PROPERTIES OF A CLASS OF PERMUTATIONS OVER FINITE FIELDS AND APPLICATIONS TO TURBO CODES

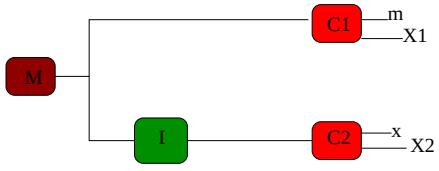
Yara B. Luis
Luis O. Perez
Ivelisse Rubio - Advisor
Department of Mathematics, University of Puerto Rico at Humacao

ABSTRACT

A permutation is an ordered arrangement of a set. A monomial x^i in $\mathbb{F}_q[x]$ gives a permutation of a finite field $\mathbb{F}_q$ if the function x^i:$\mathbb{F}_q \to \mathbb{F}_q$ is a bijection. Error control codes are used in digital communication systems to protect information from errors that might occur during transmission. Turbo encoders are very efficient codes with an important component, called the interleaver, which is a permutator. We have studied permutations of $\mathbb{F}_p = \mathbb{Z}_p$, where p is a prime, given by monomials. Here we discuss and present results and conjectures on some properties associated with good interleavers, namely their cyclic decomposition, dispersion and spreading. We describe a construction and study some properties of permutations of $\mathbb{Z}_q$ constructed using a particular ordering of the elements in the field extension $\mathbb{F}_q$ of $\mathbb{Z}_p$, for $q = p^r$ and permutations of $\mathbb{F}_q$.

1. INTRODUCTION

Error control codes are used in digital communication systems to protect information from errors that might occur during transmission. Turbo encoders are parallel concatenated encoders where two or more co- des are combined by an *interleaver* which is a permutator.



Two of the important properties of an *interleaver* are the spreading and the dispersion. We are constructing interleavers using permutations of $\mathbb{Z}_{p^r}$ and studying their properties with the intention of obtaining turbo encoders with good performance.

2. THE INTERLEAVER AND ITS PROPERTIES

An *interleaver* π is a function $\pi : \mathbb{Z}_q \to \mathbb{Z}_q$ that permutes the elements of $\mathbb{Z}_q$. This is, π is a bijection. Two important properties associated to interleavers are the *spreading* and the *dispersion*.

The spreading measures how separated are elements that were originally close. It has factors (s, t), where

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

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 randomness 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 $\frac{2|D(\pi)|}{q(q-1)}$. We say that we obtained a good dispersion if the normalized dispersion is close to 1.

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

3. CONSTRUCTION OF INTERLEAVERS

Interleavers can be constructed either in a random or in an algebraic way. The construction that is being used in actual applications is the random one. 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 in advance and do not have to be stored in memory. Unfortunally, most of the known algebraic interleavers do not have good properties. For this reason we want to construct algebraic

interleavers with good properties. Since it is believed that the cyclic decomposition of the permutation is important and there are results on the cyclic decomposition of monomial permutations [2], our first attempt will be to study permutations obtained using monomials.

4. PERMUTATIONS MONOMIALS

A monomial $x^i \epsilon\ \mathbb{F}_q[x]$ is a *permutation monomial* if the polynomial function $f : \mathbb{F}_q \to \mathbb{F}_q$; $f(x) = x^i$ is a permutation of the finite field $\mathbb{F}_q$. This happens if and only if $gcd(i, q-1) = 1$. For example, the function $\pi(x) : \mathbb{F}_7 \to \mathbb{F}_7$, $\pi(x) = x^5$ is a permutation and it can be represented as

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

The cyclic decomposition of this permutation is $(2\ 4)\ (3\ 5)$. The cyclic decomposition of permutations given by monomials has been studied in [2]. Since we are interested in the cyclic decomposition of the permutations, we will use this type of permutations.

In order to construct permutations of $\mathbb{Z}_{p^r}$ we are using permutations of $\mathbb{F}_{p^r}$ with a certain order of the elements of $\mathbb{F}_{p^r}$.

