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

Properties of Some Classes of Interleavers for Error Correcting Codes

Joyce M. Fernandez
Mathematics Department
University of Puerto Rico at Humacao
Humacao, Puerto Rico

Faculty Advisor: Dr. Ivelisse Rubio

Abstract

Interleavers are an essential component of codes such as Turbo Codes and Multi-user Codes. The interleaver permutes the information symbols. We study some properties of certain permutations given by monomials that could be related to the performance of the codes constructed with them. These properties are the dispersion and the spreading of the permutation and the distance between the different permutations on a family. We study permutations of Z_p obtained with certain monomials cx^i where the coefficient $1 \le c \le p-1$.

Keywords: Interleaver, Error Control Codes, Permutation, Turbo Code, Multi-user Code.

1. Introduction

Error control codes are used in digital communication systems to correct errors that might occur during transmission of messages. When a message passes thru an encoder, the encoder adds redundancy to the message and we obtain the codeword. Then the codeword passes thru a channel that could have noise; this adds errors to the codeword. But, at the receiver, the decoder detects and corrects the errors. An example is the information stored on a compact disc. Here the channel is the disc. The noise can be dirt. The information on the CD is encoded, so that when the CD is played, the player decodes to detect and correct the errors. Another example is the cellular phone, the digital signal is transmitted over the air and it is received by an antenna. But while this signal is traveling, interruptions could occur, for example, if we are near to a mountainous area. These are some examples of why error control codes are necessary in digital communication systems.

Turbo codes are appropriated for wireless systems because they have an effective performance on correcting errors and provide a reduction to the transmitter power levels. The interleaver is an important component of turbo codes and its function is to permute the information symbols. One of its advantages might be that consecutive information symbols will not be affected if there are consecutive errors during the message transmission. Interlerleavers can also be useful to distinguish multi-users signals. If a message is send to many antennas and signals are crossed the interleaver could also prevent that they cancel each other.

The purpose of our research is to study some properties of certain permutations that could tell us if these permutations are adequate to construct good interleavers for the above applications. The properties that we will study are the dispersion and spreading of the permutations and the distance between them. We are studying these properties in permutations of Z_p obtained with monomials cx^i, $1 \le c \le p-1$ for certain exponents i. Our goal is to generalize and extend results obtained in [1] for monomials x^i.

2. Interleavers

The interleaver is an important component of some codes. The interleaver is a bijective function $\pi : Z_n \to Z_n$ that permutes the information symbols.

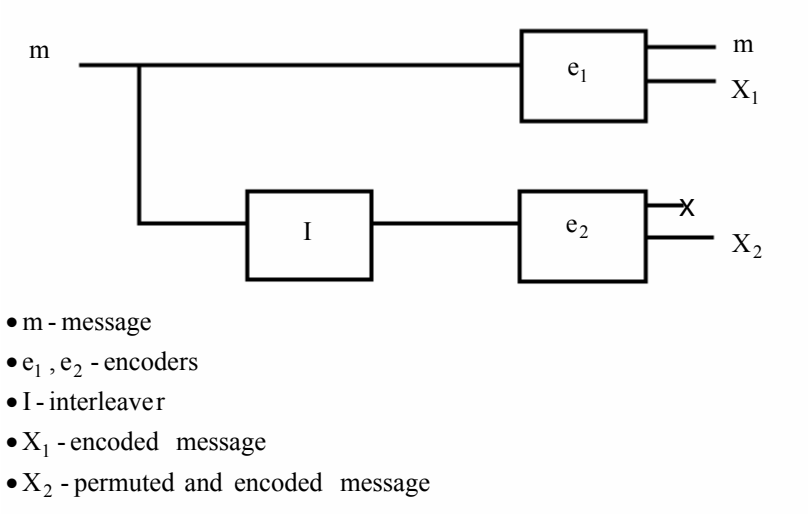

Figure 1. Turbo Code.

Figure 1 shows the encoding process of a turbo code. The codeword is the concatenation of the original message, the message encoded with encoder e_1, and the message permuted by the interleaver and then encoded with encoder $e_2 : (m, x_1, x_2)$.

Choosing interleavers randomly is one way to construct them. Turbo codes with interleavers constructed in this way have good performance, but they have to be analyzed by simulations and be stored in memory. Another method to construct interleavers is algebraically. Interleavers constructed in this way have the advantage that they could be analyzed in advance and can be generated in the moment. In this way memory space is saved and good constructions could be characterized. Unfortunately most of the interleavers that have been constructed algebraically do not have good properties.

