A New Method Mathematically Links Fast Fourier Transform Algorithms with Fast Cyclic Convolution Algorithms

Marvi Teixeira
Electrical Engineering Department
Polytechnic University of Puerto Rico
Ponce de Leon Ave 377, Hato Rey, P.R. 00918

Domingo Rodriguez
Electrical and Computer Engineering Department
University of Puerto Rico, Mayagüez Campus
Mayagüez, P.R. 00709-5000

Abstract — The cyclic convolution theorem is used to formally link certain factorizations of the DFT matrix to factorizations of the circulant matrices. As an example, the DFT matrix decomposition leading to the decimation in time fast Fourier transform is mathematically linked to a circulant matrix decomposition, which in turn leads to a fast cyclic convolution algorithm. Most importantly, permutations of the DFT matrix are shown to be related to permutations of the circulant matrices. It is therefore illustrated how certain factorizations, in one domain, could lead to fast algorithms in both domains, thus, providing further insight and needed unification.

I. INTRODUCTION

Some permutations of the DFT matrix are known to lead to convenient factorizations suitable to fast transform algorithms. In the past, using a methodology by analogy to the well known decimation in time and decimation in frequency techniques, several decompositions of the circulant matrices, leading to fast cyclic convolution algorithms, were successfully obtained [1], [2]. In the present work no analogy is used, instead, a formal mathematical derivation is offered, thus, establishing a general relation between certain permutations of the DFT matrix and permutations of the circulant matrices. Using this novel methodology a new algorithm is constructed, showing that decompositions of the DFT matrix (decimation in time FFT in this case), could trigger decompositions of the circulant matrices suitable to the formulation of fast cyclic convolution algorithms. The obtained algorithm has a regular structure with a high degree of parallelism making it suitable for VLSI or multiprocessor implementation. It uses 2.3^{M-1} multiplications and relates to the Walsh transform, therefore belonging to a class of algorithms developed in [1], [2], and shown in [3], to be special cases of multidimensional formulations. For a discussion of these algorithm's efficiency, structure and relation to the Walsh transform, the reader is referred to [1], [2], [3]. Reference [4] offers a detailed discussion of a linear convolution algorithm with a similar structure. Reference [5] further discuss the microprocessor implementation of algorithms with this kind of structure.

II. ALGORITHM FORMULATION

The sequences g and d are of length $N = 2^M$, $M \in Z$, its cyclic convolution s is:

$$s = g \circledast_N d \tag{1}$$

The convolution theorem states that:

$$(F_N)s = [(F_N)g] \cdot [(F_N)d] \tag{2}$$

where F_N is the DFT matrix. Applying to both sides of the expression the even-odd decomposition of the DFT matrix that leads to the decimation in time FFT, we obtain the following:

$$\begin{bmatrix} F_{N/2} \\ F_{N/2} \end{bmatrix} [s_e] + \left[W_N^k\right] \cdot \begin{bmatrix} F_{N/2} \\ F_{N/2} \end{bmatrix} [s_o] =$$

$$= \left[\begin{bmatrix} F_{N/2} \\ F_{N/2} \end{bmatrix} [g_e] + \left[W_N^k\right] \cdot \begin{bmatrix} F_{N/2} \\ F_{N/2} \end{bmatrix} [g_o] \right] \bullet \left[\begin{bmatrix} F_{N/2} \\ F_{N/2} \end{bmatrix} [d_e] + \left[W_N^k\right] \cdot \begin{bmatrix} F_{N/2} \\ F_{N/2} \end{bmatrix} [d_o] \right]$$

$$k = 0, \ldots, N-1 \tag{3}$$

where s_e, g_e and s_o, d_o are the even and odds entries of vectors s and d. Note that the usual minus sign appears when N is taken from 0 to N/2-1. Alternatively, the notation using summations could be used. The term at the right side is a point wise multiplication, therefore, distributive and associative properties may be applied. Applying the distributive property to the right hand side and then collecting similar terms with respect to W^k_N yields:

$$\begin{bmatrix} F_{N/2} \\ F_{N/2} \end{bmatrix} [s_e] + \left[W_N^k\right] \cdot \begin{bmatrix} F_{N/2} \\ F_{N/2} \end{bmatrix} [s_o] =$$

$$= \left[\begin{bmatrix} F_{N/2} \\ F_{N/2} \end{bmatrix} [g_e] \bullet \begin{bmatrix} F_{N/2} \\ F_{N/2} \end{bmatrix} [d_e] + [W_N^k]^2 \cdot \begin{bmatrix} F_{N/2} \\ F_{N/2} \end{bmatrix} [g_o] \bullet \begin{bmatrix} F_{N/2} \\ F_{N/2} \end{bmatrix} [d_o] \right]$$

$$+ [W_N^k] \cdot \left[\begin{bmatrix} F_{N/2} \\ F_{N/2} \end{bmatrix} [g_o] \bullet \begin{bmatrix} F_{N/2} \\ F_{N/2} \end{bmatrix} [d_e] + \begin{bmatrix} F_{N/2} \\ F_{N/2} \end{bmatrix} [g_e] \bullet \begin{bmatrix} F_{N/2} \\ F_{N/2} \end{bmatrix} [d_o] \right] \tag{4}$$

noting that;

$$(W_N^k)^2 = W_{N/2}^k, \quad k = 0, \ldots, N-1, \tag{5}$$

it follows:

$$\begin{bmatrix} F_{N/2} \\ F_{N/2} \end{bmatrix} [s_e] + [W_N^k] \cdot \begin{bmatrix} F_{N/2} \\ F_{N/2} \end{bmatrix} [s_o] = \tag{6}$$

$$= \left[\begin{bmatrix} F_{N/2} \\ F_{N/2} \end{bmatrix} [g_e] \bullet \begin{bmatrix} F_{N/2} \\ F_{N/2} \end{bmatrix} [d_e] + [W_{N/2}^k] \cdot \begin{bmatrix} F_{N/2} \\ F_{N/2} \end{bmatrix} [g_o] \bullet \begin{bmatrix} F_{N/2} \\ F_{N/2} \end{bmatrix} [d_o] \right]$$

$$+ [W_N^k] \cdot \left[\begin{bmatrix} F_{N/2} \\ F_{N/2} \end{bmatrix} [g_o] \bullet \begin{bmatrix} F_{N/2} \\ F_{N/2} \end{bmatrix} [d_e] + \begin{bmatrix} F_{N/2} \\ F_{N/2} \end{bmatrix} [g_e] \bullet \begin{bmatrix} F_{N/2} \\ F_{N/2} \end{bmatrix} [d_o] \right] \tag{7}$$

Now, letting N go from 0 to $N/2-1$:

$$[W_{N/2}^k]_{k=0,\ldots,N-1} = \begin{bmatrix} W_{N/2}^k \\ W_{N/2}^k \end{bmatrix}_{k=0,\ldots,N/2-1}$$

$$[W_N^k]_{k=0,\ldots,N-1} = \begin{bmatrix} W_N^k \\ -W_N^k \end{bmatrix}_{k=0,\ldots,N/2-1} \tag{8}$$

and noting that (6) is identical to (7), we equate coefficients of similar terms with respect to W_N^k, obtaining:

$$\begin{aligned} [F_{N/2}][s_e] &= [F_{N/2}][g_e] \cdot [F_{N/2}][d_e] \\ &\quad + W_{N/2}^k \cdot [F_{N/2}][g_o] \cdot [F_{N/2}][d_o] \\ [F_{N/2}][s_o] &= [F_{N/2}][g_o][F_{N/2}][d_e] \\ &\quad + [F_{N/2}][g_e][F_{N/2}][d_o] \end{aligned} \tag{9}$$

after taking the inverse of $F_{N/2}$ at both sides, it follows:

$$\begin{aligned} [s_e] &= [F_{N/2}]^{-1}[F_{N/2}][g_e] \cdot [F_{N/2}][d_e] \\ &\quad + [F_{N/2}]^{-1} W_{N/2}^k \cdot [F_{N/2}][g_o] \cdot [F_{N/2}][d_o] \\ [s_o] &= [F_{N/2}]^{-1}[F_{N/2}][g_o] \cdot [F_{N/2}][d_e] \\ &\quad + [F_{N/2}]^{-1}[F_{N/2}][g_e] \cdot [F_{N/2}][d_o] \end{aligned} \tag{10}$$

