Proceeding of The National Conference
On Undergraduate Research (NCUR) 2005
Washington and Lee University
Virginia Military Institute
April 21 – 23, 2005

Permutations of Z_q constructed using several monomial orderings

Yara B. Luis
University of Puerto Rico
Department of Mathematics
Humacao, PR 00791-4300

Luis O. Pérez
University of Puerto Rico
Department of Mathematics
Humacao, PR 00791-4300

Faculty Advisor: Dr. Ivelisse Rubio

Abstract

A permutation is an ordered arrangement of a set. A monomial x^i in $F_q[x]$ gives a permutation of the finite field F_q if the function x^i: $F_q \rightarrow F_q$ is a bijection. We construct permutations of Z_q in the following manner: first we associate the elements of F_q, $q=p^r$ to r-tuples of non-negative integers, then we use monomial orderings to order the elements. In this way elements of F_q are associated to elements of Z_q. Finally we apply the monomial x^i to obtain the permutation. We prove that one can obtain permutations obtained with other constructions using monomial orderings. Furthermore, using these monomial orderings we also obtain other permutations, some of which have better dispersion and spreading properties than the ones that we already knew.

1. Introduction

A monomial x^i in $F_q[x]$, $q=p^r$ gives a permutation of the finite field F_q if the function x^i: $F_q \rightarrow F_q$ is a bijection. This happens if and only if $(q-1,i)=1$. We associate the elements of F_q to r-tuples of non-negative integers. Then we order these r-tuples using several monomial orderings. These orderings allow us to create a correspondence between the elements of F_q and the elements of Z_q. The importance of this correspondence relies on the fact that we can construct interleavers, which are an important component of turbo codes, using permutations of Z_q. Hence we can apply our permutations to construct turbo codes.

Our paper is structured as follows: We begin with the "Monomial Ordering" section which has the definitions of two types of monomial orderings and some examples. Then we move on to the "Ordering F_q using Monomial Orderings" section where we show the method we utilize to order the elements of the finite field. On section four we present our result on how to obtain permutations of Z_q from permutations of F_q. We also discuss permutation monomials which are the monomials that let us construct the desired permutations once the elements of the finite field are ordered. Section five refers to the interleaver and some of its properties. In section six we give information about the different types of interleaver constructions that exist. The remaining sections state the computational results of our research, the future work we will be conducting, the acknowledgments and the references used in the course of this research.

2. Monomial Ordering

We start by enunciating a few definitions that will help us understand better the way we order elements of F_q and hence the correspondence between F_q and Z_q. It is possible to represent monomials in $F_q[x_1, x_2, \ldots, x_r]$ as vectors of length r and then order these vectors using monomial orderings. We

associate a monomial $x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_r^{\alpha_r} \in F_q[x_1, x_2, \ldots, x_r]$ to the r-tuple of exponents $(\alpha_1, \alpha_2, \ldots \alpha_r) \in Z_{\geq 0}^r$.

Definition 1. Monomial Ordering

Let *K* be a field. A monomial ordering on the polynomial ring $K[x_1, x_2, \ldots, x_r]$ is any relation > on the set of monomials $x^\gamma, \gamma \in Z_{\geq 0}^r$ satisfying the following properties:

i. > is a lineal ordering on $Z_{\geq 0}^r$.

ii. If $\gamma > \delta$ and $\kappa \in Z_{\geq 0}^r$, then $\gamma + \kappa > \delta + \kappa$.

iii. > is a well-ordering on $Z_{\geq 0}^r$.

The first type of monomial orderings that we will utilize is the Lexicographic Ordering. Intuitively, ordering monomials in this way is similar to the method used to order the words in a dictionary. The following is the formal definition.

Definition 2. ***Lexicographic Order***

Let $\gamma = (\gamma_1, \gamma_2, \ldots, \gamma_r)$ and $\delta = (\delta_1, \delta_2, \ldots, \delta_r) \in Z_{\geq 0}^r$. We say that $\gamma >_{lex} \delta$ if, in $\gamma - \delta \in Z^r$, the left-most nonzero entry is positive. We say $x^\gamma >_{lex} x^\delta$ if $\gamma >_{lex} \delta$.

Example 1. $\gamma = (0,1,0) >_{lex} (0,0,1) = \delta$ since $\gamma - \delta = (0,1,-1)$.

Unlike the Lexicographic Ordering there are several monomial orderings that take in consideration the total degree of the monomials. The Graded Lex Order is one of such monomial orderings.

