Proceeding of the National Conference
On Undergraduate Research (NCUR) 2006
Dominican University of California
San Rafael, California
April 12 - 14, 2007

Permutations of F_q that are given by binomials and decompose in cycles of length two

Yesenia Cruz Rosado
Department of Mathematics
The University of Puerto Rico at Humacao
Humacao, Puerto Rico

Faculty Advisor: Dr. Ivelisse Rubio

Abstract

This paper studies binomials that give permutations of F_q. In particular, studies the necessary and sufficient conditions to obtain permutations that decompose in cycles of length two. These types of permutations are useful for applications to coding theory and cryptography. The paper presents some binomials that are never permutations and permutation binomials that never decompose in cycles of length two. Furthermore , it gives the necessary conditions for certain permutation binomials to decompose in cycles of length two.

Keywords: Permutations, Cyclic decomposition, Binomials

1. Introduction

Let F_q be the finite field with $q = p^r$ elements, where p is a prime. We study permutations of F_q given by binomials. We started by studying binomials with terms that are permutations monomials of F_q. We proved that certain type of binomials never give permutations of F_q. We also study binomials in $F_q[x]$ of the form $\pi(x) = x^{\frac{q+1}{2}} + ax$. We found necessary conditions on these binomials so that the permutations given by them decompose in cycles of length two. Also we found the necessary conditions on the binomials so that the permutation given by them does not decompose in cycles of length two. Furthermore, we present a conjecture that states the sufficient conditions for a permutation binomial to decompose in cycles of length two. We start by presenting some background material that is needed for the rest of the paper.

1.1 finite fields

We are interested on permutations of finite fields. A **field** is an algebraic structure in which the operations of addition, subtraction, multiplication and division (except division by cero) may be performed, and the same rules which are familiar from the arithmetic of real numbers hold. A **finite field** is a field with finitely many elements. It can be proved that any finite filed has p^r elements, where p is a prime number and there is a finite field with p^r for any p prime, r positive integer.

It is easier to study finite fields F_q if we write its elements as powers of one element: a primitive root. A **primitive root** in F_q is an element that generates all $F_q^* := F_q - \{0\}$. This is, α is a primitive root in F_q if $F_q^* := \{\alpha^o, \alpha^1, \alpha^2, ..., \alpha^{q-2}\}$. It can be proved that every finite field has primitive elements α and $q-1$ is the smallest positive integer such that $\alpha^{q-1} = 1$.

Example 1. The element 2 is a primitive root in Z_{11} because it generates all elements in $Z_{11}{}^*$:
$2^0 = 1, 2^1 = 1, 2^2 = 4, 2^3 = 8, 2^4 = 5, 2^5 = 10, 2^6 = 9, 2^7 = 7, 2^8 = 3, 2^9 = 6, 2^{10} = 1$.

Lemma 1. Let $a \in F_q{}^*$, then $a^{q-1} = 1$.

Proof: Let $a \in F_q{}^*$ and α be a primitive root of F_q. Then $a = \alpha^l$, for some $l \in \{0, ..., \mathrm{q-2}\}$. This implies that $a^{q-1} = (\alpha^l)^{q-1} = (\alpha^{q-1})^l = (1)^l = 1$.□

Lemma 2. Let q be an odd prime and let $a \in F_q{}^*$. Then $a^{\frac{q-1}{2}} \in \{-1, 1\}$.

Proof: Since q is odd, $q-1$ is even and $\frac{q-1}{2}$ is an integer. Let $a \in F_q{}^*$. Then, by Lemma 1, $a^{q-1} = 1$. Therefore, $(a^{\frac{q-1}{2}})^2 - 1 = 0$. Factoring, we obtain $(a^{\frac{q-1}{2}} - 1)(a^{\frac{q-1}{2}} + 1) = 0$ and therefore $a^{\frac{q-1}{2}} = 1$ or $a^{\frac{q-1}{2}} = -1$.□

Lemma 3. Let α be a primitive root in $F_q{}^*$ and q be an odd prime. Then $\alpha^{\frac{q-1}{2}} = -1$.

