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

Analysis of Some Properties of Interleavers for Turbo Codes

Carlos Avenancio-León
Department of Mathematics
University of Puerto Rico at Humacao

Faculty Advisor: Dr. Ivelisse Rubio

Abstract

On this research we study the behavior of the permutations produced by monomials x^i over the finite field $\boldsymbol{F}_q$. In particular, we study the dispersion, spreading, fixed elements and cyclic decomposition of these permutations. Here we present some results related to this.

1. Introduction

Error correcting codes are used on digital communication systems to repair errors that might occur during information transmission. Turbo codes, presented in [1], are a class of codes that are very important because they achieve low error rate without consuming much energy.

The messages on transmission, using turbo codes, are encoded in parallel at least two times. On one of these encodings, the message is codified in its original form, on the others, it is changed by the *interleaver* before being codified. The interleaver, one of the principal components of turbo encoders, changes the position of the information symbols on each codification. This is, the information symbols are *permuted* by the interleaver. One of the effects of permuting the information symbols could be that consecutive entries of the message are not damaged by error bursts. This will depend on some properties of the interleaver, such as the spreading and dispersion, which we will define later.

Random and S-random interleavers may have good functioning but they have some disadvantages that algebraically constructed interleavers might not have. The first disadvantage of random and S-random interleavers is that they have to be stored in memory, while permutations given by algebraic interleavers can be generated at the time of codification. Another disadvantage of random and S-random interleavers is that, since we do not know their algebraic structure, their properties cannot be analyzed without running simulations. Algebraic constructions could have the advantage that their properties can be predetermined. However, at the present time random and S-random are used since still there is not an algebraic construction with better performance.

On this research we have been studying some properties of permutations given by monomials x^i over the finite field $\boldsymbol{F}_q$ to find monomials that produce good interleavers. It is known that the dispersion and spreading factors are important properties. As objectives we have: to study of the dispersion and spreading factors of permutations given by monomials x^i and to study monomials that give permutations of cycle length 2. These are important because they are their own inverse and the same implement can be used for encoding and decoding. So far we have found patterns on the exponents i of permutation monomials with good dispersion or spreading factors. Also, we have found conditions to be able to construct a second permutation monomial with dispersion, spreading, fixed points and cyclic decomposition equal to a given one.

2. Permutation Monomials

A *permutation* ð of a set A is a bijective function ð: A™ A. Monomials that produce permutations of a set are called *permutation monomials*. A permutation of the elements of the finite field $\boldsymbol{F}_q$ is given by ð$(x) = x^i$ if and only if gcd$(i, q-1) = 1$. Permutation monomials give an algebraic method to construct permutations. Using algebraic methods has the advantage that is not needed to store the permutation, as with the random and S-random interleavers. Also, it could be possible to study the properties of the interleaver without having to run simulations.

Important factors for the good functioning of an interleaver are the dispersion and spreading factors. The dispersion measures the randomness of the permutation. The spreading measures the distance between symbols that were close before being permuted by the interleaver. There is conjecture of Corrada-Bravo, University of Puerto Rico at Rio Piedras, that another factor that affects the performance of the code might be the cyclic decomposition of the permutation. The cyclic decomposition of permutations given by monomials have been studied in [1].

For an example of the cyclic decomposition consider $\boldsymbol{Z}_{11}$ and ð$(x) = x^7$. This gives the permutation:

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

In this representation, the first row are the elements of the set and the second is the image of these elements under ð. We can write ð as: ð= *(2 7 6 8) (3 9 4 5)*, which is called the cyclic decomposition of ð. If ð$(x) = x$, then x is said to be a fixed point and we do not write it in the cycle.

We have found that for a permutation ð, ð^{-1} has similar characteristics:

Theorem 2.1: *Let* ð *be a permutation of* $\boldsymbol{F}_q$*. Then, the permutation of* $\boldsymbol{F}_q$ *given by* ð^{-1} *has dispersion, spreading, fixed points and cycle length equal to the permutation given by* ð.

Proof: The proof is a direct use of the definition of dispersion, spreading, fixed points and the construction of cycles.

