<table>
<thead>
<tr>
<th>著者</th>
<th>Nakayama Kenji</th>
</tr>
</thead>
<tbody>
<tr>
<td>項目名</td>
<td>Permuted difference coefficient digital filters</td>
</tr>
<tr>
<td>出版物名</td>
<td>ICASSP, IEEE International Conference on Acoustics, Speech and Signal Processing - Proceedings</td>
</tr>
<tr>
<td>卷</td>
<td>3</td>
</tr>
<tr>
<td>頁</td>
<td>1197-1200</td>
</tr>
<tr>
<td>年</td>
<td>1981-04-01</td>
</tr>
<tr>
<td>URL</td>
<td><a href="http://hdl.handle.net/2297/6791">http://hdl.handle.net/2297/6791</a></td>
</tr>
</tbody>
</table>
A New Discrete Fourier Transform Algorithm Using Butterfly Structure Fast Convolution
KENJI NAKAYAMA, SENIOR MEMBER, IEEE

Abstract—This paper proposes a new approach to computing the
discrete Fourier transform (DFT) with the power of 2 length using the
butterfly structure number theoretic transform (NTT). An algorithm
breaking down the DFT matrix into circular matrices with the power of 2
size is newly introduced. The fast circular convolution, which is
implemented by the NTT based on the butterfly structure, can provide
significant reductions in the number of computations, as well as a simple
and regular structure. The proposed algorithm can be successively
implemented following a simple flowchart using the reduced size
submatrices. Multiplicative complexity is reduced to about 21 percent of
that by the classical FFT algorithm, preserving almost the same number
of additions.

I. INTRODUCTION

SEVERAL approaches to computing the discrete Fourier
transform (DFT) for a time sequence have been reported. The
classical fast Fourier transform (FFT) algorithm is based on
either decimations in frequency or in time, and can be
implemented on the simple butterfly structure [1], [2]. Further
efforts on computational reductions in the FFT have been
reported with respect to combinations of radices [3], [4], and
to some modifications of multiplicands [5]. Recently, both
decimations in frequency and in time have been combined to
yield computationally more efficient algorithms [6], [7].
Furthermore, a conceptually new class of algorithms has been
proposed, which divides the DFT coefficient matrix into small
size circular matrices whose sizes are prime numbers. To
calculate these matrices, fast convolution algorithms has been
applied [8]–[11]. These algorithms can sufficiently
decrease multiplicative complexity at the expense of a small
number of additions and a simple and regular structure. The
number of linear multiplications required in the DFT calcu-
lation has been generally investigated, and proved to be bounded
by twice a transform length [12], [13].

On the other hand, one of the useful approaches to
computing the circular convolutions is to use the number
theoretic transform (NTT) [14]–[22]. When the transform
length is the power of 2, the NTT can be implemented by using
the power of 2 multiplications, which are simply realized with
circular shifts, as well as a simple butterfly structure [16].
Since the existing DFT algorithms, employing the fast
convolutions, are only applied to prime factor DFTs, the
above features of the NTT cannot be utilized.

This paper proposes a new algorithm for computing the
DFT with the power of 2 transform length. The DFT
coefficient matrix is broken down into small size circular
matrices through a newly introduced matrix reformation
method. Since these submatrices also have the power of 2 size,
the butterfly structure NTT having the power of 2 multiplica-
tions can be successfully applied [23].

Section II briefly states the well known fast circular
convolution algorithm with the power of 2 length based on the
butterfly structure. In Section III, the new algorithm to break
down the DFT coefficient matrix into small size circular
matrices is provided. A general flowchart and block diagrams
showing how to carry out the proposed algorithm are
illustrated in Section IV. Section V discusses computational
complexity and shows numerical examples to compare
performances for proposed and conventional approaches.

II. FAST CIRCULAR CONVOLUTION

Fast circular convolution algorithms based on the butterfly
structure [16], [24] are briefly stated here.

Letting \( x = (x_0, x_1, \ldots, x_{N-1})' \) and \( y = (y_0, y_1, \ldots, y_{N-1})' \) be input and output sequences, respectively, the
circular convolution is expressed as follows:

\[
y = Hx
\]

\[
H = \begin{bmatrix}
h_0 & h_1 & h_2 & \cdots & h_{N-1} \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
h_2 & h_3 & h_4 & \cdots & h_1 \\
h_1 & h_2 & h_3 & \cdots & h_0
\end{bmatrix}
\]

where \( h = (h_0, h_1, \ldots, h_{N-1})' \) is an impulse response of a
system and \( (\cdot)' \) denotes the transposed vector. \( H_N(N) \) is used
to denote a matrix whose element at the \( i \)th row and \( k \)th column is given by

\[
h_{A}(i, k) = h(i, k), \quad i \leq k
\]

\[
= h(k, i), \quad i > k.
\]

\( H_N(N) \) is further divided into submatrices as

\[
H_N(N) = \begin{bmatrix}
A & B \\
\lambda B & A
\end{bmatrix}
\]

(3)

Submatrix \( A \) also includes the elements multiplied by \( \lambda \).
\( H_N(N) \) can be reformed as a product of butterfly structure
transform matrices and a diagonal matrix as follows:

\[
H_N(N) = \begin{bmatrix}
A & B \\
\lambda B & A
\end{bmatrix} \begin{bmatrix}
\mathcal{I}(N/2) & -\mathcal{I}(N/2) \\
\mathcal{I}(N/2) & \mathcal{I}(N/2)
\end{bmatrix}
\]

\[
\cdot \begin{bmatrix}
(A+\lambda B)/2 & 0 \\
0 & (A-\lambda B)/2
\end{bmatrix} \begin{bmatrix}
\mathcal{I}(N/2) & \lambda^{-1}\mathcal{I}(N/2) \\
\mathcal{I}(N/2) & -\mathcal{I}(N/2)
\end{bmatrix}
\]

(4a)

Manuscript received July 11, 1983; revised September 1, 1984.
The author is with the Transmission Division, NEC Corporation, Naka-
hara-ku, Kawasaki, 211 Japan.

0096-3518/85/1000-1197$01.00 © 1985 IEEE
where $I(N/2)$ is an $(N/2) \times (N/2)$ size unit matrix and $\lambda$ satisfies

$$\lambda^2 = \gamma. \tag{4b}$$

Equation (4b) shows the case of radix 2. A block diagram showing (4a) execution is illustrated in Fig. 1. It is easily proved that the matrices $(A \pm \lambda B)/2$ have the $H_{2N}(N/2)$ structure. Therefore, these submatrices can be further divided as (4). Repeating this matrix division procedure, the well known fast circular convolution, based on the radix 2 butterfly structure, is derived. The fast transform processes are mainly classified into two categories, depending on number systems to represent $\lambda$ and $\lambda$. When the complex number system is utilized, the fast transforms become the DFT and the inverse DFT. On the other hand, when the residue number system is employed, the number theoretic transform (NTT) and the inverse NTT can be applied [16], [22].

