Cyclic Decomposition of Permutations of Finite Fields Obtained Using Monomials

Ivelisse M. Rubio[1,⋆] and Carlos J. Corrada-Bravo[2]

[1] Department of Mathematics
University of Puerto Rico at Humacao
ive@www.uprh.edu
[2] Department of Computer Science
University of Puerto Rico at Río Piedras
ccorrada@goliath.cnnet.clu.edu

Abstract. In this paper we study permutations of finite fields $\mathbf{F}_q$ that decompose as products of cycles of the same length, and are obtained using monomials $x^i \in \mathbf{F}_q[x]$. We give the necessary and sufficient conditions on the exponent i to obtain such permutations. We also present formulas for counting the number of this type of permutations. An application to the construction of encoders for turbo codes is also discussed.

1 Introduction

Consider $\mathbf{F}_q$, the finite field with q elements. It is well known that the function $\pi : \mathbf{F}_q \longrightarrow \mathbf{F}_q$ defined by $\pi(x) = x^i$ produces a permutation of the elements in $\mathbf{F}_q$ if and only if $gcd(i, q-1) = 1$. Polynomials that produce permutations are called *permutation polynomials*. We are interested in permutations of $\mathbf{F}_q$ that decompose in cycles of the same length and are obtained using monomials x^i . When 0, 1 and -1 are the only elements fixed by the permutation, these monomials have been characterized in [6]. Here, we characterize the monomials that produce permutations of $\mathbf{F}_q$ that decompose in cycles of the same length and have any set of fixed elements. We also present formulas for counting the number of such monomials.

Applications of this type of permutations to the construction of encoders for turbo codes are being studied by the authors. Data obtained by Corrada-Bravo [2] suggests that the relation between the length of the cycles in the cyclic decomposition of the permutation and the length of the cycle of the convolutional code in the turbo code affects the performance of the code. In Section 4 we discuss the application of monomial permutations with cycles of the same length to turbo codes.

We first review some notation and present some results that will be used in the rest of the paper.

⋆ This work was supported in part by the ADVANCE Institutional Transformation Program, NSF Grant SBE-0123654, and by the PR Space Grant IDEAS-ER Program, Grant NAGP5-40091.

2 Preliminaries from Number Theory

Some of the following concepts and results are well known and can be found in almost any text in number theory. The other results are very easy to prove.

From now on p is a prime number, q is a power of a prime and n, k, l, j, h are positive integers. The *Euler function*, $\phi(n)$, denotes the number of positive integers not exceeding n that are relatively prime to n.

One of the most used concepts in this paper is the order of an element. The *order* of an integer i modulo n is the smallest positive integer j such that $i^j \equiv 1 \ (mod\ n)$ and it will be denoted by $j = ord_n(i)$.

Lemma 1. *If* $i \equiv b \ \left(mod\ p^l\right)$, *then* $i^p \equiv b^p \ \left(mod\ p^{l+1}\right)$ *for all* $l \geq 1$.

Lemma 2. *Let* $j = ord_{p^l}(i)$. *Then* $j = ord_{p^{l+1}}(i)$ *or* $jp = ord_{p^{l+1}}(i)$.

Proposition 1. $j = ord_{p^k}(i)$ *and* $j|(p-1)$ *if and only if* $j = ord_{p^l}(i)$ *for all* $1 \leq l \leq k$.

Lemma 3. *Let* $p = ord_{p^k}(i)$ *for some* $k \geq 2$. *Then either* $2 = p = ord_{p^l}(i)$ *for* $2 \leq l \leq k$ *or* $i \equiv 1 \ \left(mod\ p^l\right)$ *for* $1 \leq l \leq k$.

Lemma 4. *Let* $j = ord_s(i),\ j = ord_l(i)$ *and* $gcd(s, l) = 1$. *Then* $j = ord_{sl}(i)$.

Lemma 5. *Let* $j = ord_s(i),\ i \equiv 1 \ (mod\ l)$ *and* $gcd(s, l) = 1$. *Then* $j = ord_{sl}(i)$.

On Section 3.1 we will give formulas to count the number of permutation monomials $x^i \in \mathbf{F}_q[x]$ that decompose in cycles of the same length j. The next results will be helpful.

Proposition 2. *Let* p *be an odd prime and suppose that* $j|\phi\left(p^n\right)$. *Then, there are* $\phi(j)$ *incongruent elements of order* j *modulo* p^n.

