A Class of Permutation Binomials over Finite Fields

Xiang-dong Hou

Department of Mathematics and Statistics
University of South Florida

CanaDAM, Newfoundland, June 10-13, 2013
I. Permutation polynomials over finite fields
II. The main theorem
III. Sketch of a part of the proof
I. Permutation polynomials over finite fields
Every function from $\mathbb{F}_q$ to $\mathbb{F}_q$ can be represented by a polynomial $f \in \mathbb{F}_q[x]$.

$f \in \mathbb{F}_q[x]$ is called a permutation polynomial (PP) of $\mathbb{F}_q$ if the mapping $x \mapsto f(x)$ is a permutation of $\mathbb{F}_q$.

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 over finite fields are particularly interesting and have received much attention.
A criterion

**Criterion**

$f$ is a PP of $\mathbb{F}_q$ if and only if

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

II. The main theorem
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) \( t = 3, \ q \equiv -1 \pmod{6} \).
Statement of the theorem

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) \( t = 3, q \equiv -1 \pmod{6} \).

Remark. The result was conjectured in a recent study of PPs defined by a functional equation. (Fernando, H, Lappano 2013)
III. Sketch of a part of the proof
We will sketch the proof that \( f = tx + x^{2q-1} \) \((t \in F_q^*)\) is a PP of \( F_{q^2} \) if

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

This part of the proof is interesting because of an unexpected new tool.
Assume

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

We want to show that

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

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.
Power sum

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 \( C \neq 0 \).
Let \( \mathbb{Z}_p \) be the ring of \( p \)-adic integers. In \( \mathbb{Z}_p/p\mathbb{Z}_p (= \mathbb{F}_p) \),

\[
\left( \frac{3\alpha - 1}{2} - i + \frac{q+1}{2} \right) = \left( \frac{3\alpha - 1}{2} - i + \frac{1}{2} \right).
\]

So

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

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

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

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

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

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

(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 we must show that

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

(2)

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

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 $n, k$. 

X. Hou (Universities of South Florida)
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).}
Telescoping

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

gives the second order recurrence relation:

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

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

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 from \(G_1(n, k)\).
Telescoping

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

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 from \( G_1(n, k) \).

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 2 can be stated in the standard notation of hypergeometric series.

\[
\begin{align*}
\mathbf{2}_1 \mathbf{F}_1 & \left[ \begin{array}{c} -n, 2n+2 \\ n+2 \end{array} \right] \bigg| 3^{-2} \\
& = (-1)^n 3^{2n+1} \frac{(-n+\frac{1}{2})_{2n+1}}{(n+1)_{n+1} (n+2)_n} \mathbf{2}_1 \mathbf{F}_1 \left[ \begin{array}{c} n+\frac{3}{2}, -2n-1 \\ -n+\frac{1}{2} \end{array} \right] 3^{-2}.
\end{align*}
\]

Thank You!