computers, each trial can be made in less than 10 μs, so this many trials could be made in about 3 to 5 hours. Using special hardware for the solution of linear Boolean equations, these times could likely be improved by a factor of 10 or more.

Pless's scheme already has the disadvantage that about 38 000 sets of primitive coefficients must be stored in order to obtain the full set of initial states. An attempt to improve the security of the cipher by increasing the size of the FR's would greatly increase this storage requirement.

References

[1] C. H. Meyer and W. L. Tuchman, "Pseudorandom codes can be cracked," *Electron. Design*, vol. 23, pp. 74–76, Nov. 1972.
[2] V. S. Pless, "Encryption schemes for computer confidentiality," *IEEE Trans. Comput.*, vol. C-26, pp. 1133–1136, Nov. 1977.
[3] J. Reeds, "'Cracking' a random number generator," *Cryptologia*, vol. 1, pp. 20–26, Jan. 1977.
[4] F. Rubin, "Computer methods for decrypting random stream ciphers," *Cryptologia*, vol. 2, pp. 152–160, Apr. 1978.
[5] A. Sinkov, *Elementary Cryptanalysis A Mathematical Approach*. New York: Random House, 1968.
[6] B. Tuckerman, "A study of the Vigenere–Vernam single- and multiple-loop enciphering systems," IBM Res. Rep. RC-2879, May 1970.

Frank Rubin received the B.S. degree in mathematics from Massachusetts Institute of Technology, Cambridge, in 1962, the M.S. degree in mathematics from Brandeis University, Waltham, MA, and the Ph.D. degree in systems and information science from Syracuse University, Syracuse, NY, in 1972.

He joined the IBM Corporation, Poughkeepsie, NY, in 1964. He has worked on processing natural speech, text processing, automated flowcharting, circuit diagram layout, circuit placement and wiring, logic partitioning, online debugging aids, several assemblers and compilers, and computer architecture. He is presently an Advisory Programmer in Engineering Design Systems. His published papers are on graph theory, operations research, cryptography, transpotation, and text compression.

Dr. Rubin is a member of the Association for Computing Machinery, IEEE Computer Society, and the American Cryptogram Association.

A New Hybrid Algorithm for Computing a Fast Discrete Fourier Transform

IRVING S. REED, FELLOW, IEEE, AND T. K. TRUONG

Abstract—**In this paper for certain long transform lengths, Winograd's algorithm for computing the discrete Fourier transform (DFT) is extended considerably. This is accomplished by performing the cyclic convolution, required by Winograd's method, with the Mersenne prime number-theoretic transform developed originally by Rader. This new algorithm requires fewer multiplications than either the standard fast Fourier transform (FFT) or Winograd's more conventional algorithm. However, more additions are required.**

Index Terms—**Discrete Fourier transform (DFT), fast Fourier transform (FFT), Winograd's algorithm.**

Introduction

SEVERAL authors [1]–[13] have shown that transforms over finite fields or rings can be used to compute circular convolutions without roundoff error. Recently, Winograd [14] developed a new class of algorithms which 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.

C. M. Rader [3] defined a special class of finite Fourier-like transforms over $GF(q)$, where $q = 2^p - 1$ is a Mersenne prime for $p = 2, 3, 5, 7, 13, 17, 19, 31, 61 \cdots$. These number-theoretic transforms are used and specialized here to transform lengths of p points. The advantage of this transform over others is that it can be accomplished simply by circular shifts, i.e., no multiplications are needed [3]. The disadvantage of this transform is that the sequence length p is a prime number. As a consequence the most efficient FFT algorithm cannot be used. It is rather inefficient with regard to additions.

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

Manuscript received March 10, 1978; revised February 6, 1979. This work was supported in part by the National Aeronautics and Space Administration under Contract NAS 7-100 and by the United States Air Force Office of Scientific Research under Grant AFSOR 75-2798.

I. S. Reed is with the Department of Electrical Engineering, University of Southern California, Los Angeles, CA 90007.

T. K. Truong is with the Communications Systems Research Section, Telecommunications Science and Engineering Division, Jet Propulsion Laboratory, Californis Institute of Technology, Pasadena, CA 91103.

