# Some Properties of Orthogonal Galois-Field Spreading Sequences

J. P. C. L. Miranda and H. M. de Oliveira

CODEC – Communications Research Group
Departamento de Eletrônica e Sistemas – CTG – UFPE
C.P. 7800, 50711-970, Recife – PE, Brazil
e-mail: jump@elogica.com.br , hmo@npd.ufpe.br

*Abstract* – ***Orthogonal Galois-field spreading sequences are a new tool to perform multilevel direct sequence spread spectrum communication (DS-SS). By defining a generalised finite field correlation, main properties of these digital sequences are derived. Besides, it is shown that good correlation properties of these "carriers" allow anti-jamming and multiple access capabilities. Systems which employ Galois-field spreading sequences are the so-called Galois-Division Multiple Access (GDMA). An attempt to classify GDMA signals as spread spectrum signals, by means of a more elegant treatment, is also supplied.***

Key-words: Spread Spectrum, Finite Field Transforms, Galois-Division Multiple Access.

## 1. INTRODUCTION

Finite field transforms have successfully been applied to perform spread spectrum communications [3],[4]. These new efficient digital schemes for band-limited channels, termed Galois-Division Multiple Access (GDMA), were originally presented in [3]. It is known that GDMA systems offer compact bandwidth requirements because only leaders of cyclotomic cosets are required to be transmitted [2],[4]. In a companion paper [7], GDMA figures of merit are evaluated, as well as its performance over noisy channels.

GDMA synchronous spreading sequences are denoted Galois-carriers. The main purpose of this paper is to derive Galois-carriers properties, inasmuch they allow multiple access capability. The statement "Galois-Division can perform multiple access communications" will be clarified.

Developments in section 3 consider spread spectrum signals. But, what is a spread spectrum signal? Under which circumstances GDMA can be considered a spread spectrum system? An attempt to provide a more formal treatment of this subject is also presented in section 4.

## 2. GALOIS-CARRIERS CORRELATION PROPERTIES

In spread spectrum communications, it is important that the spreading sequences assigned to users make possible a separation between the signal of a desired user and the signals of interfering users [9]. Since this separation is made by correlating the received signal with the locally generated replica of the code signal of the desired user, one can translate this demand to look for a low cross-correlation between sequences assigned to different users. Auto-correlation is also important because it decides how well we are able to synchronise and lock the locally generated replica to the received signal. As correlation properties of Galois-carriers play a very important role in the remainder of this paper, we start investigating them. The first step in this direction is to state a few preliminaries.

**Definition 1**: Finite field direct and inverse sequences are denoted by

$$x_i = \left(x_{i0}, x_{i1}, x_{i2}, \dots, x_{i(N-1)}\right) \tag{1a}$$

and

$$x_t^* = \left(x_{t0}^*, x_{t1}^*, x_{t2}^*, \dots, x_{t(N-1)}^*\right), \tag{1b}$$

where $x_{ik}$ and $x_{tk}$* are elements constituting the direct and inverse transform kernel of a finite-field transform of blocklength N, respectively. ■

**Definition 2**: The generalised finite field correlation is given by the following expression

$$R_x(i,t) = E[x_i x_t^*] = \frac{1}{N \text{ (mod p)}} \sum_{k=0}^{N-1} x_i x_t^* \,, \tag{2}$$

where $x_i$ and $x_t$* are the above defined sequences. ■

The finite field transform chose to be applied is a design option. Let us now investigate Galois-carriers correlation properties.

**Proposition 1**: Consider the Finite Field Fourier Transform (FFFT) [8]. The correlation property for the resultant Galois-Fourier carriers $\{c_i\}$ is given by:

$$R_c(i-t) = \frac{1}{N \text{ (mod p)}} \sum_{k=0}^{N-1} \alpha^{ik} \alpha^{-tk} = \begin{cases} 1, & i \equiv t \pmod{N} \\ 0, & \text{otherwise} \end{cases}, \tag{3}$$

where $R_c(\bullet)$ is the auto-correlation function (ACF) of the sequence $\{c_i\}$.

