Cyclotomic Basis for Computing the Discrete Fourier Transform

G. Jerônimo da Silva Jr. and R. M. Campello de Souza
Department of Electronics and Systems
UFPE, CP7800, 50711-970
Recife PE, Brazil
e-mails: gilsonjr@gmail.com, ricardo@ufpe.br

***Abstract*— This paper presents a new fast algorithm for computing an N-point discrete Fourier transform. The algorithm meets the Heideman multiplicative complexity lower bound for $N = \{3, 4, 6, 8, 12\}$ and is based upon the decomposition of the elements of the transform matrix into a cyclotomic basis.**

***Keywords*— FFT; DFT; multiplicative complexity; cyclotomic basis.**

I. Introduction

Transforms are mathematical tools used in many applications of Engineering. A particularly important example is the continuous Fourier transform and its discrete version in the time and frequency domains, the discrete Fourier transform (DFT) [1], [2].

In practical application scenarios one is always looking for efficient ways, in terms of arithmetic complexity, to compute a DFT. This is a problem that fascinated many engineers and mathematicians for centuries [3] and its study has led to the development of well known fast Fourier transform (FFT) algorithms, such as the algorithms of Coley-Tukey, Good-Thomas and Winograd [4]-[6]. In [7] Heideman presented a minimum multiplicative complexity for computing an N-point DFT. Very few algorithms meet this minimum for some blocklengths and there is not a systematic way to derive them. This is the main motivation for the work reported in this paper, namely, to reach the minimum multiplicative complexity with a systematic and general algorithm.

The discrete Fourier transform of the sequence $v = (v_n)$, $n = 0, \dots, N-1$, is the sequence $V = (V_k)$, $k = 0, \dots, N-1$, defined by

$$V_k \triangleq \sum_{n=0}^{N-1} v_n W_N^{kn}, \tag{1}$$

where $W_N \triangleq e^{-j\frac{2\pi}{N}}$ is an element of order N in $\mathbb{C}$ and $j \triangleq \sqrt{-1}$. Expression (1) may be written in matrix form as

$$\mathbf{V} = \mathbf{W}\mathbf{v} \tag{2}$$

by defining

$$\mathbf{V} \triangleq \begin{bmatrix} V_0 \\ V_1 \\ \vdots \\ V_{N-1} \end{bmatrix}, \tag{3}$$

$$\mathbf{v} \triangleq \begin{bmatrix} v_0 \\ v_1 \\ \vdots \\ v_{N-1} \end{bmatrix}, \tag{4}$$

and

$$\mathbf{W} = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & W_N & \cdots & W_N^{N-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & W_N^{N-1} & \cdots & W_N^{(N-1)(N-1)} \end{bmatrix}. \tag{5}$$

Throughout the paper it is assumed that $\mathbf{v}$ is a real-valued sequence.

II. Cyclotomic Basis

The cyclotomic polynomial of order N over $\mathbb{C}$, denoted by $\Phi_N(x)$, is defined as the monic polynomial the roots of which are all elements of order N in the complex field. It can be written as

$$\Phi_N(x) = \prod_{\mathrm{ord}(\theta)=N} (x - \theta). \tag{6}$$

It can be shown, using the Möbius inversion formula [8], that

$$\Phi_N(x) = \prod_{d|N} (x^d - 1)^{\mu(N/d)}, \tag{7}$$

where $\mu(n)$ is the Möbius function [9]. The degree of $\Phi_N(x)$ is given by Euler's *totient function* $\phi(N)$, defined as the number of positive integers less than N and relatively prime to N. Cyclotomic polynomials have integer coefficients which, for N smaller than 105, are equal to 0, 1 or -1 [4].

Definition 1: A *cyclotomic basis* (CB_N) is a set in the complex field such that any element of a cyclic multiplicative group of order N (CMG_N) can be represented by a linear combination, with rational coefficients, of the elements of CB_N.

