The Fast Decoding of Reed-Solomon Codes Using Fermat Theoretic Transforms and Continued Fractions

L. R. Welch and I. S. Reed
University of Southern California

T. K. Truong
TDA Engineering Office

It is shown that Reed–Solomon (RS) codes can be decoded by using a fast Fourier transform (FFT) algorithm over finite fields $GF(F_n)$, where F_n is a Fermat prime, and continued fractions. This new transform decoding method is simpler than the standard method for RS codes. The computing time of this new decoding algorithm in software can be faster than the standard decoding method, for RS codes.

I. Introduction

Recently, Gore (Ref. 1) proposed the usage of a finite field transform over $GF(q^n)$, where q is a prime number and n is an integer, for decoding RS codes. Michelson (Ref. 2) has implemented Mandelbaum's algorithm (Ref. 3) and showed that the decoder, using a transform over $GF(q^n)$, is faster than a more standard decoder (Ref. 4). The disadvantage of this transform method is that the code length is such that the most efficient FFT algorithms cannot be used to yield fast transform decoders.

Rader (Ref. 5) proposed transforms over rings of integers modulo Fermat numbers. Such transforms can be used to compute error-free convolutions of real integer sequences. Agarwal and Burrus (Ref. 6) extended Rader's Fermat number theoretic transform by using the generator $\alpha = \sqrt{2}$ for the transform rather than $\alpha = 2$. If $\sqrt{2}$ is the generator of the transform, the transform has an FFT algorithm which can be used to calculate transforms with as many as 2^{n+2} points of integer data. This transform was extended to residue classes of quadratic integers $I_{F_n}(\sqrt[2]{2})$, where $\sqrt{2}$ is a root of $x^2 - 2 = 0$, F_n is a Fermat number and I_{F_n} denotes the set of integers mod F_n (Ref. 7). McClellan (Ref. 8) has realized recently the hardware for the Fermat prime theoretic transforms. He showed that the arithmetic used to perform these transforms required only integer additions and circular shifts.

Recently, Justesen (Ref. 9) 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.

Recently, the authors (Ref. 10) extended the transform to the finite field of type $I_{F_n}(\sqrt[8]{2})$ (isomorphic to $GF(F_n)$), where $\sqrt[8]{2}$ is a root of the polynomial $P(x) = x^8 - 2$ over $GF(F_n)$, and I_{F_n} denotes the set of integers modulo F_n. Again the arithmetic used to perform this transform requires only integer additions, circular shifts, and a minimum number of integer multiplications by powers of $\sqrt[8]{2}$. An FFT over the finite field of type $I_{F_n}(\sqrt[8]{2})$ can be used to encode and decode RS codes of as many as 2^{n+4} symbols for $n = 3,4$. Encoding and decoding can be accomplished faster and more simply than any other known standard decoder for RS codes of the same symbol range. It was also shown (Ref. 10) that the FFT over $GF(K \cdot 2^n + 1)$, where K and n are integers, can be used to encode and decode a class of RS codes. A special case of the radix—8 FFT over $GF(q^2)$, where $q = 2^p - 1$ is a Mersenne prime, was developed to encode and decode another class of RS codes.

The decoding of systematic Reed-Solomon codes using the transform over $GF(F_n)$ was composed of the following three steps (Ref. 10).

(1) Compute the FFT over $GF(F_n)$ of the received code N-tuple; i.e.,

$$S_K = \sum_{m=0}^{N-1} \gamma_m \alpha^{mK}$$

where $\gamma_m \epsilon GF(F_n)$ and α is an element of order N.

(2) Use Berlekamp's iterative algorithm (Ref. 11) to determine σ_i from the known $S_j = E_j$ for $i = 1,2,\cdots,t$ and $j = 1,2,\cdots,2t$. Then compute the remaining transform error E_j.

(3) Compute the inverse of the transform over $GF(F_n)$ of $S_K - E_K$ to obtain the corrected code.

An advantage of this transform decoding algorithm over other methods is that a FFT over $GF(F_n)$ can be used to compute the syndromes and error magnitudes. In this paper, Berlekamp's iterative algorithm can be modified by using continued fractions in $GF(F_n)$. This modified Berlekamp's algorithm can be easily implemented on a digital computer.

