Infinite Sequences over Finite Fields and New Digital Transforms

R. M. Campello de Souza, M. M. Campello de Souza,

H. M. de Oliveira, M. M. Vasconcelos

(ricardo, marciam, hmo)@ufpe.br, mmv@ee.ufpe.br

Digital Signal Processing Group - UFPE,

CP7800, CEP 50711-970 Recife PE, BRAZIL

Abstract

Digital Transforms have important applications on subjects such as channel coding, cryptography and digital signal processing. In this paper, two Fourier Transforms are considered, the discrete time Fourier transform (DTFT) and the finite field Fourier transform (FFFT). A finite field version of the DTFT is introduced and the FFFT is redefined with a complex kernel, which makes it a more appropriate finite field version of the Discrete Fourier Transform. These transforms can handle FIR and IIR filters defined over finite algebraic structures.

1 Introduction

Discrete Transforms play a very important role in engineering. Well known examples are the Discrete Fourier Transform (DFT) and the Z Transform [1]. A DFT over finite fields GF(q) (FFFT) was also defined [2] and applied to the computation of discrete convolutions through modular arithmetic. Recently, the Hartley Transform over $GF(q)$ (FFHT) was introduced [3], which has interesting applications in digital multiplexing and spread spectrum [4, 5]. The FFFT and the FFHT, instead of what happens with others discrete transforms, are examples of transforms of true digital nature.

In this paper, the Discrete Time Fourier Transform over a finite field (FFDTFT) is introduced. So far, the investigations reported in the literature about transforms defined over finite fields, only

consider finite sequences of elements from $GF(q)$, a constraint related to the problem of dealing with series convergence over a finite algebraic structure [6]. The proposed FFDTFT deals with finite and infinite sequences over finite fields. The paper also introduces a generalization of the DFT over a finite field, which results from the modification of its kernel. An FFFT with complex kernel is the appropriate finite field version for the DFT.

In the next section, some mathematical preliminaries are presented. In particular, the gaussian integers over $GF(p)$ (denominated galoisian integers) are defined and some special group families are built, in order to construct a polar representation for the galoisian integers. In section 3, infinite sequences over a Galois field are discussed, where issues on series convergence are investigated. In section 4, the Discrete Time Fourier Transform over a finite field is introduced. In section 5, a new definition for the FFFT is proposed. The paper closes with a few concluding remarks.

2 Mathematical Preliminaries

2.1 Complex Numbers over Finite Fields

The set $Ga(p)$ of gaussian integers over $GF(p)$ defined below plays an important role in the ideas introduced in this paper. Hereafter the symbol $\triangleq$ denotes *equal by definition*; $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ denote the rational, real and complex sets, respectively. δ is the Kronecker symbol.

Definition 1 *$Ga(p) \triangleq \{a + jb;\ a,\ b \in GF(p)\}$, p being an odd prime for which $j^2 = -1$ is a quadratic non-residue in $GF(p)$ (i.e., $p \equiv 3 \pmod 4$), is the set of galoisian integers over $GF(p)$.*

Let $\otimes$ denote cartesian product. It can be shown that the set $Ga(p)$ equipped with the operations $\oplus$ and $*$ defined below, is a field [7].

Proposition 1 *Let*

$$
\begin{aligned}
\oplus : Ga(p) \otimes Ga(p) &\rightarrow Ga(p) \\
(a_1 + jb_1, a_2 + jb_2) &\rightarrow (a_1 + jb_1) \oplus (a_2 + jb_2) = \\
&= (a_1 + a_2) + j(b_1 + b_2)
\end{aligned}
$$

2

and

$$* : Ga(p) \otimes Ga(p) \quad \rightarrow \quad Ga(p)$$

$$(a_1 + jb_1, a_2 + jb_2) \quad \rightarrow \quad (a_1 + jb_1) * (a_2 + jb_2) =$$

$$= (a_1 a_2 - b_1 b_2) + j(a_1 b_2 + a_2 b_1).$$

The structure $GL(p) \triangleq <Ga(p), \oplus, *>$ is a field. In fact, $GL(p)$ is isomorphic to $GF(p^2)$.