**Proof**: Let α be an element of multiplicative order N over GF($p^m$). According to (1a) and (1b), The Galois-Fourier carriers are:

$$\{c_i = \alpha^{ik}\} \text{ and } \{c_t{*} = \alpha^{-tk}\}. \tag{4}$$

From (2) we get:

$$R_c(i,t)=\frac{1}{N}\sum_{k=0}^{N-1}\alpha^{ik}\alpha^{-tk}=\frac{1}{N}\sum_{k=0}^{N-1}\alpha^{(i-t)k}=R_c(i-t).$$

Supposing now that i ≡ t (mod N), the value of ACF at the origin can be derived:

$$R_c(0)=\frac{1}{N\,(\mathrm{mod\,p})}\sum_{k=0}^{N-1}\alpha^{ik}\alpha^{-ik}\equiv 1\cdot$$

On the other hand, if i – t ≡ j ≠ 0 (mod N), then the cross-correlation between Galois-Fourier carriers is

$$\begin{aligned}R_c(j)&=\frac{1}{N\,(\mathrm{mod\ p})}\sum_{k=0}^{N-1}\alpha^{jk}\\&=\frac{1}{N}\frac{1-\alpha^{j[(N-1)+1]}}{1-\alpha^{j}}=\frac{1}{N}\frac{1-\alpha^{jN}}{1-\alpha^{j}}\equiv 0,\end{aligned}$$

since ord(α) = N. ■

Besides the FFFT, another finite field transform [1] termed Finite Field Hartley Transform (FFHT) can be used. It is a new finite field version of the integral transform introduced by R. V. L. Hartley [5]. Let GI(p) be the field of gaussian integers over a finite field GF(p).

**<u>Proposition 2</u>**: Consider the FFHT. The correlation property for resultant Galois-Hartley carriers is given by:

$$R_c(i-t)=\frac{1}{N}\sum_{k=0}^{N-1}cas_k(i)cas_k(t)=\begin{cases}1, & i\equiv t\,(\mathrm{mod}\,N)\\ 0, & \text{other cases}\end{cases}, \qquad (5)$$

where R(•) is the auto-correlation function (ACF) of the sequence $\{c_i\}$.

**Proof**: Let α be an element of multiplicative order N over GI(p). From definition 1, Galois-Hartley carriers are:

$$\{c_i=cas_k(i)\}\ \text{and}\ \{c_t{*}=cas_k(t)\}. \qquad (6)$$

It is worthwhile to mention that, due to the symmetry of $cas_k(\bullet)$, the FFHT belongs to a class of transforms for which the kernel of direct and inverse transform is exactly the same. From (2) we get:

$$R_c(i,t)=\frac{1}{N\,(\mathrm{mod\ p})}\sum_{k=0}^{N-1}cas_k(i)cas_k(t)\cdot$$

The definition of $cas_k(\bullet)$ function [1] leads to:

$$\begin{aligned}R_c(i,t)&=\frac{1}{N}\sum_{k=0}^{N-1}[\cos_k(i)+sin_k(i)][\cos_k(t)+sin_k(t)]\\&=\frac{1}{N}\sum_{k=0}^{N-1}\cos_k(i)\cos_k(t)+\frac{1}{N}\sum_{k=0}^{N-1}\cos_k(i)sin_k(t)+\\&+\frac{1}{N}\sum_{k=0}^{N-1}sin_k(i)\cos_k(t)+\frac{1}{N}\sum_{k=0}^{N-1}sin_k(i)sin_k(t)\cdot\end{aligned}$$

Once $\sin_k(\bullet)$ and $\cos_k(\bullet)$ are orthogonal to each other [1], the crossed terms vanishes:

$$R_c(i,t)=\frac{1}{N}\sum_{k=0}^{N-1}[\cos_k(i)\cos_k(t)+sin_k(i)sin_k(t)]\cdot$$

Applying now addition of arcs and symmetry properties of $\sin_k(\bullet)$ and $\cos_k(\bullet)$ [1]:

$$R_c(i,t)=\frac{1}{N}\sum_{k=0}^{N-1}\cos_k(i-t)=R_c(i-t).$$

Supposing that i ≡ t (mod N). The value of the ACF at origin can be derived:

$$R_c(0)=\frac{1}{N\,(\mathrm{mod\ p})}\sum_{k=0}^{N-1}\cos_k(0)\equiv 1\cdot$$

On the other hand, if i – t ≡ j ≠ 0 (mod N), then the cross-correlation between Galois-Hartley carriers becomes

$$R_c(j)=\frac{1}{N\,(\mathrm{mod\,p})}\sum_{k=0}^{N-1}\cos_k(j)\equiv 0,$$

since j ≠ 0. ■

## 3. Coherent Detection Over Additive Noise

Consider a GDM-based digital communication system. It is possible to consider the received signal as

$$\underline{R}=\underline{V}+\underline{W},$$

where $\underline{V}$ is the transform vector, defined over an extension field, and $\underline{W}=(W_0, W_1, ..., W_{N-1})$, is a finite field noise vector. We assume that information source symbols are equally likely. In this case such a receiver is a simple level detector. From now on y will denote a decision variable.

