UDC 004.421.2:517.443

Prots'ko I. O.[1], Teslyuk V. M.[2]

[1]PhD., Associate Professor of Informatic Systems and Technologies Department, Lviv National Polytechnic University, Lviv, Ukraine
[2] Dr.Sc, Professor of Automatic Systems of Control Department, Lviv National Polytechnic University, Lviv, Ukraine

DEVELOPMENT OF WFTA BASED ON THE HASHING ARRAY

Context. A method of efficient computation of DFT using cyclic convolutions for sizes of integer power of two has been considered. The further development of Winograd Fourier transform algorithm based on a hashing array has been proposed. The research object is the process of the reformulation the basis matrix of DFT into the block-cyclic structures. The research subject lays in the technique of the reformulation the basis matrix of DFT for sizes of integer power of two into the block-cyclic structures.

Objective. The purpose of the work is the analysis of the structure specifics the left-circulant submatrices of the basis square matrix W_N for sizes of transform $N = 2^i$ using the hashing arrays.

Method. The article considers a technique for the efficient computation of DFT using cyclic convolutions for sizes of integer power of two, which is based on the cyclic decomposition of substitution. A hashing array has been proposed for the compressed description of the block-cyclic structure of discrete basis matrix and for the efficient computation of DFT for sizes of integer power of two.

Results. A generalized block-cyclic structure of discrete basis matrix for the efficient computation of DF using cyclic convolutions for sizes of an integer power of two based on the hashing arrays has been determined. The proposed technique is relevant for concurrent programming of DFT and for its implementation in parallel systems.

Conclusions. A general block-cyclic structure of basis matrix of DFT is regularly formed with an increase in the value of the exponent of two and is recommended for use in practice when developing the efficient means of DFT. The prospects for further research will include the formation of block-cyclic structure of basis matrix of DFT for arbitrary sizes.

Keywords: fast Fourier transform, Winograd Fourier transform algorithm, hashing array, block-cyclic structure, cyclic convolution.

NOMENCLATURE

CC – cyclic convolution;
DFT – discrete Fourier transform;
FFT – fast Fourier transform;
LC – left-circulant;
WFTA – Winograd Fourier Transform Algorithm
$a_{k,n}$ – arguments of the functions of the discrete exponential basis;
$D(n)$ – hashing array;
$D'(n)$ – simplified hashing array;
$d_{i,j}$ – element of a subarray of a hashing array;
$d'_{i,j}$ – simplified element of a subarray of a hashing array;
g – primitive root;
k – number of subarrays of a hashing array;
L_i – number of elements in a subarray
m – number of multiplications;
N – length of transform;
n – size of the hashing array;
p – prime number;
s – number of additions;
W_N exponential basis of discrete Fourier transform
$X(k)$ – output data of discrete Fourier transform;
$X1(k)$ – real part of output data of discrete Fourier transform;
$X2(k)$ – imaginary part of output data of discrete Fourier transform;
$x(n)$ – input data of a finite length N of a discrete signal;
$Zc(k,n)$ – matrice of signs of the cosine functions of the discrete exponential basis;
$Zs(k,n)$ – matrice of signs of the sine functionsof the discrete exponential basis;
Ψ – set of the substitutions.

INTRODUCTION

DFT is one of the main concepts in information technology. According to this concept a periodic or an irregular signal is presented in the form of combinations of pure frequencies, which are widely used in different electronic systems. Efficient algorithms of DFT – FFT are widely used in many fields of science and technique. There are numerous variations of FFT algorithms that use properties of periodicity and symmetry of the basis of DFT [1, 2].

Another direction of development of the efficient algorithms is a possibility of computation of FFT through cyclic convolutions [3, 4]. In 1968 C. M. Rader proposed the possibility of effective computation of DFT of prime length N via cyclic convolution of length N–1 [5]. Further development was presented by Winograd Fourier Transform Algorithm [6, 7] especially for transformation of the size of power of p – prime number. Winograd algorithms use the data reindexing, where the specific reordering is based on Chinese remainder theorem, the properties of the direct product of matrices and fast cyclic convolution algorithms. Algorithms of DFT using convolutions are collected and thoroughly considered in the books [8, 9].

The purpose of the work is the analysis of the structure specifics the left-circulant submatrices of the basis square matrix W_N for sizes of transform $N = 2^i$ using the hashing arrays.

1 PROBLEM STATEMENT

Initial data of the efficient algorithms WFTA are: x(n) – input data of a finite length $N = 2i$ ($i > 2$; n=0,1,…, N–1); m – numbers of real multiplications, s – number of real additions for computation $X(n)$ output data of DFT through fast cyclic convolutions. However, WFTA algorithms lead to some irregular structures of basis matrix of DFT. This complicates the application of algorithm into actual software or hardware implementation and accordance the number of operations m, s.

The task of research is to develop a reformation of basis matrix of DFT to the regular left-circulant structures. The efficient technique of the reformation the basis matrix of

DOI 10.15588/1607-3274-2018-2-15

DFT for the computation through the cyclic convolutions use the hashing array $D(n)$ with the parameters: n – a size of an hashing array; k – a number of a subarrays of a hashing array; Li – a number of elements in a subarray. The values k, Li define the minimum amount and sizes of the cyclic convolutions and the correspondence of the number of operations m, s of the efficient algorithm.

2 LITERATURE REVIEW

WFTA has important theoretical result for computational complexity of DFT algorithm. It took some effort to translate the theoretical algorithm into actual software or hardware implementation. Therefore, these algorithms are researched and updated by many authors [10–13].

