On Decoding of Reed-Solomon Codes Over *GF*(32) and *GF*(64) Using the Transform Techniques of Winograd[1]

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

T. K. Truong and B. Benjauthrit
TDA Engineering

A new algorithm for computing a transform over GF(2^n), where n = 5, 6, is developed to encode and decode Reed-Solomon (RS) codes of length $2^n - 1$. Such an RS decoder is considerably faster than the conventional transform decoder over GF(2^n).

I. Introduction

Fast real-valued transforms over the group $(Z_2)^n$ were developed first by Green (Ref. 1) to decode the (32,6) Reed-Muller code (Ref. 2) used by JPL in the Mariner and Viking space probes. Recently Gore (Ref. 3) extended Mandelbaum's methods (Ref. 4) for decoding Reed-Solomon codes. He proposed to decode RS codes with a finite field transform over $GF(2^n)$, where n is an integer. Michelson (Ref. 5) implemented Mandelbaum's algorithm and showed that the decoder, using the transform over $GF(2^n)$, requires substantially fewer multiplications than a standard decoder (Refs. 6-8). The disadvantage of his transform method over $GF(2^n)$ is that the transform length is an odd number, so that the most efficient FFT algorithm cannot be used.

In this paper, a new algorithm based on the methods of Winograd (Refs. 9, 10) is developed to compute a transform over $GF(2^n)$ for $n = 5, 6$. This transform algorithm over $GF(2^n)$ for $n = 5, 6$ requires fewer multiplications than the conventional fast transform algorithm described by Gentleman (Ref. 11). The algorithm is presented in detail in this paper only for the cases $n = 5, 6$. This algorithm for RS codes over $GF(2^n)$, where $n = 2^m$, has been treated previously by the authors using similar procedures (Ref. 12).

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

II. Cyclic Convolutions

The following algorithm for the cyclic convolution of two sequences is based on ideas due to Winograd (Refs. 9, 10). Let $GF(2^n)$ be the Galois field of 2^n elements. Observe first that if $X(u) = x_0 + x_1 u^m$, $Y(u) = y_0 + y_1 u^m$ for $m = 1, 2$, be two polynomials over $GF(2^n)$, then the product $T'(u) = X(u)Y(u)$ is computed as follows:

$$T'(u) = X(u)\,Y(u) = c_0 + c_1 u^m + c_2 u^{2m} \tag{1}$$

where $c_0 = x_0 \cdot y_0$, $c_1 = (x_0 + x_1) \cdot (y_0 + y_1) + x_0 \cdot y_0 + x_1 \cdot y_1$, and $c_2 = x_1 \cdot y_1$. Evidently there are exactly three multiplications required to compute (1).

It is well known (Ref. 9) that if

$$X(u) = \sum_{k=0}^{n-1} x_k u^k$$

and

$$Y(u) = \sum_{k=0}^{n-1} y_k u^k$$

are $(n - 1)$-th degree polynomials, then the cyclic convolution of the coefficients of $X(u)$ and $Y(u)$ is given by the coefficients of

$$T(u) = X(u)\,Y(u) \equiv \sum_{k=0}^{n-1} Z_k u^k \bmod (u^n - 1).$$

Now factor the polynomial $u^n - 1$ over $GF(2^n)$ into irreducible relatively prime factors, i.e.,

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

where $(g_i(u), g_j(u)) = 1$ for $i \neq j$.

Then $T(u)$ mod $g_i(u)$ for $i = 1, 2, \ldots, k$ can be computed, using Eq. (1). To evaluate $T(u)$ from these residues the Chinese remainder theorem is used. To show this, consider first the cyclic convolution of 3 elements. This is given in matrix form as follows:

$$\begin{pmatrix} y_0 \\ y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} a_0 & a_1 & a_2 \\ a_1 & a_2 & a_0 \\ a_2 & a_0 & a_1 \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix} \tag{2}$$

where y_i, a_i, $x_i \in GF(2^n)$ for $i = 0, 1, 2$. The above convolution is obtained from the coefficients of

$$T(u) = (a_2 + a_0 u + a_1 u^2) \cdot (x_2 + x_1 u + x_0 u^2) \bmod (u + 1)(u^2 + u + 1) \tag{3}$$

where $(u + 1)$ and $(u^2 + u + 1)$ are the irreducible factors of $u^3 - 1$ over $GF(2)$.

To compute (3), let $m(u) = (u + 1)(u^2 + u + 1) = m_1(u)\, m_2(u) = m_1(u)\, M_1(u) = m_2(u)\, M_2(u)$. The system of congruences $T(u) = T_i(u) \bmod m_i(u)$ for $i = 1, 2$ is given by

$$T_1(u) \equiv (a_2 + a_0 u + a_1 u^2) \cdot (x_2 + x_1 u + x_0 u^2) \bmod (u - 1) = (a_2 + a_0 + a_1) \cdot (x_2 + x_1 + x_0)$$

and

$$\begin{aligned} T_2(u) &\equiv (a_2 + a_0 u + a_1 u^2) \cdot (x_2 + x_1 u + x_0 u^2) \bmod (u^2 + u + 1) \\ &\equiv [(a_2 + a_1) + (a_0 + a_1) u] \cdot [(x_2 + x_0) + (x_1 + x_0) u] \bmod (u^2 + u + 1) \end{aligned}$$

By (1), $T_2(u)$ is given by

$$\begin{aligned} T_2(u) &\equiv (a_2 + a_1) \cdot (x_2 + x_0) + [(a_2 + a_1 + a_0 + a_1) \cdot (x_2 + x_0 + x_1 + x_0) + (a_2 + a_1) \cdot (x_2 + x_0) \\ &\quad + (a_0 + a_1) \cdot (x_1 + x_0)] u + (a_0 + a_1) \cdot (x_1 + x_0) u^2 \\ &\equiv (a_2 + a_1) \cdot (x_2 + x_0) + (a_0 + a_1) \cdot (x_1 + x_0) + [(a_2 + a_0) \cdot (x_2 + x_1) \\ &\quad + (a_2 + a_1)(x_2 + x_0)] u \bmod (u^2 + u + 1) \end{aligned}$$

Evidently 3 multiplies are actually needed to compute $T_2(u)$. By Chinese remainder theorem for polynomials (Ref. 13), $T(u)$ can be reconstituted from $T_1(u)$ and $T_2(u)$ by

$$T(u) \equiv T_1(u)\, M_1(u)\, M_1^{-1}(u) + T_2(u)\, M_2(u)\, M_2^{-1}(u) \bmod u^3 - 1 \tag{4}$$

where $M_i^{-1}(u)$ uniquely satisfies the congruence

$$M_i(u)\, M_i^{-1}(u) \equiv 1 \bmod m_i(u) \text{ for } i = 1, 2.$$

These equations are satisfied by $M_1^{-1}(u) = 1$ and $M_2^{-1}(u) = u$. Hence

$$\begin{aligned} T(u) &\equiv (a_2 + a_0 + a_1) \cdot (x_2 + x_1 + x_0) + (a_2 + a_0) \cdot (x_2 + x_1) + (a_2 + a_1) \cdot (x_2 + x_0) + [(a_2 + a_0 + a_1) \cdot (x_2 + x_1 + x_0) \\ &\quad + (a_2 + a_1) \cdot (x_2 + x_0) + (a_0 + a_1) \cdot (x_1 + x_0)] u + [(a_2 + a_0 + a_1) \cdot (x_2 + x_1 + x_0) + (a_0 + a_1) \cdot (x_1 + x_0) \end{aligned}$$

$$+ (a_2 + a_0) \cdot (x_2 + x_1)]\ u^2$$

$$\equiv y_0 + y_1 u + y_2 u^2 \bmod (u^3 - 1)$$

where

$$y_0 = (a_2 + a_0 + a_1) \cdot (x_2 + x_1 + x_0) + (a_2 + a_0) \cdot (x_2 + x_1) + (a_2 + a_1) \cdot (x_2 + x_0)$$

$$y_1 = (a_2 + a_0 + a_1)(x_2 + x_1 + x_0) + (a_2 + a_1) \cdot (x_2 + x_0) + (a_0 + a_1) \cdot (x_1 + x_0) \tag{5}$$

$$y_2 = (a_2 + a_0 + a_1) \cdot (x_2 + x_1 + x_0) + (a_0 + a_1) \cdot (x_1 + x_0) + (a_2 + a_0) \cdot (x_2 + x_1)$$

If one lets

$$\begin{aligned} m_0 &= (a_2 + a_0 + a_1) \cdot (x_2 + x_1 + x_0) \\ m_1 &= (a_2 + a_0) \cdot (x_2 + x_1) \\ m_2 &= (a_2 + a_1) \cdot (x_2 + x_0) \\ m_3 &= (a_0 + a_1) \cdot (x_1 + x_0) \end{aligned} \tag{6}$$

Then (5) becomes

$$\begin{aligned} y_0 &= m_0 + m_1 + m_2 \\ y_1 &= m_0 + m_2 + m_3 \\ y_2 &= m_0 + m_3 + m_1 \end{aligned}$$

From (6) the total number of multiplications needed to perform (2) is exactly 4. Now consider cyclic convolutions of 5 elements of $GF(2^n)$. Again such a convolution can be represented in matrix form as

$$\begin{pmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \end{pmatrix} = \begin{pmatrix} a_0 & a_1 & a_2 & a_3 & a_4 \\ a_1 & a_2 & a_3 & a_4 & a_0 \\ a_2 & a_3 & a_4 & a_0 & a_1 \\ a_3 & a_4 & a_0 & a_1 & a_2 \\ a_4 & a_0 & a_1 & a_2 & a_3 \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} \tag{7}$$

where y_i, a_i, $x_i \in GF(2^n)$ for $i = 0, 1, 2, 3, 4$. The matrix in (7) is a 5 × 5 cyclic matrix. This matrix equation can be obtained also as the set of coefficients of

$$(a_4 + a_0u + a_1u^2 + a_2u^3 + a_3u^4)(x_4 + x_3u + x_2u^2 + x_1u^3 + x_0u^4) \bmod (u^5 - 1),$$

where $u^5 - 1$ factors into two irreducible factors over $GF(2)$ as follows,

$$u^5 - 1 = (u + 1)(u^4 + u^3 + u^2 + u + 1),$$

Let $m(u) = (u + 1)(u^4 + u^3 + u^2 + u + 1) = m_1(u)\, m_2(u) = m_1(u)\, M_1(u) = m_2(u)\, M_2(u)$. The system of congruences $T(u) \equiv T_i(u) \bmod m_i(u)$ for $i = 1, 2$ for this case is given by

$$T_1(u) \equiv (a_4 + a_0u + a_1u^2 + a_2u^3 + a_3u^4) \cdot (x_4 + x_3u + x_2u^2 + x_1u^3 + x_0u^4)$$

$$\equiv (a_4 + a_0 + a_1 + a_2 + a_3) \cdot (x_4 + x_3 + x_2 + x_1 + x_0) \bmod (u - 1) \tag{8a}$$

and

$$T_2(u) \equiv (a_4 + a_0u + a_1u^2 + a_2u^3 + a_3u^4) \cdot (x_4 + x_3u + x_2u^2 + x_1u^3 + x_0u^4)$$

$$\equiv [(a_4 + a_3) + (a_0 + a_3)\, u + (a_1 + a_3)\, u^2 + (a_2 + a_3)\, u^3]$$

$$\cdot [(x_4 + x_0) + (x_3 + x_0)\, u + (x_2 + x_0)\, u^2 + (x_1 + x_0)\, u^3] \bmod (u^4 + u^3 + u^2 + u + 1) \tag{8b}$$