5. AN ORDERING OF $\mathbb{F}_q$, $q = p^r$

Consider the following order of the elements of a finite field $\mathbb{F}_q$:$\{\xi_0, \xi_1, \cdots, \xi_{q-1}\}$ where

$$\xi_n = n_1\beta_1 + n_2\beta_2 + \cdots + n_r\beta_r,$$

$\{\beta_1, \beta_2, \cdots, \beta_r\}$ is a base for $\mathbb{F}_q$ over $\mathbb{Z}_p$ and

$$n = n_1 + n_2 p + \cdots + n_r p^{r-1}, 0 \le n_i \le p-1.$$

Proposition 1. *The above order of $\mathbb{F}_q$ is well defined.*

Proof: We want to see that n takes every value between 0 and $q-1$. We know that there exist p^r possibilities for n, because we have p possibilities for each n_i .

Now, we want to see that $0 \le n < p^r$. Since we have that $0 \le n_i \le p-1$, then the smallest number that n_i can take is 0. This means that our smallest n is given by:

$$n = 0 + 0p + \cdots + 0_r p^{r-1} = 0$$

which implies that $0 \le n$. On the other hand, the largest number that n can take is given by:

$$n = (p-1) + (p-1)p + \cdots + (p-1)p^{r-1}$$

$$= (p-1)(1 + p + p^2 + \cdots + p^{r-1}).$$

Since this is a geometric series, we have that

$$n = (p-1)\left(\frac{p^r - 1}{p-1}\right) = p^r - 1,$$

and this implies that the largest number n can take is $p^r - 1$. Therefore $0 \le n < p^r$. To see that every n is different for the different choices of n_i, suppose that there exist two different representations for the same n. Then,

$$n = n_1 + n_2 p + \cdots + n_r p^{r-1}$$

$$= m_1 + m_2 p + \cdots + m_r p^{r-1},$$

where $0 \le n_i < p$ and $0 \le m_i < p$. Subtracting, we have that

$$0 = n_1 - m_1 + (n_2 - m_2)\, p + \cdots + (n_r - m_r)p^{r-1}.$$

Since both representations are different then there exist an integer j, $1 \le j < r$ such that $n_j \ne m_j$, let j be the smallest such that $n_j \ne m_j$. Then,

$$0 = (n_j - m_j)p^{j-1} + \cdots + (n_r - m_r)p^{r-1}.$$

$$= [(n_j - m_j) + \cdots + (n_r - m_r)p^{r-j}]p^{j-1}.$$

This implies that

$$0 = (n_j - m_j) + (n_{j+1} - m_{j+1})p + \cdots + (n_r - m_r)p^{r-j}.$$

Solving for $n_j - m_j$ we have that

$$(m_j - n_j) = (n_{j+1} - m_{j+1})p + \cdots + (n_r - m_r)p^{r-j}$$

$$= p[(n_{j+1} - m_{j+1}) + \cdots + (n_r - m_r)p^{r-j-1}],$$

which implies that $p|(m_j - n_j)$. But $0 \le n_j, m_j < p$ implies that $\mid m_j - n_j \mid < p$ and therefore $m_j = n_j$. But this is a contradiction and hence n has an unique representation.

□

Theorem 1. *Let $q = p^r$, p a prime, and consider $\mathbb{F}_q$ with the order defined above. If $gcd(i, q-1) = 1$ then the function $\pi : \mathbb{Z}_q \to \mathbb{Z}_q$ defined by $\pi(n) = m$, where $\xi_m = (\xi_n)^i$, is a permutation of $\mathbb{Z}_q$.*

Proof: Since $\mathbb{Z}_q$ is finite, we only have to show that π is one to one. This is, we have to see that if $\pi(x) = \pi(y)$ then $x = y$. This is the same as checking that $\xi_{\pi(x)} = \xi_{\pi(y)}$ implies that $x = y$.

Suppose that $\xi_{\pi(x)} = \xi_{\pi(y)}$, and let α be a primitive root of $\mathbb{F}_q$. Then $\xi_x = \alpha^j$ and $\xi_y = \alpha^k$ for some $1 \leq j, k \leq q-1$. Then $(\xi_x)^i = \xi_{\pi(x)} = \xi_{\pi(y)} = (\xi_y)^i$ implies that $(\alpha^j)^i = (\alpha^k)^i$. By theorem 7.8 of [3] we have that $j \cdot i \equiv k \cdot i$ (mod q-1). Since $gcd(i, q-1) = 1$, $j \equiv k$ (mod q-1) and this implies $\alpha^j = \alpha^k$ in $\mathbb{F}_q$. This implies that $\xi_x = \xi_y$ and hence $x = y$. Therefore π is one to one if $gcd(i, q-1) = 1$. □

Example: Construction of the permutation of $\mathbb{F}_{2^3} = \mathbb{Z}_2/\langle x^3 + x^2 + 1\rangle$ using x^2. First, let α be a primitive root of $x^3 + x^2 + 1$. Then $\alpha^3 = \alpha^2 + 1$.