The developed in detail of WFTA by S. Zohar in [14, 15] the algorithm is presented by a series of sequential tables, which are convenient, compact, graphical representations of the sequences of arithmetic operations. The one-out-of-nine part of the paper [14, 15] sufficiently proves the basic DFT of algorithms for N = 8, 16 sizes. In the developed tables for N = 8, 16 there are the complications due to the fact that $N = 2^i$ ($i > 2$) has no primitive roots. In the developed of WFTA by S. Zohar there is a complication due to the fact that $N = 2^i$ ($i > 2$) has no primitive roots. Non-primitive elements of the cyclic group generate only a part of the set.

In the paper [14, 15] has been considered a modification of the relabeling scheme to handle this with the case $N = 16 = 2^4$. The primitive root $g = 3$ generates half of elements in the interval (l, N) of these with powers (mod N). Applying this ($r = g^{\rho} \bmod N$), and ($s = g^{\delta} \bmod N$) for other half with elaborate definition ∂ the author gets the following matrix as shown in Table 1.

In view of the complexity of the present case, the Table 1 is obtained in two stages. As a result, for S. Zohar of DFT the algorithm of size N = 16 needs m = 36 numbers of real multiplications or m = 20 numbers of real multiplications (with excluded from count multiplications by 1 and j) and s = 148 number of real additions.

There fore the DFT of the size of $N = 2^i$ ($i > 2$) has no primitive roots. Non-primitive elements of the cyclic group generate only a part of the set. Thus, the efficient technique of the reformulation the basis matrix of DFT into the block-cyclic structures for the computation through the cyclic convolutions needs to use another forms.

3 MATERIALS AND METHODS

DFT is based on the sum of the product of the input signal values and the complex trigonometric functions. DFT directly is computed by the equation given below

$$X(k) = \sum_{n=0}^{N-1} x(n) W_N{}^{nk}, \; k = 0,1,..., N-1, \qquad (1)$$

where $W_N = \exp(-j\, 2\pi /N)$; $X(k)$, $x(n)$ output and input data of a finite length N the discrete signals. The discrete exponential basis W_N of the DFT (1) may be represented by the real and the imaginary parts

$$X(k) = X1(k) + x(0) - jX2(k), \quad k = 0,1,..., N-1, \qquad (2)$$

where

$$X1(k) = \sum_{n=1}^{N-1} x(n)\, \cos(2\pi kn / N), \quad k = 0,1,..., N-1, \qquad (3)$$

$$X2(k) = \sum_{n=1}^{N-1} x(n)\, \sin(2\pi kn / N), \quad k = 1,..., N-1. \qquad (4)$$

All the N of DFT components $X(k)$ can be obtained after computation of $X1(k)$ and $X2(k)$ parts (3).

The efficient FFT algorithm using cyclic convolution is based on the decomposition [16] of the matrices of the real $X1(k)$ and the imaginary $X2(k)$ parts of DFT taken separately. Let us analyze the arguments of the functions the discrete exponential basis W_N,

$$a_{k,n} = k\, n\, \alpha_N, \quad k = 1,..., N-1, \qquad (5)$$

and especially the integer (k n) components, without $\alpha_N = 2\pi / N$.

Table 1 – The LC structure of basis matrix of arguments DFT for size N = 16

s^r	**0:**	**4:**	**8:**	**12:**	**2:**	**6:**	**10:**	**14:**	**15:**	**13:**	**7:**	**5:**	**1:**	**3:**	**9:**	**11:**
0:	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4:	0	0	0	0	8	8	8	8	12	4	12	4	4	12	4	12
8:	0	0	0	0	0	0	0	0	8	8	8	8	8	8	8	8
12:	0	0	0	0	8	8	8	8	4	12	4	12	12	4	12	4
2:	0	8	0	8	4	12	4	12	14	10	14	10	2	6	2	6
6:	0	8	0	8	12	4	12	4	10	14	10	14	6	2	6	2
10:	0	8	0	8	4	12	4	12	6	2	6	2	10	14	10	14
14:	0	8	0	8	12	4	12	4	2	6	2	6	14	10	14	10
15:	0	12	8	4	14	10	6	2	1	3	9	11	15	13	7	5
13:	0	4	8	12	10	14	2	6	3	9	11	1	13	7	5	15
7:	0	12	8	4	14	10	6	2	9	11	1	3	7	5	15	13
5:	0	4	8	12	10	14	2	6	11	1	3	9	5	15	13	7
1:	0	4	8	12	2	6	10	14	15	13	7	5	1	3	9	11
3:	0	12	8	4	6	2	14	10	13	7	5	15	3	9	11	1
9:	0	4	8	12	2	6	10	14	7	5	15	13	9	11	1	3
11:	0	12	8	4	6	2	14	10	5	15	13	7	11	1	3	9

Basis functions W_N are periodic of N. Therefore, according to the periodic property the matrix of arguments $X_a(k,n)$ of the basic functions contains the components

$$X_a(k,n)=\left[(k\,n)\bmod N\right]=\left\lfloor d_{k,n}\right\rfloor,\quad k=1,\ldots,N-1. \quad (6)$$

each parts (3, 4) respectively is equal to the matrix of arguments

$$X_a(k,n)=\begin{bmatrix}1,\ 2,\ 3,\ \ldots,\ (1\,(N-1))\bmod N\\ 2,\ 4,\ 6,\ \ldots,\ (2(N-1))\bmod N\\ \ldots\\ ((N-1)\,1)\bmod N,\ldots,((N-1)(N-1))\bmod N\end{bmatrix}. \quad (7)$$

Arguments $d_{k,n}$ of the basic functions of DFT is the decomposition of group representations $<N-1,\bullet>$ for prime N, where $\circ-$ is the group operation (6). In accordance with Cayley's theorem [17] the use of the substitutions $\{\Psi_1, \Psi_2, \Psi_3,\ldots, \Psi_{N-1},\}$ of according rows/columns the matrix (7), where algebraic structure $<\Psi, \circ>$ with $\circ$ – the substitution operation, is isomorphic to structure $<N-1,\bullet>$. In result, the $D(n)$ cyclic decomposition of substitution ψ_i is formed. Using of cycle notation, we can write in the form

$$D(n)=(d_{11},d_{12},\ldots,d_{1L1})(d_{21},d_{22},\ldots,d_{2L2})\ldots(d_{kL1},d_{kL2},\ldots,d_{kLk}), \quad (8)$$

where k – a number of a subarrays, d_{ij} – an element of a subarray, L_i – a number of elements in a subarray, n – a size of an array. The form (8) is a short representation of the set of left-circulant submatrices (LC) in the structure of basis matrix of DFT and will be called hashing array $D(n)$.

