On a Class of Permutation Polynomials over Finite Fields

November 18, 2013

Abstract

Permutation polynomials over finite fields are important in many applications, for example in coding theory and cryptography. Our goal is to provide families of polynomials that are rich in permutation polynomials, and study polynomials of the form $F_{a,b}(X) = X^m \left(X^{\frac{q-1}{2}} + aX^{\frac{q-1}{d}} + b \right)$, where $a, b \in F_q$, $q = p^r$, p prime, and $d \mid (q-1)$. We prove that the number of polynomials of the form $F_{a,b}(X)$ with value set of size $\left|V_{F_{a,b}}\right| = n$ is a multiple of d if d is even, or a multiple of $2d$ if d is odd and give a construction where, given a permutation polynomial $F_{a,b}(X)$ of $\mathbb{F}_q$, we can construct a list of d or $2d$ coefficients a', b' such that $F_{a',b'}(X)$ is also a permutation polynomial of $\mathbb{F}_q$.

1 Introduction

Permutation polynomials over finite fields are important in many applications, for example in cryptography. Binomials that produce permutations have been studied extensively. The next case to be studied are trinomials. We want to provide families of polynomials that are rich in permutation polynomials. 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 $d|(q-1)$ 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.

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.

2 Preliminaries

Definition 2.1. 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 2.2. A **finite field** $\mathbb{F}_q$, $q = p^r$, p prime, is a field with $q = p^r$ elements.

Definition 2.3. A **primitive root** $\alpha \in \mathbb{F}_q$ is a generator for the multiplicative group $\mathbb{F}_q^\times$

Example 2.4. 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 2.5. 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 2.6. 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 $\mathbb{F}_7$

3 Results

3.1 Counting permutation polynomials

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

Theorem 3.1. *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.*

Proof. We establish a correspondence between values $F_{a,b}(\alpha^k)$ of $F_{a,b}(x)$ and values $F_{a',b'}(\alpha^l)$ of $F_{a',b'}(x)$. We will show that $F_{a,b}(\alpha^k) = -\alpha \cdot F_{a',b'}(\alpha^l)$ for $k \in \{1, ..., q-1\}$, where $l = k-1$, $a' = a \cdot \alpha^{(d+2)(\frac{q-1}{2d})}$, $b' = b \cdot \alpha^{(\frac{q-1}{2})}$, α a primitive root in $\mathbb{F}_q$. Let $a = \alpha^i$, $b = \alpha^j$. Then $F_{a,b}(\alpha^k) = \alpha^k((\alpha^k)^{\frac{q-1}{2}} + \alpha^i(\alpha^k)^{\frac{q-1}{d}} + \alpha^j)$. Note that:

$$
\begin{aligned}
&F_{\alpha^{i+(d+2)\frac{q-1}{2d}}, \alpha^{j+\frac{q-1}{2}}}(\alpha^l) = \alpha^l((\alpha^l)^{\frac{q-1}{2}} + (\alpha^{i+(d+2)\frac{q-1}{2d}}) \cdot (\alpha^l)^{\frac{q-1}{d}} + \alpha^{j+\frac{q-1}{2}}) \\
&= -\alpha^l(-(\alpha^{\frac{q-1}{2}})^l + (-\alpha^i)(\alpha^{(d+2)\frac{q-1}{2d}}) \cdot (\alpha^l)^{\frac{q-1}{d}} + \alpha^j) \\
&= -\alpha^l(-(-1)^l + (-\alpha^i)(\alpha^{\frac{q-1}{2}+\frac{q-1}{d}}) \cdot (\alpha^l)^{\frac{q-1}{d}} + \alpha^j) \\
&= -\alpha^l(-(-1)^l + (-\alpha^{i+\frac{q-1}{2}})(\alpha^{\frac{q-1}{d}}) \cdot (\alpha^{\frac{lq-l}{d}}) + \alpha^j) \\
&= -\alpha^l(-(-1)^l + (-\alpha^{i+\frac{q-1}{2}})(\alpha^{\frac{q-1}{d}}) \cdot (\alpha^{\frac{lq-l}{d}}) + \alpha^j) \\
&= -\alpha^l(-(-1)^l + (\alpha^i)(\alpha^{l+1})^{\frac{q-1}{d}} + \alpha^j)
\end{aligned}
$$