Corollary 2.2: *If* $i|(q-2)$ *then the permutation given by the monomial* $x^{\frac{(i-1)(q-2-i)}{i}+i}$ *has dispersion, spreading, fixed points and cyclic decomposition equal to the permutation given by* x^i.

Proof: Consider that $x^i \quad x^{\frac{(i-1)(q-2-i)}{i}+i} = x^{\left(\frac{(i-1)(q-2-i)}{i}+i\right)i} = x^1$. This means that $x^{\frac{(i-1)(q-2-i)}{i}+i} = x^{i^{-1}}$. And the result follows from Theorem 2.1.

3. The Dispersion Factor

To construct interleavers that could give good performance it is important to study some properties, like the dispersion factor. The dispersion factor is a measure of how regular a permutation is. To have good dispersion property is to prevent patterns on the permutation. The dispersion of a permutation ð is given by the number of elements on the set $D(\text{ð}) := \{(j- i, \text{ð}(j)-\text{ð}(i)) \mid 0 \quad i < j < T\}$, where ð is a permutation of a set with T elements. The normalized dispersion is given by $\frac{2|D(p)|}{T(T-1)}$. The closer the normalized dispersion is to 1, the better it is.

The following proposition gives us an upper bound to the normalized dispersion of permutations of $\boldsymbol{Z}_p$ given by monomials with odd exponents.

Proposition 3.1: *Let p be an odd prime and* ð$(x) = x^i$ *a permutation of* $\boldsymbol{Z}_p$*. Then the normalized dispersion* ã *is such that* ã $\frac{p+3}{2p}$.

To compute the dispersion of ð, we need to count the distinct differences of the images of elements that are at the same distance. The following lemma counts the differences of images of elements that are k units apart.

Lemma 3.2: *Let p be an odd prime,* $\delta(x)=x^i$ *and define* $\Delta(n) \rightarrow \delta(n+k)-\delta(n)$, *where* $k \in \{1,\ldots, p-1\}$ *is fixed. If* $D_k=\{\Delta(n) \mid 0 \le n < n+k \le p-1\}$, *then*

$$|D_k| \le \begin{cases} \frac{p-k+2}{2}, & k \text{ odd} \\ \frac{p-k+1}{2}, & k \text{ even}. \end{cases}$$

Proof: Since p is odd and ð is a permutation monomial, $\gcd(i, p-1)=1$ implies that i must be odd. Thus, $\Delta(n)= (n+k)^i- n^i = (-n)^i-(-n-k)^i = (p-n)^i-(p-n-k)^i = \Delta(p-n-k)$. Let $\Delta(n)=a$. Then, there is at least another solution n' such that $\Delta(n')=a$. However, there are two extreme cases we need to take in consideration. First, if $n=p-n-k=n'$ (observe that, since $k=p-2n$, k needs to be odd), this is, if $n=\frac{p-k}{2}$, $\Delta(n)=a$ might have only one solution. Second, if $n=0$, $n+k<p$ but $p-n \neq p$, and therefore $\Delta(0)=a$ could have just one solution. Therefore,

$$|D_k| \le \begin{cases} \frac{p-k+2}{2}, & k \text{ odd} \\ \frac{p-k+1}{2}, & k \text{ even}. \end{cases}$$

Now we proceed to prove Proposition 3.1:

Proof of Proposition 3.1: The permutation ð has normalized dispersion $\tilde{a}= \frac{2|D(p)|}{T(T-1)}$. We have that the number of elements of the set $D(\delta)$, for $\delta(x)=x^i$ is :

$$|D(p)| = \sum_{k=1}^{p-1} |D_k| \le \sum_{k=1,\ k \text{ odd}}^{p-2} \frac{p-k+2}{2} + \sum_{k=2,\ k \text{ even}}^{p-1} \frac{p-k+1}{2} = \frac{p+1}{2} + 1 + 2\left(2+3+\ldots+\frac{p-1}{2}\right)$$

$$= \frac{p+3}{2} - 2 + \left(\frac{p-1}{2}\right)\left(\frac{p-1}{2}+1\right) = \left(\frac{p-1}{2}\right)\left(\frac{p+3}{2}\right).$$

