On a Class of Permutation Polynomials over Finite Fields

December 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 $F_{a,b}(X) = X^m \left(X^{\frac{q-1}{d_1}} + aX^{\frac{q-1}{d_2}} + b \right)$, where $a, b \in F_q$, $q = p^r$, p prime, $d_1 \mid (q-1)$ and $d_2 \mid (q-1)$. 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 $lcm(d_1, d_2)$ and give a construction where, given a permutation polynomial $F_{a,b}(X)$ of $\mathbb{F}_q$, we can construct a list of $lcm(d_1, d_2)$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

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

where $d_1|(q-1)$ and $d_2|(q-1)$ 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

Definition 3.1. Let $d_1, d_2 \in \mathbb{F}_p$ such that $d_1 \mid p$ and $d_2 \mid p$. We define the polynomial $F_{a,b}(x) = x(x^{\frac{p-1}{d_1}} + ax^{\frac{p-1}{d_2}} + b)$ with $a, b \in \mathbb{F}_q^\times$ and $V_{a,b} = Im(F_{a,b}(x))$.

Definition 3.2. Let $a = \alpha^i, b = \alpha^j$ and $\sim$ be the relation defined by $(a, b) \sim (a', b') \iff a' = \alpha^{i+h(\frac{p-1}{d_1} - \frac{p-1}{d_2})}, b' = \alpha^{j+h(\frac{p-1}{d_1})}$

Example 3.3. 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 3.4. $\sim$ defined above is a equivalence relation.

Proof. 1. Let $a = \alpha^i$, $b = \alpha^j$ and choose $h = 0$. Then $a' = \alpha^{i+0(\frac{p-1}{d_1} - \frac{p-1}{d_2})} = \alpha^i = a$ and $b' = \alpha^{j+0(\frac{p-1}{d_1})} = \alpha^j = b$. Therefore $(a, b) \sim (a, b)$ and the relation is reflexive.

2. Let $a = \alpha^i$, $b = \alpha^j$, $a' = \alpha^{i+h(\frac{p-1}{d_1} - \frac{p-1}{d_2})}$ y $b' = \alpha^{j+h(\frac{p-1}{d_1})}$ then $(a, b) \sim (a', b')$. We want to find l such that $a = \alpha^{i+h(\frac{p-1}{d_1} - \frac{p-1}{d_2})+l(\frac{p-1}{d_1} - \frac{p-1}{d_2})}$ y $b = \alpha^{j+h(\frac{p-1}{d_1})+l(\frac{p-1}{d_1})}$. Choose $l = d_1 d_2 - h$, then we obtain: $\alpha^{i+d_1 d_2(\frac{p-1}{d_1} - \frac{p-1}{d_2})} = \alpha^i = a$ and $\alpha^{j+d_1 d_2(\frac{p-1}{d_1})} = \alpha^j = b$. Therefore $(a', b') \sim (a, b)$ and the relation is symmetric.

3. Suppose that $a = \alpha^i$, $b = \alpha^j$, $a' = \alpha^{i+h(\frac{p-1}{d_1}-\frac{p-1}{d_2})}$, $b' = \alpha^{j+h(\frac{p-1}{d_1})}$, $a'' = \alpha^{i+h(\frac{p-1}{d_1}-\frac{p-1}{d_2})+l(\frac{p-1}{d_1}-\frac{p-1}{d_2})}$, $b'' = \alpha^{j+h(\frac{p-1}{d_1})+l(\frac{p-1}{d_1})}$. Therefore $(a,b) \sim (a',b')$ and $(a',b') \sim (a'',b'')$. Note that $a'' = \alpha^{i+(h+l)(\frac{p-1}{d_1}-\frac{p-1}{d_2})}$, $b'' = \alpha^{j+(h+l)(\frac{p-1}{d_1})}$, therefore $(a,b) \sim (a'',b'')$ and the relation is transitive.

In conclusion the relation is an equivalence relation.

□

Proposition 3.5. Let $[a,b]$ bet the equivalence relation (a,b). If $(a',b') \in [a,b]$, then $|V_{a',b'}| = |V_{a,b}|$

Proof. Let α be the primitive root of the finite field.

$$F_{a',b'}(\alpha^{k+1}) = \alpha^{k+1}((\alpha^{k+1})^{\frac{p-1}{d_1}} + \alpha^{i+\frac{p-1}{d_1}-\frac{p-1}{d_2}}(\alpha^{k+1})^{\frac{p-1}{d_2}} + \alpha^{j+\frac{p-1}{d_1}})$$

$$= \alpha^{k+1}((\alpha^k)^{\frac{p-1}{d_1}} \cdot \alpha^{\frac{p-1}{d_1}} + \alpha^i \cdot \frac{\alpha^{\frac{p-1}{d_1}}}{\alpha^{\frac{p-1}{d_2}}}(\alpha^k)^{\frac{p-1}{d_2}} \cdot \alpha^{\frac{p-1}{d_2}} + \alpha^j \cdot \alpha^{\frac{p-1}{d_1}})$$