In direct sequence spread spectrum (DS-SS) systems, each information symbol is multiplied by a spreading sequence [9], usually a pseudo-noise (PN) code. In our framework, Galois-carriers correspond to GDM spreading sequences [6]. Consider modulating each user symbol with a Galois-carrier. Thus, each symbol of duration T is coded into a sequence of N chips of duration $T_c$ = T / N. The increase in signalling rate spreads the spectrum of the transmitted signal by a factor of N.

**<u>Proposition 3</u>**: Galois-Fourier carriers can perform direct sequence spread spectrum.

**Proof**: Consider a DS-SS system based on Galois-field spreading sequences (4). The received sequence (noisy spread vector), defined over GF($p^m$) can be assumed as

$$R_k = v_i \alpha^{ik} + W_k,$$

where k = 0, 1, ..., N–1. Then, the correlation receiver performs the following operation so as to obtain the decision variable y:

$$\begin{aligned} y &= \frac{1}{N\ (\mathrm{mod\ p})}\sum_{k=0}^{N-1} R_k \alpha^{-ik} \\ &= \frac{1}{N}\sum_{k=0}^{N-1}\left(v_i \alpha^{ik} + W_k\right)\alpha^{-ik} \\ &= v_i\left(\frac{1}{N}\sum_{k=0}^{N-1}\alpha^{ik}\alpha^{-ik}\right) + \frac{1}{N\ (\mathrm{mod\ p})}\sum_{k=0}^{N-1} W_k \alpha^{-ik}, \end{aligned}$$

which yields, based on (3):

$$y = v_i + \frac{1}{N\ (\mathrm{mod\ p})}\sum_{k=0}^{N-1} W_k \alpha^{-ik} \cdot$$

The second term is precisely the inverse FFFT of $\{W_k\}$. Since $\{W_k\}$ is a valid Galois-Fourier spectrum, the $\{w_i\} \leftrightarrow \{W_k\}$ is a sequence on the ground field, i.e., $w_i \in$ GF(p). ■

In this paper we are not concerned with performance so finite-field noise distribution is not addressed. However, no improvement over the additive channel is observed compared with a non-spread system. A similar result can be derived to Galois-Hartley spreading sequences.

**Proposition 4**: Galois-Hartley carriers can be used to perform direct sequence spread spectrum.

**Proof**: Consider a DS-SS system based on Galois-field spreading sequences (6). The received sequence (noisy spread vector), defined over GI(p), can be described as

$$R_k = v_i cas_k(i) + W_k,$$

where k = 0, 1, ..., N–1. The correlator performs then the following operation:

$$\begin{aligned} y &= \frac{1}{N\ (\mathrm{mod\ p})}\sum_{k=0}^{N-1} R_k cas_k(i) \\ &= \frac{1}{N}\sum_{k=0}^{N-1}\left[v_i cas_k(i) + W_k\right]cas_k(i) \\ &= v_i\left[\frac{1}{N}\sum_{k=0}^{N-1} cas_k(i) cas_k(i)\right] + \frac{1}{N}\sum_{k=0}^{N-1} W_k cas_k(i) \cdot \end{aligned}$$

It follows then from proposition 2 that

$$y = v_i + \frac{1}{N\ (\mathrm{mod\ p})}\sum_{k=0}^{N-1} W_k cas_k(i) = v_i + w_i \cdot$$ ■

It can be seen that the signalling rate is increased by a factor of N, but this also increases the signal bandwidth by a factor of N.

### 3.1 Anti-Jamming Capability

Cross-correlating a Galois-carrier will spread the narrowband signal thereby reducing interfering in the information bandwidth. This feature is called interference rejection. Anti-jamming capability is more or less the same as interference rejection except the interference is now wilfully inflicted on the system. This property together with the low probability of interception (due to the low power density of spread signals) makes this technique attractive for some applications. As despreading is almost the same operation as spreading a possible jammer-signal in the channel is spread before the data detection is done. Also this jammer won’t cause problems.