II. New Approach to Decode Reed-Solomon Code Using the Transform Over GF(F_n)

In this section, a new approach is developed to define and decode RS codes. The following theorem and definitions are needed.

Theorem 1: Let q be a prime number. Also let $A(x)$ be the formal power series of form

$$A(x) = \sum_{i=0}^{\infty} a_i x^{d-i} \tag{1}$$

where $a_i \epsilon GF(q)$, the degree of $A(x)$,d, is a real integer, and $a_0 \neq 0$. Define the set

$$F = \left\{ \sum_{i=0}^{\infty} a_i x^{d-i} \Big|_{a_i \epsilon GF(q) \text{ and } d \text{ is an integer}} \right\}$$

such that addition is given by

$$G(x) = B(x) + C(x) = \sum_{i=0}^{\infty} b_i x^{e-i} + \sum_{i=0}^{\infty} c_i x^{f-i}, e \geq f$$

$$= \sum_{i=0}^{\infty} g_i x^{e-i}$$

where

$$g_i = \begin{cases} b_i, i < e - f \\ b_i + c_{i-(e-f)}, i \geq e - f \end{cases}$$

and multiplication is given by

$$H(x) = B(x) \cdot C(x) = \left(\sum_{i=0}^{\infty} b_i x^{e-i} \right) \left(\sum_{i=0}^{\infty} c_1 x^{f-i} \right)$$

$$= \sum_{i=0}^{\infty} h_i x^{e+f-i}$$

where

$$h_i = \sum_{j=0}^{i} b_j c_{i-j}$$

Then R is an infinite field.

Proof: It is evident that R satisfies the postulates of a commutative ring with unity element. An additive identity element and a multiplicative unit element in this ring are

$$D(x) = \sum_{i=0}^{\infty} d_i x^{d-i}, d_i = 0 \text{ for } i = 0,1,2,\cdots,\infty$$

and

$$F(x) = \sum_{i=0}^{\infty} f_i x^{d-i}, d = 0, f_0 = 1, f_j = 0 \; for \; j > 0$$

Every nonzero element of F, i.e.,

$$A(x) = \sum_{i=0}^{\infty} a_i x^{e-i}$$

has an inverse element $B(x)$ defined by

$$B(x) = A(x)^{-1} = \sum_{i=0}^{\infty} b_i x^{e-i}$$

where

$$b_0 = a_0^{-1}$$
$$b_i = a_0^{-1}\left(\sum_{j=1}^{i-1} a_j b_{i-j}\right) \text{ for } (i = 1,2,\cdots)$$

Hence F is a field.

If the set R is composed of all power series not containing negative powers of x, i.e.,

$$R = \left\{\sum_{i=0}^{d} a_i x^{d-i} \,\Big|_{a_i \epsilon GF(q),\, d \text{ is a positive integer}}\right\} \subset F \tag{2}$$

then it is evident that R is a subring of F. The integer part $[A(x)]$ of $A(x)$ in (1) is defined by

$$[A(x)] = \sum_{i=0}^{d} a_i x^{d-i}$$

Let $p(x)$ be the ratio of elements in R, i.e., a rational fraction form of type,

$$p(x) = \frac{\sum_{i=0}^{e} a_i x^{e-i}}{\sum_{i=0}^{f} b_i x^{f-i}}$$

where

$$\sum_{i=0}^{e} a_i x^{e-i}, \sum_{i=0}^{f} b_i x^{f-i} \epsilon R \subset F$$

By theorem 1, it can be proved that $p(x)$ is an element in the field F. An element in F of form $p(x)$ is called a rational element.