Definition 3. Graded Lex Order

Let $\gamma, \delta \in Z_{\geq 0}^r$. We say that $\gamma >_{grlex} \delta$ if $|\gamma| = \sum_{i=1}^r \gamma_i > \sum_{i=1}^r \delta_i = |\delta|$ or $|\gamma| = |\delta|$ and $\gamma >_{lex} \delta$

Example 2. $\gamma = (0,1,1) >_{grelex} (1,0,0) = \delta$ since $|(0,1,1)| = 2 > |(1,0,0)| = 1$.

When there is a "tie" between the degrees of the monomials the Lexicographic Ordering is used to break those ties. The following example illustrates this situation.

Example 3. $\gamma = (0,0,1) >_{grlex} (0,0,1) = \delta$ since $|(0,1,0)| = |(0,0,1)|$ and $(0,1,0) >_{lex} (0,0,1)$.

3. Ordering F_q using Monomial Orderings

To be able to construct permutations of Z_q from permutations of F_q we first need to order the elements of F_q.

Consider the following ordering of the elements of the finite field $F_q : \{\xi_0, \xi_1, \ldots, \xi_{q-1}\}$, where

$$\xi_n = n_{r-1}\beta_{r-1} + \cdots + n_1\beta_1 + n_0\beta_0,$$

$\{\beta_0, \beta_1, \ldots, \beta_{r-1}\}$ is a base for F_q over Z_p and $n = n_0 + n_1 p + \cdots + n_{r-1} p^{r-1}, 0 \leq n_i \leq p-1$.

We denote this order as ξ and we proved in [2] that this order is well defined. This ordering gives a natural correspondence between the elements of F_q and the elements of $Z_q : \xi_i$ correspond to *i*.

The representation of ξ_n as $n_{r-1}\beta_{r-1}+\cdots+n_1\beta_1+n_0\beta_0$ also induces a natural correspondences of the elements of ξ_n and the *r*-tuples in Z_p^r: ξ_n correspond to $(n_{r-1},\ldots,n_1,n_0)$. Now we can order the elements of F_q by ordering the corresponding *r*-tuples. For the reminder of this paper, τ denotes the ordering of the r-tuples associated to the elements of F_q with the Lexicographic Order and ϕ denotes the ordering of the r-tuples with the Graded Lex Order.

Consider $F_{2^3}=Z_2/\langle x^3+x^2+1\rangle$ with and let α be a primitive root of F_{2^3}. Note that we get a basis for F_{2^3} over Z_2 using the relation $\alpha^3=\alpha^2+1$. Table 1 shows the elements of F_{2^3} along with its *r*-tuple representation, the representation as powers of α and the ordering with the Lexicographic Order and the Graded Lex Order. The numbers in column *n* correspond to the ordering of the elements with the ξ ordering.

Table 1

n	F_q	α^j	*r*-tuple	τ	ϕ
0	0	0	(0,0,0)	0	0
1	1	α^0	(0,0,1)	1	1
2	α	α^1	(0,1,0)	2	2
3	$\alpha+1$	α^5	(0,1,1)	3	4
4	α^2	α^2	(1,0,0)	4	3
5	α^2+1	α^3	(1,0,1)	5	5
6	$\alpha^2+\alpha$	α^6	(1,1,0)	6	6
7	$\alpha^2+\alpha+1$	α^4	(1,1,1)	7	7

Note that the ξ ordering is equivalent to the Lexicographic ordering in the previous example. This equivalence always holds as it is shown below.

Theorem 1. The ordering ξ of the elements of F_q is equivalent to the Lexicographic ordering of the corresponding elements in Z_p^r.

Proof: Let $\xi_n=n_{r-1}\beta_{r-1}+\cdots+n_1\beta_1+n_0\beta_0$, $\xi_m=m_{r-1}\beta_{r-1}+\cdots+m_1\beta_1+m_0\beta_0$ for $0\le n_i,m_i\le p-1$ and

$$n=\sum_{l=o}^{r-1}n_l p^l,\ m=\sum_{l=o}^{r-1}m_l p^l$$

Note that ξ_n and ξ_m can be represented as *r*-tuples in the following way

$$\begin{aligned}\vec{n} &= (n_{r-1},\ldots,n_{i+1},n_i,\ldots,n_0)\in Z_p^r \quad \text{and}\\ \vec{m} &= (\mathrm{m_{r-1}},\ldots,\mathrm{m_{i+1}},\mathrm{m_i},\ldots,\mathrm{m_0})\in \mathrm{Z_p^r}.\end{aligned}$$