III. NEW ALGORITHM TO OBTAIN CIRCULAR SUBMATRICES

A main problem is how to break down the DFT coefficient matrix into circular submatrices with the power of 2 size. This section introduces a new algorithm for the above problem. The proposed algorithm consists of three processes, including mixed decimations in frequency and in time [6], row and column permutations, and changing the sign of matrix elements.

A. Mixed Decimations in Frequency and in Time

First, in order to make preparations and to define the notations used in the following discussions, the mixed decimations in frequency and in time are briefly stated here.

Letting $F(N)$ be the DFT coefficient matrix whose size is $N \times N$, and $f(i, k)$ be an element of $F(N)$ at the $i$th row and $k$th column, then

$$f(i, k) = \exp \left(-j2\pi ik/N\right), \quad 0 \leq i, k \leq N-1 \tag{5a}$$

$$j = \sqrt{-1}. \tag{5b}$$

Let $T_M(N)$ be a decimation matrix with a size of $N \times N$ for radix $M$. An element $t_M(i, k)$ of $T_M(N)$ at the $i$th row and $k$th column is given by

$$t_M(i, k) = \begin{cases} \left\lfloor \frac{i}{M} \right\rfloor + iM & \text{if } k = i M \\ 0 & \text{otherwise} \end{cases} \tag{6a}$$

$$t_M(i, k) = 0, \quad k \neq \left\lfloor \frac{i}{M} \right\rfloor + iM \tag{6b}$$

$$0 \leq i, k \leq N-1$$

where notations $\left\lfloor i/M \right\rfloor$ and $\left(\cdot\right)_N$ mean the maximum integer not exceeding $i/M$ and the residue number system operation with the residue modulo $N$, respectively. The decimations in frequency and in time are performed by multiplying $F(N)$ by $T_M(N)$ from the left side and the right side, respectively.

Decimation in frequency: $T_M(N)F(N)$
Decimation in time: $F(N)T_M(N)$.

Although arbitrary radices can be considered to divide the DFT matrix, radix 2 is used to describe the algorithm throughout the paper in order to make discussions simple. The results are easily extended to a case of other radices.

The DFT matrix $F(N)$ is divided into submatrices by the decimation in frequency as

$$T_2(N)F(N) = \begin{bmatrix} F_0(N/2) & F_1(N/2) \\ F_1(N/2) & -F_0(N/2) \end{bmatrix} \tag{7}$$

where $F_0(N/2)$ and $F_1(N/2)$ are submatrices with an $(N/2) \times (N/2)$ size. $F_0(N/2)$ has the same structure as $F(N)$ with reduced size

$$F_0(N/2) = F(N/2). \tag{8}$$

The decimation in frequency is further applied to dividing $F_0(N/2)$. On the other hand, $F_1(N/2)$ is broken down by the decimation in time as

$$F_1(N/2)T_2(N/2) = \begin{bmatrix} F_{10}(N/4) & F_{11}(N/4) \\ F_{10}(N/4) & -F_{11}(N/4) \end{bmatrix} \tag{9}$$

where $F_{10}(N/4)$ and $F_{11}(N/4)$ are submatrices with an $(N/4) \times (N/4)$ size. $F_{10}(N/4)$ has the same structure as $F_1(N/2)$ with the reduced size

$$F_{10}(N/4) = F_1(N/4). \tag{10}$$

Therefore, $F_{10}(N/4)$ is further broken down through the decimation in time. The matrix $F_{11}(N/4)$ is transformed into the circular convolution matrix at the second stage, that is, $H_{1/4}(N/8)$ defined by (1) and (2). It is possible to transform the submatrices, obtained after further decimations, into the circular matrices at the $m$th stages ($2 < m$). In this paper, however, the matrix transform from $F_{11}(N/4)$ to $H_{1/4}(N/8)$ is employed to describe the proposed algorithm. Extending the discussions to a general case is straightforward, and some comments are given at the end of this section.

B. Matrix Reformulation from $F_1(N/4)$ to $H_{1/4}(N/8)$

Letting $g(i, k)$ be an element of $F_1(N/4)$ at the $i$th row and $k$th column, it can be expressed from (7) and (9) as

$$g(i, k) = \exp \left(-j2\pi(k+1)(2k+1)/N\right) \tag{11}$$

$$0 \leq i, k \leq \frac{N}{4} - 1.$$
Theorem 1: Letting \( g(i, k) \) be expressed by
\[
g(i, k) = \exp (-j2\pi q(i, k)/N), \quad q(i, k) : \text{odd integer},
\]
(12)

\( q(i, k) \) satisfies
\[
\langle q(i, k) \rangle_{N/2} = 2n + 1, \quad 0 \leq n \leq \frac{N}{4} - 1
\]
(13a)
\[
\langle q(i, k) \rangle_{N/2} = \langle q(i, k') \rangle_{N/2}, \quad k \neq k'
\]
(13b)
\[
\langle q(i, k) \rangle_{N/2} = \langle q(i', k) \rangle_{N/2}, \quad i \neq i'.
\]
(13c)

Proofs for the theorems introduced in this paper are all given in the Appendixes.

Theorem 2: An integer \( n \) satisfying
\[
\left(2n + 1\right)^N = \frac{N}{2} + 1, \quad 0 < n < \frac{N}{2} - 1
\]
(14)
always exists.

Next, the element \( g(0, 0) \) is assumed to be fixed in the row and column permutation process for \( F_1(N/4) \). The circular matrices not satisfying this assumption can be easily obtained by further permuting the rows or columns.

From the \( F_1(N/4) \) properties given by Theorems 1 and 2, the next theorem concerning how to permute the rows and columns of \( F_1(N/4) \) is derived.

Theorem 3: \( F_1(N/4) \) can be transformed by permuting the rows and columns into
\[
P_1(N/4)F_1(N/4)P_2(N/4) = \begin{bmatrix} A & B \\ B & A \end{bmatrix}
\]
(15)
where \( P_1(N/4) \) and \( P_2(N/4) \) are row and column permutation matrices, respectively. Let \( a(i, k) \) and \( b(i, k) \) be elements at the \( i \)th and \( k \)th column of \( A \) and \( B \), respectively, and be expressed by
\[
a(i, k) = \exp (-j2\pi \alpha(i, k)/N)
\]
(16a)
\[
b(i, k) = \exp (-j2\pi \beta(i, k)/N)
\]
(16b)
where \( \alpha(i, k) \) and \( \beta(i, k) \) are odd numbers.

