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

Polynomials in Finite Fields

Value Sets

Permutation Polynomials

Applications:

Primitive Roots

Table of Contents

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

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