Becoming of Discrete Harmonic Transform Using Cyclic Convolutions

Ihor Prots’ko1, *, Roman Rykmas2

1Department of Civil Security, Lviv State University of Life Safety, Lviv, Ukraine
2LtdC “Uniservice”, Lviv, Ukraine

Abstract
The enumeration approaches of efficient computation discrete transform of Fourier class using cyclic convolutions is considered. The formulation of the basis matrix of transforms into the block cyclic structures is described of each approach. The analysis of the advantages and imperfections of the algorithms are discussed.

Keywords
Discrete Transform of Fourier Class, Cyclic Convolution, Efficient Algorithms

1. Introduction
The using of efficient algorithms for solving calculation tasks existed to the era of the spread of computers. Methods of Runge (1905), Danielson - Lanczos (1942), Levinson (1947) have been known for use in highly specialized areas, and did not become the fundamental works on efficient algorithms for harmonic and spectral analysis [1,2]. They are ahead of their time, though efficient algorithms for spectral estimation would were advantageous over the last hundred years. The catalyst of intensive research and development of fast computational algorithms was discrete transform of Fourier class and digital convolution based computer systems in various application areas.

Algorithm Cooley-Tukey [3] of the effective computation of discrete Fourier transform (DFT) has become a significant milestone the beginning of the intensive development of signal processing and fast computing. Only for a few years it became clear that another very different from the algorithm Cooley-Tukey (1965) was developed independently Good (1958) [4] and Thomas (1963) [5]. The existence of more efficient algorithms with computational point of comparison with the algorithm of Cooley-Tukey showed Yavne (1968) [6]. Building on experience in the field of efficient algorithms S. Winograd (1978) [7] published a more effective but also more complex algorithm for DFT, which reduced the number of multiplications, compared with the algorithm of Cooley-Tukey on the base of two, to near five times.

The profound theoretical study of the systems of orthogonal basises have led to the creation of the theory of generalized spectral analysis in the late 70's. It allowed not only to reevaluate the value of the classical Fourier analysis and the possibility of its practical application, but create a synthesis methods of real basises of Fourier class for the most effective solutions of practical problems [8, 9].

Discrete transforms and convolutions are the main operations and key tools in Signal Processing. Especially widely used are discrete Fourier transform, discrete Hartley transform, discrete cosine transform, discrete sine transform – common named discrete harmonic transforms (DHT) presenting signals in frequency domain. The discrete convolutions (linear, circular, field) find important applications in various aspects in the time-domain. The paradox looks the having connection in frequency-domain and time-domain, not only in physical but and in computational applications. There are

* Corresponding author
E-mail address: protsko@polynet.lviv.ua (I. Prots’ko), roman.rikmas@gmail.com (R. Rykmas)
many different ways to compute convolutions, more widely used the transformations of both data to the frequency domain on basis the efficient discrete transforms of Fourier class, then used the pointwise multiply and transformations back to the time domain (theorem of convolution).

A significant event associated with another trend of development the efficient algorithms, which is marked in many editions of digital signal processing, it is possibility computation of FFT through cyclic convolutions [10]. Pioneering in this area is considered to be the strategy proposed C.M. Rader of the possibility of effective computation of DFT via cyclic convolution. Various ways of implementation this strategy were proposed by Goertzel, Bluestein, Winograd and named in their honor. Along with researches on FFT developed the approaches of effective computation DFT may imply computation of direct digital convolution, called fast computation of discrete transform on Fourier class using cyclic convolutions. Therefore the significant potential of effective computation of Fourier transforms, algorithm of partitioning convolution, a method of efficient computation discrete convolutions had accumulated.

This paper is organized as follows. In two section is reviewed the famous and new approaches to the synthesis of efficient algorithm based on the cyclic convolutions. In conclusions is considered a short enumeration the advantages and imperfections of approaches of efficient computation discrete transform of Fourier class using cyclic convolutions.