We want to show that $\vec{n}>_{lex}\vec{m}$ implies that $n>m$. This is the same as showing that

$$\sum_{l=0}^{r-1} n_l p^l > \sum_{l=0}^{r-1} m_l p^l .$$

Note that $\vec{n} >_{lex} \vec{m}$ implies that in

$$\vec{n} - \vec{m} = (n_{r-1} - m_{r-1}, \ldots, n_{i+1} - m_{i+1}, n_i - m_i, \ldots, n_0 - m_0) \in Z^r ,$$

the first integer from left to right not equal to zero is positive. This implies that for some $0 \le i \le r-1$ $\mathrm{n_k} = \mathrm{m_k}$ for all $\mathrm{k > i}$ and $n_i > m_i$. Since $\mathrm{n_k} = \mathrm{m_k}$ for all $\mathrm{k > i}$, to see that $n > m$ we only have to show that

$$\sum_{l=0}^{i} n_l p^l - \sum_{l=0}^{i} m_l p_l > 0.$$

This is the same as proving that

$$\sum_{l=0}^{i} (n_l - m_l) p^l > 0.$$

This

$$(n_i - m_i) p^i + \sum_{l=0}^{i-1} (n_l - m_l) p^l > 0 .$$

Now since $n_i > m_i$ we have $(n_i - m_i) p^i > 0$ and we only have to see that

$$(n_i - m_i) p^i > \left| \sum_{l=0}^{i-1} (n_l - m_l) p^l \right|.$$

Since $n_i > m_i$ the smallest value $n_i - m_i$ can take is 1 and the maximum value that $\left| \sum_{l=0}^{i} -1 (n_l - m_l) p^l \right|$ can take is obtained when $|n_l - m_l| = p-1$, for each $l = 0, \ldots, i-1$. By the Geometric Series we have that

$$\left| \sum_{l=0}^{i-1} (n_l - m_l) p^l \right| \le \left| \sum_{l=0}^{i-1} (p-1) p^l \right| = \sum_{l=0}^{i-1} (p-1) p^l = (p-1)\left(\frac{p^i - 1}{p-1} \right) = p^i - 1 < p^i \le (n_i - m_i) p^i$$

Hence $n = \sum_{l=0}^{r-1} n_l p^l > \sum_{l=0}^{r-1} m_l p^l = m$ if $\vec{n} >_{lex} \vec{m}$.

Since these orderings are total, they represent the same orderings on the elements of F_q.

4. Permutation Monomials

Now that we know how to order the elements of a finite field, we can introduce the function that we use to construct permutations of F_q and hence permutations of Z_q.

Definition 5. A monomial $x^i \in F_q[x]$ is a *permutation monomial* if and only if the polynomial function $f : F_q \to F_q ; \quad f(x) = x^i$ is a permutation of the finite field F_q.

Example 5. The function $\pi(x) : F_7 \to F_7$, $\pi(x) = x^5$ is a permutation monomial of F_7 and it can be represented as

$$\pi = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ 0 & 1 & 4 & 5 & 2 & 3 & 6 \end{pmatrix}.$$

On this representation, the elements of the first row are the elements of F_7 and the elements of the second row are their images under π. The following is a well known characterization of permutation monomial.

Theorem 2. The monomial $x^i \in F_q[x]$ is a permutation monomial of F_q if and only if $\gcd(i, q-1) = 1$.

The next theorem tells us that we can use any permutation of F_q to obtain a permutation of Z_q. This is an obvious generalization of Theorem 1 in [2], which now we state as a corollary.

Theorem 3. Let $q = p^r$, p a prime, $\{\xi_0, \xi_1, \ldots, \xi_{q-1}\} = F_q$ and $f : F_q \to F_q$ any function. The function $\pi : Z_q \to Z_q$ defined as $\pi(n) = m$, where $f(\xi_n) = \xi_m$, is a permutation of Z_q if and only if f is a permutation of F_q.

Corollary 1. Let $f : F_q \to F_q$ be defined as $f(x) = x^i$, q and π as above. Then π is a permutation of Z_q if and only if $\gcd(i, q-1) = 1$.