By analogy with the real and complex numbers, the elements of $GF(p)$ and of $GL(p)$ are said to be real and complex, respectively.

Proposition 2 *The elements $\zeta = (a + jb) \in GL(p)$ satisfies $\zeta^{p+1} \equiv |\zeta|^2 \equiv a^2 + b^2 \pmod{p}$.*

Proof:

$$\zeta^p = (a + jb)^p \equiv a^p + j^p b^p \pmod{p},$$

once $GL(p)$ is isomorphic to $GF(p^2)$, a field of characteristic p. Since $p = 4k + 3$, $j^p = -j$, so that $\zeta^p \equiv a - jb \pmod{p} = \zeta^* \pmod{p}$. Therefore, $\zeta^{p+1} \equiv \zeta\zeta^* = |\zeta|^2 \equiv a^2 + b^2 \pmod{p}$. ∎

2.2 Polar Form for Galoisian Integers in a Finite Field

In the definition of $GL(p)$, the elements were written in cartesian form $\zeta = a + jb$. In what follows, a different representation for the elements of the multiplicative group of $GL(p)$ is proposed, which allows to write them in the form $r\varepsilon^\theta$. By analogy with the continuum, such a form is said to be polar.

Proposition 3 *Let G_r and G_θ be subgroups, of the multiplicative group G of the nonzero elements of $GL(p)$, of orders $N_r = (p-1)/2$ and $N_\theta = 2(p+1)$, respectively. Then all elements of $GL(p)$ can be written in the form $\zeta = ab$, where $a \in G_r$ and $B \in G_\theta$ [8].*

Considering that any element of a cyclic group can be written as an integer power of a group generator, it is possible to set $r = a$ and $\varepsilon^\theta = b$, where ε is a generator of G_θ. Thus, the polar representation assumes the desired form, $\zeta = r\varepsilon^\theta$.

At this point, it seems clear that r is going to play the role of the modulus of ζ. Therefore, before further exploring the polar notation, it is necessary to formally define the concept of modulus

3

of an element in a finite field. Considering the nonzero elements of GF(p), it is a well-known fact that half of them are quadratic residues of p [9]. The other half, those that do not have a square root, are the quadratic non-residues. Likewise, in the field $\mathbb{R}$ of real numbers, the elements are divided into positive and negative numbers, those that have and those that do not have a square root. The standard modulus operation in $\mathbb{R}$ always gives a positive result. By analogy, the modulus operation in GF(p) is going to be defined, such that it always results in a quadratic residue of p.

Definition 2 *The modulus of an element $a \in$ GF(p), where $p = 4k + 3$, is given by*

$$|a| \triangleq \begin{cases} a, & \text{if } a^{(p-1)/2} \equiv 1 \pmod{p} \\ -a, & \text{if } a^{(p-1)/2} \equiv -1 \pmod{p} \end{cases}.$$

Proposition 4 *The modulus of an element of GF(p) is a quadratic residue of p.*

Proof: Since $p = 4k + 3$, it implies that $(p-1)/2 = 2k + 1$, such that $(-1)^{(p-1)/2} \equiv -1 \pmod{p}$. By Euler's criterion [9], if $a^{(p-1)/2} \equiv 1 \pmod{p}$, then a is a quadratic residue of p; if $a^{(p-1)/2} \equiv -1 \pmod{p}$, then a is a quadratic non-residue of p. Therefore, $(-a)^{(p-1)/2} \equiv (-1)(-1) \equiv 1 \pmod{p}$ and it follows that $|a|$ is a quadratic residue of p. ∎

Definition 3 *The modulus of an element $a + jb \in$ GL(p), where $p = 4k + 3$, is given by*

$$|a + jb| \triangleq \left| \sqrt{|a^2 + b^2|} \right|.$$

The inner modulus sign in the above expression is necessary in order to allow the computation of the square root of the quadratic norm $a^2 + b^2$, and the outer one guarantees that such an operation results in one value only. In the continuum, such an expression reduces to the usual norm of a complex number, since both, $a^2 + b^2$ and the square root operation, produce only positive numbers.