Proposition 3. *The incongruent solutions of* $x^2 \equiv 1 \ \left(mod\ 2^k\right)$ *are:*

$$\begin{cases} \pm 1,\ \pm\left(1 + 2^{k-1}\right) & \text{if } k \geq 3 \\ \pm 1 & \text{if } k = 2 \\ 1 & \text{if } k = 1 \ . \end{cases}$$

3 Cycles of the Same Length

The cycle structure of permutation monomials $x^i \in \mathbf{F}_q[x]$ was studied by Ahmad in [1]. The cycle structure for more general polynomials, specifically Dickson polynomials, was studied by Lidl and Mullen in [4]. Here, we present the necessary and sufficient conditions on the exponent i to obtain permutations of $\mathbf{F}_q$ that decompose in cycles of the same length. We will use the following result proven in [1].

Theorem 1. *The permutation of* $\mathbf{F}_q$ *given by* x^i *has a cycle of length* j *if and only if* $j = ord_t(i)$*, where* $t|(q-1)$*. The number* N_j *of such cycles is*

$$jN_j = gcd\left(q-1, i^j-1\right) - \sum_{s|j, s<j} sN_s \ .$$

We say that a permutation has cycles of the same length j if the permutation decomposes in cycles of length j or 1. The next theorem characterizes the permutation monomials with this property.

Theorem 2. *Let* $q-1 = p_0^{k_0} p_1^{k_1} \cdots p_r^{k_r}$*. The permutation of* $\mathbf{F}_q$ *given by* x^i *has cycles of the same length* j *if and only if one of the following holds for each* $l = 0, \cdots, r$*:*

1. $i \equiv 1 \pmod{p_l^{k_l}}$
2. $j = ord_{p_l^{k_l}}(i)$ *and* $j|\,(p_l - 1)$
3. $j = ord_{p_l^{k_l}}(i),\ k_l \geq 2$ *and* $j = p_l$.

Proof. ($\Longleftarrow$) If $i \equiv 1 \pmod{p_l^{k_l}}$ for all $l = 0, 1, \cdots, r$, then x^i is the identity permutation. Suppose that $1 < j = ord_{p_l{}^{k_l}}(i)$ for some of the l's and $i \equiv 1 \pmod{p_l^{k_l}}$ for the other. Proposition 1 and Lemma 3 guaranty that $j = ord_{p_l^k}(i)$ or $i \equiv 1 \pmod{p_l^k}$ for all $l = 0, 1, \cdots, r$ and $1 \leq k \leq k_l$. Now, if $t|(q-1)$, then by Lemmas 4 and 5, we have that, $j = ord_t(i)$ or $i \equiv 1 \pmod{t}$. Hence, by Theorem 1, all the cycles have length j or 1.

($\Longrightarrow$) Suppose that all the cycles have the same length j. Then, by Theorem 1, $j = ord_t(i)$ or $i \equiv 1 \pmod{t}$ for all t that divides $q-1$. This holds in particular for $t = p_l^{k_l},\ l = 0, 1, \cdots, r$. We only have to prove that, if $j = ord_{p_l^{k_l}}(i)$ then $j|\,(p_l - 1)$ or $j = p_l,\ k_l \geq 2$.

Suppose that $1 \neq j = ord_{p_l^{k_l}}(i)$. If $k_l = 1$ then $j|\,(p_l - 1)$ and we are done. If $k_l \geq 2$ and $j \not|\,(p_l - 1)$, then Proposition 1 implies that $j \neq ord_{p_l^k}(i)$ for some $k < k_l$. Let s be the largest one such that $j \neq ord_{p_l^s}(i)$. Then $i \equiv 1 \pmod{p_l^s}$ because otherwise, by Theorem 1, there would be a cycle of length different from j. By Lemma 1, $i^{p_l} \equiv 1 \pmod{p_l^{s+1}}$. But $j = ord_{p_l^{s+1}}(i)$ implies that $j|p_l$ and hence $j = p_l$. □

The next results consider the special cases where $0, 1$ or $0, 1, -1$ are the only elements fixed by the permutation. These results were first presented on [6] but the proofs there did not use Theorem 1.