1) \( \alpha(i, k) \) and \( \beta(i, k) \) are odd numbers.
\[
\langle \alpha(i + 1, k + 1) \rangle_{N/2} = \langle \alpha(i, k) \rangle_{N/2}, \quad 0 \leq i, k \leq \frac{N}{8} - 2
\]
(17a)
\[
\langle \alpha(i + 1, 0) \rangle_{N/2} = \left\langle \alpha\left(\frac{N}{8} - 1\right) \right\rangle_{N/2}, \quad 0 \leq i \leq \frac{N}{8} - 2
\]
(17b)
\[
\langle \beta(i + 1, k + 1) \rangle_{N/2} = \langle \beta(i, k) \rangle_{N/2}, \quad 0 \leq i, k \leq \frac{N}{8} - 2
\]
(17c)
\[
\langle \beta(i + 1, 0) \rangle_{N/2} = \left\langle \beta\left(\frac{N}{8} - 1\right) \right\rangle_{N/2}, \quad 0 \leq i \leq \frac{N}{8} - 2
\]
(17d)

2) \( a(i, k) \) and \( b(i, k) \) are related by
\[
a(i, k) = -b^*(i, k)
\]
(18)
where \( c^* \) denotes complex conjugate of \( c \).

Equation (17) means that the matrices \( A \) and \( B \) have the same structure as the second stage circular convolution matrix \( H_{-1}(N/8) \), except for the polarity of the matrix elements.

The concrete row and column permutation procedure is provided in the proof of Theorem 3, and is summarized here.

Step 1: \( a(0, 0) = g(0, 0) \).

Step 2: \( a(1, 0) = \exp (-j2\pi \alpha(1, 0)/N) \)
\[
(\alpha(N/8)(1, 0)_{N/2} = 1.
\]
(20b)

Step 3: \( a\left(0, \frac{N}{8} - i\right) = \exp \left(-j\pi\alpha\left(0, \frac{N}{8} - i\right)/N\right) \)
\[
(\alpha(0, \frac{N}{8} - i)_{N/2} = (\alpha'(1, 0)_{N/2})
\]
(21a)
\[
2 \leq i \leq \frac{N}{8} - 1.
\]
(21b)

Step 4: \( a(i, 0) = \exp (-j2\pi \alpha(i, 0)/N) \)
\[
(\alpha(i, 0)_{N/2} = \left\langle \alpha\left(\frac{N}{8} - i\right) \right\rangle_{N/2}
\]
(22a)
\[
2 \leq i \leq \frac{N}{8} - 1.
\]
(22b)

The above row and column permutations in \( A \) uniquely determine the permutations in \( B \).

From (4), the matrix given by (15) is divided into
\[
\begin{bmatrix} A & B \\ B & A \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} A + B/2, & 0 \\ 0, & (A - B)/2 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0, & -1 \end{bmatrix}.
\]
(23)

Since \( A \) and \( B \) satisfy the conditions given by (17), \( (A \pm B)/2 \) also satisfies the same condition. The following theorem is held for the submatrices \( (A \pm B)/2 \).

Theorem 4: Letting \( a(i, k) \), \( a_+(i, k) \) and \( a_-(i, k) \) be elements of \( A \), \( (A + B)/2 \) and \( (A - B)/2 \) at the \( i \)th row and \( k \)th column, respectively, \( a_+(i, k) \) are given by
\[
a_+(i, k) = j \text{ Im}(a(i, k))
\]
(24a)
\[
a_-(i, k) = \text{ Re}(a(i, k))
\]
(24b)

where \( \text{Im}(\cdot) \) and \( \text{Re}(\cdot) \) mean imaginary and real parts of a complex number.

Theorem 4 indicates that the \( (A \pm B)/2 \) elements have pure imaginary and real values. Therefore, \( (A \pm B)/2 \) can be essentially regarded as real value matrices. This gives reductions in the number of computations.
The previous discussions on the matrix reformation are carried out except for the polarity of the $A$, $B$, and $(A \pm B)/2$ elements. A procedure modifying the polarity, by which the second stage circular convolution matrix $H_{-1}(N/8)$ is finally obtained, is introduced here. First, a preparatory theorem is given.

**Theorem 5:** Let $N'$ be an integer and satisfy

$$N' < N.$$  

Let $c(i, k)$ be an element of an $N \times N'$ matrix $C$ at the $i$th row and $k$th column, and be expressed by

$$c(i, k) = \exp(-j2\pi \gamma(i, k)/N), \quad \gamma(i, k) = \text{odd number}$$  

where $\gamma(i, k)$ satisfies

$$\gamma(0, 0) = 1$$

$$\gamma(N', 0) = 2^{N/2} + 1$$

$$\gamma(i, 0) = \gamma(0, i) = \gamma(0, 0)$$

$$\gamma(i, k) = \gamma(i, 0) \gamma(k, 0).$$

The matrix $C$ can be transformed into $H_{-1}(N')$ by changing the polarity of elements included in the 0th column.

Next, from Theorem 5, the following theorem concerning how to change the polarity of the elements of $A$ can be derived.

**Theorem 6:** Let $\Omega$ be a set of integer numbers, whose element $i$ satisfies

$$a(i, k) = \exp(-j2\pi \alpha(i, k)/N)$$

$$\alpha(i, 0) = \alpha(0, i) = \frac{N}{2}.$$  

The matrix $A$ can be transformed into $H_{-1}(N/8)$ by changing the polarity of elements included in the 0th column, $i$th row, and $(N/8 - 1)$th column where $i \in \Omega$.

It is easily shown that a manner of changing the sign provided by Theorem 6 is also valid for $B$ and $(A \pm B)/2$. Thus, the matrices $(A \pm B)/2$ can be changed into $H_{-1}(N/8)$ having pure imaginary and real value coefficients, respectively.

**C. Removing the Assumption of $a(0, 0) = g(0, 0)$**

Circular matrices not satisfying the assumption of $a(0, 0) = g(0, 0)$ are obtained as follows. First, it is easily proved that the structure of $H_{-1}(N)$ defined by (1) and (2) is always valid even though moving elements of the 0th column to the $(N - 1)$th column, and elements of the $(i + 1)$th column to the $i$th column, and changing the sign of elements of the $(N - 1)$th column. Through these reformatations, an arbitrary element of $A$ can be assigned to the 0th row and 0th column.

**D. General Radix and Stage**

The previous discussions are restricted to the case of obtaining $F_{11}(N/4)$ from $F(N)$ using the radix 2 decimations, and $H_{-1}(N/8)$ from $F_{11}(N/4)$. However, the proposed algorithm can be extended to a general case in the same way. When the submatrices, obtained by performing the radix $M$ decimations, $2 < M$ or further decimations on $F_{11}(N/4)$ are used to form the circular convolution matrices, the factor $\lambda$ usually becomes a complex value. Therefore, the complex number theoretic transforms [27]-[29] must be employed.