Proposition 5 *If $\zeta = a + jb = r\varepsilon^\theta$, where $r \in G_r$ and $\varepsilon^\theta \in G_\theta$, then $r = |\zeta|$.*

Proof: Every element of G$_r$ has an order that divides $(p-1)/2$. Thus, if $r \in$ G$_r$, then $r^{(p-1)/2} \equiv 1 \pmod{p}$, and $|r| = r$. Every element γ of G_θ has order that divides $2(p+1)$ and are those $c + jd$ satisfying $c^2 + d^2 \equiv \pm 1 \pmod{p}$, since that, from proposition 2, $\gamma^{2(p+1)} \equiv (c^2 + d^2)^2 \equiv 1 \pmod{p}$. Besides that, as shown in next section, the elements of the group G$_\theta$ are those $a + jb$ such that

4

$a^2 + b^2 \equiv \pm 1 \pmod{p}$. Therefore, according to definition 2, such elements have modulus equal to one, which means that $|\zeta| = |r\varepsilon^\theta| = |r||\varepsilon^\theta| = r \cdot 1 = r$. ∎

From the above it can be observed that the polar representation being introduced is consistent with the usual polar form defined over the complex field $\mathbb{C}$. The modulus belongs to $\mathrm{GF}(p)$ (the modulus is a real number) and is a quadratic residue of p (a positive number), and the exponential component ε^θ has modulus one and belongs to $\mathrm{GL}(p)$ ($e^{j\theta}$ also has modulus one and belongs to the complex field).

3 Infinite Series over Finite Fields

Given a sequence of integers $\{x[n]\}_{-\infty}^{\infty}$, it is possible to generate a sequence over $\mathrm{GF}(p)$ simply by considering $\{x[n] \pmod{p}\}_{-\infty}^{\infty}$. In general, $x[n]$ may even be a sequence of rational elements and any element $r/s \in \mathbb{Q}$ can be mapped over $\mathrm{GF}(p)$, $[r \pmod{p}] \cdot [s \pmod{p}]^{-1}$. The focus here concerns finite sequences, and *periodic* infinite sequences over a finite field.

Definition 4 *An infinite sequence of elements over GF(p) is periodic with period P, if it satisfies* $x[n] = x[n \pmod{P}]$.

Definition 5 *An infinite sequence, of elements over GF(p), that is zero valued for $n < N_1 < \infty$ $(-\infty < N_2 < n)$ and satisfies the condition on definition 4, is denominated left-sided periodic (right-sided periodic, respectively).*

For instance, consider the following right-sided sequences:

Example 1 *Let $\{x[n]\}_{-\infty}^{\infty}$, $x[n] \in GF(p)$, e.g.,*

i) $\{3^n\}_{n=0}^{\infty}$ (in GF(7)) = $\{1\ 3\ 2\ 6\ 4\ 5\ 1\ 3\ 2\ 6\ 4\ 5\ \ldots\}$ (P = 6).

ii) $\{1^n\}_{n=0}^{\infty}$ (in GF(5)) = $\{1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ \ldots\}$ (P = 1).

iii) $\{x[n]\}_{-\infty}^{\infty}$ (in GF(3)) = $\{\ldots\ 0\ 0\ 0\ 1\ 1\ 1\ 2\ 2\ 2\ 0\ 0\ 0\ \ldots\}$ (P = 9).

Is it possible to define a Discrete Time Fourier Transform for these sequences, by $X(\varepsilon^\theta) \triangleq \sum_{n=-\infty}^{\infty} x[n]\varepsilon^{-n\theta}$, where $\varepsilon \in \mathrm{GL}(p)$? Is this series convergent?