In order to compute (8b), let $c_0 = (a_4 + a_3)$, $c_1 = (a_0 + a_3)$, $c_2 = (a_1 + a_3)$, $c_3 = (a_2 + a_3)$, $d_0 = (x_4 + x_0)$, $d_1 = (x_3 + x_0)$, $d_2 = (x_2 + x_0)$, $d_3 = (x_0 + x_1)$. Thus,

$$T_2(u) = [c_0 + c_1u + c_2u^2 + c_3u^3] \cdot [d_0 + d_1u + d_2u^2 + d_3u^3] \bmod (u^4 + u^3 + u^2 + u + 1) \tag{8c}$$

Now in (8c) let

$$C(u) = [c_0 + c_1u + c_2u^2 + c_3u^3] \cdot [d_0 + d_1u + d_2u^2 + d_3u^3]$$

$$= [(c_0 + c_1u) + u^2(c_2 + c_3u)] \cdot [(d_0 + d_1u) + u^2(d_2 + d_3u)]$$

Next set $A_0 = (c_0 + c_1 u)$, $A_1 = (c_2 + c_3 u)$, $B_0 = (d_0 + d_1 u)$, $B_1 = (d_2 + d_3 u)$. Then

$$C(u) = (A_0 + u^2 A_1) \cdot (B_0 + u^2 B_1)$$

By (1) $C(u)$ is given by

$$C(u) = C_0 + C_1 u^2 + C_2 u^4$$

where

$$C_0 = A_0 \cdot B_0 = (c_0 + c_1 u) \cdot (d_0 + d_1 u)$$

$$C_2 = A_1 \cdot B_1 = (c_2 + c_3 u) \cdot (d_2 + d_3 u)$$

$$C_1 = D_1 - C_0 - C_2$$

where D_1 is defined to be

$$D_1 = (A_0 + A_1) \cdot (B_0 + B_1)$$

$$= [(c_0 + c_2) + (c_1 + c_3) u] \cdot [(d_0 + d_2) + (d_1 + d_3) u]$$

To compute C_0, C_2, D_1, use (1) again to obtain,

$$C_0 = (c_0 + c_1 u) \cdot (d_0 + d_1 u)$$

$$= c_0 \cdot d_0 + ((c_0 + c_1) \cdot (d_0 + d_1) - c_0 d_0 - c_1 d_1) u + c_1 \cdot d_1 u^2,$$

$$C_2 = (c_2 + c_3 u) \cdot (d_2 + d_3 u)$$

$$= c_2 \cdot d_2 + ((c_2 + c_3) \cdot (d_2 + d_3) - c_2 \cdot d_2 - c_3 \cdot d_3) u + c_3 \cdot d_3 u^2,$$

and

$$D_1 = [(c_0 + c_2) + (c_1 + c_3) u] \cdot [(d_0 + d_2) + (d_1 + d_3) u]$$

$$= (c_0 + c_2) \cdot (d_0 + d_2) + ((c_0 + c_2 + c_1 + c_3) \cdot (d_0 + d_2 + d_1 + d_3)$$

$$- (c_0 + c_2)(d_0 + d_2) - (c_1 + c_3)(d_1 + d_3)) u + (c_1 + c_3) \cdot (d_1 + d_3) u^2$$

Thus, finally

$$C(u) = c_0 \cdot d_0 + ((c_0 + c_1) \cdot (d_0 + d_1) - c_0 \cdot d_0 - c_1 \cdot d_1)\, u$$

$$+ ((c_0 + c_2) \cdot (d_0 + d_2) - c_0 \cdot d_0 - c_2 \cdot d_2 + c_1 \cdot d_1)\, u^2$$

$$+ ((c_0 + c_2 + c_1 + c_3) \cdot (d_0 + d_2 + d_1 + d_3) - (c_0 + c_2) \cdot (d_0 + d_2)$$

$$- (c_1 + c_3) \cdot (d_1 + d_3) - (c_0 + c_1) \cdot (d_0 + d_1) + c_0 \cdot d_0 + c_1 \cdot d_1$$

$$- (c_2 + c_3) \cdot (d_2 + d_3) + c_2 \cdot d_2 + c_3 \cdot d_3)\, u^3$$

$$+ ((c_1 + c_3)(d_1 + d_3) - c_1 \cdot d_1 - c_3 \cdot d_3 + c_2 \cdot d_2)\, u^4$$

$$+ ((c_2 + c_3) \cdot (d_2 + d_3) - c_2 \cdot d_2 - c_3 \cdot d_3)\, u^5 + c_3 \cdot d_3\, u^6$$

Hence $T_2(u) \equiv C(u) \bmod u^4 + u^3 + u^2 + u + 1$ is given by

$$T_2(u) = b_0 + b_1 u + b_2 u^2 + b_3 u^3 \tag{9}$$

where

$$b_0 = c_0 \cdot d_0 + (c_1 + c_3) \cdot (c_1 + d_3) + c_1 \cdot d_1 + (c_2 + c_3) \cdot (d_2 + d_3)$$

$$b_1 = (c_0 + c_1) \cdot (d_0 + d_1) + c_0 \cdot d_0 + (c_1 + c_3) \cdot (d_1 + d_3) + c_2 \cdot d_2$$

$$b_2 = (c_0 + c_2) \cdot (d_0 + d_2) + c_0 d_0 + (c_1 + c_3) \cdot (d_1 + d_3) + c_3 \cdot d_3$$

$$b_3 = (c_0 + c_2 + c_1 + c_3) \cdot (d_0 + d_2 + d_1 + d_3) + (c_0 + c_2) \cdot (d_0 + d_2)$$

$$+ (c_0 + c_1) \cdot (d_0 + d_1) + c_0 \cdot d_0 + (c_2 + c_3) \cdot (d_2 + d_3)$$

By the Chinese remainder theorem for polynomials (Ref. 13), $T(u)$ can be reconstituted from

$$T(u) \equiv T_1(u)\, M_1(u)\, M_1^{-1}(u) + T_2(u)\, M_2(u)\, M_2^{-1}(u) \bmod u^5 - 1 \tag{10}$$

where $M_1(u) = u^4 + u^3 + u^2 + u + 1$, $M_1^{-1}(u) = 1$, $M_2(u) = u + 1$, $M_2^{-1}(u) = u^3 + u$, and where $T_1(u)$ and $T_2(u)$ are given in (8a) and (9), respectively. By (10), $T(u)$ is

$$T(u) = y_0 + y_1 u + y_2 u^2 + y_3 u^3 + y_4 u^4 \tag{11}$$

where

$$\begin{aligned}
y_4 &= (a_0 + a_1 + a_2 + a_3 + a_4) \cdot (x_0 + x_1 + x_2 + x_3 + x_4) \\
&\quad + (a_0 + a_3) \cdot (x_3 + x_0) + (a_1 + a_3) \cdot (x_2 + x_0) + (a_0 + a_2) \cdot (x_3 + x_1) \\
&\quad + (a_2 + a_3) \cdot (x_1 + x_0) + (a_4 + a_0 + a_2 + a_1) \cdot (x_4 + x_3 + x_2 + x_1) \\
y_3 &= (a_0 + a_1 + a_2 + a_3 + a_4) \cdot (x_0 + x_1 + x_2 + x_3 + x_4) \\
&\quad + (a_0 + a_3) \cdot (x_3 + x_0) + (a_1 + a_2) \cdot (x_2 + x_1) \\
&\quad + (a_4 + a_0) \cdot (x_4 + x_3) + (a_1 + a_3) \cdot (x_2 + x_0) \\
&\quad + (a_4 + a_1) \cdot (x_4 + x_2) + (a_4 + a_3) \cdot (x_4 + x_0) \\
&\quad + (a_0 + a_2) \cdot (x_3 + x_1) + (a_2 + a_3) \cdot (x_1 + x_0) \\
y_2 &= (a_0 + a_1 + a_2 + a_3 + a_4) \cdot (x_0 + x_1 + x_2 + x_3 + x_4) \\
&\quad + (a_0 + a_3) \cdot (x_3 + x_0) + (a_4 + a_3) \cdot (x_4 + x_0) + (a_1 + a_3) \cdot (x_2 + x_0) \\
&\quad + (a_4 + a_0 + a_1 + a_2) \cdot (x_4 + x_3 + x_2 + x_1) + (a_4 + a_1) \cdot (x_4 + x_2). \\
y_1 &= (a_0 + a_1 + a_2 + a_3 + a_4) \cdot (x_0 + x_1 + x_2 + x_3 + x_4) \\
&\quad + (a_0 + a_3) \cdot (x_3 + x_0) + (a_4 + a_3) \cdot (x_4 + x_0) + (a_2 + a_3) \cdot (x_1 + x_0) \\
&\quad + (a_4 + a_0 + a_1 + a_2) \cdot (x_4 + x_3 + x_2 + x_1) + (a_4 + a_0) \cdot (x_4 + x_3), \\
y_0 &= (a_0 + a_1 + a_2 + a_3 + a_4) \cdot (x_0 + x_1 + x_2 + x_3 + x_4) \\
&\quad + (a_1 + a_3) \cdot (x_2 + x_0) + (a_4 + a_3) \cdot (x_4 + x_0) + (a_2 + a_3) \cdot (x_1 + x_0) \\
&\quad + (a_4 + a_0 + a_1 + a_2) \cdot (x_4 + x_3 + x_2 + x_1) + (a_1 + a_2) \cdot (x_2 + x_1)
\end{aligned}$$

If one lets

$$
\begin{aligned}
m_0 &= (a_0 + a_1 + a_2 + a_3 + a_4) \cdot (x_0 + x_1 + x_2 + x_3 + x_4) \\
m_1 &= (a_0 + a_3) \cdot (x_3 + x_0) \\
m_2 &= (a_1 + a_3) \cdot (x_2 + x_0) \\
m_3 &= (a_0 + a_2) \cdot (x_3 + x_1) \\
m_4 &= (a_2 + a_3) \cdot (x_1 + x_0) \\
m_5 &= (a_4 + a_0 + a_2 + a_1) \cdot (x_4 + x_3 + x_2 + x_1) \\
m_6 &= (a_1 + a_2) \cdot (x_2 + x_1) \\
m_7 &= (a_4 + a_0) \cdot (x_4 + x_3) \\
m_8 &= (a_4 + a_1) \cdot (x_4 + x_2) \\
m_9 &= (a_4 + a_3) \cdot (x_4 + x_0)
\end{aligned}
\tag{12a}
$$

Then, (11) becomes

$$
\begin{aligned}
y_0 &= m_0 + m_2 + m_9 + m_4 + m_5 + m_6 \\
y_1 &= m_0 + m_1 + m_9 + m_4 + m_5 + m_7 \\
y_2 &= m_0 + m_1 + m_9 + m_2 + m_5 + m_8 \\
y_3 &= m_0 + m_1 + m_6 + m_7 + m_2 + m_8 + m_9 + m_3 + m_4 \\
y_4 &= m_0 + m_1 + m_2 + m_3 + m_4 + m_5
\end{aligned}
\tag{12b}
$$

Hence, by (12), the total number of multiplications required to perform (7) is 10.