The point wise multiplication is avoided writing $[F_{N/2}][g_e]$ and $[F_{N/2}][g_o]$ in diagonal form, we call them Ge and Go:

$$\begin{aligned} [s_e] &= [F_{N/2}]^{-1}[G_e][F_{N/2}][d_e] \\ &\quad + [F_{N/2}]^{-1} W_{N/2}^k \cdot [G_o][F_{N/2}][d_o] \\ [s_o] &= [F_{N/2}]^{-1}[G_o][F_{N/2}][d_e] \\ &\quad + [F_{N/2}]^{-1} [G_e][F_{N/2}][d_o] \end{aligned} \tag{11}$$

in matrix form the previous expression becomes:

$$\begin{bmatrix} s_e \\ s_o \end{bmatrix} = \begin{bmatrix} [F_{N/2}]^{-1}[G_e][F_{N/2}] & [F_{N/2}]^{-1} W_{N/2}^k \cdot [G_o][F_{N/2}] \\ [F_{N/2}]^{-1}[G_o][F_{N/2}] & [F_{N/2}]^{-1} \quad [G_e][F_{N/2}] \end{bmatrix} \begin{bmatrix} d_e \\ d_o \end{bmatrix} \tag{12}$$

where we notice that all entries are itself matrices. For the second entry of the first row the following identity applies:

$$S_{N/2}[F_{N/2}]^{-1}[G_o][F_{N/2}] = [F_{N/2}]^{-1} W_{N/2}^k \cdot [G_o][F_{N/2}] \tag{13}$$

where $S_{N/2}$, will be shown to be the Cyclic Shift Operator,

$$S_{N/2} = [F_{N/2}]^{-1} W_{N/2}^k \cdot [G_o][F_{N/2}] \left[[F_{N/2}]^{-1}[G_o][F_{N/2}] \right]^{-1} \tag{14}$$

$$S_{N/2} = [F_{N/2}]^{-1} W_{N/2}^k \cdot [G_o][F_{N/2}][F_{N/2}]^{-1}[G_o]^{-1}[F_{N/2}] \tag{15}$$

$$S_{N/2} = [F_{N/2}]^{-1} W_{N/2}^k \cdot [G_o][G_o]^{-1}[F_{N/2}] \tag{16}$$

$$S_{N/2} = [F_{N/2}]^{-1} W_{N/2}^k \cdot [F_{N/2}] \tag{17}$$

$$S_{N/2} = [F_{N/2}]^{-1} [\mathrm{diag} W_{N/2}^k][F_{N/2}] \tag{18}$$

$$[F_{N/2}] S_{N/2} [F_{N/2}]^{-1} = [\mathrm{diag} W_{N/2}^k] \tag{19}$$

where the operator, whose associated matrix is diagonalized as the roots of unity by the DFT matrix is known to be the Cyclic Shift Operator; $S_{N/2}$:

$$S_{N/2} = \begin{bmatrix} 0 & 0 & 0 & . & . & 0 & 0 & 1 \\ 1 & 0 & 0 & . & . & 0 & 0 & 0 \\ 0 & 1 & 0 & . & . & 0 & 0 & 0 \\ 0 & 0 & 1 & . & . & 0 & 0 & 0 \\ . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & . \\ 0 & 0 & 0 & . & . & 1 & 0 & 0 \\ 0 & 0 & 0 & . & . & 0 & 1 & 0 \end{bmatrix} \tag{20}$$