It is a well known fact that the infinite series $\sum_1^\infty (-1)^{n+1} = 1 - 1 + 1 - 1 + 1 - \ldots$ diverges in the classic sense. However, Euler among others noticed that the arithmetic mean of the partial sums converges to 1/2. The partial sums of this series are $S_1 = 1$, $S_2 = 0$, $S_3 = 1$, $S_4 = 0$, $\ldots$ and the arithmetic mean $\sigma_n \triangleq (1/n) \sum_{k=1}^n S_k$ forms the sequence (σ_n) that converges to 1/2.

When a series converges in the sense that the arithmetic mean of the partial sums converges, it is said to be Cesàro-summable (Ernesto Cesàro (1859-1906)) [10]. Every convergent series in the usual sense is Cesàro-summable and the series sum is equal to the limit of the sequence of the partial sums arithmetic mean. That shows the Cesàro summability, is now introduced. Given $\{x[n]\}_1^\infty$, the partial sums $S[n]$ are defined according to: $S[n] \triangleq \sum_{k=1}^n x[k]$.

Definition 6 *The Cesàro sum over a finite field is defined by*

$$\sigma_n \triangleq \frac{1}{n} \sum_{k=1}^n S[k],$$

where $S[k] \in GF(p)$ are interpreted as integers.

If $\{x[n]\}_1^\infty$ is a periodic sequence over $GF(p)$, so is $\{S[n]\}_1^\infty$. Let P denote the period of the latter sequence. Therefore

$$\lim_{n \to \infty} \frac{1}{n} \sum_{k=1}^n S[k] = \lim_{n \to \infty} \frac{1}{n} \left(\sum_{k=1}^{\lfloor n/P \rfloor \cdot P} S[k] + \sum_{\substack{k=1 \ (\mathrm{mod}\ P)}}^n S[k] \right).$$

The second term, which exists only if P do not divide n, vanishes and

$$\lim_{n \to \infty} \sigma_n = \lim_{n \to \infty} \frac{\lfloor n/P \rfloor}{n} \sum_{k=1}^P S[k].$$

But

$$\lim_{n \to \infty} \frac{\lfloor n/P \rfloor}{n} = \frac{1}{P},$$

so that

$$\lim_{n \to \infty} \frac{1}{n} \sum_{k=1}^n S[k] = \frac{1}{P} \sum_{k=1}^P S[k],$$

and therefore

$$\lim_{n \to \infty} \sigma_n \pmod{p} \equiv \frac{1}{P \pmod{p}} \sum_{k=1}^P S[k] \pmod{p}.$$

The heart of the matter is taking first the limit $n \to \infty$, and then evaluate the result after reducing it modulo p.

Definition 7 *A series over a finite field is said to be Cesàro convergent to σ if and only if*

$$\sigma \triangleq \lim_{n \to \infty} \sigma_n \pmod{p} \in GF(p).$$

Corollary 1 *Every periodic series over a finite field with a nonzero period, that is, $P \not\equiv 0 \pmod{p}$, is Cesàro convergent.*

Example 2 *Considering the sequence $\{3^n\}_{n=0}^{\infty}$ from example 1,*
$\{S[k]\} = \{1\ 4\ 6\ 5\ 2\ 0\ 1\ 4\ 6\ 5\ 2\ 0\ 1\ 4 \ldots\}$, $P \equiv 6 \pmod{7}$. *Therefore, the series converges, in the Cesàro sense, to*

$$\sigma = \frac{1}{6}(1 + 4 + 6 + 5 + 2 + 0) \equiv 3 \pmod{7}.$$

4 The Discrete Time Fourier Transform in a Finite Field

4.1 Basic Sequences

The transforms considered in this paper deal with sequences $x[n]$, defined over the finite field $GF(p)$, which are obtained from the basic sequences $\delta[n]$, $u[n]$ and Aa^n.

i. The finite field impulse over $GF(p)$ (Galois impulse), denoted by $\delta[n]$, is the sequence $x[n]$ defined by

$$x[n] = \delta[n] \triangleq \begin{cases} 1, & \text{if } n \equiv 0 \pmod{2(p+1)} \\ 0, & \text{otherwise} \end{cases}.$$

By analogy with sequences defined over the infinite field $\mathbb{R}$, any sequence $x[n]$ defined over a finite field can be expressed as a sum of scalonated and time shifted Galois impulses.

ii. The finite field unit step is given by

$$x[n] = u[n] \triangleq \begin{cases} 1, & \text{if } n \geq 0 \\ 0, & \text{otherwise} \end{cases}.$$

7

iii. The exponential sequence is $x[n] = A(a)^n$, A and $a \in \text{GF}(p)$. This sequence is periodic with period P, which is the multiplicative order of $a \pmod p$.

