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 calculation 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 multiplications 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 $x = (x_0, x_1, \cdots, x_{N-1})^t$ and $y = (y_0, y_1, \cdots, y_{N-1})^t$ be input and output sequences, respectively, the circular convolution is expressed as follows:

$$y = Hx \tag{1a}$$

$$H = \begin{bmatrix} h_0 & h_1 & h_2 & \cdots & h_{N-1} \\ h_{M-1} & h_0 & h_1 & \cdots & h_{N-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ h_2 & h_3 & h_4 & \cdots & h_1 \\ h_1 & h_2 & h_3 & \cdots & h_0 \end{bmatrix} \tag{1b}$$

where $h = h_0, h_1, \cdots, h_{N-1})^t$ is an impulse response of a system and $(\cdot\cdot)^t$ denotes the transposed vector. $H_\lambda(N)$ is used to denote a matrix whose element at the ith row and kth column is given by

$$\begin{aligned} h_\lambda(i, k) &= h(i, k), \quad i \leqslant k \\ &= \lambda h(i, k), \quad i > k. \end{aligned} \tag{2}$$

$H_\lambda(N)$ is further divided into submatrices as

$$H_\lambda(N) = \begin{bmatrix} A & B \\ \lambda B & A \end{bmatrix}. \tag{3}$$

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

$$H_\lambda(N) = \begin{bmatrix} A & B \\ \lambda B & A \end{bmatrix} = \begin{bmatrix} I(N/2) & -I(N/2) \\ \bar{\lambda} I(N/2) & \bar{\lambda} I(N/2) \end{bmatrix} \cdot \begin{bmatrix} (A + \bar{\lambda} B)/2 & 0 \\ 0 & (A - \bar{\lambda} B)/2 \end{bmatrix} \begin{bmatrix} I(N/2) & \bar{\lambda} - {}^1 I(N/2) \\ -I(N/2) & \bar{\lambda}^{-1} I(N/2) \end{bmatrix} \tag{4a}$$

Manuscript received July 11, 1983; revised September 1, 1984.

The author is with the Transmission Division, NEC Corporation, Nakahara-ku, Kawasaki, 211 Japan.

0096-3518/85/1000-1197$01.00

where $I(N/2)$ is an $(N/2) \times (N/2)$ size unit matrix and $\tilde{\lambda}$ satisfies

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

Equation (4) shows the case of radix 2. A block diagram showing (4a) execution is illustrated in Fig. 1. It is easily proved that the matrices $(A \pm \tilde{\lambda}B)/2$ have the $H_{\pm\lambda}(N/2)$ 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 λ and $\tilde{\lambda}$. 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 ith row and kth column, then

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

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

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 ith row and kth column is given by

$$t_M\left(i, \left\langle \left[\frac{i}{M}\right] + iM \right\rangle_N\right) = 1, \tag{6a}$$

$$t_M(i, k) = 0, \qquad k \neq \left\langle \left[\frac{i}{M}\right] + iM \right\rangle_N \tag{6b}$$

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

where notations $[i/M]$ and $\langle\cdot\rangle_N$ 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.

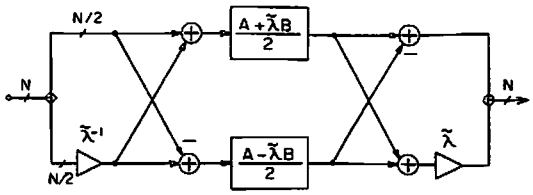

Fig. 1. Elemental block diagram for radix 2 butterfly structure fast convolution.

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

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

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, $H_{-1}(N/8)$ defined by (1) and (2). It is possible to transform the submatrices, obtained after further decimations, into the circular matrices at the mth stages $(2 < m)$. In this paper, however, the matrix transform from $F_{11}(N/4)$ to $H_{-1}(N/8)$ 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 Reformation from $F_{11}(N/4)$ to $H_{-1}(N/8)$

Letting $g(i, k)$ be an element of $F_{11}(N/4)$ at the ith row and kth column, it can be expressed from (7) and (9) as

$$g(i, k) = \exp(-j2\pi(2i+1)(2k+1)/N)$$

$$0 \leqslant i, k \leqslant \frac{N}{4} - 1. \tag{11}$$

First, two theorems are given which show properties of $F_{11}(N/4)$ and will be utilized for deriving a matrix reformation procedure.

Theorem 1: Letting $g(i, k)$ be expressed by

$$g(i, k)=\exp(-j2\pi q(i, k)/N), \quad q(i, k): \text{odd integer}, \tag{12}$$

$q(i, k)$ satisfies

$$\langle q(i, k)\rangle_{N/2}=2n+1, \quad 0\leqslant n\leqslant\frac{N}{4}-1 \tag{13a}$$

$$\langle q(i, k)\rangle_{N/2}\neq\langle q(i, k')\rangle_{N/2}, \quad k\neq k' \tag{13b}$$

$$\langle q(i, k)\rangle_{N/2}\neq\langle q(i', k)\rangle_{N/2}, \quad i\neq i'. \tag{13c}$$

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

Theorem 2: An integer n satisfying

$$\langle(2n+1)^{\frac{N}{8}}\rangle_N=\frac{N}{2}+1, \quad 0<n\leqslant\frac{N}{2}-1 \tag{14}$$

always exists.

Next, the element $g(0, 0)$ is assumed to be fixed in the row and column permutation process for $F_{11}(N/4)$. The circular matrices not satisfying this assumption can be easily obtained by further permuting the rows or columns.

From the $F_{11}(N/4)$ properties given by Theorems 1 and 2, the next theorem concerning how to permute the rows and columns of $F_{11}(N/4)$ is derived.

Theorem 3: $F_{11}(N/4)$ can be transformed by permuting the rows and columns into

$$P_1(N/4)F_{11}(N/4)P_2(N/4)=\begin{bmatrix}A & B\\ B & A\end{bmatrix} \tag{15}$$

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 ith and kth column of A and B, respectively, and be expressed by

$$a(i, k)=\exp(-j2\pi\alpha(i, k)/N) \tag{16a}$$

$$b(i, k)=\exp(-j2\pi\beta(i, k)/N)$$

$$0\leqslant i, k\leqslant\frac{N}{8}-1 \tag{16b}$$

where $\alpha(i, k)$ and $\beta(i, k)$ are odd numbers.