Hence,

$$g = \frac{2|D(p)|}{p(p-1)} \le \frac{2\left(\frac{(p-1)(p+3)}{4}\right)}{p(p-1)} = \frac{p+3}{2p}.$$

We studied closely the permutations given by the monomials x^{p-2} and x^3 for p a prime. Note that the monomial x^{p-2} is always a permutation monomial for p prime. This is because $\gcd(p-2, p-1) =1$. In contrast with the monomial x^{p-2}, x^3 is permutation monomial only if $3|(p-2)$. Otherwise it would divide $p-1$ and $\gcd(3, p-1) \neq 1$.

For the dispersion property we found that these polynomials give permutations with normalized dispersion equal to the upper limit given in Proposition 3.1 given some conditions. Before stating this result formally we are going to prove some other results.

To calculate the normalized dispersion of the permutation given by x^{p-2} and x^3 we need to count the number of elements of $D(\delta)$. Here it will be useful to rewrite $D(\delta)$ as $D(\delta) =\{(k, \Delta(n)) \mid 1 \le k < p, 0 \le n < n+k \le p-1\}$, where $\Delta(n)$ is defined as in Lemma 3.2.

We need to count how many values $\Delta(n)$ we have for each value of k. So, the dispersion is related to the number of solutions to the equation $\Delta(n) = a$. The following two lemmas count and characterize the number of solutions of $\Delta(n) =a$ for $\delta(x)= x^3$.

Lemma 3.3: *Consider* ð*(x)= x^3 and define Ä(n) › $(n+k)^3 - n^3$, where k Î {1 ,..., p-1} is fixed, n Î {0 ,..., p-2} and 1 n+k p-1. Suppose that Ä(n) =a. Then there is at most another n' such that Ä(n') =a and n'= p-n-k.*

Proof: If *Ä(n)= $(n+k)^3 - n^3$*, then *Ä(n)= $3n^2k+ 3nk^2 + k^3$*. Because the degree of *Ä(n)* is *2*, *Ä(n)=a* has at most two distinct solutions.

Now suppose that *a= Ä(i) = Ä(i+j)* for some *j 1*, *j+i < p-1*. Then *Ä(i) = Ä(i+j)* implies that *Ä(i) - Ä(i+j)=0*. This also implies that *$(3i^2k+ 3ik^2 + k^3)-(3(i+j)^2k+ 3(i+j)k^2 + k^3)=0$*. Thus, *j=0* or *j -2i-k (mod p)*. Therefore, if *n=i*, *n'=i+j=p-i-k=p-n-k* is another solution to *Ä(n) =a*.

Lemma 3.4: *Let ð(x)=x^3 and consider the conditions of lemma 3.3. The polynomial Ä(n)= a has unique solution if and only if* $n=\frac{p-k}{2}$ *or n=0.*

Proof: ( ) From the previous result, we have that *Ä(n) =a* has solutions $n_1=i$ and $n_2=p-i-k$. Suppose that there is only one solution. Then, $n_1=n_2$ or n_2 does not exist. If $n_1=n_2$, $i=p-i-k$ $n_1=n_2 = i=\frac{p-k}{2}$. If n_2 do not exists, $n_2+k=p$. Therefore, $n_1=0$.

( ) Now consider $n_1=\frac{p-k}{2}$. Then $n_2= p-\frac{p-k}{2}-k=\frac{p-k}{2}$ and the solution is unique. If $n_1=0$, $n_2+k=p$ and this contradicts $n+k < p$. Hence, this solution is also unique.

Now that we know the number of solutions of *Ä(n) =a* for each *n* we are able to count the number of elements of *D(ð)* for each *k*.

