ANALYSIS OF THE DISPERSION AND SPREADING PROPERTIES OF INTERLEAVERS FOR TURBO CODES

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

ABSTRACT

Our objective on this research is to study the behavior of the permutations produced by monomials x^i over a finite field $\mathbb{F}_q$. In particular, we are studying the dispersion, spreading, fixed elements and cyclic decomposition of these permutations. We present some conjectures 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 [3], 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 repeated at least two times. One of these repetitions of the message is codified in its original form, the others are changed by the *interleaver* before being codified. The interleaver, one of the principal components of turbo encoders, change 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, that we will define latter.

Random and S-random interleavers may have good functioning but they have some disadvantages that algebraically constructed interleavers do 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.

On this research we have been studying some properties of permutations given by monomials x^i over a finite field $\mathbb{F}_q$ 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 the monomial's behavior for permutations of cycle length 2. So far we have found patterns on the exponents i of permutation monomials with good dispersion or spreading factors. Also, we have found patterns to localize a second permutation monomial with dispersion, spreading, fixed points and cyclic decomposition equal to the first one. These patterns occur if $i|(q-2)$ and in the special case in which $3|(q-2)$.

2. PERMUTATION MONOMIALS

A permutation of a set A is a bijective function $\pi : A \longrightarrow A$. Monomials that produce permutations of a set are called permutation monomials. A permutation of the elements of a finite field $\mathbb{F}_q$ is given by $\pi(x) = x^i$ 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 is 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 regularity of the permutation.

There is conjecture of Corrada-Bravo, professor at University of Puerto Rico at Rio Piedras, that another factor might be the cyclic decomposition of the permutation. For example, if we consider $\mathbb{Z}_{11}$ and $\pi(x) = x^7$ we have the permutation:

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

We can write π as: $\pi = (2768)(3945)$, which is called the cyclic decomposition of π. If $\pi(x) = x$, then x is said to be a fixed point.

The following is the conjecture due to Corrada-Bravo:

- **Conjecture 1:** *Turbo codes constructed using monomials that produce permutations with certain cyclic decompositions have better performance.*

The cyclic decomposition of permutations given by monomials have been studied in [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 π is given by the number of elements on the set:

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

where π is a permutation of a set with T elements. The normalized dispersion is given by:

$$\frac{2|D(\pi)|}{T(T-1)}.$$

The closer the normalized dispersion is to 1, the better it will become.

The following proposition was presented in [2]:

- **Proposition**: *Consider the permutation monomial $\pi(x) = x^{q-2}$, were q is a prime. Then π has normalized dispersion γ, where $\frac{q-1}{2q} \leq \gamma \leq \frac{q+3}{2q}$.*

Within the studied monomials there was x^{q-2} for q a prime. We found that x^{q-2} always has dispersion better or equal than other monomials. We found that if and only if $3|(q-2)$, then the dispersion of other monomials is equal to the one of x^{q-2}. These monomials are x^3 and $x^{\frac{2q-1}{3}}$.

- **Conjecture 2** *Let q be a prime. The permutation of $\mathbb{F}_q$ given by x^i has dispersion equal to the upper bound $\gamma = \frac{q+3}{2q}$ if and only if $3|(q-2)$ and $i \epsilon \{3, \frac{2q-1}{3}, q-2\}$.*

For examples see the table in section 5, which shows the dispersion and spreading of several permutations.

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, t) if:

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

The spreading s is the maximum value such that $s \leq t$. 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 next conjecture relates the spreading and the form of q.

- **Conjecture 3** *Let q be a prime. If $3|(q-2)$, then the permutation given by the monomials x^3 and $x^{\frac{2q-1}{3}}$ have spreading greater than 1 if and only if q is of the form $30k+11$ or $30k+29$, for $k \epsilon \mathbb{Z}$. The spreading of the permutation given by x^{q-2} is greater than 1 if and only if q is not of the above form.*

For examples see the table in section 5, which shows the dispersion and spreading of several permutations.

5. SOME OTHER CONJECTURES

On our research we have found some patterns on permutations of $\mathbb{F}_q$ where q is prime. Our experiments showed that all the values for the dispersion and spreading, the fixed points and the cyclic decomposition were the same for two monomials. From that we have formulated the next conjectures:

- **Conjecture 4:** *Let q be a prime. 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.*

Note that if $i = q-2$ then not always exists another monomial with properties equal to x^i, because $\frac{(i-1)(q-2-i)}{i} + i = q-2$.

- **Conjecture 5:** *Let q be a prime. Given the permutation monomial x^i, there exists another permutation with dispersion, spreading, fixed points and cyclic decomposition equal to the permutation given by x^i if $i \notin \{q-2, \frac{q-3}{2}, \frac{q+1}{2}\}$.*

The following is a table of dispersion and spreading of some permutations of $\mathbb{F}_q$ given by x^i.

q	i	dispersion	spreading
23	3	.56522	1
	5	.49407	1
	7	.50988	2
	9	.49407	1
	13	.50593	2
	15	.56522	1
	17	.50593	2
	19	.50988	2
	21	.56522	2
37	5	.49099	1
	7	.48198	1
	11	.46096	1
	13	.47748	1
	17	.46697	1
	19	.36937	1
	23	.46096	1
	25	.47748	1
	29	.49099	1
	31	.48198	1
	35	.52703	1
107	3	.51401	1
	5	.46235	2
	7	.47434	1
	9	.47910	1
	11	.47346	2
	13	.45265	2
	15	.46640	1
	17	.46535	2
	19	.48651	2
	21	.42214	1
	23	.43837	3
	25	.46535	2
	27	.47011	2
	29	.47346	1
	31	.44207	2
	33	.49691	1
	35	.46341	1
	37	.44136	1
	39	.47804	1
	41	.46446	1
	43	.44136	1
	45	.49691	1
	47	.46958	2
	49	.45265	2
	51	.48298	2
	55	.47011	2
	57	.45953	1
	59	.47910	1
	61	.49744	1
	63	.47434	2
	65	.44207	1
	67	.48651	2
	69	.47434	2
	71	.51401	1
	73	.49744	1
	75	.46446	1
	77	.46658	2
	79	.48298	2
	81	.47645	1
	83	.43837	3
	85	.46235	2
	87	.47804	1
	89	.47645	1
	91	.47434	1
	93	.45953	1
	95	.46658	2
	97	.46958	2
	99	.46640	1
	101	.42214	1
	103	.46341	1
	105	.51401	2

6. FUTURE WORK

We still have some work left to do. First, we have to prove our conjectures or find counter examples to them. Also, we will look for patterns to characterize monomials that have the same dispersion, spreading, fixed elements and cyclic decomposition for $i \nmid (q-2)$ (similar to conjecture 4). We will try to find other conjectures on the spreading of permutations x^i of $\mathbb{F}_q$ for $i \neq 3, \frac{2q-1}{3}, q-2$ (similar to conjecture 3).

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.

7. ACKNOWLEDGEMENTS

Our mentor Ivelisse Rubio Canabal 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.

8. REFERENCES

[1] I. Rubio and C. Corrada, "Cyclic Decomposition of Permutations of Finite Fields Obtained Using Monomials and Applications to Turbo Codes", to appear in the Proceedings of Finite Fields and Applications Symposium, May 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] C. Borreau, A. Glavieux, and P. thitimajshima, Near Shannon limit error-correcting coding and decoding: Turbo Codes, in *Proceedings of ICC'93*, Geneva, Switzerland, May 1993.

[4] C. Heegard, S. Wicker, *Turbo Codes*, Kluwer Academic Publishers, 1999.