1) $\alpha(i, k)$ and $\beta(i, k)$ satisfy

$$\langle\alpha(i+1, k+1)\rangle_{N/2}=\langle\alpha(i, k)\rangle_{N/2}, \quad 0\leqslant i, k\leqslant\frac{N}{8}-2 \tag{17a}$$

$$\langle\alpha(i+1, 0)\rangle_{N/2}=\left\langle\alpha\left(i, \frac{N}{8}-1\right)\right\rangle_{N/2}, \quad 0\leqslant i\leqslant\frac{N}{8}-2 \tag{17b}$$

$$\langle\beta(i+1, k+1)\rangle_{N/2}=\langle\beta(i, k)\rangle_{N/2}, \quad 0\leqslant i, k\leqslant\frac{2}{8}-2 \tag{17c}$$

$$\langle\beta(i+1, 0)\rangle_{N/2}=\left\langle\beta\left(i, \frac{N}{8}-1\right)\right\rangle_{N/2}, \quad 0\leqslant i\leqslant\frac{N}{8}-2. \tag{17d}$$

2) $a(i, k)$ and $b(i, k)$ are related by

$$a(i, k)=-b^*(i, k) \tag{18}$$

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: $a(0, 0)=g(0, 0)$. (19)

Step 2: $a(1, 0)=\exp(-j2\pi\alpha(1, 0)/N)$ (20a)

$$\langle\alpha^{N/8}(1, 0)\rangle_{N/2}=1. \tag{20b}$$

Step 3: $a\left(0, \frac{N}{8}-i\right)=\exp\left(-j\pi\alpha\left(0, \frac{N}{8}-i\right)\Big/N\right)$ (21a)

$$\left\langle\alpha\left(0, \frac{N}{8}-i\right)\right\rangle_{N/2}=\langle\alpha^i(1, 0)\rangle_{N/2}$$

$$2\leqslant i\leqslant\frac{N}{8}-1. \tag{21b}$$

Step 4: $a(i, 0)=\exp(-j2\pi\alpha(i, 0)/N)$ (22a)

$$\langle\alpha(i, 0)\rangle_{N/2}=\left\langle\alpha\left(0, \frac{N}{8}-i\right)\right\rangle_{N/2}$$

$$2\leqslant i\leqslant\frac{N}{8}-1. \tag{22b}$$

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

From (4), the matrix given by (15) is divided into

$$\begin{bmatrix}A & B\\ B & A\end{bmatrix}=\begin{bmatrix}1 & -1\\ -1 & -1\end{bmatrix}\cdot\begin{bmatrix}(A+B)/2, & 0\\ 0, & (A-B)/2\end{bmatrix}\begin{bmatrix}1 & -1\\ -1 & -1\end{bmatrix}. \tag{23}$$

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 ith row and kth column, respectively, $a_\pm(i, k)$ are given by

$$a_+(i, k)=j\ \mathrm{Im}\ (a(i, k)) \tag{24a}$$

$$a_-(i, k)=\mathrm{Re}\ (a(i, k)) \tag{24b}$$

where Im $(\cdot)$ and 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

$$N' < N. \tag{25}$$

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

$$c(i, k) = \exp(-j2\pi\gamma(i, k)/N), \quad \gamma(i, k) = \text{odd number} \tag{26}$$

where $\gamma(i, k)$ satisfies

$$\gamma(0, 0) = 1 \tag{27a}$$

$$\langle \gamma^{N'}(1, 0) \rangle_N = \frac{N}{2} + 1 \tag{27b}$$

$$\gamma(i, 0) = \langle \gamma^i(1, 0) \rangle_N, \quad 2 \leqslant i \leqslant N' - 1 \tag{27c}$$

$$\gamma(0, k) = \gamma(N' - k, 0) \tag{27d}$$

$$\gamma(i, k) = \langle \gamma(i, 0)\gamma(0, k) \rangle_{N'} \quad 1 \leqslant i, k \leqslant N' - 1. \tag{27e}$$

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 Ω be a set of integer numbers, whose element i satisfies

$$a(i, k) = \exp(-j2\pi\alpha(i, k)/N) \tag{28}$$

$$\alpha(i, 0) = \langle \alpha^i(1, 0) \rangle_N + \frac{N}{2}. \tag{29}$$

The matrix A can be transformed into $H_{-1}(N/8)$ by changing the polarity of elements included in the 0th column, ith row, and $(N/8 - i)$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 ith column, and changing the sign of elements of the $(N - 1)$th column. Through these reformations, 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 λ 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 $F_0(N)$ and $F_{10}(N/4)$.

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 $j = \sqrt{-1}$ is performed at the output, the elements of $H^I_{-1}(N/8)$ have real values. The concrete element values of $H^R_{-1}(N/8)$ 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],

$$M = 2^{2^b} + 1, \tag{30}$$

the multiplicands, which appear at the ith stage $1 \leqslant i \leqslant b + 1$, become the power of 2.[1] The multiplicands λ_i at the ith stage satisfies the recurrence formula

$$\lambda_i^2 = \lambda_{i-1}, \quad 1 \leqslant i \tag{31a}$$

$$\lambda_0 = -1. \tag{31b}$$

In the ith stage, $i \leq b$, λ_i can be expressed by

$$\lambda_i = 2^{2^{b-i}}, \quad 1 \leqslant i \leqslant b. \tag{32a}$$

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

$$\lambda_{b+1} = 2^{2^{b-2}}(2^{2^{b-1}} - 1). \tag{32b}$$

[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.

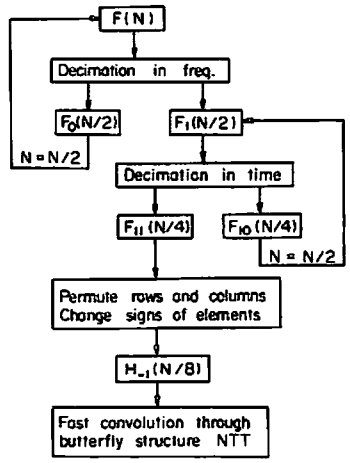

Fig. 2. General flowchart for new DFT algorithm.