Let us consider the hashing array $D(n)$ for indexing rows/columns of the matrix of the arguments (7) of DFT for sizes $N = 2^i$. The properties of symmetry and periodicity of DFT basis leads to decrease of values representing components of $d_{k,n}$ of LC submatrices with the supplement of the respective submatrices $Zc(k,n)$ and $Zs(k,n)$ of signs, which contain the value of elements $+1, -1, 0$ (indicate short $+, -, 0$). The simplified matrix components of the arguments $d'_{k,n}$ is determined for sizes $N=2^i$ through a sequence (9, 10) of operations:

$$d'_{k,n}=N-(d_{k,n}\bmod N),\ \text{ if }\ (d_{k,n}\bmod N)>N/2; \quad (9)$$

$$d'_{k,n}=\begin{cases}N/4-(d_{k,n}\bmod N-N/2),\\ \qquad \text{if}\quad N/8<(d_{k,n}\bmod N-N/2\}<N/4;\\ N/4-[N/2-(d_{k,n}\bmod N-N/2)],\\ \qquad \text{if}\quad 3N/8<(d_{k,n}\bmod N-N/2\}<N/2;\\ d_{k,n},\ \text{otherwise.}\end{cases} \quad (10)$$

$$Zc[k,n]=\begin{cases}+1,\ \text{if}\quad 3N/4<c_{k,n}<N/4;\\ 0,\ \text{if}\quad c_{k,n}=N/4,3N/4;\\ -1,\ \text{if}\quad N/4<c_{k,n}<3N/4.\end{cases} \quad (11)$$

$$Zs[k,n]=\begin{cases}+1,\ \text{if}\quad 0<c_{k,n}<N/2;\\ 0,\ \text{if}\quad c_{k,n}=0,N/2;\\ -1,\ \text{if}\quad N/2<c_{k,n}<N.\end{cases} \quad (12)$$

The subarrays of $D(n)$ reproduce Hankel circular submatrices in the structure of a basis square matrix W_N what leads to computation of cyclic convolutions $Z(n)D'(n)$ and input data $x(n)$. For example, DFT for the size $N = 16$ have the hashing array:

$$D(15)=(8)\,(4,12)\,(2,6)\,(10,14)\,(1,3,9,11)\,(15,13,7,5).$$

Using the property of symmetry of DFT the simplified hashing array $D'(8)$ contains the simplified components $d'_{k,n}$, that supplements by respective components of signs $Zc(k,n)$ and $Zs(k,n)$ components:

$$D'(7)=(0)\,(4)\,(2,2)\,(1,3,1,3),$$

$$Zc(7)=(1)\,(0)\,(+,-)\,(+,+,-,-),\ Zs(7)=(0)\,(+)\,(+,+)\,(+,+,-,-).$$

Applying hashing array $D(15)$ we reduce and define the following matrices of simplified arguments of basis with addition of sign for the cosine part as shown in Tables 2, 3, 4.

In summary, the developed algorithm of DFT for size $N = 16$ leads to the computation of one four-point cyclic convolution and two two-point cyclic convolutions. This needs $m = 8$ number of real multiplications for real input data

Table 2 – The matrix of simplified arguments of basis for the cosine/sine part, $N = 16$

k^n	0:	4:	2:	6:	1:	3:	9:	11:
0:	0	0	0	0	0	0	0	0
4:	0	0	8	8	4	4	4	4
2:	0	8	4	4	2	2	2	2
6:	0	8	4	4	2	2	2	2
1:	0	4	2	2	1	3	1	3
3:	0	4	2	2	3	1	3	1
9:	0	4	2	2	1	3	1	3
11:	0	4	2	2	3	1	3	1

Table 3 – Complementing matrix of sign for the cosine part

k^n	0:	4:	2:	6:	1:	3:	9:	11:
0:	1	1	1	1	1	1	1	1
4:	1	1	–1	–1	0	0	0	0
2:	1	–1	0	0	+	–	+	–
6:	1	–1	0	0	–	+	–	+
1:	1	0	+	–	+	+	–	–
3:	1	0	–	+	+	–	–	+
9:	1	0	+	–	–	–	+	+
11:	1	0	–	+	–	+	+	–

Table 4 – Complementing matrix of sign for the sine part

k^n	0:	4:	2:	6:	1:	3:	9:	11:
0:	0	0	0	0	0	0	0	0
4:	0	0	0	0	+1	–1	+1	–1
2:	0	0	+1	–1	+	+	+	+
6:	0	0	–1	+1	+	+	+	+
1:	0	+1	+	+	+	+	–	–
3:	0	–1	+	+	+	–	–	+
9:	0	+1	+	+	–	–	+	+
11:	0	–1	+	+	–	+	+	–

$x(n)$ or $m = 16$ for complex input data $x(n)$ before $m = 20$ of real multiplications for S. Zohar of DFT the algorithm with excluded from count the multiplications by 1 and j. As result, the comparison of the Table 1 and Table 2 of the left-circulant structure of basis matrix of arguments DFT for size $N = 16$ indicates that basis in Table 2 consists entirely of block-cyclic matrix structures.