0018-9340/79/0700-0487$00.75

The number of multiplications and additions needed to perform a cyclic convolution of 2, 3, 4, 5, 6, and 8 points are given in Table I [17]. To compute the cyclic convolution of two longer sequences of integers, a p-point transform over $GF(q)$ will be utilized in this paper. Since the latter transform can be evaluated without multiplications [3], it can be used with advantage to compute the cyclic convolution of two p-point real number sequences. The number of integer multiplications and additions needed to perform such a cyclic convolution over $GF(q)$ is precisely p (excluding the multiplications by p^{-1} in the inverse transform) and $p(p-1)$, respectively.

The DFT when the Transform Length d 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

$$A_0 = \sum_{i=0}^{d-1} a_i \tag{1}$$

and

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

where

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

That is, let

$$\bar{B} = W\bar{a} \tag{2}$$

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_j), respectively. If $d = q'$ is a prime, then by [18] one can find an element α in $GF(q')$ which generates its cyclic multiplicative subgroup of $q'-1$ elements. Using the element α, a cyclic permutation of the nonzero elements of $GF(q')$ can be defined by $\sigma(i) = \alpha^i$ for $i = 1, 2, \cdots, q'-1$. With this permutation, one can permute the indices of $\bar{B}$, $\bar{a}$, and W defined in (2) so that the matrix $\tilde{W} = (w^{\sigma(i)\sigma(j)})_{i,j\neq 0}$, is cyclic. That is,

$$\begin{aligned} B_{\sigma(j)} &= \sum_{i=1}^{q'-1} a_{\sigma(i)} w^{\sigma(i)\sigma(j)} \\ &= \sum_{i=1}^{q'-1} a_{\sigma(i)} w^{\sigma(i+j)} \qquad \text{for } j = 1, 2, \cdots, q'-1. \end{aligned} \tag{3}$$

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

Let $q'-1 = p_1 \cdot p_2 \cdots p_r$, where $(p_i, p_j) = 1$ for $i \neq j$. If one lets $a_1 = p_1 \cdot p_2 \cdots p_{r-1}$ and $b_1 = p_r$, by [15], [16] the cyclic matrix $\tilde{W}$ can be partitioned into $b_1^2 = p_r^2$ cyclic matrices each of block 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 partioned into b_2^2 cyclic matrices of block 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 cyclic matrices of block size $a_{i+1} \times a_{i+1}$. Otherwise, the procedure terminates. If the number of multiplications and additions needed to compute the cyclic convolution of p_i points is m_i and a_i for $i = 1, 2, \cdots, r$, respectively, then Winograd, Agarwal, and Cooley have shown in [16], [17] that the number of multiplications for computing a q'-point DFT is equal to $m_1 \cdot m_2 \cdots m_r$ and $a_1 p_2 \cdots p_r + m_1 a_2 p_3 \cdots p_r + m_1 m_2 a_3 p_4 \cdots p_r + \cdots + m_1 \cdots m_{r-1} a_r$, respectively.

TABLE I
COMPLEXITY OF HYBRID DFT FOR REAL AND COMPLEX DATA

$d = q'$	$q'-1$	No. Integer Mult. Real Data	No. Integer Add. Real Data	No. Integer Mult. Complex Data	No. Integer Add. Complex Data
367	$2 \cdot 3 \cdot 61$	488	61976	976	123952
373	$2^2 \cdot 3 \cdot 31$	620	41044	1240	82088
733	$2^2 \cdot 3 \cdot 61$	1220	153964	2440	307928
1831	$2 \cdot 3 \cdot 5 \cdot 61$	4880	607560	9760	1215120
1861	$2^2 \cdot 3 \cdot 5 \cdot 31$	6200	412920	12400	825840
2441	$2^3 \cdot 5 \cdot 61$	8540	1073600	17080	2147200

