Fast Algorithms for Computing Mersenne-Prime Number-Theoretic Transforms[1]

I. S. Reed
University of Southern California

T. K. Truong
TDA Engineering Office

It is shown that Winograd's algorithm can be used to compute an integer transform over GF(q), where q is a Mersenne prime. This new algorithm requires fewer multiplications than the conventional fast Fourier transform (FFT). This transform over GF(q) can be implemented readily on a digital computer. This fact makes it possible to more easily encode and decode BCH and RS codes.

I. Introduction

Several authors (Ref. 1 through 12) have shown that transforms over finite fields or rings can be used to compute numerical convolutions without round-off error. Recently, Winograd (Ref. 13) developed a new class of algorithms for computing the conventional discrete Fourier transform (DFT). This new algorithm requires substantially fewer multiplications than the conventional FFT algorithm.

In this paper, a type of Winograd algorithm is employed to evaluate the transform over $GF(q)$, where $q = 2^p - 1$ is a Mersenne prime. This transform is comparable in speed with that given by Winograd (Ref. 13 and 14).

Recently, the authors (Ref. 15 and 16) proposed that transforms over $GF(F_n)$, where $F_n = 2^{2^n} + 1$ for $n = 1, 2, 3, 4$ is a Fermat prime, can be used to define RS codes and to improve the decoding efficiency of these codes. Therefore, an FFT over $GF(q)$ can be used to decode RS codes.

In order to use the methods of Winograd for computing the transform over $GF(q)$, a new method for computing every factorization of the polynomial $u^{p-1} - 1$ over $GF(q)$ is developed. Finally, it is shown that continued fractions can be used instead of the usual Euclid's algorithm to find the required inverse element of the polynomial over the finite field $GF(q)$.

[1] This work was supported in part by the U.S. Air Force Office of Scientific Research under Grant AFOSR-75-2798.

II. Transforms Over *GF(q)*

Let $GF(q)$ be the finite field of residue classes modulo q, where $q = 2^p - 1$ is a Mersenne prime for $p = 2, 3, 5, 7, 13, 17, 19, 31, 61, \ldots$ Also let d be an integer that divides $q - 1$. Finally let the element $\gamma \epsilon GF(q)$ generate the cyclic subgroup of d elements, $G_d = (\gamma, \gamma^2, \ldots, \gamma^{d-1}, \gamma^d = 1)$ in the multiplicative group of $GF(q)$.

The transform over G_d is

$$A_j = \sum_{i=0}^{d-1} a_i \gamma^{ij} \text{ for } 0 \leqslant j \leqslant d - 1 \tag{1}$$

where $a_i \epsilon GF(q)$ for $0 \leqslant i \leqslant d - 1$

By Fermat's theorem, $2^p \equiv 2 \bmod p$. This implies $p|t$, where $t = q - 1 = 2^p - 2$. Also since $2^p - 2 \equiv 0 \bmod 3$ or 2, $t = 2^p - 2$ has the factors 2, 3, and p. The factorizations of the different numbers $t = 2^p - 2$ for $p = 13, 17, 31, 61$ are shown in Table 1. A multidimensional technique will be developed herein to calculate the transform defined in (1).

To perform the transform over $GF(q)$ defined in (1), it is necessary to find primitive elements in the d-element cyclic subgroup G_d in $GF(q)$. To do this, by (Ref. 5), it is shown that 3 is quadratic nonresidue mod q. Thus $3^{(2^p-2)/2} \equiv -1 \bmod q$. Hence by the same procedure used in the proof of Theorem 1 in Ref. 5, $\alpha = 3$ is a primitive element in $GF(q)$. Suppose $d = d_1 \cdot d_2 \ldots d_{r-1} d_r$ where $d_1 = 2, d_2 = 3, d_r = p$, and $d_i = 5, 7, 9, 11$, and 13 for $i = 3, 4, \ldots, r - 1$. The generator of G_d, a multiplicative subgroup of order d, is evidently $\gamma = \alpha^{(q-1)/d}$ where α is a primitive element of $GF(q)$. Also, γ^j is a primitive element in G_d since $(j,d) = 1$.

Now γ satisfies,

$$\gamma^d = 1 \bmod q \tag{2}$$

But also

$$2^p = 1 \bmod q \tag{3}$$

Thus, combining (2) and (3), a generator γ of G_d must exist that satisfies

$$\gamma^{d/p} = 2 \bmod q \tag{4}$$

A computer program can be used to find a primitive element γ of G_d that satisfies (4). By Th. 1, Ref.5, γ satisfied

$$\gamma^{d/2} = -1 \tag{5}$$

From (4), (5), we observe that integer multiplications by γ^{d/d_i} or its powers for $d_i = 2$ or p can be accomplished simply by circular shifts instead of multiplications. Hence, a d_i — point DFT for $d_i = 2$ or p can be evaluated without integer multiplications. It will be shown next that a d_i – point DFT for $d_i = 3, 5, 9, 11$, and 13 can be computed by using the Winograd algorithm.

III. Mathematical Preliminaries

In the next section the Chinese Remainder theorem for polynomials will be employed to compute fast transforms over $GF(q)$ of a small sequence. This well-known theorem is stated as follows without proof (see Ref. 17):

Theorem 1 (The Chinese Remainder theorem for polynomial): If $m_1(x), m_2(x), \ldots, m_k(x)$ are polynomials which are relatively prime in pairs, then the system of congruences $x(u) \equiv g_i(u) \bmod m_i(u)^{e_i}$ for $i = 1, 2, \ldots, k$ has a unique solution $x(u)$ given by

$$x(u) = \sum_{i=1}^{k} g_i(u) M_i(u) N_i(u) \tag{6a}$$

where

$$m(u) = m_1(u)^{e_1} m_2(u)^{e_2} \ldots m_k(u)^{e_k}$$

$$= m_1(u)^{e_1} M_1(u) = m_2(u)^{e_2} M_2(u) = \ldots = m_k(u)^{e_k} M_k(u)$$

and $N_i(x)$ uniquely satisfies (modulo $m_i(u)^{e_i}$) the congruence

$$M_i(u) N_i(u) \equiv 1 \bmod m_i(x)^{e_i} \tag{6b}$$

To compute the inverse element of $M(u)$, i.e., $N(u)$ required in (6b), let $S(u) = M_i(u)/m_i(u)$. Then, using a procedure precisely similar to that used for a rational element $S = a/q$, where $a \epsilon GF(q)$, described in Appendix A, it is possible to use continued fractions to develop a finite sequence of rational approximations to $S(u)$. The recursive formula for the convergents is given by

$$S_k(u) = \frac{a_k(u) p_{k-1}(u) - p_{k-2}(u)}{a_k(u) q_{k-1}(u) + q_{k-2}(u)} = \frac{p_k(u)}{q_k(u)} \tag{7}$$

where $p_{-1}(u) = 1, q_{-1}(u) = 0, p_0(u) = a_0(u)$, and $q_0(u) = 1$. The partial quotients $a_k(u)$ in (7) can be computed recursively by the following formula:

$$r_{k-2}(u) = a_k(u) r_{k-1}(u) + r_k(u), \deg r_k(u) < \deg r_{k-1}(u) \text{ for } k = 1, 2, \ldots, n-1 \tag{8}$$

where the initial conditions are $r_{-1}(u) = m_i(u), r_{-2} = M_i(u)$, and $r_{n-2}(u) = r_{n-1}(u) a_n(u)$.

By applying Euclid's algorithm to the polynomial $S(u)$ over $GF(q)$, we observe that $S_k(u) = p_k(u)/q_k(u)$ will terminate with $S_n(u) = M_i(u)/m_i(u)$ when $r_n(u) = 0$. By the same procedure used in the derivation of Eq. (6A), we obtain

$$M_i(u) q_{n-1}(u) - m_i(u) p_{n-1}(u) = (-1)^{n+1} \tag{9}$$

There are two cases to consider:

Case 1: If n is odd, then

$$M_i(u)q_{n-1}(u) + m_i(u)\,(-p_{n-1}(u)) = 1 \tag{10}$$

It follows that $N_i(u) = q_{n-1}(u)$ and $n_i(u) = -p_{n-1}(u)$ are solutions of $M(u)N_i(u) \equiv 1 \bmod m_i(u)$ and $m(u)n_i(u) \equiv 1 \bmod M_i(u)$, respectively.

Case II: If n is even, then

$$M_i(u)\,(-q_{n-1}(u)) + m_i(u)\,(p_{n-1}(u)) = 1 \tag{11}$$

Thus, $N_i(u) = -q_{n-1}(u)$ and $n_i(u) = p_{n-1}(u)$ are solutions of $N_i(u)M_i(u) \equiv 1 \bmod m_i(u)$ and $m_i(u)\,n_i(u) \equiv 1 \bmod M_i(u)$ respectively.

From (9), we see that it is necessary to compute the inverse element of a in $GF(q)$. To do this, let $S = a/q$. This inverse element is given by (A-7) in Appendix A.

The remainder of this section is based on ideas due to Winograd (Ref. 13). Let $X(u) = X_0 + X_1u + X_2u^2 + \ldots + X_nu^n$ and $Y(u) = Y_0 + Y_1u + Y_2u^2 + \ldots + Y_nu^n$ be two polynomials where $X_i,\ Y_i \epsilon GF(q)$. It is well known that the linear convolution of $X(u)$ and $Y(u)$ is the set of coefficients of the product of $X(u)$ and $Y(u)$, i.e., $T(u) = X(u) \cdot Y(u)$. By (Ref. 13), the number of multiplications required to compute the coefficients of $T(u)$ can be obtained by using the Chinese Remainder theorem for polynomials over $GF(q)$.