Thus, the matrix expression of our algorithm becomes:

$$\begin{bmatrix} s_e \\ s_o \end{bmatrix} = \begin{bmatrix} [F_{N/2}]^{-1}[G_e][F_{N/2}] & S_{N/2}[F_{N/2}]^{-1}[G_o][F_{N/2}] \\ [F_{N/2}]^{-1}[G_o][F_{N/2}] & [F_{N/2}]^{-1}[G_e][F_{N/2}] \end{bmatrix} \begin{bmatrix} d_e \\ d_o \end{bmatrix} \tag{21}$$

note that all entries are N/2 by N/2 circulant matrices, the second entry of the first row, in particular, is a circulant matrix multiplied by the shift operator. When the matrix multiplication is actually carried out, we have four N/2-points cyclic convolutions. Each of those N/2-points cyclic convolutions can in turn be formulated through the same algorithm by using N/4-points cyclic convolutions, continuing with this procedure we will finally reach four-points convolutions. Applying a well known matrix factorization, the number of N/2-points cyclic convolutions can be reduced to three, thus reducing the number of required multiplications. From (21) it follows:

$$\begin{bmatrix} s_e \\ s_o \end{bmatrix} = \begin{bmatrix} [F_{N/2}]^{-1}[G_e][F_{N/2}]de + S_{N/2}[F_{N/2}]^{-1}[G_o][F_{N/2}]do \\ [F_{N/2}]^{-1}[G_o][F_{N/2}]de + [F_{N/2}]^{-1}[G_e][F_{N/2}]do \end{bmatrix} \tag{22}$$

The factorization that reduces the number of sections from four to three it is based upon rewriting the second entry of (23) as follows:

$$\begin{aligned} &[F_{N/2}]^{-1}[G_o][F_{N/2}]de + [F_{N/2}]^{-1}[G_e][F_{N/2}]do = \\ &= -[F_{N/2}]^{-1}[G_e][F_{N/2}]de \\ &+([F_{N/2}]^{-1}[G_e][F_{N/2}] + [F_{N/2}]^{-1}[G_o][F_{N/2}])(de + do) \\ &-[F_{N/2}]^{-1}[G_o][F_{N/2}]do \end{aligned} \tag{23}$$

substituting (23) in (22) and writing as a matrix multiplication gives:

$$\begin{bmatrix} s_e \\ s_o \end{bmatrix} = \begin{bmatrix} I_{N/2} & 0 & S_{N/2} \\ -I_{N/2} & I_{N/2} & -I_{N/2} \end{bmatrix} \cdot \begin{bmatrix} [F_{N/2}]^{-1}[G_e][F_{N/2}]de \\ ([F_{N/2}]^{-1}[G_e][F_{N/2}] + [F_{N/2}]^{-1}[G_o][F_{N/2}])(de + do) \\ [F_{N/2}]^{-1}[G_o][F_{N/2}]do \end{bmatrix} \tag{24}$$

after diagonalization, the circulant matrix factorization leading to a fast cyclic convolution algorithm is finally obtained:

$$\begin{bmatrix} s_e \\ s_o \end{bmatrix} = \begin{bmatrix} I_{N/2} & 0 & S_{N/2} \\ -I_{N/2} & I_{N/2} & -I_{N/2} \end{bmatrix} \cdot \begin{bmatrix} [F_{N/2}]^{-1}[G_e][F_{N/2}] & 0 & 0 \\ 0 & [F_{N/2}]^{-1}[G_e][F_{N/2}]+[F_{N/2}]^{-1}[G_o][F_{N/2}] & 0 \\ 0 & 0 & [F_{N/2}]^{-1}[G_o][F_{N/2}] \end{bmatrix} \cdot \begin{bmatrix} I_{N/2} & 0 \\ I_{N/2} & I_{N/2} \\ 0 & I_{N/2} \end{bmatrix} \begin{bmatrix} de \\ do \end{bmatrix} \tag{25}$$