Proof: By Lemma 2, $\alpha^{\frac{q-1}{2}} \varepsilon \{-1, 1\}$. But since $q-1$ is the smallest positive integer such that $\alpha^{q-1} = 1$, we must have $\alpha^{\frac{q-1}{2}} = -1$.□

1.2 permutations

We want to find binomials that produce permutations of F_q. A permutation of a set is a reordering of the elements of the set. In other words, a **permutation** of a set X is a function $\pi : X \to X$ that is one to one and onto. A binomial that produces a permutation is called a **permutation binomial**. We want to study binomials that produce permutations of F_q that decompose in cycles of length two. The following proposition states that to get permutations of a finite set it is enough to check that the function is one to one.

Proposition 1. Let A be a finite set and consider $f : A \to A$. Then f is one to one if and only if f is onto.

Proof: We know that A is a finite field. Suppose that f is one to one, this implies that each element of A is "pair up" with only one element of A. Therefore all elements of A are covered. Hence f is onto. Suppose that f is unto, this implies that each element of A is covered. Therefore all the elements are "pair up" with only one element of A because that way all the elements will be covered. Hence f is one to one. □

As we will see in the following proposition it is enough to study binomials of the form $x^i + \alpha x^j$, to find those that produce permutations that decompose in cycles of length two.

Proposition 2. The binomial $\pi_1(\mathrm{x}) = \mathrm{ax^i + bx^j}$ is a permutation of F_q if and only if $\pi_2(\mathrm{x}) = \mathrm{x^i} + \alpha\,\mathrm{x^j}$ is a permutation of F_q, where $\alpha = \frac{b}{a}$.

Proof: Suppose that $\pi_1(\mathrm{x}) = \mathrm{ax^i + bx^j}$ gives a permutation of F_q. Then $\pi_1(\mathrm{x}) = \mathrm{ax^i + bx^j}$ is one to one. This implies that for every $l, s \in F_q$ where $l \neq s$, we have that $\pi_1(l) \neq \pi_1(s)$. This is, $\mathrm{a}(\mathrm{l})^{\mathrm{i}} + \mathrm{b}(l)^{\mathrm{j}} \neq \mathrm{a}(s)^{\mathrm{i}} + \mathrm{b}(s)^{\mathrm{j}}$. Now dividing both sides by a, we have

$\pi_2(1) = (l)^i + \frac{b}{a}(l)^j \neq (s)^i + \frac{b}{a}(s)^j = \pi_2(s)$. Hence, $l \neq s$ implies that $\pi_2(l) \neq \pi_2(s)$and $\pi_2(x)$is one to one. The other implication can be proved similarly. □

Example 2. The permutation given by the binomial $\pi(x) = x^{\frac{q+1}{2}} + ax$ in Z_{11} is

$$\begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 0 & 5 & 6 & 4 & 9 & 3 & 7 & 10 & 2 & 1 & 8 \end{pmatrix},$$

and the cyclic decomposition of this permutation is:

$$(1 \quad 5 \quad 3 \quad 4 \quad 9)(2 \quad 6 \quad 7 \quad 10 \quad 8).$$

Observe that we represented the permutation using the following notation, the first row are the elements of the field finite Z_{11} and the second row are their images under π . Note that the length of the cycles is 5. We are interested in cycles of length two. We first study how these cycles are constructed. On this example the cycle $(1 \quad 5 \quad 3 \quad 4 \quad 9)$ starts with 1 (we can choose any element for this) and continues with 5. This is because $\pi(1) = 5$. The third element is 3 because $\pi(5) = 3$. In general, we construct the cycles by taking α^i and evaluating it in $\pi(x)$ which gives us another element or the same that we evaluated. If $\pi(\alpha^i) = \alpha^i$ then α^i is a fixed point and we do not write these cycles of length 1. On the other hand, if the binomial $\pi(x)$ produces another element $\pi(\alpha^i) = \alpha^k$ the cyclic decomposition of this is $(\alpha^i \quad \alpha^k \quad \ldots)$. Since we have a different element we evaluate it in the function and repeat until we get first element. A cycle will look like $(\alpha^i \quad \pi(\alpha^i) \quad \pi^2(\alpha^i) \quad \pi^{n-1}(\alpha^i) = \alpha^i)$, where $\pi^l(\alpha^i)$, $l \in Z$, this means that π is compose with itself l times. Note that if the permutation given by a binomial in $F_q$decomposes in cycles of length two, then $\pi^2(\alpha^i) = \alpha^i$for all $0 \le i \le q-2$.

1.3 quadratic residues

One of the binomials in which we focus is $\pi(x) = x^{\frac{q+1}{2}} + ax$. It is know that $\pi(x)$ is a permutation binomial in F_q if and only if $a^2 - 1$is a quadratic residue modulo q. We have that an integer a is a **quadratic residue** modulo h if there exist another integer b such that $a = b^2 (\text{mod } h)$. We denote that a is a quadratic residue by $\eta(a) = 1$.

Example 3. Note that $2$is a quadratic residue modulo 23, because $5^2 = 2\,(\text{mod } 23)$.

Example 4. Note that $2$is not a quadratic residue modulo 5, because there is not another integer b, such that $b^2 = 2\,(\text{mod } 5)$.

2. Binomials with permutation monomials as terms

The first binomials that we study are given by permutation monomials that decompose in cycles of length two. Louis Cruz[2] found the necessary and sufficient conditions on the coefficient a such that the monomials $\pi(x) = ax^{\frac{q-3}{2}}$ and $\pi(x) = ax^{q-2}$ are permutations of F_q that decompose in cycles of length 2. We constructed binomials with these monomials as terms to see if they also produce permutations of F_q that decompose in cycles of length two. By Proposition 2 there are essentially three binomials that are given by these monomials and x^1: $\pi(x) = x^{\frac{q-3}{2}} + ax^{q-2}$, $\pi(x) = x^{q-2} - ax$ and $x^{\frac{q-3}{2}} - ax$. The binomial $\pi(x) = x^{\frac{q-3}{2}} + ax^{q-2}$ was studied by Cáceres and Colón[3]. They presented the necessary and sufficient conditions for $\pi(x) = x^{\frac{q-3}{2}} + ax^{q-2}$ over a finite field F_q of odd characteristic to be a permutation polynomial. They determined when π is self invertible and hence decompose in cycles of length two. If π is not self invertible they found the inverse. Here we prove that the binomial $\pi(x) = x^{q-2} - ax$ is not a permutation for $a \neq 0$. For the third case, in all of our examples, the binomial $x^{\frac{q-3}{2}} - ax$ is never a permutation for $a \neq 0$. We present this as a conjecture that remains to be proved.

Lemma 4. Let q be an odd prime, α a primitive root in F_q and $k \in \mathrm{Z}$. If s is such that $(q-1) \nmid (4s + 2k)$ and $l = \frac{q-1}{2} - s - k$. Then $\alpha^s \neq \alpha^l$ in F_q.

Proof: Suppose that $\alpha^s = \alpha^l$ in F_q. Then $s \equiv l$ (mod $q-1$). This is $s \equiv \frac{q-1}{2} - s - k$ (mod $q-1$), and this implies that $4s \equiv (q-1) - 2k$ (mod $q-1$). This is $(q-1) \mid (4s + 2k - (q-1))$. Hence $(q-1) \mid (4s + 2k)$ and this contradicts the hypothesis, therefore $\alpha^s \neq \alpha^l$ in F_q. □

Proposition 3. The binomial $\pi(x) = x^{q-2} - ax$ never gives a permutation in F_q, for $a \neq 0$.