$$= \alpha^{\frac{p-1}{d_1}+1} \cdot \alpha^k((\alpha^k)^{\frac{p-1}{d_1}} + \alpha^i(\alpha^k)^{\frac{p-1}{d_2}} + \alpha^j)$$

$$= C \cdot F_{a,b}(\alpha^k), \text{donde } C = \alpha^{\frac{p-1}{d_1}+1}$$

In general for each element of $F_{a,b}(\alpha^k)$ there will be a corresponding term of $F_{a',b'}(\alpha^{k+1})$ where $a' = \alpha^{i+h(\frac{p-1}{d_1}-\frac{p-1}{d_2})}$ y $b' = \alpha^{j+h(\frac{p-1}{d_1})}$. Moreover, it should be the case that $\left|V_{F_{a,b}}\right| = \left|V_{F_{a',b'}}\right|$.

Let $f : V_{a',b'} \to \alpha^{\frac{p-1}{d_1}} V_{a,b}$ given by $f(F_{a',b'}(\alpha^{k+1})) = \alpha^{\frac{p-1}{d_1}+1} F_{a,b}(\alpha^k)$. Suppose that $f(F_{a',b'}(\alpha^{k_1+1})) = f(F_{a',b'}(\alpha^{k_2+1}))$ where $k_1, k_2 \in \mathbb{F}_q$.

Consider $f(F_{a',b'}(\alpha^{k_1+1}))$

$$= f(\alpha^{k_1+1}((\alpha^{k_1+1})^{\frac{p-1}{d_1}} + \alpha^i(\alpha^{k_1+1})^{\frac{p-1}{d_2}} + \alpha^j))$$

$$= \alpha^{\frac{p-1}{d_1}+1}(\alpha^{k_1}((\alpha^{k_1})^{\frac{p-1}{d_1}} + \alpha^i(\alpha^{k_1})^{\frac{p-1}{d_2}} + \alpha^j))$$

$$= \alpha^{k_1+1}(\alpha^{\frac{p-1}{d_1}}((\alpha^{k_1})^{\frac{p-1}{d_1}} + \alpha^i(\alpha^{k_1})^{\frac{p-1}{d_2}} + \alpha^j))$$

$$= \alpha^{k_1+1}((\alpha^{k_1+1})^{\frac{p-1}{d_1}} + \alpha^{i+\frac{p-1}{d_1}-\frac{p-1}{d_2}+\frac{p-1}{d_2}}(\alpha^{k_1})^{\frac{p-1}{d_2}} + \alpha^{j+\frac{p-1}{d_1}})$$

$$= \alpha^{k_1+1}((\alpha^{k_1+1})^{\frac{p-1}{d_1}} + \alpha^{i+\frac{p-1}{d_1}-\frac{p-1}{d_2}}(\alpha^{k_1+1})^{\frac{p-1}{d_2}} + \alpha^{j+\frac{p-1}{d_1}})$$

$$= F_{a',b'}(\alpha^{k_1+1})$$

Then consider $f(F_{a',b'}(\alpha^{k_2+1}))$

$$= f(\alpha^{k_2+1}((\alpha^{k_2+1})^{\frac{p-1}{d_1}} + \alpha^i(\alpha^{k_2+1})^{\frac{p-1}{d_2}} + \alpha^j))$$

$$= \alpha^{\frac{p-1}{d_1}+1}(\alpha^{k_2}((\alpha^{k_2})^{\frac{p-1}{d_1}} + \alpha^i(\alpha^{k_2})^{\frac{p-1}{d_2}} + \alpha^j))$$

$$= \alpha^{k_2+1}(\alpha^{\frac{p-1}{d_1}}((\alpha^{k_2})^{\frac{p-1}{d_1}} + \alpha^i(\alpha^{k_2})^{\frac{p-1}{d_2}} + \alpha^j))$$

$$= \alpha^{k_2+1}((\alpha^{k_2+1})^{\frac{p-1}{d_1}} + \alpha^{i+\frac{p-1}{d_1}-\frac{p-1}{d_2}+\frac{p-1}{d_2}}(\alpha^{k_2})^{\frac{p-1}{d_2}} + \alpha^{j+\frac{p-1}{d_1}})$$

$$= \alpha^{k_2+1}((\alpha^{k_2+1})^{\frac{p-1}{d_1}} + \alpha^{i+\frac{p-1}{d_1}-\frac{p-1}{d_2}}(\alpha^{k_2+1})^{\frac{p-1}{d_2}} + \alpha^{j+\frac{p-1}{d_1}})$$

$$= F_{a',b'}(\alpha^{k_2+1})$$

In conslusion $F_{a',b'}(\alpha^{k_1+1}) = F_{a',b'}(\alpha^{k_2+1})$ therefore f is a injective function. Consider an element in the value set given by $\alpha^{\frac{p-1}{d_1}}F_{a,b}(\alpha^k)$