2. The Approaches of Computation DHT Using Cyclic Convolutions

Between of variety the algorithms, leading to efficient computations of DHT, have the historical development of fast algorithms using cyclic convolutions. To enumerate the famous approaches of efficient computation DFT on the basis of cyclic convolutions:

- for transform size N is a prime, the DFT is trivially are computed the remaining (N-1) components using an efficient cyclic convolution algorithm presented by Rader (1968) [10];
- for arbitrary transform size, individual discrete components DFT are computed using a cyclic convolution algorithm presented by Goertzel (1968) [12];
- for arbitrary transform size, chirp-algorithm define DFT via cyclic-convolution and additional multiplications presented by Bluestein (1970) [13];
- for transform the size is the integer power of prime, presented by Winograd Fourier Transform Algorithm (1978) [7].

2.1. Rader Algorithm

In first the convolutional formulation DFT is considered the publication of the Raiders [10]. Discrete Fourier transform of the basis W reduced to computing cyclic convolution sequence for the sizes equal to the prime number N. The DFT of prime length N defined as:

\[
X(n) = \sum_{k=0}^{N-1} x(k)W_n^{nk}
\]

where \( n, k = 0, 1, ..., N-1 \). Formulate of the cyclic convolution through reindexing input sequence \( x(k) \) applying for this primitive root \( g \) of the corresponding exponent. That can express (1.1) in a form:

\[
X(g^k) = \sum_{k=1}^{N-1} x(g^{-k})W_N^{nk} + x(0)
\]

which correspond cyclic convolution without the inclusion \( x(0) \). Number \( g \) corresponds to the primitive root, not necessarily the one, with the properties of \( g^{N-1} = g^0 = 1 \), \( g^k \neq 1 \), for \( 0 < k < N-1 \) and take into account that

\[
W_n^N = W_n^{(nk)modN} = W_n^{gnk} = W_n^{g^k}, W_n^1 = 1.
\]

Raiders algorithm can be used to compute the DFT of prime size \( N \) of any algebraic field. The primitive root \( g \) use in the structure of this field for indexing input sequence and the transition to a cyclic convolution.

2.2. Goertzel Algorithm

At the same time the work Goertzel [12] was appeared and devoted the computation of the individual values of DFT using convolution operation. Goertzel algorithm does not belong to the FFT, as its complexity is proportional to \( N^2 \). Since FFT algorithms compute all the components of the transformation, Goertzel algorithm can be used when it is necessary to determine the number of initial components no most \( \log_2 N \) with N components.

According Goertzel algorithm computing \( X(k) \), for \( k = 0, 1, ..., N-1 \), where \( N \)-point sequence \( x(n) \) is performed as follows. For each value of \( k \) to determine \( X(k) \), \( N \)-point sequence \( X(k) \) appears at the output of the system for which \( x(n) \) input sequence, and \( W_N^{nk} \) is the impulse response of the system, then the adoption of \( n = N \),
According Goertzel algorithm the computation $X(k)$, for $k = 0, 1, ..., N-1$, where N-point sequence $x(n)$ is performed as follows. For each value of $k$ to determine $X(k)$, N-point sequence $X(k)$ appears at the output of the system for which $x(n)$ is input sequence, and $W_N^{-nk}$ is the impulse response of the system, then the adoption of $n = N$

$$X(k) = y_d(n) \big|_{n=N},$$

$$y_i(n) = \sum_{q=1}^{N-1} x(q) W_N^{-x(n-q)}$$  (4)

Thus, $y_d(n)$ is defined as the convolution of a given sequence $x(n)$ and $W_N^{-nk}$, and $X(k)$ then simply obtained taking into $y_d(n)$ values of $n$ equal to $N$.

### 2.3. Bluestein Chirp-Algorithm

In the work Bluestein [13] is showed, that computation DFT can be reduced to perform of convolutions. Describe the main algorithm

$$X(e^{j\phi_k}) = \sum_{n=0}^{N-1} x(n) e^{-j\phi_k n},$$  (5)

where $\phi_k = \phi_0 + k\phi, \Delta \phi = 2\pi/N$.