Now suppose the channel contains an interferer: an unknown constant is added to the received signal [9]. We assume that the interfering signal remains at the same level over a time slot greater than T, a user data symbol duration.

**Proposition 5**: Galois-Fourier carriers tolerate anti-jamming communications.

**Proof**: Suppose that the spread sequence is

$$R_k = v_i \alpha^{ik} + I + W_k,$$

where I is a constant over GF($p^m$) and k = 0, 1, ..., N–1. Then the correlation receiver produces the following decision variable:

$$\begin{aligned} y &= \frac{1}{N\ (\mathrm{mod\ p})}\sum_{k=0}^{N-1} R_k \alpha^{-ik} \\ &= \frac{1}{N}\sum_{k=0}^{N-1}\left(v_i \alpha^{ik} + I + W_k\right)\alpha^{-ik} \\ &= v_i\left(\frac{1}{N}\sum_{k=0}^{N-1}\alpha^{ik}\alpha^{-ik}\right) + \frac{I}{N}\sum_{k=0}^{N-1}\alpha^{-ik} + \frac{1}{N}\sum_{k=0}^{N-1} W_k \alpha^{-ik} \\ &= v_i + \frac{1}{N\ (\mathrm{mod\ p})}\sum_{k=0}^{N-1} w_k \alpha^{-ik} \cdot \end{aligned}$$ ■

**Proposition 6**: Galois-Hartley carriers allow anti-jamming communication.

**Proof**: Let us assume that we have

$$R_k = v_i cas_k(i) + I + W_k,$$

where I is a constant over GI(p) and k = 0, 1, ..., N–1. The correlation receiver output is

$$\begin{aligned} y &= \frac{1}{N\ (\mathrm{mod\ p})}\sum_{k=0}^{N-1} R_k cas_k(i) \\ &= \frac{1}{N}\sum_{k=0}^{N-1}\left[v_i cas_k(i) + I + W_k\right]cas_k(i) \end{aligned}$$

$$= v_i\left(\frac{1}{N}\sum_{k=0}^{N-1} cas_k(i)cas_k(i)\right) + \frac{I}{N}\sum_{k=0}^{N-1} cas_k(i)$$

$$+\frac{1}{N}\sum_{k=0}^{N-1} W_k cas_k(i)$$

$$= v_i + w_i \cdot \qquad \blacksquare$$

In both cases, the interference is suppressed by despreading (correlation) operation.

## 3.2 Multiple Access Capability

If multiple users transmit a spread spectrum signal at the same time, the receiver will still be able to distinguish between users provided that each user has a unique sequence that has null cross-correlation with the other sequences. Correlating the received signal with a sequence signal from a certain user will then only despread this user signal. Thus, the desired signal can be extracted.

Now assume there are N users (transmitters), where the k$^{th}$ transmitter modulates data with its particular spreading sequence subscript k. In this case, the Galois-carriers can be interpreted as signature codes. As we shall see, the zero cross-correlations and impulse-valued auto-correlations of Galois-carriers allow direct sequence multiple access. Suppose that all users are simultaneously transmitting, and we are interested in recovering the signal from j$^{th}$-user. Let us assume a perfect time synchronisation between users.

**Proposition 7**: Galois-Fourier carriers can be used to perform direct-sequence multiple access.

**Proof**: The received vector is:

$$R_k = \sum_{i=0}^{N-1}\left(v_i\alpha^{ik}\right) + W_k \cdot$$

It follows that the correlation receiver for the j$^{th}$-user generates the decision variable y$_j$:

$$y_j = \frac{1}{N \text{ (mod p)}}\sum_{k=0}^{N-1} R_k\alpha^{-jk}$$

$$= \frac{1}{N}\sum_{k=0}^{N-1}\left( v_j\alpha^{jk} + \sum_{\substack{i=0\\ i\neq j}}^{N-1} v_i\alpha^{ik} + W_k \right)\alpha^{-jk}$$

$$= v_j\left(\frac{1}{N}\sum_{k=0}^{N-1}\alpha^{jk}\alpha^{-jk}\right) + \sum_{\substack{i=0\\ i\neq j}}^{N-1} v_i\left(\frac{1}{N}\sum_{k=0}^{N-1}\alpha^{ik}\alpha^{-jk}\right)$$

$$+\frac{1}{N}\sum_{k=0}^{N-1} W_k\alpha^{-jk}$$

$$\equiv v_j + \frac{1}{N}\sum_{k=0}^{N-1} W_k\alpha^{-jk} \cdot \qquad \blacksquare$$