Let $GF(F_n)$ be the finite field, where $F_n = 2^{2^n} + 1$ is a Fermat prime for $n = 1,2,3,4$. It was shown in Ref. 10 that the field of type $I_{F_n}(\sqrt[8]{2})$ is isomorphic to $GF(F_n)$ for $n = 3,4$ and that $\alpha = \sqrt[8]{2} \epsilon GF(F_n)$ is an element of order 2^{n+4}. In these fields a systematic RS code can be specified in $GF(F_n)$ as follows:

Assume the code length for the RS code is $N = 2^{n+4}$. Let a code word be represented by $f(x)$, a polynomial of degree $N - 1$ over $GF(F_n)$. The generator polynomial of $g(x)$ is defined as

$$g(x) = \sum_{i=1}^{d-1} (x - \alpha^i)$$

where

$$d = 2^K < N = 2^{n+4}$$

and $\alpha = \sqrt[8]{2}, \alpha^2 = (\sqrt[8]{2})^2, \cdots, \alpha^d = (\sqrt[8]{2})^d$ are the roots of $g(x)$ in $GF(F_n)$. The resultant RS code with N symbols, which is a multiple of the generator polynomial, is composed of $d - 1$ parity check symbols and $N - (d - 1)$ information symbols, where d is the minimum distance of the RS code. If t is the number of errors, the code will correct, then $d = 2t + 1$.

Suppose that the code word $f(x) = f_0 + f_1 x + \cdots + f_{N-1}x^{N-1}$ is transmitted over a noisy channel. The received code word $R(x) = \gamma_0 + \gamma_1 x + \cdots + \gamma_{N-1}x^{N-1}$ is composed of the original code word with the addition of possible errors, i.e.,

$$\gamma(x) = f(x) + e(x)$$

where $e(x) = e_0 + e_1 x + e_2 x^2 + \cdots + e_{N-1}x^{N-1}$ is an error polynomial.

Upon receiving the message $\gamma(x)$, the first step in the decoding process is to take the FFT of the message in $I_{F_n}(\sqrt[8]{2})$. The transform is taken of the received N-tuple message $(\gamma_0, \gamma_1, \cdots, \gamma_{N-1})$, the coefficients of the polynomial $\gamma(x)$. This transform is

$$\begin{aligned} S_K &= \sum_{n=0}^{N-1} \gamma_n (\sqrt[8]{2})^{Kn} \\ &= \sum_{n=0}^{N-1} (f_n + e_n)(\sqrt[8]{2})^{Kn} \\ &= \sum_{n=0}^{N-1} f_n (\sqrt[8]{2})^{Kn} + \sum_{n=0}^{N-1} e_n (\sqrt[8]{2})^{Kn} \\ &= F_K + E_K \text{ for } K = 0,1,\cdots,N-1 \end{aligned}$$

Since $f(x)$ is a multiple of $g(x)$, $f(\alpha^i) = 0$ $i = 1,2,\cdots,d-1$.

Hence,

$$S_K = E_K = e(\sqrt[8]{2})^K = \sum_{n=0}^{N-1} e_n(\sqrt[8]{2})^{Kn}$$
$$= \sum_{n=0}^{N-1} e_n[(\sqrt[8]{2})^n]^K \text{ for } k = 1,2, \cdots ,d-1 \tag{3}$$

where $E_K \epsilon GF(F_n)$ is periodic with N. Let Y_i and X_i be the ith error magnitudes and the ith error location, respectively. Then the syndrome in (3) becomes

$$S_K = E_K = \sum_{i=1}^{t} Y_i X_i^K \text{ for } k = 1,2, \cdots ,d-1 \tag{4}$$

The generating function of the sequence (E_K) is defined as a formal power series. That is,

$$E(x) = E_1x^{-1} + E_2x^{-2} + E_3x^{-3} + \cdots = \sum_{K=1}^{\infty} E_K x^{-K} \tag{5}$$

where

$$E_K \epsilon GF(F_n)$$

Substituting (4) into (5), one gets

$$E(x) = \sum_{K=1}^{\infty} \sum_{i=1}^{t} Y_i X_i^K x^{-K}$$
$$= \sum_{i=1}^{t} Y_i \sum_{K=1}^{\infty} (X_i x^{-1})^K$$
$$= \sum_{i=1}^{t} Y_i \frac{X_i x^{-1}}{1 - X_i x^{-1}}$$