We can see that $\alpha = W_N$ is a root of $\Phi_N(x)$. Therefore, from equation $\Phi(\alpha) = 0$, we can write all elements of $CMG_N = \{\alpha^0, \dots, \alpha^{N-1}\}$ as linear combination, with integer coefficients, of the elements $\{1, \alpha, \alpha^2, \dots, \alpha^{\phi(N)-1}\}$. This motivates the following definition.

Definition 2: A *canonical cyclotomic basis* (CCB) is the cyclotomic basis formed by $CCB_N = \{1, \alpha, \alpha^2, \ldots, \alpha^{\phi(N)-1}\}$ relative to CMG_N, where α is a generator of CMG_N.

Example 1: For $N = 6$, $\alpha = W_6$ is a root of $\Phi_6(x) = x^2 - x + 1$, or $\Phi(\alpha) = \alpha^2 - \alpha + 1 = 0$. The set $CCB_6 = \{1, \alpha\}$ is a canonical cyclotomic basis of the multiplicative group $CMG_6 = \{1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5\}$. The representation of the elements of CMG_6 as a linear combination of $\{1, \alpha\}$ is

$$\begin{array}{ll} \alpha^0 = 1 & \alpha^3 = -1 \\ \alpha^1 = \alpha & \alpha^4 = -\alpha \\ \alpha^2 = -1+\alpha & \alpha^5 = 1-\alpha, \end{array}$$

or simply

$$\begin{bmatrix} \alpha^0 \\ \alpha^1 \\ \alpha^2 \\ \alpha^3 \\ \alpha^4 \\ \alpha^5 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ -1 & 1 \\ -1 & 0 \\ 0 & -1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} \alpha^0 \\ \alpha^1 \end{bmatrix}.$$

$CB_6 = \{1, \alpha^5\}$ is another canonical basis for CMG_6.

In general we can write, for all CMG_N,

$$\begin{bmatrix} \alpha^0 \\ \vdots \\ \alpha^{N-1} \end{bmatrix} = R_c \begin{bmatrix} \alpha^0 \\ \vdots \\ \alpha^{\phi(N)-1} \end{bmatrix}, \tag{8}$$

where $\alpha = W_N$ and $R_c(N \text{ x } \Phi(N))$ is said to be the *rectangular canonical matrix*, the elements of which are integers. This is always possible if we write $\alpha^n = \alpha^n (mod\ \Phi_N(\alpha))$, for all $n = 0, 1, \ldots, N-1$.

We can make a basis change to represent a CMG_N under another CB_N. To do this, simply express the elements of the new basis as

$$\begin{bmatrix} \alpha^{i_1} \\ \vdots \\ \alpha^{i_{\phi(N)}} \end{bmatrix} = Q \begin{bmatrix} \alpha^0 \\ \vdots \\ \alpha^{\phi(N)-1} \end{bmatrix}, \tag{9}$$

where the nth row of Q is the i_nth row of R_c for all $n = 1, \ldots, \phi(N)$. Q is a square matrix and if it is nonsingular, then

$$\begin{bmatrix} \alpha^0 \\ \vdots \\ \alpha^{\phi(N)-1} \end{bmatrix} = Q^{-1} \begin{bmatrix} \alpha^{i_1} \\ \vdots \\ \alpha^{i_{\phi(N)}} \end{bmatrix} \tag{10}$$

and a CMG_N can be expressed by the new basis

$$\begin{bmatrix} \alpha^0 \\ \vdots \\ \alpha^{N-1} \end{bmatrix} = R_c Q^{-1} \begin{bmatrix} \alpha^{i_1} \\ \vdots \\ \alpha^{i_{\phi(N)}} \end{bmatrix}, \tag{11}$$

where $R = R_c Q^{-1}$ is a general rectangular decomposition matrix. Therefore, we can decompose a CMG_N into any cyclotomic basis, $CB_N = \{\alpha^{i_1}, \ldots, \alpha^{i_{\phi(N)}}\}$, provided Q has an inverse. The following example illustrates this point.