**IV. IMPLEMENTATION OF THE NEW ALGORITHM**

**A. General Flowchart**

Fig. 2 shows a general flowchart for the new algorithm using the radix 2 decimations and the second stage circular convolution matrix. The operations are repeated using the reduced size matrices having the same structures as $F_3(N)$ and $F_6(N/4)$.

**B. Block Diagrams**

Fig. 3 shows block diagrams of the method wherein the decimations in frequency and in time given by (7) and (9) are carried out. FDS and TDS are frequency and time decimation shuffles. The matrix reformation procedure from $F_{11}(N/4)$ to $H_{-1}(N/8)$ is illustrated in Fig. 4(a). Since the multiplication of $j = -1$ is performed at the output, the elements of $H_{-1}(N/8)$ have real values. The concrete element values of $H_{-1}(N/8)$ in the case of a 32 point DFT are given at the end of this section. Furthermore, a general block diagram for $H_{-1}(N/8)$ implementation through the NTT and the inverse NTT is shown in Fig. 4(b). Since the $H_{-1}(N/8)$ size is the power of 2, each stage in the NTT and the inverse NTT can be realized using the butterfly structure [16], which provides a regular and simple structure and reductions in the numbers of additions and data transforms.

**C. Number Theoretic Transform**

By using the Fermat number as the residue modulo [16],

$$M = 2^b + 1,$$

the multiplicands, which appear at the $i$th stage $1 \leq i \leq b + 1$, become the power of 2. The multiplicands $\lambda_i$ at the $i$th stage satisfies the recurrence formula

$$\lambda_i = \lambda_{i-1}, \quad 1 \leq i \leq b + 1$$

$$\lambda_0 = -1.$$  

In the $i$th stage, $i \leq b$, $\lambda_i$ can be expressed by

$$\lambda_i = 2^b \lambda_{i-1}, \quad 1 \leq i \leq b.$$  

Furthermore, $\lambda_{b+1}$ at the $(b + 1)$th stage has a simple number [16],

$$\lambda_{b+1} = 2^{b-2}(2^{b-1} - 1).$$

The matrix $H_{-1}(N/8)$ is called the second stage circular convolution matrix. On the other hand, the stages in the NTT and the inverse NTT are numbered from the first stage.
Fig. 2. General flowchart for new DFT algorithm.

Fig. 3. Block diagrams showing decimations in frequency (a) and in time (b). FDS and TDS are frequency and time decimation shuffles, respectively.

Fig. 4. (a) Matrix reformation process from \( F_{11}(N/4) \) to \( H_{11}(N/8) \). (b) Fast convolution through NTT and inverse NTT.

As a whole, from the first stage to the \((b + 1)\)th stage, the multiplications of \( \lambda_i \) can be replaced by circular shifts. When \( H_{11}(N/8) \) transform length is greater than \( 2^{b+1} \), there exist two approaches to computing the circular convolution, according to the residue modulo employed.

**Modulo** \( 2^{16} + 1 \): In this case, it is possible to express \( 2^{\sqrt{2}}, 1 \leq i \leq 11 \) by elements in the residue number system. Therefore, the one-dimensional butterfly structure can be applied. Multipliers in the \( i \)th stage, \( b + 2 \leq i \), are fixed constants which do not depend on the DFT matrix elements.

**Modulo** \( 2^{32} + 1 \): On the contrary, the residue number system with modulo \( 2^{32} + 1 \) is not a prime number. The maximum possible transform length for the one-dimensional butterfly structure becomes \( 2^{b+2} \), that is, \( 2^{32+2} = 128 \), where multipliers have the power of 2. Therefore, in the case of \( 2^{b+1} < N/8 \), some modification must be required. In this paper, the following matrix size reduction method is adopted [17].

\[
H_{11}(M) = \begin{bmatrix} A & B \\ \lambda B & A \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} B - A & 0 & 0 \\ 0 & A & 0 \\ 0 & 0 & \lambda B - A \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 1 & 1 \\ 0 & 1 \end{bmatrix}.
\] (33)

Matrices \( B - A, A, \) and \( \lambda B - A \) have the same structure as \( H_{11}(M) \) with the reduced size \((M/2) \times (M/2)\). When \( M/2 \) is still larger than \( 2^{b+1} \), the above matrix dividing is further repeated until the reduced size becomes \( 2^{b+1} \), that is, \( 2^{5+1} = 64 \).

D. Example for 32 Point DFT

**Matrix Reformation**: \( F_{11}(N/4) \) is obtained through the decimations in frequency and in time as follows:

\[
F_{11}(N/4) = \begin{bmatrix} w^1 & w^3 & w^5 & w^7 & w^9 & w^{11} & w^{13} & w^{15} \\
 w^2 & w^6 & w^{10} & -w^5 & -w^9 & -w^{11} & w^1 & w^3 & w^7 \\
 w^4 & w^{12} & w^{14} & -w^3 & -w^7 & w^11 & -w^5 & -w^9 & w^7 \\
 w^5 & w^9 & w^{13} & -w^3 & -w^5 & w^{11} & -w^7 & w^1 & w^3 \\
 w^6 & w^{12} & w^{14} & -w^1 & -w^5 & w^7 & -w^3 & w^9 & w^7 \\
 w^7 & w^{11} & w^{13} & -w^1 & -w^3 & w^5 & -w^9 & w^7 & w^3 \\
 w^8 & w^{12} & w^{10} & -w^2 & -w^6 & w^{11} & -w^7 & w^3 & w^5 \\
 w^{15} & w^{13} & w^{11} & w^9 & w^7 & w^5 & w^3 & w^1 & \end{bmatrix}
\] (34a)

where
\[
w = \exp(-j2\pi/N), \quad N = 32.
\] (34b)

**Step 1**: The element \( a(0, 0) \) is fixed as
\[
a(0, 0) = g(0, 0) = \exp(-j2\pi/N).
\] (35)

**Step 2**: The element \( a(1, 0) \) is determined so as to satisfy
\[
a(1, 0) = \exp(-j2\pi/(1, 0)/N)
\] (36a)

where
\[
a(1, 0) = 1.
\] (36b)

The element \( g(1, 0) \) of \( F_{11}(N/4) \) with \( q(1, 0) = 3 \) is used for \( a(1, 0) \).

