Value Sets Of A Class Of Trinomials

Christian A. Rodriguez
Alex D. Santos

Department of Computer Science
University of Puerto Rico, Rio Piedras

December 2, 2013

Table of Contents

1 Introduction

2 Our Problem

3 Results

Polynomials in Finite Fields

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

Definition

Let $f(x)$ be a polynomial defined over a finite field $\mathbb{F}_q$. This is $f : \mathbb{F}_q \to \mathbb{F}_q$.

Example

Consider the polynomial $f(x) = x + 3$ defined over $\mathbb{F}_5$. We have that the domian of f is $\{0, 1, 2, 3, 4\}$.

Value Sets

Definition

Let $f(x)$ be a polynomial defined over a finite field $\mathbb{F}_q$. Then the ***value set*** *of f is defined as $V_f = \{f(a) \mid a \in \mathbb{F}_q\}$*

Example

Consider the polynomial $f(x) = x^2$ defined over $\mathbb{F}_5$. We have that $f(0) = 0, f(1) = 1, f(2) = 4, f(3) = 4, f(4) = 1$, so $V_f = \{0, 1, 4\}$.

Permutation Polynomials

Definition

A polynomial $f(x)$ defined over $\mathbb{F}_q$ is a permutation polynomial if and only if $V_f = \mathbb{F}_q$.

Example

Let $f(x) = x + 3$ defined over $\mathbb{F}_7$. We have that $V_f = \{3, 4, 5, 6, 0, 1, 2\}$ so $f(x)$ is a permutation polynomial over $\mathbb{F}_7$

Example

Let $f(x) = x^2$ defined over $\mathbb{F}_5$. We have that $V_f = \{0, 1, 4\}$ so $f(x)$ is not a permutation polynomial over $\mathbb{F}_5$.

Primitive Roots

Definition

*A **primitive root** $\alpha \in \mathbb{F}_q$ is a generator for the multiplicative group $\mathbb{F}_q^\times$*

Example

Consider $\mathbb{F}_7$. We have that $3^1 = 3, 3^2 = 2, 3^3 = 6, 3^4 = 4$, $3^5 = 5, 3^6 = 1$, so 3 is a primitive root of $\mathbb{F}_7$.

Example

Consider $\mathbb{F}_7$. We have that $2^1 = 2, 2^2 = 4, 2^3 = 1, 2^4 = 2$, $2^5 = 4, 2^6 = 1$, so 2 is not a primitive root of $\mathbb{F}_7$.

Table of Contents

1 Introduction

2 Our Problem

3 Results

Our Polynomial

Let $d_1, d_2 \in \mathbb{F}_q$ such that $d_1 \mid q-1$ y $d_2 \mid q-1$. We are interested in the polynomial:

$$F_{a,b}(x) = x(x^{\frac{q-1}{d_1}} + ax^{\frac{q-1}{d_2}} + b)$$

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

Denote the value set of this polynomial $V_{a,b}$.

Our Polynomial

Let $d_1, d_2 \in \mathbb{F}_q$ such that $d_1 \mid q-1$ y $d_2 \mid q-1$. We are interested in the polynomial:

$$F_{a,b}(x) = x(x^{\frac{q-1}{d_1}} + ax^{\frac{q-1}{d_2}} + b)$$

with $a, b \in \mathbb{F}_q^{\times}$.
Denote the value set of this polynomial $V_{a,b}$.

The class of equivalence (a, b)

Let $a = \alpha^i, b = \alpha^j$ and $\sim$ the relation defined as $(a, b) \sim (a', b')$ $<=> a' = \alpha^{i+h(\frac{q-1}{d_1} - \frac{q-1}{d_2})}, b' = \alpha^{j+h(\frac{q-1}{d_1})}$

Example

The class of equivalence (a, b)

Proposition

The relation $\sim$ defined above is an equivalence relation.

Problem

Our Problem

Study the value set of polynomials of the form $F_{a,b}(x) = x(x^{\frac{q-1}{d_1}} + ax^{\frac{q-1}{d_2}} + b)$ *and determine conditions in* a, b *such that they are permutation polynomials.*

Table of Contents

1 Introduction

2 Our Problem

3 Results

Value set correspondence

Proposition

Let $[a, b]$ *be the class of equivalence of* (a, b). *If* $(a', b') \in [a, b]$, *then* $|V_{a',b'}| = |V_{a,b}|$.

Size of equivalence classes

Proposition

$|[a, b]| = lcm(d_1, d_2)$ where $lcm(x, y)$ is the least common multiple of x and y.

Polynomials with Value sets of the same size

Proposition

The number of polynomials of the form $F_{a,b}(x)$ with $|V_{a,b}| = n$ is a multiple of $|[a, b]|$

Future Work

- Find necessary and sufficient conditions such that $V_{a,b} = \mathbb{F}_q$
- Study our results on the family of polynomials of the form $F_{a,b}(x) = x^m(x^{\frac{q-1}{d_1}} + ax^{\frac{q-1}{d_2}} + b)$