Proposition 3.5: *Let ð(x)=x^3, and define Ä(n) › $(n+k)^3 - n^3$, where k Î {1 ,..., p-1} is fixed. If D_k={Ä(n)| 0 n < n+k p-1}, then*

$$|D_k| = \begin{cases} \frac{p-k+2}{2}, & k \text{ odd} \\ \frac{p-k+1}{2}, & k \text{ even}. \end{cases}$$

Proof: For every *k* we have *p-k* differences *Ä(n)* (may be not distinct). If *k* is odd $n=\frac{p-k}{2}$ exists. Therefore, by Lemma 3.3, since each *Ä(n) =a* has two solutions except for when *n=0* and $n=\frac{p-k}{2}$, we obtain that $|D_k|= \frac{p-k-2}{2}+2=\frac{p-k+2}{2}$. If *k* is even $n=\frac{p-k}{2}$ do not exists. Thus, *Ä(0)* is the only difference that appears once, and $|D_k|= \frac{p-k-1}{2}+1=\frac{p-k+1}{2}$.

The following result was presented by I. Rubio in [2]:

Lemma 3.6: *Let ð(x)=x^{p-2}, and fix k Î {1 ,..., p-2}. Define Ä(n):=$(n+k)^{p-2}-n^{p-2}$. If D_k={ Ä(n) |1 n < n+k p-1} then*

$$|D_k| = \begin{cases} \frac{p-k}{2}, & k \text{ odd} \\ \frac{p-k-1}{2}, & k \text{ even}. \end{cases}$$

Note that in Lemma 3.6 the sets D_k do not include values *Ä(0)*. The following lemma addresses this case.

Lemma 3.7: *Let (x)=x^{p-2}, and fix k Î {1 ,..., p-1}. Suppose that Ä(0)=a. Then n=0 is the only solution to Ä(n)=a for all k if and only if 3|(p-2).*

Proof: If $Ä(0)=Ä(i)$, for i Î $Æ_p^*$, then $(i+k)^{p-2}-i^{p-2}=k^{p-2}$ $(i+k)^{p-2}= k^{p-2} + i^{p-2}$ $(i+k)^{p-1}=(k^{p-2}+i^{p-2})(i+k)=k^{p-1}+ ik^{p-2}+ i^{p-2}k + i^{p-1}$. Since $\smile^{p-1}=1$ for all $\smile$ Î $Æ_p^*$ the equation reduces to $1= ik^{p-2}+ i^{p-2}k + 2$ ”$-1= ik^{p-2} + i^{p-2}k$ ”$-1(ik)= (ik)ik^{p-2}+ (ik)i^{p-2}k= k^2 + i^2$ ”$k^2 +ki+ i^2=0$. Solving for i we obtain $i= \frac{-k \pm \sqrt{k^2 - 4k^2}}{2}$.

These solutions are in Z_p if and only if $\sqrt{-3} \in Z_p$. Making use of the Division Algorithm Theorem and of the fact that p is a prime, we have that p must be of the form $12m+á$, for m Î Z and $á$ Î $\{5, 11\}$, if $3|(p-2)$, or $á$ Î $\{1, 7\}$, if $3\_(p-2)$.

By Theorems A.1 and A.3 we have that

$$(3/p)= \begin{cases} (-1/p)(3/p)=(1)(-1)=-1, \text{ if } a=5; \\ (-1/p)(3/p)=(-1)(1)=-1, \text{ if } a=11; \\ (-1/p)(3/p)=(1)(1)=1, \text{ if } a=1; \\ (-1/p)(3/p)=(-1)(-1)=1, \text{ if } a=7. \end{cases}$$

Since $3|(p-2)$ if and only if p $5, 11 \pmod{12}$, these solutions are unique in Z_p if $3|(p-2)$.

We have that if $á$ Î $\{1, 7\}$, that is, if $3\_(p-2)$, then, if we set $k=1$, $i= \frac{-1\pm\sqrt{-3}}{2}$ is a solution distinct from 0 if and only if $0<i<p-1$. Since i $\in Z_p$ we must prove just that i ¹ 0 and i ¹ $p-1=-1$. First, if $i=0$, $k^2 +ki+ i^2=1=0$, which is a contradiction. Therefore i ¹$0$. If $i=-1$, then $k^2 +ki+ i^2=1=0$, which is also a contradiction. Therefore, when $3\_(p-2)$, $Ä(0)$ is at least once a repeated difference.

