Proceedings of The National Conference
On Undergraduate Research (NCUR) 2006
The University of North Carolina at Asheville
Asheville, North Carolina
April 6-8, 2006

Permutations that Decompose in Cycles of Length 2 and are Given by Monomials

Louis J. Cruz
Department of Mathematics
University of Puerto Rico at Humacao
Humacao, Puerto Rico

Faculty Advisor: Dr. Ivelisse Rubio

Abstract

In this paper permutations of finite fields F_q given by monomials ax^i are studied In particular, the necessary and sufficient conditions in the coefficient *a* and the exponent i to obtain permutations that decompose into cycles of length 2 are studied.

Keywords: Permutations, Cycles, Finite Fields.

1. Introduction

A permutation is a reordering of the elements in a set. Our principal interest is to find permutations of finite fields that decompose in cycles of length 2. We study permutations of $F_{q,}$ $q = p^r$, *p* prime, that are given by monomials of the form ax^i and decompose in cycles of length 2. Here we present some partial results on the necessary and sufficient conditions on the coefficient *a* and the exponent *i* to obtain this type of permutations.

Permutations can be used for the construction of interleavers for error control codes. Error control codes are used in communications systems to protect the information of errors that can occur during transmission. Permutations that decompose in cycles of length 2 are particularly useful because they are their own inverse and hence the same technology can be used for encoding and decoding.

2. Preliminaries

We begin by presenting the necessary background for the rest of the paper.

2.1. Finite fields

We are interested in permutations of finite fields F_q. The following concepts and results about finite fields will be used in the rest of the paper.

Let **F** be a non-empty set with two operations $(+,*)$. We say that **F** is a *field* if it satisfies the following properties. For all a,b,c , in **F** one must have,

1) If $a \in$ **F** and $b \in$ **F**, then $a + b \in$ **F**.
2) $a + (b + c) = (a + b) + c.$
3) $a + b = b + a.$
4) There is an element 0_F in **F** such that $a + 0_F = a = 0_F + a$ for every $a \in$ **F.**
5) For each $a \in$ **F**, the equation $a + x = 0_F$ has a solution in **F.**
6) If $a \in$ **F** and $b \in$ **F**, then $a * b \in$ **F**.
7) $a * (b * c) = (a * b) * c.$
8) $a * b = b * a$ for all $a, b \in$ **F**.
9) There exist an element $1_F \neq 0_F$ such that $a * 1_F = a = 1_F * a$ for all $a \in$ **F**.
10) For each $a \neq 0_F$, the equation $a * x = 1_F$ has a solution in **F**.
11) $a * (b + c) = a * b + a * c$, and $(a + b) * c = a * c + b * c.$

A *finite field* is a field with a finite number of elements. It is well known that every finite field has $q = p^r$ elements, where *p* is a prime number. The none-zero elements of a finite field, $F_q^* := F_q \setminus \{0\}$, can be generated by a single element called a primitive root. More formally,

Definition 1. *Let* $\alpha \in F_q$. *We say that* α *is a* ***primitive root*** *of* F_q *if and only if* α *generates all the elements of*

$F_q^* = F_q \setminus \{0\}$. This is, $F_q^* = \{\alpha^{0,}, \alpha^1, ..., \alpha^{q-2}\}.$

Example 1. *In* Z_{13}, *2 is a primitive root. Note that,*

$$2^0 = 1,\ 2^1 = 2,\ 2^2 = 4,\ 2^3 = 8,\ 2^4 = 3,\ 2^5 = 6,\ 2^6 = 12, 2^7 = 11,\ 2^8 = 9,\ 2^9 = 5,\ 2^{10} = 10,\ 2^{11} = 7\,.$$

It is known that every finite field F_q has a primitive root α and it is easy to see that $\alpha^{q-1} = 1$. The next proposition follows easily from this fact.

Proposition 1. *Let* $\alpha \in F_q^*$. *Then ,* $\alpha^{q-1} = 1.$

Definition 2. *Let* $\alpha \in Z_n$ *and gcd* $(\alpha, n) = 1$. *We say that j is the* ***order*** *of* α *in* Z_n *and write* $j = ord_n(a)$ *if j is the smallest positive integer such that* $\alpha^j \equiv 1$*(mod n). Similarly, we say that j is the order of* α *in* F_q *if j is the smallest positive integer such that* $\alpha^j \equiv 1$ *(mod q).*

Note that, in Example 1, the smallest positive integer j such that $2^j \equiv 1$ (mod 13) is 12. This is not a coincidence; in fact, the order of a primitive root in F_q is always *q-1*.

