Technical Report 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

We are studying the coefficients a and b that make a polynomial a permutation polynomial. Let $p \equiv 1 \bmod 3$. We consider the polynomial $F(x) = x^{\frac{p+1}{2}} + ax^{\frac{p+5}{6}} + bx$ defined over a finite field $\mathbb{F}_q$.

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

Recall that all elements in $\mathbb{F}_q$ 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 $n = 6k + r$. This partitions $F(x)$ into 6 classes:

- $F(\alpha^{6k}) = \alpha^{6k}(1 + a + b)$
- $F(\alpha^{6k+1}) = \alpha^{6k}(-\alpha + a\alpha^{\frac{p+5}{6}} + b\alpha)$
- $F(\alpha^{6k+2}) = \alpha^{6k}(\alpha^2 + a\alpha^{\frac{p+5}{3}} + b\alpha^2)$

- $F(\alpha^{6k+3}) = \alpha^{6k}(-\alpha^3 - a\alpha^3 + b\alpha^3)$
- $F(\alpha^{6k+4}) = \alpha^{6k}(\alpha^4 + a\alpha^{2\frac{p+5}{3}} + b\alpha^4)$
- $F(\alpha^{6k+5}) = \alpha^{6k}(-\alpha^5 + a\alpha^{5\frac{p+5}{6}} + b\alpha^5)$

2 Preliminaries

We study polynomials defined over finite fields.

Definition 1. *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.

Definition 2. *A polynomial* $f(x)$ *defined over* $\mathbb{F}_q$ *is called a* ***permutation polynomial*** *if* $f(x)$ *acts as a permutation over the elements of* $\mathbb{F}_q$*.*

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* $a = qb + r$*,* $0 \leq r < b$

3 The amount of Permutation Polynomials of our class is divisible by 2

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

Conjecture 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

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

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.