**Step 3**: The elements \( a(0, N/8 - i), 2 \leq i \leq N/8 - 1 \) are determined using \( a(1, 0) \) as
\[
a(0, N/8 - i) = \exp(-j2\pi/(0, N/8 - i)/N)
\] (37a)

where
\[
(\alpha^{N/8}(1, 0))_{N/2} = \alpha(1, 0)
\] (37b)

\[
\alpha(1, 0) = 3.
\] (37c)
They become
\begin{align}
\langle \alpha(0, 1) \rangle_{N/2} &= \langle 3 \rangle_{16} = 11 \\
\langle \alpha(0, 2) \rangle_{N/2} &= \langle 3 \rangle_{16} = 9 \\
\langle \alpha(0, 3) \rangle_{N/2} &= \langle 3 \rangle_{16} = 3.
\end{align}
(38a)  
(38b)  
(38c)

\[ a(i, 0) = \exp \left( -j2\pi \alpha(i, 0)/N \right) \]  
(39a)

\[ \langle \alpha(i, 0) \rangle_{N/2} = \left( \alpha(0, \frac{N}{8} - i) \right)_{N/2} \]  
(39b)

After the row and column permutations, \( F_{11}(N/4) \) can be changed into
\[
\begin{bmatrix}
\omega^{1} & \omega^{11} & \omega^{9} & \omega^{3} & \omega^{15} & \omega^{5} & \omega^{7} & \omega^{13} \\
\omega^{2} & -\omega^{11} & \omega^{9} & \omega^{5} & \omega^{13} & -\omega^{5} & \omega^{7} & \omega^{15} \\
\omega^{3} & -\omega^{11} & -\omega^{3} & -\omega^{13} & \omega^{15} & -\omega^{5} & \omega^{7} & \omega^{15} \\
\omega^{11} & -\omega^{9} & -\omega^{15} & \omega^{13} & \omega^{15} & -\omega^{5} & \omega^{7} & \omega^{15} \\
\omega^{15} & \omega^{5} & \omega^{9} & \omega^{3} & \omega^{15} & \omega^{5} & \omega^{9} & \omega^{3} \\
\omega^{11} & -\omega^{9} & -\omega^{3} & -\omega^{15} & \omega^{13} & -\omega^{3} & -\omega^{15} & \omega^{13} \\
\omega^{15} & \omega^{5} & \omega^{9} & \omega^{3} & -\omega^{15} & \omega^{13} & -\omega^{3} & -\omega^{15} \\
\omega^{7} & \omega^{11} & -\omega^{9} & -\omega^{3} & -\omega^{15} & \omega^{13} & -\omega^{3} & -\omega^{15}
\end{bmatrix}
\]
(40)

where \( P_{1}(N/4) \) and \( P_{2}(N/4) \) are row and column permutation matrices. Equation (40) shows that the reformed \( F_{11}(N/4) \) satisfies the conditions given by (16)–(18).

**Step 5:** In the matrix \( A \), \( \alpha(1, 0) \) satisfies
\begin{align}
\langle \alpha^{2}(1, 0) \rangle_{N} &= 9 \\
\langle \alpha^{2}(1, 0) \rangle_{N} &= 27 = 11 + \frac{N}{2}.
\end{align}
(41a)  
(41b)

From Theorem 6, \( A \) can be transformed into \( H_{-1}(N/8) \) by changing the sign of the elements in the 6th column, the third row, and the first column as follows:
\[
\tilde{A} = Q_{1}AQ_{2} =
\begin{bmatrix}
-\omega^{1} & -\omega^{11} & \omega^{9} & \omega^{3} \\
-\omega^{2} & -\omega^{11} & -\omega^{9} & \omega^{3} \\
-\omega^{3} & -\omega^{11} & -\omega^{9} & -\omega^{11} \\
\omega^{11} & -\omega^{9} & -\omega^{3} & -\omega^{11}
\end{bmatrix}
\]  
(42a)

At the same time, \( B \) is automatically reformatted as
\[
\tilde{B} = Q_{1}BQ_{2} =
\begin{bmatrix}
-\omega^{15} & -\omega^{5} & \omega^{7} & \omega^{13} \\
-\omega^{13} & -\omega^{15} & -\omega^{5} & \omega^{7} \\
-\omega^{7} & -\omega^{13} & -\omega^{15} & -\omega^{5} \\
\omega^{5} & -\omega^{7} & -\omega^{13} & -\omega^{15}
\end{bmatrix}
\]  
(42b)

Sign change matrices \( Q_{1} \) and \( Q_{2} \) are given by
\[
Q_{1} =
\begin{bmatrix}
1 & 1 & 0 \\
0 & 1 & -1
\end{bmatrix}
\]  
(43a)

Further, \( (\tilde{A} \pm \tilde{B})/2 \) becomes
\[
\frac{\tilde{A} + \tilde{B}}{2} = jH_{-1}(N/8)
\]
(44a)

\[
\frac{\tilde{A} - \tilde{B}}{2} = H_{-1}(N/8)
\]
(44b)

Thus, the matrices \( (\tilde{A} \pm \tilde{B})/2 \) become the second stage circular convolution matrices having pure imaginary and real value elements, respectively.

**Block Diagrams:** Fig. 5(a) shows a whole block diagram for a 32 point DFT. The matrices \( F_{10}(N/4) \) and \( F_{11}(N/8) \) are transformed into \( H_{E_{0}}(N/8) \) and \( H_{E_{1}}(N/16) \), respectively. The \( F_{11}(N/4) \) implementation is shown in Fig. 5(b). The other matrices in the block diagram are further divided into small size matrices.

**V. Computational Complexity**

Numbers of computations, such as additions, multiplications, and circular shifts, required in the proposed algorithm are obtained following the general flowchart shown in Fig. 2. Input sequence values are assumed to be complex. The case of a real value sequence is briefly stated later. The numbers of computations are evaluated based on real computations.

**A. Addition**

Additions are required in both processes of getting \( H_{-1}(N/2^{n+2}) \) from \( F_{6}(N/2^{2}) \) and \( F_{10}(N/2^{2+n}) \), and of implementing \( H_{-1}(N/2^{n+2}) \) through NTT and INTT.

