

Value Sets of a Class of Trinomials

Christian A. Rodriguez
Alex D. Santos

Department of Computer Science
University of Puerto Rico, Río Piedras

December 17, 2013

Table of Contents

- 1 Introduction
- 2 Our Problem
- 3 Results

Table of Contents

1 Introduction

2 Our Problem

3 Results

Finite Fields

Definition

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

Example

$$\mathbb{F}_7 = 0, 1, 2, 3, 4, 5, 6$$

Polynomials in Finite Fields

Definition

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

Example

Consider $f(x) = x + 3$ over \mathbb{F}_5 . The domain 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 $f(x) = x^2$ defined over \mathbb{F}_5 . Note:
 $f(0) = 0, f(1) = 1, f(2) = 4, f(3) = 4, f(4) = 1$, 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 $V_f = \mathbb{F}_q$.

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 $f(x) = x + 3$ over \mathbb{F}_5 . Note: $V_f = \{3, 4, 0, 1, 2\}$ so $f(x)$ is a permutation polynomial over \mathbb{F}_5

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 $f(x) = x + 3$ over \mathbb{F}_5 . Note: $V_f = \{3, 4, 0, 1, 2\}$ so $f(x)$ is a permutation polynomial over \mathbb{F}_5

Example

Let $f(x) = x^2$ 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

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 . Since $3^1 = 3, 3^2 = 2, 3^3 = 6, 3^4 = 4, 3^5 = 5, 3^6 = 1$, 3 is a primitive root of \mathbb{F}_7 .

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 . Since $3^1 = 3, 3^2 = 2, 3^3 = 6, 3^4 = 4, 3^5 = 5, 3^6 = 1$, 3 is a primitive root of \mathbb{F}_7 .

Example

Consider \mathbb{F}_7 . Since $2^1 = 2, 2^2 = 4, 2^3 = 1, 2^4 = 2, 2^5 = 4, 2^6 = 1$, 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 $V_{a,b}$.

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

The class of equivalence $[a, b]$

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

Let $a = \alpha^i, b = \alpha^j, \alpha$ a primitive root in \mathbb{F}_q and \sim the relation defined as $(a, b) \sim (a', b')$

$$\iff a' = \alpha^{i+h(\frac{q-1}{d_1} - \frac{q-1}{d_2})}, b' = \alpha^{j+h(\frac{q-1}{d_1})}$$

Example

Let $q = 13, d_1 = 2, d_2 = 3$, then we have $\alpha = 2$ and take $a = 4 = 2^2, b = 8 = 2^3$. Now $(a, b) \sim (a', b')$ if and only if $a' = \alpha^{2+2h}, b' = \alpha^{3+6h}$. For example $(a, b) \sim (3, 5)$

The class of equivalence $[a, b]$

Proposition

The relation \sim defined above is an equivalence relation.

Value set correspondence

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

Lemma

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

Example

Let $q = 13$, $d_1 = 2$, $d_2 = 3$, $a = 4$, $b = 8$. Since $(4, 8) \sim (3, 5)$ we have that $|V_{4,8}| = |V_{3,5}|$

Size of equivalence classes

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

Lemma

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

Example

Let $q = 13$, $d_1 = 2$, $d_2 = 3$, $a = 4$, $b = 8$. Note that $\text{lcm}(2, 3) = 6$. These are the elements of (a, b) :

$$(4, 8), (3, 5), (12, 8), (9, 5), (10, 8), (1, 5), (4, 8)$$

Polynomial Results

Proposition

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

Corollary

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

Future Work

- Study our results on the family of polynomials of the form

$$F_{a,b}(X) = X^m(X^{\frac{q-1}{d_1}} + aX^{\frac{q-1}{d_2}} + b)$$

- Find necessary and sufficient conditions such that

$$V_{a,b} = \mathbb{F}_q$$