2.2. Permutations

A *permutation* π of a set A is a bijection $\pi : A \rightarrow A.$ Let F_q be the finite field with q elements. It is well known that a monomial $ax^i, a \in F_q^*$ gives a permutations of F_q if and only if *gcd(i, q-1)=1.* We call this type of monomials *permutation monomials.*

Example 2. *Let* $A = Z_{11}$ *and define* $\pi : Z_{11} \rightarrow Z_{11}$ *by* $\pi(x) = x^3$. *Since gcd(3,10) = 1,* $\pi(x)$ *is a permutation monomial of* Z_{11}. *This permutation can be represented in the following way, where all the elements of the domain are in the first row and in the second row is their image:*

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

Another way to represent permutations is with its decomposition in cycles. To represent the permutations in this way one takes an initial value *b* and place it in the beginning of a cycle *(b).* Then take the value that we obtained when evaluating *b* in $\pi(x)$ and place it to the side of *b.* Now take π *(b)* and evaluate it again in the same function. If when doing this one obtains the initial value *b*, then the cycle finishes and the cycle is *(b* π *(b)).* If not, one repeats the evaluation with the previous result until the initial value *b* is obtained.

Note that the elements in the cycle are the result of composing the function with itself and evaluating it in *b*. The cycle finishes when one obtains the initial value b. Each cycle will have the form, $(b \;\; \pi(b) \;\; \pi(\pi(b)) \ldots \pi^n(b) = b)$ where $\pi^n(b)$ means π composed with itself *n* times and evaluated in *b,* and *n* is the smaller value so that $\pi^n(b) = b$. If $\pi(b) = b$, then *b* is called a fixed point and one does not write the cycle.

Continuing with the previous example, the cyclic decomposition of the permutation of Z_{11} given by $\pi(x) = x^3$ is:

(2 8 6 7) (3 5 4 9).

We are interested in permutations of F_q given by monomials ax^i that decompose in cycles of length 2. For example, the permutation of Z_{13} given by $\pi(x) = 2x^{11}$ decomposes in cycles of length 2. The permutation is:

$$\begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 0 & 2 & 1 & 5 & 7 & 3 & 9 & 4 & 10 & 6 & 8 & 12 & 11 \end{pmatrix}.$$

The cyclic decomposition of this permutation is:

(1 2) (3 5) (4 7) (6 9) (10 8) (11 12).

3. Permutation Monomials

A *permutation monomial* in A is a monomial such that when it is evaluated in the elements of A produces a permutation of A. Consider F_q, the finite field with *q* elements. It is well known that the function $\pi : F_q \rightarrow F_q$ defined by $\pi(x) = ax^i, a \in F_q^{\,*}$, produces a permutation of F_q if and only if *gcd(i, q-1)=1.* We are interested in permutations of F_q that decompose in cycles of length 2 and are obtained using monomials ax^i.

3.1. Permutation monomials x^i

Theorem 2 in [2] gives the necessary and sufficient conditions to obtain permutation monomials x^i that decompose in cycles of the same length. The following proposition is a corollary to Theorem 2 and gives the necessary and sufficient conditions on the exponent *i* to obtain permutations that decompose in cycles of length 2 and are given by monomials x^i.

Proposition 2. *Let* $q-1=p_1^{k_1}p_2^{k_2}...p_r^{k_r}, k_i \in Z, k_i \geq 1$. *The permutation of* F_q *given by* x^i *decomposes in cycles of the length 2 if and only if one of the followings holds for each l=1…r.*

1) $i \equiv 1 \pmod{p_l^{k_l}}$
2) $2 = ord_{p_l^{k_l}}(i)$

Example 3. *Consider* Z_{17}. *Table 1 illustrates Proposition 2.*

Table 1. cyclic decomposition of permutations given by x^i and the order of i mod 16.