To show this, let us choose $m + n + 1$ distinct scalars, i.e., $\alpha_0, \alpha_1, \ldots, \alpha_{n+m}$. Then $T(u)$ with degree $n + m$ is equal to

$$T(u) = X(u) \cdot Y(u) \bmod (u - \alpha_0) \cdot (u - \alpha_1) \ldots (u - \alpha_{n+m}) \tag{12a}$$

or

$$T(u) = X(u) \cdot Y(u) \bmod \prod_{i=0}^{m+n-1} (u - \alpha_i) + X_nY_n \prod_{i=0}^{m+n-1} (u - \alpha_i) \tag{12b}$$

Since $(u - \alpha_i)$ for $i = 0, 1, \ldots, m + n$ are relatively prime in pairs, then by theorem 1, the system of congruences,

$$T_k(u) = X(\alpha_k) \cdot Y(\alpha_k) \equiv T(u) \bmod (u - \alpha_k) \text{ for } k = 0, 1, 2, \ldots, n + m$$

has a unique solution $T(u)$ given by

$$T(u) = \sum_{k=0}^{m+n} T_k(u)M_k(u)N_k(u)$$

where

$$m(u) = m_1(u)m_2(u), \ldots m_k(u)$$

$$= (u - \alpha_0)\,(u - \alpha_1) \ldots (u - \alpha_{n+m})$$

$$= m_0(u)M_0(u) = m_1(u)M_1(u) = \ldots = m_{m+n}(u)M_{m+n}(u)$$

and $N_k(u)$ uniquely satisfies (module $m_k(u)$) the congruences

$$M_k(u)N_k(u) \equiv 1 \bmod m_k(u) \text{ for } k = 0, 1, 2, \ldots, m + n$$

It can be shown that $T(u)$ given by (12a) can be reconstructed by

$$T(u) = \sum_{k=0}^{m+n} \left[\frac{\prod_{\substack{j=0 \\ j\neq k}}^{m+n} (u - \alpha_j)}{\prod_{\substack{j=0 \\ j\neq k}}^{m+n} (\alpha_k - \alpha_j)} \right] X(\alpha_k) \cdot Y(\alpha_k) \tag{13a}$$

If for example, one chooses $\alpha_k = \pm 2^n$ for $n \geqq 0$, then each $T_k(u) = X(\alpha_k) \cdot Y(\alpha_k)$ can be computed with one multiply. Similarly, $T(u)$ given by (12b) is given by

$$T(u) = \sum_{k=0}^{m+n-1} \left[\frac{\prod_{\substack{j=0 \\ j\neq k}}^{m+n-1} (u - \alpha_j)}{\prod_{\substack{j=0 \\ j\neq k}}^{m+n-1} (\alpha_k - \alpha_j)} \right] X(\alpha_k) \cdot Y(\alpha_k) + X_n Y_n \sum_{i=0}^{m+n-1} (u - \alpha_i) \tag{13b}$$

The cyclic convolution of $(X_0, X_1, \ldots, X_{n-1})$ and $(Y_0, Y_1, \ldots, Y_{n-1})$ can be expressed as

$$\begin{pmatrix} \Psi_0 \\ \Psi_1 \\ \cdot \\ \cdot \\ \cdot \\ \Psi_{n-1} \end{pmatrix} = \begin{pmatrix} X_0 & X_1 & \ldots & X_{n-2} & X_{n-1} \\ X_1 & X_2 & \ldots & X_{n-1} & X_0 \\ \cdot & & & & \\ \cdot & & & & \\ \cdot & & & & \\ X_{n-1} & X_0 & \ldots & X_{n-3} & X_{n-2} \end{pmatrix} \begin{pmatrix} Y_0 \\ Y_1 \\ \cdot \\ \cdot \\ \cdot \\ Y_{n-1} \end{pmatrix} \tag{13c}$$

As noted by Winograd, the cyclic $m \times n$ matrix in (13c) can be regarded as a "multiplication table" for the groups Z_n of the integers module n. If $n = n_1 \cdot n_2$, where n_1 and n_2 are relatively prime, then by the Chinese Remainder theorem (Theorem 1 above for the integers) Z_n is isomorphic to the direct product $Z_{n_1} \times Z_{n_2}$ of groups Z_{n_1} and Z_{n_2}. This fact is used to prove that a permutation of the rows and columns of the cyclic matrix in (13c) exists so that the resulting matrix is partitioned into blocks of $n_2 \times n_2$ cyclic matrices and so that the blocks form a $n_1 \times n_1$ cyclic matrix. This is proved in detail in Theorem 1 of Appendix B.

To illustrate the above, let n be $6 = 2 \cdot 3$. Since 2 and 3 are relatively prime, by the Chinese Remainder theorem an isomorphism

$$k \leftrightarrow (k_1, k_2)$$

exists between an integer k module 6 and the pair of integers k_1 and k_2 module 2 and 3, respectively, from the relationship,

$$k \equiv k_1 3 + k_2 4 \pmod 6$$

Now suppose one has the cyclic convolution,

$$\begin{pmatrix} \Psi_0 \\ \Psi_1 \\ \Psi_2 \\ \Psi_3 \\ \Psi_4 \\ \Psi_5 \end{pmatrix} = \begin{pmatrix} X_0 & X_1 & X_2 & X_3 & X_4 & X_5 \\ X_1 & X_2 & X_3 & X_4 & X_5 & X_0 \\ X_2 & X_3 & X_4 & X_5 & X_0 & X_1 \\ X_3 & X_4 & X_5 & X_0 & X_1 & X_2 \\ X_4 & X_5 & X_0 & X_1 & X_2 & X_3 \\ X_5 & X_0 & X_1 & X_2 & X_3 & X_4 \end{pmatrix} \begin{pmatrix} Y_0 \\ Y_1 \\ Y_2 \\ Y_3 \\ Y_4 \\ Y_5 \end{pmatrix} \tag{13d}$$

By Theorem 1 in Appendix B, there exists a permution defined by

$$\pi = \alpha^{-1}\beta = \begin{pmatrix} (0,0) & (0,1) & (0,2) & (1,0) & (1,1) & (1,2) \\ 0 & 4 & 2 & 3 & 1 & 5 \end{pmatrix} \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 \\ (0,0) & (0,1) & (0,2) & (1,0) & (1,1) & (1,2) \end{pmatrix}$$

$$= \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 \\ 0 & 4 & 2 & 3 & 1 & 5 \end{pmatrix}$$

of the rows and columns so that the above cyclic matrix can be partitioned into blocks of 3×3 cyclic matrices, such that the blocks form a 2×2 cyclic matrix. In other words, let the variable $Y_k = Y_{(k_1,k_2)}$, $X_k \equiv X_{(k_1,k_2)}$ and $\Psi_k \equiv \Psi_{(k_1,k_2)}$ be rearranged in such a manner that the first component k_1 of the index pair (k_1,k_2) is set to 0 and component k_2 is in ascending order, and that secondly component k_1 is set to 1 and component k_2 is in ascending order. The variable $X_{(k_1,k_2)}$ for (13c) are then rearranged in the order:

$$X_{(0,0)}, X_{(0,1)}, X_{(0,2)}, X_{(1,0)}, X_{(1,1)}, X_{(1,2)}$$

or in the variables X_k are in the order:

$$X_0, X_4, X_2, X_3, X_1, X_5$$

If such a rearrangement is made on variables Y_k, X_k, and Ψ_k, respectively, the cyclic convolution (13d) has the form,

$$\begin{pmatrix} \Psi_0 \\ \Psi_4 \\ \Psi_2 \\ \Psi_3 \\ \Psi_1 \\ \Psi_5 \end{pmatrix} = \begin{pmatrix} X_0 & X_4 & X_2 & X_3 & X_1 & X_5 \\ X_4 & X_2 & X_0 & X_1 & X_5 & X_3 \\ X_2 & X_0 & X_4 & X_5 & X_3 & X_1 \\ X_3 & X_1 & X_5 & X_0 & X_4 & X_2 \\ X_1 & X_5 & X_3 & X_4 & X_2 & X_0 \\ X_5 & X_3 & X_1 & X_2 & X_0 & X_4 \end{pmatrix} \begin{pmatrix} Y_0 \\ Y_4 \\ Y_2 \\ Y_3 \\ Y_1 \\ Y_5 \end{pmatrix} \tag{13e}$$

This cyclic matrix has been partitioned into 3 X 3 blocks of 2 X 2 matrices. This technique, due to Winograd, of partitioning cyclic matrices, will be used repeatedly in the next section.