4 RESULTS

Let us consider the specifics of the structure the LC submatrices of the basis square matrix W_N for sizes of transform $N = 2^i$. Being based on substitutions of matrix rows/columns of data components of arguments the basic functions of DFT are formed by the hashing arrays $D(n)$. The examples of the hashing arrays $D(n)$ and $D'(n)$, $Zc(n)$, $Zs(n)$ (excluded (0) elements) are presented. For N=32 the hashing array consists of k=4 subarrays:

$$D(31) = (1,3,9,27,17,19,25,11)(5,15,13,7,21,31,29,23)(2,6,18,22)(10,30,26,14)(4,12)(20,28)(8,24)(16).$$

The simplified hashing array with the decrease values of elements $d'_{k,n}$ of the arguments (11) correspond to: $D'(31) = (1,3,9,5,15,13,7,11)(5,15,13,7,11,1,3,9)(2,6,14,10)(10,2,6,14)(4,12)(12,4)(8,8)(16)$.

The reduced simplified hashing array with the decrease values of elements $d'_{k,n}$ of the arguments is represented:

$$D'(15) = (1,3,9,5,15,13,7,11)(2,6,14,10)(4,12)(8)(16),$$

$$D'(15) = (1,3,7,5,\ 1,3,7,5)(2,6,2,6)(4,4)(8)(0),$$

and complemented with according arrays of signs

$$Zc(15) = (+,+,-,+,-,-,+,-)(+,+,-,-)(+,-)(-1),$$

$$Zs(15) = (+,+,+,-,-,-,-,+)(+,+,-,-)(+,+)(+)(0).$$

The left-circulant structures of basis matrix of arguments of DFT for size $N = 32$ for the real or the imaginary part is presented in Table 5.

For $N = 64$ the hashing array consists of $k = 5$ subarrays:

$$D(63) = (1,3,9,27,17,51,25,11,33,35,41,59,49,19,57,43)(5,15,45,7,21,63,61,55,37,47,13,39,53,31,29,23)(2,6,18,54,34,38,50,22)(10,30,26,14,42,62,58,46)(4,12,36,44)(20,60,52,28)(8,24)(40,56)(16,48)(32).$$

The reduced simplified hashing array with the decrease values of elements $d'_{k,n}$ of the arguments is presented:

$$D'(31) = (1,3,9,27,17,13,25,11,31,29,23,5,15,19,7,21)(2,6,18,10,30,26,14,22)(4,12,28,20)(8,24)(16)(32),$$

$$D'(31) = (1,3,9,5,15,13,7,11,1,3,9,5,15,13,7,11)(2,6,14,10,2,6,14,10)(4,12,4,12)(8,8)(0),$$

$$Zc(31) = (+,+,+,-,-,+,-,+,-,-,-,+,+,-,+,-)(+,+,-,+,-,-,\ +,-)(+,+,-,-)(+,-)(-1),$$

$$Zs(31) = (+,+,+,+,+,-,+,+,-,-,-,-,-,+,-,-)(+,+,+,-,-,-,\ -,+)(+,+,-,-)(+,+)(0).$$

The hashing array $D'(n)$ of DFT for size $N=2^i$ ($i>2$) could be described in general form:

$$D'(2^{i-1}-1) = D'_1\{2^{i-1}\}\ D'_2\{2^{i-2}\}\ldots D'_{k-1}\{2^1\}\ D'_k\{2^0\}, \quad (13)$$

where $D'_j\{\text{number of elements of the arguments}\}$ (j=1,...,k) of hashing subarrays. Therefore, the general structure of basis matrix of DFT for the real or the imaginary part can be represented in form of Table 6.

Analysis of the structure of submatrices in basis matrix of DFT in Table 5, 6 defines, that some LC submatrices have first row in the form of the reiteration the group of elements, because the simplified hashing subarray $D'_i(n)$ has the form:

$$D'_j(n_k) = (d'_{kL1}, d'_{kL2}, \ldots, d'_{kLj},\ d'_{kL1}, d'_{kL2}, \ldots, d'_{kLj}), \quad (14)$$

and respectively we have the reduction of the size of cyclic convolution in twice.

The conversion of DFT into left-circulant structures is performed on the basis of the hashing arrays. As a result, block cyclic structures of basis matrix of DFT for sizes $N = 2^n$ can be described by the versions of the hashing arrays as shown in Table 7.

Table 5 – The LC structure of basis matrix of arguments DFT for size $N = 32$

s^r	0:	1:	3:	9:	5:	15:	13:	7:	11:	2:	6:	14:	10:	4:	12:	8:
0:	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4:	0	1	3	7	5	1	3	7	5	2	6	2	6	4	4	8
8:	0	3	7	5	1	3	7	5	1	6	2	6	2	4	4	8
12:	0	7	5	1	3	7	5	1	3	2	6	2	6	4	4	8
2:	0	5	1	3	7	5	1	3	7	6	2	6	2	4	4	8
6:	0	1	3	7	5	1	3	7	5	2	6	2	6	4	4	8
10:	0	3	7	5	1	3	7	5	1	6	2	6	2	4	4	8
14:	0	7	5	1	3	7	5	1	3	2	6	2	6	4	4	8
15:	0	5	1	3	7	5	1	3	7	6	2	6	2	4	4	8
13:	0	2	6	2	6	2	6	2	6	4	4	4	4	8	8	16
7:	0	6	2	6	2	6	2	6	2	4	4	4	4	8	8	16
5:	0	2	6	2	6	2	6	2	6	4	4	4	4	8	8	16
1:	0	6	2	6	2	6	2	6	2	4	4	4	4	8	8	16
3:	0	4	4	4	4	4	4	4	4	8	8	8	8	16	16	0
9:	0	4	4	4	4	4	4	4	4	8	8	8	8	16	16	0
11:	0	8	8	8	8	8	8	8	8	16	16	0	0	16	16	0