Theorem 1 below, due to Winograd (Ref. 10), will be needed in the following.

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 matrix.

In order to compute transforms of length $2^n - 1$ over $GF(2^n)$ for $n = 5$ it will be necessary to compute a convolution of 15 values over $GF(2^n)$. Such a cyclic convolution can again be expressed in matrix form as a 15×15 cyclic matrix. The permutation π in Theorem 1 for this 15×15 cyclic matrix is given by

$$\pi = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 0 & 6 & 12 & 3 & 9 & 10 & 1 & 7 & 13 & 4 & 5 & 11 & 2 & 8 & 14 \end{pmatrix}$$

With this π the rows and columns of a 15×15 cyclic matrix can be partitioned into blocks of 5×5 cyclic matrices, such that each block forms a 3×3 cyclic matrix. This 15-point cyclic convolution in cyclic matrix form of 5×5 blocks is as follows:

$$\begin{pmatrix} E_0 \\ E_1 \\ E_2 \end{pmatrix} = \begin{pmatrix} A & B & C \\ B & C & A \\ C & A & B \end{pmatrix} \begin{pmatrix} Y_0 \\ Y_1 \\ Y_2 \end{pmatrix} \tag{13}$$

where

$$E_0 = \begin{pmatrix} y_0 \\ y_6 \\ y_{12} \\ y_3 \\ y_9 \end{pmatrix}, \quad E_1 = \begin{pmatrix} y_{10} \\ y_1 \\ y_7 \\ y_{13} \\ y_4 \end{pmatrix}, \quad E_3 = \begin{pmatrix} y_5 \\ y_{11} \\ y_2 \\ y_8 \\ y_{14} \end{pmatrix},$$

$$A = \begin{pmatrix} a_0 & a_6 & a_{12} & a_3 & a_9 \\ a_6 & a_{12} & a_3 & a_9 & a_0 \\ a_{12} & a_3 & a_9 & a_0 & a_6 \\ a_3 & a_9 & a_0 & a_6 & a_{12} \\ a_9 & a_0 & a_6 & a_{12} & a_3 \end{pmatrix}$$

$$B = \begin{pmatrix} a_{10} & a_1 & a_7 & a_{13} & a_4 \\ a_1 & a_7 & a_{13} & a_4 & a_{10} \\ a_7 & a_{13} & a_4 & a_{10} & a_1 \\ a_{13} & a_4 & a_{10} & a_1 & a_7 \\ a_4 & a_{10} & a_1 & a_7 & a_{13} \end{pmatrix}$$

$$C = \begin{pmatrix} a_5 & a_{11} & a_2 & a_8 & a_{14} \\ a_{11} & a_2 & a_8 & a_{14} & a_5 \\ a_2 & a_8 & a_{14} & a_5 & a_{11} \\ a_8 & a_{14} & a_5 & a_{11} & a_2 \\ a_{14} & a_5 & a_{11} & a_2 & a_8 \end{pmatrix} \qquad Y_0 = \begin{pmatrix} x_0 \\ x_6 \\ x_{12} \\ x_3 \\ x_9 \end{pmatrix}$$

$$Y_1 = \begin{pmatrix} x_{10} \\ x_1 \\ x_7 \\ x_{13} \\ x_4 \end{pmatrix}, \qquad Y_2 = \begin{pmatrix} x_5 \\ x_{11} \\ x_2 \\ x_8 \\ x_{14} \end{pmatrix}$$

Now make the correspondences: $a_0 \leftrightarrow A$, $a_1 \leftrightarrow B$, $a_2 \leftrightarrow C$, $y_0 \leftrightarrow E_0$, $y_1 \leftrightarrow E_1$, $y_2 \leftrightarrow E_2$, $x_0 \leftrightarrow Y_0$, $x_1 \leftrightarrow Y_1$, $x_2 \leftrightarrow Y_2$; then by a procedure precisely similar to that used to compute the cyclic convolution of 3 elements, defined in (2), one obtains

$$\begin{aligned} E_0 &= M_0 + M_1 + M_2 \\ E_1 &= M_0 + M_2 + M_3 \\ E_2 &= M_0 + M_3 + M_1 \end{aligned} \tag{14}$$

where

$$\begin{aligned} M_0 &= (A + B + C) \cdot (Y_0 + Y_1 + Y_2) \\ M_1 &= (C + A) \cdot (Y_1 + Y_2) \\ M_2 &= (C + B) \cdot (Y_2 + Y_0) \\ M_3 &= (A + B) \cdot (Y_0 + Y_1) \end{aligned}$$

Equation (14) requires 4 (5 X 5) cyclic matrix multiplies. To find M_i for $i = 0, 1, 2, 3$, one needs to multiply matrices of form $(A + B + C)$, $(C + A)$, $(C + B)$, and $(A + B)$ by vectors $(Y_0 + Y_1 + Y_2)$, $(Y_1 + Y_2)$, $(Y_2 + Y_0)$, and $(Y_0 + Y_1)$, respectively. For example consider $M_1 = (C + A) \cdot (Y_1 + Y_2)$

$$M_1 = \begin{pmatrix} f_0 \\ f_1 \\ f_2 \\ f_3 \\ f_4 \end{pmatrix} = \begin{pmatrix} a_0 + a_5, a_6 + a_{11}, a_{12} + a_2, a_3 + a_8, a_9 + a_{14} \\ a_6 + a_{11}, a_{12} + a_2, a_3 + a_8, a_9 + a_{14}, a_0 + a_5 \\ a_{12} + a_2, a_3 + a_8, a_9 + a_{14}, a_0 + a_5, a_6 + a_{11} \\ a_3 + a_8, a_9 + a_{14}, a_0 + a_5, a_6 + a_{11}, a_{12} + a_2 \\ a_9 + a_{14}, a_0 + a_5, a_6 + a_{11}, a_{12} + a_2, a_3 + a_8 \end{pmatrix} \begin{pmatrix} x_{10} + x_5 \\ x_1 + x_{11} \\ x_7 + x_2 \\ x_{13} + x_8 \\ x_4 + x_{14} \end{pmatrix}$$

Using the 5-point cyclic matrix in (7) and making the correspondences, $f_0 \leftrightarrow y_0$, $f_1 \leftrightarrow y_1$, $f_2 \leftrightarrow y_2$, $f_3 \leftrightarrow y_3$, $f_4 \leftrightarrow y_4$, $a_0 \leftrightarrow a_0 + a_5$, $a_1 \leftrightarrow a_6 + a_{11}$, $a_2 \leftrightarrow a_{12} + a_2$, $a_3 \leftrightarrow a_3 + a_8$, $a_4 \leftrightarrow a_9 + a_{14}$, $x_0 \leftrightarrow x_{10} + x_5$, $x_1 \leftrightarrow x_1 + x_{11}$, $x_2 \leftrightarrow x_7 + x_2$, $x_3 \leftrightarrow x_{13} + x_8$, $x_4 \leftrightarrow x_4 + x_{14}$, one obtains

$$M_1 = \begin{pmatrix} f_0 \\ f_1 \\ f_2 \\ f_3 \\ f_4 \end{pmatrix} = \begin{pmatrix} F_0 + F_2 + F_9 + F_4 + F_5 + F_6 \\ F_0 + F_1 + F_9 + F_4 + F_5 + F_7 \\ F_0 + F_1 + F_9 + F_2 + F_5 + F_8 \\ F_0 + F_1 + F_6 + F_7 + F_2 + F_8 + F_9 + F_3 + F_4 \\ F_0 + F_1 + F_2 + F_3 + F_4 + F_5 \end{pmatrix} \tag{15}$$

where

$$F_0 = (a_0 + a_5 + a_6 + a_{11} + a_{12} + a_2 + a_3 + a_8 + a_9 + a_{14}) \cdot (x_{10} + x_5 + x_1 + x_{11} + x_7 + x_2 + x_{13} + x_8 + x_4 + x_{14}),$$

$$F_1 = (a_0 + a_5 + a_3 + a_8) \cdot (x_{13} + x_8 + x_{10} + x_5),$$

$$F_2 = (a_6 + a_{11} + a_3 + a_8) \cdot (x_7 + x_2 + x_{10} + x_5),$$

$$F_3 = (a_0 + a_5 + a_{12} + a_2) \cdot (x_1 + x_{11} + x_{13} + x_8),$$

$$F_4 = (a_{12} + a_2 + a_3 + a_8) \cdot (x_{10} + x_5 + x_1 + x_{11}),$$

$$F_5 = (a_0 + a_5 + a_6 + a_{11} + a_{12} + a_2 + a_9 + a_{14}) \cdot (x_1 + x_{11} + x_7 + x_2 + x_{13} + x_8 + x_4 + x_{14})$$

$$F_6 = (a_6 + a_{11} + a_{12} + a_2) \cdot (x_1 + x_{11} + x_7 + x_2)$$

$$F_7 = (a_0 + a_5 + a_9 + a_{14}) \cdot (x_{13} + x_8 + x_4 + x_{14})$$

$$F_8 = (a_6 + a_{11} + a_9 + a_{14}) \cdot (x_7 + x_2 + x_4 + x_{14})$$

$$F_9 = (a_3 + a_8 + a_9 + a_{14}) \cdot (x_{10} + x_5 + x_4 + x_{14})$$

Equation (15) requires 10 multiplies. In a similar manner each of the matrices M_0, M_2, M_3 can be obtained using 10 multiplications. Thus by (14) the total number of multiplications needed to compute (13) is 40.

III. A New Algorithm for Computing a Transform over $GF(2^n)$ of $2^n - 1$ Points for $n = 5, 6$

Let $GF(2^n)$ be the finite field of 2^n elements. Assume that N is an integer that divides $2^n - 1$. Next, let the element $\gamma \epsilon GF(2^n)$ generate the cyclic subgroup of N elements, $G_N = \{\gamma, \gamma^2, \ldots, \gamma^N = 1\}$, in the multiplicative group of $GF(2^n)$. The transform over this subgroup G_N is defined by

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

where $a_i \epsilon GF(2^n)$. Rewrite this in matrix form as

$$\bar{A} = W' \bar{a}, \tag{16}$$

where

$W' = (w'_{i,j})$ and $w'_{i,j} = \gamma^{ij}$.

