
\end{cases} \]

\[ \sum_{x \in \mathbb{F}_q} \zeta_p^{\text{Tr}_{q/p}(af(x))} = 0 \text{ for all } a \in \mathbb{F}_q^*, \]

where $p = \text{char } \mathbb{F}_q$, $\zeta_p = e^{2\pi i/p}$.

For every $y \in \mathbb{F}_q$, $f(x) = y$ has at least one solution $x \in \mathbb{F}_q$. 
$f$ is a PP of $\mathbb{F}_q$ if and only if one of the following holds

$$\sum_{x \in \mathbb{F}_q} f(x)^s = \begin{cases} 0 & \text{if } 1 \leq s \leq q - 2, \\ -1 & \text{if } s = q - 1. \end{cases}$$

$$\sum_{x \in \mathbb{F}_q} \zeta_p \text{Tr}_{q/p}(af(x)) = 0 \text{ for all } a \in \mathbb{F}_q^*,$$

where $p = \text{char } \mathbb{F}_q$, $\zeta_p = e^{2\pi i / p}$.

For every $y \in \mathbb{F}_q$, $f(x) = y$ has at least one solution $x \in \mathbb{F}_q$.

For every $y \in \mathbb{F}_q$, $f(x) = y$ has at most one solution $x \in \mathbb{F}_q$. 
II. Main results

2. Main results
Theorem 1. Let $f = tx + x^{2q-1} \in \mathbb{F}_q[x]$, where $t \in \mathbb{F}_q^*$. Then $f$ is a PP of $\mathbb{F}_{q^2}$ if and only if one of the following occurs:

(i) $t = 1$, $q \equiv 1 \pmod{4}$;
(ii) $t = -3$, $q \equiv \pm 1 \pmod{12}$;
(iii) $t = 3$, $q \equiv -1 \pmod{6}$.

Theorem 2. Let $f = -x + tx^{q} + x^{2q-1} \in \mathbb{F}_q[x]$, where $q > 2$ and $t \in \mathbb{F}_q^*$. Then $f$ is a PP of $\mathbb{F}_{q^2}$ if and only if one of the following occurs:

(i) $q$ is even and $\text{Tr}_{q/2}(1t) = 0$;
(ii) $q \equiv 1 \pmod{8}$ and $t^2 = -2$.
Theorems

**Theorem 1.** Let \( f = tx + x^{2q-1} \in \mathbb{F}_q[x] \), where \( t \in \mathbb{F}_q^* \). Then \( f \) is a PP of \( \mathbb{F}_{q^2} \) if and only if one of the following occurs:

(i) \( t = 1, q \equiv 1 \pmod{4} \);
(ii) \( t = -3, q \equiv \pm 1 \pmod{12} \);
(iii) \( t = 3, q \equiv -1 \pmod{6} \).

**Theorem 2.** Let \( f = -x + tx^q + x^{2q-1} \in \mathbb{F}_q[x] \), where \( q > 2 \) and \( t \in \mathbb{F}_q^* \). Then \( f \) is a PP of \( \mathbb{F}_{q^2} \) if and only if one of the following occurs:

(i) \( q \) is even and \( \text{Tr}_{q/2}(1/t) = 0 \);
(ii) \( q \equiv 1 \pmod{8} \) and \( t^2 = -2 \).
3. Background and connections

3. Background and connections
What leads to the consideration of the polynomials in Theorems 1 and 2?

The Dickson polynomial
\[ \downarrow \]
The reversed Dickson polynomial (RDP)
\[ \downarrow \]
The polynomial \( g_{n,q} \) (\( q \)-ary version of RDP)
\[ \downarrow \]
\[ t x + x^{2q-1}, -x + t x^q + x^{2q-1} \]
Let $D_n(x, y) \in \mathbb{Z}[x, y]$ be defined by

$$x^n + y^n = D_n(x + y, xy).$$

**The Dickson polynomial:** $D_n(x, 1)$, PP of $\mathbb{F}_q$ if and only if $\gcd(n, q^2 - 1) = 1$.

**The reversed Dickson polynomial:** $D_n(1, x)$, new interesting PPs, connections to APN, conjectures. (H, Mullen, Sellers, Yucas, 2009)
The polynomial $g_{n,q} — 1$