It is clear that 0 and 1 are always fixed by the permutation x^i. Fixed elements are the same as cycles of length 1, so, by Theorem 1, an element is fixed if and only if $i \equiv 1 \pmod{t}$, where $t|(q-1)$. Note that -1 is a fixed element if and only if $i \equiv 1 \pmod{2}$. Hence, $0, 1, -1$ are the only elements fixed by the permutation if and only if $i \not\equiv 1 \pmod{t}$ for any $t \neq 2$ such that $t|(q-1)$.

We first consider q being such that 4 does not divide $q-1$.

Theorem 3. *Let* $q-1 = p_0^{k_0} p_1^{k_1} \cdots p_r^{k_r},\ p_0 = 2,\ k_0 = 0, 1$. *The permutation of* $\mathbf{F}_q$ *given by* x^i *decomposes in cycles with the same length* j *and* $0, 1, -1$ *or* $0, 1$ *are the only fixed elements if and only if* $j = ord_{p_l^{k_l}}(i)$ *and* $j | (p_l - 1)$ *for* $p_l \neq 2$.

Proof. ($\Longrightarrow$) Suppose that all the cycles have length j and $0, 1, -1$ or $0, 1$ are the only fixed elements. Then $j = ord_{p_l^k}(i)$ for $p_l \neq 2,\ k \leq k_l$ and, by Proposition 1, $j | (p_l - 1)$.

($\Longleftarrow$) Suppose that $j = ord_{p_l^{k_l}}(i)$ and $j | (p_l - 1)$ for $p_l \neq 2$. Then, Theorem 2 implies that all the cycles have the same length j. Also, Proposition 1 implies that $j = ord_{p_l^h}(i),\ h \leq k_l,\ p_l \neq 2$. Hence $i \not\equiv 1\ (mod\ t)$ for any $t | (q-1), t \neq 2$ and the only possible fixed elements are $0, 1, -1$. □

In the case where 4 divides $q - 1$ there are only two monomials that give permutations that decompose in cycles of the same length and have $0, 1, -1$ as the only fixed elements. Also, the length of the cycles on such permutations is always 2.

Theorem 4. *Let* $q-1 = p_0^{k_0} p_1^{k_1} \cdots p_r^{k_r}$, *where* $p_0 = 2,\ k_0 \geq 2$. *The permutation of* $\mathbf{F}_q$ *given by* x^i *decomposes in cycles of the same length* j *and* $0, 1, -1$ *are the only fixed elements if and only if* $j = ord_{p_l^{k_l}}(i)$ *for* $p_l \neq 2,\ j = ord_{2^h}(i)$ *for* $2 \leq h \leq k_0$, *and* $j = 2$.

Proof. By the arguments given before Theorem 3, $0, 1, -1$ are the only fixed elements if and only if $i \not\equiv 1\ \left(mod\ p_l^h\right)$ for $p_l \neq 2,\ h \leq k_l$, and for $p_0 = 2,\ 2 \leq h \leq k_0$. Since $j | (p_0 - 1)$ would imply that $j = 1$, the result now follows applying Theorem 2. □

Corollary 1. *Let* $q-1 = p_0^{k_0} p_1^{k_1} \cdots p_r^{k_r}$, *where* $p_0 = 2,\ k_0 > 2$. *The permutation of* $\mathbf{F}_q$ *given by* x^i *decomposes in cycles of the same length* j *and* $0, 1, -1$ *are the only fixed elements if and only if* $j = 2$ *and* $i = q - 2$ *or* $i = \frac{q-3}{2}$.

Proof. By Proposition 3, for $k_0 > 2$, $2 = ord_{2^{k_0}}(i)$ if and only if $i \equiv -1$ or $i \equiv \pm\left(1 + 2^{k_0 - 1}\right)\ \left(mod\ 2^{k_0}\right)$. But $2 = ord_4(i)$ if and only if $i \equiv -1$ or $i \equiv -1 - 2^{k_0 - 1}\ \left(mod\ 2^{k_0}\right)$.