Also let

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

and

$$A_j = A_0 + B_j \qquad \text{for} \qquad j = 1, 2, \ldots N - 1$$

where

$$B_j = \sum_{i=1}^{N-1} a_i \gamma^{ij}$$

That is, let

$$\overline{B} = W\overline{a} \tag{17}$$

where W is the $(N - 1) \times (N - 1)$ matrix $(\gamma^{ij})_{i,j\neq 0}$ and $\overline{a}$, $\overline{B}$ are the column matrices (a_i) and (B_j), respectively.

If N is a prime number p, one can find an element $\alpha \epsilon GF(p)$ which generates the cyclic subgroup of $p - 1$ elements. Hence a permutation or substitution σ can be defined by

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

where all the elements of this substitution are taken modulo p.

Using the above permutation, by (Ref. 14), one can permute the indices of $\overline{B}$, $\overline{a}$, W defined in (17) so that matrix $\tilde{W} = (\gamma^{\sigma(i)\sigma(j)})_{i,j\neq 0}$ is cyclic. That is,

$$B_{\sigma(j)} = \sum_{i=1}^{p-1} a_{\sigma(i)} \gamma^{\sigma(i)\sigma(j)}$$

$$= \sum_{i=1}^{p-1} a_{\sigma(i)} \gamma^{\alpha^{i+j}}$$

$$= \sum_{i=1}^{p-1} a_{\sigma(i)} \gamma^{\sigma(i+j)} \qquad \text{for} \qquad j = 1, 2, \ldots, p - 1 \tag{18a}$$

This is reexpressed in matrix form as

$$\tilde{B} = \tilde{W}\,\tilde{a} \tag{18b}$$

where

$\tilde{B} = (B_{\sigma(j)})$, $\tilde{W} = (\gamma^{\sigma(i+j)})_{i,j\neq 0}$, and $\tilde{a} = (a_{\sigma(i)})$.

By (18a), $B_{\sigma(j)}$ is a cyclic convolution of $a_{\sigma(i)}$ and $\gamma^{\sigma(i)}$ for $j = 1, 2, \cdots p-1$.

Let $p - 1 = p_1 \cdot p_2 \cdots p_r$ be the factorization of $p - 1$ into primes. 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 $a_1 \times a_1$ cyclic matrix can be partitioned into b_2^2 matrices of size $a_2 \times a_2$. In general, $a_i = a_{i+1} \times b_{i+1}$, 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 $i = 1, 2, \cdots, r$, then Winograd has shown (Ref. 10) that the number of multiplications needed to compute a $(p-1)$-point cyclic convolution is equal to $N = m_1 \cdot m_2 \cdots m_r$.

Let $N = N_1 N_2 \cdots N_k$, where $(N_i, N_j) = 1$ for $i \neq j$. Using the Chinese remainder theorem for integers it is shown by Winograd in Refs. 9, 10 that the transform matrix W' defined in (16) can be transformed into the direct product of W_1', W_2', $\cdots$, W_k', where W_i' is the matrix of an N_i-point transform. Assume that m_i is the number of multiplications needed to perform an N_i-point transform over $GF(2^n)$ for $i = 1, 2, \ldots, k$. Then, the number of multiplications required to compute an N-point transform is $m_1 \cdot m_2 \cdots m_k$.

A. Transform over $GF(2^5)$ of 31 Points

Consider the finite field $GF(2^5)$. Since $N = 2^5 - 1 = 31$ is a prime p, the cyclic convolution algorithm developed in the previous section can be used to calculate the transform of 15 points over $GF(2^5)$. For $N = 31$, the permutation σ is given by

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 & 19 & 20 \\ 3 & 9 & 27 & 19 & 26 & 16 & 17 & 20 & 29 & 25 & 13 & 8 & 24 & 10 & 30 & 28 & 22 & 4 & 12 & 5 \end{pmatrix}$$

$$\begin{pmatrix} 21 & 22 & 23 & 24 & 25 & 26 & 27 & 28 & 29 & 30 \\ 15 & 14 & 11 & 2 & 6 & 18 & 23 & 7 & 21 & 1 \end{pmatrix} \bmod 31$$

Let γ be a 31-st root of unity in $GF(2^5)$. Using the above permutation, one can permute the indices of $\bar{B}$, $\bar{a}$, W defined in (17) so that the matrix, $\tilde{W} = (\gamma^{\sigma(i+j)})_{i,j\neq 0}$ is cyclic for $i = 1, 2, \ldots, 30$ and $j = 1, 2, \ldots, 30$. By Theorem 1, the cyclic matrix $\tilde{W}$ can be first partitioned into 5×5 blocks as follows:

$$\tilde{W} = (A, B, C, \ldots)$$

In terms of this matrix the convolution (18b) is given by

$$\begin{pmatrix} T_1 \\ T_2 \\ T_3 \\ T_4 \\ T_5 \\ T_6 \end{pmatrix} = \begin{pmatrix} A & B & C & D & E & F \\ B & C & A & E & F & D \\ C & A & B & F & D & E \\ D & E & F & A & B & C \\ E & F & D & B & C & A \\ F & D & E & C & A & B \end{pmatrix} \begin{pmatrix} S_1 \\ S_2 \\ S_3 \\ S_4 \\ S_5 \\ S_6 \end{pmatrix} \tag{19}$$

where

$$T_1 = \begin{pmatrix} b_3 \\ b_{17} \\ b_{24} \\ b_{12} \\ b_6 \end{pmatrix}, \quad T_2 = \begin{pmatrix} b_{13} \\ b_{22} \\ b_{11} \\ b_{21} \\ b_{26} \end{pmatrix}, \quad T_3 = \begin{pmatrix} b_{15} \\ b_{23} \\ b_{27} \\ b_{29} \\ b_{30} \end{pmatrix}, \quad T_4 = \begin{pmatrix} b_{28} \\ b_{14} \\ b_7 \\ b_{19} \\ b_{25} \end{pmatrix},$$

$$T_5 = \begin{pmatrix} b_{18} \\ b_9 \\ b_{20} \\ b_{10} \\ b_5 \end{pmatrix}, \quad T_6 = \begin{pmatrix} b_{16} \\ b_8 \\ b_4 \\ b_2 \\ b_1 \end{pmatrix}, \quad A = \begin{pmatrix} \gamma^9 & \gamma^{20} & \gamma^{10} & \gamma^5 & \gamma^{18} \\ \gamma^{20} & \gamma^{10} & \gamma^5 & \gamma^{18} & \gamma^9 \\ \gamma^{10} & \gamma^5 & \gamma^{18} & \gamma^9 & \gamma^{20} \\ \gamma^5 & \gamma^{18} & \gamma^9 & \gamma^{20} & \gamma^{10} \\ \gamma^{18} & \gamma^9 & \gamma^{20} & \gamma^{10} & \gamma^5 \end{pmatrix}$$

$$B = \begin{pmatrix} \gamma^8 & \gamma^4 & \gamma^2 & \gamma^1 & \gamma^{16} \\ \gamma^4 & \gamma^2 & \gamma^1 & \gamma^{16} & \gamma^8 \\ \gamma^2 & \gamma^1 & \gamma^{16} & \gamma^8 & \gamma^4 \\ \gamma^1 & \gamma^{16} & \gamma^8 & \gamma^4 & \gamma^2 \\ \gamma^{16} & \gamma^8 & \gamma^4 & \gamma^2 & \gamma^1 \end{pmatrix}, \quad C = \begin{pmatrix} \gamma^{14} & \gamma^7 & \gamma^{19} & \gamma^{25} & \gamma^{28} \\ \gamma^7 & \gamma^{19} & \gamma^{25} & \gamma^{28} & \gamma^{14} \\ \gamma^{19} & \gamma^{25} & \gamma^{28} & \gamma^{14} & \gamma^7 \\ \gamma^{25} & \gamma^{28} & \gamma^{14} & \gamma^7 & \gamma^{19} \\ \gamma^{28} & \gamma^{14} & \gamma^7 & \gamma^{19} & \gamma^{25} \end{pmatrix}$$

$$D = \begin{pmatrix} \gamma^{22} & \gamma^{11} & \gamma^{21} & \gamma^{26} & \gamma^{13} \\ \gamma^{11} & \gamma^{21} & \gamma^{26} & \gamma^{13} & \gamma^{22} \\ \gamma^{21} & \gamma^{26} & \gamma^{13} & \gamma^{22} & \gamma^{11} \\ \gamma^{26} & \gamma^{13} & \gamma^{22} & \gamma^{11} & \gamma^{21} \\ \gamma^{13} & \gamma^{22} & \gamma^{11} & \gamma^{21} & \gamma^{26} \end{pmatrix}, \quad E = \begin{pmatrix} \gamma^{23} & \gamma^{27} & \gamma^{29} & \gamma^{30} & \gamma^{15} \\ \gamma^{27} & \gamma^{29} & \gamma^{30} & \gamma^{15} & \gamma^{23} \\ \gamma^{29} & \gamma^{30} & \gamma^{15} & \gamma^{23} & \gamma^{27} \\ \gamma^{30} & \gamma^{15} & \gamma^{23} & \gamma^{27} & \gamma^{29} \\ \gamma^{15} & \gamma^{23} & \gamma^{27} & \gamma^{29} & \gamma^{30} \end{pmatrix}$$

$$F = \begin{pmatrix} \gamma^{17} & \gamma^{24} & \gamma^{12} & \gamma^{6} & \gamma^{3} \\ \gamma^{24} & \gamma^{12} & \gamma^{6} & \gamma^{3} & \gamma^{17} \\ \gamma^{12} & \gamma^{6} & \gamma^{3} & \gamma^{17} & \gamma^{24} \\ \gamma^{6} & \gamma^{3} & \gamma^{17} & \gamma^{24} & \gamma^{12} \\ \gamma^{3} & \gamma^{17} & \gamma^{24} & \gamma^{12} & \gamma^{6} \end{pmatrix}, \quad S_1 = \begin{pmatrix} a_3 \\ a_{17} \\ a_{24} \\ a_{12} \\ a_6 \end{pmatrix}, \quad S_2 = \begin{pmatrix} a_{13} \\ a_{22} \\ a_{11} \\ a_{21} \\ a_{26} \end{pmatrix}$$

$$S_3 = \begin{pmatrix} a_{15} \\ a_{23} \\ a_{27} \\ a_{29} \\ a_{30} \end{pmatrix}, \quad S_4 = \begin{pmatrix} a_{28} \\ a_{14} \\ a_7 \\ a_{19} \\ a_{25} \end{pmatrix} \quad S_5 = \begin{pmatrix} a_{18} \\ a_9 \\ a_{20} \\ a_{10} \\ a_5 \end{pmatrix}, \quad S_6 = \begin{pmatrix} a_{16} \\ a_8 \\ a_4 \\ a_2 \\ a_1 \end{pmatrix}$$

Observe that the matrix equation (19) can be further reduced as follows:

$$N = \begin{pmatrix} F_0 \\ F_1 \end{pmatrix} = \begin{pmatrix} J & K \\ K & J \end{pmatrix} \begin{pmatrix} E_0 \\ E_1 \end{pmatrix} = \begin{pmatrix} J(E_0 + E_1) + (J + K) \cdot E_1 \\ J(E_0 + E_1) + (J + K) \cdot E_0 \end{pmatrix}$$

where

$$F_0 = \begin{pmatrix} T_1 \\ T_2 \\ T_3 \end{pmatrix}, \quad F_2 = \begin{pmatrix} T_4 \\ T_5 \\ T_6 \end{pmatrix}, \quad J = \begin{pmatrix} A & B & C \\ B & C & A \\ C & A & B \end{pmatrix},$$

and

$$K = \begin{pmatrix} D & E & F \\ E & F & D \\ F & D & E \end{pmatrix}$$

Now let

$$U_1 = (E_0 + E_1) \cdot J$$

$$U_2 = (J + K) \cdot E_1 \tag{20}$$

$$U_3 = (J + K) \cdot E_0$$

Then $F_0 = U_1 + U_2$, $F_1 = U_1 + U_3$. Thus, $3(15 \times 15)$ cyclic matrix multiplies are necessary to perform (20). By a procedure precisely similar to that used to compute the 15×15 cyclic convolution in (13), the number of multiplications needed to compute U_1 in (20) is 40. In a similar manner, each of the matrices U_2 and U_3 in (20) can be obtained with 40 multiplications. Thus, the total number of multiplications needed to perform (19) is $3 \times 40 = 120$.