RDP:

$$D_n(1, x(1 - x)) = x^n + (1 - x)^n.$$ 

In characteristic 2

$$D_n(1, x^2 - x) = \sum_{a \in \mathbb{F}_2} (x + a)^n.$$ 

A natural generalization: $g_{n,q} \in \mathbb{F}_p[x]$ ($p = \text{char } \mathbb{F}_q$) defined by

$$g_{n,q}(x^q - x) = \sum_{a \in \mathbb{F}_q} (x + a)^n.$$
The polynomial $g_{n,q} — 2$

- There are many interesting new PPs in the family $g_{n,q}$.
- Many unsolved questions.
- The ultimate goal: determine all triples $(n, e; q)$ for which $g_{n,q}$ is a PP of $\mathbb{F}_{q^e}$.
- Computer search: Many desirable triples have $n = q^\alpha - q^\beta - 1$.
- $g_{q^{2i}-q-1,q}(x) = (i - 1)y - iy^{2q-1}, \ x \in \mathbb{F}_{q^2}, \ y = x^{q^2-q-1}$.
- $g_{q^{2i+1}-q-1,q}(x) = iy - y^q - iy^{2q-1}, \ x \in \mathbb{F}_{q^2}, \ y = x^{q^2-q-1}$.
- Theorems 1 and 2 determine the PPs in the above two items.
Related work

We have

\[ t x + x^{2q-1} = x(t + x^{2(q-1)}), \]
\[ -x + t x^q + x^{2q-1} = x(-1 + t x^{q-1} + x^{2(q-1)}). \]

There are criteria for a polynomial of the form \( x^r h(\frac{x^{q-1}}{d}) \) to be a PP of \( \mathbb{F}_q \), where \( d, r > 0, d \mid q - 1 \), and \( h \in \mathbb{F}_q[x] \). (Akbary and Wang 06,07; Wan and Lidl 91; Wang 07; Zieve 09.)

Those criteria are not explicit enough to imply Theorems 1 and 2.
4. Sketch of proof: Theorem 1
Recall Theorem 1

**Theorem 1.** Let $f = tx + x^{2q-1} \in \mathbb{F}_q[x]$, where $t \in \mathbb{F}_q^*$. Then $f$ is a PP of $\mathbb{F}_{q^2}$ if and only if one of the following occurs:

(i) $t = 1, \quad q \equiv 1 \pmod{4}$;
(ii) $t = -3, \quad q \equiv \pm 1 \pmod{12}$;
(iii) $t = 3, \quad q \equiv -1 \pmod{6}$.

We will sketch the following part of the proof: Assume *(ii)* $t = -3, q \equiv \pm 1 \pmod{12}$, or *(iii)* $t = 3, q \equiv -1 \pmod{6}$.

Then $f$ is a PP of $\mathbb{F}_{q^2}$.

We want to show that

$$
\sum_{x \in \mathbb{F}_{q^2}^*} f(x) s = 0 \quad \text{for all } 1 \leq s \leq q^2 - 2.
$$

It can be shown that the power sum is 0 unless $s = \alpha + \beta q$, where $\alpha, \beta \geq 0, \alpha + \beta = q - 1$ and $\alpha$ is odd.
Recall Theorem 1

**Theorem 1.** Let \( f = tx + x^{2q-1} \in \mathbb{F}_q[x] \), where \( t \in \mathbb{F}_q^* \). Then \( f \) is a PP of \( \mathbb{F}_{q^2} \) if and only if one of the following occurs:

(i) \( t = 1, \; q \equiv 1 \pmod{4} \);
(ii) \( t = -3, \; q \equiv \pm 1 \pmod{12} \);
(iii) \( t = 3, \; q \equiv -1 \pmod{6} \).