Proof: Let $k \in \mathrm{Z}$, α a primitive root and $a = \alpha^k$. Also let s be such that be $(q-1) \nmid (4s + 2k)$ and l such that $l = \frac{q-1}{2} - k - s$. By Lemma 4, $\alpha^s \neq \alpha^l$ in F_q. We will show that $\pi(\alpha^s) = \pi(\alpha^l)$ and this will imply that π is not one to one and hence is not a permutation. Now $l = \frac{q-1}{2} - k - s$ implies that $\alpha^{K+l+s} = \alpha^{\frac{q-1}{2}} = -1$ and therefore $\alpha^{s+l+k} + 1 = 0$. This implies that: $0 = [(\alpha^l) - (\alpha^s)][1 + \alpha^k \alpha^s \alpha^l] =$ $(\alpha^l) - \alpha^k(\alpha^{2s})(\alpha^l) - (\alpha^s) + \alpha^k(\alpha^{2l})(\alpha^s) = (\alpha^s)^{q-1}(\alpha^l) - \alpha^k(\alpha^{2s})(\alpha^l) - (\alpha^s)(\alpha^l)^{q-1} + \alpha^k(\alpha^{2l})(\alpha^s) =$, now multiplying by $(\alpha^l)^{-1}(\alpha^s)^{-1}$ we have:
$(\alpha^s)^{q-2}(\alpha^l)^0 - \alpha^k(\alpha^s)(\alpha^l)^0 - (\alpha^s)^0(\alpha^l)^{q-2} + \alpha^k(\alpha^l)(\alpha^s)^0 = \pi(\alpha^s) - \pi(\alpha^l)$. This implies that $0 = \pi(\alpha^s) - \pi(\alpha^l)$ and $\pi(\alpha^s) = \pi(\alpha^l)$. Hence we found $\alpha^l \alpha^s$ such that $\alpha^s \neq \alpha^l$ and $\pi(\alpha^s) = \pi(\alpha^l)$ and therefore π is not one on one in F_q. □

Conjecture 1. Let q be odd and $q > 5$. The binomial $\pi(x) = x^{\frac{q-3}{2}} - ax$ is never a permutation binomial of F_q, for $a \neq 0$.

4. Permutations given by $\pi(x) = x^{\frac{q+1}{2}} + ax$ that decompose in cycles of length 2.

The binomials that we tried in Section II where not permutation binomials or have been studied before. In this section we will work with binomials that are know to be binomial permutations and study the necessary and sufficient conditions for them to decompose in cycles of length two. These permutation binomials are given by $\pi(x) = x^{\frac{q+1}{2}} + ax$. The following theorem[1] states when the binomials $\pi(x)$ are permutation binomials.

Theorem 1. Given an odd number $q = p^r$, the binomial $\pi(x) = x^{\frac{q+1}{2}} + ax$, is a permutation binomial of F_q if and only if $\eta(a^2 - 1) = 1$.

We present different results related to these permutation binomials, that were derived from the study of the necessary and sufficient conditions on a such that the permutation decompose in cycles of length two. Also we establish necessary and sufficient conditions for the binomial $\pi(x)$ to have fixed points.

Proposition 4. Let $\pi(x) = x^{\frac{q+1}{2}} + ax$ be a permutation of F_q and let α be a primitive root in F_q. Then α^i is a fixed point if and only if i is even and $a = 0$ or i is odd and $a = 2$.