B. Transform over $GF(2^6)$ of 63 Points

Since $N = 2^6 - 1 = 63 = N_1 \cdot N_2 = 7 \cdot 9$, by Winograd's algorithm one needs to compute an N_i-point transform over $GF(2^6)$ for $N_i = 7$ or 9. The algorithms for computing these transforms over $GF(2^6)$ are given in Appendix A. Let integer i for $0 \leqslant i < 63$ be represented by a pair $(i_1, i_2) = (i \bmod 3, i \bmod 5)$. Since 7 and 9 are relatively prime, by the Chinese remainder theorem,

$$i \equiv i_1 \cdot 36 + i_2 \cdot 28 \bmod 63 \tag{21}$$

is the required representation.

Let γ be the 63rd root of unity in $GF(2^6)$. Also let $\gamma_1 \equiv \gamma^9 \bmod 2$ and $\gamma_2 \equiv \gamma^7 \bmod 2$ be the 7th and 9th roots of unity in $GF(2^6)$, respectively. The 63rd point transform over $GF(2^6)$ in i_1 and i_2 is

$$A_j = \sum_{i=0}^{63} a_i \gamma^{ij}$$

$$A_{(j_1,j_2)} = \sum_{i_1=0}^{6} \left[\sum_{i_2=0}^{8} a_{(i_1,i_2)} \gamma_2^{i_2 j_2} \right] \gamma_1^{i_1 j_1} \tag{22}$$

$$= \sum_{i_1=0}^{6} a_{i_1}(j_2) \gamma_1^{i_1 j_1}$$

where

$$a_{i_1}(j_2) = \sum_{i_2=0}^{8} a_{(i_1,i_2)}\, \gamma_2^{i_2 j_2} \qquad \begin{array}{l} \text{for } j_1 = 0, 1, 2, \ldots, 6 \\ \text{and } j_2 = 0, 1, 2, \ldots, 8 \end{array}$$

or in matrix notation

$$(a_{i_1}(j_2)) = W_2'\, \bar{a}_{i_1}$$

where

$$W_2' = \begin{pmatrix} \gamma_2^0 & \gamma_2^0 & \gamma_2^0 & \gamma_2^0 & \gamma_2^0 & \gamma_2^0 & \gamma_2^0 & \gamma_2^0 & \gamma_2^0 \\ \gamma_2^0 & \gamma_2^1 & \gamma_2^2 & \gamma_2^3 & \gamma_2^4 & \gamma_2^5 & \gamma_2^6 & \gamma_2^7 & \gamma_2^8 \\ \gamma_2^0 & \gamma_2^2 & \gamma_2^4 & \gamma_2^6 & \gamma_2^8 & \gamma_2^1 & \gamma_2^3 & \gamma_2^5 & \gamma_2^7 \\ \gamma_2^0 & \gamma_2^3 & \gamma_2^6 & \gamma_2^0 & \gamma_2^3 & \gamma_2^6 & \gamma_2^0 & \gamma_2^3 & \gamma_2^6 \\ \gamma_2^0 & \gamma_2^4 & \gamma_2^8 & \gamma_2^3 & \gamma_2^7 & \gamma_2^2 & \gamma_2^6 & \gamma_2^1 & \gamma_2^5 \\ \gamma_2^0 & \gamma_2^5 & \gamma_2^1 & \gamma_2^6 & \gamma_2^2 & \gamma_2^7 & \gamma_2^3 & \gamma_2^8 & \gamma_2^4 \\ \gamma_2^0 & \gamma_2^6 & \gamma_2^3 & \gamma_2^0 & \gamma_2^6 & \gamma_2^3 & \gamma_2^0 & \gamma_2^6 & \gamma_2^3 \\ \gamma_2^0 & \gamma_2^7 & \gamma_2^5 & \gamma_2^3 & \gamma_2^1 & \gamma_2^8 & \gamma_2^6 & \gamma_2^4 & \gamma_2^2 \\ \gamma_2^0 & \gamma_2^8 & \gamma_2^7 & \gamma_2^6 & \gamma_2^5 & \gamma_2^4 & \gamma_2^3 & \gamma_2^2 & \gamma_2^1 \end{pmatrix}$$

$$\bar{a}_{i_1} = \begin{pmatrix} a_{(i_1,0)} \\ a_{(i_1,1)} \\ a_{(i_1,2)} \\ a_{(i_1,3)} \\ a_{(i_1,4)} \\ a_{(i_1,5)} \\ a_{(i_1,6)} \\ a_{(i_1,7)} \\ a_{(i_1,8)} \end{pmatrix}$$

Thus, (22) becomes

$$\overline{A}_{j_1} = \sum_{i_1=0}^{6} \gamma_1^{i_1 j_1} W_2' \overline{a}_{i_1} \qquad \text{for } j_1 = 0, 1, 2, \ldots, 6$$

or

$$\begin{pmatrix} \overline{A}_0 \\ \overline{A}_1 \\ \overline{A}_2 \\ \overline{A}_3 \\ \overline{A}_4 \\ \overline{A}_5 \\ \overline{A}_6 \end{pmatrix} = \begin{pmatrix} W_2' & W_2' & W_2' & W_2' & W_2' & W_2' & W_2' \\ W_2' & W_2'\gamma_1^1 & W_2'\gamma_1^2 & W_2'\gamma_1^3 & W_2'\gamma_1^4 & W_2'\gamma_1^5 & W_2'\gamma_1^6 \\ W_2' & W_2'\gamma_1^2 & W_2'\gamma_1^4 & W_2'\gamma_1^6 & W_2'\gamma_1^1 & W_2'\gamma_1^3 & W_2'\gamma_1^5 \\ W_2' & W_2'\gamma_1^3 & W_2'\gamma_1^6 & W_2'\gamma_1^2 & W_2'\gamma_1^5 & W_2'\gamma_1^1 & W_2'\gamma_1^4 \\ W_2' & W_2'\gamma_1^4 & W_2'\gamma_1^1 & W_2'\gamma_1^5 & W_2'\gamma_1^2 & W_2'\gamma_1^6 & W_2'\gamma_1^3 \\ W_2' & W_2'\gamma_1^5 & W_2'\gamma_1^3 & W_2'\gamma_1^1 & W_2'\gamma_1^6 & W_2'\gamma_1^4 & W_2'\gamma_1^2 \\ W_2' & W_2'\gamma_1^6 & W_2'\gamma_1^5 & W_2'\gamma_1^4 & W_2'\gamma_1^3 & W_2'\gamma_1^2 & W_2'\gamma_1^1 \end{pmatrix} \begin{pmatrix} \overline{a}_0 \\ \overline{a}_1 \\ \overline{a}_2 \\ \overline{a}_3 \\ \overline{a}_4 \\ \overline{a}_5 \\ \overline{a}_6 \end{pmatrix}$$

Now by (21), one obtains $\overline{A_0}$ in terms of A_k as

$$\overline{A}_0 = \begin{pmatrix} A_{(0,0)} \\ A_{(0,1)} \\ A_{(0,2)} \\ A_{(0,3)} \\ A_{(0,4)} \\ A_{(0,5)} \\ A_{(0,6)} \\ A_{(0,7)} \\ A_{(0,8)} \end{pmatrix} = \begin{pmatrix} A_0 \\ A_{28} \\ A_{56} \\ A_{21} \\ A_{49} \\ A_{14} \\ A_{42} \\ A_7 \\ A_{35} \end{pmatrix}$$

Similarly

$$\overline{A}_1 = \begin{pmatrix} A_{(1,0)} \\ A_{(1,1)} \\ A_{(1,2)} \\ A_{(1,3)} \\ A_{(1,4)} \\ A_{(1,5)} \\ A_{(1,6)} \\ A_{(1,7)} \\ A_{(1,8)} \end{pmatrix} = \begin{pmatrix} A_{36} \\ A_{1} \\ A_{29} \\ A_{57} \\ A_{22} \\ A_{50} \\ A_{15} \\ A_{43} \\ A_{8} \end{pmatrix}, \quad \overline{A}_2 = \begin{pmatrix} A_{(2,0)} \\ A_{(2,1)} \\ A_{(2,2)} \\ A_{(2,3)} \\ A_{(2,4)} \\ A_{(2,5)} \\ A_{(2,6)} \\ A_{(2,7)} \\ A_{(2,8)} \end{pmatrix} = \begin{pmatrix} A_{9} \\ A_{37} \\ A_{2} \\ A_{30} \\ A_{58} \\ A_{23} \\ A_{51} \\ A_{16} \\ A_{44} \end{pmatrix},$$

$$\overline{A}_3 = \begin{pmatrix} A_{(3,0)} \\ A_{(3,1)} \\ A_{(3,2)} \\ A_{(3,3)} \\ A_{(3,4)} \\ A_{(3,5)} \\ A_{(3,6)} \\ A_{(3,7)} \\ A_{(3,8)} \end{pmatrix} = \begin{pmatrix} A_{45} \\ A_{10} \\ A_{38} \\ A_{3} \\ A_{31} \\ A_{59} \\ A_{24} \\ A_{52} \\ A_{17} \end{pmatrix}, \quad \overline{A}_4 = \begin{pmatrix} A_{(4,0)} \\ A_{(4,1)} \\ A_{(4,2)} \\ A_{(4,3)} \\ A_{(4,4)} \\ A_{(4,5)} \\ A_{(4,6)} \\ A_{(4,7)} \\ A_{(4,8)} \end{pmatrix} = \begin{pmatrix} A_{18} \\ A_{46} \\ A_{11} \\ A_{39} \\ A_{4} \\ A_{32} \\ A_{60} \\ A_{25} \\ A_{53} \end{pmatrix}$$