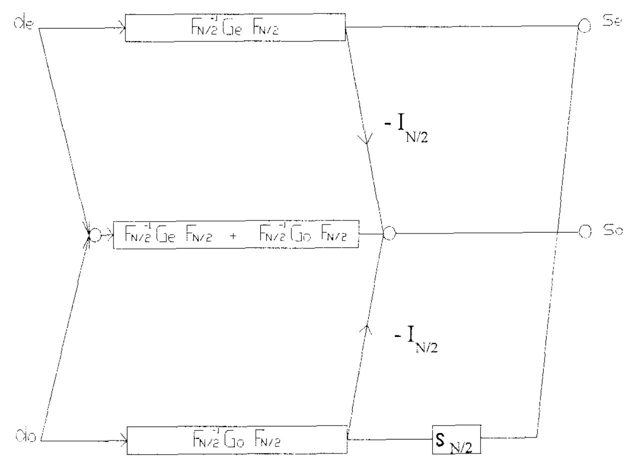

Fig. 1. Block diagram for the fast cyclic convolution algorithm.

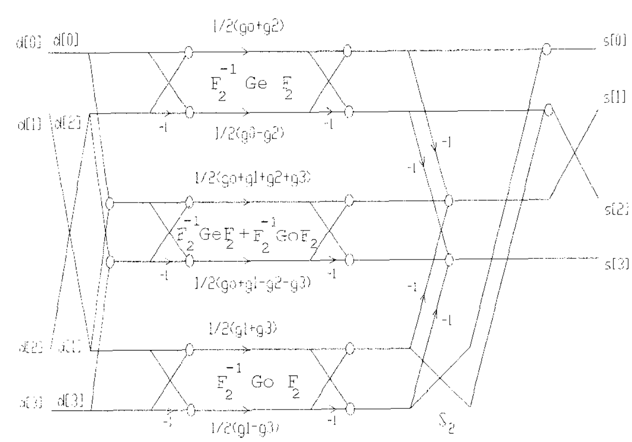

Fig. 2. Signal flow graph for N=4

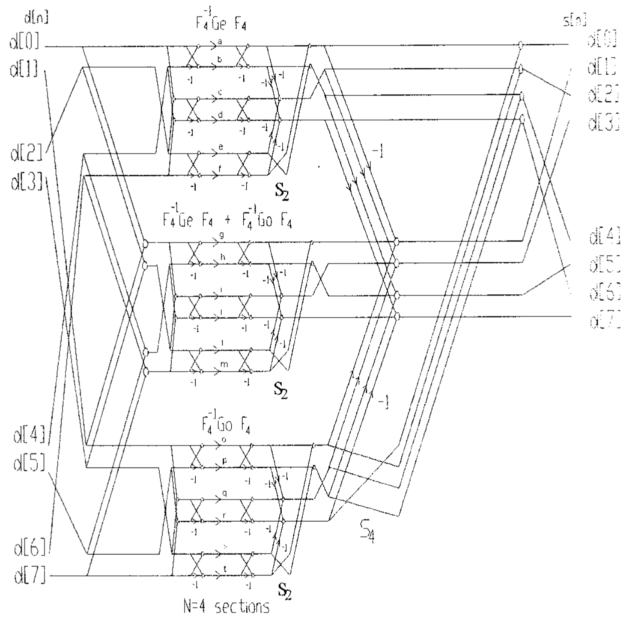

Fig. 3. Signal flow graph for N = 8

III. PERMUTATIONS OF THE DFT MATRIX AND THEIR RELATION TO PERMUTATIONS OF THE CIRCULANT MATRICES

Some permutations of the DFT matrix lead to convenient factorizations suitable to fast algorithms formulations. In the past, by analogy, some of those decompositions were successfully tried on the circulant matrices, [1], [2]. This gives a motivation for formally establishing a relation between permutations of the DFT matrix, and permutations of the circulant matrices.

Given a permutation of the DFT matrix, we will be looking for a corresponding permutation of the circulant matrices and the convolved signals, such that:

a) The permuted circulant matrix is diagonalized by the permuted DFT matrix.

b) An expression with the form of the cyclic convolution theorem, still holds.

c) Given an appropriate pre permuted version of the input signal, and post permuting the result, the new permuted version of the circulant matrix is appropriate to compute the cyclic convolution of the original signals.

