A Fast DFT Algorithm Using Complex Integer Transforms[1]

I. S. Reed
University of Southern California
Department of Electrical Engineering

T. K. Truong
Tracking and Data Acquisition Engineering Section

In this article Winograd's algorithm for computing the discrete Fourier transform (DFT) is extended considerably for certain large transform lengths. This is accomplished by performing the cyclic convolution, required by Winograd's method, by a fast transform over certain complex integer fields developed previously by the authors. This new algorithm requires fewer multiplications than either the standard fast Fourier transform (FFT) or Winograd's more conventional algorithm.

I. Introduction

Several authors (Refs. 1-12) have shown that transforms over finite fields or rings can be used to compute circular convolutions without round-off error. Recently, Winograd (Ref. 13) developed a new class of algorithms that depend heavily on the computation of a cyclic convolution for computing the conventional discrete Fourier transform (DFT). This new algorithm, for a few hundred transform points, requires substantially fewer multiplications than the conventional fast Fourier transform (FFT) algorithm.

The authors (Ref. 5) defined a special class of finite Fourier-like transforms over $GF(q^2)$ where $q = 2^p - 1$ is a Mersene prime for $p = 2,3,5,7,13,17,19,31,61 \ldots$. These transforms have a transform length of d points, where $d|8p$. The advantage of this transform over others is that it can be accomplished simply by circular shifts instead of by multiplications (Ref. 11).

In this paper, it is shown that Winograd's algorithm can be combined with the above-mentioned Fourier-like transform over $GF(q^2)$ to yield a new hybrid algorithm for computing the discrete Fourier transform (DFT). By this means a fast method for accurately computing the DFT of a sequence of complex numbers of very long transform lengths is obtained.

II. Cyclic Convolution

The following algorithm for the cyclic convolution of two sequences is based on ideas due to Winograd (Ref. 13). Let the field of rationals be R. Also let $X(u) = x_0 + x_1u + x_2u^2 + \ldots + x_nu^{n-1}$, $Y(u) = y_0 + y_1u + y_2u^2 + \ldots + y_nu^{n-1}$ be two polynomials over R. The product $T(u) = X(u) \cdot Y(u)$ can be computed by

[1]This work was supported in part by the U.S. Air Force Office of Scientific Research.

$$T(u) = X(u) \cdot Y(u) \bmod \prod_{i=0}^{2n-2} (u - \alpha_i) \qquad (1)$$

where

$$\alpha_i \in R.$$

It is shown in (Ref. 13) that a minimum of $2n - 1$ multiplications are needed to compute Eq. (1).

It is readily shown that the cyclic convolution of $X(u)$ and $Y(u)$ is the set of coefficients of the polynomial

$$T'(u) = X(u) \cdot Y(u) \bmod (u^n - 1)$$

Let the polynomial $u^n - 1$ be factored into irreducible relatively prime factors, i.e.,

$$u^n - 1 = \prod_{i=1}^{K} g_i(u)$$

where

$$(g_i(u), g_j(u)) = 1 \text{ for } i \neq j$$

Then $T'(u)$ mod $g_i(u)$ for $i = 1,2,\ldots,k$ can be computed, using Eq. (1). Finally, the Chinese Remainder Theorem is used to evaluate $T(u)$ from these residues. The above summarizes Winograd's method for performing a cyclic convolution.

The following theorem is due to Winograd (Ref. 14).

Theorem 1. Let a and b be relatively prime positive integers and A be the cyclic $ab \times ab$ matrix, given by

$$A(x,y) = f(x + y \bmod a \cdot b), \qquad 0 \leqslant x,y < ab$$

If π is a permutation of the set of integers $\{0, 1, \ldots, ab - 1\}$, let

$$B(x,y) = A(\pi(x), \pi(y))$$

Then there exists a permutation π such that, if B is partitioned into $b \times b$ submatrices, each submatrix is cyclic and the submatrices form an $a \times a$ cyclic matrices.

It was shown by Winograd (Ref. 14) that the number of multiplications needed to perform a circular convolution of 2,3,4,5 and 6 points is 2,4,5,10 and 8 multiplications, respectively. To compute the cyclic convolution of two longer sequences of complex integers, a d-point transform over $GF(q^2)$ where $d|8p$ is utilized here. Since the latter transform can be evaluted without multiplications (Ref. 11), it can be used with considerable advantage to compute a cyclic convolution without roundoff error of two d-point complex number sequences. Hence, for the transform over $GF(q^2)$, the number of integer complex multiplications needed to perform a circular convolution is precisely d.