The following table has the representations of the elements of $\mathbb{F}_{2^3}$ as powers of the primitive root and as elements of a vector space.

n	1	2	3	4	5	6	7
ξ_n	1	α	$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$
α^j	α^0	α^1	α^5	α^2	α^3	α^6	α^4

From our table we obtain the following relation:

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

Evaluating each element in x^2 we get

$$\begin{aligned}&(\alpha^0, \alpha^2, \alpha^3, \alpha^4, \alpha^6, \alpha^5, \alpha^1, 0)\\ &= (\xi_1, \xi_4, \xi_5, \xi_7, \xi_6, \xi_3, \xi_2, 0)\end{aligned}$$

Taking the subscript n from the ξ_n we obtain the permutation π

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

This permutation decomposes in cycles of length 3 and has two fixed points:$0, 1$. The cyclic decomposition is $(2\ 4\ 7)\ (3\ 5\ 6)$. To obtain the dispersion we first find the elements in $D(\pi)$:

$(1,3), (1,1), (1,2), (1,-1), (1,-3), (1,-2),$
$(2,4), (2,3), (2,1), (2,-4), (2,-3),$
$(3,6), (3,2), (3,-2), (3,-5), (3,-6),$
$(4,5), (4,-1), (4,-3), (4,-7),$
$(5,2), (5,-2), (5,-5),$
$(6,1), (6,-4),$
$(7,-1).$

Since we have $D(\pi)$, we can compute the normalized dispersion which is:

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

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

We have a program in Maple that construct the permutations and compute the spreading, dispersion and cyclic decomposition of the permutations. With this program we have obtained the following and many other results.

q	i	cycles length	Number of fixed point	Dispersion
169	167	2	2	.6317976895
625	623	2	2	.8062769231
1024	1022	2	1	.8134660618
2048	2046	2	1	.8132036784

From our results we have been able to see some patterns and based on them patterns we have formulated the following conjectures.

Conjecture 1: Let p be a prime, $p > 3$. If $i = p^s$,$1 \leq s < r$ then the dispersion d of the permutation $\mathbb{F}_{p^r}$ given by x^i is such that $d \leq 0.3400$.

We believe that this happens because

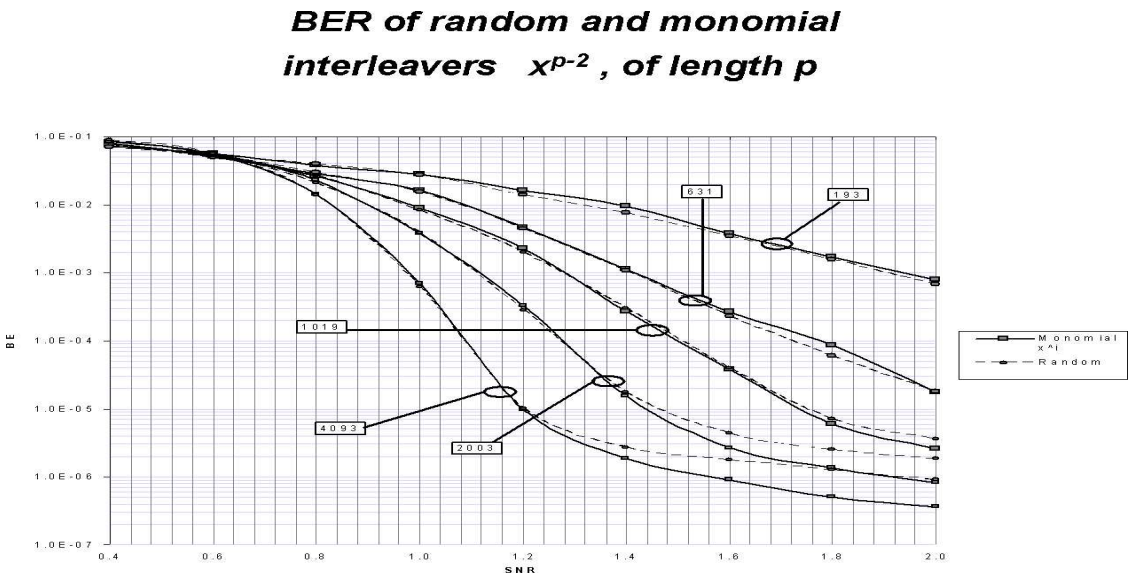
$$(\xi_l)^{p^s} = \left(\sum_{k=0}^{r-1} a_i \alpha^i\right)^{p^s} = \sum_{k=0}^{r-1} a_i \alpha^{ip^s},$$