It is also readily established that Ψ_k of the cyclic convolution (13c) is the k-th coefficient of the polynomial

$$T(u) = X(u)Y(u) \bmod (u^n - 1) \tag{13f}$$

where

$$X(u) = X_0 + X_1 u + \ldots + X_{n-1} u^{n-1}$$

and

$$Y(u) = Y_0 + Y_1 u + \ldots + Y_{n-1} u^{n-1}$$

Since $u^n - 1$ can be factored into polynomials over $GF(q)$, i.e.,

$$u^n - 1 = \prod_{i=1}^{k} g_k(u)$$

such that

$$(g_i(u), g_j(u)) = 1$$

for $j \neq i$, then, by the Chinese Remainder theorem, the coefficients of $T(u)$ mod $(u^n - 1)$ can be computed from the system of congruences defined by

$$T_i(u) = T(u) \bmod g_i(u) \text{ for } i = 1, 2, \ldots k \tag{14}$$

To get the factors, $g_i(u)$ defined in (14), first factor $u^n - 1$ into a product of irreducible polynomials. Each $g_i(u)$ is a product of one or more of these factors. Assume that α is an element of order n possible in some extension field of $GF(q)$. Then $\alpha^0, \alpha^1, \alpha^2, \ldots, \alpha^{n-1}$ are all roots of $u^n - 1$ over $GF(q)$. By Th. 4.32, Ref. 17, it follows that

$$u^n - 1 = \prod_{\substack{d \\ d|n}} Q^{(d)}(u) \tag{15}$$

where $Q^{(d)}(u)$ is a polynomial whose roots are all elements of order d. $Q^{(d)}(u)$ is called the cyclotomic polynomial. By Th. 4.33, Ref. 17, the cyclotomic polynomial is given by

$$Q^{(d)}(u) = \prod_{\substack{d \\ k|d}} (u^{d/k} - 1)^{\mu(d)} \tag{16}$$

where $\mu(d)$ is the Moebius function defined by

$$\mu(d) = \begin{cases} 1 & \text{if } d = 1 \\ (-1)^k & \text{if } d \text{ is the product of } k \text{ distinct primes} \\ 0 & \text{if } d \text{ contains any repeated prime factors.} \end{cases}$$

If n is a factor of $q - 1 = 2^p - 1$, then one can find an element α of order n in $GF(q)$ such that $\alpha^0, \alpha^1, \ldots, \alpha^{n-1}$ are elements in $GF(q)$ and roots of $u^n - 1$. That is,

$$u^n - 1 = \sum_{i=0}^{n-1} (u - \alpha^i), \text{ where } \alpha^i \epsilon GF(q)$$

Otherwise, one needs to compute the factorization of the $Q^{(d)}(u)$ into irreducible factors. To achieve this, if α is a root of $Q^{(d)}(u)$ with degree ℓ, then α is an element of order d in some field of characteristic q. By Th. 4.408, Ref. 17, α^{p^i} for $i = 0, 1, 2, \ldots, \ell - 1$ are all roots of $Q^{(d)}(u)$. Suppose β is one of these roots. There are two cases to consider:

Case I: If $q \equiv 1 \bmod n$, then $\beta^q \equiv \beta \bmod q$. By Th. 4.407, Ref. 17, β is an element in $GF(q)$, thus, the factorization of $Q^{(d)}(u)$ is

$$Q^{(d)}(u) = \sum_{i=0}^{\ell-1} (u - \alpha_i), \text{ where } \alpha_i \epsilon GF(q)$$

Case II: If $q \not\equiv 1 \bmod n$, then $\beta^q \not\equiv \beta \bmod q$. By Th. 4.407, Ref. 17, this implies that $\beta \notin GF(q)$. Thus, $Q^{(d)}(u)$ is an irreducible polynomial over $GF(q)$.

IV. Winograd's Algorithm for Computing the Transform over *GF(q)*

The discrete Fourier transform can be defined by

$$A_0 = \sum_{i=0}^{d-1} a_i \tag{17a}$$

and

$$A_j = a_0 + \sum_{i=1}^{d-1} a_i \gamma^{ij} \text{ for } j = 1, 2, \ldots, d-1$$

or

$$A = B + Ia_0 = Wa + Ia_0 \tag{17b}$$

where

$$B = \begin{pmatrix} b_1 \\ b_2 \\ \cdot \\ \cdot \\ \cdot \\ b_{d-1} \end{pmatrix}, \quad W = (\gamma^{ij})_{i,j\neq 0}, \quad a = \begin{pmatrix} a_1 \\ a_2 \\ \cdot \\ \cdot \\ \cdot \\ a_{d-1} \end{pmatrix}$$

and I is a unit matrix. If d is a prime, i.e., $d = p$, one can find an element $\alpha \in GF(p)$ which generates the cyclic subgroup of $d-1$ elements, so that a permutation or substitution σ can be defined by

$$\sigma = \begin{pmatrix} 1, 2, & \ldots & p-2, p-1 \\ \alpha, \alpha^2, & \ldots & \alpha^{p-2}, \alpha^{p-1} = 1 \end{pmatrix}$$

Using the above permutation, one can permute the indices of B, defined in (17b), so that the matrix $\overline{W} = (\gamma^{\sigma(i)\sigma(j)})_{i,j\neq 0}$ is cyclic. That is,

$$B_{\sigma(j)} = \sum_{i=1}^{p-1} a_{\sigma(i)} \gamma^{\sigma(i)\sigma(j)} \text{ for } j = 1, 2, \ldots, p-1$$

or

$$\overline{B} = \overline{W}\,\overline{a} \tag{18}$$

where

$$\bar{B} = \begin{pmatrix} B_{\sigma(1)} \\ B_{\sigma(2)} \\ \cdot \\ \cdot \\ \cdot \\ B_{\sigma(p-1)} \end{pmatrix}, \quad \bar{W} = (\gamma^{\sigma(i)\sigma(j)})_{i,j\neq 0}$$

and

$$\bar{a} = \begin{pmatrix} a_{\sigma(1)} \\ a_{\sigma(2)} \\ \cdot \\ \cdot \\ \cdot \\ a_{\sigma(p-1)} \end{pmatrix}$$

From (18), $B_{\sigma(j)}$ is a cyclic convolution of $a_{\sigma(p-j)}$ and $\gamma^{\sigma(j)}$ for $j = 1, 2, \ldots, p-1$. Thus by the last section Eq. (18) is the set of coefficients of

$$T(u) = \left(\sum_{i=1}^{p-1} a_{\sigma(p-i)} u^{i-1}\right)\left(\sum_{i=1}^{p-1} \gamma^{\sigma(i)} u^{i-1}\right) \bmod u^{p-1} - 1$$

Using the algorithm for factoring the polynomial $u^n - 1$ over $GF(q)$, described at the end of the last section, one can factor $u^{p-1} - 1$ over $GF(q)$ into irreducible relatively prime factors. That is,

$$u^{p-1} - 1 = \prod_{i=1}^{k} g_i(u), \text{ where } (g_i(u), g_j(u)) = 1 \text{ for } i \neq j$$

After computing the residues of $T(u)$ mod $g_i(u)$ for $i = 1, 2, \ldots k$, the Chinese Remainder theorem can be used to evaluate $T(u)$ with these residues. If $d = p^r$ is a factor of q, where $p \neq 2$, the number of integers relatively prime to p^r is $(p-1)p^{r-1}$. In this case, by Ref. 18, a set

$$\left\{\gamma, \gamma^2, \ldots, \gamma^{(p-1)p^{r-1}} = 1\right\}$$

in $GF(q)$ can be found which is a cyclic group. Thus, by a procedure similar to that used to compute the above case for $d = p$, a p^r point DFT can be obtained.

Now consider a d_i-point DFT over $GF(q)$ for d_i = 3 or 5 or 7 or 9 or 11 or 13. For a 3-point DFT over $GF(q)$, it is straightforward to show that the number of multiplications used to perform this transform is 2. Consider $d_i = 5$. Since 2 is a primitive element in $GF(5)$, the permutation σ is given by

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

using the above permutation, the matrix $\bar{B}$ in (17b) is

$$\bar{B} = \bar{w}\ \bar{a}$$

where

$$\bar{B} = \begin{pmatrix} b_{\sigma(1)} \\ b_{\sigma(2)} \\ b_{\sigma(3)} \\ b_{\sigma(4)} \end{pmatrix}, \quad \bar{W} = (\gamma^{\sigma(i)\sigma(j)})_{i,j \neq 0} \text{ and } \bar{a} = \begin{pmatrix} a_{\sigma(1)} \\ a_{\sigma(2)} \\ a_{\sigma(3)} \\ a_{\sigma(4)} \end{pmatrix}$$

More explicitly $\bar{B}$ is

$$\begin{pmatrix} b_2 \\ b_4 \\ b_3 \\ b_1 \end{pmatrix} = \begin{pmatrix} \gamma^4, \gamma^3, \gamma, \gamma^2 \\ \gamma^3, \gamma, \gamma^2, \gamma^4 \\ \gamma, \gamma^2, \gamma^4, \gamma^3 \\ \gamma^2, \gamma^4, \gamma^3, \gamma \end{pmatrix} \begin{pmatrix} a_2 \\ a_4 \\ a_3 \\ a_1 \end{pmatrix} \tag{19}$$

where γ is a 5th root of unity in $GF(q)$. $T(u)$ in (19) is obtained by computing the set of coefficients of

$$T(u) = X(u) \cdot Y(u)$$

$$= (\gamma^2 + \gamma^4 u + \gamma^3 u^2 + \gamma u^3) \cdot (a_1 + a_3 u + a_4 u^2 + a_2 u^3) \bmod u^4 - 1 = (u - 1)(u + 1)(u^2 + 1)$$