We want interleavers that result in codes with good performance. We are using an algebraic method to construct them. Specifically, we are using permutation monomials cx^i. We are basing our work on permutation monomials x^i that have worked well. In particular, we have interest in permutations that decompose in cycles of length two because these permutations are their own inverse. Therefore, these permutations have an implementation advantage because the same technology that is constructed to encode the information, could be used to decode it.

2.1. Interleaver properties

Let π be a permutation of Z_n. The dispersion and the spreading are properties of a permutation that have been associated to the performance of turbo codes. The distance between permutations has been associated to the performance of codes for multiple users, where several interleavers are used at the same time. We want to study these properties for permutations given by monomials cx^i.

There are several results for permutations of finite fields F_q, $q = p^r$ and p a prime, obtained with monomials x^i. We need permutations of Z_n. One can obtain permutations of Z_{p^r}, by ordering the elements of the finite field F_{p^r} and then associating them to Z_{p^r}.

In [2] Y. Luis and L. Pérez studied permutations of Z_{p^r} constructed from permutations of F_{p^r} that were given by monomials x^i. Here we study permutations of Z_p given by monomials cx^i.

2.1.1. dispersion

The dispersion is a factor that measures the interleaver randomness. The dispersion is given by the number of elements in the set $D(\pi) = \{(j-i, \pi(j)-\pi(i)) \mid 0 \le i < j < n\}$. After obtaining the dispersion, we calculate the normalized dispersion $\gamma = \frac{2 \mid D(\pi)}{n(n-1)}$. The closer the normalized dispersion is to 1, the best it is.

Example 1. We present an example of the calculation of the dispersion that will help us to understand some of the results below.

To calculate the dispersion, we first fix the distance *j-i* between the images of the permutation. This gives the first entry of the tuples $(j-i, \pi(j)-\pi(i))$. Then, for each *j-i* we calculate the difference between the images that are *j-i* units apart and count the number of different differences. The dispersion is the total of different tuples.

Consider, Z_{11}, $\pi(x) = 2x^7$. The permutation obtained can be represented by

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

The following "dispersion triangle" has all the tuples $(j-i,\ \pi(j)-\pi(i))$. The column at its right is the number of different differences for each distance *j-i*.

j-i = 1	(1,1) (1,4) (1,3) (1,-4) (1,-1) (1,-4) (1,3)(1,4) (1,1)	5
j-i = 2	(2,5) (2,7) (2,-1) (2,-5) (2,-5) (2,-1) (2,7) (2,5)	4
j-i = 3	(3,8) (3,3) (3,-2) (3,-9) (3,-2) (3,3) (3,8)	4
j-i = 4	(4,4) (4,2) (4,-6) (4,-6) (4,2) (4,4)	3
j-i = 5	(5,3) (5,-2) (5-3) (5,-2) (5,3)	3
j-i = 6	(6,-1) (6,1) (6,1) (6,-1)	2
j-i = 7	(7,2) (7,5) (7,2)	2
j-i = 8	(8,6) (8,6)	1
j-i = 9	(9,7)	1

Using the formula $\gamma = \frac{2 \mid D(\pi) \mid}{n(n-1)}, n = 10$, we obtain that the normalized spreading of π is $\frac{2(25)}{10(9)} = \frac{50}{90} \approx 0.555555556$.

2.1.2. spreading

The spreading measures how separate are the elements that originally were near. An interleaver has spreading factor *s*, if *s* is the largest integer such that $\mid i-j \mid \le s \Rightarrow \mid \pi(i)-\pi(j) \mid \ge s$. The closer the spreading is to $\sqrt{\frac{n}{2}}$, the best it is.

2.1.3 distance between interleavers

This parameter relates two different permutations. It measures how far apart are images of one permutation π_2 that, as images of the other permutation π_1, were near. Formally, let π_1 and π_2 be permutations of Z_p. The distance between π_1 and π_2 is the largest *s* such that $|x-y| \le s \Rightarrow \left|\pi_2^{-1}(\pi_1(x)) - \pi_2^{-1}(\pi_1(y))\right| \ge s$.
The distance between permutations is associated to the performance of codes for multi-user.

Example 2. Consider Z_{11}, $\pi_1(x) = x^7, \pi_2(x) = 2x^7$

$$\pi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ \underline{1} & 7 & \underline{9} & 5 & 3 & 8 & 6 & 2 & 4 & 10 \end{pmatrix} \quad \pi_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 2 & 3 & \underline{7} & 10 & 6 & 5 & \underline{1} & 4 & 8 & \underline{9} \end{pmatrix}$$

In the above example, note that all the images of π_1 that are at most 2 units apart are images in π_2 that are at least 2 units apart. Also note that 5 and 1 are images under π_1 that are 3 units apart but, as images of π_2, they are 1 unit apart. This implies that the distance between π_1 and π_2 is 2.