Letting the DFT matrix size \( N \) be \( 2^{L} \), the following numbers of additions are required in the matrix reformation process.
\[
F_{6}(N/2^{2}) \rightarrow H_{-1}(N/2^{n+3}) : 4 \cdot 2^{L-1}, \quad 0 \leq i \leq L-1
\]
(45)

\[
F_{10}(N/2^{2}) \rightarrow H_{-1}(N/2^{2+n}) : (i-1)4 \cdot 2^{L-1}, \quad 2 \leq i \leq L-1.
\]
(45)
matrices, the total number of additions becomes

$$O_A^{(i)} = \sum_{i=0}^{L-1} 4 \cdot 2^{L-i} + \sum_{i=2}^{L-1} 4(i-1)2^{L-i}. \quad (46)$$

The number of additions needed in the fast convolution of $H_{-1}(N/2')$, $L - i < b + 1$ is given by

$$4 \cdot 2^{L-i}(L-i). \quad (47)$$

Since the number of $H_{-1}(N/2')$ is $2(i - 2)$, additions required in computing all circular convolutions become

$$O_A^{(D)} = \sum_{i=0}^{L-1} 8(i-2)(L-i)2^{L-i}, \quad \text{if } L < b + 1. \quad (48)$$

When $b + 1 < L - 3$, there exist two approaches, depending on the modulo, as mentioned previously. In the case of modulo $2^{16} + 1$, additions are further required only in the $\sqrt{2}$ multiplication. Thus, $O_A^{(D)}$ given by (48) is modified as

Modulo $2^{16} + 1$: $O_A^{(D)} = \sum_{i=3}^{L-1} 8(i-2)(L-i)2^{L-i}$

$$+ \sum_{i=3}^{L-1} 4(i-2)2^{L-i}. \quad (49)$$

On the other hand, when modulo $2^{32} + 1$ is employed, $H_{-1}(N/2')$, $b + 2 \leq L - i$ must be broken down into $H_{-1}(2^{b+1})$, following (33). This matrix breaking down process requires the following additions:

$$2 \cdot 2^{L-i} \sum_{k=1}^{L-b-1-i} \left(\frac{3}{2}\right)^k. \quad (50)$$

Since the number of $H_{-1}(2^{b+1})$ obtained from $H_{-1}(N/2')$ is $3^{L-b-1-i}$, additions required in computing $H_{-1}(N/2')$ become

$$4 \left(b + \frac{3}{2}\right)2^{L-i}\left(\frac{3}{2}\right)^{L-b-1-i}. \quad (51)$$

The above equation includes the additions required in the $\sqrt{2}$ multiplication. Taking the repetition into account, the number of additions, which are required in the fast convolution processes with modulo $2^{32} + 1$, becomes

Modulo $2^{32} + 1$: $O_A^{(D)}$

$$= \sum_{i=3}^{L-1} 8(i-2)(L-i)2^{L-i}$$

$$+ \sum_{i=3}^{L-b-1} 2(i-2)\left\{4 \left(b + \frac{3}{2}\right)2^{L-i}\left(\frac{3}{2}\right)^{L-b-1-i} + 2 \cdot 2^{L-i} \sum_{k=1}^{L-b-1-i} \left(\frac{3}{2}\right)^k\right\} \quad (52a)$$

$$i_1 = \max \{3, L - b\}. \quad (52b)$$

The total number of additions which are required in the proposed DFT algorithm is given as a sum of $O_A^{(i)}$ and $O_A^{(D)}$.

$$O_A = O_A^{(i)} + O_A^{(D)} \quad (53)$$

B. Multiplication

Multiplications are classified into two categories, depending on the multiplicands. They include linear numbers consisting of the DFT matrix elements and fixed constants which do not depend on the input data.

Linear Multiplication: The linear multiplications are needed at the diagonal matrices in the fast convolution processes. In the case of $L - 3 \leq b + 1$, the number of them is given by

$$O_{LM} = \sum_{i=3}^{L} 4(i-2)2^{L-i}, \quad L - 3 \leq b + 1. \quad (54)$$

When $b + 1 < L - 3$, two approaches, depending on the modulo, must be considered. The fast convolution with modulo $2^{16} + 1$ does not require additional linear multiplications. On the other hand, when modulo $2^{32} + 1$ is employed, since $H_{-1}(N/2')$, $b + 1 < L - i$ must be broken down into $3^{L-b-1-i}$ matrices with $2^{b+1} \times 2^{b+1}$ size, as mentioned previously, $O_{LM}$ given by (54) is modified as

Modulo $2^{32} + 1$: $O_{LM} = \sum_{i=b}^{L} 4(i-2)2^{L-i}$

$$+ \sum_{i=3}^{L-b-2} 4(i-2)2^{L-i}\left(\frac{3}{2}\right)^{L-b-1-i} \quad (55a)$$

$$i_2 = \max \{3, L - b - 1\}. \quad (55b)$$
Fixed Constant Multiplication: At the \( i \)th stage, \( b + 1 < i \) of NTT and INTT with modulo \( 2^{16} + 1 \), \( \lambda_i \) becomes a fixed constant. Therefore, the number of the fixed constant multiplications is given by

\[
O_{PM} = \sum_{i=3}^{L-b-2} 4(i-2)2^{L-i}(L-b-1-i).
\]  

(56)

C. Circular Shift

The number of the circular shifts required in the fast convolutions also depends on the modulo, and can be counted in the same way as those of additions and multiplications. The results are provided here.

\[
O_S = \sum_{i=1}^{L-1} 4(i-2)(L-i)2^{L-i} + \sum_{i=1}^{L-b-1} 4(i-2)(b+2)2^{L-i} \quad (57a)
\]

\[
i_i = \max \{3, L-b\}. \quad (57b)
\]

D. Real Input Sequence

As the block diagram in Fig. 4 shows, the multiplications of \( j(=\sqrt{-1}) \) are performed after the fast convolutions. Therefore, if the input sequence values are real, the numbers of computations required before the multiplications of \( j \) are simply reduced to halves of those required for the complex input sequence. After the multiplication of \( j \), the numbers of computations are the same as those for the complex input sequence.

E. Computational Complexity Comparison

First, numerical examples for \( O_{A1}^{(1)}, O_{A2}^{(2)}, O_{LM}, O_{PM}, \) and \( O_S \) are given in Table I. Furthermore, the numbers of computations required in the radix 2 FFT algorithm, Winograd's algorithm, and the proposed algorithm are listed in Table II. Numerical data in these tables show the numbers of real computations for the DFT of a complex input sequence. The numbers of additions and multiplications required in the FFT algorithm are given by

\[
O_{A,FFT} = 2NL + \frac{3}{2} N(L-2)
\]

(59)

\[
O_{M,FFT} = \frac{3}{2} N(L-2)
\]

(60)

where complex multiplication is carried out using three real multiplications and three real additions [6]. Multiplications are classified into the two categories including linear and fixed constant multiplications. The minimum number of linear multiplications needed to compute the power of 2 size DFT is also contained in Table II [12].

In the proposed algorithm, one approach with modulo \( 2^{32} + 1 \) can provide the smaller numbers of multiplications, which include both the linear and fixed constant multiplications, than that by the other method with modulo \( 2^{16} + 1 \) throughout all DFT sizes. For large size DFT's, however, the modulo \( 2^{16} + 1 \) approach requires fewer numbers of additions and circular shifts than those obtained by employing modulo \( 2^{32} + 1 \). In any case, the proposed algorithm efficiency seems to be somewhat bounded by the DFT size, which is up to about \( 2^{11} = 2048 \).