III. The DFT When Transform Length Is a Prime $d = q'$

The DFT is defined by

$$A_j = \sum_{i=0}^{d-1} a_i w^{ij}$$

where w is a dth root of unity. Let

$$A_0 = \sum_{i=0}^{d-1} a_i \qquad (2a)$$

and

$$A_j = a_0 + B_j \quad \text{for} \quad j = 1,2,\ldots,d-1$$

where

$$B_j = \sum_{i=1}^{d-1} a_i w^{ij}$$

That is, let

$$\bar{B} = W\bar{a} \qquad (2b)$$

where W is the $(d - 1) \times (d - 1)$ matrix (w^{ij}) and $\bar{a}, \bar{B}$ are the column matrices (a_i) and (B_k), respectively. If $d = q'$ is a prime, then, by Ref. 12 one can find an element α in $GF(q')$ that generates its cyclic multiplicative subgroup of $q' - 1$ elements. Using the element α a cyclic permutation of the elements of $GF(q')$ can be defined by

$$\alpha = \begin{pmatrix} 1, & 2, \ldots, q' - 2, q' - 1 \\ \alpha, \alpha^2, \ldots, \alpha^{q'-2}, & \alpha^{q'-1} \end{pmatrix} \qquad (2c)$$

With this permutation, one can permute the indices of $\bar{B}, \bar{a}, W$ defined in Eq. (2b) so that the matrix $\bar{W} = (w^{\sigma(i)\sigma(j)})_{i,\, j\neq 0}$, is cyclic. That is,

$$B_{\sigma(j)} = \sum_{i=1}^{q'-1} a_{\sigma(i)} w^{\sigma(i)\sigma(j)}$$

$$= \sum_{i=1}^{q'-1} a_{\sigma(i)} w^{\sigma(i+j)}$$

for

$$j = 1,2,\ldots,q'-1 \tag{3}$$

Thus, $B_{\sigma(j)}$ is a cyclic convolution of $a_{\sigma(i)}$ and $w^{\sigma(i)}$ for $j = 1,2,\ldots,q'-1$.

Let $q'-1 = p_1 \cdot p_2 \cdots p_r$ be the factorization of $q'-1$ into prime integers. If one lets $a_1 = p_1 \cdot p_2 \cdots p_{r-1}$ and $b_1 = p_r$, by Theorem 1 the cyclic matrix can be partitioned into $b_1^2 = p_r^2$ matrices of size $a_1 \times a_1$. Next let $a_1 = a_2 \times b_2$, where $a_2 = p_1 \cdots p_{r-2}$ and $b_2 = p_{r-1}$. If a_2 is not a prime, then each $a_1 \times a_1$ cyclic matrix can be partitioned into b_2^2 matrices of size $a_2 \times a_2$. In general, $a_i = a_{i+1} \cdot b_{i+1}$, where b_{i+1} is a prime. If $a_{i+1} \neq 1$, then each $a_i \times a_i$ cyclic matrix can be partitioned into b_{i+1}^2 matrices of size $a_{i+1} \times a_{i+1}$. Otherwise, the procedure terminates. If the number of multiplications used to compute the cyclic convolution of p_i points is m_i for $i = 1,2,\ldots,r$, then the number of multiplications for computing a q'-point DFT is equal to $N = m_1 \cdot m_2 \cdots m_r$.

For most applications the two Mersenne primes $2^{31}-1$ and $2^{61}-1$ will provide enough bit accuracy and dynamic range for computing the DFT. For these primes, we choose the prime q' to have the form

$$q' = 1 + a \cdot 2^2 \cdot p$$

where $2^2 \cdot p | (2^p - 1)^2 - 1$ for $p = 31$ or 61 and $a = 3$ or 5. Such values for the prime q' are 373, 733, 1861, and 2441. If $d = q'$ is the transform length of the DFT, then, by Theorem 1, there exists a permutation of rows and columns so that the cyclic matrix $\bar{W}$ can be partitioned into blocks of $(2^2 \cdot p) \times (2^2 \cdot p)$ cyclic matrices, such that the blocks form an $a \times a$ cyclic matrix. A cyclic convolution of $a = 3$ or 5 complex number points can be accomplished by Winograd's algorithm. As it was mentioned in the last section, the transform of length $2^2 \cdot p$ over $GF(q^2)$ can be used to compute the cyclic convolution of $2^2 \cdot p$ complex number points. The number of multiplications needed to perform this convolution is $2^2 \cdot p$. Hence for a prime q' the total number of multiplications, needed to perform a DFT of $d = q'$ complex number points is shown in Table 1. To illustrate the above procedure consider the following example.