$$\overline{A}_5 = \begin{pmatrix} A_{(5,0)} \\ A_{(5,1)} \\ A_{(5,2)} \\ A_{(5,3)} \\ A_{(5,4)} \\ A_{(5,5)} \\ A_{(5,6)} \\ A_{(5,7)} \\ A_{(5,8)} \end{pmatrix} = \begin{pmatrix} A_{54} \\ A_{19} \\ A_{47} \\ A_{12} \\ A_{40} \\ A_{5} \\ A_{33} \\ A_{61} \\ A_{26} \end{pmatrix}, \quad \overline{A}_6 = \begin{pmatrix} A_{(6,0)} \\ A_{(6,1)} \\ A_{(6,2)} \\ A_{(6,3)} \\ A_{(6,4)} \\ A_{(6,5)} \\ A_{(6,6)} \\ A_{(6,7)} \\ A_{(6,8)} \end{pmatrix} = \begin{pmatrix} A_{27} \\ A_{55} \\ A_{20} \\ A_{48} \\ A_{13} \\ A_{41} \\ A_{6} \\ A_{34} \\ A_{62} \end{pmatrix}$$

$$\overline{a}_0 = \begin{pmatrix} a_0 \\ a_{28} \\ a_{56} \\ a_{21} \\ a_{49} \\ a_{14} \\ a_{42} \\ a_7 \\ a_{35} \end{pmatrix}, \quad \overline{a}_1 = \begin{pmatrix} a_{36} \\ a_1 \\ a_{29} \\ a_{57} \\ a_{22} \\ a_{50} \\ a_{15} \\ a_{43} \\ a_8 \end{pmatrix}, \quad \overline{a}_2 = \begin{pmatrix} a_9 \\ a_{37} \\ a_2 \\ a_{30} \\ a_{58} \\ a_{23} \\ a_{51} \\ a_{16} \\ a_{44} \end{pmatrix}$$

$$\bar{a}_3 = \begin{pmatrix} a_{45} \\ a_{10} \\ a_{38} \\ a_3 \\ a_{31} \\ a_{59} \\ a_{24} \\ a_{52} \\ a_{17} \end{pmatrix}, \bar{a}_4 = \begin{pmatrix} a_{18} \\ a_{46} \\ a_{11} \\ a_{39} \\ a_4 \\ a_{32} \\ a_{60} \\ a_{25} \\ a_{53} \end{pmatrix}, \bar{a}_5 = \begin{pmatrix} a_{54} \\ a_{19} \\ a_{47} \\ a_{12} \\ a_{40} \\ a_5 \\ a_{33} \\ a_{61} \\ a_{26} \end{pmatrix}, \bar{a}_6 = \begin{pmatrix} a_{27} \\ a_{55} \\ a_{20} \\ a_{48} \\ a_{13} \\ a_{41} \\ a_6 \\ a_{34} \\ a_{62} \end{pmatrix}$$

Using the 7-point transform in (1B) and making the correspondences, $\gamma^0 \longleftrightarrow W_2'$, $\gamma' \longleftrightarrow W_2'\gamma_1$, $\gamma^2 \longleftrightarrow W_2'\gamma_1^2$, $\gamma^3 \longleftrightarrow W_3'\gamma_1^3$, $\gamma^4 \longleftrightarrow W_2'\gamma_1^4$, $\gamma^5 \longleftrightarrow W_2'\gamma_1^5$, $\gamma^6 \longleftrightarrow W_2'\gamma_1^6$, one obtains

$$A_0 = M_0$$

$$A_1 = M_0 + M_1 + M_2 + M_3 + M_4 + M_5 + M_6$$

$$A_2 = M_0 + M_1 + M_7 + M_2 + M_4 + M_8 + M_5$$

$$A_3 = M_0 + M_1 + M_3 + M_7 + M_9 + M_{10} + M_{11}$$

$$A_4 = M_0 + M_1 + M_3 + M_7 + M_4 + M_6 + M_8$$

$$A_5 = M_0 + M_1 + M_7 + M_2 + M_9 + M_{11} + M_{12}$$

$$A_6 = M_0 + M_1 + M_2 + M_3 + M_9 + M_{12} + M_{10}$$

where

$$M_0 = W_2' \cdot (\bar{a}_0 + \bar{a}_1 + \bar{a}_2 + \bar{a}_3 + \bar{a}_4 + \bar{a}_5 + \bar{a}_6)$$

$$M_1 = W_2' \cdot (\gamma^2 + \gamma^1 + \gamma^4 + 1) \cdot (\bar{a}_3 + \bar{a}_4 + \bar{a}_5 + \bar{a}_2 + \bar{a}_6 + \bar{a}_1)$$

$$M_2 = W_2' \cdot (\gamma^2 + \gamma^1) \cdot (\bar{a}_5 + \bar{a}_2 + \bar{a}_3 + \bar{a}_4) \tag{23}$$

$$M_3 = W_2' \cdot (\gamma^4 + \gamma^2)(\bar{a}_6 + \bar{a}_1 + \bar{a}_5 + \bar{a}_2)$$

$$M_4 = W_2' \cdot (\bar{a}_3 + \bar{a}_5 + \bar{a}_6)$$

$$M_5 = W_2' \cdot (\gamma^2 + \gamma^5 + \gamma^1 + \gamma^6) \cdot (\bar{a}_5 + \bar{a}_3)$$

$$M_6 = W_2' \cdot (\gamma^4 + \gamma^3 + \gamma^2 + \gamma^5) \cdot (\bar{a}_6 + \bar{a}_5)$$

$$M_7 = W_2' \cdot (\gamma^4 + \gamma^1) \cdot (\bar{a}_6 + \bar{a}_1 + \bar{a}_3 + \bar{a}_4)$$

$$M_8 = W_2' \cdot (\gamma^4 + \gamma^3 + \gamma^1 + \gamma^6) \cdot (\bar{a}_6 + \bar{a}_3)$$

$$M_9 = W_2' \cdot (\bar{a}_4 + \bar{a}_2 + \bar{a}_1) \tag{23}$$

$$M_{10} = W_2' \cdot (\gamma^4 + \gamma^3 + \gamma^2 + \gamma^5) \cdot (\bar{a}_1 + \bar{a}_2)$$

$$M_{11} = W_2' \cdot (\gamma^4 + \gamma^3 + \gamma^1 + \gamma^6) \cdot (\bar{a}_1 + \bar{a}_4)$$

$$M_{12} = W_2' \cdot (\gamma^2 + \gamma^5 + \gamma^1 + \gamma^6) \cdot (\bar{a}_2 + \bar{a}_4)$$

Observe that all thirteen matrix multiplies in (23) are 9-point convolutions of exactly the same form as (8B). Thus one may compute M_j for $j = 0, 1, 2, 3, \ldots, 12$ in (23) with a procedure similar to that used to compute the convolution defined by (8B). Thus, the number of multiplications for computing M_j for $j = 0, 1, 2, \ldots, 12$ is 16, excluding multiplications by γ^0. Hence, the total number of multiplications needed is $13 \times 16 = 208$.

IV. Comparison of New Algorithm with Gentleman's Algorithm

If $N = 2^n - 1 = N_1 \cdot N_2 \cdots N_k$ where $(N_i, N_j) = 1$ for $i \neq j$, Gentleman shows in References 5 and 11 that an N-point transform of such an N requires $N(N_1 + N_2 + \cdots + N_k - k + 1)$ multiplications, including multiplications by unity. The present algorithm for computing the $(2^n - 1)$-point transform for $n = 5$, 6 and Gentleman's algorithm are compared in Table 1. The number of multiplications needed to perform these algorithms is given in both cases. Evidently for $n = 5$ and 6 the new algorithm for computing the $(2^n - 1)$-point transform requires considerably fewer multiplications than Gentleman's algorithm.

V. Transform Decoder for Reed-Solomon Codes

It is shown in References 12 and 15 that RS codes can be decoded with a fast transform algorithm over $GP(p^n)$ and continued fractions. There it was shown that the transform over $GF(p^n)$ where p is a prime and n is an integer can be used to compute the syndrome and error magnitudes. It follows from References 5 and 16 that the number of multiplications required to perform the syndrome and error magnitude calculations for the standard decoder is approximately $(N - 1)(d - 1) + t^2$, where N is the block length of the RS code in $GF(2^n)$, $d = 2t + 1$ is the minimum distance of the code and t is the number of allowable errors. (Note that the performance of the conventional decoder is dependent on the number of allowable errors.)

For (31, 15) and (63, 33) RS codes, the number of multiplications needed to compute the syndrome and the error magnitudes is given in Table 2. The new algorithm, Gentleman's algorithm, and the standard algorithm are compared in Table 2 in terms of the number of multiplications needed to compute the syndrome and the error magnitudes for decoding these RS codes.

Appendix A

Consider $N_i = 7$. Let γ be a 7th root of unity in $GF(2^6)$. The transform over $GF(2^6)$ is expressible as

$$\begin{pmatrix} A_0 \\ A_1 \\ A_2 \\ A_3 \\ A_4 \\ A_5 \\ A_6 \end{pmatrix} = \begin{pmatrix} \gamma^0 & \gamma^0 & \gamma^0 & \gamma^0 & \gamma^0 & \gamma^0 & \gamma^0 \\ \gamma^0 & \gamma^1 & \gamma^2 & \gamma^3 & \gamma^4 & \gamma^5 & \gamma^6 \\ \gamma^0 & \gamma^2 & \gamma^4 & \gamma^6 & \gamma^1 & \gamma^3 & \gamma^5 \\ \gamma^0 & \gamma^3 & \gamma^6 & \gamma^2 & \gamma^5 & \gamma^1 & \gamma^4 \\ \gamma^0 & \gamma^4 & \gamma^1 & \gamma^5 & \gamma^2 & \gamma^6 & \gamma^3 \\ \gamma^0 & \gamma^5 & \gamma^3 & \gamma^1 & \gamma^6 & \gamma^4 & \gamma^2 \\ \gamma^0 & \gamma^6 & \gamma^5 & \gamma^4 & \gamma^3 & \gamma^2 & \gamma^1 \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \end{pmatrix} \tag{A-1}$$

The permutation σ of $N = 7$ 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 (A-1), one obtains a 6×6 cyclic matrix equation. By Theorem 1, there exists a permutation π of rows and columns so that the 6×6 cyclic matrix can be partitioned into a 2×2 block matrix of 3×3 cyclic matrices as

$$\begin{pmatrix} B_3 \\ B_5 \\ B_6 \\ B_4 \\ B_2 \\ B_1 \end{pmatrix} = \begin{pmatrix} \gamma^2 & \gamma^1 & \gamma^4 & \gamma^5 & \gamma^6 & \gamma^3 \\ \gamma^1 & \gamma^4 & \gamma^2 & \gamma^6 & \gamma^3 & \gamma^5 \\ \gamma^4 & \gamma^2 & \gamma^1 & \gamma^3 & \gamma^5 & \gamma^6 \\ \gamma^5 & \gamma^6 & \gamma^3 & \gamma^2 & \gamma^1 & \gamma^4 \\ \gamma^6 & \gamma^3 & \gamma^5 & \gamma^1 & \gamma^4 & \gamma^2 \\ \gamma^3 & \gamma^5 & \gamma^6 & \gamma^4 & \gamma^2 & \gamma^1 \end{pmatrix} \begin{pmatrix} a_3 \\ a_5 \\ a_6 \\ a_4 \\ a_2 \\ a_1 \end{pmatrix} \tag{A-2}$$

or

$$\begin{pmatrix} E_1 \\ E_2 \end{pmatrix} = \begin{pmatrix} A & B \\ B & A \end{pmatrix} \begin{pmatrix} X_1 \\ X_2 \end{pmatrix}$$

$$= \begin{pmatrix} (X_1 + X_2) \cdot A + (B - A) \cdot X_2 \\ (X_1 + X_2) \cdot A + (B - A) \cdot X_1 \end{pmatrix}$$

$$= \begin{pmatrix} D + E \\ D + F \end{pmatrix}$$

where

$D = (X_1 + X_2) \cdot A$, $E = (B - A) \cdot X_2$, $F = (B - A) \cdot X_1$.