Let h and d, be the coordinate vector representations of the N -point sequences.
Let H_N, be the circulant matrix and therefore; $s = H_N d$
Let p, be any permutation matrix.
Let $(F_N)p = F_{New}$, be a permuted version of the DFT matrix.
Let $p^{-1}d = d_{New}$, be a permuted version of the signal d
Let H_{New}, be the corresponding, permuted version of the circulant matrix.
The cyclic convolution theorem states:

$$(F_N)s = (F_N)h \,.\, (F_N)d \tag{26}$$

and multiplying for pp^{-1}, in order to introduce F_{New} without altering the equality, gives:

$$(F_N)pp^{-1}s = (F_N)pp^{-1}h \,.\, (F_N)pp^{-1}d \tag{27}$$
$$(F_N)p(p^{-1}s) = (F_N)p(p^{-1}h) \,.\, (F_N)p(p^{-1}d) \tag{28}$$

since $(F_N)p = F_{New}$, $p^{-1}d = d_{New}$, $p^{-1}h = h_{New}$ and $p^{-1}s = s_{New}$, it follows:

$$F_{New}(s_{New}) = F_{New}(h_{New}) \cdot F_{New}(d_{New}) \tag{29}$$
$$(s_{New}) = (F_{New})^{-1}[F_{New}(h_{New}) \cdot F_{New}(d_{New})] \tag{30}$$
$$(s_{New}) = H_{New}(d_{New}) \tag{31}$$

Therefore to completely satisfy b) we still have to determine H_{New} in terms of H_N;

$$(p^{-1}s) = ((F_N)p)^{-1}\,[(F_N)p(p^{-1}h) \,.\, (F_N)p(p^{-1}d)] \tag{32}$$
$$(p^{-1}s) = p^{-1}(F_N)^{-1}\,[(F_N h) \,.\, (F_N)p(p^{-1}d)] \tag{33}$$
$$(p^{-1}s) = p^{-1}(F_N)^{-1}\,(F_N h) \,.\, (F_N)p(p^{-1}d) \tag{34}$$

and in order to eliminate the point wise multiplication, we write $F_N h = H$ in diagonal form, D_H,

$$(p^{-1}s) = p^{-1}(F_N)^{-1}D_H\,(F_N)p(p^{-1}d) \tag{35}$$

It is well known that

$$H_N = F_N{}^{-1}D_H F_N \tag{36}$$

and substituting (36) in (35) gives:

$$(p^{-1}s) = p^{-1}\,H_N\,p\,(p^{-1}d) \tag{37}$$

finally H_{New} can now be defined as:

$$H_{New} = p^{-1}\,H_N\,p \tag{38}$$

where substituting (38) in (37) gives (31). Therefore condition b) is completely satisfied.

Substituting (36) in (38) gives:

$$H_{New} = p^{-1}(F_N)^{-1}D_H\,(F_N)p \tag{39}$$

which can be written in terms of F_{New} as follows:

$$H_{New} = ((F_N)p)^{-1} D_H (F_N)p = (F_{New})^{-1} D_H (F_{New}) \quad (40)$$

or

$$D_H = (F_{New}) H_{New} (F_{New})^{-1} \quad (41)$$

Therefore condition a), it is also completely satisfied. Considering that $(F_N)p = F_{New}$ and $H_{New} = p^{-1} H_N p$ the equivalence between (36) and (41) is clearly seen:

$$D_H = (F_N)p\,(p^{-1} H_N p)\,((F_N)p)^{-1} \quad (42)$$
$$= (F_N)p\,p^{-1} H_N\, p\,p^{-1} (F_N)^{-1}$$
$$D_H = (F_N) H_N (F_N)^{-1} \quad (43)$$

Now, substituting (38) in (37) we verify that condition c) it is also satisfied:

$$(p^{-1}s) = H_{New}(p^{-1}d) \quad (44)$$
$$s = p\, H_{New}(p^{-1}d) \quad (45)$$

Therefore, factorization (21) can also be obtained applying to a N by N circulant matrix the same permutation p, as indicated in (38), which when applied to the DFT matrix leads to the decimation in time FFT.