Example 2: For $N = 8$ we have, from (7), $\Phi_8(x) = 1 + x^4$. Computing the rectangular canonical matrix R_c(8x4) we obtain the following decomposition using $CCB_8 = \{1, \alpha, \alpha^2, \alpha^3\}$,

$$\begin{bmatrix} \alpha^0 \\ \alpha^1 \\ \alpha^2 \\ \alpha^3 \\ \alpha^4 \\ \alpha^5 \\ \alpha^6 \\ \alpha^7 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix} \begin{bmatrix} 1 \\ \alpha \\ \alpha^2 \\ \alpha^3 \end{bmatrix}.$$

We can make a basis change to represent CMG_8 upon a new cyclotomic basis $CB_8 = \{1, \alpha^6, \alpha, \alpha^7\}$. Using the R_c matrix, we can write

$$\begin{bmatrix} 1 \\ j \\ \alpha \\ \alpha^* \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix} \begin{bmatrix} 1 \\ \alpha \\ \alpha^2 \\ \alpha^3 \end{bmatrix},$$

where α^* denotes the complex conjugate of α. Since the matrix Q is invertible, the decomposition matrix is $R = R_c Q^{-1}$, leading to

$$\begin{bmatrix} \alpha^0 \\ \alpha^1 \\ \alpha^2 \\ \alpha^3 \\ \alpha^4 \\ \alpha^5 \\ \alpha^6 \\ \alpha^7 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ j \\ \alpha \\ \alpha^* \end{bmatrix}.$$

It is also possible to choose an appropriate CB_N so as to separate the real and imaginary parts, as shown in the next example.

Example 3: For $N = 6$, we can take as a cyclotomic basis the set $\{1/2, (\alpha - \alpha^5)/2\}$ and, using the matrix R_c from Example 1, it is possible to write

$$\begin{bmatrix} 1/2 \\ (\alpha^1 - \alpha^5)/2 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1 & 0 \\ -1 & 2 \end{bmatrix} \begin{bmatrix} \alpha^0 \\ \alpha^1 \end{bmatrix}.$$

Computing $R_c Q^{-1}$ yields

$$\begin{bmatrix} 1 \\ \alpha^1 \\ \alpha^2 \\ \alpha^3 \\ \alpha^4 \\ \alpha^5 \end{bmatrix} = \begin{bmatrix} 2 & 0 \\ 1 & 1 \\ -1 & 1 \\ -2 & 0 \\ -1 & -1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 1/2 \\ (\alpha-\alpha^5)/2 \end{bmatrix}$$

and it is clear that $(\alpha-\alpha^5)/2 = j\text{Im}(\alpha)$, where Im(.) denotes the imaginary part of the argument.

This example inspires two new definitions.

Definition 3: A *sine and cosine cyclotomic basis* (sin/cos-CB) is the basis, with $\phi(N)$ elements, $CB_N = \{1, (\alpha-\alpha^{N-1})/2, (\alpha+\alpha^{N-1})/2, (\alpha^2-\alpha^{N-2})/2, \ldots\}$, or simply $CB_N = \{1, j\text{Im}(\alpha), \text{Re}(\alpha), j\text{Im}(\alpha^2), \ldots\}$.

Definition 4: A *cosine cyclotomic basis* (cos-CB) is the basis, with $\phi(N)$ elements, $N \equiv 0 \pmod 4$, $CB_N = \{1, \alpha^{N/4}, (\alpha+\alpha^{N-1})/2, (\alpha^{1+N/4}+\alpha^{N/4-1})/2, \ldots\}$, or simply $CB_N = \{1, -j, \text{Re}(\alpha), j\text{Re}(\alpha), \text{Re}(\alpha^2), j\text{Re}(\alpha^2), \ldots\}$.

