Generating Permutation Trinomials over Finite Fields

Christian A. Rodríguez Alex D. Santos
Computer Science Department, School of Natural Sciences

September 22, 2014

Abstract

Permutation polynomials over finite fields have many applications in areas such as coding theory and cryptography. We consider polynomials of the form $F_{a,b}(X) = X\left(X^{\frac{q-1}{d_1}} + aX^{\frac{q-1}{d_2}} + b\right)$, where $a, b \in \mathbb{F}_q^*$ and $d_1 < d_2$. We construct partitions of these polynomials where polynomials in the same partition have value sets of equal cardinality. As a consequence we provide families of permutation polynomials.

Resumen

Los polinomios de permutación definidos sobre cuerpos finitos tienen muchas aplicaciones en campos como la teoría de códigos y la criptografía. Consideramos polinomios de la forma $F_{a,b}(X) = X\left(X^{\frac{q-1}{d_1}} + aX^{\frac{q-1}{d_2}} + b\right)$, donde $a, b \in \mathbb{F}_q^*$ y $d_1 < d_2$. Construimos particiones de estos polinomios en las que los polinomios en la misma partición tienen conjuntos de valores con la misma cardinalidad. Como consecuencia proveemos familias de polinomios de permutación.

1 Introduction

Many people have studied permutation polynomials over finite fields because of their applications in cryptography and coding theory. Moreover, permutation polynomials provide an efficient way of generating permutations when working with a limited amount of storage.

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. Expressing this operator in terms of a permutation polynomial is simple and efficient.

Permutation polynomials are a very broad field of study and researchers have studied them by cases (?, ?). It is known that a polynomial of the form $X^d + a$ is a permutation polynomial over $\mathbb{F}_q$ if and only if $gcd(d, q-1) = 1$ (?, ?). Binomials that produce permutation polynomials have been studied extensively. The next logical case to be studied are trinomials.

We have found that within the family of polynomials of the form

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

where $a, b \in \mathbb{F}_q^*$ and $d_1 < d_2$, there are many permutation polynomials. Given a pair of coefficients (a, b) such that $F_{a,b}(X)$ is a permutation polynomial, we provide a construction to obtain $lcm(d_1, d_2) - 1$ other permutation polynomials.

2 Preliminaries

We begin by introducing some background concepts.

Definition 2.1. A **permutation** of a set A is an ordering of the elements of A.

Example 2.2. Consider $A = \{0, 1, 2, 3, 4\}$. Then $4, 2, 3, 1, 0$ and $2, 1, 0, 4, 3$ are permutations of the set A.

A function $f : A \to A$ gives a permutation of A if and only if f is one to one and onto.

Definition 2.3. Let f be a function defined over a set A. The **value set** of f is defined as $V(f) = \{f(a) \mid a \in A\}$.

Example 2.4. Consider $f : \mathbb{Z} \to \mathbb{Z}$, $f(X) = X^2$. Then $V(f) = \{0, 1, 4, 9, ...\}$.

We are interested in functions $f : A \to A$ where $V(f) = A$ and A is a finite field.

Definition 2.5. A **finite field** $\mathbb{F}_q$ is a field with $q = p^r$ elements, where p is a prime.

Example 2.6. Let $q = 5$. Then $\mathbb{F}_5 = \{0, 1, 2, 3, 4\}$ with the operations of addition and multiplication modulo 5 is a field. In general, $\mathbb{F}_p = \mathbb{Z}_p$ for p prime.

Since $\mathbb{F}_q$ is finite, we have that a polynomial is a permutation polynomial of $\mathbb{F}_q$ if it gives a one to one function $f : \mathbb{F}_q \to \mathbb{F}_q$. Also, a polynomial $f(X)$ is a permutation polynomial of $\mathbb{F}_q$ if and only if $V(f) = \mathbb{F}_q$.