**Proposition 8**: Galois-Hartley carriers can also be used to perform direct-sequence multiple access.

**Proof**: The received signal is:

$$R_k = \sum_{i=0}^{N-1}\left[v_i cas_k(i)\right] + W_k \cdot$$

The correlation receiver for the j$^{th}$-user generates the decision variable:

$$y_j = \frac{1}{N}\sum_{k=0}^{N-1} R_k cas_k(j)$$

$$= \frac{1}{N}\sum_{k=0}^{N-1}\left[ v_j cas_k(j) + \sum_{\substack{i=0\\ i\neq j}}^{N-1} v_i cas_k(i) + W_k \right] cas_k(j)$$

$$= v_j\left[\frac{1}{N}\sum_{k=0}^{N-1} cas_k(j)cas_k(j)\right] +$$

$$+\sum_{\substack{i=0\\ i\neq j}}^{N-1} v_i\left[\frac{1}{N}\sum_{k=0}^{N-1} cas_k(i)cas_k(j)\right]$$

$$+\frac{1}{N}\sum_{k=0}^{N-1} W_k cas_k(j)$$

$$\equiv v_j + w_j \cdot \qquad \blacksquare$$

Therefore, the cross-correlation property of Galois-carriers allows simultaneous transmission in the same channel. This property grants spread spectrum based on finite field transforms to be used as a new digital multiple access method: the Galois-Division Multiple Access, or GDMA.

## 4. GDMA Spread Spectrum Signals

Properties derived in section 3 assumed GDMA signals as spread spectrum signals. In order to enjoy the features of wideband, we have to show that such an assumption is true. A rather unconventional definition (but found to be satisfactory) of a spread spectrum signal is given below [6].

**Definition 3**: A spread spectrum signal is a signal whose Fourier bandwidth is substantially greater than its Shannon bandwidth. ■

In other words, a spread spectrum signal is a signal that uses much more bandwidth than it needs. The Fourier bandwidth denotes the ordinary notion of bandwidth and the Shannon bandwidth is defined as one-half the minimum number of dimensions per second required to represent the modulated signal in a signal space, i.e., B = N / 2T dim / sec.

For GDMA systems, the signal space is GF(p$^m$) or GI(p), depending on the finite field transform chosen. Once field elements can be viewed as m-dimensional vectors with GF(p)-valued components, we are dealing with an m-dimensional signal space. Therefore:

$$B_{GDMA} = \frac{1}{2}\frac{m}{T}. \qquad (7)$$

The ratio of transmitted bandwidth to information bandwidth denotes the processing gain $G_p$ of the spread spectrum system. Here $G_p = N$. For our purposes, the following definition provides a better tool (than $G_p$) to investigate, according to definition 3, if a transmitted signal is in fact a spread spectrum signal.

**Definition 4**: The spreading factor of a modulated signal is the ratio of its Fourier bandwidth to its Shannon bandwidth, i.e.,

$$\gamma = \frac{W}{B}. \qquad (8)$$

For every modulated signal, $\gamma \geq 1$. A spread spectrum signal is a signal with "large" $\gamma$, say $\gamma > 5$. Of course the precise line between a spread spectrum signal and an unspread one is rather arbitrary.

Example 1: Suppose that cyclotomic compression is not used. Each user modulates a user-specific Galois-carrier of length N (equal to the total number of users) with one data symbol in each symbol period of duration T. The full spectrum modulated signal can be written as

$$s(t) = \sum_{i=0}^{N-1} v_i c_i h\left(\frac{N}{T}t - i\right), 0 \leq t < T,$$

where $\underline{v}$ is the incoming data over GF(p), $\underline{c}$ are the Galois-carriers, and $h\left(\frac{N}{T}t\right), 0 \leq t < T$ is the formatting pulse of a chip. Hence, the Fourier bandwidth W is:

$$2W = \frac{N}{T} \rightarrow W_{GDMA} = \frac{N}{2T}. \qquad (9)$$

The spreading factor computation is carried out substituting (7) and (9) into (8):

$$\gamma_{GDMA} = \frac{N}{2T}\frac{2T}{m} = \frac{N}{m}.$$

Since the number of users is $N = p^m - 1$,

$$\gamma_{GDMA} = \frac{p^m - 1}{m}.$$

Indeed, binary non-expanded alphabet transmissions has $\gamma = 1$ and no spreading is achieved.