Let

$$m(u) = (u - 1)(u + 1)(u^2 + 1) = m_1(u) m_2(u) m_3(u)$$

$$= m_1(u) M_1(u) = m_2(u) M_2(u) = m_3(u) M_3(u)$$

The system of congruences $T(u) \equiv T_i(u) \bmod m_i(u)$ for $i = 1, 2, 3$ is given by

$$T_1(u) = X(1) \cdot Y(1) \equiv (\gamma^2 + \gamma^4 + \gamma^3 + \gamma) \cdot (a_1 + a_3 + a_4 + a_2)$$

$$\equiv -(a_1 + a_3 + a_4 + a_2) \equiv C_1 \bmod u - 1,$$

$$T_2(u) = X(-1) \cdot Y(-1) \equiv (\gamma^2 - \gamma^4 + \gamma^3 - \gamma) \cdot (a_1 - a_3 + a_4 - a_2)$$

$$\equiv C_2 \bmod u + 1,$$

and

$$T_3(u) = X(u) \cdot Y(u)$$

$$\equiv [(\gamma^4 - \gamma)\, u + (\gamma^2 - \gamma^3)] \cdot [(a_3 - a_2)\, u + (a_1 - a_4)]$$

$$\equiv [(au + b) \cdot (cu + d)] \bmod u^2 + 1 \tag{20}$$

where

$$C_1, C_2, a, b, c, d \epsilon GF(q)$$

In order to compute (20), by Eq. (12b),

$$B(u) = (au + b)\,(cu + d)$$

$$= (au + b)\,(cu + d) \bmod u(u + 1) + a \cdot c\, u(u + 1)$$

Let

$$R(u) = (au + b)\,(cu + d) \bmod u(u + 1)$$

Then,

$$R_1(u) \equiv b \cdot d \equiv K_1 \bmod u,$$

$$R_2(u) \equiv (b - a) \cdot (d - c) \equiv K_2 \bmod u + 1,$$

where $K_1, K_2 \epsilon GF(q)$. Using Eq. (6a) this yields

$$R(u) = K_1 + (K_1 - K_2)u$$

Thus,

$$B(u) = K_1 + (K_1 - K_2 + K_3)u + K_3u^2, \text{ where } K_3 = a \cdot c$$

Hence,

$$T_3(u) \equiv (K_1 - K_3) + (K_1 - K_2 + K_3)u$$

$$\equiv C_3 + C_4u \bmod u^2 + 1$$

where

$$C_3 = K_1 - K_3 \text{ and } C_4 = (K_1 - K_2 + K_3)$$

Using Eq. (6a), $T(u)$ is

$$T(u) = 2^{p-2}(C_1 - C_2 - 2C_4)u^3 + (C_1 + C_2 - C_3)u^2 + (C_1 - C_2 + 2C_4)u + (C_1 + C_2 + 2C_3)$$

$$= b_1u^3 + b_3u^2 + b_4u + b_2$$

It follows from this example that the number of integer multiplications used to perform a 5-point transform is 4.

For $d_i = 7$, 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 (17b), one obtains $\overline{B} = \overline{W}\overline{a}$ as

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

where γ is a 7th root of unity in $GF(q)$.

In the last section it was mentioned that there exists a permutation π of rows and columns so that the above cyclic matrix can be partitioned into a 2 X 2 block matrix of 3 X 3 cyclic blocks in the manner given in (13e). This permutation of the rows and columns is

$$\begin{pmatrix} b_3 \\ b_5 \\ b_6 \\ b_4 \\ b_2 \\ b_7 \end{pmatrix} = \begin{pmatrix} \gamma^2\gamma^1\gamma^4\gamma^5\gamma^6\gamma^3 \\ \gamma^1\gamma^4\gamma^2\gamma^6\gamma^3\gamma^5 \\ \gamma^4\gamma^2\gamma^1\gamma^3\gamma^5\gamma^6 \\ \gamma^5\gamma^6\gamma^3\gamma^2\gamma^1\gamma^4 \\ \gamma^6\gamma^3\gamma^5\gamma^1\gamma^4\gamma^2 \\ \gamma^3\gamma^5\gamma^6\gamma^4\gamma^2\gamma^1 \end{pmatrix} \begin{pmatrix} a_3 \\ a_5 \\ a_6 \\ a_4 \\ a_2 \\ a_7 \end{pmatrix} \tag{21a}$$

This has the form

$$\begin{pmatrix} E_1 \\ E_2 \end{pmatrix} = \begin{pmatrix} A & B \\ B & A \end{pmatrix} \begin{pmatrix} Y_1 \\ Y_2 \end{pmatrix} = 2^{-1} \begin{pmatrix} (A+B)(Y_1+Y_2)+(A-B)(Y_1-Y_2) \\ (A+B)(Y_1+Y_2)-(A-B)(Y_1-Y_2) \end{pmatrix}$$

$$= 2^{p-1} \begin{pmatrix} D+E \\ D-E \end{pmatrix} \tag{21b}$$

Since A and B are cyclic matrices, it is evident that the matrices $A + B$ and $A - B$ are also cyclic matrices. In (21b), D is defined as

$$D = \begin{pmatrix} d_0 \\ d_1 \\ d_2 \end{pmatrix} = \begin{pmatrix} X_0 & X_1 & X_2 \\ X_1 & X_2 & X_0 \\ X_2 & X_0 & X_1 \end{pmatrix} \begin{pmatrix} Y_0 \\ Y_1 \\ Y_2 \end{pmatrix} \tag{22}$$

This matrix can be obtained by computing the set of coefficients of

$$T(u) = (X_2 + X_0u + X_1u^2)(Y_2 + Y_1u + Y_0u^2) \bmod u^3 - 1 = (u-1)(u^2+u+1) \tag{23}$$

The system of congruences, given in (23), is

$$T_1(u) = (X_0 + X_1 + X_2) \cdot (Y_0 + Y_1 + Y_2) \equiv C_1 \bmod (u-1)$$

and

$$T_2(u) \equiv [(X_2 - X_1) + (X_0 - X_1)u] \cdot [(Y_2 - Y_0) + (Y_1 - Y_0)u]$$

$$\equiv C_2 + C_3u \bmod u^2 + u + 1$$

where $C_1, C_2, C_3 \epsilon GF(q)$. By the same procedure for computing Eq. (20), $T_2(u)$ can be obtained, using only 3 multiplications. By (6a), $T(u)$ is given by

$$T(u) = [3^{-1}(C_1 + C_2 + C_3) - C_2] + [3^{-1}(C_1 + C_2 + C_3) - C_3]\, u + [3^{-1}(C_1 + C_2 + C_3)]u^2$$

$$= d_0 + d_1 u + d_2 u^2 \tag{24}$$

In a similar fashion matrix E, given in (21b), can also be obtained. Thus, the number of multiplications used to perform a 7-point transform is 8.

Consider $d_i = 3^2$. Since the integers 1, 2, 4, 5, 7, 8 are relatively prime to 9, the permutation σ is defined by

$$\sigma = \begin{pmatrix} 1, 2, 4, 5, 7, 8 \\ 2, 4, 8, 7, 5, 1 \end{pmatrix} \tag{25}$$

Rearranging the rows and columns of B in such a manner that the elements of the matrix with indices relatively prime to 9 form a block, one has,

$$\begin{pmatrix} b_1 \\ b_2 \\ b_4 \\ b_5 \\ b_7 \\ b_8 \\ b_3 \\ b_6 \end{pmatrix} = \begin{pmatrix} \gamma^{1\cdot1}, \gamma^{1\cdot2}, \gamma^{1\cdot4}, \gamma^{1\cdot5}, \gamma^{1\cdot7}, \gamma^{1\cdot8}, \gamma^{1\cdot3}, \gamma^{1\cdot6} \\ \gamma^{2\cdot1}, \gamma^{2\cdot2}, \gamma^{2\cdot4}, \gamma^{2\cdot5}, \gamma^{2\cdot7}, \gamma^{2\cdot8}, \gamma^{2\cdot3}, \gamma^{2\cdot6} \\ \gamma^{4\cdot1}, \gamma^{4\cdot2}, \gamma^{4\cdot4}, \gamma^{4\cdot5}, \gamma^{4\cdot7}, \gamma^{4\cdot8}, \gamma^{4\cdot3}, \gamma^{4\cdot6} \\ \gamma^{5\cdot1}, \gamma^{5\cdot2}, \gamma^{5\cdot4}, \gamma^{5\cdot5}, \gamma^{5\cdot7}, \gamma^{5\cdot8}, \gamma^{5\cdot3}, \gamma^{5\cdot6} \\ \gamma^{7\cdot1}, \gamma^{7\cdot2}, \gamma^{7\cdot4}, \gamma^{7\cdot5}, \gamma^{7\cdot7}, \gamma^{7\cdot8}, \gamma^{7\cdot3}, \gamma^{5\cdot6} \\ \gamma^{8\cdot1}, \gamma^{8\cdot2}, \gamma^{8\cdot4}, \gamma^{8\cdot5}, \gamma^{8\cdot7}, \gamma^{8\cdot8}, \gamma^{8\cdot3}, \gamma^{8\cdot6} \\ \gamma^{3\cdot1}, \gamma^{3\cdot2}, \gamma^{3\cdot4}, \gamma^{3\cdot5}, \gamma^{3\cdot7}, \gamma^{3\cdot8}, \gamma^{3\cdot3}, \gamma^{3\cdot6} \\ \gamma^{6\cdot1}, \gamma^{6\cdot2}, \gamma^{6\cdot4}, \gamma^{6\cdot5}, \gamma^{6\cdot7}, \gamma^{6\cdot8}, \gamma^{6\cdot3}, \gamma^{6\cdot6} \end{pmatrix} \begin{pmatrix} a_1 \\ a_2 \\ a_4 \\ a_5 \\ a_7 \\ a_8 \\ a_3 \\ a_6 \end{pmatrix} \tag{26}$$