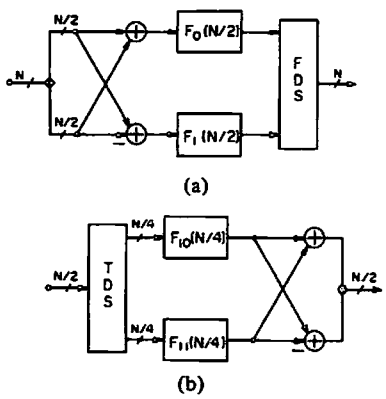

Fig. 3. Block diagrams showing decimations in frequency (a) and in time (b). FDS and TDS are frequency and time decimation shuffles, respectively.

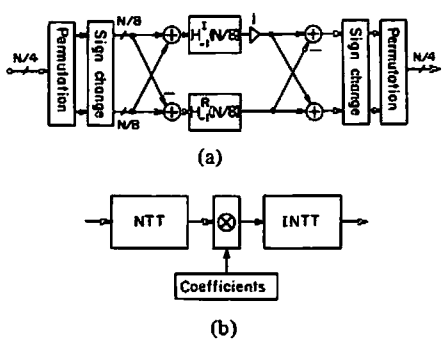

Fig. 4. (a) Matrix reformation process from $F_{11}(N/4)$ to $H_{-1}^{R,I}(N/8)$. (b) Fast convolution through NTT and inverse NTT.

As a whole, from the first stage to the $(b + 1)$th stage, the multiplications of λ_i can be replaced by circular shifts. When $H_{-1}(N/8)$ 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 $2^t\sqrt{2}$, $1 \leq t \leq 11$ by elements in the residue number system. Therefore, the one-dimensional butterfly structure can be applied. Multiplicands in the ith 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, $2^{5+2} = 128$, 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].

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

Matrices $B - A$, A, and $\lambda B - A$ have the same structure as $H_\lambda(M)$ 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:

$$F_{11}(N/4) = \begin{bmatrix} w^1 & w^3 & w^5 & w^7 & w^9 & w^{11} & w^{13} & w^{15} \\ w^3 & w^9 & w^{15} & -w^5 & -w^{11} & w^1 & w^7 & w^{13} \\ w^5 & w^{15} & -w^9 & w^3 & w^{13} & -w^7 & w^1 & w^{11} \\ w^7 & -w^5 & w^3 & -w^1 & -w^{15} & w^{13} & -w^{11} & w^9 \\ w^9 & -w^{11} & w^{13} & -w^{15} & -w^1 & w^3 & -w^5 & w^7 \\ w^{11} & w^1 & -w^7 & w^{13} & w^3 & -w^9 & w^{15} & w^5 \\ w^{13} & w^7 & w^1 & -w^{11} & -w^5 & w^{15} & w^9 & w^3 \\ w^{15} & w^{13} & w^{11} & w^9 & w^7 & w^5 & w^3 & w^1 \end{bmatrix} \quad (34a)$$

where

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

Step 1: The element $a(0, 0)$ is fixed as

$$a(0, 0) = g(0, 0) = \exp(-j2\pi/N). \quad (35)$$

Step 2: The element $a(1, 0)$ is determined so as to satisfy

$$a(1, 0) = \exp(-j2\pi\alpha(1, 0)/N) \quad (36a)$$

where

$$\langle \alpha^{N/8}(1, 0) \rangle_{N/2} = 1. \quad (36b)$$

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

$$a(0, N/8 - i) = \exp(-j2\pi\alpha(0, N/8 - i)/N) \quad (37a)$$

where

$$\langle \alpha(0, N/8 - i) \rangle_{N/2} = \langle \alpha^i(1, 0) \rangle_{N/2} \quad (37b)$$

$$\alpha(1, 0) = 3. \quad (37c)$$

They become

$$\langle \alpha(0,\ 1)\rangle_{N/2} = \langle 3^3\rangle_{16} = 11 \tag{38a}$$

$$\langle \alpha(0,\ 2)\rangle_{N/2} = \langle 3^2\rangle_{16} = 9 \tag{38b}$$

$$\langle \alpha(0,\ 3)\rangle_{N/2} = \langle 3^1\rangle_{16} = 3. \tag{38c}$$

$$a(i,\ 0) = \exp\ (-j2\pi\alpha(i,\ 0)/N) \tag{39a}$$

$$\langle \alpha(i,\ 0)\rangle_{N/2} = \left\langle \alpha\left(0,\ \frac{N}{8} - i\right)\right\rangle_{N/2}. \tag{39b}$$

After the row and column permutations, $F_{11}(N/4)$ can be changed into

$$P_1(N/4)F_{11}(N/4)P_2(N/4)$$

$$= \left[\begin{array}{cccc:cccc} w^1 & w^{11} & w^9 & w^3 & w^{15} & w^5 & w^7 & w^{13} \\ w^3 & w^1 & -w^{11} & w^9 & w^{13} & w^{15} & -w^5 & w^7 \\ w^9 & w^3 & -w^1 & -w^{11} & w^7 & w^{13} & -w^{15} & -w^5 \\ w^{11} & -w^9 & w^3 & w^1 & w^5 & -w^7 & w^{13} & w^{15} \\ \hdashline w^{15} & w^5 & w^7 & w^{13} & w^1 & w^{11} & w^9 & w^3 \\ w^{13} & w^{15} & -w^5 & w^7 & w^3 & w^1 & -w^{11} & w^9 \\ w^7 & w^{13} & -w^{15} & -w^5 & w^9 & w^3 & -w^1 & -w^{11} \\ w^5 & -w^7 & w^{13} & w^{15} & w^{11} & -w^9 & w^3 & w^1 \end{array}\right]$$

$$= \begin{bmatrix} A & B \\ B & A \end{bmatrix} \tag{40}$$

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

$$\langle \alpha^2(1,\ 0)\rangle_N = 9 \tag{41a}$$

$$\langle \alpha^3(1,\ 0)\rangle_N = 27 = 11 + \frac{N}{2}. \tag{41b}$$

From Theorem 6, A can be transformed into $H_{-1}(N/8)$ by changing the sign of the elements in the 0th column, the third row, and the first column as follows:

$$\tilde{A} = Q_1 A Q_2 = \begin{bmatrix} -w^1 & -w^{11} & w^9 & w^3 \\ -w^3 & -w^1 & -w^{11} & w^9 \\ -w^9 & -w^3 & -w^1 & -w^{11} \\ w^{11} & -w^9 & -w^3 & -w^1 \end{bmatrix}. \tag{42a}$$