Example 2: Suppose that cyclotomic compression is now used. Each user modulates a user-specific Galois-carrier of length ν (equal to the number of cyclotomic cosets associated with a finite field transform spectrum) still with one data symbol in each symbol period of duration T. After selecting only cyclotomic leaders for transmission, the modulated signal is now

$$s'(t) = \sum_{i=0}^{\nu-1} v_i c_i h\left(\frac{\nu}{T}t - i\right), 0 \leq t < T,$$

where $\underline{v}$ is the incoming data and $\underline{c}$ are the Galois-carriers. Hence, the Fourier bandwidth of this compressed signal is:

$$2W' = \frac{\nu}{T} \rightarrow W'_{GDMA} = \frac{\nu}{2T}. \qquad (10)$$

Taking (7) and (10) into (8) yields:

$$\gamma'_{GDMA} = \frac{\nu}{2T}\frac{2T}{m} = \frac{\nu}{m}.$$

Finally, the ratio $\gamma_{GDMA}$ to $\gamma'_{GDMA}$ can be derived:

$$\frac{\gamma_{GDMA}}{\gamma'_{GDMA}} = \frac{N}{m} \times \frac{m}{\nu} = \gamma_{cc},$$

where $\gamma_{cc} = N / \nu$ is exactly the bandwidth compactness factor early introduced [2].

## 5. Concluding Remarks

This paper introduces a generalised finite field correlation, which allows the deriving of interesting properties for Galois-carriers. Among these properties, the most important one is that GDM systems have multiple access capabilities, yielding thus new digital multiple access schemes: GDMA.

It was also shown that transmitted GDMA signals are indeed spread spectrum when m > 1, i.e., provided that higher alphabet extensions are taken. This is a desirable feature, once increased alphabets have the property of increasing the compactness factor ($\gamma_{cc}$) and decreasing bandwidth requirements, achieving better spectral efficiency regarding TDMA schemes.

The retrial of the user information requires that the receiver's own copy of the spreading sequence be synchronised with the received version. Effects of imperfect synchronisation over GDMA systems are left to be investigated.

## Acknowledgements

The first author thanks The Brazilian National Council for Research and Development (CNPq) for its partial financial support.

## REFERENCES

[1] R. M. Campello de Souza, H. M. de Oliveira and A. N. Kauffman, The Hartley Transform in a Finite Field, *Revista. da Soc. Bras. de Telecomunicações*, Vol.14 – Número 1, pp. 46 – 54, June 1999.

[2] H. M. de Oliveira, R. M. Campello de Souza and A. N. Kauffman, Efficient Multiplex for Band-Limited Channels, WCC '99 – *Workshop on Coding and Cryptography*, Paris, France, pp. 235 – 241, January 1999.

[3] H. M. de Oliveira and R. M. Campello de Souza, *Orthogonal Multilevel Spreading Sequence Design*, Coding, Communications and Broadcasting, Research Studies Press, Baldock, UK, pp. 291 – 301, 2000.

[4] H. M. de Oliveira, J. P. C. L. Miranda and R. M. Campello de Souza, *Spread Spectrum Based on Finite Field Fourier Transforms,* ICSECIT 2001 – International Conference on Systems Engineering, Communications and Information Technologies, Punta Arenas, Chile, ISBN 956-7189-11-0, April 2001.

[5] R. V. L. Hartley, A more symmetrical Fourier analysis applied to transmission problems, *proc. IRE*, vol. 30, pp. 144 – 150, 1942.

[6] J. L. Massey, Towards an Information Theory of Spread Spectrum Systems, in: *Code Division Multiple Access Communications*, Eds. S.G. Glisic and P.A. Leppänen, Boston, Dordrecht and London, Kluwer, pp. 29 – 46, 1995.

[7] J. P. C. L. Miranda and H. M. de Oliveira, *On Galois-Field Division Multiple Access Systems: Figures of Merit and Performance Evaluation*, 19º Congresso Brasileiro de Telecomunicações, Fortaleza–CE, Brazil, September 2001.

[8] J. M. Pollard, The Fast Fourier Transform in a Finite Field, *Math. Comput.*, vol. 25, Nº 114, pp. 365 – 374, April 1971.

[9] R. Prasad, CDMA For Wireless Personal Communications, Artech House Publishers, Boston-London, pp. 15 – 59, 1996.