Then, by the previous theorem and Proposition 3, we have cycles of the same length j and $0, 1, -1$ are the only fixed elements if and only if $i \equiv -1$ or $i \equiv -1 - 2^{k_0 - 1}\ \left(mod\ 2^{k_0}\right)$, and $i \equiv -1\ \left(mod\ p_l^{k_l}\right)$. Hence, there are only two i's such that the permutation x^i decomposes in cycles of the same length $j = 2$ and have $0, 1, -1$ as the only fixed elements. Noting that $\frac{q-3}{2} + 1 + 2^{k_0 - 1} = \frac{2^{k_0}\left(p_1^{k_1} \cdots p_r^{k_r} + 1\right)}{2} = 2^{k_0} s$, for some $s \in \mathbb{Z}$, we get that $i \equiv -1\ (mod\ q-1)$ and $i \equiv \frac{q-3}{2}\ (mod\ q-1)$ are the only solutions. □

Corollary 2. *Let* $q - 1 = 4 p_1^{k_1} \cdots p_r^{k_r}$. *The permutation of* $\mathbf{F}_q$ *given by* x^i *decomposes in cycles of the same length* j *and* $0, 1, -1$ *are the only fixed elements if and only if* $j = 2$ *and* $i = q - 2$.

Proof. By arguments similar to those given in the previous proof, the only i such that x^i gives a permutation with cycles of the same length $j = 2$ and have $0, 1, -1$ as the only fixed elements is $i \equiv -1 \pmod{q-1}$. □

3.1 Counting the Number of Permutation Monomials that Decompose in Cycles of the Same Length

In this section we give formulas for counting the number of permutation monomials that decompose in cycles of the same length j. To do this, we define a bijection between the set of all the i such that x^i decompose in cycles of the same length j and another set. Let $q-1 = p_0^{k_0} p_1^{k_1} \cdots p_r^{k_r}$, and define

$$U_j = \left\{ i \mid x^i \text{ is a permutation of } \mathbf{F}_q \text{ that decomposes in cycles of length } j \right\} .$$

and

$$W_j = \Big\{ (w_0, w_1, \cdots, w_r) \mid w_n \in \mathbb{Z}_{p_n^{k_n}},\ j = ord_{p_n^{k_n}}(w_n) \text{ for } j \mid (p_n - 1), \text{ or } j = ord_{p_n^{k_n}}(w_n) \text{ for } k_n \geq 2 \text{ and } j = p_n, \text{ or } w_n \equiv 1 \pmod{p_n^{k_n}} \Big\} .$$

Lemma 6. *Let $q-1 = p_0^{k_0} p_1^{k_1} \cdots p_r^{k_r}$ and U_j and W_j be defined as above. Let $f_j : U_j \longrightarrow W_j$ be defined by $f_j(i) = (w_0, w_1, \cdots, w_r)$, where $i \equiv w_n \pmod{p_n^{k_n}}$ for $0 \leq n \leq r$. Then f_j is a bijection.*

Proof. Note that by Theorem 2, if x^i decomposes in cycles of length j if and only if for each $0 \leq n \leq r$, we have that $j = ord_{p_n^{k_n}}(i)$ for $j \mid (p_n - 1)$, or $j = ord_{p_n^{k_n}}(i)$ for $k_n \geq 2$ and $j = p_n$, or $i \equiv 1 \pmod{p_n^{k_n}}$. Since $i \equiv w_n \pmod{p_n^{k_n}}$ for $0 \leq n \leq r$ we have that $f_j(U_j) \subseteq W_j$.

To see that f_j is onto, let $(w_0, w_1, \cdots, w_r) \in W_j$. We need to find i such that x^i decomposes in cycles of length j and $i \equiv w_n \pmod{p_n^{k_n}}$ for $0 \leq n \leq r$. By the definition of W_j and Theorem 2, we just have to find a solution to the system

$$\begin{cases} i \equiv w_0 \pmod{p_0^{k_0}} \\ i \equiv w_1 \pmod{p_1^{k_1}} \\ \quad \vdots \\ i \equiv w_r \pmod{p_r^{k_r}} \end{cases} .$$

The Chinese Remainder Theorem guaranties that there is a unique solution modulo $q-1 = p_0^{k_0} p_1^{k_1} \cdots p_r^{k_r}$.