We will sketch the following part of the proof: Assume

(ii) \( t = -3, \; q \equiv \pm 1 \pmod{12} \), or
(iii) \( t = 3, \; q \equiv -1 \pmod{6} \).

Then \( f \) is a PP of \( \mathbb{F}_{q^2} \).
Recall Theorem 1

Theorem 1. Let $f = tx + x^{2q-1} \in \mathbb{F}_q[x]$, where $t \in \mathbb{F}_q^*$. Then $f$ is a PP of $\mathbb{F}_{q^2}$ if and only if one of the following occurs:

(i) $t = 1$, $q \equiv 1 \pmod{4}$;
(ii) $t = -3$, $q \equiv \pm 1 \pmod{12}$;
(iii) $t = 3$, $q \equiv -1 \pmod{6}$.

We will sketch the following part of the proof: Assume

(ii) $t = -3$, $q \equiv \pm 1 \pmod{12}$, or
(iii) $t = 3$, $q \equiv -1 \pmod{6}$.

Then $f$ is a PP of $\mathbb{F}_{q^2}$.

We want to show that

$$\sum_{x \in \mathbb{F}_{q^2}^*} f(x)^s = 0 \quad \text{for all } 1 \leq s \leq q^2 - 2.$$

It can be shown that the power sum is 0 unless $s = \alpha + \beta q$, where $\alpha, \beta \geq 0$, $\alpha + \beta = q - 1$ and $\alpha$ is odd.
Assume

- (ii) $t = -3$, $q \equiv \pm 1 \pmod{12}$, or (iii) $t = 3$, $q \equiv -1 \pmod{6}$;
- $s = \alpha + \beta q$, where $\alpha, \beta \geq 0$, $\alpha + \beta = q - 1$ and $\alpha$ is odd.

We found that

$$C \sum_{x \in \mathbb{F}^*_q} f(x)^s =$$

$$\sum_i \binom{\alpha}{i} \left( \frac{3\alpha - 1}{2} - i \right) (-1)^i 3^{2i+1} + \sum_i \binom{\alpha}{i} \left( \frac{3\alpha - 1}{2} - i + \frac{q+1}{2} \right) (-1)^i 3^{2i},$$

where $C \neq 0$. 
So the question is to show

\[
\sum_i \binom{\alpha}{i} \left( \frac{3\alpha - 1}{2} - i \right)(-1)^i 3^{2i+1} + \sum_i \binom{\alpha}{i} \left( \frac{3\alpha - 1}{2} - i + \frac{q+1}{2} \right)(-1)^i 3^{2i}
\equiv 0 \pmod{p}.
\]

We will see that there is curious identity hidden in the above congruence.
Lucas’ Theorem

Let $p = \text{char} \mathbb{F}_q$ and let $\mathbb{Z}_p$ be the ring of $p$-adic integers. For $z \in \mathbb{Z}_p$ and $a \in \mathbb{Z}$ with $a \geq 0$, written in the form $z = \sum_{n \geq 0} z_n p^n$, $a = \sum_{n \geq 0} a_n p^n$, $0 \leq z_n, a_n \leq p - 1$, we have

$$
\binom{z}{a} \equiv \prod_{n \geq 0} \binom{z_n}{a_n} \pmod{p}.
$$

Therefore, if $z, z' \in \mathbb{Z}_p$ such that $\nu_p(z - z') > \log_p a$, where $\nu_p$ is the $p$-adic order, we have $\binom{z}{a} \equiv \binom{z'}{a} \pmod{p}$. 