Lemmas 3.6 and 3.7 for $ð(x)=x^{p-2}$ were the analogous to Lemmas 3.3 and 3.4 for $ð(x)=x^3$. In the same way the following proposition is the analogous of Proposition 3.5. This proposition and the following theorem improves the result on Theorem 4 of [1]. They give the necessary and sufficient conditions to attain the upper bound in the Proposition 3.1.

Proposition 3.8: *Let* $ð(x)=x^{p-2}$, *and fix* k Î $\{1 ,..., p-1\}$. *Define* $Ä(n):=(n+k)^{p-2}-n^{p-2}$. *For* $D_k=\{ Ä(n) \mid 0$ $n < n+k$ $p-1\}$,

$$|D_k| = \begin{cases} \frac{p-k+2}{2}, & k \text{ odd} \\ \frac{p-k+1}{2}, & k \text{ even}. \end{cases}$$

for each k if and only if $3|(p-2)$.

Proof: From Lemma 3.6 we know that, for 1 $n < n+k$ $p-1$,

$$|D_k| = \begin{cases} \frac{p-k}{2}, & k \text{ odd} \\ \frac{p-k-1}{2}, & k \text{ even}. \end{cases}$$

If $3|(p-2)$, $Ä(0)$ is a unique difference and, for 01 $n < n+k$ $p-1$ and each k,

$$|D_k| = \begin{cases} \frac{p-k+2}{2}, & k \text{ odd} \\ \frac{p-k+1}{2}, & k \text{ even}. \end{cases}$$

If $3\_(p-2)$ then $Ä(0)$ is not unique for some k's and hence this is not true.

Now we have been able to compute the cardinality of the subset D_k of $D(ð)$ for each k. The sum of the cardinalities of all these subsets will give us the number of elements in $D(ð)$ and therefore we will be able

to compute the normalized dispersion of the permutations given by $\delta(x)=x^3$, $\delta(x)=x^{p-2}$ and, making use of Theorem 2.1, $\delta(x)= x^{\frac{2p-1}{3}}$. This is stated in the following theorem:

Theorem 3.9: *Let p be a prime. The permutation of $\mathbf{F}_p$ given by x^i has dispersion equal to the upper bound* $\tilde{a}= \frac{p+3}{2p}$ *if 3|(p-2) and i* $\in \{3, \frac{2p-1}{3}, p-2\}$.

Proof: The permutation δ has normalized dispersion $\tilde{a}=\frac{2|D(p)|}{p(p-1)}$. We have that the number of distinct differences $|D(\delta)|$, for $\delta(x)=x^3$ or $\delta(x)=x^{p-2}$, is

$$|D(p)| = \sum_{k=1}^{p-1} |D_k| = \sum_{k=1,\ k\ odd}^{p-2} \frac{p-k+2}{2} + \sum_{k=2,\ k\ even}^{p-1} \frac{p-k+1}{2} = \frac{p+1}{2} + 1 + 2\left(2+3+\ldots+\frac{p-1}{2}\right)$$

$$= \frac{p+3}{2} - 2 + \left(\frac{p-1}{2}\right)\left(\frac{p-1}{2}+1\right) = \left(\frac{p-1}{2}\right)\left(\frac{p+3}{2}\right).$$

Hence,

$$g = \frac{2|D(p)|}{p(p-1)} = \frac{2\left(\frac{(p-1)(p+3)}{4}\right)}{p(p-1)} = \frac{p+3}{2p}.$$

Therefore, $\delta(x)=x^3$ and $\delta(x)=x^{p-2}$ have normalized dispersion equal to the upper bound $\tilde{a}= \frac{p+3}{2p}$. Since $\frac{2p-1}{3} = 3^{-1}$, by theorem 2.1 $\delta(x)= x^{\frac{2p-1}{3}}$ also has normalized dispersion equal to $\tilde{a}= \frac{p+3}{2p}$.

4. The Spreading Factor

The spreading is another important property of an interleaver. It is a measure of how distant are interleaved symbols that were originally close to each other. It is said that an interleaver have spreading factors s if $|i-j| < s \Rightarrow |\delta(i)-\delta(j)| \geq s$. The closer s is to $\sqrt{\frac{T}{2}}$, where T is the length of the block that is being permuted, the better the spreading is.