3. Interleavers Constructed Using Monomials cx^i

C. Corrada and I. Rubio [1] studied permutations of Z_p^r given by monomials x^i. They obtained bounds for the dispersion and good simulation results for turbo codes with interleavers for Z_p constructed with x^{p-2}. Since the results with this monomial were good, we decided to study generalizations of this monomial first. We studied the dispersion, spreading of permutations obtained with cx^{p-2}, $1 \le c \le p-1$, and the distances between them.

In [1] an upper bound and a lower bound for the dispersion of permutations of Z_p given by x^{p-2} were obtained. Here we will prove that the dispersion of cx^{p-2} is the same for all $1 \le c \le p-1$. If one looks carefully to Example 1, one notes that, for each *j-i,* there are pairs of tuples that are the same and they occur in the same positions. This is not a coincidence. To prove this we use polynomials with roots related to the number of elements in the "dispersion triangle" that are the same and note that the number of roots of the polynomial is not affected when we multiply by a constant. From now on, π is a permutation of Z_p.

In the following proposition we construct a polynomial *g(x)* so that for each distance *s=j-i*, the number of roots of the polynomial is equal to the number of tuples that are equal to $(s = j-i, \pi(j) - \pi(i))$, where $\pi(x) = cx^{p-2}$. The proposition says that, for each *s* and each *i*, there are at most 2 tuples that are the same.

Proposition 1. *Let p be a prime,* $s \in \{1,2,..., p-2\}$. *Consider the polynomial* $g(x) = c(i+s)^{p-2} - ci^{p-2} - c(i+x+s)^{p-2} + c(i+x)^{p-2} \in Z_p[x]$, *where* $c \ne 0$, $i \ge 1$ *and* $i + s \le p-1$. *Then, the only roots of g(x) in* Z_p *such that* $i+\alpha+s$, $i+\alpha \in Z_p^*$ *are* $\alpha = 0$ *and* $\alpha = -2i - s$.

Proof: Let $g(x) = c(i+s)^{p-2} - ci^{p-2} - c(i+x+s)^{p-2} + c(i+x)^{p-2}$. Then,
$g(x) = c[(i+s)^{p-2} - i^{p-2} - (i+x+s)^{p-2} + (i+x)^{p-2}] = cd(x)$, where
$d(x) = (i+s)^{p-2} - i^{p-2} - (i+x+s)^{p-2} + (i+x)^{p-2}$. Hence, *g(x)* and *d(x)* have exactly the same roots. It was proven in [1] that the roots of *d(x)* are $\alpha = 0$ and $\alpha = -2i - s$.

□

The following corollary says that, for each *s=j-i*, the only *i* for which there could only be one tuple equal to $(s = j - i, \pi(j) - \pi(i))$ is $i = \frac{p-s}{2}$.

Corollary 1. *Let p be a prime,* $s \in \{1,2,..., p-2\}$.
Consider the polynomial $g(x) = c(i+s)^{p-2} - ci^{p-2} - c(i+x+s)^{p-2} + c(i+x)^{p-2} \in Z_p[x]$ *where* $1 \le i,\ i+s \le p-1$.
Then, the only root of g(x) in Z_p *such that* $i + \alpha + s$, $i + \alpha \in Z_p^*$ *is* $\alpha = 0$, *if and only if* $i = \frac{p-s}{2}$.

Proof: Like in the previous proposition, *g(x)=cd(x),* and therefore *g(x)* and *d(x)* have the same roots. It was proven in [1] that *d(x)* has only one root if and only if $-2i - s = 0$. This happens if and only if $i = \frac{p-s}{2}$.

□

Theorem 1. *Let* $\pi(x) = cx^{p-2}$ *be a permutation of* Z_p . *The dispersion of* cx^{p-2} *is the same for all* $1 \le c \le p-1$.

Proof: The polynomial *g(x)* used in the previous proposition counted the number of tuples $(s = j - i,\ \pi(j) - \pi(i))$ **,** $\pi(x) = cx^{p-2}$ that are the same for each *s* and each *i.* We noted that this dot not change for different values of $c \neq 0$. This implies that the number of elements in the sets $\{(j - i,\ \pi(j) - \pi(i)) \mid \pi(x) = cx^{p-2}, 1 \le i < j \le p-1\}$ is the same for all $c \neq 0$.

□

We found that Theorem 1 is not true for a general exponent. For example, consider $\pi_1(x) = x^7$ and $\pi_2(x) = 5x^7$ as permutations of Z_{17} . For these polynomials, the normalized dispersion is $\gamma_{\pi_1} = \frac{1}{2}$ and $\gamma_{\pi_2} = \frac{8}{15}$.