In \( \mathbb{Z}_p/p\mathbb{Z}_p (= \mathbb{F}_p) \), \( \left( \frac{\frac{3\alpha-1}{2} - i + \frac{q+1}2}{\alpha} \right) = \left( \frac{\frac{3\alpha-1}{2} - i + \frac{1}2}{\alpha} \right) \). So

\[
\sum_i \binom{\alpha}{i} \left( \frac{\frac{3\alpha-1}{2} - i}{\alpha} \right) (-1)^i 3^{2i+1} + \sum_i \binom{\alpha}{i} \left( \frac{\frac{3\alpha-1}{2} - i + \frac{q+1}{2}}{\alpha} \right) (-1)^i 3^{2i}
\]

\[
= \sum_i \binom{\alpha}{i} \left( \frac{\frac{3\alpha-1}{2} - i}{\alpha} \right) (-1)^i 3^{2i+1} + \sum_i \binom{\alpha}{i} \left( \frac{\frac{3\alpha-1}{2} - i + \frac{1}{2}}{\alpha} \right) (-1)^i 3^{2i}
\]

\[
= \frac{1}{\alpha! 2^\alpha} \left[ \sum_i \binom{2n+1}{i} \left( \prod_{j=1}^{2n+1} (6n - 2i + 4 - 2j) \right) (-1)^i 3^{2i+1}
\]

\[
+ \sum_i \binom{2n+1}{i} \left( \prod_{j=1}^{2n+1} (6n - 2i + 5 - 2j) \right) (-1)^i 3^{2i} \right],
\]

where \( \alpha = 2n+1 \).
An interesting development

Let

\[ S_1(n) = \sum_i \binom{2n+1}{i} \left( \prod_{j=1}^{2n+1} (6n - 2i + 4 - 2j) \right) (-1)^i 3^{2i+1}, \]

\[ S_2(n) = \sum_i \binom{2n+1}{i} \left( \prod_{j=1}^{2n+1} (6n - 2i + 5 - 2j) \right) (-1)^i 3^{2i}. \]

The goal is to show that

\[ \frac{1}{\alpha! 2^{\alpha}} (S_1(n) + S_2(n)) = 0 \quad \text{in} \quad \mathbb{Z}_p/p\mathbb{Z}_p. \] (1)

At least we should have \( S_1(n) + S_2(n) = 0 \) in \( \mathbb{Z}_p/p\mathbb{Z}_p \).

\( S_1(n) \) and \( S_2(n) \) are independent of \( p \) and \( p \) is “arbitrary”. So must show that

\[ S_1(n) + S_2(n) = 0 \quad \text{in} \quad \mathbb{Z}. \] (2)

Note that (2) implies (1).
Theorem 3. Let

\[ S_1(n) = \sum_i \binom{2n+1}{i} \left( \prod_{j=1}^{2n+1} (6n - 2i + 4 - 2j) \right) (-1)^i 3^{2i+1}, \]

\[ S_2(n) = \sum_i \binom{2n+1}{i} \left( \prod_{j=1}^{2n+1} (6n - 2i + 5 - 2j) \right) (-1)^i 3^{2i}. \]

Then

\[ S_1(n) + S_2(n) = 0. \]
Proof of Theorem 3

We have \( S_1(n) = \sum_k F_1(n, k) \) and \( S_2(n) = \sum_k F_2(n, k) \), where

\[
F_1(n, k) = \binom{2n+1}{k} \left( \prod_{j=1}^{2n+1} (6n - 2k + 4 - 2j) \right) (-1)^k 3^{2k+1},
\]

\[
F_2(n, k) = \binom{2n+1}{k} \left( \prod_{j=1}^{2n+1} (6n - 2k + 5 - 2j) \right) (-1)^k 3^{2k}.
\]

Using Zeilberger’s algorithm, we find that

\[
F_1(n + 2, k) + 24(36n^2 + 126n + 113)F_1(n + 1, k) + 46656(n + 1)^2(2n + 3)^2 F_1(n, k) = G_1(n, k + 1) - G_1(n, k),
\]

where \( G_1(n, k) = F_1(n, k)R_1(n, k) \) and \( R_1(n, k) \) is some complicated rational function in \( n, k \).
In case you would like details

