On a Class of Permutation Polynomials

Christian A. Rodríguez; Alex D. Santos; Ivelisse Rubio; Francis Castro;
Department of Computer Science,
University of Puerto Rico, Rio Piedras Campus

Abstract

Given $q = p^r$, d_1 and d_2, we construct partitions of polynomials of the form $F_{a,b}(X) = X\left(X^{\frac{q-1}{d_1}} + aX^{\frac{q-1}{d_2}} + b\right)$, where $a, b \in \mathbb{F}_q^*$, that have value sets of the same cardinality. As a consequence we provide families of permutation polynomials and of polynomials with small value sets.

Preliminaries

Definition. *A **permutation** of a set A is an ordering of the elements of A. A function $f : A \to A$ gives a permutation of A if and only if f is one to one and onto.*

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

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

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 $\mathbb{F}_7$.*

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

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

Motivation

Binomials that produce permutations of finite fields have been studied extensively. The next case to be studied are trinomials. We have found that within the family of polynomials of the form $F_{a,b}(X) = X\left(X^{\frac{q-1}{d_1}} + aX^{\frac{q-1}{d_2}} + b\right)$, there are many permutation polynomials. We want to find conditions in a, b that guarantee that $F_{a,b}(X)$ is a permutation polynomial and count how many permutation polynomials exist in each family.

Applications

- The encryption operator of some cryptosystems is a permutation of a finite field $\mathbb{F}_q$ and needs to be efficiently computable. Expressing this operator in terms of a polynomial is simple and efficient.
- Polynomials with minimal value sets have been connected with curves with a large number of rational

Problem

Study the value set of polynomials of the form

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

over finite fields $\mathbb{F}_q$ and determine conditions in a, b such that they are permutation polynomials.

Results - Value Sets

Let α be a primitive root of $\mathbb{F}_q$ we define a relation to construct equivalence classes of polynomials with value sets of the same cardinality.

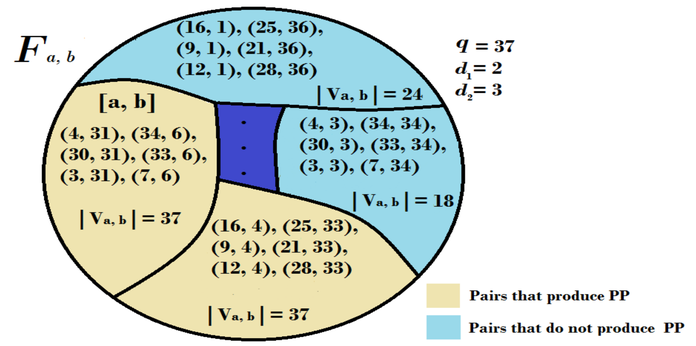
Definition 1. *Let $a = \alpha^i, b = \alpha^j$ and $\sim$ be the relation in $\mathbb{F}_q^* \times \mathbb{F}_q^*$ defined by $(a, b) \sim (a', b') \iff a' = \alpha^{i+h(\frac{q-1}{d_1} - \frac{q-1}{d_2})}, b' = \alpha^{j+h(\frac{q-1}{d_1})}$, where $h \in \mathbb{Z}$.*

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

Lemma 1. *The relation $\sim$ in Def 1 is an equivalence relation in $\mathbb{F}_q^* \times \mathbb{F}_q^*$.*

The equivalence relation defined above induces an equivalence relation in the set of polynomials of the form $F_{a,b}(X) = X(X^{\frac{q-1}{d_1}} + aX^{\frac{q-1}{d_2}} + b)$ with equivalence classes $[F_{a,b}] = [F_{\alpha^i,\alpha^j}] = \left\{ F_{a',b'} | a' = \alpha^{i+h(\frac{q-1}{d_1} - \frac{q-1}{d_2})}, b' = \alpha^{j+h(\frac{q-1}{d_1})} \right\}$. This provides a construction for polynomials with value sets of the same cardinality.

Theorem 1. *Suppose that $F_{a,b} \sim F_{a',b'}$ where $\sim$ is the equivalence relation of Lemma 1. Then $|V(F_{a,b})| = |V(F_{a',b'})|$*



* The polynomials within each cell have value sets of the same size. The size of the value sets associated to different cells might or might not be equal.

Results - Permutation Polynomials

Proposition 1. $|[F_{a,b}]| = lcm(d_1, d_2)$.

Starting from one polynomial we can construct lcm(d_1, d_2) other polynomials.

$$(4, 3), (34, 34), (30, 3), (33, 34), (3, 3), (7, 34)$$

Theorem 2. *The number of polynomials of the form $F_{a,b}(X)$ with $|V_{a,b}| = n$ is a multiple of $lcm(d_1, d_2)$.*

A direct result of Theorem 2 is the specific case where $|V_{a,b}| = q$, when we have permutation polynomials. Also, the construction above provides a way to obtain families of permutation polynomials.

Corollary 1. *The number of permutation polynomials of the form $F_{a,b}(X)$ is a multiple of $lcm(d_1, d_2)$.*

$\mathbb{F}_q$	d_1, d_2	number of pp
$\mathbb{F}_{11}$	1, 2	36
$\mathbb{F}_{11}$	2, 2	46
$\mathbb{F}_{11}$	10, 5	10
$\mathbb{F}_{31}$	5, 1	30
$\mathbb{F}_{31}$	6, 2	18
$\mathbb{F}_{31}$	10, 10	30
$\mathbb{F}_{37}$	2, 3	12
$\mathbb{F}_{37}$	2, 4	132
$\mathbb{F}_{37}$	6, 6	36

Ongoing 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 the possible cardinalities of the value sets.
- Find necessary and sufficient conditions such that $V_{a,b} = \mathbb{F}_q$ and $V_{a,b}$ is of minimal cardinality.
- Collect data on the number of permutation polynomials of this form for different values of d_1 and d_2 and compare results with the number of binomial permutation polynomials.

References

[1] Panario, D., Mullen, G., *Handbook of Finite Fields*. CRC Press (2013).

[2] Wan, D., Lidl, R. *Permutation Polynomials of the Form $x^r f(x^{\frac{q-1}{d}})$ and Their Group Structure*. Mh. Math. 112, 149-163 (1991).

[3] Mullen, G., Stevens H. *Polynomial Functions (mod m)*. Acta Math. Hung.