Define the upper left 6 X 6 matrix of (26) as

$$\begin{pmatrix} y_1 \\ y_2 \\ y_4 \\ y_5 \\ y_7 \\ y_8 \end{pmatrix} = \begin{pmatrix} \gamma^{1\cdot1}, \gamma^{1\cdot2}, \gamma^{1\cdot4}, \gamma^{1\cdot5}, \gamma^{1\cdot7}, \gamma^{1\cdot8} \\ \gamma^{2\cdot1}, \gamma^{2\cdot2}, \gamma^{2\cdot4}, \gamma^{2\cdot5}, \gamma^{2\cdot7}, \gamma^{2\cdot8} \\ \gamma^{4\cdot1}, \gamma^{4\cdot2}, \gamma^{4\cdot4}, \gamma^{4\cdot5}, \gamma^{4\cdot7}, \gamma^{4\cdot8} \\ \gamma^{5\cdot1}, \gamma^{5\cdot2}, \gamma^{5\cdot4}, \gamma^{5\cdot5}, \gamma^{5\cdot7}, \gamma^{5\cdot8} \\ \gamma^{7\cdot1}, \gamma^{7\cdot2}, \gamma^{7\cdot4}, \gamma^{7\cdot5}, \gamma^{7\cdot7}, \gamma^{7\cdot8} \\ \gamma^{8\cdot1}, \gamma^{8\cdot2}, \gamma^{8\cdot4}, \gamma^{8\cdot5}, \gamma^{8\cdot7}, \gamma^{8\cdot8} \end{pmatrix} \begin{pmatrix} a_1 \\ a_2 \\ a_4 \\ a_5 \\ a_7 \\ a_8 \end{pmatrix} \tag{27}$$

Applying the permutations defined in (25) to the indices of (26), one obtains

$$\begin{pmatrix} y_2 \\ y_4 \\ y_8 \\ y_7 \\ y_5 \\ y_1 \end{pmatrix} = \begin{pmatrix} \gamma^4, \gamma^8, \gamma^7, \gamma^5, \gamma^1, \gamma^2 \\ \gamma^8, \gamma^7, \gamma^5, \gamma^1, \gamma^2, \gamma^4 \\ \gamma^7, \gamma^5, \gamma^1, \gamma^2, \gamma^4, \gamma^8 \\ \gamma^5, \gamma^1, \gamma^2, \gamma^4, \gamma^8, \gamma^7 \\ \gamma^1, \gamma^2, \gamma^4, \gamma^8, \gamma^7, \gamma^5 \\ \gamma^2, \gamma^4, \gamma^8, \gamma^7, \gamma^5, \gamma^1 \end{pmatrix} \begin{pmatrix} a_2 \\ a_4 \\ a_8 \\ a_7 \\ a_5 \\ a_1 \end{pmatrix}$$

By a similar procedure used to partition the matrix (13e) the above matrix becomes a 2 X 2 block matrix of 3 X 3 cyclic blocks as follows:

$$\begin{pmatrix} y_2 \\ y_5 \\ y_8 \\ y_7 \\ y_4 \\ y_1 \end{pmatrix} = \begin{pmatrix} \gamma^4, \gamma^1, \gamma^7, \gamma^5, \gamma^8, \gamma^2 \\ \gamma^1, \gamma^7, \gamma^4, \gamma^8, \gamma^2, \gamma^5 \\ \gamma^7, \gamma^4, \gamma^1, \gamma^2, \gamma^5, \gamma^8 \\ \gamma^5, \gamma^8, \gamma^2, \gamma^4, \gamma^1, \gamma^7 \\ \gamma^8, \gamma^2, \gamma^5, \gamma^1, \gamma^7, \gamma^4 \\ \gamma^2, \gamma^5, \gamma^8, \gamma^7, \gamma^4, \gamma^1 \end{pmatrix} \begin{pmatrix} a_2 \\ a_5 \\ a_8 \\ a_7 \\ a_4 \\ a_1 \end{pmatrix} \tag{28}$$

Using the same procedure for computing the 6 X 6 cyclic matrix, described previously, we know that the number of multiplications required to perform (28) is 8. The last two columns of the matrix defined in (26) can be obtained by computing the following 2 X 2 cyclic matrix,

$$\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} \gamma^3 & \gamma^6 \\ \gamma^6 & \gamma^3 \end{pmatrix} \begin{pmatrix} a_3 \\ a_6 \end{pmatrix} \tag{29}$$

The last two rows of the matrix defined in (26) can be obtained by computing the following cyclic matrix

$$\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} \gamma^3 & \gamma^6 \\ \gamma^6 & \gamma^3 \end{pmatrix} \begin{pmatrix} a_1 + a_4 + a_7 \\ a_2 + a_5 + a_8 \end{pmatrix} \tag{30}$$

Note that the computation of (29) and (30) are the same as computing the 2 X 2 cyclic matrix in a 3-point DFT. Hence, the total number of multiplications used to perform this transform is 12.

For $d_i = 11$, the permutation σ is given by

$$\sigma = \begin{pmatrix} 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 \\ 2, 4, 8, 5, 10, 9, 7, 3, 6, 1 \end{pmatrix}$$

Applying the above permutation to (17b) one obtains $\overline{B} = \overline{W}\overline{a}$, i.e.,

$$\begin{pmatrix} b_2 \\ b_4 \\ b_8 \\ b_5 \\ b_{10} \\ b_9 \\ b_7 \\ b_3 \\ b_6 \\ b_1 \end{pmatrix} = \begin{pmatrix} \gamma^4, \gamma^8, \gamma^5, \gamma^{10}, \gamma^9, \gamma^7, \gamma^3, \gamma^6, \gamma^1, \gamma^2 \\ \gamma^8, \gamma^5, \gamma^{10}, \gamma^9, \gamma^7, \gamma^3, \gamma^6, \gamma^1, \gamma^2, \gamma^4 \\ \gamma^5, \gamma^{10}, \gamma^9, \gamma^7, \gamma^3, \gamma^6, \gamma^1, \gamma^2, \gamma^4, \gamma^8 \\ \gamma^{10}, \gamma^9, \gamma^7, \gamma^3, \gamma^6, \gamma^1, \gamma^2, \gamma^4, \gamma^8, \gamma^5 \\ \gamma^9, \gamma^7, \gamma^3, \gamma^6, \gamma^1, \gamma^2, \gamma^4, \gamma^8, \gamma^5, \gamma^{10} \\ \gamma^7, \gamma^3, \gamma^6, \gamma^1, \gamma^2, \gamma^4, \gamma^8, \gamma^5, \gamma^{10}, \gamma^9 \\ \gamma^3, \gamma^6, \gamma^1, \gamma^2, \gamma^4, \gamma^8, \gamma^5, \gamma^{10}, \gamma^9, \gamma^7 \\ \gamma^6, \gamma^1, \gamma^2, \gamma^4, \gamma^8, \gamma^5, \gamma^{10}, \gamma^9, \gamma^7, \gamma^3 \\ \gamma^1, \gamma^2, \gamma^4, \gamma^8, \gamma^5, \gamma^{10}, \gamma^9, \gamma^7, \gamma^3, \gamma^6 \\ \gamma^2, \gamma^4, \gamma^8, \gamma^5, \gamma^{10}, \gamma^9, \gamma^7, \gamma^3, \gamma^6, \gamma^1 \end{pmatrix} \begin{pmatrix} a_2 \\ a_4 \\ a_8 \\ a_5 \\ a_{10} \\ a_9 \\ a_7 \\ a_3 \\ a_6 \\ a_1 \end{pmatrix}$$

where γ is a 11th root of unity in $GF(q)$. By the same procedure used to partition the matrix given in (13e) and (21a) the above matrix can be partitioned into blocks of 5×5 cyclic matrices, such that the blocks form a 2×2 cyclic matrix. That is,

$$\begin{pmatrix} b_2 \\ b_7 \\ b_8 \\ b_6 \\ b_{10} \\ b_9 \\ b_4 \\ b_3 \\ b_5 \\ b_1 \end{pmatrix} = \begin{pmatrix} \gamma^4, \gamma^3, \gamma^5, \gamma^1, \gamma^9 & \gamma^7, \gamma^8, \gamma^6, \gamma^{10}, \gamma^2 \\ \gamma^3, \gamma^5, \gamma^1, \gamma^9, \gamma^4 & \gamma^8, \gamma^6, \gamma^{10}, \gamma^2, \gamma^7 \\ \gamma^5, \gamma^1, \gamma^9, \gamma^4, \gamma^3 & \gamma^6, \gamma^{10}, \gamma^2, \gamma^7, \gamma^8 \\ \gamma^1, \gamma^9, \gamma^4, \gamma^3, \gamma^5 & \gamma^{10}, \gamma^2, \gamma^7, \gamma^8, \gamma^6 \\ \gamma^9, \gamma^4, \gamma^3, \gamma^5, \gamma^1 & \gamma^2, \gamma^7, \gamma^8, \gamma^6, \gamma^{10} \\ \gamma^7, \gamma^8, \gamma^6, \gamma^{10}, \gamma^2 & \gamma^4, \gamma^3, \gamma^5, \gamma^1, \gamma^9 \\ \gamma^8, \gamma^6, \gamma^{10}, \gamma^2, \gamma^7 & \gamma^3, \gamma^5, \gamma^1, \gamma^9, \gamma^4 \\ \gamma^6, \gamma^{10}, \gamma^2, \gamma^7, \gamma^8 & \gamma^5, \gamma^1, \gamma^9, \gamma^4, \gamma^3 \\ \gamma^{10}, \gamma^2, \gamma^7, \gamma^8, \gamma^6 & \gamma^1, \gamma^9, \gamma^4, \gamma^3, \gamma^5 \\ \gamma^2, \gamma^7, \gamma^8, \gamma^6, \gamma^{10} & \gamma^9, \gamma^4, \gamma^3, \gamma^5, \gamma^1 \end{pmatrix} \begin{pmatrix} a_2 \\ a_7 \\ a_8 \\ a_6 \\ a_{10} \\ a_9 \\ a_4 \\ a_3 \\ a_5 \\ a_1 \end{pmatrix}$$

This has a form similar to the matrix (21b), where A and B are 5×5 cyclic matrices. The corresponding 5-point vectors D and E can be obtained by direct computations without using 5-point cyclic convolutions. Thus, the number of multiplications needed to perform a 11-point transform is 50.