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, one can choose the prime q' to have the form

$$q' = 1 + (a \cdot 2^n) \cdot p \qquad \text{for } n = 1, 2, 3$$

where $p = 31$ or 61 and $a = 3$ or 5. Such values for the prime q' are 367, 373, 733, 1831, 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 $\tilde{W}$ can be partitioned into blocks of $p \times p$ cyclic matrices, such that the blocks form a $(2^n \cdot a) \times (2^n \cdot a)$ cyclic matrix. This cyclic matrix can be reduced further by Winograd's method. First $q'-1 = 2^n \cdot a \cdot p$ is an even number and $w^{2^n \cdot ap} = w^{-1}$ where w is the dth root of unity in the field of complex numbers. For such a case, Winograd showed that the elements in the $p \times p$ cyclic matrices finally required by the transform are either all real or imaginary numbers. To show this, consider the case $n = 1$. For this case, $q'-1 = 2 \cdot a \cdot p$. The permutation is given by $\sigma(i) = \alpha^i$ for $i = 1, 2, \cdots, ap, \cdots, 2ap$, where α is a generator of the multiplicative subgroup in $GF(q')$, consisting of $q'-1 = 2ap$ elements. Applying this permutation to (2) and using the fact that $\alpha^{ap} \equiv -1 \bmod q'$, one obtains the cyclic matrix equation in terms of w as follows:

$$\begin{bmatrix} \phi_0 \\ \phi_1 \\ \vdots \\ \phi_{m-2} \\ \phi_{m-1} \end{bmatrix} = \begin{bmatrix} x_1 x_2 & \cdots & x_{m/2} & & \cdots & x_m x_0 \\ x_2 x_3 & \cdots & x_{(m/2)+1} & & & x_0 x_1 \\ \vdots & & & & & \vdots \\ x_m x_0 x_1 & \cdots & & x_{(m/2)-1} & \cdots & x_{m-1} \\ x_0 x_1 x_2 & \cdots & & x_{m/2} & \cdots & x_m \end{bmatrix} \begin{bmatrix} y_0 \\ y_1 \\ \vdots \\ y_{m-2} \\ y_{m-1} \end{bmatrix} \tag{4}$$

where $m = 2ap$, $\phi_k = b_{\sigma(k)}$, $x_0 = w^{\alpha}$, $x_1 = w^{\alpha^2}, \cdots, x_{ap} = w^{-1}$, $x_{ap+1} = w^{-\alpha}, \cdots, x_{2ap} = w$ and $y_k = a_{\sigma(k)}$.

When it is clear, we let $[\ ]^C$ represent the cyclic convolu-

tion of a matrix as shown in (4). Also let $[\ ]^T$ denote the transpose of a matrix. Then (4) may be rewritten as

$$[\phi_0, \phi_1, \cdots, \phi_{m-2}, \phi_{m-1}]^T = [x_1, x_2, \cdots, x_{m/2}, \cdots, x_m, x_0]^C \cdot [y_0, y_1, \cdots, y_{m-2}, y_{m-1}]^T. \tag{5}$$

By [15], [16], the above cyclic $2 \times ap$ matrix equation can be partitioned into blocks of $ap \times ap$ cyclic matrices, so that the blocks form a 2×2 cyclic matrix. To illustrate this, note first that 2 and $a \cdot p$ are relatively prime. Thus, by the Chinese Remainder Theorem, an isomorphism exists between an integer k modulo m, the pairs of integers k_1 and k_2 modulo 2, and $a \cdot p$, respectively, i.e., $k \rightarrow (k_1, k_2)$. This relationship between k and (k_1, k_2) is

$$k = k_1 M_1^{-1} + k_2 M_2^{-1} \bmod m$$

where M_1^{-1} and M_2^{-1} satisfy the congruences $a \cdot pM_1^{-1} \equiv 1 \bmod 2$ and $2M_2^{-1} \equiv 1 \bmod a \cdot p$, respectively.