Example. Consider the DFT for $d = 7$ points. Let the input function be defined by

$$a_n = 1 + \hat{i}0 \qquad 0 \leqslant n \leqslant 1$$

$$= 0 + \hat{i}0 \qquad 2 \leqslant n \leqslant 6$$

By Eq. (2a), this transform is

$$A_0 = \sum_{i=0}^{6} a_i = 2 + \hat{i}0 \tag{3a}$$

and

$$A_j = a_0 + b_j \quad \text{for} \quad j = 1,2,\ldots,6 \tag{3b}$$

where

$$b_j = \sum_{i=1}^{6-1} a_i w^{ij}, \quad w = e^{i2\pi/7}$$

For $d = 7$, the permutation σ is given by

$$\sigma = \begin{pmatrix} 1, 2, 3, 4, 5, 6 \\ 3, 2, 6, 4, 5, 1 \end{pmatrix}$$

Applying the above permutation to Eq. (3b), one obtains $\bar{B} = \bar{W}\bar{a}$ as

$$\begin{pmatrix} b_3 \\ b_2 \\ b_6 \\ b_4 \\ b_5 \\ b_1 \end{pmatrix} = \begin{pmatrix} w^2 & w^6 & w^4 & w^5 & w^1 & w^3 \\ w^6 & w^4 & w^5 & w^1 & w^3 & w^2 \\ w^4 & w^5 & w^1 & w^3 & w^2 & w^6 \\ w^5 & w^1 & w^3 & w^2 & w^6 & w^4 \\ w^1 & w^3 & w^2 & w^6 & w^4 & w^5 \\ w^3 & w^2 & w^6 & w^4 & w^5 & w^1 \end{pmatrix} \begin{pmatrix} a_3 \\ a_2 \\ a_6 \\ a_4 \\ a_5 \\ a_1 \end{pmatrix}$$

By Theorem 1, there exists a permutation π of rows and columns so that the above cyclic matrix can be partitioned into 2 X 2 block matrix of 3 X 3 cyclic blocks as follows

$$\begin{pmatrix} b_3 \\ b_5 \\ b_6 \\ b_4 \\ b_2 \\ b_1 \end{pmatrix} = \begin{pmatrix} w^2 & w^1 & w^4 & w^5 & w^6 & w^3 \\ w^1 & w^4 & w^2 & w^6 & w^3 & w^5 \\ w^4 & w^2 & w^1 & w^3 & w^5 & w^6 \\ w^5 & w^6 & w^3 & w^2 & w^1 & w^4 \\ w^6 & w^3 & w^5 & w^1 & w^4 & w^2 \\ w^3 & w^5 & w^6 & w^4 & w^2 & w^1 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$$

This matrix equation has the block forms,

$$\begin{pmatrix} B_1 \\ B_2 \end{pmatrix} = \begin{pmatrix} C & D \\ D & C \end{pmatrix} \begin{pmatrix} Z_1 \\ Z_2 \end{pmatrix}$$

$$= 2^{-1} \begin{pmatrix} (C+D)(Z_1+Z_2)+(C-D)(Z_1-Z_2) \\ (C+D)(Z_1+Z_2)-(C-D)(Z_1-Z_2) \end{pmatrix}$$

$$= 2^{-1} \begin{pmatrix} E+F \\ E-F \end{pmatrix} \qquad (4)$$

Since C and D are 3 X 3 cyclic matrices, it is evident that the matrices $C+D$ and $C-D$ are also 3 X 3 cyclic matrices. In (4), E is

$$E = \begin{pmatrix} e_0 \\ e_1 \\ e_2 \end{pmatrix} = \begin{pmatrix} -0.445, & 1.247, & -1.802 \\ 1.247, & -1.802, & -0.445 \\ -1.802, & -0.445, & 1.247 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \qquad (5)$$

where approximately $1/2Re(w^2 + w^5) = -0.445$, $1/2Re(w^1 + w^6) = 1.247$, etc. Let $a_0 = -1.802$, $a_1 = -0.445$, $a_2 = 1.247$ and $y_0 = 0$, $y_1 = 1$, $y_2 = 0$. Then the matrix defined in Eq. (4) can be obtained by computing the convolution of the two sequences a_n and b_n. To do this use a transform $GF(q^2)$ where $q = 2^3 - 1$.