For $d_i = 13$, the permutation σ is given by

$$\sigma = \begin{pmatrix} 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12 \\ 2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7, 1 \end{pmatrix}$$

Applying the above permutation σ to (17b), this yields

$$\begin{pmatrix} b_2 \\ b_4 \\ b_8 \\ b_3 \\ b_6 \\ b_{12} \\ b_{11} \\ b_9 \\ b_5 \\ b_{10} \\ b_7 \\ b_1 \end{pmatrix} = \begin{pmatrix} \gamma^4, \gamma^8, \gamma^3, \gamma^6, \gamma^{12}, \gamma^{11}, \gamma^9, \gamma^5, \gamma^{10}, \gamma^7, \gamma^1, \gamma^2 \\ \gamma^8, \gamma^3, \gamma^6, \gamma^{12}, \gamma^{11}, \gamma^9, \gamma^5, \gamma^{10}, \gamma^7, \gamma^1, \gamma^2, \gamma^4 \\ \gamma^3, \gamma^6, \gamma^{12}, \gamma^{11}, \gamma^9, \gamma^5, \gamma^{10}, \gamma^7, \gamma^1, \gamma^2, \gamma^4, \gamma^8 \\ \gamma^6, \gamma^{12}, \gamma^{11}, \gamma^9, \gamma^5, \gamma^{10}, \gamma^7, \gamma^1, \gamma^2, \gamma^4, \gamma^8, \gamma^3 \\ \gamma^{12}, \gamma^{11}, \gamma^9, \gamma^5, \gamma^{10}, \gamma^7, \gamma^1, \gamma^2, \gamma^4, \gamma^8, \gamma^3, \gamma^6 \\ \gamma^{11}, \gamma^9, \gamma^5, \gamma^{10}, \gamma^7, \gamma^1, \gamma^2, \gamma^4, \gamma^8, \gamma^3, \gamma^6, \gamma^{12} \\ \gamma^9, \gamma^5, \gamma^{10}, \gamma^7, \gamma^1, \gamma^2, \gamma^4, \gamma^8, \gamma^3, \gamma^6, \gamma^{12}, \gamma^{11} \\ \gamma^5, \gamma^{10}, \gamma^7, \gamma^1, \gamma^2, \gamma^4, \gamma^8, \gamma^3, \gamma^6, \gamma^{12}, \gamma^{11}, \gamma^9 \\ \gamma^{10}, \gamma^7, \gamma^1, \gamma^2, \gamma^4, \gamma^8, \gamma^3, \gamma^6, \gamma^{12}, \gamma^{11}, \gamma^9, \gamma^5 \\ \gamma^7, \gamma^1, \gamma^2, \gamma^4, \gamma^8, \gamma^3, \gamma^6, \gamma^{12}, \gamma^{11}, \gamma^9, \gamma^5, \gamma^{10} \\ \gamma^1, \gamma^2, \gamma^4, \gamma^8, \gamma^3, \gamma^6, \gamma^{12}, \gamma^{11}, \gamma^9, \gamma^5, \gamma^{10}, \gamma^7 \\ \gamma^2, \gamma^4, \gamma^8, \gamma^3, \gamma^6, \gamma^{12}, \gamma^{11}, \gamma^9, \gamma^5, \gamma^{10}, \gamma^7, \gamma^1 \end{pmatrix} \begin{pmatrix} a_2 \\ a_4 \\ a_8 \\ a_3 \\ a_6 \\ a_{12} \\ a_{11} \\ a_9 \\ a_5 \\ a_{10} \\ a_7 \\ a_1 \end{pmatrix}$$

where γ is a 13th root of unity in $GF(q)$. Then by a similar procedure used to partition the matrix (13e) or (21a), the above matrix can be partitioned into blocks of 4×4 cyclic matrices, such that the blocks form a 3×3 cyclic matrix. That is,

$$\begin{pmatrix} E_0 \\ E_1 \\ E_2 \end{pmatrix} = \begin{pmatrix} A\ B\ C \\ B\ C\ A \\ C\ A\ B \end{pmatrix} \begin{pmatrix} Y_0 \\ Y_1 \\ Y_2 \end{pmatrix} \tag{31}$$

where

$$E_0 = \begin{pmatrix} b_2 \\ b_{10} \\ b_{11} \\ b_3 \end{pmatrix}, \quad E_1 = \begin{pmatrix} b_6 \\ b_4 \\ b_7 \\ b_9 \end{pmatrix}, \quad E_2 = \begin{pmatrix} b_5 \\ b_{12} \\ b_8 \\ b_{11} \end{pmatrix}$$

$$A = \begin{pmatrix} \gamma^4\gamma^7\gamma^9\gamma^6 \\ \gamma^7\gamma^9\gamma^6\gamma^4 \\ \gamma^9\gamma^6\gamma^4\gamma^7 \\ \gamma^6\gamma^4\gamma^7\gamma^9 \end{pmatrix} \quad B = \begin{pmatrix} \gamma^{12}\gamma^8\gamma^1\gamma^5 \\ \gamma^8\gamma^1\gamma^5\gamma^{12} \\ \gamma^1\gamma^5\gamma^{12}\gamma^8 \\ \gamma^5\gamma^{12}\gamma^8\gamma^1 \end{pmatrix}$$

$$C = \begin{pmatrix} \gamma^{10}\gamma^{11}\gamma^3\gamma^2 \\ \gamma^{11}\gamma^3\gamma^2\gamma^{10} \\ \gamma^3\gamma^2\gamma^{10}\gamma^{11} \\ \gamma^2\gamma^{10}\gamma^{11}\gamma^3 \end{pmatrix} \quad Y_0 = \begin{pmatrix} a_2 \\ a_{10} \\ a_{11} \\ a_3 \end{pmatrix}$$

$$Y_1 = \begin{pmatrix} a_6 \\ a_4 \\ a_7 \\ a_9 \end{pmatrix} \quad Y_2 = \begin{pmatrix} a_5 \\ a_{12} \\ a_8 \\ a_{11} \end{pmatrix}$$

Note that A, B, and C are 4 X 4 cyclic matrices. Using the same procedure for computing the system given by (23), the above system can be obtained as

$$\begin{aligned} E_0 &= 3^{-1}(C_1 + C_2 + C_3) - C_2 \\ E_1 &= 3^{-1}(C_1 + C_2 + C_3) - C_3 \\ E_2 &= 3^{-1}(C_1 + C_2 + C_3) \end{aligned} \tag{32}$$

where

$$C_1 = (C + A + B)(Y_0 + Y_1 + Y_2)$$

$$C_2 = M_1 - M_2 = (C - B)(Y_2 - Y_0) - (A - B)(Y_1 - Y_0)$$

$$C_3 = M_1 - M_3 = (C - B)(Y_2 - Y_0) - (C - A)(Y_2 - Y_0)$$

In (32), it is evident that the computation of C_1 or M_1 or M_2 or M_3 requires 5 multiplies. Hence the total number of multiplications needed to perform the transform defined by (31) is 16.

The total number of integer multiplications of d_i-point transform over $GF(q)$ for d_i = 2, 3, 5, 7, 9, 11, 13, P is shown in Table 2.

V. The DFT Over *GF(q)* by Multidimensional Techniques

To compute the transform of longer sequences, let $d = d_1 \cdot d_2 \ldots d_r$, where $(d_i, d_j) = 1$, for $i \neq j$, and let R_d be the ring of integers modulo d. Then, by using the Chinese Remainder theorem (Theorem 1 for integers), it can be shown that the direct sum of rings

$$R_d = R_{d_1} \dotplus R_{d_2} \dotplus \ldots \dotplus R_{d_r}$$

$$= \left\{(\alpha_1, \alpha_2, \ldots, \alpha_r) \mid \alpha_k \epsilon R_{d_k} \text{ for } k = 1, \ldots, r\right\}$$

where

$$(\alpha_1, \alpha_2, \ldots, \alpha_r) + (\beta_1, \beta_2, \ldots, \beta_r) = (\alpha_1 + \beta_1, \alpha_2 + \beta_2, \ldots, \alpha_r + \beta_r)$$

and

$$(\alpha_1, \alpha_2, \ldots, \alpha_r) \cdot (\beta_1, \beta_2, \ldots, \beta_r) = (\alpha_1 \cdot \beta_1, \alpha_2 \cdot \beta_2, \ldots, \alpha_r \cdot \beta_r)$$

is a ring of d elements which is isomorphic to the ring R_d. If $d = d_1 \cdot d_2 \ldots d_r$, by using the direct sum of finite rings, it is shown in Ref. 13 that the d-point DFT over $GF(q)$ defined in (1) can be decomposed into multidimensional DFT as follows:

$$A_{(j_1, j_2, \ldots, j_r)} = \sum_{i_1=0}^{d_1-1} \sum_{i_2=0}^{d_2-1} \cdots \sum_{i_r=0}^{d_r-1} a_{(i_1, i_2, \ldots i_r)} \gamma^{(i_1 j_1, 0 \ldots 0)}$$

$$\gamma^{(0, i_2 j_2, \ldots, 0)} \cdots \gamma^{(0, \ldots, i_r j_r)}$$

$$= \sum_{i_1=0}^{d_1-1} \sum_{i_2=0}^{d_2-1} \cdots \sum_{i_r=0}^{d_r-1} a_{(i_1, i_2, \ldots, i_r)} \gamma^{(1,0,\ldots,0)^{i_1 j_1}}$$

$$\gamma^{(0,1,0,\ldots,0)^{i_2 j_2}} \cdots \gamma^{(0,0,\ldots,1)^{i_r j_r}}$$

$$\equiv \sum_{i_1=0}^{d_1-1} \sum_{i_2=0}^{d_2-1} \cdots \sum_{i_r=0}^{d_r-1} a_{(i_1, i_2, \ldots, i_r)} \gamma_1^{i_1 j_1} \gamma_2^{i_2 j_2} \cdots \gamma_r^{i_r j_r} \tag{33}$$

where $\gamma_k = \gamma^{(0, \ldots 0, 1, 0, \ldots 0)}$ with the 1 in the k-th position as a d_k-th root of unity in R_{d_k}. Assume the number of multiplications used to perform d_i-point DFT for $i = 1, 2, \ldots r$ is m_i. Then, by (33), it is evident that the number of multiplications for computing d-point DFT over $GF(q)$ is equal to

$$N = d_1 \cdot d_2 \ldots d_{r-1} m_r + d_1 \cdot d_2 \ldots d_{r-2} d_r m_{r-1} + \ldots + d_2 d_3 \ldots d_r m_1$$

A simple example for computing the DFT over $GF(q)$ by using multidimensional techniques is now presented.