\[ R_1(n, k) = -\frac{32k(3n - k + 2)}{(n - k + 1)(n - k + 2) \prod_{j=2}^{5}(2n - k + j)} \cdot (264240 - 321108k + 142242k^2 \\
- 27228k^3 + 1902k^4 + 1434774n - 1559605kn + 612100k^2n - 102647k^3n \\
+ 6194k^4n + 3361281n^2 - 3199801kn^2 + 1081204k^2n^2 - 152528k^3n^2 \\
+ 7484k^4n^2 + 4437783n^3 - 3594830kn^3 + 1003340k^2n^3 - 111631k^3n^3 \\
+ 3976k^4n^3 + 3611829n^4 - 2388503kn^4 + 515900k^2n^4 - 40234k^3n^4 \\
+ 784k^4n^4 + 1855833n^5 - 938595kn^5 + 139350k^2n^5 - 5712k^3n^5 \\
+ 587970n^6 - 201978kn^6 + 15444k^2n^6 + 105030n^7 - 18360kn^7 + 8100n^8).\]
Proof of Theorem 3 completed

Summing

\[
F_1(n + 2, k) + 24(36n^2 + 126n + 113)F_1(n + 1, k) \\
+ 46656(n + 1)^2(2n + 3)^2 F_1(n, k) \\
= G_1(n, k + 1) - G_1(n, k)
\]

over \( k \) gives the second order recurrence relation:

\[
S_1(n + 2) + 24(36n^2 + 126n + 113)S_1(n + 1) + 46656(n + 1)^2(2n + 3)^2 S_1(n) = 0.
\]
Proof of Theorem 3 completed

Summing

\[ F_1(n + 2, k) + 24(36n^2 + 126n + 113)F_1(n + 1, k) \]
\[ + 46656(n + 1)^2(2n + 3)^2F_1(n, k) \]
\[ = G_1(n, k + 1) - G_1(n, k) \]

over \( k \) gives the second order recurrence relation:

\[ S_1(n + 2) + 24(36n^2 + 126n + 113)S_1(n + 1) + 46656(n + 1)^2(2n + 3)^2S_1(n) = 0. \]

In the same way we found that \( S_2(n) \) satisfies the same recurrence relation even though \( G_2(n, k) \) is different form \( G_1(n, k) \).
Proof of Theorem 3 completed

Summing

\[ F_1(n + 2, k) + 24(36n^2 + 126n + 113)F_1(n + 1, k) \]
\[ + 46656(n + 1)^2(2n + 3)^2F_1(n, k) \]
\[ = G_1(n, k + 1) - G_1(n, k) \]

over \( k \) gives the second order recurrence relation:

\[ S_1(n+2) + 24(36n^2 + 126n + 113)S_1(n+1) + 46656(n+1)^2(2n+3)^2S_1(n) = 0. \]

In the same way we found that \( S_2(n) \) satisfies the same recurrence relation even though \( G_2(n, k) \) is different form \( G_1(n, k) \).

It is easy to check that \( S_1(0) = 6 = -S_2(0) \) and \( S_1(1) = -3312 = -S_2(1) \). Hence

\[ S_1(n) + S_2(n) = 0. \]
Theorem 3 can be stated in the standard notation of hypergeometric series.

\[
\begin{align*}
2F_1 \left[ \begin{array}{c}
-n, 2n+2 \\
n+2
\end{array} \right| 3^{-2} \\
= (-1)^n \frac{3^{2n+1}}{(n+1)_{n+1} (n+2)_n} \cdot 2F_1 \left[ \begin{array}{c}
\frac{n+3}{2}, \frac{-2n-1}{2} \\
-n+\frac{1}{2}
\end{array} \right| 3^{-2} \right].
\end{align*}
\]
5. Sketch of proof: Theorem 2
Theorem 2. Let \( f = -x + tx^q + x^{2q-1} \in \mathbb{F}_q[x] \), where \( q > 2 \) and \( t \in \mathbb{F}_q^* \). Then \( f \) is a PP of \( \mathbb{F}_{q^2} \) if and only if one of the following occurs:

(i) \( q \) is even and \( \text{Tr}_{q/2}(\frac{1}{t}) = 0 \);

(ii) \( q \equiv 1 \pmod{8} \) and \( t^2 = -2 \).
Theorem 2. Let \( f = -x + tx^q + x^{2q-1} \in \mathbb{F}_q[x] \), where \( q > 2 \) and \( t \in \mathbb{F}_q^* \). Then \( f \) is a PP of \( \mathbb{F}_q^2 \) if and only if one of the following occurs:

(i) \( q \) is even and \( \text{Tr}_{q/2}(\frac{1}{t}) = 0 \);

(ii) \( q \equiv 1 \pmod{8} \) and \( t^2 = -2 \).

