Construction of Families of Permutation Trinomials over Finite Fields

Christian A. Rodriguez
Alex D. Santos

Department of Computer Science
University of Puerto Rico, Río Piedras

March 4, 2014

Table of Contents

Table of Contents

Finite Fields

Definition

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

Example

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

Addition:
$2 + 2 = 4$
$4 + 4 = 8 \pmod 7 = 1$

Multiplication:
$2 \cdot 2 = 4$
$4 \cdot 4 = 16 \pmod 7 = 2$

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: $V(f) = \{0, 1, 3, 2, 4\}$ 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: $V(f) = \{0, 1, 3, 2, 4\}$ 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* $\mathbb{F}_q^\times$

$$\mathbb{F}_7$$

Primitive Roots

Definition

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

$$\mathbb{F}_7$$

$$\begin{aligned} 3^1 &= 3 \\ 3^2 &= 2 \\ 3^3 &= 6 \\ 3^4 &= 4 \\ 3^5 &= 5 \\ 3^6 &= 1 \end{aligned}$$

Primitive Roots

Definition

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

$$\mathbb{F}_7$$

$$\begin{aligned} 3^1 &= 3 \\ 3^2 &= 2 \\ 3^3 &= 6 \\ 3^4 &= 4 \\ 3^5 &= 5 \\ 3^6 &= 1 \end{aligned} \qquad\qquad \begin{aligned} 2^1 &= 2 \\ 2^2 &= 4 \\ 2^3 &= 1 \\ 2^4 &= 2 \\ 2^5 &= 4 \\ 2^6 &= 1 \end{aligned}$$

Table of Contents

Our Problem

- Everyting is known about Permutation Monomials
- Permutation Binomials have been studied extensively
- The next case is to study Permutation Trinomials

Our Polynomial

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

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

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

Denote the value set of this polynomial $V(f_{a,b})$.

Our Polynomial

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

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

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

Denote the value set of this polynomial $V(f_{a,b})$.

Problem

Our Problem

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

Table of Contents

The class of equivalence $[a, b]$

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

$a = \alpha^i, b = \alpha^j$, α a primitive root in $\mathbb{F}_q$

The class of equivalence $[a, b]$

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

$a = \alpha^i, b = \alpha^j$, α a primitive root in $\mathbb{F}_q$

$\sim$ defined as $(a, b) \sim (a', b') \iff$

The class of equivalence $[a, b]$

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

$a = \alpha^i, b = \alpha^j$, α a primitive root in $\mathbb{F}_q$

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

The class of equivalence $[a, b]$

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

$a = \alpha^i, b = \alpha^j$, α a primitive root in $\mathbb{F}_q$

$\sim$ defined as $(a, b) \sim (a', b') \iff$

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

$b' = \alpha^{j+h(\frac{q-1}{d_1})}$

The class of equivalence $[a, b]$

$$q = 13$$
$$d_1 = 2$$
$$d_2 = 3$$
$$\alpha = 2$$
$$a = 4 = 2^2$$
$$b = 8 = 2^3$$

The class of equivalence $[a, b]$

$$q = 13$$
$$d_1 = 2$$
$$d_2 = 3$$
$$\alpha = 2$$
$$a = 4 = 2^2$$
$$b = 8 = 2^3$$

$$(2^2, 2^3) \sim (a', b') \iff a' = 2^{2+2h}, b' = 2^{3+6h}$$

The class of equivalence $[a, b]$

$$q = 13$$
$$d_1 = 2$$
$$d_2 = 3$$
$$\alpha = 2$$
$$a = 4 = 2^2$$
$$b = 8 = 2^3$$

$$(2^2, 2^3) \sim (a', b') \iff a' = 2^{2+2h}, b' = 2^{3+6h}$$

Example ($h = 1$): $(2^2, 2^3) \sim (2^4, 2^9)$.

The class of equivalence $[a, b]$

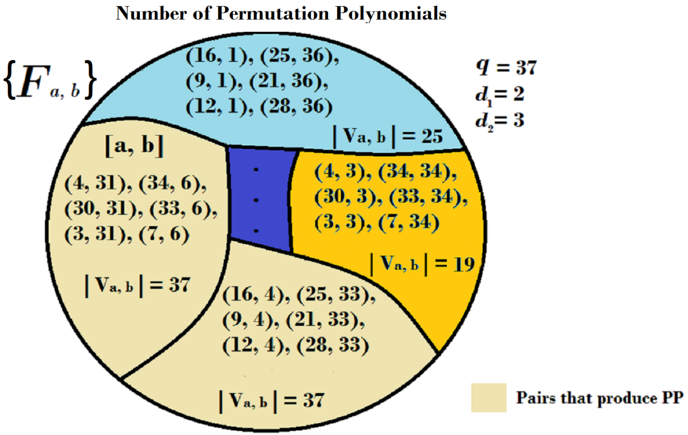
Lemma

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

$f_{a,b}$ with equivalence classes:

$$[f_{a,b}] = [f_{\alpha^i,\alpha^j}] = \{f_{a',b'} \mid (a,b) \sim (a',b')\}$$

Polynomial Results



Value set correspondence

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

Theorem

Suppose that $f_{a,b} \sim f_{a',b'}$ *then* $|V(f_{a,b})| = |V(f_{a',b'})|$.

Example

Let $q = 13, d_1 = 2, d_2 = 3, a = 4, b = 8$. Since $(2^2, 2^3) \sim (2^4, 2^9)$ we have that $|V(f_{2^2,2^3})| = |V(f_{2^4,2^9})|$

Size of equivalence classes

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

Proposition

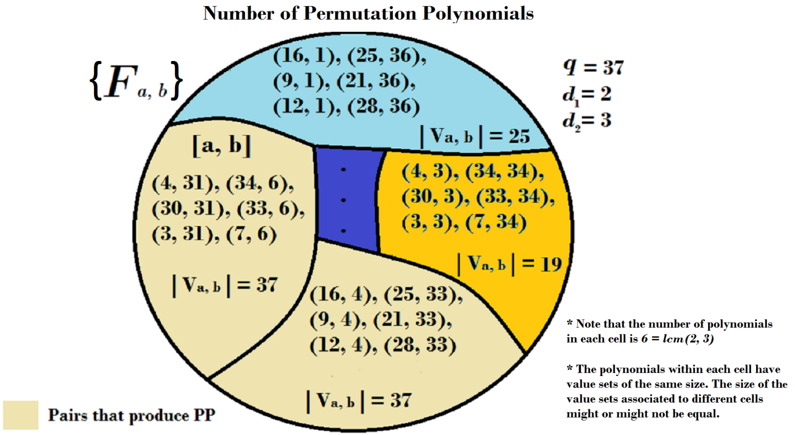
$|[f_{a,b}]| = lcm(d_1, d_2)$ where $lcm(x, y)$ is the least common multiple of x and y.

Example

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

$$(2^2, 2^3), (2^4, 2^9), (2^6, 2^3), (2^8, 2^9), (2^10, 2^3), (2^{12}, 2^9), (2^2, 2^3)$$

Polynomials Results



Polynomial Results

Proposition

The number of polynomials of the form $f_{a,b}(X)$ with $|V(f_{a,b})| = n$ is a multiple of $lcm(d_1, d_2)$

Corollary

The number of permutation polynomials of the form $f_{a,b}(X)$ is a multiple of $lcm(d_1, d_2)$

Future Work

- Find necessary and sufficient conditions such that $V(f_{a,b}) = \mathbb{F}_q$
- Collect data on number of permutation polynomials of the form $f_{a,b}$ for different values of d_1 and d_2 and compare results with number of permutation polynomials.