Thus

$$E(x) = E_1x^{-1} + E_2x^{-2} + E_3x^{-3} + \cdots$$
$$= \sum_{i=1}^{t} Y_i \frac{X_i}{x - X_i} = \frac{P(x)}{\sigma(x)} \tag{6}$$

where

$$P(x) \text{ and } \sigma(x) = \prod_{i=1}^{t} (x - X_i) \,\epsilon R$$

Note that $E(x)$ is a rational element in F. Since

$$\sigma(x) = x^t - \sigma_1 x^{t-1} + \sigma_2 x^{t-2} + \cdots + (-1)^t \sigma_t, \text{ then}$$

$$\sigma(X_i) = 0 = X_i^t - \sigma_1 X_i^{t-1} + \sigma_2 X_i^{t-2}$$
$$+ \cdots + (-1)^t \sigma_t, \text{ for } i = 1,2, \cdots, t$$

Multiplying the above equation by $Y_i X_i^j$, one gets,

$$Y_i X_i^{t+j} - \sigma_1 X_i^{j+t-1} + \sigma_2 Y_i X_i^{j+t-2} + \cdots + (-1)^t \sigma_t Y_i X_i^j$$

Summing on i for $i = 1,2, \cdots, t$, then

$$\sum_{i=1}^{t} Y_i X_i^{j+t} - \sigma_1 \sum_{i=1}^{t} Y_i X_i^{j+t-1} + \cdots + (-1)^t \sigma_t \sum_{i=1}^{t} Y_i X_i^j = 0$$

Using (4), we have,

$$S_{j+t} - \sigma_1 S_{j+t-1} + \cdots + (-1)^t \sigma_t S_j = 0, \qquad \text{for } j \leq t$$

and

$$E_{j+t} - \sigma_1 E_{j+t-1} + \cdots + (-1)^t \sigma_t E_j = 0 \qquad \text{for } j > t \tag{7}$$

It will be shown in the next section that $\sigma(x)$ in (6) can be calculated by using continued fraction approximations when only the first $2t$ coefficients of $E(x)$, i.e., $S_1, S_2, \cdots, S_{d-1}$ are known. If the coefficients of $\sigma(x)$, i.e., σ_i for $i = 1,2, \cdots, t$, are known, then Eq. (7) is used to obtain E_o, E_d, $E_{d+1}, \cdots, E_{N-1}$, and the transform of the N-tuple error pattern i.e., $(E_0, E_1, E_2, E_3, \cdots, E_{N-1})$ is obtained. Thus, the N-tuple error pattern $(e_0, e_1, \cdots, e_{N-1})$ is found by taking the inverse transform over I_{F_n} $(\sqrt[8]{2})$ of E_K for $k = 0, 1, \cdots, N-1$. Finally, the original N-tuple code word can be computed by subtracting e_n from the received code word r_n.

III. Implementing Berlekamp's Algorithm by Using Continued Fraction Approximations

It was shown in the previous section that $E(x) = P(x)/\sigma(x)$ in (6) is a rational element in the field of all formal power series F. Thus, using a procedure precisely similar to that used for rational elements in the real number field, described in Appendix A, it is possible to use continued fractions to develop a finite sequence of rational approximations to $E(x)$. That is, the recursive formula on convergents is given by,

$$E_x(x) = \frac{q_S(x) P_{S-1}(x) - P_{S-2}(x)}{q_S(x) \sigma_{S-1}(x) + \sigma_{S-2}(x)} = \frac{P_S(x)}{\sigma_S(x)} \tag{8}$$

where

$$P_1(x) = q_1(x), P_0(x) = 1, \sigma_0(x) = 0, \sigma_1(x) = 1.$$

The partial quotients $q_S(x)$ in (8) can be computed by the following formula recursively,

$$R_{S-2}(x) = q_S(x)R_{S-1}(x) + R_S(x) \tag{9}$$

where $R_{-1}(x) = E(x)$, $R_0(x) = 1$ and $q_S(x)$ is obtained as the "integer part" of $R_{S-2}(x)/R_{S-1}(x)$ and $R_S(x)$ is the "remainder"; and

$$(-1)^s R_S(x) = \sigma_S(x)E(x) = P_S(x) \tag{10}$$

where $\sigma_S(x)$ and $P_S(x)$ also satisfy the recursion in Eq. (9) with the initial values given in Eq. (8). By applying Euclid's algorithm to the rational element $E(x)$ in F, observe that $E(x) = P_S(x)/\sigma_S(x)$ will be terminated when $R_S(x) = 0$.

