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 $F_{a,b}(x) = x^{\frac{q+1}{2}} + ax^{\frac{q+1}{d}} + bx$, 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 2. *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 3. *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 $\mathbb{F}_7$*

Motivation

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

$$F_{a,b}(x) = x^{\frac{q+1}{2}} + ax^{\frac{q+1}{d}} + bx$$

there are many permutation polynomials. We want to find conditions in $[a, b]$ that garanty that the polynomial is a permutation polynomial, and to count how many there are.

Problem

To determine conditions in a, b such that polynomials of the form

$$F_{a,b}(x) = x^{\frac{q+1}{2}} + ax^{\frac{q+1}{d}} + bx$$

over a finite field $\mathbb{F}_q$ with $a, b \in \mathbb{F}_q$ and $d \mid q-1$ are permutation polynomials and determine how many there are for each d.

Results

The following theorem gives information on the amount of polynomials with the same value set.

Theorem 1. *Fix $n \in \mathbb{N}$, $n \leq q$. The number of polynomials of the form $F_{a,b}(x)$ with $\left|V_{F_{a,b}}\right| = n$ is a multiple of d if d is even, or a multiple of $2d$ if d is odd.*

Our main result on permutation polynomials follows as a result of this theorem.

Corollary 1. *The number of permutation polynomials over $\mathbb{F}_q$ of the form $F_{a,b}(x)$ is a multiple of d if d is even, or a multiple of $2d$ if d is odd.*

Given coeffcients $[a, b]$ for which $F_{a,b}(x)$ is a permutation polynomial of $\mathbb{F}_q$, we can construct a list of d or $2d$ coefficients $[a', b']$ such that $F_{a',b'}(x)$ are also permutation polynomials of $\mathbb{F}_q$ as follows:

Construction: Let $d|(q-1)$, d odd, and $F_{a,b}(x) = x^{\frac{q+1}{2}} + ax^{\frac{q+1}{d}} + bx$ a permutation polynomial of $\mathbb{F}_q$, where $a = \alpha^i$, $b = \alpha^j$. Then $F_{a',b'}(x)$ is also a permutation polynomial for $[a', b'] \in \left\{\alpha^{i+k(d+2)\frac{q-1}{2d}}, \alpha^{j+k\frac{q-1}{2}} \mid k = 1, ..., 2d-1\right\}$

Example 1. *Fix $d = 3$ and $q = 37$. We know that $F_{4,31}(x) = x^{19} + 4x^{\frac{38}{3}} + 31x$ is a permutation polynomial over $\mathbb{F}_{37}$, and there are 12 permutation polynomials of this form. Since $4 = 2^2 = \alpha^2, 31 = 2^9 = \alpha^9$, we obtain 5 pairs $[a', b']$ and new permutation polynomials $F_{a',b'}(x)$ using our construction:*

$[7 = \alpha^{2+5\cdot 6}, 6 = \alpha^{9+18}]$, $[3 = \alpha^{2+2(5\cdot 6)}, 31 = \alpha^{9+2(18)}]$,
$[33 = \alpha^{2+3(5\cdot 6)}, 6 = \alpha^{9+3(18)}]$, $[30 = \alpha^{2+4(5\cdot 6)}, 31 = \alpha^{9+4(18)}]$,

Applications

Permutations of finite fields have many applications in Coding Theory and Cryptography. One such example is 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 defined as a permutation of the field $\mathbb{F}_q$ with the decryption operator defined as the inverse of this permutation. Both of these operators need to be efficiently computable, thus it is easy to see that expressing these operators in terms of permutation polynomials is simple and efficient.

Ongoing Work

Once we have one permutation polynomial, we can construct d or $2d$ of them (depending on the parity of d). We now need to characterize which polynomials $F_{a,b}(x)$ are permutation polynomials. For this, we are studying the size of the value sets of $F_{a,b}(x)$. We divide the value set into subsets:

Definition. *Let $F_{a,b}(x) = x^{\frac{q+1}{2}} + ax^{\frac{q+1}{d}} + bx$ be a polynomial defined over $\mathbb{F}_q$ where $d \mid q-1$. We define the sets $A_l = \left\{F_{a,b}(\alpha^{dk+i}) \mid k = 0, ..., \frac{q-1}{d}\right\}$ for $i = 0, ..., d-1$, where α is a primitive root of $\mathbb{F}_q$.*

For these subsets we have proved the following lemmas

Lemma 1. *Let $F_{a,b}(x)$ be defined over $\mathbb{F}_q$ and A_l be defined as above. We have that $|A_l| = \frac{q-1}{d}$ or $A_l = \{0\}$*

Lemma 2. *Let $F_{a,b}(x)$ be defined over $\mathbb{F}_q$. The sets A_l defined above are such that, for $l \neq k$, $A_l \cap A_k = \emptyset$ or $A_l = A_k$.*

Proposition 1. *Let $F_{a,b}(x)$ be defined over $\mathbb{F}_q$ and A_l be defined as above. $F_{a,b}(x)$ is a permutation polynomial if and only if $A_l \cap A_k = \emptyset$ for $0 \leq l, k \leq d-1$.*

Aim:

- Find necessary and sufficient conditions on the coefficients $a = \alpha^i, b = \alpha^j$ such that $A_l \cap A_k = \emptyset$
- Study our results on the family of polynomials of the form $F_{a,b}(x) = x^{\frac{q+1}{2}+m} + ax^{\frac{q+1}{d}+m} + bx^m$

References

The source code and compiled executables with an interactive interface are available at
http://www.cs.unibas.ch/personen/amberg