Example 2.7. Consider the polynomial $f(X) = X+3$ defined over $\mathbb{F}_7$. We have that $f(0) = 3, f(1) = 4, f(2) = 5, f(3) = 6, f(4) = 0, f(5) = 1, f(6) = 2$ and $V(f) = \{0, 1, 2, 3, 4, 5, 6\} = \mathbb{F}_7$. Therefore $f(X)$ is a permutation polynomial over $\mathbb{F}_7$.

An important property of finite fields, used throughout our results, is the existence of a primitive root. This is an element of the field that generates all the elements in the field, except 0.

Definition 2.8. A **primitive root** $\alpha \in \mathbb{F}_q$ is a generator of the multiplicative group $\mathbb{F}_q^* = \mathbb{F}_q - \{0\}$.

Example 2.9. Consider the finite field $\mathbb{F}_7$. We have that $3^1 = 3, 3^2 = 2, 3^3 = 6, 3^4 = 4, 3^5 = 5, 3^6 = 1$. Therefore 3 is a primitive root of $\mathbb{F}_7$.

Example 2.10. Consider the finite field $\mathbb{F}_7$. We have that $2^1 = 2, 2^2 = 4, 2^3 = 1, 2^4 = 2, 2^5 = 4, 2^6 = 1$. Therefore 2 is not a primitive root of $\mathbb{F}_7$.

Primitive roots are useful in many topics because of the properties they have. We are interested in the following property that relates powers of a primitive root. This property is fundamental in order to prove many of our results.

Proposition 2.11. Let α be a primitive root of $\mathbb{F}_q$. Then $\alpha^i = \alpha^j$ if and only if $i \equiv j \pmod{q-1}$.

3 Families of Polynomials with Value Sets of the Same Cardinality

We consider polynomials of the form $F_{a,b}(X) = X\left(X^{\frac{q-1}{d_1}} + aX^{\frac{q-1}{d_2}} + b\right)$ over $\mathbb{F}_q$. Given d_1 and d_2 these polynomials are characterized by the coefficients a and b. In this section we provide a way to, given a polynomial with value set of cardinality n, generate $lcm(d_1, d_2) - 1$ more polynomials with value sets of the same cardinality n. For a fixed q, d_1, d_2, we define a relation in the set P_{d_1,d_2} of all polynomials of the form $F_{a,b}(X)$ relating the pair of coefficients (a, b) expressed as powers of a primitive root $\alpha \in \mathbb{F}_q$.

Polynomials over finite fields with value sets of maximum size q are permutation polynomials and have many applications as we mentioned before. Polynomials with minimal value sets are also of interest (?, ?).

Definition 3.1. Consider $P_{d_1,d_2} = \left\{X(X^{\frac{q-1}{d_1}} + aX^{\frac{q-1}{d_2}} + b) \mid a, b \in \mathbb{F}_q^*\right\}$, and let

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

be two polynomials over $\mathbb{F}_q$ with $a, b, a', b' \in \mathbb{F}_q^*$. We say $F_{a,b}(X) \sim F_{a',b'}(X)$ if and only if $(a, b) = (\alpha^i, \alpha^j)$ and $(a', b') = (\alpha^{i+h(\frac{q-1}{d_1}-\frac{q-1}{d_2})}, \alpha^{j+h(\frac{q-1}{d_1})})$, where α is a primitive root of $\mathbb{F}_q$ and $h \in \mathbb{Z}$.

Example 3.2. Let $q = 13, d_1 = 2, d_2 = 3, \alpha = 2$. Then $a = 4 = 2^2, b = 8 = 2^3$. Now $(2^2, 2^3) \sim (a', b') \iff a' = 2^{2+h(6-4)}, b' = 2^{3+h(6)}$ for some $h \in \mathbb{Z}$. Therefore $(2^2, 2^3) \sim (2^4, 2^9) \sim (2^6, 2^3)$ and so on.

Note that $\sim$ is defined in a way that allows us to construct polynomials related to each other. Given a polynomial $F_{a,b}(X)$, it is easy to construct $F_{a',b'}(X)$ such that $F_{a,b}(X) \sim F_{a',b'}(X)$. This relation is fundamental in our results and, as the following lemma states, it partitions the set P_{d_1,d_2}.