The norm of $A(x)\epsilon F$ will be used below in the proofs of theorem 2. This norm is defined as follows:

Definition

The norm of $A(x) = \sum_{i=0}^{\infty} a_i x^{d-i}$, $\|A(x)\|$, is defined by $\|A(x)\| = 2^d$

where d is a degree of $A(x)$

The properties of norm $\|A(x)\|$ are

a) $\|AB\| = \|A\| \cdot \|B\|$

b) $\|A\| > 0$ and $\|A\| = 0 \quad$ if $A = 0$

c) $\|A^{-1}\| = \dfrac{1}{\|A\|}$

d) $\|A \pm B\| \leq \max(\|A\|, \|B\|)$ if $\|A\| = \|B\|$ and $\|A \pm B\| = \max(\|A\|, \|B\|)$ if $\|A\| \neq \|B\|$

Lemma 1: Let n be the smallest finite integer such that $R_n(x) = 0$, where $R_S(x)$ is defined in (10); i.e., $E(x) = P_n(x)/\sigma_n(x)$. Then $\|R_S(x)\|$ is a monotone decreasing sequence for $s = 0,1,2,\cdots,n$ and $\|\sigma_S(x)\|$ is a monotone increasing sequence for $s = 0,1,2,\cdots,n$.

Proof:

By (9), one gets,

$$R_{S-2}(x) = q_S(x)R_{S-1}(x) + R_S(x)$$

where $\deg R_S(x) < R_{S-1}(x)$. This implies $\|R_S(x)\| < \|R_{S-1}(x)\|$ for $n = 1,2,\cdots,n$. Furthermore, since $\sigma_1(x) = 1$ and $\sigma_0(x) = 0$, then $\|\sigma_1(x)\| > \|\sigma_0(x)\|$. Assume $\|\sigma_{S-1}(x)\| > \|\sigma_{S-2}(x)\|$ for all $s \leq n$. By (8),

$$\sigma_S(x) = q_S(x)\sigma_{S-1}(x) + \sigma_{S-2}(x)$$

It follows from the norm properties that

$$\begin{aligned} \|\sigma_S(x)\| &= \|q_S(x)\sigma_{S-1}(x) + \sigma_{S-2}(x)\| \\ &= \|q_S(x)\sigma_{S-1}(x)\| = \|q_S(x)\|\|\sigma_{S-1}(x)\| \end{aligned} \tag{11}$$

But, by (9),

$$\begin{aligned} \|q_S(x)R_{S-1}(x)\| &= \|R_S(x) - R_{S-2}(x)\| \\ &= \|R_{S-2}(x)\| \end{aligned}$$

$$\|\mathrm{q_S}(x)\| = \frac{\|R_{S-2}(x)\|}{\|R_{S-1}(x)\|} > 1$$

Thus, (11) becomes

$$\|\sigma_S(x)\| > \|\sigma_{S-1}(x)\| \qquad \text{for } 1 \leq s \leq n.$$

To compute the norm of the difference $E(x) - P_S(x)/\sigma_S(x)$, we observe that

$$\left\| E(x) - \frac{P_S(x)}{\sigma_S(x)} \right\| = \frac{\|S(x)\sigma_S(x) - P_S(x)\|}{\|\sigma_S(x)\|} = \frac{\|R_S(x)\|}{\|\sigma_S(x)\|}$$

Then, by lemma 1,

$$\left\| E(x) - \frac{P_S(x)}{\sigma_S(x)} \right\| < \left\| E(x) - \frac{P_{S+1}(x)}{\sigma_{S+1}(x)} \right\|, \qquad \text{for } 0 \leq s \leq n-1 \tag{12}$$

For decoding RS codes over $GF(F_n)$, we only know the first $2t$ coefficients of $E(x)$ in (6). That is,

$$E(x) = E_1x^{-1} + E_2x^{-2} + \cdots E_{2t}x^{-2t} \underbrace{+ Xx^{-2t-1} + \cdots}_{X(x)}$$

where $X(x)$ is an unknown element in F. The following theorem is developed to recover the rational element $E(x)$ in F precisely when only the first $2t$ coefficients of $E(x)$ in (6) are known.

