On a Class of Permutation Polynomials

Christian A. Rodríguez
Alex D. Santos
University of Puerto Rico
Rio Piedras Campus
Department of Computer Science

Abstract

A polynomial $f(x)$ defined over a set A is called a **permutation polynomial** if $f(x)$ acts as a permutation over the elements of A. This is, if $f : A \to A$ is 1-1 and onto. We are studying the coefficients a and b that make polynomials of the form $F_{a,b}(x) = x^{\frac{p+1}{2}} + ax^{\frac{p+5}{6}} + bx$ a permutation polynomial where $a, b \in \mathbb{F}_q^\times$. More specifically we study the family of polynomials: $F_{a,b}(x) = x^{\frac{p+1}{2}} + ax^{\frac{p+5}{6}} + bx$. Our approach in studying $F(x)$ is to use the division algorithm to consider $x = \alpha^n$ where $n = 6k + r, r = 0, ..., 5$. If $F_{a,b}(x)$ is a permutation, this partitions $\mathbb{F}_q^\times$ into 6 classes: $F_{a,b}(\alpha^{6k+r})$ for $r = 0, ..., 5$.

1 Introduction

Let $\mathbb{F}_q$ be the Finite Field with $q = p^r$ elements, where p is a prime. We are studying the coefficients a and b that make polynomials of the form $F_{a,b}(x) = x^{\frac{p+1}{2}} + ax^{\frac{p+5}{6}} + bx$ a permutation polynomial where $a, b \in \mathbb{F}_q^\times$.

It is known that polynomials of the form x^d defined over $\mathbb{F}_q$ permute $\mathbb{F}_q$ if and only if $gdc(d, q-1) = 1$. Also, for polynomials of the form $f(x) = x^{\frac{q+1}{2}} + ax$ defined over $\mathbb{F}_q$ with $a \in \mathbb{F}_q$ if $q = p$ then $f(x)$ is a permutation polynomial if $a^2 - 1$ is a quadratic residue. If $q \neq p$ then $f(x)$ never permutes $\mathbb{F}_q$.

Masuda-Zeive studied polynomials of the form $f(x) = x^{d_1} + ax^{d_2}$ defined

over $\mathbb{F}_p$ with $a \neq 0$ and discovered that if $f(x)$ is a permutation polynomial then $gcd(p-1, d_1 - d_2) > \sqrt{p} - 1$. He also discovered that if $f(x)$ permutes $\mathbb{F}_p$ then $p - 1 \leq (d_1 - 1)max\{d_2, gcd(d_1 - d_2, p - 1)\}$. Note that this second condition only improves on the first when $d_2 = 1$ and $d_1 - 1 \mid p - 1$

It is from these previous results that Francis Castro started studying polynomials of the form $x^{\frac{p-1}{3}} + ax$ and $x^{\frac{p-1}{6}} + ax$, but to no avail. Then he suggested the study of our family of polynomials: $F_{a,b}(x) = x^{\frac{p+1}{2}} + ax^{\frac{p+5}{6}} + bx$

Recall that all elements in $\mathbb{F}_q^\times$ can be expressed as a power of the primitive root $\alpha \in \mathbb{F}_q$. Our approach in studying $F(x)$ is to use the division algorithm to consider $x = \alpha^n$ where $n = 6k + r, r = 0, ..., 5$. If $F_{a,b}(x)$ is a permutation, this partitions $\mathbb{F}_q^\times$ into 6 classes: $F_{a,b}(\alpha^{6k+r})$ for $r = 0, ..., 5$

2 Preliminaries

Definition 1. *A polynomial $f(x)$ defined over a set A is called a **permutation polynomial** if $f(x)$ acts as a permutation over the elements of A. This is, if $f : A \to A$ is 1-1 and onto.*

We study permutation polynomials defined over finite fields $\mathbb{F}_q$. This is, polynomials that permute the elements of $\mathbb{F}_q$

Definition 2. *A **finite field** $\mathbb{F}_q$, $q = p^r$, p prime is a field with q elements.*

Specifically, we study polynomials that permute the elements of the field. This is, polynomials that when evaluated over the field produce all elements in the field.