Let the variables $x_k = x_{(k_1,k_2)}$ be rearranged in the order

$$x_{(0,0)}, x_{(0,1)}, x_{(0,2)}, \cdots, x_{(0,ap-1)}, x_{(1,0)}, x_{(1,1)}, x_{(1,2)}, \cdots, x_{(1,ap-1)}.$$

If such a rearrangement is also made on the variables y_k and Φ_k, respectively, the cyclic convolution (5) has the block form

$$[X_1, X_2]^T = [A, B]^C [Y_1, Y_2]^T \tag{6}$$

where

$$X_1 = [\phi_{(0,0)}, \phi_{(0,1)}, \cdots, \phi_{(0,ap-1)}]^T,$$
$$X_2 = [\phi_{(1,0)}, \phi_{(1,1)}, \cdots, \phi_{(1,ap-1)}]^T,$$
$$Y_1 = [y_{(0,0)}, y_{(0,1)}, \cdots, y_{(0,ap-1)}]^T,$$
$$Y_2 = [y_{(1,0)}, y_{(1,1)}, \cdots, y_{(1,ap-1)}]^T,$$
$$A = [x_{(1,1)}, x_{(1,2)}, \cdots, x_{(1,ap-1)}, x_{(1,0)}]^C,$$

and

$$B = [x_{(0,1)}, x_{(0,2)}, \cdots, x_{(0,ap-1)}, x_{(0,0)}]^C.$$

Since

$$x_{(0,ap-1)} = w^{\alpha(0,ap-1)+(1,1)} = w^{\alpha(1,0)} = w^{-1},$$

then

$$x_{(1,j)} = w^{\alpha(1,j)+(1,1)} = w^{\alpha(0,j+1)} = w^{\alpha(1,0)+(1,j+1)} = w^{-\alpha(1,j+1)} = w^{-\alpha(0,j)+(1,1)} = x^*_{(0,j)},$$

for $j = 0, 1, \cdots, ap - 1$ where * denotes complex conjugation. Thus, in (6) the cyclic matrix A is the complex conjugate of the cyclic matrix B, i.e.,

$$A = B^*. \tag{7}$$

The matrix equation in (6) can be obtained by computing the set of coefficients of

$$T(u) \equiv (B + Au) \cdot (Y_2 + Y_1 u) \bmod (u^2 - 1) \tag{8}$$

where $u^2 - 1 \equiv (u - 1)(u + 1)$ and $u - 1$ and $u + 1$ are relatively prime polynomials.

Taking the congruences of $T(u)$ in (8) modulo $u - 1$ and $u + 1$, respectively,

$$T_1(u) \equiv (B + A) \cdot (Y_2 + Y_1) \bmod u - 1 \tag{9a}$$

and

$$T_2(u) \equiv (B - A) \cdot (Y_2 - Y_1) \bmod u + 1. \tag{9b}$$

By the Chinese Remainder Theorem $T(u)$ can be reconstituted from (9a) and (9b) as follows:

$$\begin{aligned} T(u) &= 2^{-1}[(B + A) \cdot (Y_2 + Y_1) - (B - A)(Y_2 - Y_1) \\ &\quad + ((B + A) \cdot (Y_2 + Y_1) + (B - A) \cdot (Y_2 - Y_1))u] \\ &= X_1 + X_2 u. \end{aligned}$$

