# On a Class of Permutation Polynomials

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

**Abstract**

El abstract lo dejamos para el final

## 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 $a, b \in \mathbb{F}_q^{\times}$.

1. Results on binomials
2. Francis' motivation to chose $F(x)$

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** $\alpha$ 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 $a = qb + r$, $0 \le r < |b|$*

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.** $A_i = \{F(\alpha^{6k+i}) \mid k = 0, ..., \frac{p-1}{6}\}$

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

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

*Proof.* Falta pasar el proof de esto. □

# 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

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

,

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

First note that

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

Also note that

$$6(k + 2) + i + 3 = 6k + 12 + i + 3 = 6k + i + 15$$
$$6(k + 3) + i - 3 = 6k + 18 + i - 3 = 6k + i + 15$$

Finally:

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

$\square$

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.

3

# References

We need to add references.