Definition 8 *The Discrete Time Fourier Transform (DTFT) of a sequence $x[n]$ over GF(p) is the function $X(\varepsilon^\theta)$, defined in GL(p), given by*

$$X(\varepsilon^\theta) \triangleq \sum_{n=-\infty}^{\infty} x[n]\varepsilon^{-n\theta},$$

where $\varepsilon \in G_\theta$ has multiplicative order $2(p+1)$.

In the infinite series defined above, the convergence is considered in the sense of definition 7.

Example 3 *The right exponential sequence over GF(p). Let $x[n] = a^n u[n]$, $a \in GF(p)$. In this case, since $x[n]$ is nonzero only for $n \geq 0$, then*

$$X(\varepsilon^\theta) \triangleq \sum_{n=-\infty}^{\infty} a^n u[n]\varepsilon^{n\theta} = \sum_{n=0}^{\infty}(a\varepsilon^{-\theta})^n.$$

Computing the partial sums:

$$
\begin{aligned}
S_1 &= 1 \\
S_2 &= 1 + a\varepsilon^{-\theta} \\
S_3 &= 1 + a\varepsilon^{-\theta} + (a\varepsilon^{-\theta})^2 \\
\vdots \quad & \vdots \qquad \ddots \ddots \ddots \\
S_{N-1} &= 1 + a\varepsilon^{-\theta} + (a\varepsilon^{-\theta})^2 + (a\varepsilon^{-\theta})^3 + \ldots + (a\varepsilon^{-\theta})^{N-2} \\
S_{N-2} &= 1 + a\varepsilon^{-\theta} + (a\varepsilon^{-\theta})^2 + (a\varepsilon^{-\theta})^3 + \ldots + (a\varepsilon^{-\theta})^{N-2} + (a\varepsilon^{-\theta})^{N-1}.
\end{aligned}
$$

Denoting by N the multiplicative order of $(a\varepsilon^{-\theta})$, the sequence $S[k]$ has a period equal to N. Therefore, it is possible to write

$$\sigma_N = \frac{1}{N}\sum_{i=0}^{N-1}(N-i)(a\varepsilon^{-\theta})^i,$$

or

$$\sigma_N = \frac{(a\varepsilon^{-\theta})^n - 1}{a\varepsilon^{-\theta} - 1} - \frac{1}{N}\sum_{i=0}^{N-1} i(a\varepsilon^{-\theta})^i,$$

Since $(a\varepsilon^{-\theta})$ has multiplicative order N,

$$\sigma_N = -\frac{\varepsilon^\theta}{N} \sum_{i=0}^{N-1} i a^i \varepsilon^{-\theta(-i-1)},$$

which is the same as

$$\sigma_N = \frac{\varepsilon^\theta}{N} \sum_{i=0}^{N-1} \frac{d}{d\varepsilon^\theta}(a^i(\varepsilon^\theta)^{-i}),$$

so that

$$\sigma_N = \frac{\varepsilon^\theta}{N} \frac{d}{d\varepsilon^\theta} \sum_{i=0}^{N-1} (a\varepsilon^{-\theta})^i.$$

A simple manipulation shows that the last expression is equal to

$$\sigma_N = \frac{1}{1 - a\varepsilon^{-\theta}},$$

which is the FFDTFT $X(\varepsilon^\theta)$.