Denote $e^{-j\Delta \phi} = W$, then for $\phi_k$ can find that

$$X(e^{j\phi_k}) = \sum_{n=0}^{N-1} x(n) e^{-j\phi_k n} W^{-nk}.$$  (6)

Instead the power $W$ define as $nk = (1/2) [n^2 - k^2 - (k-n)^2]$

$$X(e^{j\phi_k}) = \sum_{n=0}^{N-1} x(n) e^{-j\phi_k n} W^{n^2/2} W^{-x(n-k)^2/2}. $$  (7)

Denote that

$$z(n) = e^{-j\phi_k n} W^{x(n)^2/2}, $$  (8)

then

$$X(e^{j\phi_k}) = W^{x(n)^2/2} \sum_{n=0}^{N-1} z(n) W^{-x(n-k)^2/2}.$$  (9)

Accordance the expression:

$$\sum_{n=0}^{N-1} z(n) W^{-(n-k)^2/2} = 1$$  (10)

corresponds the definition of convolution.

This chirp-algorithm transforms DFT of size N to N-point circular convolution and 2N additional products. The algorithm contains N multiplications, cyclic convolution and the following N point multiplication. From the computational point of view algorithm Bluestein do not match the efficiency. Nevertheless chirp-algorithm in certain applications it has a simpler hardware implementation.

### 2.4. Winograd Algorithms of DFT

Further development of FFT algorithms and efficient algorithms for cyclic convolution are considered in publications S. Winograd. After 10 years, developing the approach of Good-Thomas, Winograd [7] published a more efficient, but also much more complex algorithm that reduces the computation of DFT through computing of the short convolutions (with the number of multiplications 5 times less than the algorithm of Cooley-Tukey).

Publications Winograd further develop Raiders approach of effective computation of DFT through cyclic convolution for sequences of a prime and power of a prime number [14]. S. Winograd has derived formula for computational complexity of DFT with minimum multiplicative component. Winograd algorithms used for data reindexing the specific reordering based on Chinese remainder theorem, the properties of the direct product of matrices and cyclic convolution algorithms. Winograd FFT is designed for efficient computation of DFT of small sizes using for reduce the computation of cyclic convolutions the modular arithmetic in the ring of polynomials.

In the case of equal the size of transform DFT the power of prime $N = p^r$, according the algorithm Winograd, first from the set \{1,2,3,4,...,p^r - 1\} separate numbers of multiple of N. This subset is reduced to a cyclic convolution of size $(p^r-1)(p-1)$, which forms the basis of the algorithm. Branches $(p^r-1)$ rows and columns can be computed by the algorithm Winograd to convolution of less size. For example, $N = 3^2 = 9$, separates the grouping numbers 0,3,6, is the basis of the 6-point convolution and four 2-point convolutions. Thus, the transform of sizes $N = p^r$, can be computed using one cyclic convolution of $p^{r-1}(p-1)$-point, two of $p^{r-2}(p-1)$-point, four of $p^{r-3}(p-1)$, ..., $2^{r-1}$ convolution of $(p-1)$-point.

In the case, the size of transform DFT the power of prime $N = p^r$, according the algorithm Winograd, first to separate from the set \{1,2,3,4,...,p^r - 1\} numbers of multiple of N. This subset is reduced to a cyclic convolution of size $(p^r-1)(p-1)$, which forms a part of the basis of the algorithm. The subarray of $(p^r-1)$ rows and columns can be computed by the algorithm Winograd to convolution of less size. For example, $N = 3^2 = 9$, separates the grouping numbers 0,3,6, is the basis of transform of the 6-point convolution and four 2-point convolutions. Thus, the transform of sizes $N = p^r$, can be computed using one cyclic convolution of $p^{r-1}(p-1)$-point, two of $p^{r-2}(p-1)$-point, four of $p^{r-3}(p-1)$, ..., $2^{r-1}$ convolution of $(p-1)$-point.

In the case, the transform of sizes of $N = N_1 x N_2 x ... x N_k$,
where $N_i$ mutually prime numbers, Winograd algorithm are based on matrix representation of the sizes $N$ in the form of a direct product $\otimes$ of matrices $N_i$. $p$-point DFT

$$W_N \equiv W_0 = W_{N_1} \otimes W_{N_2} \otimes \ldots \otimes W_{N_k},$$

(11)

and reduce the computation to $N$ point cyclic convolutions using modular arithmetic in the ring of polynomials. The rule reindexing of information data based on the Chinese remainder theorem.