At the same time, B is automatically reformed as

$$\tilde{B} = Q_1 B Q_2 = \begin{bmatrix} -w^{15} & -w^5 & w^7 & w^{13} \\ -w^{13} & -w^{15} & -w^5 & w^7 \\ -w^7 & -w^{13} & -w^{15} & -w^5 \\ w^5 & -w^7 & -w^{13} & -w^{15} \end{bmatrix}. \tag{42b}$$

Sign change matrices Q_1 and Q_2 are given by

$$Q_1 = \begin{bmatrix} 1 & & & 0 \\ & 1 & & \\ & & 1 & \\ 0 & & & -1 \end{bmatrix} \tag{43a}$$

$$Q_2 = \begin{bmatrix} -1 & & & 0 \\ & -1 & & \\ & & 1 & \\ 0 & & & 1 \end{bmatrix}. \tag{43b}$$

Furthermore, $(\tilde{A} \pm \tilde{B})/2$ becomes

$$\frac{\tilde{A}+\tilde{B}}{2} = jH^I_{-1}(N/8)$$

$$= j \begin{bmatrix} -S(1) & -S(5) & S(7) & S(3) \\ -S(3) & -S(1) & -S(5) & S(7) \\ -S(7) & -S(3) & -S(1) & -S(5) \\ S(5) & -S(7) & -S(3) & -S(1) \end{bmatrix},\ S(i)$$

$$= \sin\ (2\pi i/N) \tag{44a}$$

$$\frac{\tilde{A}-\tilde{B}}{2} = H^R_{-1}(N/8)$$

$$= \begin{bmatrix} -C(1) & C(5) & -C(7) & C(3) \\ -C(3) & -C(1) & C(5) & -C(7) \\ C(7) & -C(3) & -C(1) & C(5) \\ -C(5) & C(7) & -C(3) & -C(1) \end{bmatrix},\ C(i)$$

$$= \cos\ (2\pi i/N). \tag{44b}$$

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 $F_{11}(N/4)$ and $F_{11}(N/8)$ are transformed into $H^R_{-1}(N/8)$ and $H^R_{-1}(N/16)$, 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 $H_{-1}(N/2^{i+3})$ from $F_0(N/2^i)$ and $F_{10}(N/2^{i+2})$, and of implementing $H_{-1}(N/2^{i+3})$ 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.

$$F_0(N/2^i) \rightarrow H_{-1}(N/2^{i+3}) : 4 \cdot 2^{L-i},\quad 0 \leqslant i \leqslant L-1$$

$$F_{10}(N/2^i) \rightarrow H_{-1}(N/2^{i+1}) : (i-1)4 \cdot 2^{L-i},\quad 2 \leqslant i \leqslant L-1. \tag{45}$$

Since the same operations are repeated on the reduced size

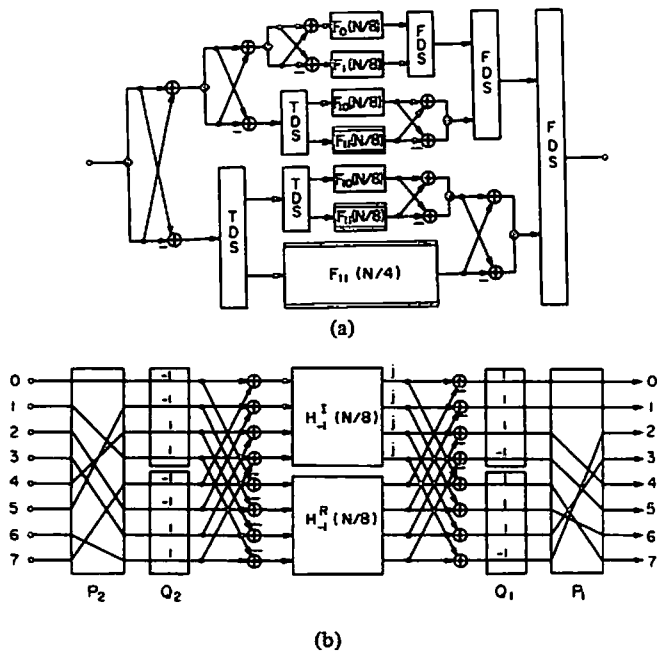

Fig. 5. (a) Block diagram for new DFT algorithm (32 point DFT). (b) $F_{11}(N/4)$ implementation through fast convolution.

matrices, the total number of additions becomes

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

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

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

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

$$O_A^{(2)} = \sum_{i=3}^{L-1} 8(i-2)(L-i)2^{L-i}, \quad L-3 < b+1. \tag{48}$$

When $b + 1 \leqslant L - 3$, 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, $O_A^{(2)}$ given by (48) is modified as

$$\text{Modulo } 2^{16}+1 : O_A^{(2)} = \sum_{i=3}^{L-1} 8(i-2)(L-i)2^{L-i} + \sum_{i=3}^{L-b-1} 4(i-2)2^{L-i}. \tag{49}$$

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

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

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

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

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

$$\text{Modulo } 2^{32}+1 : O_A^{(2)} = \sum_{i=i_1}^{L-1} 8(i-2)(L-i)2^{L-i} + \sum_{i=3}^{L-b-1} 2(i-2)\left\{4\left(b+\frac{3}{2}\right)2^{L-i}\left(\frac{3}{2}\right)^{L-b-1-i} + 2 \cdot 2^{L-i}\sum_{k=1}^{L-B-1-i}\left(\frac{3}{2}\right)^k\right\} \tag{52a}$$

$$i_1 = \max\{3,\ L-b\}. \tag{52b}$$

The total number of additions which are required in the proposed DFT algorithm is given as a sum of $O_A^{(1)}$ and $O_A^{(2)}$.