Example: Let $q = 2^5 - 1$ and $d = 2^5 - 2 = 2 \cdot 3 \cdot 5 = d_1 d_2 d_3$. Compute the 30-point DFT over $GF(q)$.

Since $\alpha = 3$ is a primitive element in $GF(31)$, then 3^j is also a primitive element in $GF(31)$ for $j = 7, 11, 13, 17, 19, 21, 23, 27, 29$. The choice of $r = 3^{19}$ yields

$$(\gamma)^6 = (3^{19})^6 \equiv 3^{24} \equiv 2 \bmod 31$$

Thus, one can find the primitive element $\gamma = 3^{19}$ such that $\gamma_1 = \gamma^{(1,0,0)} = \gamma^{15} = -1, \gamma_2 = \gamma^{(0,1,0)} = \gamma^{10} = -6$, $\gamma_3 = \gamma^{(0,0,1)} = \gamma^6 = 2$ are the elements of order 2, 3, 5, respectively. By (33), this FFT algorithm consists of the following 3 stages:

Stage 1:

$$A^1_{(i_1,i_2,j_3)} = \sum_{i_3=0}^{4} a_{(i_1,i_2,i_3)} \gamma^{(0,0,1)^{i_3 j_3}}$$

$$= \sum_{i_3=0}^{4} a_{(i_1,i_2,i_3)} 2^{i_3 j_3} \text{ for } j_3 = 0,1,2,3,4 \tag{34}$$

Stage 2:

$$A^2_{(i_1,j_2,j_3)} = \sum_{i_2=0}^{2} A^1_{(i_1,i_2,j_3)} \gamma^{(0,1,0)^{i_2 j_2}}$$

$$= \sum_{i_2=0}^{2} A^1_{(i_1,i_2,j_3)} (-6)^{i_2 j_2} \text{ for } j_2 = 0,1,2$$

Stage 3:

$$A^3_{(j_1,j_2,j_3)} = \sum_{i_1=0}^{1} A^2_{(i_1,j_2,j_3)} \gamma^{(1,0,0)^{i_1 j_1}}$$

$$= \sum_{i_1=0}^{1} A^2_{(i_1,j_2,j_3)} (-1)^{i_1 j_1} \text{ for } j_1 = 0,1$$

In (34), we observe that both $A^1_{(i_1,i_2,j_3)}$ and $A^3_{(j_1,j_2,j_3)}$ can be evaluated without multiplications and that $A^2_{(i_1,j_2,j_3)}$ is a 3-point DFT over $GF(q)$. By Table 1, the number of multiplications used to perform $A^2_{(i_1,j_2,j_3)}$ for $j_2 = 0, 1, 2$ is 1. This requires a total of $N = 26 \cdot 0 + 10 \cdot 1 + 15 \cdot 0 = 10$ integer multiplications modulo 31 for evaluating (30).

For most applications to digital filters, the two most important Mersenne primes are $2^{31} - 1$ and $2^{61} - 1$. The number of real integer multiplications used to perform a DFT over $GF(q)$ of $d = 2 \cdot p \cdot r_3$, where $r_3 = 5, 7, 9, 11$, or 13 for $q = 2^{31} - 1$ and $q = 2^{61} - 1$ is given in Table 3. The present algorithm, and Winograd's new algorithm (Ref. 13) are compared in Table 3 by giving the number of real multiplications needed to perform these algorithms. These results for Winograd's algorithm come from Table 2, in Reference 13.

In Table 3, one can see that the transform over $GF(q)$ appears comparable in speed with that given by Winograd (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 at the Jet Propulsion Laboratory for their early support, suggestions, and encouragement of the research which led to this paper. We also thank Dr. C. A. Greenhall for his mathematical suggestions.

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 Convolutions," *IEEE Trans. Inform. Theory,* 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. Inform. Theory,* 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., and 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. Golomb, S. W.: "Properties of the Sequences $3 \cdot 2^n + 1$," *Math. Comput.* 1976, 30, pp. 657-663.

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

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

12. Reed, I. S., Truong, T. K., and Liu, K. Y., "A New Fast Algorithm for Computing Complex Number-Theoretic Transforms", *Electron Lett.*, 1977, pp. 278-82.

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

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

15. J. Justesen, "On the Complexity of Decoding of Reed-Solomon Codes," IEEE Trans. Inform Theory, Vol. IT-22, March 1976, pp. 237-238.

16. I. S. Reed, R. A. Scholtz, T. K. Truong, L. R. Welch, "The Fast Decoding of Reed-Solomon Codes Using Fermat Theoretic Transforms and Continued Fractions," to be published in IEEE Trans. Inform theory.

17. E. R. Berlekamp, Algebraic Coding Theory, New York, McGraw Hill, 1968, Chapter 7.

18. I. M. Vinogradov, Elements of Number Theory, Dover Publications, New York, 1954.

Table 1. Factorization of the integers $2^p - 2$

p	$2^p - 2$
13	$3^2 \cdot 2 \cdot 5 \cdot 7 \cdot 13$
17	$2 \cdot 3 \cdot 5 \cdot 17 \cdot 257$
31	$2 \cdot 3^2 \cdot 7 \cdot 11 \cdot 31 \cdot 331 \cdot 151$
61	$2 \cdot 3^2 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 \cdot 31 \cdot 41 \cdot 61 \cdot 151 \cdot 331 \cdot 1321$

Table 2. The complexity of transforms over *GF(q)* of small sequences where $q = 2^p - 1$

d_i	No. of Integer Multiplications
2	0
3	1
5	4
7	8
9	12
11	50
13	21
p	0

Table 3. The complexity of the transform over *GF(q)* where $q = 2^{31} - 1$ and $q = 2^{61} - 1$

d	No. real integer multiplications of transform over $GF(2^{31} - 1)$	No. real integer multiplications of transform over $GF(2^{61} - 1)$	No. real integer multiplications of Winograd's new algorithm for real data
60			72
62	0		
120			144
122		0	
168			216
186	62		
240			324
310	248		
366		122	
420			648
434	496		
504			936
558	744		
610		488	
806	1302		
840			1296
854		976	
1008			2106
1098		1464	
1586		1952	
1674	2790		
2520			5616
3348		5490	

Appendix A

Let $a \in GF(q)$, where $(a,q) = 1$ and also let $S = a/q$. In this Appendix, it will be shown that the inverse element of a can be obtained by using continued fractions.

If $S = a/q$, where $a \in GF(q)$, using Euclid's algorithm, i.e.,

$$r_{k-2} = a_k r_{k-1} + r_k,\ 0 < r_k < r_{k-1} \text{ for } k = 1,2,\ldots,n-1 \tag{A-1}$$

with initial conditions $r_{-1} = q$, $r_{-2} = a$ and $r_{n-2} = r_{n-1}a_n$, one generates the sequence of the partial quotients, $a_0, a_1, \ldots, a_n$. By (A-1), S can be developed into a continued fraction.

$$S = a_0 + (a_1 + (\ldots(a_k + \alpha_k)^{-1} \ldots)^{-1} \ldots)^{-1},\ k \leqslant n \tag{A-2}$$

By setting $\alpha_k = 0$ in (A-2), one can determine a k^{th} order approximation to S, which is called a *convergent,*

$$S_k = a_0 + (a_1 + (\ldots(\ldots(a_k)^{-1} \ldots)^{-1} \ldots)^{-1})^{-1}$$

From (A-1), $S_0 \cdot S_1, \ldots, S_k, \ldots$ will terminate with S_n since $r_n = 0$. Thus, $S_n = a/q$, where n is a finite number.

A recursive formula for convergents is generated as follows:

$$S_0 = \frac{a_0}{1} = \frac{p_0}{q_0}$$

$$S_1 = a_0 + \frac{1}{a_1} = \frac{a_1a_0 + 1}{a_1 \cdot 1 + 0} = \frac{a_1p_0 + p_{-1}}{a_1q_0 + q_{-1}} = \frac{p_1}{q_1}$$

$$S_2 = a_0 + \frac{1}{a_1 + \frac{1}{a_2}} = \frac{(a_1 + 1/a_2)p_0 + p_{-1}}{(a_1 + 1/a_2)q_0 + q_{-1}} = \frac{a_2p_1 + p_0}{a_2q_1 + q_0} = \frac{p_2}{q_2}$$

The recursive convergents are defined as

$$S_k = \frac{a_kp_{k-1} + p_{k-2}}{a_kq_{k-1} + q_{k-2}} = \frac{p_k}{q_k} \tag{A-3}$$

where $p_{-1} = 1$, $q_{-1} = 0$, $p_0 = a_0$, and $q_0 = 1$ for $k = 1,2,\ldots,n$.