The advantage of choosing a sin/cos-CB or a cos-CB is that the basis are purely real or imaginary. In this case we have

$$\begin{bmatrix} \alpha^0 \\ \vdots \\ \alpha^{N-1} \end{bmatrix} = R \begin{bmatrix} \gamma_1 \\ \vdots \\ \gamma_{\phi(N)} \end{bmatrix}, \tag{12}$$

where R is a general rectangular decomposition matrix with integer elements (depending on the basis choice), and $\gamma_1, \gamma_2, \ldots, \gamma_{\phi(N)}$ is the cyclotomic basis formed from purely real or imaginary constants. If r_{ij}, $i = 0, 1, \ldots, N-1$, $j = 1, \ldots, \phi(N)$, denotes the elements of R, then

$$\alpha^i = \sum_{j=1}^{\phi(N)} r_{ij}\gamma_j. \tag{13}$$

Equation (13) characterizes decompositions over cyclotomic basis. If $N \equiv 0 \pmod 4$ a cos-CB can be used and $\{1, -j\} \in CB_N$. Otherwise, a sine/cos-CB can be used and only $\{1\} \in CB_N$.

III. A New Fast Fourier Transform Algorithm

The algorithm is constructed by decomposing the DFT matrix W over a cyclotomic basis. Equation (2) can be rewritten as

$$\mathbf{V} = \underbrace{\begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & \alpha & \cdots & \alpha^{N-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{N-1} & \cdots & \alpha^{(N-1)(N-1)} \end{bmatrix}}_{\text{decompose in } CB_N} \mathbf{v}, \tag{14}$$

where $\alpha = W_N$. Therefore, it becomes

$$\mathbf{V} = (\gamma_1 A_1 + \gamma_2 A_2 + \ldots + \gamma_{\phi(N)} A_{\phi(N)})\mathbf{v}, \tag{15}$$

or

$$\mathbf{V} = \sum_{i=1}^{\phi(N)} \gamma_i A_i \mathbf{v}, \tag{16}$$

where the elements of the matrices A_i are rational numbers. In most cases, these are small integers.

Apparently, there is not a significant improvement in the multiplicative complexity for computing V, since it is related to the products $\gamma_i A_i \mathbf{v}$. However, these products can be made in a very effective way.

Theorem 1: Let γ be a purely real or imaginary constant, A an integer matrix and $\mathbf{v}$ a vector of variables. The computation of $\mathbf{s} = \gamma A\mathbf{v}$ requires rank(A) real multiplications.

Proof: With $l = \text{rank}(A)$, there are l linearly independent rows of A, namely $r_1, r_2, \ldots, r_l$. There are l real multiplications

$$s_{j_i} = \gamma(r_i\mathbf{v}), \tag{17}$$

for each $i = 1, 2, \ldots, l$, and all other rows can be expressed by

$$r_m = \sum_{i=1}^{l} b_{mi} r_i, \tag{18}$$

where $b_{mi} \in \mathbb{Q}$. Therefore, any component s_m can be computed by

$$s_m = \gamma(r_m\mathbf{v}), \tag{19}$$

$$s_m = \gamma \sum_{i=1}^{l} b_{mi} r_i \mathbf{v}, \tag{20}$$

$$s_m = \sum_{i=1}^{l} b_{mi}(\gamma r_i \mathbf{v}), \tag{21}$$

$$s_m = \sum_{i=1}^{l} b_{mi} s_{j_i}, \tag{22}$$

where multiplications by b_{mi} are considered trivial, and all s_m can be computed by trivial combinations of l multiplications. ■

Using Theorem 1 and (16), the multiplicative complexity, M_r, is given by

$$M_r = \sum_{i=2}^{\phi(N)} \text{rank}(A_i), \tag{23}$$

since that $\gamma_1 = 1$ (trivial multiplication). If cos-CB is used, $\gamma_2 = j$, and

$$M_r = \sum_{i=1}^{\phi(N)/2-1} \text{rank}\left(\begin{bmatrix} A_{2i+1} \\ A_{2(i+1)} \end{bmatrix}\right), \tag{24}$$

since that $\gamma_{2(i+1)} = -j\gamma_{2i+1}$ in this basis.