Table 6 – The left-circulant general structure of basis matrix DFT for size $N = 2^n$

$D'_1\{2^{n-1}\}$	$D'_2\{2^{n-2}\}$	…	$D'_{n-1}\{2^1\}$	$D'_n(2^0)$
				$D'_n(2^0)$
			$D_{n-1}\{2^1\}$	$D'_n(2^0)$
				$D'_n(2^0)$
		…	$D'_{n-1}\{2^1\}$	$D'_n(2^0)$
				$D'_n(2^0)$
			$D'_{n-1}\{2^1\}$	$D'_n(2^0)$
				$D'_n(2^0)$
	$D'_2\{2^{n-2}\}$	…	$D'_{n-1}\{2^1\}$	$D'_n(2^0)$
				$D'_n(2^0)$
			$D'_{n-1}\{2^1\}$	$D'_n(2^0)$
				$D'_n(2^0)$
		…	$D'_{n-1}\{2^1\}$	$D'_n(2^0)$
				$D'_n(2^0)$
			$D'_{n-1}\{2^1\}$	$D'_n(2^0)$
				$D'_n(2^0)$
$D'_2\{2^{n-2}\}$		$D'_2\{2^{n-2}\}$		
…	…	…	…	
$D_{n-1}\{2^1\}$	D_{n-1}	D_{n-1}	D_{n-1}	$D_{n-1}\{2^1\}$
D_n … … …	… … … …	… … … …	… … … …	… … … D_n

Table 7 – The versions of hashing arrays $D(2^n–1)$ of DFT for sizes $N = 2^n$

The versions	Hashing arrays $D(2^n\text{-}1)$
n–2) $D(2^n–1)$	$D_1\{2^{n-2}\}$ $D_2\{2^{n-2}\}$ $D_3\{2^{n-3}\}$ $D_4\{2^{n-3}\}$… $D_{k-2}\{2^1\}$ $D_{k-1}\{2^1\}$ $D_k\{2^0\}$;
n–3) $D(2^n–1)$	$D_1\{2^{n-3}\}$ $D_2\{2^{n-3}\}$ $D_3\{2^{n-3}\}$ $D_4\{2^{n-3}\}$ $D_5\{2^{n-4}\}D_6\{2^{n-4}\}…D_{k-2}\{2^1\}D_{-1}\{2^1\}D_k\{2^0\}$;
…	…
1) $D(2^n–1)$	$D_1\{2^1\}D_2\{2^1\}...D_{k-2}\{2^1\}D_{k-1}\{2^0\}...D_k\{2^0\}$;

In case, DFT for sizes $N = 32 = 2^5$ has such versions of hashing arrays:

3) $D(2^5–1)$=
=(1,5,25,29,17,21,9,13)(3,15,11,23,19,31,27,7)(2,10,18,26)(6,30,22,14)(4,20)(8)(24)(12,28) (16).

The structure of processing module is shown in Fig.1, that computation of cosine or sine part of DFT of size $N = 2^n$ corresponds to the Table 6 and defines the half of output data.

The matrix structure of DFT for size $N = 2^n$ defines serial-parallel combination in the U of the results of cyclic convolutions (CC) for sizes $N = 2^i$, i=2,3,…,n–2 (Fig. 1). The implementations of efficient computation (CC) use availability of the fast convolution algorithms [3].

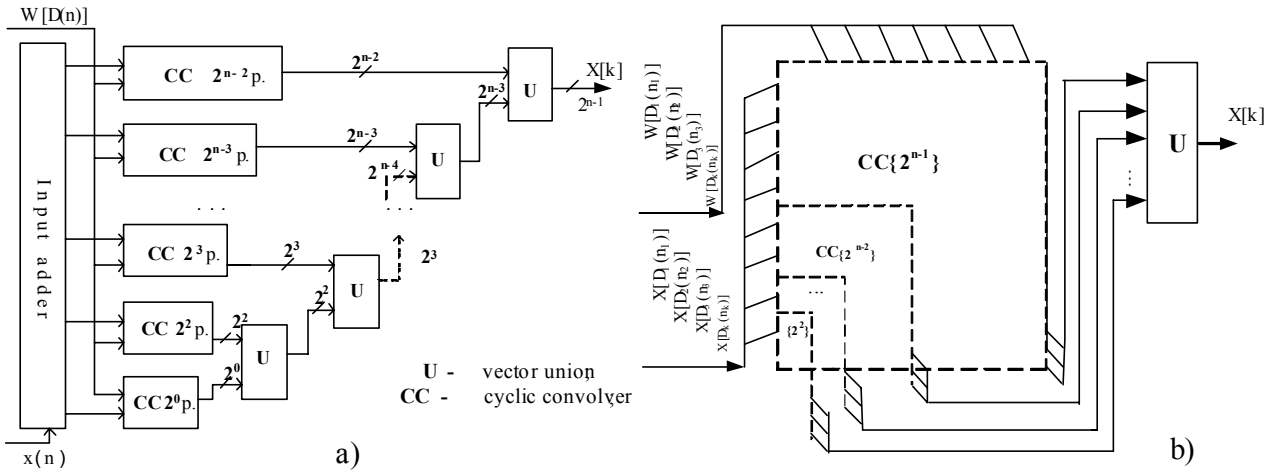

Figure 1 – Structure of processing module for a) concurrency and b) sequential computation of cosine or sine parts of DFT for size $N = 2^n$

The performances of the computation using general block-cyclic structure of basis matrix DFT is an advantage of the proposed developed WFTA. The representation of the structure of basis matrix of DFT via hashing arrays covers the whole structure and is not studied separately as the developed of WFTA by S. Zohar.

