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

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 means that the domain of f is equal 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

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

Applications:

Primitive Roots

Definition

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

Example

Consider the finite field $\mathbb{F}_7$. 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 $\mathbb{F}_7$.

Table of Contents

Our Polynomial

The class of equivalence (a, b)

Definirla

The class of equivalence (a, b)

Demostrar que es clase de equivalencia

Problem

Table of Contents

Value set correspondence

Prop 1.4

Size of equivalence classes

Prop 1.5

Polynomials with Value sets of the same size

Prop 1.6 NO ESTA DEMOSTRADA EN EL PAPER

Future Work

Conditions on a, b that provide us with PP. Otras mas.