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

Outline

I. Permutation polynomials over finite fields
II. The main theorem
III. Sketch of a part of the proof

I. Permutation polynomials over finite fields

Introduction

- 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

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

II. The main theorem

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) $t = 3$, $q \equiv -1 \pmod 6$.

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

Part of the proof

- We will sketch the proof that $f = tx + x^{2q-1}$ ($t \in \mathbb{F}_q^*$) is a PP of $\mathbb{F}_{q^2}$ 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.

Basic idea

Assume

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

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

We want to show that

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

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

We found that

$$C \sum_{x \in \mathbb{F}_{q^2}^*} f(x)^s =$$

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

where $C \neq 0$.

p-adic integers

Let $\mathbb{Z}_p$ be the ring of p-adic integers. In $\mathbb{Z}_p/p\mathbb{Z}_p$ $(=\mathbb{F}_p)$, $\binom{\frac{3\alpha-1}{2}-i+\frac{q+1}{2}}{\alpha} = \binom{\frac{3\alpha-1}{2}-i+\frac{1}{2}}{\alpha}$. So

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

$$= \sum_i \binom{\alpha}{i}\binom{\frac{3\alpha-1}{2}-i}{\alpha}(-1)^i 3^{2i+1} + \sum_i \binom{\alpha}{i}\binom{\frac{3\alpha-1}{2}-i+\frac{1}{2}}{\alpha}(-1)^i 3^{2i}$$

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

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

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

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

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

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

Note that (2) implies (1).

Theorem 2

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

$$\begin{aligned} &F_1(n+2,k) + 24(36n^2+126n+113)F_1(n+1,k) \\ &\quad + 46656(n+1)^2(2n+3)^2F_1(n,k) \\ &= G_1(n,k+1) - G_1(n,k), \end{aligned}$$

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

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

Proof of Theorem 2 completed

Telescoping

$$\begin{aligned} & F_1(n+2,k) + 24(36n^2+126n+113)F_1(n+1,k) \\ & \quad + 46656(n+1)^2(2n+3)^2F_1(n,k) \\ = & G_1(n,k+1) - G_1(n,k) \end{aligned}$$

gives the second order recurrence relation:

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

Proof of Theorem 2 completed

Telescoping

$$\begin{aligned} & F_1(n+2,k) + 24(36n^2+126n+113)F_1(n+1,k) \\ & \quad + 46656(n+1)^2(2n+3)^2F_1(n,k) \\ = & G_1(n,k+1) - G_1(n,k) \end{aligned}$$

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 $G_1(n,k)$.

Proof of Theorem 2 completed

Telescoping

$$\begin{aligned} & F_1(n+2,k) + 24(36n^2+126n+113)F_1(n+1,k) \\ & + 46656(n+1)^2(2n+3)^2F_1(n,k) \\ = & G_1(n,k+1) - G_1(n,k) \end{aligned}$$

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

$$S_1(n) + S_2(n) = 0.$$

hypergeometric indentity

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

$$
\begin{aligned}
&{}_2F_1\left[\begin{matrix}-n,\ 2n+2\\ n+2\end{matrix}\,\middle|\, 3^{-2}\right]\\
&=(-1)^n\,3^{2n+1}\,\frac{(-n+\frac{1}{2})_{2n+1}}{(n+1)_{n+1}\,(n+2)_n}\;{}_2F_1\left[\begin{matrix}n+\frac{3}{2},\ -2n-1\\ -n+\frac{1}{2}\end{matrix}\,\middle|\, 3^{-2}\right].
\end{aligned}
$$

References

- N. Fernando, X. Hou, S. D. Lappano, *A new approach to permutation polynomials over finite fields, II*, Finite Fields Appl. **22** (2013), 122 – 158.
- X. Hou, *A class of permutation binomials over finite fields*, J. Number Theory, to appear.

Thank You!