This is reexpressed in matrix form as

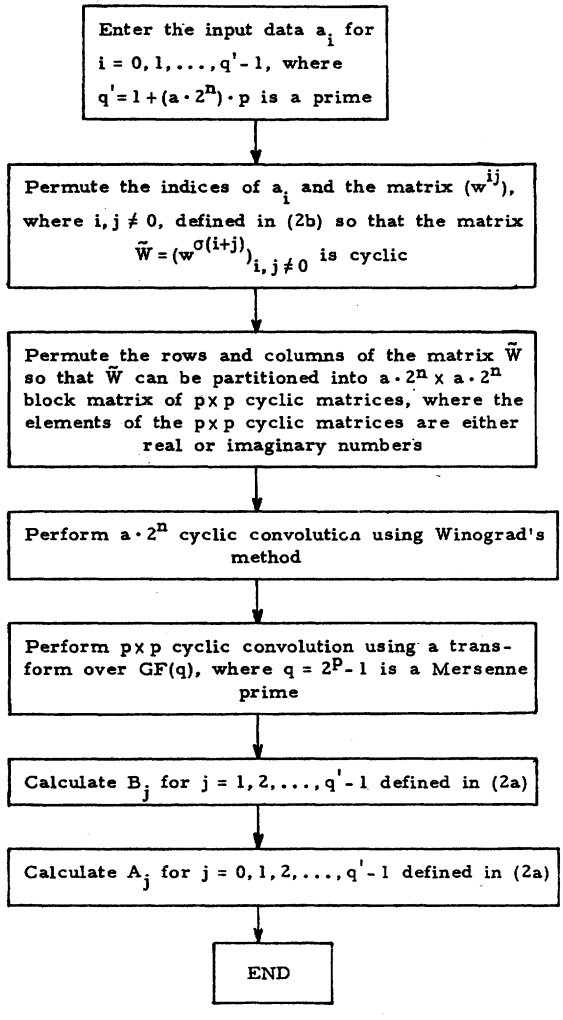
$$\begin{bmatrix} X_1 \\ X_2 \end{bmatrix} = \begin{bmatrix} (B + A) \cdot (Y_2 + Y_1) + (A - B) \cdot (Y_2 - Y_1) \\ (A + B) \cdot (Y_2 + Y_1) - (A - B) \cdot (Y_2 - Y_1) \end{bmatrix}. \tag{10}$$

By (7), the elements of the cyclic matrices $(B + A)$ and $(A - B)$ in (10) are evidently real and imaginary numbers. Since $(a, p) = 1$, the cyclic matrices $(B + A)$ and $(A - B)$ can be partitioned into blocks of $p \times p$ cyclic matrices such that the blocks themselves form $a \times a$ cyclic matrices. Thus, the elements of these $p \times p$ cyclic matrix blocks are either real numbers or imaginary numbers, never complex numbers. Hence, if the input datum is real, then a multiplication by an element in such a $p \times p$ cyclic matrix requires only one real multiplication. If the input datum is a complex number, then a multiplication by an element in such a $p \times p$ cyclic matrix requires two real multiplications.

Using a procedure precisely similar to that used above for $n = 1$, it can be shown that the elements in the required $p \times p$ cyclic matrices of the $2^n \cdot ap$ cyclic matrix for $n = 2, 3$ are also either real numbers or imaginary numbers. It was pointed out in the last section that a transform of length p over $GF(q)$ can be used to compute the cyclic convolution of p real number points. The register wordlength required to compute a transform of length p over $GF(q)$ is $p + 1$. The number of multiplications and additions needed to perform this convolution is p and $2(p - 1)p$, respectively. If one combines this with the number of multiplications and additions needed for Winograd's algorithm for the prime q', the total number of multiplications and additions required to perform a DFT of $d = q'$ real or complex number points can be computed. The results are shown in Table I.

It has been shown that Winograd's algorithm can be combined with a transform over $GF(q)$ to yield a new rather fast hybrid algorithm for computing the DFT of real and complex values. A flowchart of this new hybrid algorithm is shown on the following page.

HYBRID ALGORITHM FOR COMPUTING DFT FLOW-CHART



In this algorithm, it is necessary to compute the cyclic convolution of p real number points. This cyclic convolution of two p-point sequences of real number points is given by

$$c_k = \sum_{n=0}^{p-1} e_n f_{(k-n)} \qquad \text{for } k = 0, 1, 2, \cdots, p-1 \quad (11)$$

where c_k, e_n, $f_n \in GF(q)$, and $(k-n)$ denotes the residue of $k-n$ mod p. To compute this convolution the components of the truncated real number e_n and f_n must be converted first to integers a_n and b_n with dynamic ranges A and B, respectively. In [6], [9], it was shown that a sufficient dynamic range constraint for A and B is

$$A \leq \frac{q-1}{2Bp}. \quad (12)$$

If the circular convolution of a_n and b_n is denoted by c'_k for $k = 0, 1, 2, \cdots, p-1$, then using the procedure described in the example of [7], c'_k can be obtained by using fast transforms over $GF(q)$. c_k in (11) can be obtained by scaling back c'_k to the scale of the original real numbers for $k = 0, 1, 2, \cdots, p-1$. Evidently, the only error made in this computation of the c'_k's is the truncation error.