Let

$$I_k = p_kq_{k-1} - q_k\,p_{k-1}$$

By (A-3),

$$I_k = p_k q_{k-1} - q_k p_{k-1} = -I_{k-1} \tag{A-4}$$

Since $I_0 = p_0 q_{-1} - q_0 p_{-1} = a_0 \cdot 0 - 1 \cdot 1 = -1$, one has by (A-4), $I_1 = -I_0 = 1$. With the above result, one has $I_k = (-1)^{k+1}$. It follows that

$$p_k q_{k-1} - q_k p_{k-1} = (-1)^{k+1} \text{ for } k \geqslant 0 \tag{A-5}$$

If $n = k$, then $S_n = p_n/q_n = a/q$. Thus, (A-5) becomes

$$aq_{n-1} - qp_{n-1} = (-1)^{n+1} \tag{A-6}$$

It follows from (A-6) that the solutions of $a\,x \equiv 1 \bmod q$ are given by

$$x \equiv q_{n-1} \bmod q \text{ if } n \text{ is odd,}$$

$$x \equiv -q_{n-1} \bmod q \text{ if } n \text{ is even} \tag{A-7}$$

In order to determine an upper bound on the number of partial quotients to form a continued fraction for a/q, $1 < a < q$, the following lemma and theorem are needed:

Lemma 1: Sequence $\{q_k\}$ defined in (A-3) as a function of $a_1, a_2, \ldots, a_k$ increases most slowly for $a_1 = a_2 = \ldots = a_k = 1$ for all k.

Proof: By (A-3), $q_k = a_k q_{k-1} + q_{k-2}$, where $q_k \geqslant 1$ for all k and $q_1 = a_1$. q_1 is a minimum for $q_1 = a_1 = 1$. For purposes of induction, assume the theorem is true for all $a \leqslant k \leqslant n$, i.e., $\underset{a_1, \ldots, a_k}{\text{Min}} q_k$ is achieved for $a_1 = a_2 = \ldots = a_k = 1$ for $k \leqslant n$. Now

$$q_{n+1} = a_{n+1} q_n + q_{n-1}$$

so that

$$\underset{a_1, \ldots, a_k}{\text{Min}} q_{n+1} = \left(\underset{a_{n+1}}{\text{Min}}\, a_{n+1}\right) \left(\underset{a_1, \ldots, a_n}{\text{Min}}\, q_n\right) + \left(\underset{a_1, \ldots, a_{n-1}}{\text{Min}}\, q_{n-1}\right)$$

$$= 1(q_n \mid a_1 = a_2 \ldots a_n = 1) + (q_{n-1} \mid a_1 = a_2 \ldots a_{n-1} = 1)$$

$$= q_{n+1} \mid a_1 = a_2 \ldots a_{n+1} = 1$$

and the induction is complete.

Definition: The number b_n is called a *Fibonacci number* if $b_n = b_{n-1} + b_{n-2}$ with $b_0 = 1, b_1 = 1$.

Theorem 2: Let b_n be a Fibonacci number. If $b_{n-1} \leqslant p \leqslant b_n$ then, the upper bound on the number of partial quotients needed to form a continued fractions for a/q, $1 < a < q$, is n.

Proof: If $1 = a_1 = a_2 = a_3 \ldots$, then $q_0 = 1$, $q_1 = 1$, $q_2 = 1 + 1 = 2$, $q_3 = q_2 + q_1 = 2 + 1 = 3$, $q_4 = 3 + 2 = 5$, etc. These are the *Fibonacci numbers*, b_n for $(n = 0, 1, 2, \ldots)$. Thus, if $q_n = q$ is a Fibonacci number, then $a_1 = a_2 = \ldots a_n = 1$. Thus, by lemma, the largest value of n is achieved.

If $q_k = q$ for $b_{n-1} < q \leqslant b_n$, then, by the lemma, $b_k < q_k = q \leqslant b_n$. Hence $k < n$, and n is the upper bound of partial quotients to form continued fractions for a/q, $1 < a < q$.

A simple example is now presented for finding the inverse element in $GF(q)$.

Example: Let $GF(q)$ be the field of integers modulo the Mersenne prime $q = 2^7 - 1$. Find an inverse element of 19 in $GF(127)$.

Let $a = 19$ and let $S = 19/127$. From the tabular form (Table A-1) when $k = n = 4$, one observes $r_4 = 0$. Thus, $S = S_4 = 19/127$. Hence, $q_3 = 20$. By (A-7), $a^{-1} \equiv -20 \equiv 107 \bmod 127$ is the inverse element of 19. Since $b_4 = 5 < q_4 = 127 < b_{11} = 144$, by Theorem 2, the upper bound on the numbers of partial quotients is 11.

Table A-1. A computation of convergents to a continued fraction

k	$r_{k-2} = q\, r_{k-1} + r_k$	a_k	r_k	$p_k = a_k p_{k-1} + p_{k=2}$	$q_k = a_k q_{k-1} + q_{k-2}$	$S_k = p_k/q_k$
−2						
−1						
0	$19 = 0 \cdot 127 + 19$	0	19	$p_0 = 0 \cdot 1 + 0 = 0 = a_0$	$q_0 = 0 \cdot 0 + 1 = 1$	$S_0 = 0$
1	$127 = 6 \cdot 19 + 13$	6	13	$p_1 = 6 \cdot 0 + 1 = 1$	$q_1 = 6 \cdot 1 + 0 = a_1$	$S_1 = 1/6$
2	$19 = 1 \cdot 13 + 6$	1	6	$p_2 = 1 \circ 1 + 0 = 1$	$q_2 = 1 \cdot 6 + 1 = 7$	$S_2 = 1/7$
3	$13 = 2 \circ 6 + 1$	2	1	$p_3 = 2 \cdot 1 + 1 = 3$	$q_3 = 2 \cdot 7 + 6 = 20$	$S_3 = 3/20$
4	$6 = 6 \cdot 1$	6	0	$p_4 = 6 \cdot 3 + 1 = 19$	$q_4 = 6 \cdot 20 + 7 = 127$	$S_4 = 19/127$

Appendix B

Let a and b be relatively prime and let A be a cyclic $ab \times ab$ matrix. In this Appendix, it will be shown in the following theorem that there exists a permutation π of the rows and columns so that A can be partitioned into blocks of $b \times b$ cyclic matrices, such that the blocks form a $a \times a$ cyclic matrix.

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

$$A_{(x,y)} = f_{(x+y \bmod ab)}, \quad 0 \leqslant x,y < ab$$

If π is a permutation of $\{0,1,\ldots, ab - 1\}$, 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, then each submatrix is cyclic and the submatrices form a $a \times a$ cyclic matrix.

Proof: Let $Z_n = \{0,1,\ldots,n - 1\}$ be the additive group of integers modulo n. By the Chinese Remainder Theorem, the mapping α: $Z_{ab} \rightarrow Z_a \times Z_b$ given by

$$\alpha(x) = (x \bmod a,\ x \bmod b),\ x \epsilon Z_{ab}$$

is an isomorphism. Define also the mapping β: $Z_{ab} \rightarrow Z_a \times Z_b$ given by

$$\beta(x) = \left(u = \frac{x - v}{b},\ v \equiv x \bmod b\right)$$

for $x \epsilon Z_{ab}$. Then β is a one-to-one and onto mapping, and $\beta^{-1}(u,v) = bu + v,\ u \epsilon Z_a,\ v \epsilon Z_b$.

Let $\pi = \alpha^{-1}\beta$. Then π is a permutation of Z_{ab}. Let $\beta_{ij}, i,j \epsilon Z_a$, be the $(i,j)^{\text{th}}$ $b \times b$ submatrix of B. Then for $v,w \epsilon Z_b$,

$$\begin{aligned} B_{ij}(v,w) &= B_{(bi+v,\ bj+w)} \\ &= B_{(\beta^{-1}(i,v),\ \beta^{-1}(j,w))} \\ &= A_{(\pi\beta^{-1}(i,v),\pi\beta^{-1}(j,w))} \\ &= A_{(\alpha^{-1}(i,v),\alpha^{-1}(j,w))} \\ &= f_{((\alpha^{-1}(i,v)+\alpha^{-1}(j,w)) \bmod a \cdot b)} \end{aligned}$$

Since α^{-1} is an isomorphism

$$\beta_{ij}(v,w) = f_{(\alpha^{-1}((i+j) \bmod a,\ (v+w) \bmod b))}$$

If we fix i and j in the above eq., it is evident that the $(i,j)^{\text{th}}$ $b \times b$ submatrix of B is cyclic matrix. Similarly, by fixing v and w, the submatrices B_{ij} form a $a \times a$ cyclic matrix.

Example: Let $a = 2$, $b = 3$. Then $\alpha(x) = (x \bmod 2, x \bmod 3)$ and $\alpha^{-1}(u,v) = 3u + 4v \bmod 6$. Also $\beta(x) = (u = (x - v)/3, v \equiv x \bmod 3)$ and $\beta^{-1}(u,v) = 3u + v$. Finally $\pi = \left(\begin{smallmatrix} 0 & 1 & 2 & 3 & 4 & 5 \\ 0 & 4 & 2 & 3 & 1 & 5 \end{smallmatrix}\right)$ or the 2-cycle (14).