On a Class of Permutation Polynomials

Christian A. Rodríguez & Alex D. Santos
University of Puerto Rico, Rio Piedras
Department of Computer Science

Abstract

Permutation polynomias over finite fields are important in many applications, for example in cryptography. We want to provide rich families of polynomials that are permutation polynomials. In particular we study polynomials of the form $F_{a,b}(x) = x^{\frac{q+1}{2}} + a \cdot x^{\frac{q-1}{d}} + b \cdot x$ 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 1. *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 $V_f = \{f(a) \mid a \in \mathbb{F}_q\}$*

Definition. *Consider a finite field $\mathbb{F}_q$. A polynomial $f(x)$ defined over $\mathbb{F}_q$ is said to be a permutation polynomial if $V_f = \mathbb{F}_q$.*

Example 2. *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 $\mathbb{F}_7$*

Problem

We study the number of polynomials of the form $F_{a,b}(x) = x^{\frac{q+1}{2}} + a \cdot x^{\frac{q+1}{d}} + b \cdot x$ over finite fields that are permutation polynomials.

Value set of a class of polynomials

Our interest is studying the value set of a specific class of permutation polynomials. The class of polynomials we consider is defined as follows:

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

Where $a, b \in \mathbb{F}_q$ and $d \mid q-1$. More formally, we would like to characterize the value set V_F of $F_{a,b}(x)$ based on the parameters a and b. It is easy to see that $F_{a,b}(0) = 0 \; \forall a, b \in \mathbb{F}_q$, it follows that 0 is always in V_F. For a fixed pair a, b we separate $V_F \setminus \{0\}$ into smaller subsets in the following way:

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

Using properties of these sets we will characterize V_F. First we would like to note that for $i \neq j$ the sets A_i and A_j are either equal, or distinct.

Lemma 1. *Let $F_{a,b}(x)$ be defined over $\mathbb{F}_q$. For two sets A_i and A_j we must have that either $A_i \cap A_j = \emptyset$ or $A_i = A_j$.*

Lemma 1 provides an immediate characterization of the value set and insight on conditions to make $F_{a,b}(x)$ a permutation polynomial. In our studies we also determine the size of the sets A_i.

Lemma 2. *Let $F_{a,b}(x)$ be defined over $\mathbb{F}_q$ and A_i be defined as above. We have that $|A_i| = \frac{q-1}{d}$ or $A_i = \{0\}$*

Now we are also interested in correlations between the pairs a, b and the value sets of distinct polynomials of the for $F_{a,b}(x)$. We proved a lemma that gives us a correspondence among some of these polynomials. In other words, these polynomials have the same value set.

Lemma 3. *Let $F_{a,b}(x)$ defined over $\mathbb{F}_q$ and let α denote a primitive root of $\mathbb{F}_q$. If we write $a = \alpha^i$ and $b = \alpha^j$ then we have that*

$$F_{\alpha^i,\alpha^j}(\alpha^k) = -\alpha \cdot F_{\alpha^{i+(d+2)\cdot\frac{q-1}{2d}},\alpha^{j+\frac{q-1}{2}}}(\alpha^{k-1})$$

From lemma 1 we know that for a fixed polynomial the sets A_i are either distinct or equal. Finally from lemma 3 we have that up to $2d$ distinct polynomials of the form $F_{a,b}(x)$ have the same value set. This information gives us the following theorem:

Proposition 1. *Let $F_{a,b}(x)$ be defined over $\mathbb{F}_q$. Then we have that the amount of polynomials of the form $F_{a,b}(x)$ such that $|V_F| = r \cdot \frac{q-1}{d} + 1, r \leq d$ is divisible by $2d$ when d is odd and by d otherwise.*

Conditions for permutations of the from $F_{a,b}($

Permutation polynomials over finite fields are polynomials whose value set is equal to the field. Using our previous results we present work on when the family of polynomials of the form $F_{a,b}(x)$ is a permutation polynomial.
If we define the value set V_F in terms of the sets A_i then it follows from lemma 1 that all of the elements between these sets should *cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.*

Also, a particular case of proposition 1 is the case when $r = d$ and $|V_F| = q$, or $V_F = \mathbb{F}_q$. This case is exactly when $F_{a,b}(x)$ is a permutation polynomial over $\mathbb{F}_q$. And so it is easy to see that corollary 1 follows easily from proposition 1.

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.

Future Work

- Verify if our results work for polynomials of the form

$$F_{a,b}(x) = x^{\frac{q+1}{2}+m} + a \cdot x^{\frac{q+1}{d}+m} + b \cdot x^m \quad (1)$$

  where $m \in \mathbb{F}_q$

- Verify if there exist conditions for the pair $[a, b]$ such that 1 & **??** are permutation polynomials.

References

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