$$O_A = O_A^{(1)} + O_A^{(2)} \tag{53}$$

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 $L - 3 \leqslant b + 1$, the number of them is given by

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

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 $H_{-1}(N/2^i)$, $b + 1 < L - i$ 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

$$\text{Modulo } 2^{32}+1 : O_{LM} = \sum_{i=i_2}^{L} 4(i-2)2^{L-i} + \sum_{i=3}^{L-b-2} 4(i-2)2^{L-i}\left(\frac{3}{2}\right)^{L-b-1-i} \tag{55a}$$

$$i_2 = \max\{3,\ L-b-1\}. \tag{55b}$$

Fixed Constant Multiplication: At the ith stage, $b + 1 < i$ of NTT and INTT with modulo $2^{16} + 1$, λ_i becomes a fixed constant. Therefore, the number of the fixed constant multiplications is given by

$$\text{Modulo } 2^{16}+1 : O_{FM}=\sum_{i=3}^{L-b-2} 4(i-2)2^{L-i}(L-b-1-i). \tag{56}$$

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.

$$\text{Modulo } 2^{16}+1 : O_S=\sum_{i=i_1}^{L-1} 4(i-2)(L-i)2^{L-i} + \sum_{i=3}^{L-b-1} 4(i-2)(b+2)2^{L-i} \tag{57a}$$

$$i_1=\max\ \{3,\ L-b\}. \tag{57b}$$

$$\text{Modulo } 2^{32}+1 : O_S=\sum_{i=i_1}^{L-1} 4(i-2)(L-i)2^{L-i} + \sum_{i=3}^{L-b-1} 4(i-2)(b+2)2^{L-i}\left(\frac{3}{2}\right)^{L-b-1-i}. \tag{58}$$

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 $O_A^{(1)}$, $O_A^{(2)}$, O_{LM}, O_{FM}, 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 value input sequence. The numbers of additions and multiplications required in the FFT algorithm are given by

$$O_{A,\text{FFT}}=2NL+\frac{3}{2}N(L-2) \tag{59}$$

$$O_{M,\text{FFT}}=\frac{3}{2}N(L-2) \tag{60}$$

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

TABLE I
NUMERICAL EXAMPLES FOR NUMBERS OF REAL COMPUTATIONS REQUIRED IN EACH PROCESS OF PROPOSED DFT ALGORITHM FOR COMPLEX INPUT SEQUENCE

DFT Size	$O_A^{(1)}$	$O_A^{(2)}$		O_{LM}		O_{FM}	O_S	
		16*	32**	16	32	16	16	32
32	336	96	96	44	44	0	48	48
64	712	368	368	104	104	0	184	184
128	1472	1152	1152	228	228	0	576	576
256	3000	3344	3216	480	480	0	1736	1608
512	6064	8864	8608	988	988	256	4432	4432
1024	12200	22064	24752	2008	2264	1536	10200	12632
2048	24480	52672	74688	4052	5844	5888	22112	36960

Modulo : $2^{16}+1$ (*), $2^{32}+1$ (**)

TABLE II
NUMBER OF REAL COMPUTATIONS REQUIRED IN (a) FFT ALGORITHM, WINOGRAD'S ALGORITHM IN [12], PROPOSED ALGORITHM, (b) AND WFTA IN [13] FOR COMPLEX INPUT SEQUENCE

DFT Size	Radix 2 FFT		Ref.[12]	New DFT (Modulo: $2^{16}+1$)			New DFT (Modulo: $2^{32}+1$)		
	Mult**	Add	L.Mult*	Mult	Add	Shift	Mult	Add	Shift
32	144	304	36	44	432	48	44	432	48
64	384	1152	89	104	1080	184	104	1080	184
128	960	2752	204	228	2624	576	228	2624	576
256	2304	6400	445	480	6344	1736	480	6216	1608
512	5376	14592	940	1244	14928	4432	988	14672	4432
1024	12288	32768	1945	3544	34264	10200	2264	36952	12632
2048	27648	72704	3972	9940	77152	22112	5844	99168	36960

*Linear Multiplication, **Linear and Fixed Multiplications.

(a)

DFT Size	Mult	Add
30	72	384
60	144	888
120	288	2076
280	864	7148
520	1926	11352
1008	3564	34668
2520	9504	99628

(b)

number of additions is almost the same, except for a 2048 point DFT. The simple butterfly structure used in the FFT is also preserved.

When computational complexity is estimated by the linear multiplication only, Winograd's algorithm is slightly superior to the proposed algorithm. In both software and hardware implementations, however, multiplication is actually required for the fixed constant multiplicands. In these cases, the proposed algorithm becomes more efficient.

Consequently, it can be concluded that the proposed new algorithm can reduce the multiplicative complexity to the same level as that attained by using Winograd's approach, while preserving the same number of additions and the butterfly structure as in the classical FFT algorithm.

Actual implementations on a general purpose computer and a microprocessor system are now under investigation. Results will be reported in another paper.

IV. Conclusion

A new algorithm for computing the DFT of the power of 2 length time sequence has been proposed in this paper. The DFT coefficient matrix is broken down into the power of 2 size circular matrices. The butterfly structure NTT is applied to implementing the circular convolutions. Compared with the radix 2 FFT, the number of multiplications, which does not include the circular shifts, can be reduced to about 21 percent, and the number of additions and the butterfly structure are preserved. When efficiency is estimated by the multiplicative complexity, which includes only the linear multiplications, the proposed algorithm is slightly inferior to Winograd's algorithm. If fixed constant multiplications are further taken into account, however, the new algorithm becomes more efficient.