Since A and B are cyclic matrices, it is evident that the matrix $B - A$ is also a cyclic matrix. In (A-2), D is defined as

$$D = \begin{pmatrix} d_0 \\ d_1 \\ d_2 \end{pmatrix} = \begin{pmatrix} \gamma^2 & \gamma^1 & \gamma^4 \\ \gamma^1 & \gamma^4 & \gamma^2 \\ \gamma^4 & \gamma^2 & \gamma^1 \end{pmatrix} \begin{pmatrix} Y_0 \\ Y_1 \\ Y_2 \end{pmatrix}$$

where

$Y_0 = a_3 + a_4$, $Y_1 = a_5 + a_2$, and $Y_2 = a_6 + a_1$.

Using the 3-point cyclic convolution in (2) and making the correspondences, $a_0 \leftrightarrow \gamma^2$, $a_1 \leftrightarrow \gamma^1$, $a_2 \leftrightarrow \gamma^4$, $x_0 \leftrightarrow Y_0$, $x_1 \leftrightarrow Y_1$, $x_2 \leftrightarrow Y_2$, $y_0 \leftrightarrow d_0$, $y_1 \leftrightarrow d_1$, $y_2 \leftrightarrow d_2$, one obtains

$$D = \begin{pmatrix} d_0 \\ d_1 \\ d_2 \end{pmatrix} = \begin{pmatrix} (\gamma^4 + \gamma^2 + \gamma^1) \cdot (a_3 + a_4 + a_5 + a_2 + a_6 + a_1) + (\gamma^4 + \gamma^2) \\ \cdot (a_6 + a_1 + a_2 + a_5) + (\gamma^4 + \gamma^1) \cdot (a_6 + a_1 + a_3 + a_4) \\ (\gamma^4 + \gamma^2 + \gamma^1) \cdot (a_3 + a_4 + a_5 + a_2 + a_6 + a_1) + (\gamma^4 + \gamma^1) \\ \cdot (a_6 + a_1 + a_3 + a_4) + (\gamma^2 + \gamma^1) \cdot (a_5 + a_2 + a_3 + a_4) \\ (\gamma^4 + \gamma^1 + \gamma^2) \cdot (a_3 + a_4 + a_5 + a_2 + a_6 + a_1) + (\gamma^2 + \gamma^1) \\ \cdot (a_5 + a_2 + a_3 + a_4) + (\gamma^4 + \gamma^2) \cdot (a_6 + a_1 + a_5 + a_2) \end{pmatrix} \quad \text{(A-3)}$$

Similarly,

$$E = \begin{pmatrix} e_0 \\ e_1 \\ e_2 \end{pmatrix} = \begin{pmatrix} \gamma^2 + \gamma^5 & \gamma^1 + \gamma^6 & \gamma^4 + \gamma^3 \\ \gamma^1 + \gamma^6 & \gamma^4 + \gamma^3 & \gamma^2 + \gamma^5 \\ \gamma^4 + \gamma^3 & \gamma^2 + \gamma^5 & \gamma^1 + \gamma^6 \end{pmatrix} \begin{pmatrix} a_4 \\ a_2 \\ a_1 \end{pmatrix}$$

$$= \begin{pmatrix} (\gamma^4 + \gamma^3 + \gamma^2 + \gamma^5 + \gamma^1 + \gamma^6) \cdot (a_4 + a_2 + a_1) + (\gamma^4 + \gamma^3 + \gamma^2 + \gamma^5) \cdot (a_1 + a_2) + (\gamma^4 + \gamma^3 + \gamma^1 + \gamma^6) \cdot (a_1 + a_4) \\ (\gamma^4 + \gamma^3 + \gamma^2 + \gamma^5 + \gamma^1 + \gamma^6) \cdot (a_4 + a_2 + a_1) + (\gamma^4 + \gamma^3 + \gamma^1 + \gamma^6) \cdot (a_1 + a_4) + (\gamma^2 + \gamma^5 + \gamma^1 + \gamma^6) \cdot (a_2 + a_4) \\ (\gamma^4 + \gamma^3 + \gamma^2 + \gamma^5 + \gamma^1 + \gamma^6) \cdot (a_4 + a_2 + a_1) + (\gamma^2 + \gamma^5 + \gamma^1 + \gamma^6) \cdot (a_2 + a_4) + (\gamma^4 + \gamma^3 + \gamma^2 + \gamma^5) \cdot (a_1 + a_2) \end{pmatrix} \quad \text{(A-4)}$$

and

$$F = \begin{pmatrix} f_0 \\ f_1 \\ f_2 \end{pmatrix} = \begin{pmatrix} \gamma^2 + \gamma^5 & \gamma^1 + \gamma^6 & \gamma^4 + \gamma^3 \\ \gamma^1 + \gamma^6 & \gamma^4 + \gamma^3 & \gamma^2 + \gamma^5 \\ \gamma^4 + \gamma^3 & \gamma^2 + \gamma^5 & \gamma^1 + \gamma^6 \end{pmatrix} \begin{pmatrix} a_3 \\ a_5 \\ a_6 \end{pmatrix}$$

$$= \begin{pmatrix} (\gamma^4 + \gamma^3 + \gamma^2 + \gamma^5 + \gamma^1 + \gamma^6) \cdot (a_3 + a_5 + a_6) + (\gamma^4 + \gamma^3 + \gamma^2 + \gamma^5) \cdot (a_6 + a_5) + (\gamma^4 + \gamma^3 + \gamma^1 + \gamma^6) \cdot (a_6 + a_3) \\ (\gamma^4 + \gamma^3 + \gamma^2 + \gamma^5 + \gamma^1 + \gamma^6) \cdot (a_3 + a_5 + a_6) + (\gamma^4 + \gamma^3 + \gamma^1 + \gamma^6) \cdot (a_6 + a_5) + (\gamma^4 + \gamma^3 + \gamma^1 + \gamma^6) \cdot (a_5 + a_3) \\ (\gamma^4 + \gamma^3 + \gamma^2 + \gamma^5 + \gamma^1 + \gamma^6) \cdot (a_3 + a_5 + a_6) + (\gamma^2 + \gamma^5 + \gamma^1 + \gamma^6) \cdot (a_5 + a_3) + (\gamma^4 + \gamma^3 + \gamma^2 + \gamma^5) \cdot (a_6 + a_5) \end{pmatrix} \quad \text{(A-5)}$$

Each of the Eqs. (A-3), (A-4), and (A-5) requires 4 multiplies.

Let

$$m_0 = 1 \cdot (a_0 + a_1 + a_2 + a_3 + a_4 + a_5 + a_6)$$

$$m_1 = (\gamma^2 + \gamma^1 + \gamma^4 + 1) \cdot (a_3 + a_4 + a_5 + a_2 + a_6 + a_1)$$

$$m_2 = (\gamma^2 + \gamma^1) \cdot (a_5 + a_2 + a_3 + a_4)$$

$$m_3 = (\gamma^4 + \gamma^2) \cdot (a_6 + a_1 + a_5 + a_2)$$

$$m_4 = 1 \cdot (a_3 + a_5 + a_6)$$

$$m_5 = (\gamma^2 + \gamma^5 + \gamma^1 + \gamma^6) \cdot (a_5 + a_3)$$

$$m_6 = (\gamma^4 + \gamma^3 + \gamma^2 + \gamma^5) \cdot (a_6 + a_5)$$

$$m_7 = (\gamma^4 + \gamma^1) \cdot (a_6 + a_1 + a_3 + a_4)$$

$$m_8 = (\gamma^4 + \gamma^3 + \gamma^1 + \gamma^6) \cdot (a_6 + a_3)$$

$$m_9 = 1 \cdot (a_4 + a_2 + a_1)$$

$$m_{10} = (\gamma^4 + \gamma^3 + \gamma^2 + \gamma^5) \cdot (a_1 + a_2)$$

$$m_{11} = (\gamma^4 + \gamma^3 + \gamma^1 + \gamma^6) \cdot (a_1 + a_4)$$

$$m_{12} = (\gamma^2 + \gamma^5 + \gamma^1 + \gamma^6) \cdot (a_2 + a_4)$$

Thus, by (A-1), (A-2), (A-3), (A-4), and (A-5), one obtains

$$\begin{aligned}
A_0 &= m_0 \\
A_1 &= m_0 + m_1 + m_2 + m_3 + m_4 + m_5 + m_6 \\
A_2 &= m_0 + m_1 + m_7 + m_2 + m_4 + m_8 + m_5 \\
A_3 &= m_0 + m_1 + m_3 + m_7 + m_9 + m_{10} + m_{11} \\
A_4 &= m_0 + m_1 + m_3 + m_7 + m_4 + m_6 + m_8 \\
A_5 &= m_0 + m_1 + m_7 + m_2 + m_9 + m_{11} + m_{12} \\
A_6 &= m_0 + m_1 + m_2 + m_3 + m_9 + m_{12} + m_{10}
\end{aligned} \tag{A-6}$$

Thus, by (A-6), one observes that the number of multiplications needed to perform a 7-point transform over $GF(2^7)$ is 13, including the multiplications by unit $\gamma^0 = 1$.