Lemma 3.3. *The relation $\sim$ in Definition 3.1 is an equivalence relation in P_{d_1,d_2}.*

Proof. We will prove that the relation is reflexive, symmetric and transitive:

1. Let $F_{a,b}(X) \in P_{d_1,d_2}$. Then $a' = \alpha^{i+0(\frac{p-1}{d_1}-\frac{q-1}{d_2})} = \alpha^i = a$ and $b' = \alpha^{j+0(\frac{q-1}{d_1})} = \alpha^j = b$. Therefore $F_{a,b}(X) \sim F_{a',b'}(X) = F_{a,b}(X)$ and $\sim$ is **reflexive**.

2. Suppose that $F_{a,b}(X) \sim F_{a',b'}(X)$. Then, for $a = \alpha^i, b = \alpha^j$ we have that $a' = \alpha^{i+h(\frac{q-1}{d_1}-\frac{q-1}{d_2})}, b' = \alpha^{j+h(\frac{q-1}{d_1})}$ for some $h \in \mathbb{Z}$. Note that $(a')' = \alpha^{i+h(\frac{q-1}{d_1}-\frac{q-1}{d_2})-h(\frac{q-1}{d_1}-\frac{q-1}{d_2})} = \alpha^i = a$ and $(b')' = \alpha^{j+h(\frac{q-1}{d_1})-h(\frac{q-1}{d_1})} = \alpha^j = b$. This implies that $F_{a',b'}(X) \sim F_{(a')',(b')'}(X) = F_{a,b}(X)$. Therefore $F_{a',b'}(X) \sim F_{a,b}(X)$ and the relation is **symmetric**.

3. Suppose that $F_{a,b}(X) \sim F_{a',b'}(X)$ and $F_{a',b'}(X) \sim F_{(a')',(b')'}(X)$. Then, for $a = \alpha^i$, $b = \alpha^j$ we have that $a' = \alpha^{i+h(\frac{q-1}{d_1}-\frac{q-1}{d_2})}$, $b' = \alpha^{j+h(\frac{q-1}{d_1})}$ and $(a')' = \alpha^{i+h(\frac{q-1}{d_1}-\frac{q-1}{d_2})+l(\frac{q-1}{d_1}-\frac{q-1}{d_2})}$, $(b')' = \alpha^{j+h(\frac{q-1}{d_1})+l(\frac{q-1}{d_1})}$ for some $h, l \in \mathbb{Z}$. Note that $(a')' = \alpha^{i+(h+l)(\frac{q-1}{d_1}-\frac{q-1}{d_2})}$, $(b')' = \alpha^{j+(h+l)(\frac{q-1}{d_1})}$, hence $F_{a,b}(X) \sim F_{(a')',(b')'}$ and the relation is **transitive**.

Because the relation is reflexive, symmetric and transitive, we can conclude that the relation is an equivalence relation in P_{d_1,d_2}. □

We denote by $[F_{a,b}(X)]$ the equivalence class that contains the polynomial $F_{a,b}(X)$. Using the equivalence relation $\sim$ we can express our results in a very concise way. The next theorem states that any two polynomials related by $\sim$ must have value sets of the same cardinality.

Theorem 3.4. *Suppose that $F_{a,b}(X) \sim F_{a',b'}(X)$. Then $|V(F_{a,b})| = |V(F_{a',b'})|$.*

Proof. First, note that $F_{a,b}(0) = 0$ for all pairs $(a, b) \in \mathbb{F}_q^* \times \mathbb{F}_q^*$. Therefore we must have that $F_{a,b}(0) = F_{a',b'}(0) = 0$. Let α be a primitive root of the finite field. Now for any $x \neq 0$, $x = \alpha^i$. Let $F_{a',b'}(\alpha^{k+1}) \in V(F_{a',b'})$, where $a' = \alpha^{i+h(\frac{q-1}{d_1}-\frac{q-1}{d_2})}$, $b' = \alpha^{j+h(\frac{q-1}{d_1})}$ and $a = \alpha^i$, $b = \alpha^j$. Then