The developed algorithm of DFT for size $N = 32, 64, 128$ leads to the computation with the numbers of real multiplications $m = 24, 68, 198$ for real input data $x(n)$ with excluded from count multiplications by 1 and j. In case, we use the fast cyclic convolution algorithms with a minimum number of multiplications. The minimum known the numbers of multiplications have the so-called split-radix algorithm of DFT for an arbitrary fixed $N=2^n$ [18]. The numbers of multiplications of our solution are less in the comparison the split-radix FFT with the numbers $m = 34, 98, 258$ represented in [19] as shown in Fig. 2.

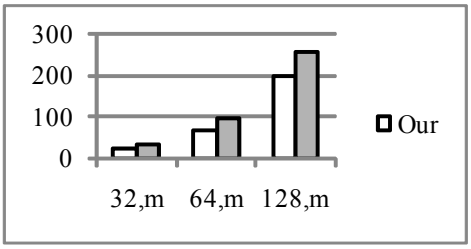

Figure 2 – Comparison of our solution and [19] by the numbers of multiplications of DFT for size $N = 32, 64, 128$

5 DISCUSSION

The computation of real or the imaginary parts of DFT traditionally is executed during three sequential stages: pre-processing, processing, post processing. The computation of cyclic convolutions includes all multiplications of algorithm DFT using of cyclic convolutions on processing stage. The number of arithmetic operations on the basis of this approach is largely dependent on the choice of fast cyclic convolution algorithm (with a minimum number of multiplications or the balance of the operations the additions with the multiplications, and so on).

The proposed algorithm is more flexible in the comparison with the conventional algorithms as it can be applied for realization with length of any power of two. The analysis on the level of simplified hashing array $D'(n)$ with supplement of respective subarrays of $Zc(n)$, $Zs(n)$ signs reduces the amount of computation of cyclic convolutions. The formulation of DFT into left-circulant structures has been found to be very efficient for hardware implementation using VLSI technology [20].

Separate computations of cyclic convolutions (Fig.1), on which we structure the basis matrix of DFT according to the hashing arrays $D(2^n-1)$, and the combinations of convolutions results make the proposed technique important for concurrent programming and for its implementation in parallel systems.

CONCLUSIONS

The article represents the formulation technique of the efficient algorithms of DFT based on the cyclic convolutions for sizes of integer power of two. The developed algorithms are more general than the Rader-Winograd algorithms. The article is further development the algorithm of WFTA by S. Zohar for length of power of two. The number of arithmetic operations on the basis of this technique is defined of fast cyclic convolution algorithms. We have good results in the comparison with of well known algorithms of FFT in case using the fast convolutions with a minimum number of multiplications.

ACKNOWLEDGMENTS

The work was performed as part of research work "Intelligent Information Technologies of Multi-level Management of the Energy Efficiency in the Region" (number of state registration 0117U004450) of Automatic Systems of Control Department of Lviv National Polytechnic University.

REFERENCES

1. Duhamel P. Fast Fourier Transform: A tutorial Review and a State of the Art / P. Duhamel, M. Vitterli // Signal Processing. – 1990. – Vol.19. – P. 259-299. DOI: 10.1016/0165-1684(90)90158-U.
2. Chu E. Inside the FFT black box. Serial and Parallel Fast Fourier Transform Algorithms / E. Chu, A. George. – Boca Raton: CRC Press LLC, 2000.
3. Tolimiery R. Algorithms for Discrete Fourier Transform and Convolution / R. Tolimiery, M. An, C. Lu. – New York : Springer-Verlag, (s.ed.), 1997. – 267 p. DOI: 10.1007/978-1-4757-2767-8.
4. Prots'ko I. Becoming of Discrete Harmonic Transform Using Cyclic Convolutions / I. Prots'ko, R. Rykmas // American Journal of Circuits, Systems and Signal Processing. – 2015. – Vol. 1. – P.114–119.
5. Rader C. M. Discrete Fourier Transforms When the Number of Data Samples is Prime / C. M. Rader // Proceedings of IEEE. – 1968. – Vol. 56. – P. 1107–1108. DOI: 10.1109/PROC.1968.6477.
6. Winograd S. On computing the discrete Fourier transform / S. Winograd // Proceedings National Academy of Science USA, Mathematics. – 1976. – Vol. 73, No. 4. – P. 1005–1006. DOI: 10.1073/pnas.73.4.1005.
7. Winograd S. On computing the discrete Fourier transforms / S. Winograd // Mathematics of Computation. – 1978. – Vol. 32. – P. 175–199. DOI: 10.1090/S0025-5718-1978-0468306-4.
8. Blahut R. E. Fast algorithms for signal processing / R. E. Blahut. – Cambridge : University Press, 2010. DOI: 10.1017/CBO9780511760921.
9. Nussbaumer H. J. Fast Fourier Transform and Convolution Algorithms / H. J. Nussbaumer. – Berlin, Heidelberg : Springer-Verlag, 1982. DOI: 10.1007/978-3-642-81897-4.
10. Lu C. Extension of Winograd Multiplicative Algorithm to Transform Size $N = p^2q$, p^2q^r and Their Implementation. Proceedings of International Conference on Acoustic / C. Lu, R. Tolimieri. – Speech, Signal Processing (ICASSP 89). Scotland, 1989.
11. Silverman H. F. An introduction to Programming the Winograd Fourier Transform algorithm (WFTA) / H. F. Silverman // IEEE Transactions on Acoustic, Speech, Signal Processing (ASSP). – 1977. – Vol. 25, No. 2. – P. 152–165. DOI: 10.1109/TASSP.1977.1162924
12. Patterson R. W. Fixed Point Error Analysis of Winograd Fourier Transform Algorithms / R. W. Patterson, J. H. McClellan // IEEE Transactions on Acoustic, Speech, Signal Processing (ASSP). – 1978. – P. 447–455. DOI: 10.1109/TASSP.1978.1163134.
13. Lavoie P. A high-speed CMOS implementation of the Winograd Fourier transform algorithm / P. Lavoie // IEEE Transactions of Signal Processing. – 1996. – Vol. 44, No. 8. – P. 2121–2126. DOI: 10.1109/78.533738