Appendix 1

Proof of Theorem 1

Since

$$(2i+1)(2k+1)=2n+1+m_1\frac{N}{2}+m_2N$$

$$0\leqslant n\leqslant\frac{N}{4}-1,\quad m_1,\quad m_2=\text{integer} \tag{A1}$$

$\langle q(i,\ k)\rangle_{N/2}$ becomes

$$\langle q(i,\ k)\rangle_{N/2}=\langle(2i+1)(2k+1)\rangle_{N/2}=2n+1,\quad 0\leqslant n\leqslant\frac{N}{4}-1. \tag{A2}$$

The number of all possible values given by (A2) is $N/4$. Therefore, in order to prove (13b) and (13c), it is sufficient to show that $q(i,\ k)$ for elements included in the same row and column are different. Let k' be an integer defined by

$$k'=k+\Delta k,\quad 0<\Delta k\leqslant\frac{N}{4}-1. \tag{A3}$$

Since

$$(2i+1)(2k'+1)=(2i+1)(2k+1)+2\Delta k(2i+1),$$

$$0\leqslant i,\ k\leqslant\frac{N}{4}-1, \tag{A4}$$

the following equation holds:

$$\langle g(i,\ k')\rangle_{N/2}=\langle g(i,\ k)\rangle_{N/2}, \tag{A5}$$

if, and only if, Δk satisfies

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

$$\delta=0\text{ or }1. \tag{A6}$$

The following combinations of m and δ exist:

$$m\neq 0,\ \delta=1 \tag{A7a}$$

$$m\neq 0,\ \delta=0 \tag{A7b}$$

$$m=0,\ \delta=1. \tag{A7c}$$

Under the conditions given by (A7a), A7b), and (A7c), Δk 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 Δk 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

$$16\leqslant N. \tag{A8}$$

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

$$\langle(2n+1)^{\frac{N}{8}}\rangle_N=\frac{N}{2}+1,\quad 0<n\leqslant\frac{N}{2}-1. \tag{A9}$$

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

$$\langle(2n+1)^{\frac{N}{8}}\rangle_{2N}=mN+\frac{N}{2}+1,\quad m:\text{integer}. \tag{A10}$$

Furthermore, both sides of (A10) are squared:

$$\langle(2n+1)^{\frac{2N}{8}}\rangle_{2N}=\left\langle\left(mN+\frac{N}{2}+1\right)^2\right\rangle_{2N}=N+1. \tag{A11}$$

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 $q(0,\ 0)=1$, and from (15), it is necessary that $\beta(0,\ 0)$ satisfies

$$\langle\beta^2(0,\ 0)\rangle_N=1. \tag{A12}$$

From Theorem 1, $\langle\beta(0, 0)\rangle_N$ is generally expressed by $2n + 1 + \delta N/2$. Substitute $2n + 1 + \delta N/2$ into (A12):

$$\left\langle\left(2n+1+\delta\frac{N}{2}\right)^2\right\rangle_N=\langle 4n^2+4n+1\rangle_N,\ 0\leqslant n\leqslant\frac{N}{4}-1. \tag{A13}$$

Therefore, n is required to satisfy

$$4n(n+1)=mN,\quad m:\text{integer}, \tag{A14}$$

Taking the range of n

$$0\leqslant n\leqslant\frac{N}{4}-1 \tag{A15}$$

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

$$\beta(0,\ 0)=\frac{N}{2}-1. \tag{A16}$$

Thus, $\beta(0, 0)$ satisfying (A12) exists among $2n + 1, 0 \leqslant n \leqslant (N/2) - 1$.

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

$$\left\langle\alpha(1,\ 0)\alpha\left(0,\ \frac{N}{8}-i\right)\right\rangle_{N/2}=\left\langle\alpha\left(\frac{N}{8}-i-1,\ 0\right)\right\rangle_{N/2},\quad 1\leqslant i\leqslant\frac{N}{8}-1 \tag{A17}$$

and

$$\langle\alpha(1,\ 0)\rangle_{N/2}=\left\langle\alpha\left(0,\ \frac{N}{8}-1\right)\right\rangle_{N/2}. \tag{A18}$$

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

$$\left\langle\alpha\left(0,\ \frac{N}{8}-i\right)\right\rangle_{N/2}=\langle\alpha^i(1,\ 0)\rangle_{N/2}. \tag{A19}$$

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

$$\langle\alpha^{\frac{N}{8}}(1,\ 0)\rangle_{N/2}=1. \tag{A20}$$

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

$$\langle\alpha(i,\ 0)\rangle_{N/2}=\langle\alpha^i(1,\ 0)\rangle_{N/2}. \tag{A21}$$

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

$$\langle\alpha(1,\ 0)\rangle_{N/2}\neq 1, \tag{A22}$$

$\alpha(0, N/8 - i)$ 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

$$a(i,\ k)=\exp\ (-j2\pi\alpha(i,\ 0)\alpha(0,\ k)/N),\quad 1\leqslant i,\ k\leqslant\frac{N}{8}-1. \tag{A23}$$

From (A19) and (A21),

$$\langle\alpha(i,\ 0)\alpha(0,\ k)\rangle_{N/2}=\langle\alpha^{\frac{N}{8}+i-k}(1,\ 0)\rangle_{N/2'}. \tag{A24}$$

Then

$$\langle\alpha(i+1,\ 0)\alpha(0,\ k+1)\rangle_{N/2}=\langle\alpha(i,\ 0)\alpha(0,\ k)\rangle_{N/2}. \tag{A25}$$

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

$$\left\langle\alpha(i,\ 0)\alpha\left(0,\ \frac{N}{8}-1\right)\right\rangle_{N/2}=\langle\alpha^{i+1}(1,\ 0)\rangle_{N/2} \tag{A26}$$

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

$$b(i,\ 0)=\exp\ (-j2\pi\alpha(i,\ 0)\beta(0,\ 0)/N) \tag{A27}$$

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

$$\langle\beta^{\frac{N}{8}}(1,\ 0)\rangle_{N/2}=\left\langle\left(\alpha(1,\ 0)\left(\frac{N}{2}-1\right)\right)^{\frac{N}{8}}\right\rangle_{N/2}=\langle\alpha^{\frac{N}{8}}(1,\ 0)\rangle_{N/2}=1 \tag{A28}$$

where

$$16\leqslant N.$$

The other elements in the 0th column are expressed by

$$\beta(i,\ 0)=\langle\alpha(i,\ 0)\beta(0,\ 0)\rangle_N=\left\langle\alpha(i,\ 0)\left(\frac{N}{2}-1\right)\right\rangle_N,\quad 1\leqslant i\leqslant\frac{N}{8}-1. \tag{A29a}$$