The dynamic range constraint A of the input sequence given in (12) is generally very pessimistic. It was shown in [19] that for integer convolutions, one can lessen the severity of the dynamic range constraint (12) and still maintain c_k in the interval $\pm(q-1)/2$ with a small probability of overflow.

To illustrate this new hybrid algorithm consider the following example.

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

$$a_n = 1 \qquad \text{for } n = 0, 2$$
$$= 0 \qquad \text{for } n = 1, 3, 4, 5, 6.$$

By (1), this transform is

$$A_0 = \sum_{i=0}^{6} a_i = 2 + \hat{i}0 \quad (13a)$$

and

$$A_j = a_0 + b_j \qquad \text{for } j = 1, 2, \cdots, 6 \quad (13b)$$

where

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

For $d = 7$, the permutation σ is given by $\sigma(i) = \alpha^i \bmod 7$ for $i = 1, 2, \cdots, 6$. Applying the above permutation to (13b), one obtains $\tilde{B} = \tilde{W}\tilde{a}$ as

$$[b_3, b_2, b_6, b_4, b_5, b_1]^T = [w^2, w^6, w^4, w^5, w^1, w^3]^C[a_3, a_2, a_6, a_4, a_5, a_1]^T. \quad (14)$$

By [15] and [16], there exists a permutation π of rows and columns so that the above cyclic matrix can be partitioned into 2×2 block matrix of 3×3 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 form

$$[B_1, B_2]^T = [C, D]^C[Z_1, Z_2]^T$$
$$= 2^{-1}[(C+D)(Z_1+Z_2) + (C-D)(Z_1-Z_2),$$
$$(C+D)(Z_1+Z_2) - (C-D)(Z_1-Z_2)]^T$$
$$= 2^{-1}[E+F, E-F]^T. \quad (15)$$

Since C and D are 3×3 cyclic matrices, it is evident that the matrices $C+D$ and $C-D$ are also 3×3 cyclic matrices. (Note that for a 6×6 cyclic matrix in (14), the powers of w in E and F in (15) are real numbers and imaginary numbers, respectively.) In (15), E is

$$E = [e_0, e_1, e_2]^T = [-0.445, 1.247, -1.802]^C[0, 1, 0]^T \quad (16)$$

where approximately $\frac{1}{2}\text{Re}(w^2 + w^5) = -0.445$, $\frac{1}{2}\text{Re}(w^1 +$

$w^6) = 1.247$, 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 equation defined in (16) can be obtained by computing the convolution of the two sequences a_n and y_n. This requires using a transform over $GF(q)$. In order to avoid overflow one needs to choose $q = 7$ so that the integer components of a_n, y_n lie in the interval $\pm(7-1)/2$.

By [7], 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 $GF(7)$ 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 $X_0 = 0$, $X_1 = 3$, and $X_2 = 1$.

Similarly, the transform over $GF(q)$ of sequence y_n is

$$Y_k = \sum_{n=0}^{3-1} y_n \cdot 2^{nk} = 2^k \qquad \text{for } k = 0, 1, 2.$$

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

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

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

In a similar fashion, matrix F, given in (15), can also be obtained as $f_0 = -\hat{i}$, $f_1 = \hat{i} \cdot 0$, and $f_2 = -\hat{i}$. Thus, by (15), one obtains $b_1 = \frac{1}{2}\hat{i}$, $b_2 = -\frac{1}{2}$, $b_3 = (1-\hat{i})/2$, $b_4 = (1+\hat{i})/2$, $b_5 = -\frac{1}{2}$, and $b_6 = -\hat{i}/2$. Hence, finally $A_0 = 2 + \hat{i}0$, $A_1 = 1 + \frac{1}{2}\hat{i}$, $A_2 = \frac{1}{2} + \hat{i}0$, $A_3 = \frac{1}{2}(3-\hat{i})$, $A_4 = \frac{1}{2}(3+\hat{i})$, $A_5 = \frac{1}{2} + \hat{i}0$, and $A_6 = 1 - \frac{1}{2}\hat{i}$. For this example, the dynamic range of $GF(7)$ is inadequate. Also, there is a large truncation error due to the course approximation used for 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 suggested above have more than adequate dynamic range to compute the DFT with small truncation error.