$= -\alpha^{k-1}(-(-1)^{k-1} + (\alpha^i)(\alpha^k)^{\frac{q-1}{d}} + \alpha^j)$ with $k = l+1$ and $l = k-1$
$= C \cdot \alpha^k((-1)^k + (\alpha^i)(\alpha^k)^{\frac{q-1}{d}} + \alpha^j)$ where $C = -\alpha^{-1}$

In general for each term of $F_{a,b}(\alpha^k)$ there is going to be a correspondant term of $F_{a',b'}(\alpha^l)$ where $a' = \alpha^{i+(d+2)\frac{q-1}{2d}}$ and $b' = \alpha^{j+\frac{q-1}{2}}$. Moreover it must be the case that $\left|V_{F_{a,b}}\right| = \left|V_{F_{a',b'}}\right|$.

Note that we can repeat this process using $a'' = a' \cdot \alpha^{(d+2)(\frac{q-1}{2d})}$, $b'' = b' \cdot \alpha^{(\frac{q-1}{2})}$. We argue that this process can be repeated at most $d-1$ times when d is even, and $2d-1$ times when d is odd.

If d is even then we can construct a chain of d pairs $[a,b] \in \left\{\alpha^{i+m(d+2)\frac{q-1}{2d}}, \alpha^{j+m\frac{q-1}{2}} \mid m = 0, ..., d-1\right\}$ such that $F_{a,b}(x)$ has the same size value set for all pairs. When $m = d$ we have that $a = \alpha^{i+(d)(d+2)(\frac{q-1}{2d})} = \alpha^{i+(d+2)(\frac{q-1}{2})} = \alpha^{i+(d)(\frac{q-1}{2})+(q-1)} = \alpha^i$ and $b = \alpha^{j+d\frac{q-1}{2}} = \alpha^j$.

If d is odd we construct a chain of $2d$ pairs $[a,b] \in \left\{\alpha^{i+m(d+2)\frac{q-1}{2d}}, \alpha^{j+m\frac{q-1}{2}} \mid m = 0, ..., 2d-1\right\}$ such that $F_{a,b}(x)$ has the same size value set for all pairs. When $m = 2d$ we have that $a = \alpha^{i+(2d)(d+2)(\frac{q-1}{2d})} = \alpha^{i+(d+2)(q-1)} = \alpha^{i+(d)(q-1)+(2)(q-1)} = \alpha^i$ and $b = \alpha^{j+2d\frac{q-1}{2}} = \alpha^{j+q-1} = \alpha^j$.

Now if we have a polynomial of the form $F_{a,b}(x)$ with $\left|V_{F_{a,b}}\right| = n$ we can construct d or $2d$ distinct pairs $[a,b]$ such that we get polynomials with the same size value set, depending on the parity of d. Therefore 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. □

Corollary 3.2. 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 coefficients $[a,b]$ 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 $F_{a',b'}(x)$ is also permutation polynomial of $\mathbb{F}_q$ using theorem 3.1 as follows:

Construction 3.3. Let $d|(q-1), d$ odd, and $F_{a,b}(x) = x^{\frac{q+1}{2}} + ax^{\frac{q+d-1}{d}} + bx$ be 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 3.4. Fix $d = 3$ and $q = 43$. There exists 48 pairs $[a,b]$ such that $F_{a,b}(x) = x^{22} + ax^{15} + bx$. In particular, we know that $F_{1,17}(x) = x^{22} + 1x^{15} + 17x$ is a permutation polynomial over $\mathbb{F}_{43}$. Using $1 = 3^{42} = \alpha^{42}, 17 = 3^{38} = \alpha^{38}$, we obtain 5 other pairs $[a',b']$ and new permutation polynomials $F_{a',b'}(x)$ using our construction:

$$[7 = \alpha^{42+5\cdot 7}, 26 = \alpha^{38+21}], [6 = \alpha^{42+2(5\cdot 7)}, 17 = \alpha^{38+2(21)}],$$
$$[42 = \alpha^{42+3(5\cdot 7)}, 26 = \alpha^{38+3(21)}],$$
$$[36 = \alpha^{42+4(5\cdot 7)}, 17 = \alpha^{38+4(21)}],$$
$$[37 = \alpha^{42+5(5\cdot 7)}, 26 = \alpha^{38+5(21)}]$$

Knowing a permutation polynomial we can construct d or $2d$ of them (depending on the parity of d). We still need to characterize which polynomials are permutation polynomials. For this, we are studying the size of the value sets of $F_{a,b}(x)$.