By (Ref. 6), the sequence of a_n is converted first to a sequence of integers x_n in the dynamic range $A = 2$. Since 2 is a 3rd root of unity the transform over $GF(7^2)$ of x_n is

$$X_k = \sum_{n=0}^{3-1} x_n \cdot 2^{nk} = -1 + 2^{2k} \qquad \text{for } k = 0,1,2$$

Thus $X_0 = 0$, $X_1 = 3$, $X_2 = 1$.

Similarly, the DFT of sequence y_n is

$$Y_k = \sum_{n=0}^{3-1} y_n \cdot 2^{nk} = 1 \cdot 2^{2k}$$

for

$$k = 0,1,2$$

That is, $Y_0 = 1$, $Y_1 = 2$, $Y_2 = 4$. But $E_k = X_k \cdot Y_k$, i.e., $E_0 = 0$, $E_1 = 6$, $E_2 = 4$. These are the only integer multiplications needed to perform this DFT. The inverse transform of E_k is

$$e_k = 3^{-1} \sum_{i=0}^{3-1} E_k \cdot 2^{-nk} \qquad \text{for} \quad k = 0,1,2$$

or $e_0 = 1$, $e_1 = -1$, $e_2 = 0$.

In a similar fashion matrix F, given in Eq. (4) can also be obtained as $f_0 = -\hat{i}$, $f_1 = \hat{i} \cdot 0$, $f_2 = -\hat{i}$. Thus, by Eq. (4), one obtains $b_1 = 1/2\hat{i}$, $b_2 = -1/2\hat{i}$, $b_3 = (1 - \hat{i})/2$, $b_4 = (1 + \hat{i})/2$, $b_5 = -1/2$, $b_6 = -\hat{i}/2$. Hence, finally $A_0 = 2 + \hat{i}0$, $A_1 = 1 + 1/2\hat{i}$, $A_2 = 1/2 + \hat{i}0$, $A_3 = 1/2(3 - \hat{i})$, $A_4 = 1/2(3 + \hat{i})$, $A_5 = 1/2 + \hat{i}0$, $A_6 = 1 - 1/2\hat{i}$. For this example, the dynamic range of $GF(7)$ is inadequate. There is a large truncation error due to the approximation of the roots of unity. Evidently, the DFT in this example has an accuracy of precisely 2 binary digits, including the sign bit. This example, though only illustrative, suggests that the large finite fields given above have more than adequate dynamic range to compute the DFT with small truncation error.

IV. Transforms of Very Long Sequences

In order to compute the DFT of much longer sequences than considered in the last section, let $d = d_1 \cdot d_2 \ldots d_r$, where $(d_i, d_j) = 1$ for $i \neq j$. By using the Chinese Remainder Theorem (Ref. 15), it is shown by Winograd in (Ref. 13) that the DFT matrix W can be transformed into the direct product

of $W_1, W_2, \ldots, W_r$, where W_i is the matrix of a d_i-point DFT. Assume the number of multiplications used to perform the d_i-point DFT for $i = 1,2, \ldots, r$ is m_i. Then, the number of multiplications for computing a d-point DFT is $N = m_1 \cdot m_2 \ldots m_r$. To illustrate this, see the example for computing a 12-point DFT given in Ref. 14. By the same procedure used in the computation of this example, the number of integer multiplications needed to perform the transforms of longer sequences of complex numbers can be obtained by using Table 1 above and Table 1 in Ref. 13. These numbers are given in Table 2. The present algorithm, and conventional FFT algorithm (Ref. 16) are compared in Table 2 by giving the number of real multiplications needed to perform these algorithms. The number of real multiplications needed to perform a transform of a few thousand points is given in Table 2 of Ref. 13.

Acknowledgement

The authors wish to thank Dr. N. A. Renzetti, Manager of Tracking and Data Acquisition Engineering, and the members of the Advanced Engineering Group in that organization for their early support, suggestions, and encouragement of the research that led to this paper.