4.2   The Inverse FFDTFT

Lemma 1 *If $\varepsilon \in G_\theta$ has multiplicative order $2(p+1)$, then*

$$\sum_{\theta=0}^{2(p+1)-1} \varepsilon^{\theta k} = \begin{cases} 2(p+1), & \text{if } k \equiv 0 \pmod{2(p+1)} \\ 0, & \text{otherwise} \end{cases}.$$

Proof: For $k \equiv 0 \pmod{2(p+1)}$, the sum is clearly equal to $2(p+1)$. Otherwise,

$$\sum_{\theta=0}^{2(p+1)-1} \varepsilon^{\theta k} = \frac{1 - \varepsilon^{k2(p+1)}}{1 - \varepsilon^k}$$

and the result follows. ∎

Theorem 1 (the inversion formula) *The inverse finite field discrete time Fourier transform is given by*

$$x[n] = \frac{1}{2(p+1)} \sum_{\theta=0}^{2(p+1)-1} X(\varepsilon^\theta)\varepsilon^{\theta n}.$$

Proof: By definition $X(\varepsilon^\theta) \triangleq \sum_{k=-\infty}^{\infty} x[k]\varepsilon^{-k\theta}$ Multiplying both sides by $\varepsilon^{n\theta}$ and summing over θ, we have

$$\sum_{\theta=0}^{2(p+1)-1} X(\varepsilon^\theta)\varepsilon^{\theta n} = \sum_{\theta=0}^{2(p+1)-1} \left(\sum_{k=-\infty}^{\infty} x[k]\varepsilon^{-k\theta} \right)\varepsilon^{\theta n}.$$

Changing the order of the sums, the right side of the expression above becomes

$$\sum_{\theta=0}^{2(p+1)-1} X(\varepsilon^{\theta})\varepsilon^{\theta n} = \sum_{k=-\infty}^{\infty} x[k]\left(\sum_{\theta=0}^{2(p+1)-1} \varepsilon^{\theta(n-k)}\right)$$

But, from lemma 1, the internal sum is nonzero only for $k = n$, so that

$$\sum_{\theta=0}^{2(p+1)-1} X(\varepsilon^{\theta})\varepsilon^{\theta n} = 2(p+1)x[n]$$

and the result follows. ∎

It is interesting to notice that, although the direct FFDTFT involves an infinite sum, being capable of handling infinite sequences, its inverse requires only a finite sum over the phase group G_{θ}. the finite field discrete time Fourier transform introduced in this work satisfies most properties of the usual DTFT defined over the complex field $\mathbb{C}$, such as linearity, time shift, scaling and so on.

Example 4 *The inverse FFDTFT of the plane spectrum $X(\varepsilon^{\theta}) = 1$ is*

$$x[n] = \frac{1}{2(p+1)} \sum_{\theta=0}^{2(p+1)-1} \varepsilon^{\theta n},$$

and, from lemma 1, follows $x[n] = \delta[n]$, as expected.

5   Redefining the Finite Field Fourier Transform

The Discrete Fourier Transform is a commonly used tool in Electrical Engineering. In a general setting, the DFT of a sequence $v = (v_i) \in \mathbb{E}$, is the sequence $V = (V_k) \in \mathbb{F}$ of elements

$$V_k \triangleq \sum_{i=0}^{N-1} v_i W^{ik}$$

where i, $k = 0$, 1,…, $N-1$ and W is an Nth root of unity in $\mathbb{F}$.

If $\mathbb{E}$ is the field $\mathbb{R}$ of real numbers and $\mathbb{F} = \mathbb{C}$ then, $W = (\exp -j2\pi/N)$ and we have the usual DFT. In this case the transformed vector is, in general, complex.

If $\mathbb{E} = \mathrm{GF}(p)$ and $\mathbb{F} = \mathrm{GF}(p^m)$, with $m \geq 1$, then $W = a$ is an element of multiplicative order N of $\mathrm{GF}(p^m)$. In this case, we have the Finite Field Fourier Transform. The FFFT definition with a kernel $W = a \in \mathrm{GF}(p^m)$, makes the transformation to be a *real* one.

10

For the above, a definition of the FFFT analogous to the usual DFT, should use a *complex* kernel. In this case, we have not only a more appropriate version of the FFFT, but also a greater flexibility in the transform length.