where α is a primitive root for $\mathbb{F}_{p^r}$. Because of this property many of the differences of $(\xi_l)^{p^s}$ that are at a given distance will give the same value. For example at a distance t, if $a_0 \neq p - t$ then we have that $\xi_{l+t} = a_0 + t + \sum_{k=1}^{r-1} a_k \alpha^k$. This says that $(\xi_{l+t})^{p^s} = \left(a_0 + t + \sum_{k=1}^{r-1} a_k \alpha^k\right)^{P^S} = a_0 + t + \sum_{k=1}^{r-1} a_k \alpha^{kp^s}$ and $(\xi_{l+t})^{p^s} - (\xi_l)^{p^s} = t$.

Conjecture 2: Let x^i be a permutation of $\mathbb{F}_{p^r}$. Then if there exist two or more permutations that decompose in cycles of the same length and have the same number of fixed point then these permutations will have the same fixed points.

6. APPLICATIONS TO TURBO CODES

We have found permutations that decompose in cycles of length 2, have good dispersion and perform well in simulations. Cycles of length 2 are important because



Simulations by C. Corrada, Department of Computer Science, University of Puerto Rico at Rio Piedras

they are easy to implement because the permutation is its own inverse. Above is a graph of the results of simulations done by Carlos Corrada. The graph compares the performance of random and algebraic interleavers. The monomial used for the algebraic interleaver was x^{p-2} and the permutation decomposes in cycles of length 2 for different block lengths p.

7. OTHER RESULTS

In addition to our results on the construction of the permutations and the conjectures on the dispersion, cycle length and fixed points of the permutations, we also have the following result:

Proposition 2. *Let x^i be a permutation monomial of $\mathbb{F}_{p^r}$ and $m-1$ the number of fixed points. Then $m|(q-i)$.*

Proof: Let m be the number of fixed points of the permutation. By Theorem 4 of [4], $m = (i-1, q-1)$. Hence $m|(q-1)$. This implies that $i-1 = m \cdot k$ and $q-1 = m \cdot l$ where $k, l \in \mathbb{Z}$. Subtracting two equations we have that

$$q - 1 - (i-1) = m \cdot l - m \cdot k),$$

$$q - i = m(l-k).$$

Therefore $m|(q-i)$. □

8. FUTURE WORK

We still have to study our results further in order to prove our conjectures or find counterexamples and eventually characterize the permutation monomials that give algebraic interleavers with good properties.

9. ACKNOWLEDGMENTS

We want to thank professors Ivelisse Rubio, UPR- Humacao, Carlos Corrada UPR-Rio Piedras, and José Sotero UPR- Humacao, for their help on our research project. Part of this research has been funded by the UPR- Humacao CSEMS program, Grant 0123169 and AMP.

10. REFERENCES

[1] Luis O. Perez and Yara B. Luis, *Properties of a Type of Permutations over Finite Fields*, Progress Report, UPR-Humacao, 2003.

[2] I. Rubio and C. Corrada, Deterministic Interleavers for Turbo Codes with Random-like Performance and Simple Implementation, *Proceedings of the 3rd International Symposium on Turbo Codes*, September 2003.

[3] T. Hungerford, *Abstract Algebra*, 2nd ed., Saunders, 1997.

[4] Luis Medina, *Factorización parcial de Grupos*, Technical Report, UPR-Humacao, 2003.