14. Zohar S. Faster Fourier Transformation: The Algorithm of S. Winograd / S. Zohar // Jet Propulsion Laboratory, JPL Publication 78–104, under NASA Contract No. NAS7-100. – 1979. – P. 1–93.
15. Zohar S. Winograd's discrete Fourier transform algorithm // In book Two-dimensional Digital Signal Processing. Transforms and Median Filters / T. S. Huang. – Berlin, Heidelberg, New York : Springer-Verlag, 1981. – P. 89–152.
16. Prots'ko I. The generalized technique of computation the discrete harmonic transforms / I. Prots'ko // Proceedings of the IVth International Conference MEMSTECH'2008, Polyana, 21–24 may 2008. – P. 101–102.
17. Thomas W. J. Abstract Algebra Theory and Applications / W. J. Thomas. – Stephen F. Austin State University, 2009.
18. Johnson S. G. A modified split-radix FFT with fewer arithmetic operations / S. G. Johnson, M. Frigo // IEEE Transactions of Signal processing. – 2007. – Vol. 55, No. 1. – P. 111–119. DOI: 10.1109/TSP.2006.882087
19. Duhamel P. Implementation of "Split-Radix" FFT Algorithms for Complex, Real, and Real-Symmetric Data / P. Duhamel // IEEE Transactions on Acoustic, Speech, and Signal Processing. – 1986. – Vol. 34, No. 2. – P. 285–295. DOI: 10.1109/TASSP.1986.1164811
20. ASIC Implementation of High Speed Processor for Calculating Discrete Fourier Transformation using Circular Convolution Technique / [P. Saha, A. Banerjee, A. Dandapat, P. Bhattacharyya] // WSEAS Transaction on Circuits and Systems. – 2011. – Vol. 10. – P. 278–288.

Article was submitted 10.11.2017.
After revision 25.12.2017.

Процько І. О.[1], Теслюк В. М.[2]

[1]Канд. техн. наук, доцент кафедри інформаційних систем і технологій, Національний університет «Львівська політехніка», Львів, Україна

[2]Д-р техн. наук, професор кафедри автоматизованих систем управління, Національний університет «Львівська політехніка», Львів, Україна

РОЗВИТОК АВПФ НА ОСНОВІ ТВІРНОГО МАСИВУ

Актуальність. Розглянуто метод ефективного обчислення ДПФ з використанням циклічних згорток для обсягів цілої степені два. Проаналізовано подальший розвиток Алгоритму Віноградa перетворення Фур'є на основі твірного масиву. Об'єктом дослідження є процес реформулювання базисної матриці ДПФ в блочно-циклічні структури. Предмет дослідження полягає в методі реформулювання базисної матриці ДПФ обсягів цілої степені два в блочно-циклічні структури.

Мета роботи полягає в проведенні аналізу особливостей розміщення ліво-циркулянтних підматриць в структурі базисної квадратної матриці W_N для обсягів перетворення $N = 2^i$ на основі використання твірних масивів.

Метод. У статті розглядається методика ефективного обчислення ДПФ з використанням циклічних згорток для обсягів рівних цілій степені два, що базується на циклічному розкладі підстановки. Запропоновано застосування твірного масиву для стислого опису і обчислення блочно-циклічної структури дискретної базисної матриці ДПФ обсягів цілої степені два.

Результати. Визначено загальну блочно-циклічну структуру дискретної базисної матриці для ефективного обчислення ДПФ з використанням циклічних згорток для обсягів цілої степені два на основі твірних масивів. Запропонована методика актуальна для паралельного програмування ДПФ та реалізації в паралельних обчислювальних системах.

Висновки. Загальна блочно-циклічна структура базисної матриці ДПФ регулярно нарощується зі збільшенням значення показника цілої степені два і рекомендується для використання на практиці при розробці ефективних засобів ДПФ. Перспективи подальших досліджень включатимуть формування блочно-циклічних структур базисної матриці ДПФ для довільних розмірів.

Ключові слова: швидке перетворення Фур'є, алгоритм Віноградa перетворення Фур'є, твірний масив, блочно-циклічна структура, циклічна згортка.

Процько И. Е.[1], Теслюк В. М.[2]

[1]Канд. техн. наук, доцент кафедры информационных систем и технологий, Национальный университет "Львівська политэхника", Львив, Украина

[2]Д-р техн. наук, професор кафедры автоматизованных систем управления, Национальный университет "Львівська политэхника", Львив, Украина

РАЗВИТИЕ АВПФ НА ОСНОВАНИИ ОБРАЗУЮЩЕГО МАССИВА

Актуальность. Рассмотрен метод эффективного вычисления ДПФ с использованием циклических сверток для длин равных целой степени два. Проанализировано дальнейшее развитие алгоритма Винограда преобразования Фурье на основании образующего массива. Об'єктом исследования есть процесс реформулирования базисной матрицы ДПФ в блочно-циклические структуры. Предметом исследования есть метод реформулирования базисной матрицы ДПФ для длин равных целой степени два в блочно-циклические структуры.

Цель работы заключается в проведении анализа особенностей размещения лево-циркулянтных подматриц в структуре базисной квадратной матрицы W_N для длин преобразования $N = 2^i$ с использованием образующих массивов.

Об'єктом дослідження є процес реформулювання базисної матриці ДПФ в блочно-циклічні структури. Предмет дослідження полягає в методі реформулювання базисної матриці ДПФ обсягів цілої степені два в блочно-циклічні структури.