i	Cyclic decomposition	$ord_{2^4}(i)$
3	(2 8) (3 10 14 7) (4 13) (5 6 12 11) (9 5)	4
5	(2 15) (3 5 14 12) (6 7 11 10) (8 9)	4
7	(2 9) (3 11) (4 13) (5 10) (6 14) (7 12) (8 15)	2
9	(3 14) (5 12) (6 11) (7 10)	2
11	(2 8) (3 7 14 10) (4 13) (5 11 12 6) (9 15)	4
13	(2 15) (3 12 14 5) (6 10 11 7) (8 9)	4
15	(2 9) (3 6) (4 13) (5 7) (8 15) (10 12) (11 14)	2

Also in [2], Theorem 5 gives a formula for counting the number of monomials x^i that produce permutations of F_q that decompose in cycles of the same length *j*. The following proposition is a corollary to this theorem and counts the number of monomials x^i that decompose in cycles of length 2.

Proposition 3. *Let* $q-1=2^k p_1^{k_1}...p_r^{k_r}, k, k_i \in Z, k \geq 0,\ k_i \geq 1$. *The number of permutations* x^i *of* F_q *that decompose in cycles of length 2 is:*

$$\begin{cases} 2^r - 1 & if \quad k = 0{,}1 \\ 2^{r+1} - 1 & if \quad k = 2 \\ 2^{r+2} - 1 & if \quad k \geq 3 \end{cases}.$$

Note that this proposition predicts that there are 3 monomials x^i that produce permutations of Z_{17} that decompose in cycles of length 2 and this is exactly what we saw in Example 3.

The previous results apply to case of monomials of the form x^i . The purpose of this work is to generalize these results. We want to find results for monomials ax^i where $a \in F_q^*, a \neq 1$. We found that, in some cases, ax^i decompose in cycles of length 2 for all $a \in F_q^*$, in others, we need additional conditions to obtain cycles of length 2 for $a \neq 1$. Here we present some partial results of when the permutations given by ax^i decompose in cycles of length 2.

Our first result presents a case where the permutations given by ax^i decompose in cycles of length 2 for all $a \in F_q^{\ *}$.

Theorem 1. *Let* $\pi(x) = ax^{q-2}, a \in F_q^{\ *}$. *Then* π *gives a permutation of* F_q *that decomposes in cycles of length 2 for all* $a \in F_q^{\ *}$.

Proof: We first prove that ax^{q-2} is a permutation monomial of F_q. We have to see that *gcd(q-1, q-2)=1.*

Suppose that *d* is the greatest common divisor of *q-2* and *q-1*. Then *q-2=dk* and *q-1=dl* where *k,l* $\in Z$. This implies that *dl=q-1=q-2+1=dk+1* and *dl=dk+1*. Therefore *d(l-k)=1* and this implies that *d* divides 1. Since *d* is a positive integer, *d=1*. Hence ax^{q-2} is a permutation monomial of F_q.

To construct the cycles of the permutation of F_q given by ax^{q-2}, an element $b \in F_q^{\ *}$ is evaluated in the function $\pi(x) = ax^{q-2}$ and the result is evaluated again in the same function to obtain:

$$(b \quad ab^{q-2} \quad a(ab^{q-2})^{q-2} ...)$$

To have cycles of the length 2, we must have, $a(ab^{q-2})^{q-2} = b$. Now,

$$a(ab^{q-2})^{q-2} = a^{q-1}b^{q^2-4q+4} = a^{q-1}b^{(q-1)(q-3)+1} = a^{q-1}(b^{q-3})^{q-1}b.$$

Using Proposition 1, we have that $a^{q-1}(b^{q-3})^{q-1}b = b$ and therefore the cycles have length 2.

□

Before, we mentioned that the monomials ax^i are permutations monomials of F_q if and only if *gcd(q-1,i) =1*. The next lemma gives the condition for the monomials $ax^{\frac{q-3}{2}}$.