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

$$\beta(i,\ 0)=\left\langle\frac{N}{2}-\alpha(i,\ 0)\right\rangle_N. \tag{A29b}$$

Furthermore, elements in the 0th row are expressed by

$$\beta(0,\ k)=\langle\alpha(0,\ k)\beta(0,\ 0)\rangle_N,\quad 1\leqslant k\leqslant\frac{N}{8}-1 \tag{A30a}$$

$$=\left\langle\alpha(0,\ k)\left(\frac{N}{2}-1\right)\right\rangle_N \tag{A30b}$$

$$= \left\langle \frac{N}{2} - \alpha(0,\ k) \right\rangle_N . \quad \text{(A30c)}$$

Elements in arbitrary rows and columns can be obtained using the above expressions for the 0th row and 0th column elements, as follows:

$$b(i,\ k) = \exp\ (-j2\pi\beta(i,\ 0)\alpha(0,\ k)/N) \quad \text{(A31a)}$$

$$= \exp\ (-j2\pi\alpha(i,\ 0)\beta(0,\ k)/N), \quad 1 \leqslant i,\ k \leqslant \frac{N}{8} - 1. \quad \text{(A31b)}$$

From (A30c),

$$b(i,\ k) = \exp\left(-j2\pi\left(\frac{N}{2} - \alpha(i,\ 0)\alpha(0,\ k)\right)/N\right). \quad \text{(A32)}$$

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

$$b(i,\ k) = -\exp\ (j2\pi\alpha(i,\ 0)\alpha(0,\ k)/N). \quad \text{(A33)}$$

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

$$b(i,\ k) = -a^*(i,\ k). \quad \text{(A34)}$$

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

$$b(i,\ k) = -a^*(i,\ k). \quad (18)$$

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

$$a_+(i,\ k) = (a(i,\ k) - a^*(i,\ k))/2 = j\ \mathrm{Im}\ (a(i,\ k)) \quad \text{(A35a)}$$

$$a_-(i,\ k) = (a(i,\ k) + a^*(i,\ k))/2 = \mathrm{Re}\ (a(i,\ k)). \quad \text{(A35b)}$$

Q.E.D.

Appendix 5

Proof of Theorem 5

First, under the condition

$$i \geqslant k, \quad \text{(A36)}$$

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

$$\gamma(i,\ k) = \langle \gamma^i(1,\ 0)\gamma^{N'-k}(1,\ 0) \rangle_N \quad \text{(A37a)}$$

$$= \langle \gamma^{N'+i-k}(1,\ 0) \rangle_N . \quad \text{(A37b)}$$

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

$$\gamma(i,\ k) = \langle \gamma^{i-k}(1,\ 0) \rangle_N + \frac{N}{2} \quad \text{(A38a)}$$

$$= \gamma(i-k,\ 0) + \frac{N}{2} . \quad \text{(A38b)}$$

Then

$$c(i,\ k) = -c(i-k,\ 0). \quad \text{(A39)}$$

Next, in the case of

$$i < k, \quad \text{(A40)}$$

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

$$\gamma(i,\ k) = \langle \gamma^{N'+i-k}(1,\ 0) \rangle_N = \gamma(0,\ k-i) \quad \text{(A41)}$$

and

$$c(i,\ k) = c(0,\ k-i). \quad \text{(A42)}$$

Furthermore, the following relation is also obtained

$$\gamma(i,\ N'-1) = \langle \gamma^i(1,\ 0)\gamma^{N'-N'+1}(1,\ 0) \rangle_N$$

$$= \langle \gamma^{i+1}(1,\ 0) \rangle_N = \gamma(i+1,\ 0). \quad \text{(A43)}$$

This means

$$c(i,\ N'-1) = c(i+1,\ 0). \quad \text{(A44)}$$

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 0th column elements. Therefore, the matrix C can be changed into the second stage convolution matrix $H_{-1}(N')$ by reversing the signs of the 0th column elements. Q.E.D.

Appendix 6

Proof of Theorem 6

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

$$\alpha(i,\ k) = \langle \alpha(i,\ 0)\alpha(0,\ k) \rangle_N$$

$$= \langle \alpha^i(1,\ 0)\alpha(0,\ k) \rangle_N + \frac{N}{2} . \quad \text{(A45)}$$

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

$$\alpha(0,\ k) = \alpha\left(\frac{N}{8} - k,\ 0\right) = \langle \alpha^{\frac{N}{8}-k}(1,\ 0) \rangle_N , \quad \text{(A46)}$$

then

$$\alpha(i,\ k) = \langle \alpha^{\frac{N}{8}+i-k}(1,\ 0) \rangle_N + \frac{N}{2} . \quad \text{(A47)}$$

On the other hand, if the number $8/N - k$ is included in the set Ω,

$$\alpha(0,\ k) = \langle \alpha^{\frac{N}{8}-k}(1,\ 0) \rangle_N + \frac{N}{2} , \quad \text{(A48)}$$

then

$$\alpha(i,\ k) = \langle \alpha^{\frac{N}{8}+i-k}(1,\ 0) \rangle_N . \quad \text{(A49)}$$

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 ith row and the $(N/8 - i)$th column elements of C where i is included in the integer set Ω. 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 $H_{-1}(N/8)$ through changing the signs of the 0th column, ith row, and $(N/8 - i)$th column elements. Q.E.D.

References

[1] J. W. Cooley and J. W. Tukey, "An algorithm for the machine calculation of complex Fourier series," *Math. Comput.*, vol. 19, pp. 297–301, Apr. 1965.

[2] W. T. Cochran, "What is the fast Fourier transform?," *IEEE Trans. Audio Electroacoust.*, vol. AU-15, pp. 45–55, June 1967.