Our approach in studying these permutation polynomials utilizes two important concepts. The first is primitive roots of finite fields.

Definition 3. *A **primitive root** α of a finite field $\mathbb{F}_q$ is a generator of the multiplicative group $\mathbb{F}_q^\times$*

The second important concept is the Division Algorithm.

Theorem 1 (Division Algorithm)**.** *Given integers a and b, with $b > 0$ there exists unique integers q and r satisfying $a = qb + r$, $0 \leq r < |b|$*

We mentioned that using primitive roots and the division algorithm we could partition $\mathbb{F}_q$ into 6 sets. We now define a notation for these sets.

Definition 4. $A_i = \{F_{a,b}(\alpha^{6k+i}) \mid k = 0, ..., \frac{p-1}{6}\}$

Also note that the elements of each of these sets are either distinct or all 0, as we show in the following lemma:

Lemma 1. *For $i = 1, ..., 5$, either $|A_i| = \frac{p-1}{6}$ or $A_i = \{0\}$*

Proof. Suppose that $F_{a,b}(\alpha^{6k+i}) = F_{a,b}(\alpha^{6l+i})$ with $k < l \leq \frac{p-1}{6}$. Note that:

$$F_{a,b}(\alpha^{6k+i}) = F_{a,b}(\alpha^{6l+i})$$
$$\alpha^{6k+i}((\alpha^{6k+i})^{\frac{p-1}{2}} + a(\alpha^{6k+i})^{\frac{p-1}{6}} + b) = \alpha^{6l+i}((\alpha^{6l+i})^{\frac{p-1}{2}} + a(\alpha^{6l+i})^{\frac{p-1}{6}} + b)$$
$$\alpha^{6k+i}((-1)^i + a(\alpha^{i\cdot\frac{p-1}{6}}) + b) = \alpha^{6l+i}((-1)^i + a(\alpha^{i\cdot\frac{p-1}{6}}) + b)$$

Note that if $((-1)^i + a(\alpha^{i\cdot\frac{p-1}{6}}) + b) = 0$ it is easy to see that $A_i = \{0\}$. Now if we assume that $((-1)^i + a(\alpha^{i\cdot\frac{p-1}{6}}) + b) \neq 0$ then we get:

$$\alpha^{6k+i} = \alpha^{6l+i}$$
$$\alpha^{6k} = \alpha^{6l}$$

This is a contradiction, since $\alpha^i \neq \alpha^j$ for all $i \neq j$, $i, j \leq p-1$. In this case all elements in A_i are distinct and since we have $\frac{p-1}{6}$ elements, then $|A_i| = \frac{p-1}{6}$. □

Lemma 2. *$F_{a,b}(x) = x^{\frac{p+1}{2}} + ax^{\frac{p+5}{6}} + bx$ over $\mathbb{F}_q$ is a permutation polynomial if and only if $A_i \cap A_j = \emptyset$ for all $i \neq j, 0 \leq i, j \leq 5$*

Francis y Yo demostramos el siguiente lemma. La demostracion es bastante sencilla:

Lemma 3. *Let A_i and A_j be two sets as defined previously. It must be the case that either $A_i \cap A_j = \emptyset$ or $A_i = A_j$*

Proof. First we note that if $A_i = A_j = \{0\}$ then the proof is trivial. Now for the case where $|A_i| = |A_j| = \frac{p-1}{6}$, suppose that $A_i \cap A_j$ is not empty. This implies that there exists some $k, l \in \mathbb{F}_q$ such that

$$\alpha^{6k+i}((\alpha^{6k+i})^{\frac{p-1}{2}} + a(\alpha^{6k+i})^{\frac{p-1}{6}} + b) = \alpha^{6l+j}((\alpha^{6l+j})^{\frac{p-1}{2}} + a(\alpha^{6l+j})^{\frac{p-1}{6}} + b)$$