□

Theorem 5. *Let $q-1 = p_0^{k_0} p_1^{k_1} \cdots p_r^{k_r}$. Then, the number of permutations x^i of $\mathbf{F}_q$ with cycles of the same length $j \neq 1$ is*

$$\prod_{n=0}^{r} f\left(j, p_n^{k_n}\right) - 1, \tag{1}$$

where, for p_n odd,

$$f\left(j, p_n^{k_n}\right) = \begin{cases} 1+\phi(j) & \text{if } \ j \,|\, (p_n - 1) \\ 1+\phi(j) & \text{if } \ j = p_n \text{ and } k_n \geq 2 \\ 1 & \text{otherwise,} \end{cases} \tag{2}$$

and, for $p_n = 2$,

$$f\left(j, 2^k\right) = \begin{cases} 4 & \text{if } \ j = 2, \ k \geq 3 \\ 2 & \text{if } \ j = 2, \ k = 2 \\ 1 & \text{if } \ j = 2, \ k = 1, \quad \text{or } \ j > 2 \ . \end{cases} \tag{3}$$

Proof. From the previous lemma we have that counting the x^i with cycles of length j is the same as counting the elements in W_j. For each $0 \leq n \leq r$, we have to count the number $f\left(j, p_n^{k_n}\right)$ of elements in $\mathbb{Z}_{p_n^{k_n}}$ of order 1, or of order j if $j \,|\, (p_n - 1)$ or $j = p_n$. Formula 1 give us the number of all possible x^i with cycles of length j; we subtract 1 for the case where $i \equiv 1 \ (mod\ q-1)$, that is when all the elements are fixed.

By Proposition 2, there are $\phi(j)$ elements of order j and one element congruent to 1 in $\mathbb{Z}_{p_n^{k_n}}$ for each p_n odd. This give us (2). For the case $p_n = 2$ and $j > 2$, by Theorem 2, one must have that $i \equiv 1 \ \left(mod\ 2^k\right)$ and hence $f\left(j, 2^k\right) = 1$ for $j > 2$. The other cases on (3) follow from Proposition 3. □

Now consider the case where the permutation x^i has cycles of length j and $0, 1, -1$ are the only elements fixed by the permutation. This case is of particular interest for the application to turbo codes as we will explain in the next section.

Corollary 2 says that, when $q - 1 = 4p_1^{k_1} \cdots p_r^{k_r}$, the only permutation $x^i \in \mathbf{F}_q[x]$ that decomposes in cycles of the same length and has $0, 1, -1$ as the only fixed elements is x^{q-2}. For the case when $q - 1 = 2^k p_1^{k_1} \cdots p_r^{k_r}$, $k > 2$, Corollary 1 give us two permutation monomials with this property: x^{q-2} and $x^{\frac{q-3}{2}}$. The following proposition give us the number of monomials with this property for the other cases.

Proposition 4. *Let $q - 1 = p_0^k p_1^{k_1} \cdots p_r^{k_r}$, $k = 0, 1$. The number of monomials $x^i \in \mathbf{F}_q[x]$ with cycles of length j and have $0, 1$ or $0, 1, -1$ as the only fixed elements is $\phi(j)^r$ if $j \,|\, (p_n - 1)$ for all $1 \leq n \leq r$, and 0 otherwise.*

Proof. By Theorem 3, x^i has cycles of length j and $0, 1$ or $0, 1, -1$ are the only fixed elements only if $j \,|\, (p_n - 1)$ for all $1 \leq n \leq r$. Suppose that $j \,|\, (p_n - 1)$ for all $1 \leq n \leq r$. As in in Lemma 6, we can construct a bijection between the set of monomials x^i that decompose in cycles of length j and have $0, 1$ or $0, 1, -1$ as the only fixed elements and the set

$$W_j = \left\{ (w_1, w_2, \cdots, w_r) \mid w_n \in \mathbb{Z}_{p_n^{k_n}},\ j = ord_{p_n^{k_n}}(w_n) \right\} .$$

Again, counting the number of such monomials is the same as counting the number of elements in W_j. Hence, by Proposition 2, there are $\phi(j)^r$ monomials $x^i \in \mathbf{F}_q[x]$ that have cycles of length j and have $0, 1$ or $0, 1, -1$ as the only fixed elements. □

4 Application to Turbo Codes

Error control codes are used in digital communication systems to protect information from errors that might occur during transmission. Turbo codes are specially suitable for satellite communication systems since they provide error control performance with a good reduction in the transmitter power levels.

One of the main components of a turbo encoder is the interleaver, which permutes the information symbols. The current practice to construct interleavers is to choose them randomly. The fact that these interleavers are found by computer search implies that they have to be stored in memory. Although good performance can be obtained with this type of construction, it is bad for implementation as well as for performance analysis. To avoid this problem, researchers have considered deterministic constructions that can be generated on the fly and that perform as well as random interleavers.