Example 4: We start with the simplest nontrivial example, the 3-point DFT. To find the decomposition based on the sin/cos-CB, we use the procedure describe in section II, which results in the expression

$$\begin{bmatrix} \alpha^0 \\ \alpha^1 \\ \alpha^2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ -0.5 & 1 \\ -0.5 & -1 \end{bmatrix} \begin{bmatrix} 1 \\ -j\sin(2\pi/3) \end{bmatrix}.$$

Applying it to the 3x3 DFT matrix yields

$$\mathbf{W} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & -0.5 & -0.5 \\ 1 & -0.5 & -0.5 \end{bmatrix} -j\sin(2\pi/3) \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & -1 \\ 0 & -1 & 1 \end{bmatrix}.$$

Considering the array $\mathbf{L}$ of all linearly independent rows of A_1 and A_2, we have

$$\mathbf{S} = \mathbf{L}\mathbf{v} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & -0.5 & -0.5 \\ 0 & 1 & -1 \end{bmatrix} \begin{bmatrix} v_0 \\ v_1 \\ v_2 \end{bmatrix} = \begin{bmatrix} S_0 \\ S_1 \\ S_2 \end{bmatrix}.$$

Since that $\mathbf{V} = \mathbf{W}\mathbf{v}$, defining

$$m_1 = -j\sin(2\pi/3)S_2,$$

we may write

$$\mathbf{V} = \begin{bmatrix} S_0 \\ S_1 + m_1 \\ S_1 - m_1 \end{bmatrix}.$$

Therefore, the matrix $\mathbf{W}$ can be expressed as

$$\mathbf{W} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & -1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \gamma_2 \end{bmatrix} \begin{bmatrix} 1 & 1 & 1 \\ 1 & -0.5 & -0.5 \\ 0 & 1 & -1 \end{bmatrix}.$$

This algorithm implements the 3-point DFT with the minimum number of multiplications, a better performance than the Winograd algorithm, which implements it with two multiplications [6].

Example 5: We derive the 8-point FFT algorithm using the same procedure as in the previous example. In this case the cos-CB is used,

$$\begin{bmatrix} \alpha^0 \\ \alpha^1 \\ \alpha^2 \\ \alpha^3 \\ \alpha^4 \\ \alpha^5 \\ \alpha^6 \\ \alpha^7 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 1 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & -1 & -1 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & -1 \end{bmatrix} \begin{bmatrix} 1 \\ -j \\ \frac{\sqrt{2}}{2} \\ -j\frac{\sqrt{2}}{2} \end{bmatrix}.$$

Using it to decompose the 8-point DFT matrix, leads to

$$\mathbf{W} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 1 & 0 & -1 & 0 & 1 & 0 & -1 & 0 \\ 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 1 & 0 & -1 & 0 & 1 & 0 & -1 & 0 \\ 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \end{bmatrix}
-j \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 & 0 & 1 & 0 & -1 \\ 0 & 0 & -1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & -1 & 0 \\ 0 & -1 & 0 & 1 & 0 & -1 & 0 & 1 \\ 0 & 0 & -1 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}
+\frac{\sqrt{2}}{2} \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & -1 & 0 & -1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 1 & 0 & 1 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 1 & 0 & 1 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & -1 & 0 & -1 & 0 & 1 \end{bmatrix}
-j\frac{\sqrt{2}}{2} \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & -1 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & -1 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & -1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & -1 & 0 & 1 & 0 & 1 \end{bmatrix}.$$

The algorithm is obtained from (16). As in example 4, we use the array of all linearly independent rows of all matrices A_i to write

$$\mathbf{S} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 1 & 0 & -1 & 0 & 1 & 0 & -1 & 0 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 0 & 0 & 1 & 0 & 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 & 0 & 1 & 0 & -1 \\ 0 & 1 & 0 & -1 & 0 & -1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & -1 & 0 & -1 \end{bmatrix} \mathbf{v},$$

$$\mathbf{S} = \begin{bmatrix} S_0 \\ S_1 \\ S_2 \\ S_3 \\ S_4 \\ S_5 \\ S_6 \\ S_7 \end{bmatrix}.$$