$$\begin{aligned} F_{a',b'}(\alpha^{k+1}) &= \alpha^{k+1}\left((\alpha^{k+1})^{\frac{q-1}{d_1}} + \alpha^{i+\frac{q-1}{d_1}-\frac{q-1}{d_2}}(\alpha^{k+1})^{\frac{q-1}{d_2}} + \alpha^{j+\frac{q-1}{d_1}}\right) \\ &= \alpha^{k+1}\left((\alpha^k)^{\frac{q-1}{d_1}} \cdot \alpha^{\frac{q-1}{d_1}} + \alpha^i \cdot \alpha^{\frac{q-1}{d_1}}(\alpha^k)^{\frac{q-1}{d_2}} + \alpha^j \cdot \alpha^{\frac{q-1}{d_1}}\right) \\ &= \alpha^{\frac{q-1}{d_1}+1} \cdot \alpha^k\left((\alpha^k)^{\frac{q-1}{d_1}} + \alpha^i(\alpha^k)^{\frac{q-1}{d_2}} + \alpha^j\right) \\ &= \alpha^{\frac{q-1}{d_1}+1} \cdot F_{a,b}(\alpha^k) \in \alpha^{\frac{q-1}{d_1}+1}V(F_{a,b}). \end{aligned} \tag{3.1}$$

In general, for each term $F_{a,b}(\alpha^k)$ of $V(F_{a,b})$ there exists a corresponding term $F_{a',b'}(\alpha^{k+1})$ of $V(F_{a',b'})$.

Let $f : V(F_{a',b'}) \to \alpha^{\frac{q-1}{d_1}+1}V(F_{a,b})$ be given by $f(F_{a',b'}(\alpha^{k+1})) = \alpha^{\frac{q-1}{d_1}+1}F_{a,b}(\alpha^k)$. Suppose that $f(F_{a',b'}(\alpha^{k_1+1})) = f(F_{a',b'}(\alpha^{k_2+1}))$ where $k_1, k_2 \in \mathbb{Z}$. Then we have that $\alpha^{\frac{q-1}{d_1}+1}F_{a,b}(\alpha^{k_1}) = \alpha^{\frac{q-1}{d_1}+1}F_{a,b}(\alpha^{k_2})$ and (3.1) imply that $F_{a',b'}(\alpha^{k_1+1}) = F_{a,b}(\alpha^{k_2+1})$. Therefore f is one to one.

Now consider an element $y \in \alpha^{\frac{q-1}{d_1}+1}V(F_{a,b})$. Then $y = \alpha^{\frac{q-1}{d_1}+1}F_{a,b}(\alpha^k)$ for some $k \in \mathbb{Z}$ and $y = f(F_{a',b'}(\alpha^{k+1}))$. Note that the correspondence between $V(F_{a',b'})$ and $\alpha^{\frac{q-1}{d_1}+1}V(F_{a,b})$ gives a bijection between $V(F_{a',b'})$ and $V(F_{a,b})$. Therefore $\mid V(F_{a',b'}) \mid = \mid V(F_{a,b}) \mid$.

□

Example 3.5. From Example 3.2 we have that $(2^2, 2^3) \sim (2^4, 2^9)$. Therefore $|V(F_{2^2,2^3})| = |V(F_{2^4,2^9})|$.

Theorem 3.4 gives us a way to construct a polynomial with value set of cardinality n, given a polynomial with value set of cardinality n. In particular, given a permutation polynomial of $\mathbb{F}_q$ of the form $F_{a,b}(X)$ we can construct another permutation polynomial $F_{a',b'}(X)$ of $\mathbb{F}_q$. We state this formally in the following corollary.

Corollary 3.6. Suppose $F_{a,b}(X)$ is a permutation polynomial of $\mathbb{F}_q$ and that $F_{a,b}(X) \sim F_{a',b'}(X)$. Then $F_{a',b'}(X)$ is also a permutation polynomial of $\mathbb{F}_q$.