Lemma 1. *Let* $q = p^r$, $p \neq 2$. *Then* $ax^{\frac{q-3}{2}}$ *is a permutation monomial of* F_q *if and only if 4 | (q-1).*

Proof: $(\Leftarrow)$ Suppose that *4 | (q-1)*. Then *q-1=4k*. To see that $ax^{\frac{q-3}{2}}$ gives permutation of F_q, we must prove that $\gcd\left(q-1, \quad \frac{q-3}{2}\right)$ *=1.*

Since $\frac{q-3}{2} = \frac{q-1-2}{2}$, replacing *q-1* by *4k* , we obtain: $\frac{q-3}{2} = \frac{4k-2}{2}$ =2*k-1*. Therefore $\gcd\left(q-1, \quad \frac{q-3}{2}\right)$ *=1* if and only if *gcd(4k, 2k-2)=1.*

Suppose that *d* is the greatest common divisor of *4k* and *2k-1*. Then , *4k=dl* and *2k-1=dm* for some *l,m* $\in Z$. Now multiplying *2k-1* by 2, we obtain *4k-2=2dm*. But from the first equation we have that *4k-2=dl-2*. Hence, *dl-2=2dm*. This implies that *2=d(l-2m)* and *d* divides *2*. Since *d* is a positive integer, this means that that *d=1 or d=2.*

Since *d* divide *2k-1*, *d* must be 1. Therefore, *gcd* $\left(q - 1, \frac{q - 3}{2} \right)$ = *gcd(4k, 2k-1)=1*. This implies that $ax^{\frac{q-3}{2}}$ is a permutation monomial of F_q .

$(\Rightarrow)$ Suppose that $ax^{\frac{q-3}{2}}$ is a permutation monomial of F_q . Then *gcd* $\left(\frac{q-3}{2}, \quad q-1 \right)$ =1. Also $p \neq 2$ and $q = p^r$ imply that *2* | *(q-1)*. Now *gcd* $\left(\frac{q-3}{2}, \ q-1 \right)$ =1 implies that *2* does not divide $\frac{q - 3}{2}$. Therefore, $\frac{q-3}{2}$ *=2k+1,k*$\in Z$. Now solving for *q*, we obtain that *q=4k+4+1*. This implies that *q-1=4(k+1)* and hence, *4|(q-1).*

□

It is known that the permutations given by $x^{\frac{q-3}{2}}$ decompose in cycles of length 2 (see [3]), but when the coefficient of $ax^{\frac{q-3}{2}}$ is not equals to 1 not all the permutations decompose in cycles of length 2. The next theorem gives the necessary and sufficient conditions such that $ax^{\frac{q-3}{2}}$ gives a permutations of F_q that decompose in cycles of length 2.

Theorem 2. *Let* $q = p^r, p \neq 2$ *and let* α *be a primitive root of* F_q. *Then* $ax^{\frac{q-3}{2}}$ *gives a permutation of* F_q *that decompose in cycles of length 2 if and only if* $a = \alpha^{2k}, k \in Z$ *and 4 | (q-1).*

Proof: $(\Leftarrow)$ Suppose that *4 | (q-1)* and $a = \alpha^{2k}$. Then, by the previous lemma, $ax^{\frac{q-3}{2}}$ is permutation monomial of F_q .

To construct the cycles of the permutation of F_q given by $ax^{\frac{q-3}{2}}$, an element $b \in F_q^*$ is evaluated in the function $\pi(x) = \alpha^{2k} x^{\frac{q-3}{2}}$ and the result is evaluated again in the same function.

$$\left(b \quad \alpha^{2k} b^{\frac{q-3}{2}} \quad \alpha^{2k} \left(\alpha^{2k} b^{\frac{q-3}{2}} \right)^{\frac{q-3}{2}} = \alpha^{2k} \alpha^{2k\left(\frac{q-3}{2}\right)} b^{\left(\frac{q-3}{2}\right)\left(\frac{q-3}{2}\right)} \ldots \right).$$

To have cycles of length 2, one must have that, $\alpha^{2k} \alpha^{2k\left(\frac{q-3}{2}\right)} b^{\left(\frac{q-3}{2}\right)\left(\frac{q-3}{2}\right)} = b$. Now,

$$\alpha^{2k} \alpha^{2k\left(\frac{q-3}{2}\right)} b^{\left(\frac{q-3}{2}\right)\left(\frac{q-3}{2}\right)} = \alpha^{2k\left(1+\frac{q-3}{2}\right)} b^{\frac{q^2-6q+9}{4}} = \alpha^{2k\left(\frac{q-1}{2}\right)} b^{\frac{(q-1)(q-5)+4}{4}} = \left(\alpha^{q-1}\right)^k \left(b^{q-1}\right)^l b \, ,$$

where $l = \frac{q-5}{4} = \frac{q-1-4}{4} \in Z$ because *4 | (q-1)*. Using Proposition 1, we have that $\left(\alpha^{q-1}\right)^k \left(b^{q-1}\right)^l b = b$, and therefore the cycles have length 2.