However, these algorithms have their own specific features for each size of $N$ associated with reindexing input sequence and consequently obtained some irregular structures. Therefore, these algorithms are researched and updated by many authors [15, 16].

### 3. The Further Approaches of Computation DHT Using Cyclic Convolutions

The efficient cyclic convolutions will lead to efficient computations of DHT. These algorithms present in the various forms and based the properly rearranging the basic matrix are leaded to pseudo/quasi cyclic structures. The techniques can reform the size of transform to different set of the less sizes the cyclic structures. The paper [17] shows that when the length of a $p$ prime is such that $(p-1)/2$ is odd, the DCT can be computed as two cyclic convolutions, each of length $(p-1)/2$. The paper [18] proposes to decompose the computation of the $N$ point DCT into two matrix-vector multiplications, where each matrix is of size $(M-1) \times (M-1)$ and $M = N/2$. Each of the decomposed matrix-vector products is then converted into a pair of $[(M-1)/2]$ point circular convolution-like operations for reduced-complexity of concurrent systolization.

Modern computation of discrete transform of Fourier class the signals are used the generalized scheme of efficient algorithms. For many well-known fast algorithms are applied purely algebraic methods. The mathematical principles establish by the each algorithm, and justified its structure. Synthesis of fast algorithms often use a direct method based on the properties of the base matrix of transform and indirectly method, which involved other fast algorithms of discrete transform [19].

There are other general approaches to the theoretical basis of the possibility the cyclic formulation of discrete harmonic transforms.

### 3.1. Chan-Siu Algorithm

The strategy of cyclic or skew-cyclic structures identification within the transform matrix is investigated in many papers. A general solution is proposed to realize the discrete cosine transform of any length via cyclic convolutions in paper [20]. The algorithm of the discrete cosine transform (DCT/IDCT) with any length $N$ is formulated by using two $N$-length linear convolutions or two cyclic convolutions form, such that one can easily implement with technologies that are well suited for doing convolutions.

In such case, are made some modifications, such that we can make use of cyclic convolutions

$$Y(k) = [2T(k) + x(0) \cos(k\pi/2N)],$$

(12)

$$T(k) = 1/2 \left[ H(k) + H(2N-k) + G(k) + G(2N-k) \right] \sec(k^2\pi/2N),$$

(13)

where $k=0,1,\ldots,N-1$. For items of the sequence $\{T(k)\}$, we can first compute two sequences, $\{H(k)+H(2N-k)\}$ and $\{G(k)+G(2N-k)\}$ and both are in cyclic convolution form.

This is an efficient and effective approach as it can avoid complicated data routing and data management. This algorithm is not optimal in minimizing any measure of computational complexity, but it involves some regular forms that are most suitable for the realization using technologies and structures which are well suited for doing convolutions. On the other hand, this algorithm is much more flexible than any available DCT algorithm as it can be applied to realize DCT/IDCT with any length.

### 3.2. Wagh Algorithm

In paper [21] is considered a generalized algorithm which consists of partitioning the DCT kernel into submatrices which through the proper rows and columns shuffling and negations can be made equivalent to the group tables (or parts of them) of appropriate Abelian groups.

Paper defines a generalized convolution with respect to an Abelian group $G$. Index the sequences $u$ and $v$ by the elements of $G$. Then their convolved sequence $w$ is given by

$$w(h) = \sum g u(g) \cdot v(n \cdot g)$$

(14)

That this convolution with respect to $G \equiv C_{n_1} \times C_{n_2} \times \ldots \times C_{n_r}$ can be computed through $W = U \ast V$ where $U$, $V$, and $W$ are $r$-dimensional arrays and $\ast$ denotes an $r$-dimensional cyclic convolution.

The computations pertaining to the submatrices can be carried out using multidimensional cyclic convolutions. In other words, the work of the algorithm is based on the Abelian group of positive integers relatively prime to $N$ or less $N$ with the multiplication taking modulo $N$. The group and group operation is defined as $A (N, *)$. This paper prove
Theorem 1, which corresponds to the general computation of DCT through cyclic convolutions of sequences formed by a accordance rule. However, the formation of cyclic submatrices in the structure of the base kernel transformation is complicated of a significant number of reindexing elements what respectively define the complexity of the synthesis of computational algorithm.