[3] R. C. Singleton, "A method for computing the fast Fourier transform with auxiliary memory and limited high speed storage," *IEEE Trans. Audio Electroacoust.*, vol. AU-15, pp. 91–98, June 1967.

[4] R. C. Singleton, "An algorithm for computing the mixed radix fast Fourier transform," *IEEE Trans. Audio Electroacoust.*, vol. AU-17, pp. 93–103, June 1969.

[5] C. M. Rader and N. M. Brenner, "A new principle for fast Fourier transform," *IEEE Trans. Acoust., Speech, Signal Processing*, vol. ASSP-24, pp. 264–265, Apr. 1976.

[6] K. Nakayama, "Fast Fourier transform using mixed frequency and time decimations" (in Japanese), *IECE Japan, Rep. Tech. Meeting on Circuits Syst.*, vol. CAS 79-94, pp. 49–54, Oct. 1979.

[7] C. Caraiscos and B. Liu, "Two dimensional DFT using mixed time and frequency decimations," in *Proc. IEEE Int. Conf. Acoust., Speech, Signal Processing*, pp. 24–27, Paris, May 1982.

[8] S. Winograd, "On computing the discrete Fourier transform," *Math. Comput.*, vol. 32, pp. 175–199, Jan. 1978.

[9] H. Silverman, "An introduction to programming the Winograd Fourier transform algorithm (WFTA)," *IEEE Trans. Acoust., Speech, Signal Processing*, vol. ASSP-25, pp. 152–165, Apr. 1977.

[10] D. P. Kolba and T. W. Parks, "A prime factor FFT algorithm using high speed convolution," *IEEE Trans. Acoust., Speech, Signal Processing*, vol. ASSP-25, pp. 281–294, Aug. 1977.

[11] C. M. Rader, "Discrete Fourier transforms when the number of data samples is prime," *Proc. IEEE*, vol. 56, pp. 1107–1108, June 1968.

[12] S. Winograd, "Signal processing and complexity of computation," in *Proc. IEEE Int. Conf. Acoust., Speech, Signal Processing*, pp. 94–101, 1980.

[13] S. Winograd, "Arithmetic complexity of computations," CBMS monograph, SIAM.

[14] J. M. Pollard, "The fast Fourier transform in a finite field," *Math. Comput.*, vol. 25, pp. 365–374, Apr. 1971.

[15] C. M. Rader, "Discrete convolution via Mersenne transforms," *IEEE Trans. Comput.*, vol. C-21, pp. 1269–1273, Dec. 1972.

[16] R. C. Agarwal and C. S. Burrus, "Fast convolution using Fermat number transforms with applications to digital filtering," *IEEE Trans. Acoust., Speech, Signal Processing*, vol. ASSP-22, pp. 87–97, Apr. 1974.

[17] R. C. Agarwal and C. S. Burrus, "Fast one-dimensional convolution by multidimensional techniques," *IEEE Trans. Acoust., Speech, Signal Processing*, vol. ASSP-22, pp. 1–10, Feb. 1974.

[18] R. C. Agarwal and C. S. Burrus, "Number-theoretic transforms to implement fast digital convolution," *Proc. IEEE*, vol. 63, pp. 556–560, Apr. 1975.

[19] I. S. Reed and T. K. Truong, "The use of finite fields compute convolutions," *IEEE Trans. Inform. Theory*, vol. IT-21, pp. 208–213, Mar. 1975.

[20] R. C. Agarwal and J. W. Cooley, "New algorithms for digital convolution," *IEEE Trans. Acoust., Speech, Signal Processing*, vol. ASSP-25, pp. 392–409, Oct. 1977.

[21] I. S. Reed and T. K. Truong, "A new hybrid algorithm for computing a fast discrete Fourier transform," *IEEE Trans. Comput.*, vol. C-28, pp. 487–492, July 1979.

[22] J. H. McClellan and C. M. Rader, *Number Theory in Digital Signal Processing*, Prentice-Hall, Inc., New Jersey, 1979.

[23] K. Nakayama, "A discrete Fourier transform algorithm using fast convolution" (in Japanese), *IECE Japan, Rep. Tech. Meeting on Circuits Syst.*, vol. CAS 82-105, pp. 17–24, Nov. 1982.

[24] A. V. Oppenheim and R. W. Schafer, *Digital Signal Processing*, Prentice-Hall, Inc., New Jersey, 1975.

[25] J. H. McClellan, "Hardware realization of a Fermat number transform," *IEEE Trans. Acoust., Speech, Signal Processing*, vol. ASSP-24, pp. 216–225, June 1976.

[26] L. M. Leibowitz, "A simplified binary arithmetic for the Fermat number transform," *IEEE Trans. Acoust., Speech, Signal Processing*, vol. ASSP-24, pp. 356–359, Oct. 1976.

[27] I. S. Reed and T. K. Truong, "Complex integer convolution over a discrete sum of Galois fields," *IEEE Trans. Inform. Theory*, vol. IT-21, pp. 657–661, Nov. 1975.

[28] E. Vegh and L. M. Leibowitz, "Fast complex convolution in finite rings," *IEEE Trans. Acoust., Speech, Signal Processing*, vol. ASSP-24, pp. 343–344, Aug. 1976.

[29] H. J. Nussbaumer, "Digital filtering using complex Mersenne transforms," *IBM J. Res. Develop.*, vol. 20, pp. 498–504, Sept. 1976.

Kenji Nakayama (M'82–SM'84) received the B.E. and Dr. degrees in electronics engineering from the Tokyo Institute of Technology (TIT), Tokyo, Japan, in 1971 and 1983, respectively.

From 1971 to 1972 he was engaged in research on classical network theory at the TIT. Since he joined Nippon Electric Co., Ltd. (renamed NEC Corporation from Apr. 1983) in 1972, he has worked on the research and development of filter design techniques for *LC*, digital and switched capacitor filters, and computationally efficient algorithms in digital signal processing. He is now supervisor of the Devices Dept., Transmission Division.

Dr. Nakayama is a member of the Institute of Electronics and Communication Engineers (IECE) of Japan.