Making a comparison between the FFT and the proposed algorithms, it can be read from Table II that a major number of linear multiplications in the FFT algorithm are replaced by the power of 2 multiplications. The \( 2^n \) multiplication can be easily implemented on digital machines as circular shift. The number of multiplications is reduced into about 21 percent. The
the following equation holds:

$$\langle g(i, k') \rangle_{N/2} = \langle g(i, k) \rangle_{N/2},$$  \hspace{1cm}  \text{(A5)}$$

if, and only if, $\Delta k$ satisfies

$$2\Delta k(2i + 1) = mN + \delta \frac{N}{2}, \quad m : \text{integer},$$

$$\delta = 0 \text{ or } 1. \hspace{1cm} \text{(A6)}$$

The following combinations of $m$ and $\delta$ exist:

$$m \neq 0, \quad \delta = 1 \hspace{1cm} \text{(A7a)}$$

$$m \neq 0, \quad \delta = 0 \hspace{1cm} \text{(A7b)}$$

$$m = 0, \quad \delta = 1. \hspace{1cm} \text{(A7c)}$$

Under the conditions given by (A7a), (A7b), and (A7c), $\Delta k$ is required to be at least $N/4$, $N/2$, and $N/4$, respectively, in order to satisfy (A6). From (A3), however, the maximum value of $\Delta k$ is $N/4 - 1$ and the above requirement is not satisfied. This means (A6) and, at the same time (A5), do not hold. The same discussion is valid for the row. Q.E.D.

**APPENDIX 2**

**PROOF OF THEOREM 2**

$N$ is assumed to satisfy

$$16 \leq N. \hspace{1cm} \text{(A8)}$$

It is easily proved that Theorem 2 holds for $N = 16$. Now, let the following equation hold for any $N$ satisfying (A8):

$$\langle (2n + 1)^2 \rangle_{N/2} = \frac{N}{2} + 1, \quad 0 \leq n \leq \frac{N}{2} - 1. \hspace{1cm} \text{(A9)}$$

Using the residue modulo of $2N$, (A9) is rewritten as

$$\langle (2n + 1)^2 \rangle_{2N} = mN + \frac{N}{2} + 1, \quad m : \text{integer}. \hspace{1cm} \text{(A10)}$$

Furthermore, both sides of (A10) are squared:

$$\langle (2n + 1)^4 \rangle_{2N} = \left( mN + \frac{N}{2} + 1 \right)^2 \equiv N + 1. \hspace{1cm} \text{(A11)}$$

This equation shows that Theorem 2 holds for the residue modulo of $2N$. Thus, following the above recurrence formula, starting from residue modulo 16, Theorem 2 can be proved. Q.E.D.

**APPENDIX 3**

**PROOF OF THEOREM 3**

First, row and column permutations are derived by which elements at the 0th row and 0th column of $A$ satisfy (15) and (17). Since $a(0, 0)$ is fixed to $g(0, 0)$ where $g(0, 0) = 1$, and from (15), it is necessary that $\beta(0, 0)$ satisfies

$$\langle \beta^2(0, 0) \rangle_N = 1. \hspace{1cm} \text{(A12)}$$
From Theorem 1, \( \beta(0, 0), \alpha \) is generally expressed by \( 2n + 1 + \delta N/2 \). Substitute \( 2n + 1 + \delta N/2 \) into (A12):

\[
\left( \frac{2n + 1 + \delta}{2} \right)^{N} = (4n^{2} + 4n + 1)N, \quad 0 \leq n \leq \frac{N}{4} - 1.
\]

(A13)

Therefore, \( n \) is required to satisfy

\[
4n(n+1) = mN, \quad m : \text{integer},
\]

(A14)

Taking the range of \( n \)

\[
0 \leq n \leq \frac{N}{4} - 1
\]

(A15)

into account, \( \beta(0, 0) \) is obtained as

\[
\beta(0, 0) = \frac{N}{2} - 1.
\]

(A16)

Thus, \( \beta(0, 0) \) satisfying (A12) exists among \( 2n + 1, 0 \leq n \leq \frac{N}{2} - 1 \).

From (17) for the 0th and first rows, the following recurrence formulas must be satisfied.

\[
\left( \alpha(1, 0) \alpha \left( 0, \frac{N}{8} - i \right) \right)_{N/2} = \left( \alpha \left( \frac{N}{8} - i - 1, 0 \right) \right)_{N/2},
\]

\[
1 \leq i \leq \frac{N}{8} - 1
\]

(A17)

and

\[
\left( \alpha(1, 0) \alpha \left( 0, \frac{N}{8} - 1 \right) \right)_{N/2} = \alpha(1, 0)_{N/2}.
\]

(A18)

Therefore, \( \alpha(N/8 - i, 0) \) is expressed using \( \alpha(1, 0) \) as

\[
\left( \alpha \left( 0, \frac{N}{8} - i \right) \right)_{N/2} = \alpha(1, 0)_{N/2}.
\]

(A19)

At the same time, \( \alpha(1, 0) \) is required to satisfy

\[
\left( \alpha \left( 1, 0 \right) \right)_{N/2} = 1.
\]

(A20)

Since, from Theorem 2, a number satisfying (A20) always exists among \( 2n + 1, 0 \leq n \leq \frac{N}{2} - 1 \), this number is assigned to \( \alpha(1, 0) \). Furthermore, from (17), \( \alpha(i, 0)_{N/2} \) is required to be equal to \( \alpha(0, N/8 - i)_{N/2} \); then

\[
\left( \alpha(i, 0) \right)_{N/2} = \alpha(1, 0)_{N/2}.
\]

(A21)

Since \( \alpha(1, 0) \) is \( 2n + 1, \alpha(0, N/8 - i) \) satisfying \( A19 \) also becomes a number among \( 2n + 1, 0 \leq n \leq \frac{N}{2} - 1 \). Furthermore, since

\[
\left( \alpha(1, 0) \right)_{N/2} \neq 1,
\]

(A22)

\( \alpha(0, N/8 - i) \) and \( \alpha(0, N/8 - i') \), \( i \neq i' \) are different from each other. Thus, \( \alpha(0, N/8 - i) \) and \( \alpha(i, 0) \) satisfying (A19) and (A21) can be chosen from \( g(0, k) \) and \( g(i, 0) \), respectively.

Next, after the elements of the 0th row and 0th column are determined so as to satisfy \( A19 \) and (A21), it can be proved that (17) holds for elements included in arbitrary rows and columns of \( A \), as follows.