3.2 Size of the value set

We divide the value set into subsets:

Definition 3.5. Let $F_{a,b}(x) = x^{\frac{q+1}{2}} + ax^{\frac{q+d-1}{d}} + bx$ be a polynomial defined over $\mathbb{F}_q$, where $d \mid (q-1)$. We define the sets $A_l = \left\{F_{a,b}(\alpha^{dk+l}) \mid k = 0, ..., \frac{q-1}{d}\right\}$ for $l = 0, ..., d-1$, where α is a primitive root of $\mathbb{F}_q$.

For these subsets we have proved the following lemmas

Lemma 3.6. *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 $A_l = \{0\}$*

Proof. Suppose that $F_{a,b}(\alpha^{dk+i}) = F_{a,b}(\alpha^{dl+i})$ with $k < l \leq \frac{q-1}{d}$. Note that:

$$F_{a,b}(\alpha^{dk+i}) = F_{a,b}(\alpha^{dl+i})$$
$$\alpha^{dk+i}((\alpha^{dk+i})^{\frac{q-1}{2}} + a(\alpha^{dk+i})^{\frac{q-1}{d}} + b) = \alpha^{dl+i}((\alpha^{dl+i})^{\frac{q-1}{2}} + a(\alpha^{dl+i})^{\frac{q-1}{d}} + b)$$
$$\alpha^{dk+i}((-1)^i + a(\alpha^{i\cdot\frac{q-1}{d}}) + b) = \alpha^{dl+i}((-1)^i + a(\alpha^{i\cdot\frac{q-1}{d}}) + b)$$

Also note that if $((-1)^i + a(\alpha^{i\cdot\frac{q-1}{d}}) + b) = 0$ it is easy to see that $A_l = \{0\}$. Now if we assume that $((-1)^i + a(\alpha^{i\cdot\frac{q-1}{d}}) + b) \neq 0$ then we get:

$$\alpha^{dk+i} = \alpha^{dl+i}$$
$$\alpha^{dk} = \alpha^{dl}$$

This is a contradiction, since $\alpha^i \neq \alpha^j$ for all $i \neq j$, $i, j \leq q-1$. In this case all elements in A_l are distinct and since we have $\frac{q-1}{d}$ elements, then $|A_l| = \frac{q-1}{d}$. □

Lemma 3.7. *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 $A_l = A_k$.*

Proof. First we note that if $A_k = A_l = \{0\}$ then the proof is trivial. Now for the case where $|A_k| = |A_l| = \frac{q-1}{d}$, suppose that $A_k \cap A_l$ is not empty. This implies that there exists some $k, l \in \mathbb{F}_q$ such that

$$\alpha^{dk+i}((\alpha^{dk+i})^{\frac{q-1}{2}} + a(\alpha^{dk+i})^{\frac{q-1}{d}} + b) = \alpha^{dl+j}((\alpha^{dl+j})^{\frac{q-1}{2}} + a(\alpha^{dl+j})^{\frac{q-1}{d}} + b)$$

Note that to we can multiply both sides by $\alpha^{d\cdot m}$ for $m = 0, ..., \frac{q-1}{d}$ to get $\frac{q-1}{d}$ distinct elements of the form:

$$\alpha^{d(k+m)+i}((\alpha^{dk+i})^{\frac{q-1}{2}} + a(\alpha^{qk+i})^{\frac{q-1}{d}} + b) = \alpha^{d(l+m)+j}((\alpha^{dl+j})^{\frac{q-1}{2}} + a(\alpha^{dl+j})^{\frac{q-1}{d}} + b)$$

Since we are in the case where $|A_k| = |A_l| = \frac{q-1}{d}$ it follows that $A_k = A_l$ □

Proposition 3.8. 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 $A_l \neq \{0\}$ and $A_l \cap A_k = \emptyset$ for $0 \leq l, k \leq d-1$.

3.3 Future work

- Find necessary and sufficient conditions on the coefficients $a = \alpha^i$, $b = \alpha^j$ such that $A_l \neq \{0\}$ and $A_l \cap A_k = \emptyset$
- Study our results on the family of polynomials of the form $F_{a,b}(x) = x^{\frac{q-1}{2}+m} + ax^{\frac{q-1}{d}+m} + bx^m$