Proof: Let α be a primitive root in F_q. Suppose that α^i is a fixed point of F_q. Then $\pi(\alpha^i) = \alpha^i$. This is $(\alpha^i)^{\frac{q+1}{2}} + a\alpha^i = \alpha^i$. Now we have that $((\alpha)\alpha^{\frac{q-1}{2}})^i + a\alpha^i = (-\alpha)^i + a\alpha^i = \alpha^i$. This implies that, if i is even, we have $\alpha^i + a\alpha^i = \alpha^i$, which means that $a = 0$. Now if i is odd, factorizing we have $\alpha^i(a-2) = 0$ which means that $a = 2$. Let $a = 2$ and i be odd. Then $\pi(\alpha^i) = (\alpha^i)^{\frac{q+1}{2}} + 2\alpha^i = ((\alpha)\alpha^{\frac{q-1}{2}})^i + 2\alpha^i = (-\alpha)^i + 2\alpha^i = -\alpha^i + 2\alpha^i = \alpha^i$. Hence $\pi(\alpha^i) = \alpha^i$ and α^i is a fixed point. Let $a = 0$ and i be even. Then $\pi(\alpha^i) = (\alpha^i)^{\frac{q+1}{2}} + 0\alpha^i = ((\alpha)\alpha^{\frac{q-1}{2}})^i = (-\alpha)^i = \alpha^i$. Hence $\pi(\alpha^i) = \alpha^i$ and α^i is a fixed point. □

Proposition 5. Suppose that $\pi(x) = x^{\frac{q+1}{2}} + 2x$ is a permutation of F_q that decompose in cycles of length two. Then $4 \nmid (q-1)$.

Proof: We will prove by the counterpositive. Let α be a primitive root in F_q. Since the coefficient of x in $\pi(x)$ is $a = 2$, then from Proposition 4 we have that for all $0 \le i \le q-2$, where i is odd $\pi(\alpha^i) = \alpha^i$. Since there are $q-1$ possible values for i, this means that there are $\frac{q-1}{2}$ values of i that are odd and therefore $\frac{q-1}{2} + 1$, fixed points counting the fixed point 0. Suppose that $\pi(x)$ decomposes in cycles of length two, this means that the $\frac{q-1}{2}$ elements that are not fixed points are contain in cycles of length two. Therefore we have, $\frac{q-1}{4}$ cycles of length two. But this is a contradiction because $4 \nmid (q-1)$. Hence $\pi(x)$ does not decompose in cycles of length two in F_q .□

Proposition 6. Let $\pi(x) = x^{\frac{q+1}{2}}$ a permutation of F_q. Then $\pi(x)$ decompose in cycles of length two if and only if $4 \mid (q-1)$.

Proof: ($\Rightarrow$) We will prove the counterpositive. This is, we will prove that if $4 \nmid (q-1)$, then $\pi(x)$ does not decompose in cycles of length two. Suppose that $4 \nmid (q-1)$ and let α be a primitive root in F_q. Since the coefficient of x in $\pi(x)$ is $a = 0$, then from Proposition 4 we have that for all $0 \le i \le q-2$, where i is even $\pi(\alpha^i) = \alpha^i$. Since there are $q-1$ possible values for i, this means that there are $\frac{q-1}{2}$ values of i that are even and therefore $\frac{q-1}{2} + 1$, fixed points counting the fixed point 0. Suppose that $\pi(x)$ decomposes in cycles of length two, this means that the $\frac{q-1}{2}$ elements that are not fixed points are contained in cycles of length two. Therefore we have, $\frac{q-1}{4}$ cycles of length two. But this is a contradiction because $4 \nmid (q-1)$. Hence $\pi(x)$ does not decompose in cycles of length two in F_q.

(⇐) Let $4|(q-1)$ and α be a primitive root in F_q. Suppose that $\pi(x)$ decompose in cycles of length two. This is $\pi(\pi(\alpha))=\alpha$, and $((\alpha)^{\frac{q+1}{2}})^{\frac{q+1}{2}} = ((\alpha)^{\frac{q-1}{2}}\alpha)^{\frac{q+1}{2}} = (-\alpha)^{\frac{q+1}{2}} =$ $(-\alpha)^{\frac{q-1}{2}}(-\alpha) =$ $(-1)^{\frac{q-1}{2}}(\alpha)^{\frac{q-1}{2}}(-\alpha) =$ $(-1)^{\frac{q-1}{2}}(\alpha)$. Now, since $4|(q-1)$, this means that $4k=q-1, k\in \mathrm{Z}$ and $\frac{q-1}{2}=2k$. This means that $(-1)^{\frac{q-1}{2}} = (-1)^{2k} = 1$ and $\pi(\pi(\alpha))=\alpha$. Hence $\pi(x)$ decompose in cycles of length two. □

Proposition 7. Let $\pi(x) = x^{\frac{q+1}{2}} + ax$, $a \neq 0$ be a permutation of F_q that decomposes in cycles of length two, then $a^2 = 2$.