Definition 9 *Let $f = (f_0, f_1, \ldots, f_{N-1})$ be a vector of length N with components over $GF(q)$, where $q = p^r$. Then the vector $F = (F_0, F_1, \ldots, F_{N-1})$, with components over $GL(q^m)$ given by*

$$F_k = \sum_{i=0}^{N-1} f_i \zeta^{ki}$$

where ζ is an element of order N in $GL(q^m)$, is the Finite Field Fourier Transform of f.

This FFFT has the same properties as the one introduced by Pollard [2]. Indeed, the last one turns out to be a particular case of the definition 12, when $\zeta = a + jb$ and $b = 0$.

Proposition 6 *The Finite Field Fourier Transform in definition 9 has lengths N, which divide $q^{2m} - 1$.*

Proof: The transform has length N, given by the order of the element $\zeta \in GL(q^m)$. Since $|GL(q^m)| = q^{2m} - 1$, the result follows. ∎

Observe that, since $q^{2m} - 1 = (q^m - 1)(q^m + 1)$, new lengths which are divisors of $q^m + 1$ are now possible for the FFFT.

6   Final Remarks

This paper deals with discrete Fourier transforms defined over finite fields. Initially, some mathematical preliminaries were presented, which lead to the construction of *complex* numbers over a finite field. Afterwards, the problem of constructing finite field transforms capable to deal with infinite sequences defined over a Galois Field $GF(p)$, was approached. To deal with such sequences, the concept of "Cesàro convergence" was used, and it was shown that periodic sequences over $GF(p)$ converge to the arithmetic mean of the Cesàro sums of the sequence. As a direct consequence of this, a new transform, the discrete time Fourier transform over a finite field, was introduced and its inversion formula was presented.

The Fourier transform over a finite field was also considered and a new definition for it was proposed. This formulation, not only generalizes it, but better mimics DFT, since it contains a complex kernel. The new definition allows a greater flexibility in the choice of lengths to the transform.

The transforms here introduced are able to process finite and infinite sequences and, hence, are useful tools to work with FIR and IIR filters defined over finite algebraic structures.

References

[1] A. V. Oppenheim, R. W. Schafer e J. R. Buck, *Discrete-Time Signal Processing*, Prentice-Hall, 1999.

[2] J. M. Pollard, The Fast Fourier Transform in a Finite Field, Math. Comput., vol. 25, No. 114, pp. 365-374, Apr. 1971.

[3] R. M. Campello de Souza, H. M. de Oliveira and A. N. Kauffman, Trigonometry in Finite Fields and a New Hartley Transform, Proc. of the IEEE Int. Symp. on Info. Theory, p.293, Cambridge, MA, Aug. 1998.

[4] H. M. de Oliveira, R. M. Campello de Souza and A. N. Kauffman, Efficient Multiplex for Band-Limited Channels: Galois-Field Division Multiple Access, Proceedings of the 1999 Workshop on Coding and Cryptography - WCC '99, pp. 235-241, Paris, Jan. 1999.

[5] H. M. de Oliveira, R. M. Campello de Souza, Orthogonal Multilevel Spreading Sequence Design, in Coding, Communications and Broadcasting, pp. 291-303, Eds. P. Farrell, M. Darnell and B. Honary, Research Studies Press / John Wiley, 2000.

[6] T. Cooklev, A. Nishihara and M. Sablatash, Theory of Filter banks over Finite Fields, IEEE Asia Pacific Conference on Circuits and Systems, APCCAS'94, pp. 260-265, 1994.

[7] R. E. Blahut, *Fast Algorithms for Digital Signal Processing*, Addison Wesley, 1985.

[8] R. Lidl e H. Niederreiter, *Introduction to Finite Fields and their Applications*, Cambridge University press, 1986.

[9] D.M. Burton, *Elementary Number Theory*, McGraw-Hill, 1997.

[10] R. G. Bartle, *The Elements of Real Analysis*, John Wiley, 1967.