



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 $F_{a,b}(x) = x^{\frac{q-1}{2}} + ax^{\frac{q+d-1}{d}} + bx$, 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 $f : A \rightarrow A$ 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 3. 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 4. 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

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

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

where $d \mid (q-1)$ 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.

PROBLEM

Study the value set of polynomials of the form

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

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 $a = \alpha^i, b = \alpha^j$ 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 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 $(a, b) \sim (3, 5)$

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

This equivalence relation links the coefficients $[a, b]$ to the Value Sets of our polynomials. The equivalence relation defined in Def 1 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 $[F_{a,b}] = [F_{\alpha^i, \alpha^j}] = \left\{ F_{a',b'} \mid a' = \alpha^{i+h(\frac{q-1}{d_1}-\frac{q-1}{d_2})}, b' = \alpha^{j+h(\frac{q-1}{d_1})} \right\}$

Lemma 2. Suppose that $F_{a,b} \sim F_{a',b'}$ where \sim is the relationship defined in Definition 1. Then $|V(F_{a,b})| = |V(F_{a',b'})|$

Example 2. Let $q = 13, d_1 = 2, d_2 = 3, a = 4, b = 8$. Since $(4, 8) \sim (3, 5)$ we have that $|V(F_{4,8})| = |V(F_{3,5})|$. In fact $V(F_{4,8}) = \{0, 1, 2, 3, 10, 11, 12\}$, $V(F_{3,5}) = \{0, 2, 4, 6, 7, 9, 11\}$. Note that even though the sizes are equal the value sets are not.

Lemma 3. $|[F_{a,b}]| = \text{lcm}(d_1, d_2)$.

RESULTS

Example 5. Let $q = 13, d_1 = 2, d_2 = 3, a = 4, b = 8$. Note that $\text{lcm}(2, 3) = 6$. These are the elements of $F_{a,b}$:

$$F_{4,8}, F_{3,5}, F_{12,8}, F_{9,5}, F_{10,8}, F_{1,5}, F_{4,8}$$

Using all of our previous lemmas we can provide some information about the number of polynomials of the form $F_{a,b}(X)$ with a specific size of value set.

Proposition 1. 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 $|[a, b]|$

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 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.