The following two theorems relate the form of p with the spreading of the permutation given by $\delta(x) =x^3$ and $\delta(x) =x^{p-2}$ respectively:

Theorem 4.1: *Let p be a prime. If 3|(p-2), then the permutation given by the monomials x^3 and $x^{\frac{2p-1}{3}}$ have spreading greater than 1 if and only if p is of the form 30l + 11 or 30l + 29, for l* $\in \mathbf{Z}$.

Proof: Let $\delta(x)=x^3$ and define $\Delta(x)=\delta(x+1)-\delta(x)$. By the Division Algorithm we find that an integer q is of the form $30l+\alpha$, for $l \in \mathbf{Z}$ and $\alpha \in \{0,1,2,\ldots,29\}$. If $q=p$ then, $\alpha \in \{1,7,9,11,13,17,19,23,29\}$. To fit $3|(p-2)$, we must restrict the values of α even more. Hence, $\alpha \in \{11,17,23,29\}$.

By definition, we have spreading $s=1$ if and only if exists $i \in \mathbf{Z}_p$ such that $\Delta(i)=1$ or $\Delta(i)=-1$, for $k= 1$ and $1 \leq i \leq p-2$. Easily we can see that the polynomial $\Delta(i)= (i+1)^3-i^3= 3i^2+3i+1=1$ has solutions $i=0$ and $i=p-1$. Since $1 \leq i \leq p-2$, $\Delta(i)=1$ has no solutions for the spreading calculation.

For the case $\Delta(i)=-1$ we have four cases:

Case p=30l+11: Using the quadratic formula we know that $i= -1(2)^{-1} \pm (2)^{-1}\sqrt{1-(4)(2)(3)^{-1}} = 15l+5 \pm (2)^{-1}\sqrt{1-(4)(2)(10l+4)} = 15l+5 \pm (2)^{-1}\sqrt{(10l+2)} = 15l+5 \pm (2)^{-1}\sqrt{(3)^{-1}-2} = 15l+5 \pm (2)^{-1}$

$\sqrt{(3)^{-2}(3-2\times 3^2)} = 15l+5 \pm (2)^{-1}(3)^{-1}\sqrt{-1}\sqrt{3}\sqrt{5}$. By Theorem A.1, $(1/p)=(-1)^{\frac{p-1}{2}}$. Hence, $(-1/p)$ is quadratic residue if and only if l is odd. By Theorem A.3, $(3/p)=1$ if $p \equiv \pm 1 \pmod{12}$, and $(3/p)=-1$ if $p \equiv \pm 5 \pmod{12}$. If l is odd $p \equiv 5 \pmod{12}$ $(3/p)=-1$. If l is even, then $p \equiv -1 \pmod{12}$ $(3/p)=1$. So long we have that $(-1(3)/p)=-1$. Since $(5/p)=1$ by Theorem A.4, $(-1(3)(5)/p) = -1$ and therefore i is no solution.

Case p=30l+17: In this case $i = -1(2)^{-1} \pm (2)^{-1}\sqrt{1-(4)(2)(3)^{-1}} = 15l+8 \pm (2)^{-1}\sqrt{1-(4)(2)(10l+6)} = 15l+8 \pm (2)^{-1}\sqrt{(10l+4} = 15l+8 \pm (2)^{-1}\sqrt{(3)^{-1}-2} = 15l+8 \pm (2)^{-1}\sqrt{(3)^{-2}(3-2\times 3^2)} = 15l+8 \pm (2)^{-1}(3)^{-1}\sqrt{-1}\sqrt{3}\sqrt{5}$. When l is odd, following the same procedure as in the first case, $(3/p)=1$ and $(-1/p)=-1$. If l is even $(3/p)=-1$ and $(-1/p)=1$. By Theorem A.4, $(5/p)=-1$. Thus, $(-1(3)(5)/p) = 1$ and i is solution to $Ä(i)=-1$.