An element \( a(i, k) \), \( i \neq 0 \) and \( k \neq 0 \) can be expressed using \( \alpha(i, 0) \) and \( \alpha(0, k) \) as

\[
a(i, k) = \exp \left( -\beta 2\pi \alpha(1, 0) \alpha(0, k)/N \right), \quad 1 \leq i, k \leq \frac{N}{8} - 1.
\]

(A23)

From \( A19 \) and (A21),

\[
\left( \alpha(i, 0) \alpha(0, k) \right)_{N/2} = \left( \alpha \left( \frac{N}{8} - i - 1, 1 \right) \right)_{N/2}.
\]

(A24)

Then

\[
\left( \alpha(i + 1, 0) \alpha(0, k + 1) \right)_{N/2} = \left( \alpha(i, 0) \alpha(0, k) \right)_{N/2}.
\]

(A25)

This proves (17a). In a similar way,

\[
\left( \alpha(i, 0) \alpha \left( 0, \frac{N}{8} - 1 \right) \right)_{N/2} = \left( \alpha \left( \frac{N}{8} - 1, 1 \right) \right)_{N/2}
\]

(A26)

is obtained, and (17b) is proved.

From the row and column permutations in \( A \), the permutations for \( B \) are uniquely determined as follows. Elements in the 0th column are expressed by

\[
b(i, 0) = \exp \left( -\beta 2\pi \alpha(i, 0) \beta(0, 0)/N \right)
\]

(A27)

where \( \beta(0, 0) \) is \( N/2 - 1 \), as given by (A16). The following condition for \( \beta(1, 0) \) is obtained.

\[
\left( \beta \left( \frac{N}{8} - 1, 0 \right) \right)_{N/2} = \left( \alpha \left( \frac{N}{8} - 1, 1 \right) \right)_{N/2} = 1
\]

(A28)

where

\[
16 \leq N.
\]

The other elements in the 0th column are expressed by

\[
\beta(i, 0) = \left( \alpha(i, 0) \beta(0, 0) \right)_{N} = \left( \alpha(i, 0) \left( \frac{N}{2} - 1 \right) \right)_{N},
\]

\[
1 \leq i \leq \frac{N}{8} - 1.
\]

(A29a)

Since \( \alpha(i, 0) = 2n + 1, 1 \leq n \leq N/2 - 1, \beta(i, 0) \) becomes

\[
\beta(i, 0) = \left( \frac{N}{2} - \alpha(i, 0) \right)_{N}.
\]

(A29b)

Furthermore, elements in the 0th row are expressed by

\[
\beta(0, k) = \left( \alpha(0, k) \beta(0, 0) \right)_{N}, \quad 1 \leq k \leq \frac{N}{8} - 1
\]

(A30a)

\[
= \left( \alpha(0, k) \left( \frac{N}{2} - 1 \right) \right)_{N}
\]

(A30b)
\[ b(i, k) = \exp\left(-j2\pi i k/N\right) \]

From (A30c),

\[ b(i, k) = \exp\left(-j2\pi \left(\frac{N}{2} - \alpha(i, 0)\alpha(0, k)\right)\right)/N. \]

Therefore, \( b(i, k) \) can be rewritten as

\[ b(i, k) = -\exp\left(j2\pi \alpha(i, 0)\alpha(0, k)/N\right). \]

From (A23), \( b(i, k) \) is related to \( a(i, k) \) as

\[ b(i, k) = -a^*(i, k). \]

Equation (18) is proved by (A34). Furthermore, (17c) and (17d) can be proved taking into account the relation between \( b(i, k) \) and \( a(i, k) \), and the \( \alpha(i, k) \) property given by (17a) and (17b).

Q.E.D.

**APPENDIX 4**

**PROOF OF THEOREM 4**

From Theorem 3, \( a(i, k) \) and \( b(i, k) \) are related by

\[ b(i, k) = -a^*(i, k). \]

From this relation, \( a_\pm(i, k) \) are easily obtained as

\[ a_+(i, k) = (a(i, k) - a^*(i, k))/2 = j \text{ Im} \left(a(i, k)\right) \]

\[ a_-(i, k) = (a(i, k) + a^*(i, k))/2 = \text{ Re} \left(a(i, k)\right). \]

Q.E.D.

**APPENDIX 5**

**PROOF OF THEOREM 5**

First, under the condition

\[ i \geq k, \]

\( \gamma(i, k) \) is expressed by

\[ \gamma(i, k) = \gamma(i, 0) + k - 1 \]

From (27b) and a \( \gamma(i, k) \) value, which is an odd number,

\[ \gamma(i, k) = \gamma^\prime(1, 0) + \frac{N}{2} \]

Thus

\[ c(i, k) = -c(i - k, 0). \]

Next, in the case of

\[ i < k, \]

the expressions (A38) and (A39) are modified as

\[ \gamma(i, k) = \gamma(i, 0) + i - k \]

and

\[ c(i, k) = c(i - k, 0). \]

Furthermore, the following relation is also obtained

\[ \gamma(i, N' - 1) = \gamma(1, 0)N' + i - k \]

This means

\[ c(i, N' - 1) = c(i + 1, 0). \]

Equations (A39), (A42), and (A44) show that the structure of \( C \) is the same as that of \( H_{-1}(N') \), except for the signs of the \( i \)th column elements. Therefore, the matrix \( C \) can be changed into the second stage convolution matrix \( H_{-1}(N') \) by reversing the signs of the \( k \)th column elements.

Q.E.D.

**APPENDIX 6**

**PROOF OF THEOREM 6**

When \( i \) is an element of the integer set \( \Omega \), a factor \( \alpha(i, k) \) for \( a(i, k) \) can be expressed by

\[ \alpha(i, k) = \langle a(i, 0)\alpha(0, k) \rangle_N \]

\[ = \langle a(1, 0)\alpha(0, k) \rangle_N + \frac{N}{2}. \]

If \( \alpha(0, k) \) satisfies

\[ \alpha(0, k) = \alpha(i, 0) = \alpha(1, 0)N + \frac{N}{2}. \]

then

\[ \alpha(i, k) = \alpha(1, 0) + \frac{N}{2}. \]

On the other hand, if the number \( 8N' - k \) is included in the set \( \Omega \),

\[ \alpha(0, k) = \alpha(1, 0)N + \frac{N}{2}, \]

then

\[ \alpha(i, k) = \alpha(1, 0) + \frac{N}{2}. \]
Comparing expressions (27), (A47), and (A49), it can be shown that the matrix $A$ structure is the same as that obtained by changing the signs of the $i$th row and the $(N/8 - i)$th column elements of $C$ where $i$ is included in the integer set $\Omega$. Therefore, taking into account the sign change rule for $C$ given by Theorem 5, $A$ can be transformed into a matrix having the same structure of $H_{F}$ $(N/8)$ through changing the signs of the $i$th column, $i$th row, and $(N/8 - i)$th column elements.

Q.E.D.

REFERENCES