Proof: Let α be a primitive root in F_q. Since $\pi(x)$ is a permutation that decomposes in cycles of length two. Then for all $0 \le i \le q-2$, that is not a fixed point we have that $\pi^2(\alpha^i) = \alpha^i$. This is $((\alpha^{\frac{q-1}{2}}\alpha)^i + a\alpha^i)^{\frac{q+1}{2}} + a((\alpha^{\frac{q-1}{2}}\alpha)^i + a\alpha^i) = \alpha^i$ such that $((-\alpha)^i + a\alpha^i)^{\frac{q+1}{2}} + a((-\alpha)^i + a\alpha^i) = \alpha^i$. This has to be true for all i even and odd. Therefore, when i is even or odd, we have that $\alpha^i(a-1)(a-1) = \alpha^i$ or $\alpha^i(a+1)(a+1) = \alpha^i$ which implies that $a=0$ or $a=-2$, but these coefficients generates fixed points. Also when i is odd or even we have that $\alpha^i(a+1)(a-1) = \alpha^i$ which implies that $a^2 = 2$. Hence if $\pi(x)$ gives a permutation of F_q that decomposes in cycles of length two, then $a^2 = 2$. □

Studying the necessary and sufficient conditions for $\pi(x)$ to decompose in cycles of length two we have reach an important conjecture, that is establish below.

Conjecture 2. Let α be such that $a^2 - 1$ is a quadratic residue mod q and suppose that $a^2 = 2 \bmod q$. Then the binomial $\pi(x) = x^{\frac{q+1}{2}} + ax$ decomposes in cycles of length two in F_q or $\pi(x) = x^{\frac{q+1}{2}} - ax$ decomposes in cycles of length two in F_q.

Proposition 8. There are fields for which no binomial of the form $\pi(x) = x^{\frac{q+1}{2}} + ax$ where $a^2 - 1$ is a quadratic residue, produces a permutation of F_q that decompose in cycles of length two.

Example 5. Z_{11} is a field for which no binomial of the form $\pi(x) = x^{\frac{q+1}{2}} + ax$ produces a permutation that decomposes in cycles of length two.

4. Conclusions and Work in Progress

In this section, we present necessary conditions for the binomial permutation $\pi(x) = x^{\frac{q+1}{2}} + 2x$ to decompose in cycles of length two. Also we presented that certain types of binomials never give permutations of F_q. Furthermore we presented a variety of conjectures. The first one states that a certain type of binomial never gives a permutation and the other one state the sufficient condition for a permutation binomial to decompose in cycles of length two. We plan for our future work to find and characterize the fields for which no binomial of the form $\pi(x) = x^{\frac{q+1}{2}} + ax$ is a permutation binomial of F_q, that decomposes in cycles of length two. Also we want to study other binomials. Last but not least we want to prove the conjecture or find a counterexample.

5. Acknowledgements

This work has been supported in part by the National Security Agency, Grant Number H98230-04-C-0486; and the National Science Foundation CSEMS Program at the UPRH, Grant Number 0123169.

6. References

Journals

1. R. Lidl, H. Niederreiter, Encyclopedia of Mathematics and its applications: Finite Fields. Cambridge University Press, 1997, 20.
2. L. Cruz, "*Permutations that Decompose in Cycles of Length 2 and are Given by Monomials*", Proceedings of the NCUR. (April, 2005).
3. A. Cáceres, & O. Colón, "*Some Criteria for Permutation Binomials*", (September, 1997), University of Puerto Rico at Humacao.