Case p=30l+23: Here $i = -1(2)^{-1} \pm (2)^{-1}\sqrt{1-(4)(2)(3)^{-1}} = 15l+11 \pm (2)^{-1}\sqrt{1-(4)(2)(10l+8)} = 15l+11 \pm (2)^{-1}\sqrt{(10l+6} = 15l+11 \pm (2)^{-1}\sqrt{(3)^{-1}-2} = 15l+11 \pm (2)^{-1}\sqrt{(3)^{-2}(3-2\times 3^2)} = 15l+11 \pm (2)^{-1}(3)^{-1}\sqrt{-1}\sqrt{3}\sqrt{5}$. Doing as in case 1 we obtain that $(-1/p)=1$ and $(3/p)=-1$ for odd l's and $(-1/p)=-1$ and $(3/p)=1$ for even l's. Also we have that $(5/p)=-1$. Hence, $(-1(3)(5)/p) = 1$ and i is solution to $Ä(i)=-1$.

Case p=30k+29: This time $i = -1(2)^{-1} \pm (2)^{-1}\sqrt{1-(4)(2)(3)^{-1}} = 15l+14 \pm (2)^{-1}\sqrt{1-(4)(2)(10l+10)} = 15l+14 \pm (2)^{-1}\sqrt{(10l+8} = 15l+14 \pm (2)^{-1}\sqrt{(3)^{-1}-2} = 15l+14 \pm (2)^{-1}\sqrt{(3)^{-2}(3-2\times 3^2)} = 15l+14 \pm (2)^{-1}(3)^{-1}\sqrt{-1}\sqrt{3}\sqrt{5}$. For odd l's, $(-1/p)=-1$ and $(3/p)=1$. For even l's $(-1/p)=1$ and $(3/p)=-1$. Because $(5/p)=1$, $(-1(3)(5)/p) = -1$ and there is no solution to $Ä(i)=-1$..

If there are no solutions to $Ä(i)=1$ or $Ä(i)=-1$, by definition, the spreading is greater than 1. Else, it is 1. Since $\frac{2p-1}{3} = 3^{-1}$, by Theorem 2.1, this result is also true for $ð(x) = x^{\frac{2p-1}{3}}$.

Theorem 4.2: *Let p be a prime. The spreading of the permutation given by $ð(x)=x^{p-2}$ is 2 if p is of the form 30l + 17 or 30l + 23, for $l \in Z$. Otherwise the spreading is 1.*

Proof: Define $Ä(x) = (i+k)^{p-2} - i^{p-2}$ with $k \in \{1,..., p-1\}$. Since p is a prime, it is of the form $30l+á$, with $á \in \{1,7,9,11, 13,17,19,23,29\}$. To have a spreading better than 1 implies to have neither $Ä(i)=1$ nor $Ä(i)=-1$ for every $i \in Z_p$ such that $1 \le i \le p-2$, $k=1$. If $Ä(i)=1$, $(i+k)^{p-2} - i^{p-2}=1$. Multiplying by $i(i+k)$ we obtain $i(i+k)(i+k)^{p-2} - i(i+k)i^{p-2} = -k = 1(i)(i+k)) \Rightarrow i^2 + ik + k = 0 \Rightarrow i = \frac{-k \pm \sqrt{k^2-4k}}{2}$. If $k=1$ this simplifies to $i = \frac{-1 \pm \sqrt{-3}}{2}$ and it is already solved in the proof of Lemma 3.7. From those results we know that if $3 \not| (p-2)$, this is, if $á \in \{1, 7, 13, 19\}$, $Ä(i)=1$ for some i. Therefore if $á \in \{1, 7, 13, 19\}$, $ð(x)=x^{p-2}$ gives permutations with spreading 1.