Example 6. Let $F_{2^3} = Z_2 / \langle x^3 + x^2 + 1 \rangle$. We can construct a permutation of Z_{2^3} using the permutation monomial $f(x) = x^2$. From Table 1 we obtain the following relation among the element of F_8 ordered with the ξ order and the powers of the primitive root α

$$(\xi_0, \xi_1, \xi_2, \ldots, \xi_7) = (0, \alpha^0, \alpha^1, \alpha^5, \alpha^2, \alpha^3, \alpha^6, \alpha^4).$$

Evaluating each element in $x^2 \in F_{2^3}$ we get

$$(0, \alpha^0, \alpha^2, \alpha^3, \alpha^4, \alpha^6, \alpha^5, \alpha^1) = (\xi_0, \xi_1, \xi_4, \xi_5, \xi_7, \xi_6, \xi_3, \xi_2).$$

Taking the indices n from the ξ_n we construct the permutation π

$$\pi = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 0 & 1 & 4 & 5 & 7 & 6 & 3 & 2 \end{pmatrix}.$$

Recall from our previous section that the ξ ordering is equivalent to the Lex ordering; hence this permutation is the same if we order the elements of F_{2^3} with the Lexicographic Ordering. Now we present a permutation constructed with the same monomial but with the elements of F_{2^3} ordered using the Graded Lex Ordering.

Example 7. From Table 1 we obtain the following relation among the element of F_8 ordered with the Graded Lex Order and the powers of the primitive root α

$$(\phi_0, \phi_1, \phi_2, \ldots, \phi_7) = (0, \alpha^0, \alpha^1, \alpha^2, \alpha^5, \alpha^3, \alpha^6, \alpha^4).$$

Evaluating each element in $x^2 \in F_{2^3}$ we get

$$(0, \alpha^0, \alpha^2, \alpha^4, \alpha^3, \alpha^6, \alpha^5, \alpha^1) = (\phi_0, \phi_1, \phi_3, \phi_7, \phi_5, \phi_6, \phi_4, \phi_2).$$

Taking the indices n from the ϕ_n we obtain the permutation π

$$\pi = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 0 & 1 & 3 & 7 & 5 & 6 & 4 & 2 \end{pmatrix}$$

Note that this permutation is different from the one obtained with the lex ordering.

5. The interleaver and its properties

As we mentioned in the introduction once we have the permutations of Z_q we can use them as interleavers in the construction of turbo encoders.

An *interleaver* π is a bijective function $\pi : Z_q \to Z_q$. Two important properties associated to interleavers are the *spreading* and the *dispersion*.

The spreading measures how separated are elements that were originally close. It can be thought as measuring the randomness of the permutation. It has factors (s,t), if

$$|i-j| < s \Rightarrow |\pi(i) - \pi(j)| \geq t .$$

The spreading of the interleaver is the maximum value s such that $s \leq t$. Let q be the number of symbols to be permuted. The closest to $\sqrt{\frac{q}{2}}$ the spreading is, the better spreading the interleaver has.

The dispersion measures the regularity of the interleaver. It is defined as the number of elements in the set:

$$D(\pi) = \{(j-i, \pi(j) - \pi(i)), 0 \leq i < j < q\} .$$

The normalized dispersion is $\frac{2|D(\pi)|}{q(q-1)}$. The closest to 1 the dispersion is, the better it is.

To illustrate the computation of the dispersion, recall from Example 6 the following permutation of $F_{2^3} = Z_2 / \langle x^3 + x^2 + 1 \rangle$.

$$\pi = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 0 & 1 & 4 & 5 & 7 & 6 & 3 & 2 \end{pmatrix}$$

To obtain the dispersion we first find the list of the differences

(1, 3), (1, 1), (1, 2), (1,–1), (1, 3), (1,–1), (1,–2),
(2, 4), (2, 3), (2, 1), (2,–4), (2,–4), (2,–3),
(3, 6), (3, 2), (3,–2), (3,–5), (3,–6),
(4, 5), (4,–1), (4,–3), (4,–7),
(5, 2), (5,–2), (5,–5),
(6, 1), (6,–4),
(7,–1).

Note that $|D(\pi)| = 26$. Since we have $|D(\pi)|$, we can compute the normalized dispersion which is:

$$\frac{2|D(\pi)|}{q(q-1)} = \frac{2*26}{8(8-1)} \approx 0.9285714286$$

This is an excellent dispersion.

To compute the spreading of the permutation we look for the factors (s,t). Recall that we require that $s \le t$. The pairs $\left(|i-j|, |\pi(i)-\pi(j)|\right)$ are: $(1,3),(1,1),(1,2)$. Then, $s = 2$ and $t = 1$ note that $2 \not\le 1$. Therefore the spreading is 1.

Carlos Corrada, *UPR-Rio Piedras,* conjectured that the cyclic decomposition of the permutation is another important property of the interleaver.

6. Construction of Interleavers

Interleavers can be constructed either in a random or in an algebraic way. Currently the random construction is the one being used. Random interleavers have good properties but they need to be stored in memory and have to be analyzed by simulations. In the other hand, algebraic interleavers can be studied and analyzed before hand and do not have to be stored in memory. We study permutations obtained with other permutation monomials because most of the other known algebraic interleavers do not have good properties and we wish to find such interleavers with good properties. Another reason for studying permutation monomials is because it is believed that the cyclic decomposition of the permutation is important and there are results on the cyclic decomposition of monomial permutations [7]. In the next section we take a look at some of our results. From these one can see that we found permutations with very good dispersion properties.