Most of the known methods for constructing interleavers algebraically do not produce interleavers that perform well. Some of the properties associated to the interleaver that are important to obtain "good" turbo encoders are the spreading and the dispersion factors. An article by Takeshita and Costello [7] as well as data obtained by Corrada-Bravo [2] suggested that another important property of an interleaver is the length of the cycles in the cyclic decomposition of the permutation in relation to the length of the cycle of the convolutional code in the turbo code.

We are constructing interleavers using permutation monomials that give permutations with a fixed length of cycles and studying the spreading and dispersion properties as well as the performance of the codes. In particular, we are studying permutations that only fix $0, 1, -1$ because, usually, permutations with few fixed elements have good dispersion. Also, it is very simple to construct monomials $x^i \in \mathbf{F}_q[x]$ that give permutations that decompose in cycles of the same length j and only fix $0, 1, -1$: if $4|(q-1)$ and $j = 2$, x^{q-2} and $x^{\frac{q-3}{2}}$ are the only choices; for $q - 1 = p_0^k p_1^{k_1} \cdots p_r^{k_r}$, $k = 0, 1$ and $j|\,(p_n - 1)$ for all $1 \leq n \leq r$, we only have to find i such that

$$\begin{cases} i \equiv 1 \pmod 2 \\ i \equiv w_1 \pmod{p_1^{k_1}} \\ \quad \vdots \\ i \equiv w_r \pmod{p_r^{k_r}} \end{cases} .$$

The proof of the Chinese Remainder Theorem gives an easy way to construct these i's.

Our simulations show that although our interleavers do not have better dispersion or spreading than random interleavers, interleavers with certain length of the cycles perform as well or better than them. More details on this can be found on [3]

Graphs with large girth have been used for the construction of regular and irregular low density parity check (LDPC) codes and recently, in [8] the author derived interleavers for turbo codes from graphs which have large girth. The *girth* (the length of the shortest cycle) of the turbo code graph, captures the relation between the cycle length of interleavers and the cycle length of the convolutional codes. We are carrying further studies on this relation in an attempt to answer the question as to which other parameters are necessary to established how an interleaver is going to perform. With this approach, we hope to be able to predict the performance of a turbo code with a particular interleaver, based on the cycle length of the convolutional code and the cycle structure of the interleaver. This would remove of the analysis (up to a degree) the painstaking and time consuming task of simulation.

Acknowledgments

The authors want to thank Professor Gary Mullen for suggesting the use of Theorem 1 to prove some of the results in this paper. We also appreciate the contribution of the following students from the University of Puerto Rico at Humacao: Marian Hernández-Viera, Yara Luis, Luis Medina-Rivera, Aida Navarro, Liannette Passapera, and Everilis Santana-Vega.

References

1. S. Ahmad, Cycle structure of automorphisms of finite cyclic groups, *J. Comb. Thy.* **6** (1969), 370-374.
2. C. J. Corrada-Bravo, *Sequence Designs for Applications in Ultra-wideband Systems and Turbo Codes*, Ph.D. Thesis, Univesity of Southern California, August, 2002.
3. C. J. Corrada-Bravo and I. Rubio, "Deterministic Interleavers for Turbo Codes with Random-like Performance and Simple Implementation", *Proceedings of the International Symposium on Turbo Codes*, September, 2003, pp 555-558.
4. R. Lidl, G.L. Mullen, Cycle Structure of Dickson Permutation Polynomials, *Mathematical Journal of Okayama University* **33** (1991), 1-11.
5. K. Rosen, *Elementary Number Theory and its Applications*, Fourth Edition, Addison Wesley, 1999.
6. I. Rubio, *Cyclic Decomposition of Monomial Permutations*, M.S. Thesis, University of Puerto Rico, Río Piedras, 1988.
7. O. Takeshita and D. Costello "New deterministic interleaver designs for turbo Codes", *IEEE-IT*, Vol. 46, pp. 1988-2006, Sept. 2000.
8. P. O. Vontobel, "On the Construction of Turbo Code Interleavers Based on Graphs with Large Girth", *Proc. IEEE Intern. Conf. Communications*, Vol.3, pp.1408-1412, New York, NY, USA, Apr. 28-May 2, 2002.