All the polynomials in an equivalence class of P_{d_1,d_2} under the relation $\sim$ have value sets of the same cardinality. The next result tells the number of polynomials in each equivalence class.

Proposition 3.7. $|[F_{a,b}(X)]| = lcm(d_1, d_2)$

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

$$(\alpha^i, \alpha^j) \to (\alpha^{i+(\frac{q-1}{d_1}-\frac{q-1}{d_2})}, \alpha^{j+(\frac{q-1}{d_1})}) \to (\alpha^{i+2(\frac{q-1}{d_1}-\frac{q-1}{d_2})}, \alpha^{j+2(\frac{q-1}{d_1})}) \to \cdots \to (\alpha^{i+h(\frac{q-1}{d_1}-\frac{q-1}{d_2})}, \alpha^{j+h(\frac{q-1}{d_1})}) = (\alpha^i, \alpha^j).$$

Note that if $h = lcm(d_1, d_2)$, $h(\frac{q-1}{d_1} - \frac{q-1}{d_2}) = l(q-1)$ for some $l \in \mathbb{Z}$ and $h(\frac{q-1}{d_1}) = m(q-1)$ for some $m \in \mathbb{Z}$. We just have to see that $lcm(d_1, d_2)$ is the smallest integer such that this occurs.

Suppose there exists c such that $\alpha^{i+c(\frac{q-1}{d_1}-\frac{q-1}{d_2})} = \alpha^i$ and $\alpha^{j+c(\frac{q-1}{d_1})} = \alpha^j$. This implies that $\alpha^{c(\frac{q-1}{d_1}-\frac{q-1}{d_2})} = 1$, and $\alpha^{c(\frac{q-1}{d_1})} = 1$, this is only possible if c is a multiple of d_1 and d_2. Therefore $lcm(d_1, d_2)$ is the smallest integer such that this happens.

This implies that all elements in the chain with $h = 1, 2, ..., lcm(d_1, d_2)$ are different and therefore we must have that $|[F_{a,b}(X)]| = lcm(d_1, d_2)$.

□

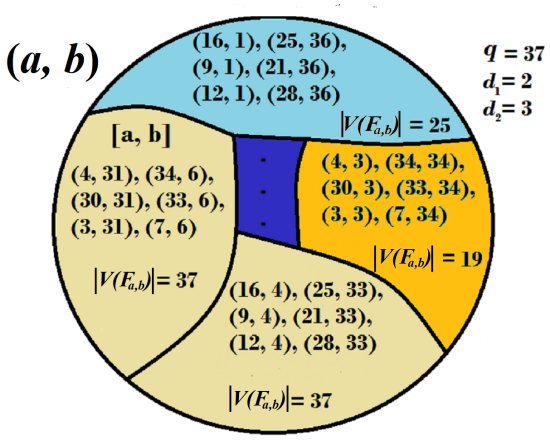

Figure 1: The set of equivalence classes of $P_{2,3}$ with $q = 37$. All pairs of coefficients in a cell are related by $\sim$. Note that the number of pairs in each cell is $6 = lcm(2, 3)$. The polynomials associated to the elements in a cell have value sets of the same cardinality. The cardinality of the value sets associated to different cells might or might not be equal.

Example 3.8. Consider Example 3.2 again where $q = 13, d_1 = 2, d_2 = 3, a = 4, b = 8$. Note that $lcm(2, 3) = 6$ and the elements of $[F_{a,b}(X)]$ are:

$$\begin{array}{cccccccc} (2^2, 2^3) & (2^4, 2^9) & (2^6, 2^3) & (2^8, 2^9) & (2^{10}, 2^3) & (2^{12}, 2^9) & (2^2, 2^3) \\ (4, 8) & (3, 5) & (12, 8) & (9, 5) & (10, 8) & (1, 5) & (4, 8). \end{array}$$

It is important to note that the result given in Proposition 3.7 does not depend on $\mathbb{F}_q$, only on the chosen d_1 and d_2. Using Proposition 3.7 we can partition the set P_{d_1,d_2} of polynomials of the form $F_{a,b}(X)$ into equivalence classes, each of cardinality $lcm(d_1, d_2)$. Moreover, using Theorem 3.4 we can say that all of the polynomials in the same equivalence class have value sets of equal cardinality. Given a polynomial with value set of cardinality n, we can combine our previous results to provide $lcm(d_1, d_2) - 1$ more polynomials with value set of cardinality n. Although we cannot say if these are all of the polynomials that have a value set of cardinality n, we know that if there exists another polynomial with value set of cardinality n, there exists at least $lcm(d_1, d_2) - 1$ more. This leads to our main result.