$(\Rightarrow)$ Since $\pi(x) = ax^{\frac{q-3}{2}}$ is permutation of F_q, Lemma 1 implies that *4 | (q-1)*. Now, let $a = \alpha^i$ and $b \in F_q^*$. We have two cases: 1) b is in a cycle of length 2, or 2) b is a fixed point.

Case 1): Suppose that $b \in F_q^*$ is in a cycle of length 2. Then , $\alpha^i \left(\alpha^i b^{\frac{q-3}{2}}\right)^{\frac{q-3}{2}} = b$. Now we simplify $\alpha^i \left(\alpha^i b^{\frac{q-3}{2}}\right)^{\frac{q-3}{2}}$ and obtain $\alpha^i \alpha^{i\left(\frac{q-3}{2}\right)} b^{\frac{q^2-6q+9}{4}} = \alpha^{i\left(\frac{q-1}{2}\right)} b^{\frac{q^2-6q+9}{4}} = b$. Now we rewrite $b^{\frac{q^2-6q+9}{4}}$ as $b^{(q-1)\left(\frac{q-5}{4}\right)+1} = b^{(q-1)l} b = b$, where $l = \frac{q-5}{4}$ and *l* is an integer. By Proposition 1 we have that $(b^{(q-1)l})b = b$. This implies that $b = \alpha^{i\left(\frac{q-1}{2}\right)} b^{\frac{q^2-6q+9}{4}} = \alpha^{i\left(\frac{q-1}{2}\right)} b$. This implies that $\alpha^{i\left(\frac{q-1}{2}\right)} = 1$ and hence $i\left(\frac{q-1}{2}\right) \equiv 0 \mod (q-1)$. Therefore $i\left(\frac{q-1}{2}\right) = (q-1)k,\ k \in Z$. Therefore, *i=2k* $k \in Z$ and $a = \alpha^{2k}$.

Case 2): Suppose now that b is a fixed point. This means that $\alpha^i b^{\frac{q-3}{2}} = b$. Hence, $\alpha^i = b^{1-\frac{q-3}{2}} = b^{-\left(\frac{q-5}{2}\right)}$. Since *q-1=4k*, $k \in Z$,$\frac{q-5}{2} = \frac{q-1-4}{2}$ *=2k-2, l=k-1*,Also, since α is a primitive root in F_q, $b = \alpha^j$ for some $j \in Z$. Therefore, $\alpha^i = \left(\alpha^{-j}\right)^{\frac{q-5}{2}} = \left(\alpha^{-j}\right)^{2l}$. This implies that $i = 2h$, some $h \in Z$ and hence $a = \alpha^{2h}$.

□

4. Conclusions and work in progress

The results presented on this paper are partials results. We found necessaries and sufficient conditions in the coefficient *a*, of some monomials ax^i, to obtain permutations that decompose in cycles of length 2. We are still working on the following problems.

1. Given any exponent *i* such that x^i decomposes in cycles of length 2, find the necessary and sufficient conditions on the coefficient *a* such that ax^i also decompose in cycles of length 2.
2. Are there permutations given by ax^i that decompose in cycles of length 2 even if the permutation given by x^i does not decompose in cycles of length 2?
3. Is there another exponent *i* such that ax^i decompose in cycles of length 2 for all $a \in F_q^*$?

5. Acknowledgments

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

Books

1. Rudolf Lidl and Harlald Neidderreiter, *Encyclopedia of Mathematics and its Applications Vol 20, Finite Fields*", 2^{nd} ed. (United Kingdom: Cambridge University Press, 1997).

2. I. Rubio and C. Corrada-Bravo, " Cyclic Decomposition of Permutations of Finite Fields Obtained using Monomials and Applications to Turbo Codes", in *Finite Fields and Applications*, LNCS 2948, ed. Mullen, Poli, Stichtenoth (New York: Springer, 2004), 254.

3. Thomas Hungerford, *Abstrac Algebra: An Introduction,* 2^{nd} ed. (Florida: Saunders, 1997).

Journals

4. Yara B. Luis and Luis O. Pérez, "Permutations of Z_{p^r} , constructed using several monomial orderings", Proceedings of the 2005 NCUR. (April, 2005).