We will sketch the following part of the proof of Theorem 2: Assume \( q \equiv 1 \pmod{8} \), \( t \in \mathbb{F}_q^* \), \( t^2 = -2 \). We show that for every \( y \in \mathbb{F}_q^2 \), the equation

\[-x + tx^q + x^{2q-1} = y \quad (3)\]

has at least one solution \( x \in \mathbb{F}_q^2 \).
\[-x + tx^q + x^{2q-1} = y \text{ (part 1)}\]

It $y \in \mathbb{F}_q$, $x = \frac{y}{t}$ is a solution. So assume $y \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$.

Assume $y^{q-1} - y^{1-q} \neq 0$. ($y^{q-1} - y^{1-q} = 0$ is an easier case we ignore here.)

**Basic Idea:** Try to find a solution of the form

$$x = \left(\frac{y}{t + (y^{q-1} - y^{1-q})u}\right)^q,$$  \hspace{1cm} (4)

where $u \in \mathbb{F}_q$ is to be determined.
It \( y \in \mathbb{F}_q, x = \frac{y}{t} \) is a solution. So assume \( y \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q \).
Assume \( y^{q-1} - y^{1-q} \neq 0 \). (\( y^{q-1} - y^{1-q} = 0 \) is an easier case we ignore here.)

**Basic Idea:** Try to find a solution of the form

\[
x = \left( \frac{y}{t + (y^{q-1} - y^{1-q})u} \right)^q,
\]

where \( u \in \mathbb{F}_q \) is to be determined.

How did we guess out this form? From \( -x + tx^q + x^{2q-1} = y \) we have

\[
x^{-q}y = t + x^{q-1} - x^{1-q} = t + (y^{q-1} - y^{1-q})u,
\]

where

\[
u = \frac{x^{q-1} - x^{1-q}}{y^{q-1} - y^{1-q}} \in \mathbb{F}_q.
\]
\[-x + tx^q + x^{2q-1} = y \text{ (part 2)}\]

Using \( x = \left( \frac{y}{t+(y^{q-1}-y^{1-q})u} \right)^q \) and \( t^2 = -2 \), the equation

\[-x + tx^q + x^{2q-1} = y \]

becomes

\[u^3 - u^2 + \frac{2 - 2ts}{s^2 - 4} u + \frac{2}{s^2 - 4} = 0,\]

where \( s = y^{q-1} + y^{1-q} \in \mathbb{F}_q \).
Using $x = \left( \frac{y}{t+(y^{q-1}-y^{1-q})u} \right)^q$ and $t^2 = -2$, the equation

$$-x + tx^q + x^{2q-1} = y$$

becomes

$$u^3 - u^2 + \frac{2 - 2ts}{s^2 - 4} u + \frac{2}{s^2 - 4} = 0,$$

where $s = y^{q-1} + y^{1-q} \in \mathbb{F}_q$.

**Note:** $s^2 - 4 = (y^{q-1} - y^{1-q})^2$, which is a nonsquare in $\mathbb{F}_q^*$ since $y^{q-1} - y^{1-q} \notin \mathbb{F}_q$. 

-X. Hou (Universities of South Florida)
\[ -x + tx^q + x^{2q-1} = y \ (\text{part 2}) \]

Using \( x = \left( \frac{y}{t+(y^{q-1}-y^{1-q})u} \right)^q \) and \( t^2 = -2 \), the equation

\[ -x + tx^q + x^{2q-1} = y \]

becomes

\[ u^3 - u^2 + \frac{2 - 2ts}{s^2 - 4} u + \frac{2}{s^2 - 4} = 0, \]

where \( s = y^{q-1} + y^{1-q} \in \mathbb{F}_q \).