If $Ä(i)=-1$, then $(i+k)^{p-2} - i^{p-2} = -1$ $i(i+k)(i+k)^{p-2} - i(i+k)i^{p-2} = -k = -1(i)(i+k)) \Rightarrow i^2 + ik - k = 0$ $i = \frac{-k \pm \sqrt{k^2+4k}}{2}$. Since $k=1$, $i = \frac{-1 \pm \sqrt{5}}{2}$. By Theorem A.4, i is solution if and only if $p=30l+11$ or $p=30l+29$. By the fact that $\sqrt{5} \neq 1$ and $\sqrt{5} \neq -1$, we have that $i \neq 0, -1$ and we can conclude that i is a solution such that $1 \le i < i+k \le p-1$. Hence, when $p=30l+11$ or $p=30l+29$, the permutation given by $ð(x)=x^{p-2}$ has spreading 1.

We have seen that $Ä(i) \neq -1$ and $Ä(i) \neq 1$ when $p=30l+17$ or $p=30l+23$. From this follows that the permutation given by $ð(x)=x^{p-2}$ has spreading at least two.

If a permutation has spreading 3, $\Delta(i) \neq 1, -1, 2, -2$ for $k=1$ and $k=2$. If $\Delta(i)=2$ and $k=1$, then $(i+k)^{p-2} - i^{p-2} = 2$ $i(i+k)(i+k)^{p-2} - i(i+k)i^{p-2} = -k = 2(i)(i+k)) \Rightarrow 2i^2 + 2ik + k = 0$ $i = \frac{-2 \pm 2\sqrt{-1}}{2}$. Making use of Theorem A.1,we find that $\sqrt{-1}$ is solvable for $p=30l+17$ if l even. If l is odd it is solvable for $p=30l+23$. Hence, the spreading is not 3 under these circumstances.

If $\Delta(i)=-2$ and $k=1$, following the same procedure, we have that $i = \frac{-2 \pm 2\sqrt{3}}{2}$. Now, making use of Theorem A.3 we find that $\sqrt{3}$ is solvable for $p=30l+17$ if l is odd. If l even, it is solvable for $p=30l+23$.
We can observe that the spreading is not 3, for $p=30l+17$ and $p=30l+23$, in both cases l *odd* and l *even*. Therefore the spreading is never greater than 2 for the permutation given by $\delta(x)=x^{p-2}$.

5. Future Work

There is still much work to do in the area of permutation monomials applied to Turbo Codes. The spreading and dispersion factors as well as all the other properties of permutation monomials need to be studied much more. Simulations need to be ran in order to check the performance of codes constructed with the different interleavers.

6. Acknowledgments

Our mentor Ivelisse Rubio has been a guide for us in this research, giving us the tools and help we needed much times. Our work was supported by the UPRH-NSF CESMS Program, Grant Number 0123169 and the PR-NASA Space Grant.

7. References

1. 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.*.

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

3. C. Heegard, S. Wicker, *Turbo Codes*, Kluwer Academic Publishers, 1999.

4. D. Burton, *Elementary Number Theory*, Allyn and Bacon Inc., 1976.

Appendix A: Used Results from Number Theory

To prove some of our results we used the Legendre symbol and quadratic reciprocity. Here we include the results about quadratic reciprocity that we used.

Definition: *Let p be an odd prime and gcd(a, p)= 1. The Legendre symbol (a/p) is defined by (a/p) =1, if a is quadratic residue of p, and (a/p) =-1, if a is quadratic nonresidue of p.*

Theorem A.1: *Let p be an odd prime and a and b be integers which are relatively prime to p. Then the Legendre symbol has the following properties:*

1. *If $a \equiv b \pmod p$, then (a/b)=(b/p).*
2. *(ab/p)=(a/p)(b/p)*
3. *(1/p)=1 and (-1/p)= $(-1)^{\frac{p-1}{2}}$*

Theorem A.2: *If p is an odd prime, then (2/p)=1 if $p \equiv \pm 1 \pmod 8$ or (2/p)= -1, if $p \equiv \pm 3 \pmod 8$.*

Theorem A.3: *If p ¹ 3 is an odd prime, then (3/p)= 1, if p ±1 (mod 12) or (3/p)= -1 , if p ±5 (mod 12).*

Theorem A.4: *If p ¹ 53 is an odd prime, then (5/p)= 1, if p ±1 (mod 5) or (5/p)= -1 , if p ±2 (mod 5).*