We are computing the distances between permutations cx^i for different values of *c* to see if we can characterize the coefficients that give permutations with large distances between them. The result in the following theorem will simplify our study because it says that some of the distances are the same.

Lemma 1. *The monomial* cx^{p-2} , $c \in Z_p^*$, *is its own inverse.*

Proof: On Theorem 1 in [3], L. Cruz proved that the permutation of Z_p given by cx^{p-2} decomposes in cycles of length 2 for all $1 \le c \le p-1$. This is equivalent to say that the monomial cx^{p-2} is its own inverse.

□

Theorem 2. *Let* $\pi(x) = cx^{p-2}$ *be a permutation of* Z_p . *The distance between* x^{p-2} *and* cx^{p-2} *is the same as the distance between* x^{p-2} *and (p-c)*x^{p-2} *for all* $1 \le c \le p-1$.

Proof: Let $d(x^{p-2}, cx^{p-2})$ denote the distance between x^{p-2} and cx^{p-2}. We want to show that $d(x^{p-2}, cx^{p-2}) = d(x^{p-2}, (p-c)x^{p-2})$. Suppose that $s = d(x^{p-2}, cx^{p-2})$ and let $\pi_1(x) = x^{p-2}$ and $\pi_2(x) = cx^{p-2}$. Then $|x - y| \le s \Rightarrow |\pi_2^{-1}(\pi_1(x)) - \pi_2^{-1}(\pi_1(y))| \ge s$ and s is the largest such that this happens. Since cx^{p-2} is its own inverse, $\pi_2^{-1}(x) = \pi_2(x)$ and we have that $|\pi_2(\pi_1(x)) - \pi_2(\pi_1(y))| \ge s$. This is,

$|c(x^{p-2})^{p-2} - c(y^{p-2})^{p-2}| \geq s$. Again, since x^{p-2} is its own inverse, $\left(x^{p-2}\right)^{p-2} = x$ and, $|cx - cy| \geq s$. We want to see that, $d(x^{p-2}, (p-c)x^{p-2}) = s$. Let $\pi_3(p-c)x^{p-2}$. Since $|x - y| \leq s \Rightarrow |cx - cy| \geq s$, we have that, $|-(cx - cy)| \geq s$ and $|-cx - -cy| \geq s$. Then, since -c= p-c in Z_p, $|(p-c)x - (p-c)y| \geq s$. This implies that $|(p-c)(x^{p-2})^{p-2} - (p-c)(y^{p-2})^{p-2}| \geq s$ and therefore $|\pi_3(\pi_1(x)) - \pi_3(\pi_1(y))| \geq s$. Since $(p\text{-}c)x^{p-2}$ is its own inverse we have that $|{\pi_3}^{-1}(\pi_1(x)) - {\pi_3}^{-1}(\pi_1(y))| \geq s$. Hence, $d(x^{p-2}, (p-c)x^{p-2} = s$. By the symmetry of the argument, s is the largest one such that this happens.

□

4. Conclusions and Work in Progress

The results presented here are partial results. We are still working on the following

1. We obtained examples where the spreading of permutations given by cx^i, where $c \neq 1$ is better than the spreading of the one given by x^i. We have to study this more carefully to try to characterize the coefficient that give better spreading.
2. We need to try to characterize the coefficients c for which the distances between the permutations are better.
3. We need to run simulations of the codes constructed with our interleavers and compare the results with the codes constructed with x^i that performed well.
4. We still need to study permutations of Z_{p^r} and those given by cx^i.

5. Acknowledgements

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

6. References

Journals

1. C. Corrada, I. Rubio, "Algebraic Construction of Interleavers Using Permutation Monomials", *Proceedings of the IEEE International Conference on Communications*, (June 2004).

2. Y. Luis, L. Pérez, "Properties of a Class of Permutations Over Finite Fields and Applications on Turbo Codes", *Proceedings of the National Conference On Undergraduate Research (NCUR)*, (2005).

3. L. Cruz, "Permutations that Decompose in Cycles of Length 2 and are Given by Monomials.", To appear in *Proceedings of the National Conference On Undergraduate Research (NCUR*), (2006).

4. L. Ping, "Interleave-Division Multiple Access and Chip-by Chip Iterative Multi-User Detection", *IEEE Radio Communication*s, (June 2005):S19.

5. M. Hernandez, "Properties of Interleavers for Turbo Codes Constructed Using Permutation Monomials", *Proceedings of the National Conference On Undergraduate Research (NCUR)*, (March 2003).