Theorem 2: Let $E(x) = P(x)/\sigma(x)$ in (6) be a rational element in F defined by theorem 1, where $P(x)$ and $\sigma(x)\epsilon R$ are defined in (2) and $\|E(x)\| < 1$. Let $X(x)$ be an unknown element in F such that $\deg X(x) < -2 \deg \sigma(x)$. If the first $\deg X(x) + 1$ coefficients of $E(x)$ are known, i.e.,

$$\begin{aligned} E(x) + X(x) = E_1x^{-1} + E_2x^{-2} + \cdots + E_{\deg X(x)+1}x^{\deg X(x)+1} \\ + Xx^{\deg X(x)} + \cdots \end{aligned}$$

where

$$X(x) = Xx^{\deg X(x)} + \cdots$$

Then $E(x)$ can be obtained by using the continued fraction algorithm operating on $E(x) + X(x)$.

Proof: By (10), we know that

$$\begin{aligned}(-1)^S R_S(x) &= \sigma_S(x)[E(x) + X(x)] - P_S(x) \\ &= (\sigma_S(x)E(x) - P_S(x)) + \sigma_S(x)X(x)\end{aligned}$$

where $\sigma_S(x)X(x)$ indicates the location of the unknown coefficients in $R_S(x)$.

We see that following the Euclidean division of $R_{S-2}(x)$ by $R_{S-1}(x)$, it follows immediately that $q_S(x)$, which is independent of $X(x)$, can be determined if and only if

$$\begin{aligned}\deg R_{S-1}(x) - \deg \sigma_{S-1}(x)X(x) > \deg R_{S-2}(x) \\ - \deg R_{S-1}(x) = \deg q_S(x) \text{ for } S \geq 2 \qquad (13)\end{aligned}$$

(Note that the left side of (13) indicates the number of known coefficients in the divisor and the right side of (13) indicates the degree of the partial quotient $q_S(x)$.) It follows from (13) that

$$2^{2 \deg R_{S-1}(x)} > 2^{\deg R_{S-2}(x) + \deg \sigma_{S-1}(x) X(x)}$$

By the properties of norm, (13) becomes

$$\| R_{S-1}(x) \|^2 > \| R_{S-2}(x) \| \, \| \sigma_{S-1}(x) \| \, \| X(x) \| \qquad (14)$$

But, by (11) in the proof of the lemma 1, one has,

$$\| \sigma_S(x) \| = \| q_S(x) \| \, \| \sigma_{S-1}(x) \| \qquad (15)$$

Since, by (9),

$$\| R_{S-2}(x) \| = \| q_S(x) R_{S-1}(x) + R_S(x) \| \qquad (16)$$

Then, by the lemma 1, (16) becomes

$$\| R_{S-2}(x) \| = \| q_S(x) R_{S-1}(x) \| = \| q_S(x) \| \cdot \| R_{S-1}(x) \| \qquad (17)$$

From (8), one gets

$$\| \sigma_1(x) \| = 1 \qquad (18)$$

and

$$\| R_0(x) \| = 1$$

Thus, from (15), (17), (18), we have

$$\| \sigma_{S-1}(x) \| = \| R_{S-2}(x) \|^{-1} \qquad (19)$$

Substituting (19) into (14), one obtains

$$\| R_{S-1}(x) \|^2 > \| X(x) \|$$

Hence $q_S(x)$, which is independent of $X(x)$, is obtained by the Euclidean division of $R_{S-2}(x)$ by $R_{S-1}(x)$ if and only if

$$\| R_{S-1}(x) \|^2 > \| X(x) \| \qquad (20)$$

Let $q_n(x)$ be the last partial quotients such that $q_n(x)$, which is independent of $X(x)$, can be determined by the Euclidean division algorithm. It follows from (20) that