**Note:** \( s^2 - 4 = (y^{q-1} - y^{1-q})^2 \), which is a nonsquare in \( \mathbb{F}_q^* \) since

\( y^{q-1} - y^{1-q} \notin \mathbb{F}_q \).

The question is to show that

\[ g(u) = u^3 - u^2 + \frac{2 - 2ts}{s^2 - 4} u + \frac{2}{s^2 - 4} \in \mathbb{F}_q[u] \]

has at least one root in \( \mathbb{F}_q \).
Discriminant of $g$

$$g(u) = u^3 - u^2 + \frac{2 - 2ts}{s^2 - 4} u + \frac{2}{s^2 - 4}.$$ 

If $g$ is irreducible over $\mathbb{F}_q$, its discriminant $D(g)$ is a square of $\mathbb{F}^*_q$. 

$(\text{Gal}(g/\mathbb{F}_q) = \text{Aut}(\mathbb{F}_{q^3}/\mathbb{F}_q) = A_3 \Rightarrow D(g) \text{ is a square of } \mathbb{F}^*_q.)$

So the question is show that $D(g)$ is not a square of $\mathbb{F}^*_q$.

$$D(g) = -4 \left( \frac{2 - 2ts}{s^2 - 4} \right)^3 - 27 \left( \frac{2}{s^2 - 4} \right)^2 + \left( \frac{2 - 2ts}{s^2 - 4} \right)^2$$

$$+ 4 \cdot \frac{2}{s^2 - 4} - 18 \cdot \frac{2 - 2ts}{s^2 - 4} \cdot \frac{2}{s^2 - 4}$$

$$= \cdots \text{(using } t^2 = -2 \text{)}$$
Discriminant of $g$

$$g(u) = u^3 - u^2 + \frac{2 - 2ts}{s^2 - 4}u + \frac{2}{s^2 - 4}.$$  

If $g$ is irreducible over $\mathbb{F}_q$, its discriminant $D(g)$ is a square of $\mathbb{F}_q^*$.  

$$\text{Gal}(g/\mathbb{F}_q) = \text{Aut}(\mathbb{F}_{q^3}/\mathbb{F}_q) = A_3 \Rightarrow D(g) \text{ is a square of } \mathbb{F}_q^*.$$  

So the question is show that $D(g)$ is not a square of $\mathbb{F}_q^*$.  

$$D(g) = -4\left(\frac{2 - 2ts}{s^2 - 4}\right)^3 - 27\left(\frac{2}{s^2 - 4}\right)^2 + \left(\frac{2 - 2ts}{s^2 - 4}\right)^2$$  

$$+ 4 \cdot \frac{2}{s^2 - 4} - 18 \cdot \frac{2 - 2ts}{s^2 - 4} \cdot \frac{2}{s^2 - 4}$$  

$$= \cdots \text{ (using } t^2 = -2)$$  

$$= -\frac{16(s + 5t)^2}{(s^2 - 4)^3}.$$  

X. Hou (Universities of South Florida)  
permutation binomial/trinomial  
Fq11 30 / 39
Discriminant of $g$

$$g(u) = u^3 - u^2 + \frac{2 - 2ts}{s^2 - 4} u + \frac{2}{s^2 - 4}.$$ 

If $g$ is irreducible over $\mathbb{F}_q$, its discriminant $D(g)$ is a square of $\mathbb{F}_q^*$. 

$$(\text{Gal}(g/\mathbb{F}_q) = \text{Aut}(\mathbb{F}_{q^3}/\mathbb{F}_q) = A_3 \Rightarrow D(g) \text{ is a square of } \mathbb{F}_q^*.)$$

So the question is show that $D(g)$ is not a square of $\mathbb{F}_q^*$. 