7. Computational Results

We wrote programs in Maple to construct permutations using permutation monomials and the monomial orderings mentioned before. The following table shows some of the results obtained with the programs. The first column contains the finite fields, the second the exponents *i* of the monomials and the remaining columns contain the dispersion factor for permutations constructed with the ξ ordering (D_ξ) and the Graded Lex Ordering (D_ϕ) respectively.

Table 2

$F_q = Z_p / \langle p(x) \rangle$	i	D_ξ	D_ϕ
$F_8 = Z_2 / \langle x^3 + x^2 + 1 \rangle$	2	0.928571	0.750000
$F_8 = Z_2 / \langle x^3 + x^2 + 1 \rangle$	6	0.857143	0.857142
$F_{27} = Z_3 / \langle x^3 + 2x^2 + 1 \rangle$	17	0.880341	0.820512
$F_{27} = Z_3 / \langle x^3 + 2x^2 + 1 \rangle$	25	0.868946	0.831908
$F_{243} = Z_3 / \langle x^5 + x^4 + x^2 + 1 \rangle$	227	0.818590	0.818896
$F_{243} = Z_3 / \langle x^5 + x^4 + x^2 + 1 \rangle$	241	0.819304	0.811753
$F_{729} = Z_3 / \langle x^6 + x^5 + 2 \rangle$	605	0.815207	0.812399
$F_{729} = Z_3 / \langle x^6 + x^5 + 2 \rangle$	727	0.817664	0.812644
$F_{125} = Z_5 / \langle x^3 + x^2 + 2 \rangle$	119	0.817677	0.817419
$F_{125} = Z_5 / \langle x^3 + x^2 + 2 \rangle$	123	0.807613	0.818193

$F_{625} = Z_5 / \langle x^4 + x^3 + x + 3 \rangle$	31	0.801918	0.811918
$F_{625} = Z_5 / \langle x^4 + x^3 + x + 3 \rangle$	623	0.806277	0.813246

Rubio and Corrada worked with $q = p$ and found that the best dispersion was obtained when $i = q - 2$ and calculated $v = \frac{p+3}{2p}$ as the upper bound. The latter does not hold for our latest constructions (that consider $q = p^r, r \neq 1$) as can be observed in Table 2 where the best dispersion is obtained for exponents different from $i = q - 2$. Furthermore, we have obtained permutations with a spreading higher than one which was seldom observed in our previous work.

8. Future Work

We still have to study our results further in order to find any patterns that would help us characterize the permutation monomials that give algebraic interleavers with good properties. We also need to run simulations to see the performance of codes constructed with our interleavers and study the relation of the spreading, cyclic decomposition and dispersion if there is any. Additionally we need to construct permutation monomials with other monomial orderings.

9. Acknowledgments

We want to thank Professor Ivelisse Rubio, UPR- Humacao for her help on our research project. Part of this research has been funded by the UPR- Humacao CSEMS program, Grant # 0123169, NSA, Grant # H98230-04-C-0486 and AMP.

10. References

Technical Reports

1) Luis O. Pérez and Yara B. Luis, *Properties of a Type of Permutations over Finite Fields*, Progress Report, UPR-Humacao, 2003.
2) Y. Luis and L. Pérez-Báez, *Properties of a Class of Permutations Over Finite Fields and Applications to Turbo Codes, Proceedings of the Computing Research Conference, April 2004.*

Books

3) T. Hungerford, *Abstract Algebra*, 2nd edition , Saunders, 1997.
4) David Cox, John Little and Donal O'Shea, *Ideals, Varieties and Algorithms*, 2nd edition, Springer, 1996.
5) C. Heegard and S. Wicker, Turbo Coding, Kluwer, 1999

Journals (print)

6) C. Corrada and I. Rubio, *Deterministic Interleavers for Turbo Codes with Random-lik Performance and Simple Implementation*, Proceedings of the 3rd International Symposium on Turbo Codes, September 2003.
7) C. Corrada and I. Rubio, *Algebraic Construction of Interleavers using Permutation Monomials*, IEEE International Conference on Communications, 2004.
8) I. Rubio and C. Corrada, *Cyclic Decomposition of Permutations of Finite Fields Obtained Using Monomials*, Finite Fields and applications, LNCS 2948, pp 254-261, 2004.