References

1. Pollar, J. M., "The Fast Fourier Transform in a Finite Field," *Math. Comput.*, 1971, 25, pp. 365-374.

2. Schonhage, A. and Strassen, V., "Schnelle Multiplication Grosser Zahlen," *Computing*, 1971, 7, pp. 281-292.

3. Rader, C. M., "Discrete Convolution via Mersenne Transforms," *IEEE Trans. Comp.*, 1972, C-21, pp. 1269-1273.

4. Agarwal, R. C. and Burrus, C. S., "Number Theoretic Transforms to Implement Fast Digital Convolution," *Proc. IEEE*, 1975, 63, pp. 550-560.

5. Reed, I. S. and Truong, T. K., "The Use of Finite Fields to Compute Convolution," *IEEE Trans.*, 1975, IT-21, pp. 208-213.

6. Reed, I. S. and Truong, T. K., "Complex Integer Convolution Over a Direct Sum of Galois Fields," *IEEE Trans.*, 1975, IT-21, pp. 657-661.

7. Vegh, E. and Leibowitz, L. M., "Fast Complex Convolution in Finite Rings," *IEEE Trans.*, 1976, ASSP-24, pp. 343-344.

8. Golomb, S. W., Reed, I. S., and Truong, T. K., "Integer Convolutions Over the Finite Field $GF(3 \cdot 2^n + 1)$," *SIAM J. on Applied Math.*, Vol. 32, No. 2, March 1977.

9. Pollar, J. M., "Implementation of Number-Theoretic Transforms," *Electro. Lett.*, 1976, 12, pp. 378-379.

10. Liu, K. Y., Reed, I. S., and Truong, T. K., "Fast Number-Theoretic Transforms for Digital Filtering," *Electron. Lett.*, 1976, 12, pp. 644-646.

11. Reed, I. S., Truong, T. K., and Liu, K. Y., "A New Fast Algorithm for Computing Complex Number-Theoretic Transforms," *Electron. Lett.*, 1977, pp. 278-280.

12. Reed, I. S. and Truong, T. K., "Fast Algorithms for Computing Mersenne-Prime Number-Theoretic Transforms," *The Deep Space Network Progress Report 42-41,* pp. 176-205, Jet Propulsion Laboratory, Pasadena, California, October 15, 1977.

13. Winograd, S., "On Computing the Discrete Fourier Transform," *Proc. Nat. Acad. Sci. USA*, 1976, 73, pp. 1005-1006.

14. Winograd, S., "On Computing the Discrete Fourier Transform," Research Report, Math. Science Dept., IBM Thomas J. Watson Research Center, Yorktown Heights, New York, 10592.

15. Niven, I. and Zuckerman, H. S., *An Introduction to the Theory of Numbers*, John Wiley and Sons, Inc., New York, 1966.

16. Cooley, J. W., and Tukey, J. W., "An Algorithm for the Machine Calculation of Complex Fourier Series," *Math. Comput.*, Vol. 19, pp. 297-301, April, 1965.

Table I. Complexity of complex number DFT of prime number length

$d = p$	$p - 1$	No. of Integer Complex Multiplications
373	$2^2 \cdot 3 \cdot 31$	496
733	$2^2 \cdot 3 \cdot 61$	976
1831	$2 \cdot 3 \cdot 5 \cdot 61$	4880
1861	$2^2 \cdot 3 \cdot 5 \cdot 31$	4960
2441	$2^3 \cdot 5 \cdot 61$	4880

Table 2. Complexity of new algorithm for DFT

d	Factors	New algorithm No integer multiplications complex data	Radix-2 FFT No. real multiplications $2d\log_2 d$
4096	2^{12}		98,304
4476	373 X 4 X 3	23,904	
8192	2^{13}		212,992
8796	733 X 4 X 3	46,944	
16384	2^{14}		458,752
20888	373 X 8 X 7	143,424	
32768	2^{15}		983,040
41048	733 X 8 X 7	281,664	
62664	373 X 8 X 7 X 3	430,272	
65536	2^{16}		2,097,152
123144	733 X 8 X 7 X 3	844,992	
131072	2^{17}		4,456,448
262144	2^{18}		9,437,184
268560	373 X 16 X 9 X 5	2,796,768	
524288	2^{19}		19,922,944
527760	733 X 16 X 9 X 5	5,492,448	