Note that to we can multiply both sides by $\alpha^{6\cdot m}$ for $m = 0, ..., \frac{p-1}{6}$ to get $\frac{p-1}{6}$ distinct elements of the form:

$$\alpha^{6(k+m)+i}((\alpha^{6k+i})^{\frac{p-1}{2}} + a(\alpha^{6k+i})^{\frac{p-1}{6}} + b) = \alpha^{6(l+m)+j}((\alpha^{6l+j})^{\frac{p-1}{2}} + a(\alpha^{6l+j})^{\frac{p-1}{6}} + b)$$

Since we are in the case where $|A_i| = |A_j| = \frac{p-1}{6}$ it follows that $A_i = A_j$ □

3 The number of Permutation Polynomials $x^{\frac{p+1}{2}} + ax^{\frac{p+5}{6}} + bx$ over $\mathbb{F}_q$ is even

In our study of possible pairs (a, b) that produce permutation polynomials, examples we have calculated led us to the following conjecture.

Proposition 1. *Consider the polynomial $F(x)$. If (a, b) produces a permutation, then $(a, -b)$ also produces a permutation.*

In the case of $q = 31$ we have proved this conjecture. We found a correspondence between the classes we defined above by evaluating our polynomial in (a, b) and $(a, -b)$. This way we proved that whenever one of the pairs produces a permutation polynomial, so does the other.

Proof. Let $P_{31}(x, a, b) = x(x^{\frac{p-1}{2}} + ax^{\frac{p-1}{6}} + b)$ defined over $\mathbb{F}_{31}$. We will prove that $P_{31}(\alpha^{6k+i}, a, b) = P_{31}(\alpha^{6l+j}, a, -b)$ where

$$l = \begin{cases} k + 2 \bmod 5, & 0 \leq i \leq 2 \\ k + 3 \bmod 5, & 3 \leq i \leq 5 \end{cases}$$

,

$$j = \begin{cases} i + 3, & 0 \leq i \leq 2 \\ i - 3, & 3 \leq i \leq 5 \end{cases}$$

First note that

$$\begin{aligned} &P_{31}(\alpha^{6k+i}, a, b) \\ &= \alpha^{6k+i}((\alpha^{6k+i})^{\frac{p-1}{2}} + a(\alpha^{6k+i})^{\frac{p-1}{6}} + b) \\ &= \alpha^{6k+i}((-1)^i + a\alpha^{i\frac{p-1}{6}} + b) \end{aligned}$$

Also note that

$$\begin{aligned} 6(k+2) + i + 3 &= 6k + 12 + i + 3 = 6k + i + 15 \\ 6(k+3) + i - 3 &= 6k + 18 + i - 3 = 6k + i + 15 \end{aligned}$$

Finally:

$$
\begin{aligned}
&P_{31}(\alpha^{6l+j}, a, -b) \\
&= -\alpha^{6k+i}((-\alpha^{6k+i})^{\frac{p-1}{2}} + a(-\alpha^6 k + i)^{\frac{p-1}{6}} - b) \\
&= -\alpha^{6k+i}((-1)^{\frac{p-1}{2}}(\alpha^{6k+i})^{\frac{p-1}{2}} + a(-1)^{\frac{p-1}{6}}(\alpha^6 k + i)^{\frac{p-1}{6}} - b) \\
&= -\alpha^{6k+i}(-(-1)^i - a\alpha^{i\frac{p-1}{6}} - b) \\
&= \alpha^{6k+i}((-1)^i + a\alpha^{i\frac{p-1}{6}} + b)
\end{aligned}
$$

□

Our proof utilizes the fact that $\frac{p-1}{2} = \frac{30}{2} = 15$ is odd. In the generalization there must exist another variable that fixes this fact when $\frac{p-1}{2}$ is even.

References

We need to add references.