Theorem 3.9. *The number of polynomials* $F_{a,b}(X) \in P_{d_1,d_2}$ *with* $|V(F_{a,b}(X))| = n$ *is a multiple of* $lcm(d_1, d_2)$.

Proof. Fix q, d_1 and d_2. Consider the set P_{d_1,d_2} of all polynomials of the form $F_{a,b}(X)$. If there are no polynomials in P_{d_1,d_2} with value set of cardinality n, we are done. Let $F_{a,b}(X) \in P_{d_1,d_2}$ be such that $|V(F_{a,b})| = n$. Using Theorems 3.4 and 3.7 we can construct $lcm(d_1, d_2) - 1$ more polynomials $F_{a',b'}(X) \in P_{d_1,d_2}$, such that $|V(F_{a',b'})| = n$.

Note that for each polynomial in P_{d_1,d_2} with value set of cardinality n we may repeat the process above and obtain up to $lcm(d_1, d_2)$ polynomials in P_{d_1,d_2} with value set of cardinality n. By counting the polynomials it is easy to see that we will have a multiple of $lcm(d_1, d_2)$, which proves the theorem. □

Theorem 3.9 states that for any given value set of cardinality n, the amount of polynomials with value sets of that cardinality will always be a multiple of $lcm(d_1, d_2)$. Recall that we are

interested in providing ways to construct permutation polynomials, hence we are interested in the particular case when $n = q$.

Corollary 3.10. For any $\mathbb{F}_q$ the number of permutation polynomials of $\mathbb{F}_q$ of the form $F_{a,b}(X)$ is a multiple of $lcm(d_1, d_2)$.

In summary, we provide a straightforward way to construct up to $lcm(d_1, d_2)$ polynomials of the form $F_{a,b}(X)$ with value set of cardinality n, given a polynomial of the form $F_{a,b}(X)$ with value set of cardinality n. Moreover, we proved that the amount of polynomials of the form $F_{a,b}(X)$ with value set of cardinality n will always be a multiple of $lcm(d_1, d_2)$. In particular, these results hold when we are given a permutation polynomial of the form $F_{a,b}(X)$.

4 Acknowledgements

This research has been supported by a grant from the Center of Undergraduate Research in Mathematics (CURM) from Brigham Young University, NSF grant #DMS-1148695, and was conducted under the direction of Prof. Ivelisse Rubio, Department of Computer Science, and Prof. Francis Castro, Department of Mathematics, University of Puerto Rico, Río Piedras.

References

Borges, H., & Conceição, R. (2013). On the characterization of minimal value set polynomials. *Journal of Number Theory*, *133*, 2021–2035.

Laigle-Chapuy, Y. (1988). When does a polinomial over a finite field permute the elements of the field? *The American Mathematical Monthly*, *95*, 243-246.

Lidl, R., & Mullen, G. (2013). On the characterization of minimal value set polynomials. *Journal of Number Theory*, *133*, 2021–2035.

Panario, D., & Mullen, G. (2013). Handbook of finite fields. *CRC Press*.

Wan, D., & Lidl, R. (1991). Permutation polynomials of the form $x^r f(x^{(q-1)/d})$ and their group structure. *Monatshefte für Mathematik*, *112*, 149-163.

Zieve, M. (2009). On some permutation polynomials over f_q of the form $x^r * h(x^(q-1)/d)))$. *Proc. Amer. Math. Soc.*, *137*, 2209-2216.