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

Permutation polynomials over finite fields are important in many applications, for example in cryptography. We want to provide families of polynomials that are rich in permutation polynomials. In particular we study polynomials of the form $F_{a,b}(X) = X(X^{\frac{q-1}{d_1}} + aX^{\frac{q-1}{d_2}} + b)$, where $a, b \in \mathbb{F}_q^*$, $q = p^r$, p prime, and $d \mid (q-1)$.

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 $\mathbb{F}_q^\times$*

Example 4. *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 $\mathbb{F}_q$. Then 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 $V_f = \mathbb{F}_q$.

Example 5. *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 $\mathbb{F}_7$*

Example 6. *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 $f(x)$ is not a permutation polynomial over $\mathbb{F}_5$*

Motivation

Binomials that produce permutations have been studied extensively. The next case to be studied are trinomials. We have found that within the family of polynomials of the form

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

where $d|(q-1)$ there are many permutation polynomials. We want to find conditions in a, b that guarantee that

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

We are interested in studying the coefficients a and b in our polynomial. We define a relation between these coefficients in order to simplify notation.

Definition 1. *Let $a = \alpha^i, b = \alpha^j$, α 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 1. *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 $(a, b) \sim (3, 5)$*

Proposition 1. *The relation $\sim$ defined above is an equivalence relation.*

Lemma 1. *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 2. *Let $q = 13, d_1 = 2, d_2 = 3, a = 4, b = 8$. Since $(4, 8) \sim (3, 5)$ we have that $|V_{4,8}| = |V_{3,5}|$*

Lemma 2. *$|[a, b]| = lcm(d_1, d_2)$ where $lcm(x, y)$ is the least common multiple of x and y.*

Example 3. *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):*

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

Using lemma 1 and lemma 2 we characterize the size of the Value Set of our polynomial.

Proposition 2. *The number of polynomials of the form $F_{a,b}(x)$ with $|V_{a,b}| = n$ is a multiple of $|[a, b]|$*

Corollary 1. *The number of permutation polynomials of the form $F_{a,b}(x)$ is a multiple of $|[a, b]|$*

Results

The following construction shows how to obtain all of the pairs in a particular class of equivalence (a, b) given one of it's members.
Aqui Va la contruccion con el ejemplo anterior

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

Applications

An example of applications of permutation polynomials over finite fields are RSA-type cryptosystems. In some of these systems secret messages are encoded as elements of a field $\mathbb{F}_q$ with a sufficiently large q. The encryption operator used for these systems is a permutation of the field $\mathbb{F}_q$ and needs to be efficiently computable. It is easy to see that expressing this operator in terms of a permutation polynomial is simple and efficient.

References

- Lidl, Rudolf, and Harald Niederreiter. *Finite Fields*. Reading, Mass.: Addison-Wesley Pub. Co., Advanced Book Program/World Science Division, 1983. Print.
- 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).
- Mullen, G., Stevens H. *Polynomial Functions (mod m)*. Acta Math. Hung. 44(3-4) (1984), 237-241.