3.3. General DHT Algorithm Using Cyclic Convolution

In [22, 23] are considered the general technique for efficient computation of discrete harmonic transform of sequences of arbitrary number of points using cyclic convolutions. The formed hashing arrays in algorithm define partitioning of the harmonic basis into the submatrices which can be made through shuffling of the rows and columns. The hashing arrays, used in the algorithms of synthesis, are more versatile and generally better in terms of indexing mapping in comparison with the existing algorithms. The algebraic system \(<N-1,*\>\) with operation on set \(\{1,2,...,N-1\}\) corresponds to equivalent basis matrix of discrete harmonic transform. In case the size of transform \(N\) is prime, algebraic system \(<N-1,*\>\) is of Abel group. Besides, the algebraic system \(<N-1,*\>\) with prime \(N\) presents cyclic group, and table of operation of algebraic system is a Hankel circular matrix. Elements of cyclic group are equal to natural power of generate element \(\alpha \in \mathbb{G}\). The generate element \(\alpha\) of cyclic group is a primitive root, and \(\alpha\) is not the only one. Primitive element will be \(\alpha^{N-1}\) also. Therefore, all elements of cyclic group can be determined by the powers of primitive element. Non-primitive elements of cyclic group generate a part of set, and the other part of set is formed by multiplication of two elements by modulo \(N\). Let us analyze Hankel matrix of arguments of degree \((N\times N)\) as substitution of \(\pi_i\) for each row (column) \(a_i, i \in \{1,2,...,x\}\) to first row (columns) of matrix, where \(N\) is prime. The summation of substitutions \(\{\psi_1, \psi_2, \psi_3, \psi_4, \psi_5,..., \psi_x\}\) with operation form cyclic group. The quantity of generating and non-primitive elements is the same for substitutions and algebraic system \(<N-1,*\>\) with the operation \(*= (n \times k) \text{ mod } N\) of multiplication of the arguments by modulo \(N\). Based on the substitutions of rows/columns from data of basis matrix, \(P(n)\) hashing arrays are

\[
P(n) = P(n_1)P(n_2)\ldots P(n_k),
\]

\[
S(n) = S(n_1)S(n_2)\ldots S(n_k).
\]

\(P(n)\) corresponds of the cyclic decomposition of substitution. Forming hashing array briefly defines the block cyclic structures of basis matrix. The analysis of the structure of basis matrix defines the specific of computational algorithm for different types of DHT. The concurrency and low complexity of these algorithms are well suited for the software implementations and integrated circuits hardware solutions.

4. Conclusions

There are implemented different algorithms of DHT using cyclic convolutions [24, 25]. The development efficient computations of DHT using cyclic convolutions passed from individual discrete components, a prime length, a prime-factor length, not mutually prime factor length and to algorithm for an arbitrary length sequence of transform. The indexing techniques can form the size of transform to different set of the less sizes of cyclic structures. Some of algorithm is not optimal in minimizing any measure of computational complexity. Though the efficient algorithmic schemes of discrete transform of Fourier class using cyclic convolutions are now available and have found great efficiency in hardware implementation applying VLSI technology [26-29]. Indeed, the cyclic convolution or circular correlation structure support a high speed performance, low computational complexity, low values for the input/output contacts.

Therefore, approaches and means of the representation DHT to the computation through of discrete cyclic structures need further investigations and development.

References


119 Ihor Prots’ko and Roman Rykmas: Becoming of Discrete Harmonic Transform Using Cyclic Convolutions


Bibliography

Ihor Prots’ko received the engineer degree and Ph.D. degree from Lviv Polytechnic University in 1981 and 1999, Ukraine. He has a wide scientific and technical background covering Electronics and Computer Science. Currently he is the Assoc. Prof. of Lviv State University of Life Safety. His research interests include fast algorithms of discrete harmonic transforms and special-purpose digital means.

Roman Rykmas received a Master of Engineering (Computer Science) from National University “Lviv Polytechnic” in 2013, Ukraine. He works in the LtdC “Uniservice”, Lviv, where has been developing CAD. His current research interests include fast digital algorithms and their use in CAD/CAE systems.