Let

$$m_1 = \frac{\sqrt{2}}{2} S_4,$$

and

$$m_2 = -j\frac{\sqrt{2}}{2} S_5.$$

The DFT is computed by

$$\mathbf{V} = \begin{bmatrix} S_0 \\ S_1 - jS_4 + m_1 + m_2 \\ S_2 - jS_5 \\ S_1 + jS_4 - m_1 + m_2 \\ S_3 \\ S_1 - jS_4 + m_1 - m_2 \\ S_2 + jS_5 \\ S_1 + jS_4 - m_1 - m_2 \end{bmatrix},$$

or

$$\mathbf{V} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & -j & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & -j & 0 & 0 \\ 0 & 1 & 0 & 0 & j & 0 & -1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & -j & 0 & 1 & -1 \\ 0 & 0 & 1 & 0 & 0 & j & 0 & 0 \\ 0 & 1 & 0 & 0 & j & 0 & -1 & -1 \end{bmatrix} \begin{bmatrix} S_0 \\ S_1 \\ S_2 \\ S_3 \\ S_4 \\ S_5 \\ m_1 \\ m_2 \end{bmatrix}$$

Table I shows the multiplicative complexity, for several values of N, of the FFT proposed in this paper and that of some well known algorithms. The Heideman lower bound is also indicated on the table.

It can be observed in Table I, that the CBD-FFT has the minimum number of multiplications for $N = 3, 4, 6, 8, 12$. The algorithm also presents a better performance than the classical Coley-Tukey and Good-Thomas algorithms for most small values of N up to 96.

IV. Conclusions

A new algebraic approach, called cyclotomic basis decomposition, was introduced and used as a tool to provide good algorithms, in terms of multiplicative complexity, for computing the discrete Fourier transform. The FFT based on this new approach presents a better performance than standard FFT algorithms known in the literature, for various blocklengths.

TABLE I
Real multiplicative complexity of: CBD - cyclotomic basis decomposition FFT; HLB - Heideman lower bound; CT/GT - Combination of the two most popular FFT algorithms, fully optimized, the Cooley-Tukey and Good-Thomas algorithms; SW-FFT - Small Winograd FFT.

N	(CBD-FFT)	(HLB)	(CT/GT)	(SW-FFT)
3	1	1	8	2
4	0	0	0	0
5	5	4	32	5
6	2	2	16	-
7	13	7	72	8
8	2	2	4	2
9	10	8	60	10
10	10	8	64	-
12	4	4	32	-
16	12	10	20	10
20	20	16	128	-
24	14	12	108	-
32	54	32	88	-
48	64	38	252	-
64	224	84	208	-
96	258	105	648	-

Acknowledgements

The authors are grateful to Dr. Hélio M. de Oliveira for his valuable suggestions to this work. The first author was partially funded by CNPq.

References

[1] A. V. Oppenheim, A. S. Willsky, and S. H. Nawab, *Signals and Systems*, 2nd ed. Prentice Hall, 1996.
[2] A. V. Oppenheim, R. W. Schafer, and J. R. Buck, *Discrete-Time Signal Processing*, 3rd ed. Prentice Hall, 2009.
[3] M. Heideman, D. Johnson, and C. Burrus, "Gauss and the history of the fast fourier transform," *ASSP Magazine, IEEE*, vol. 1, no. 4, pp. 14–21, Oct 1984.
[4] R. E. Blahut, *Fast Algorithms for Digital Signal Processing*. Addison-Wesley Publishing Company, 1984.
[5] J. W. Cooley and J. W. Tukey, "An algorithm for the machine calculation of complex Fourier series," *Mathematics of Computation*, vol. 19, no. 90, pp. 297–301, 1965.
[6] S. Winograd, "On computing the discrete Fourier transform," *Mathematics of Computation*, vol. 32, no. 141, pp. 175–199, Jan 1978.
[7] M. T. Heideman, *Multiplicative Complexity, Convolution, and the DFT*, 2nd ed. Springer-Verlag, 1988.
[8] R. J. McEliece, *Finite Fields for Computer Scientists and Engineers*. Kluwer Academic Publishers, 1987.
[9] D. M. Burton, *Elementary Number Theory*, 6th ed. McGraw-Hill, 2007.