Transforms of Very Long Sequences

In order to compute the DFT of much longer sequences than considered in the last section, let $d = d_1 \cdot d_2 \cdots d_r$, where $(d_i, d_j) = 1$ for $i \neq j$. By using the Chinese Remainder Theorem [20], it is shown by Winograd in [14] that the DFT matrix W can be transformed into the direct product of W_1, $W_2, \cdots, W_r$, where W_i is the matrix of a d_i-point DFT. Assume the number of multiplications and additions used to perform the d_i-point DFT for $i = 1, 2, \cdots, r$ is m_i and a_i, respectively. Then, the number of multiplications and additions for computing a d-point DFT is $m_1 \cdot m_2 \cdots m_r$ and $a_1 d_2 \cdots d_r + m_1 a_2 d_3 \cdots d_r + m_1 m_2 a_3 d_4 \cdots p_r + m_1 \cdots m_{r-1} a_r$, respectively. To illustrate this, see Winograd's example for computing a 12-point DFT given in [16]. By the same procedure used in the computation of this example, the number of integer multiplications and additions needed to perform the transforms of longer sequences of complex numbers can be obtained by using Table I of this paper and [14, table I]. These numbers are given in Table II. The present algorithm and conventional FFT algorithm [21] are compared in Table II by giving the number of real multiplications and additions needed to perform these algorithms. The number of real multiplications and additions needed to perform a transform of a few thousand points is given in [14, table II].

TABLE II
COMPLEXITY OF NEW HYBRID ALGORITHM FOR DFT

d	Factors	New Algorithm		Radix-2 FFT	
		No. Integer Mult. Complex Data	No. Integer Add. Complex Data	No. Real Mult. $2d \log_2 d$	No. Real Add. $3d \log_2 d$
4096	2^{12}			98,304	147,456
4476	3 x 4 x 373	14,880	1,020,864		
8192	2^{13}			212,992	319,488
8796	3 x 4 x 733	28,800	3,765,504		
16384	2^{14}			458,752	688,128
20888	7 x 8 x 373	89,280	6,299,748		
32768	2^{15}			983,040	1,474,560
41048	7 x 8 x 733	175,680	22,936,068		
62664	3 x 7 x 8 x 373	267,840	19,149,900		
65536	2^{16}			2,097,152	3,145,728
123144	3 x 7 x 8 x 733	527,040	69,300,780		
131072	2^{17}			4,456,448	6684672
262144	2^{18}			9,437,184	14,155,776
268560	5 x 9 x 16 x 373	1,740,960	124,534,776		
524288	2^{19}			19,922,944	29,884,416
527760	5 x 9 x 16 x 733	3,425,760	450,573,816		

Acknowledgment

The authors wish to thank Dr. N. A. Renzetti, Manager of Tracking and Data Acquisition Engineering at the Jet Propulsion Laboratory for his continued support and encouragement of the research which led to this paper.

References

[1] J. M. Pollard, "The fast Fourier transform in a finite field," *Math. Comput.*, vol. 25, pp. 365–374, 1971.
[2] A. Schonhage and V. Strassen, "Schnelle multiplication grosser zahlen," *Computing*, vol. 7, pp. 281–292, 1971.
[3] C. M. Rader, "Discrete convolution via Mersenne transforms," *IEEE Trans. Comput.*, vol. C-21, pp. 1269–1273, Dec. 1972.
[4] R. C. Agarwal and C. S. Burrus, "Number theoretic transforms to implement fast digital convolution," *Proc. IEEE*, vol. 63, pp. 550–560, 1975.
[5] ——, "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.
[6] I. S. Reed and T. K. Truong, "The use of finite fields to compute convolution," *IEEE Trans. Inform. Theory*, vol. IT-21, pp. 208–213, 1975.
[7] ——, "Complex integer convolution over a direct sum of galois fields," *IEEE Trans. Inform. Theory*, vol. IT-21, pp. 657–661, 1975.
[8] E. Vegh and L. M. Leibowitz, "Fast complex convolution in finite rings," *IEEE Trans. Acoust., Speech, Signal Processing*, vol. ASSP-24, pp. 343–344, 1976.