Consider $N_i = 3^2$. Let γ be the 9th root of unity. Since 1, 2, 4, 5, 7, 8 are relatively prime to 9, the permutation σ is defined by

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

Rearranging the rows and columns of W defined in (17) in such a manner that the elements of matrix with indices relatively prime to 9 form a block, one has

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

Applying the permutation defined in (A-7) to the indices of the upper left 6×6 matrix of (A-8), 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 Theorem 1, the above matrix can be partitioned into a 2×2 block matrix of 3×3 cyclic blocks as

$$\begin{pmatrix} Y_2 \\ Y_5 \\ Y_8 \\ Y_7 \\ Y_4 \\ Y_1 \end{pmatrix} = \begin{pmatrix} \gamma^4 & \gamma^1 & \gamma^7 & \gamma^5 & \gamma^8 & \gamma^2 \\ \gamma^1 & \gamma^7 & \gamma^4 & \gamma^8 & \gamma^2 & \gamma^5 \\ \gamma^7 & \gamma^4 & \gamma^1 & \gamma^2 & \gamma^5 & \gamma^8 \\ \gamma^5 & \gamma^8 & \gamma^2 & \gamma^4 & \gamma^1 & \gamma^7 \\ \gamma^8 & \gamma^2 & \gamma^5 & \gamma^1 & \gamma^7 & \gamma^4 \\ \gamma^2 & \gamma^5 & \gamma^8 & \gamma^7 & \gamma^4 & \gamma^1 \end{pmatrix} \begin{pmatrix} a_2 \\ a_5 \\ a_8 \\ a_7 \\ a_4 \\ a_1 \end{pmatrix} \tag{A-9}$$

Now if one makes the correspondences, $\gamma^2 \leftrightarrow \gamma^4$, $\gamma^1 \leftrightarrow \gamma^1$, $\gamma^4 \leftrightarrow \gamma^7$, $\gamma^5 \leftrightarrow \gamma^5$, $\gamma^6 \leftrightarrow \gamma^8$, $\gamma^3 \leftrightarrow \gamma^2$, $B_3 \leftrightarrow Y_2$, $B_5 \leftrightarrow Y_5$, $B_6 \leftrightarrow Y_8$, $B_4 \leftrightarrow Y_7$, $B_2 \leftrightarrow Y_4$, $B_1 \leftrightarrow Y_1$, $a_3 \leftrightarrow a_2$, $a_5 \leftrightarrow a_5$, $a_6 \leftrightarrow a_8$, $a_4 \leftrightarrow a_7$, $a_2 \leftrightarrow a_4$, $a_1 \leftrightarrow a_1$ in (A-2), then by a procedure similar to that used to compute the matrix defined in (A-2), one obtains

$$
\begin{aligned}
Y_1 &= m_1 + m_2 + m_3 + m_4 + m_5 + m_6 \\
Y_4 &= m_1 + m_7 + m_2 + m_4 + m_8 + m_5 \\
Y_2 &= m_1 + m_3 + m_7 + m_9 + m_{10} + m_{11} \\
Y_7 &= m_1 + m_3 + m_7 + m_4 + m_6 + m_8 \\
Y_5 &= m_1 + m_7 + m_2 + m_9 + m_{11} + m_{12} \\
Y_8 &= m_1 + m_2 + m_3 + m_9 + m_{12} + m_{10}
\end{aligned}
$$

where

$$
\begin{aligned}
m_1 &= (\gamma^4 + \gamma^1 + \gamma^7) \cdot (a_2 + a_7 + a_5 + a_4 + a_8 + a_1) \\
m_2 &= (\gamma^4 + \gamma^1) \cdot (a_5 + a_4 + a_2 + a_7) \\
m_3 &= (\gamma^7 + \gamma^4) \cdot (a_8 + a_1 + a_5 + a_4) \\
m_4 &= 1 \cdot (a_2 + a_5 + a_8) \\
m_5 &= (\gamma^4 + \gamma^5 + \gamma^1 + \gamma^8) \cdot (a_5 + a_2) \\
m_6 &= (\gamma^7 + \gamma^2 + \gamma^4 + \gamma^5) \cdot (a_8 + a_5) \\
m_7 &= (\gamma^7 + \gamma^1) \cdot (a_8 + a_1 + a_2 + a_7) \\
m_8 &= (\gamma^7 + \gamma^2 + \gamma^1 + \gamma^8) \cdot (a_8 + a_2) \\
m_9 &= 1 \cdot (a_7 + a_4 + a_1) \\
m_{10} &= (\gamma^7 + \gamma^2 + \gamma^4 + \gamma^5) \cdot (a_1 + a_4) \\
m_{11} &= (\gamma^7 + \gamma^2 + \gamma^1 + \gamma^8) \cdot (a_1 + a_7) \\
m_{12} &= (\gamma^4 + \gamma^5 + \gamma^1 + \gamma^8) \cdot (a_4 + a_7)
\end{aligned}
\qquad \text{(A-10)}
$$

From (A-10), we know that the number of multiplications required to perform (32) is 10 excluding multiplications by γ^0

The last two columns of the matrix defined in (A-8) can be obtained by computing the following 2 X 2 cyclic matrix

$$\begin{pmatrix} X_1 \\ X_2 \end{pmatrix} = \begin{pmatrix} \gamma^3 & \gamma^6 \\ \gamma^6 & \gamma^3 \end{pmatrix} \begin{pmatrix} a_3 \\ a_6 \end{pmatrix} = \begin{pmatrix} \gamma^3 (a_3 + a_6) + (\gamma^3 + \gamma^6) a_6 \\ \gamma^3 (a_3 + a_6) + (\gamma^3 + \gamma^6) a_3 \end{pmatrix} \tag{A-11}$$

The last two rows of the matrix defined in (A-8) can be obtained by computing the following cyclic matrix

$$\begin{pmatrix} Z_1 \\ Z_2 \end{pmatrix} = \begin{pmatrix} \gamma^3 & \gamma^6 \\ \gamma^6 & \gamma^3 \end{pmatrix} \begin{pmatrix} a_1 + a_4 + a_7 \\ a_2 + a_5 + a_8 \end{pmatrix} \tag{A-12}$$

$$= \begin{pmatrix} \gamma^3 (a_1 + a_4 + a_7 + a_2 + a_5 + a_8) + (\gamma^3 + \gamma^6)(a_2 + a_5 + a_8) \\ \gamma^3 (a_1 + a_4 + a_7 + a_2 + a_5 + a_8) + (\gamma^3 + \gamma^6)(a_1 + a_4 + a_7) \end{pmatrix}$$

Note that the number of multiplications used to perform (A-11) or (A-12) is 3. Thus, the algorithm for computing the 9-point transform is

$$\begin{aligned}
b_0 &= 1 \cdot (a_0 + a_1 + a_2 + a_3 + a_4 + a_5 + a_6 + a_7 + a_8) \\
b_1 &= Y_1 + X_1 + 1 \cdot a_0 \\
b_2 &= Y_2 + X_2 + 1 \cdot a_0 \\
b_3 &= Z_1 + Z_2 + 1 \cdot a_3 + 1 \cdot a_6 + 1 \cdot a_0 \\
b_4 &= Y_4 + X_1 + 1 \cdot a_0 \\
b_5 &= Y_5 + X_2 + 1 \cdot a_0 \\
b_6 &= Z_2 + Z_1 + 1 \cdot a_3 + 1 \cdot a_6 + 1 \cdot a_0 \\
b_7 &= Y_7 + X_1 + 1 \cdot a_0 \\
b_8 &= Y_8 + X_2 + 1 \cdot a_0
\end{aligned} \tag{A-13}$$

From (A-13), the total number of multiplications needed to perform a 9-point transform is 16, excluding multiplications by the unit $\gamma^0 = 1$.

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.

References

1. R. R. Green, "Analysis of a Serial Orthogonal Decoder," *Space Programs Summary 37-53*, Vol. III, 1968, pp. 185-187.
2. I. S. Reed, "A Class of Multiple-Error-Correcting Codes and the Decoding Scheme," *IRE Trans.*, PGIT-4, 1954, pp. 38-49.
3. W. C. Gore, "Transmitting Binary Symbols with Reed-Solomon Code," Johns Hopkins EE Report No. 73-5, April 1973.
4. D. Mandelbaum, "On Decoding Reed-Solomon Codes," *IEEE Trans. on Inform. Theory*, Vol. IT-17, No. 6, pp. 707-712, November 1971.
5. A. Michelson, "A New Decoder for the Reed-Solomon Codes Using a Fast Transform Technique," Systems Engineering Technical Memorandum, No. 52, Electronic Systems Group Eastern Division GTE Sylvania, August 1975.
6. W. W. Peterson, "Error-Correcting Codes," MIT Press, Cambridge, Mass., 1961, pp. 168-169.
7. S. Lin, "An Introduction to Error-Correcting Codes," Englewood Cliffs, N. J., Prentice-Hall, 1970.
8. J. Odenwalder, et al., "Hybrid Coding Systems Study Final Report," Linkabit Corp., NASA CR 114,486, Sept. 1972.
9. S. Winograd, "On Computing the Discrete Fourier Transform," *Proc. Nat. Acad. Sci. USA*, 1976, 73, pp. 1005-1006.
10. S. Winograd, "On Computing the Discrete Fourier Transform," Research Report, Math. Science Dept., IBM Thomas J. Watson Research Center, Yorktown Heights, New York, 10592.
11. W. M. Gentleman, "Matrix Multiplication and Fast Fourier Transforms," *Bell System Technical Journal*, 1968, pp. 1099-1103.
12. I. S. Reed, T. K. Truong, and B. Benjauthrit, "Transform Decoding of Reed-Solomon Codes over $GF(2^{2^n})$ Using the Techniques of Winograd," Submitted to *IEEE Trans. on Inform Theory.*
13. E. R. Berlekamp, Algebraic Coding Theory, New York, McGraw Hall, 1968.
14. I. S. Reed and T. K. Truong, "Fast Mersenne Prime Transforms for Digital Filters," to be published in the Proceedings of IEEE.
15. I. S. Reed, R. A. Scholtz, T. K. Truong, and 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.*
16. G. D. Forney, "On Decoding BCH Codes," *IEEE Transactions on Information Theory*, IT-11, October 1965.

Table 1. The Complexity of Transform over $GF(2^n)$ for $n = 5, 6$

$N = 2^n - 1$	Factors $N_1 \cdot N_2 \ldots N_k$	No. Mult. of New algorithm	No. Mult. of Gentleman's algorithm $N(N_1 + N_2 + \cdots + N_k - k + 1)$
$2^5 - 1$	31	120	961
$2^6 - 1$	7-9	$13 \cdot 16 = 208$	$63(7 + 9 - 1) = 945$

Table 2. The Complexity of Decoding RS of $2^n - 1$ Points for n = 5, 6

N	Factors $N_1 \cdot N_2 \cdots N_k$	No. mult. of new algorithm	No. mult. of Gentleman's algorithm $2N(N_1 + N_2 + N_3 + \cdots - k + 1)$	No. mult. of the standard algorithm $(N - 1)(d - 1) + t^2$
31	31	$2 \times 120 = 240$	$2 \times 961 = 1922$	$30 \times 16 + 8^2 = 544$
63	7-9	$2 \times 208 = 416$	$2 \times 945 = 1890$	$62 \times 30 + 15^2 = 2085$