Now, for completeness, it will be shown that the permuted version of the circulant matrices, can be written as a linear combination of the powers of a permuted version of the cyclic shift operator. It is well known that a circulant matrix can be written in terms of the cyclic shift operator as follows [6]:

$$H_N = \sum_{n=0}^{N-1} h_n S_N^n \quad (46)$$

Substituting (46) in (38), and using linearity of the permutation operator, gives:

$$H_{New} = p^{-1} H_N p = p^{-1}\Big(\sum_{n=0}^{N-1} h_n S_N^n\Big) p = \sum_{n=0}^{N-1} h_n p^{-1} (S_N^n)\, p \quad (47)$$

$$H_{New} = \sum_{n=0}^{N-1} h_n (p^{-1} S_N p)^n = \sum_{n=0}^{N-1} h_n (S_{New})^n \quad (48)$$

where S_{New}, which is defined as:

$$S_{New} = p^{-1} S_N\, p$$

is not necessarily a shift operator anymore, as well as H_{New} is not necessarily circulant anymore. Note that (48) follows from (47), since:

$$(p^{-1} S_N\, p)^n =$$
$$= (p^{-1} S_N\, p)(p^{-1} S_N\, p) \cdots (p^{-1} S_N\, p)(p^{-1} S_N\, p)$$
$$= (p^{-1} S_N\, S_N\, S_N \cdots S_N\, S_N\, p)$$
$$= p^{-1} (S_N)^n\, p \quad (49)$$

In addition, note that the permuted version of the cyclic shift operator matrix is diagonalized as the roots of unity by the permuted version of the DFT matrix. This can be seen as follows:

$$(F_{New}) S_{New} (F_{New})^{-1} = (F_N\, p)(p^{-1} S_N\, p)(F_N\, p)^{-1} \quad (50)$$
$$= F_N\, p\, p^{-1} S_N\, p\, p^{-1} F_N^{-1}$$
$$= F_N\, S_N\, F_N^{-1} = \operatorname{diag} W^{k}{}_N \quad (51)$$

where (51) is known to diagonalize as the roots of unity.

IV. Conclusions

The DFT matrix factorization leading to the decimation in time FFT, has been mathematically linked to a factorization of the circulant matrices. This factorization, in turn, has been shown to lead to a fast cyclic convolution algorithm. Most importantly, permutations of the DFT matrix have been related to permutations of the circulant matrices. The previous results suggest that factorizations in the discrete frequency domain, have associated factorizations in the discrete time domain, with the cyclic convolution theorem being one link among such decompositions. Some of these factorizations, as it was shown, could lead to fast algorithms in both domains, thus, providing further unification and the possibility of obtaining additional algorithms from a single original decomposition.

References

[1] D. A. Pitassi, "Fast convolution using the Walsh transform," Proc. Conf. on Applications of Walsh Functions, pp. 130-133, Washington D. C., April 1971.

[2] W. F. Davis, "A class of efficient convolution algorithms," Proc. Conf. on Applications of Walsh Functions, pp. 318-319, Washington D.C., March 1972.

[3] R. C. Agarwal and C. S. Burrus, " Fast one dimensional digital convolution by multidimensional techniques," IEEE Transactions on Acoustics, Speech, and Signal Processing, Vol ASSP-22, N°1, pp. 1-10, February 1974.

[4] H. K. Kwan and M. T. Tsim, "High speed 1-D FIR digital filtering architecture using polynomial convolution," Proc. of ICASSP, Dallas, 1987.

[5] R. Meyer, R. Reng and K.Schwarz, " Convolution algorithms on DSP processors," Proc. of ICASSP, Toronto, Canada, 1991.

[6] R. Tolimieri and C. Lu, *Algorithms for Discrete Fourier Transform and Convolution*, Springer-Verlag, New York, N.Y. 1989.