$$\alpha^{\frac{p-1}{d_1}}F_{a,b}(\alpha^k) = \alpha^{\frac{p-1}{d_1}+1}(\alpha^k((\alpha^k)^{\frac{p-1}{d_1}} + \alpha^i(\alpha^k)^{\frac{p-1}{d_2}} + \alpha^j))$$

$$= \alpha^{k+1}(\alpha^{\frac{p-1}{d_1}}((\alpha^k)^{\frac{p-1}{d_1}} + \alpha^i(\alpha^k)^{\frac{p-1}{d_2}} + \alpha^j))$$

$$= \alpha^{k+1}((\alpha^{k+1})^{\frac{p-1}{d_1}} + \alpha^{i+\frac{p-1}{d_1}-\frac{p-1}{d_2}+\frac{p-1}{d_2}}(\alpha^k)^{\frac{p-1}{d_2}} + \alpha^{j+\frac{p-1}{d_1}})$$

$$= \alpha^{k+1}((\alpha^{k+1})^{\frac{p-1}{d_1}} + \alpha^{i+\frac{p-1}{d_1}-\frac{p-1}{d_2}}(\alpha^{k+1})^{\frac{p-1}{d_2}} + \alpha^{j+\frac{p-1}{d_1}})$$

$$= F_{a',b'}(\alpha^{k+1})$$

In brief for each element in the value set, $\alpha^{\frac{p-1}{d_1}}F_{a,b}(\alpha^k)$, there exists an element in the domain, $F_{a',b'}(\alpha^{k+1})$. Therefore f is a bijective function and we can conclude that $|V_{a',b'}| = |V_{a,b}|$.

□

Example 3.6. Let $q = 13, d_1 = 2, d_2 = 3, a = 4, b = 8$. Since $(4,8) \sim (3,5)$ we have that $|V_{4,8}| = |V_{3,5}|$

Proposition 3.7. *$|[a,b]| = lcm(d_1,d_2)$ where $lcm(x,y)$ is the least common multiple of x and y.*

Proof. Suppose that $a = \alpha^i$, $b = \alpha^j$. Note that we can obtain the elements of $[a,b]$ applying the transformation $f : (a,b) \to (a\cdot\alpha^{(\frac{p-1}{d_1}-\frac{p-1}{d_2})}, b\cdot\alpha^{(\frac{p-1}{d_1})})$ multiple times. Now note that:

$$\begin{aligned}
&f(a\cdot\alpha^{i+(lcm(d_1,d_2)-1)(\frac{p-1}{d_1}-\frac{p-1}{d_2})}, b\cdot\alpha^{j+(lcm(d_1,d_2)-1)(\frac{p-1}{d_1})})\\
&=(\alpha^{i+lcm(d_1,d_2)(\frac{p-1}{d_1}-\frac{p-1}{d_2})}, \alpha^{j+lcm(d_1,d_2)(\frac{p-1}{d_1})})\\
&=(\alpha^{i+lcm(d_1,d_2)(\frac{p-1}{d_1})-lcm(d_1,d_2)(\frac{p-1}{d_2})}, \alpha^{j+lcm(d_1,d_2)(\frac{p-1}{d_1})})\\
&=(\alpha^{i+\frac{d_1d_2}{gcd(d_1,d_2)}(\frac{p-1}{d_1})-\frac{d_1d_2}{gcd(d_1,d_2)}(\frac{p-1}{d_2})}, \alpha^{j+\frac{d_1d_2}{gcd(d_1,d_2)}(\frac{p-1}{d_1})})\\
&=(\alpha^{i+\frac{d_2}{gcd(d_1,d_2)}(p-1)-\frac{d_2}{gcd(d_1,d_2)}(p-1)}, \alpha^{j+\frac{d_2}{gcd(d_1,d_2)}(p-1)})\\
&=(\alpha^i,\alpha^j)
\end{aligned}$$

Therefore applying the transformation $lcm(d_1, d_2)$ times, we obtain a chain of elements in $[a, b]$. Now suppose that $c < lcm(d_1, d_2)$ such that $\alpha^{i+c(\frac{p-1}{d_1}-\frac{p-1}{d_2})} = \alpha^i$ and $\alpha^{j+c(\frac{p-1}{d_1})} = \alpha^j$. This implies that implica $\alpha^{c(\frac{p-1}{d_1}-\frac{p-1}{d_2})} = 1$, then $\alpha^{c(\frac{p-1}{d_1})-c(\frac{p-1}{d_2})} = 1$, this is only possible if c is a multiple of d_1 and d_2 but $c < lcm(d_1, d_2)$ and $lcm(d_1, d_2)$ is the smallest element such that this occurs. Therefore the amount of elements in the equivalence relation $[a, b]$ is equal to $lcm(d_1, d_2)$.

□

Example 3.8. 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):

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

Proposition 3.9. The number of polynomials $F_{a',b'}(x)$ with $|V_{a,b}| = n$ is a multiple of $|[a, b]|$

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