[9] S. W. Golomb, I. S. Reed, and T. K. Truong, "Integer convolutions over the finite field $GF(3 \cdot 2^n + 1)$," *SIAM J. Appl. Math.*, vol. 32, Mar. 1977.
[10] J. M. Pollard, "Implementation of number-theoretic transforms," *Electro. Lett.*, vol. 12, pp. 378–379, 1976.
[11] K. Y. Liu, I. S. Reed, and T. K. Truong, "Fast number-theoretic transforms for digital filtering," *Electron. Lett.*, vol. 12, pp. 644–646, 1976.
[12] I. S. Reed, T. K. Truong, and K. Y. Liu, "A new fast algorithm for computing complex number-theoretic transforms," *Electron. Lett.*, pp. 278–280, 1977.
[13] I. S. Reed and T. K. Truong, "Fast Mersenne-prime transforms for digital filtering," *Proc. IEE*, vol. 125, pp. 433–440, May 1978.
[14] S. Winograd "On computing the discrete Fourier transform," *Proc. Nat. Acad. Sci. U.S.*, vol. 73, pp. 1005–1006, 1976.
[15] I. J. Good, "The interaction algorithm and practical Fourier analysis," *J. Royal Statis. Sci.*, Ser. B, vol. 20, pp. 361–372, 1958, "Addendum," vol. 22, MR 21 1674; MR 23 A 4231, pp. 372–375, 1960.
[16] S. Winograd, "On computing the discrete Fourier transform," Res. Dept. Math. Sci., IBM T. J. Watson Res. Ctr., Yorktown Hts., NY Res. Rep.
[17] R. C. Agarwal and J. W. Cooley, "New algorithm for digital convolution," *IEEE Trans. Acoust., Speech, Signal Processing*, vol. ASSP-25, pp. 392–410, Oct. 1977.
[18] C. M. Rader, "Discrete Fourier transforms when the number of data samples is prime," *Proc. IEEE*, vol. 56, pp. 1107–1108, June 1968.
[19] I. S. Reed, Y. S. Kwoh, T. K. Truong, and E. L. Hall, "X-ray reconstruction by finite field transforms," *IEEE Trans. Nucl. Sci.*, vol. NS-24, pp. 843–849, Feb. 1977.
[20] I. Niven and H. S. Zuckerman, *An Introduction to the Theory of Numbers*. New York: Wiley, 1966.
[21] 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.

Irving S. Reed (SM'69–F'73) was born in Seattle, WA, on November 12, 1923. He received the B.S. and Ph.D. degrees in mathematics from the California Institute of Technology, Pasadena, in 1944 and 1949, respectively.

From 1951 to 1960 he was associated with Lincoln Laboratory, Massachusetts Institute of Technology, Lexington. From 1960 to 1963 he was a Senior Staff Member of the RAND Corporation, Santa Monica, CA. Since 1963 he has been a Professor of Electrical Engineering and Computer Science at the University of Southern California, Los Angeles. He is also a Consultant to RAND and a Director of the Technology Corporation, Santa Monica, CA. His research interests include mathematics, computer design, coding theory, stochastic processes, and information theory.

T. K. Truong was born in Cholon, Vietnam, on December 4, 1944. He received the B.S. degree in electrical engineering from the National Cheng-Kung University, Taiwan, in 1967, and the M.S. degree in electrical engineering from Washington University, St. Louis, MO, in 1971, and the Ph.D. degree from the University of Southern California, Los Angeles, in 1976.

Since 1976 he has been with the System Engineering Technical Staff of the Jet Propulsion Laboratory, Pasadena, CA. He is also currently a part-time Research Scientist at the University of Southern California. His research interests include the areas of mathematics, computer logic, and coding theory.