$$D(g) = -4\left(\frac{2 - 2ts}{s^2 - 4}\right)^3 - 27\left(\frac{2}{s^2 - 4}\right)^2 + \left(\frac{2 - 2ts}{s^2 - 4}\right)^2$$

$$+ 4 \cdot \frac{2}{s^2 - 4} - 18 \cdot \frac{2 - 2ts}{s^2 - 4} \cdot \frac{2}{s^2 - 4}$$

$$= \cdots \text{ (using } t^2 = -2)$$

$$= -16(s + 5t)^2 \quad \frac{1}{(s^2 - 4)^3}.$$ 

$-16(s + 5t)^2$ is a square ($q \equiv 1 \pmod{8}$), $s^2 - 4$ is not, so $D(g)$ is not a square of $\mathbb{F}_q^*$. QED.
By Theorem 2, for $q \equiv 1 \pmod{8}$ and $t^2 = -2$, we have

$$\sum_{x \in \mathbb{F}_{q^2}} f(x)^s = 0, \quad 1 \leq s \leq q^2 - 2.$$ 

What information can be derived from these identities?
Corollary 1. For integer $a \geq 0$, define

$$H(a) = \sum_{j,i \geq 0} \binom{a}{i} \left(\frac{a}{2} + j\right) \left(2j + 2\left\{\frac{a-1}{2}\right\} + i\right) (-2)^j,$$

where $\{x\} = x - \lfloor x \rfloor$. Then for all powers $q$ of a prime $p$ with $q \equiv 1 \pmod{8}$,

$$H(a) + H(q - 1 - a) \equiv 0 \pmod{p}, \quad 0 \leq a \leq q - 1.$$

**Question:** Is there a direct proof of Corollary 1?

**Remark.** Each of the sequences $H(2n)$ and $H(2n + 1)$ satisfies a recurrence relation of order 4 (found by the Zeilberger algorithm for hypergeometric multi sums).
Corollary 2.

For integer $a \geq 0$, define

$$S(a) = \sum_{0 \leq j \leq \frac{a-1}{2}} \sum_{0 \leq i \leq 2j+2\left\{\frac{a-1}{2}\right\}} (-2)^j {a \choose i} \left( a + 2j + 2\left\{\frac{a-1}{2}\right\} - i \right)$$

$$\cdot \left[ \left( \left\lfloor \frac{a}{2} \right\rfloor + j \right) + \left( \left\lfloor \frac{a}{2} \right\rfloor + \frac{1}{2} + j \right) \right]$$

Assume $q \equiv 1 \pmod{8}$. Then

$$S(a) \equiv 0 \pmod{p} \quad \text{for} \quad \frac{q-1}{2} \leq a \leq q - 1.$$ 

Question: Direct proof?

Conjecture. We have

$$S(a) \equiv \begin{cases} 0 \pmod{3} & \text{if } a = 0 \text{ or } 3^{2k+1} \leq a \leq 3^{2k+2} - 1 \text{ for some } k \geq 0, \\ -1 \pmod{3} & \text{otherwise.} \end{cases}$$
6. What’s next?
\[ f = ax + bx^q + x^{2q-1} \]

PPs of \( \mathbb{F}_{q^2} \) of the form \( f = ax + bx^q + x^{2q-1} \in \mathbb{F}_q[x] \): recently determined.
\[ f = ax + bx^q + x^{2q-1} \]

- PPs of \( \mathbb{F}_{q^2} \) of the form \( f = ax + bx^q + x^{2q-1} \in \mathbb{F}_q[x] \): recently determined.

- What about \( f = ax + bx^q + x^{2q-1} \in \mathbb{F}_{q^2}[x] \)? Work ongoing. Optimistic but need luck.
Some references — 1


Some references — 2

- A. Masuda, D. Panario, Q. Wang, *The number of permutation binomials over* \(\mathbb{F}_{4p+1}\) *where* \(p\) *and* \(4p + 1\) *are primes*, Electron. J. Combin. 13
Some references — 3

- 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 (2009), 2209 – 2216.
Thank You!