Метод. В статье рассматривается методика эффективного вычисления ДПФ с использованием циклических сверток для длин равних целой степени два, основанная на циклическом разложении подстановки. Предложено использовать образующий массив для сжатого описания и вычисления блочно-циклической структуры дискретной базисной матрицы ДПФ длин равних целой степени два.

Результаты. Определена обобщенная блочно-циклическая структура дискретной базисной матрицы для эффективного вычисления ДПФ с использованием циклических сверток для длин равных целой степени два на основании образующих массивов. Предложенная методика актуальна для параллельного программирования ДПФ и реализации в параллельных вычислительных системах.

Выводы. Общая блочно-циклическая структура базисной матрицы ДПФ регулярным образом формируется с увеличением значения показателя целой степени два и рекомендуется для использования на практике при разработке эффективных средств ДПФ. Перспективы дальнейших исследований будут включать формирование блочно-циклических структур базовой матрицы ДПФ для произвольных размеров преобразования.

Ключевые слова: быстрое преобразование Фурье, алгоритм Винограда преобразования Фурье, образующий массив, блочно-циклическая структура, циклическая свертка.

REFERENCES

1. Duhamel P., Vitterli M. Fast Fourier Transform: A tutorial Review and a State of the Art, *Signal Processing*, 1990, Vol.19, pp. 259–299. DOI: 10.1016/0165-1684(90)90158-U.
2. Chu E., George A. Inside the FFT black box. Serial and Parallel Fast Fourier Transform Algorithms. Boca Raton, CRC Press LLC, 2000.
3. Tolimiery R., An M., Lu C. Algorithms for Discrete Fourier Transform and Convolution. New York, Springer-Verlag, (s.ed.), 1997, 267 p. DOI: 10.1007/978-1-4757-2767-8.
4. Prots'ko I., Rykmas R. Becoming of Discrete Harmonic Transform Using Cyclic Convolutions, *American Journal of Circuits, Systems and Signal Processing,* 2015, Vol. 1, pp. 114–119.
5. Rader C. M. Discrete Fourier Transforms When the Number of Data Samples is Prime, *Proceedings of IEEE*, 1968, Vol. 56, pp. 1107–1108. DOI: 10.1109/PROC.1968.6477.
6. Winograd S. On computing the discrete Fourier transform, *Proceedings National Academy of Science USA, Mathematics*, 1976, Vol. 73, No 4, pp. 1005–1006. DOI: 10.1073/pnas.73.4.1005.
7. Winograd S. On computing the discrete Fourier transforms, *Mathematics of Computation*, 1978, Vol. 32, pp. 175–199. DOI: 10.1090/S0025-5718-1978-0468306-4.
8. Blahut R. E. Fast algorithms for signal processing. Cambridge, University Press, 2010. DOI: 10.1017/CBO9780511760921.
9. Nussbaumer H. J. Fast Fourier Transform and Convolution Algorithms. Berlin, Heidelberg, Springer-Verlag, 1982. DOI: 10.1007/978-3-642-81897-4.
10. Lu C., Tolimieri R. Extension of Winograd Multiplicative Algorithm to Transform Size $N = p^2q$, p^2q^r and Their Implementation. Proceedings of International Conference on Acoustic, Speech, Signal Processing (ICASSP 89). Scotland, 1989.
11. Silverman H. F. An introduction to Programming the Winograd Fourier Transform algorithm (WFTA), *IEEE Transactions on Acoustic, Speech, Signal Processing (ASSP)*, 1977, Vol. 25, No. 2, pp. 152–165. DOI: 10.1109/TASSP.1977.1162924
12. Patterson R. W., McClellan J. H. Fixed Point Error Analysis of Winograd Fourier Transform Algorithms, *IEEE Transactions on Acoustic, Speech, Signal Processing (ASSP)*, 1978, pp. 447–455. DOI: 10.1109/TASSP.1978.1163134.
13. Lavoie P. A high-speed CMOS implementation of the Winograd Fourier transform algorithm, *IEEE Transactions of Signal Processing*, 1996,Vol. 44, No. 8, pp. 2121–2126. DOI: 10.1109/78.533738
14. Zohar S. Faster Fourier Transformation: The Algorithm of S. Winograd, *Jet Propulsion Laboratory, JPL Publication 78-104*, under NASA Contract No. NAS7-100, 1979, pp. 1–93.
15. Zohar S. Winograd's discrete Fourier transform algorithm, *In book Two-dimensional Digital Signal Processing. Transforms and Median Filters*. Berlin, Heidelberg, New York, Springer-Verlag, 1981, pp. 89–152.
16. Prots'ko I. The generalized technique of computation the discrete harmonic transforms, *Proceedings of the IVth International Conference MEMSTECH'2008, Polyana*, 21–24 may 2008, pp.101–102.
17. Thomas W. J. Abstract Algebra Theory and Applications. Stephen F. Austin State University, 2009.
18. Johnson S. G., Frigo M. A modified split-radix FFT with fewer arithmetic operations, *IEEE Transactions of Signal processing*, 2007, Vol. 55, No. 1, pp. 111–119. DOI: 10.1109/TSP.2006.882087
19. Duhamel P. Implementation of "Split-Radix" FFT Algorithms for Complex, Real, and Real-Symmetric Data, *IEEE Transactions on Acoustic, Speech, and Signal Processing*, 1986, Vol. 34, No. 2, pp. 285–295. DOI: 10.1109/TASSP.1986.1164811
20. Saha P., Banerjee A., Dandapat A., Bhattacharyya P. ASIC Implementation of High Speed Processor for Calculating Discrete Fourier Transformation using Circular Convolution Technique, *WSEAS Transaction on Circuits and Systems*, 2011, Vol. 10, pp. 278–288.