$$\| R_n(x) \|^2 \leq \| X(x) \| \qquad (21)$$

By (19), (21) becomes

$$\| \sigma_{n+1}(x) \|^{-2} \leq \| X(x) \|$$

This implies

$$\| X(x) \|^{-1} \leq \| \sigma_{n+1}(x) \|^2 \qquad (22)$$

Since $\| \sigma(x) \|^2 < \| X(x) \|^{-1}$, thus (22) becomes,

$$\| \sigma(x) \|^2 < \| \sigma_{n+1}(x) \|^2 \qquad (23)$$

Consider either

$$\left\| E(x) - \frac{P_n(x)}{\sigma_n(x)} \right\| = \left\| E(x) - \frac{P(x)}{\sigma(x)} \right\|$$

or

$$\left\| E(x) - \frac{P_n(x)}{\sigma_n(x)} \right\| > \left\| E(x) - \frac{P(x)}{\sigma(x)} \right\|$$

If

$$\left\| E(x) - \frac{P_n(x)}{\sigma_n(x)} \right\| = \left\| E(x) - \frac{P(x)}{\sigma(x)} \right\| = 0$$

then

$$E(x) = \frac{P(x)}{\sigma(x)} = \frac{P_n(x)}{\sigma_n(x)}.$$

If

$$\left\|E(x) - \frac{P_n(x)}{\sigma_n(x)}\right\| > \left\|E(x) - \frac{P(x)}{\sigma(x)}\right\| = 0,$$

then

$$\left\|E(x) - \frac{P_n(x)}{\sigma_n(x)}\right\| = \left\|\left(E(x) - \frac{P_{n+1}(x)}{\sigma_{n+1}(x)}\right) + \left(\frac{P_{n+1}(x)}{\sigma_{n+1}(x)} - \frac{P_n(x)}{\sigma_n(x)}\right)\right\| \leq \max \left(\left\|E(x) - \frac{P_{n+1}(x)}{\sigma_{n+1}(x)}\right\|, \left\|\frac{P_{n+1}(x)}{\sigma_{n+1}(x)} - \frac{P_n(x)}{\sigma_n(x)}\right\|\right) \qquad (24)$$

By (12), (24) becomes either

$$\left\|E(x) - \frac{P_n(x)}{\sigma_n(x)}\right\| = \left\|E(x) - \frac{P_{n+1}(x)}{\sigma_{n+1}(x)}\right\|$$

or

$$\left\|E(x) - \frac{P_n(x)}{\sigma_n(x)}\right\| \leq \left\|\frac{P_{n+1}(x)}{\sigma_{n+1}(x)} - \frac{P_n(x)}{\sigma_n(x)}\right\|.$$

If

$$\left\|E(x) - \frac{P_n(x)}{\sigma_n(x)}\right\| = \left\|E(x) - \frac{P_{n+1}(x)}{\sigma_{n+1}(x)}\right\|,$$

this implies $R_n(x) = R_{n+1}(x) = 0$. If

$$\left\|E(x) - \frac{P_n(x)}{\sigma_n(x)}\right\| \leq \left\|\frac{P_{n+1}(x)}{\sigma_{n+1}(x)} - \frac{P_n(x)}{\sigma_n(x)}\right\| = \frac{\|P_{n+1}(x)\sigma_n(x) - \sigma_{n+1}(x)P_n(x)\|}{\|\sigma_{n+1}(x)\| \cdot \|\sigma_n(x)\|} \qquad (25)$$

By the same procedure used in the derivation of (A-10) in Appendix A, (25) becomes

$$\left\|\frac{P(x)}{\sigma(x)} - \frac{P_n(x)}{\sigma_n(x)}\right\| \leq \frac{1}{\|\sigma_{n+1}(x)\| \, \|\sigma_n(x)\|} \qquad (26)$$

Multiplying (26) by $\|\sigma(x)\| \, \|\sigma_n(x)\|$ gives

$$\|P(x)\sigma_n(x) - P_n(x)\sigma(x)\| \leq \frac{\|\sigma(x)\|}{\|\sigma_{n+1}(x)\|}$$

By (23), this yields,

$$\|P(x)\sigma_n(x) - P_n(x)\sigma(x)\| < 1,$$

which implies

$$\|P(x)\sigma_n(x) - P_n(x)\sigma(x)\| = 0$$

Then

$$\frac{P(x)}{\sigma(x)} = \frac{P_n(x)}{\sigma_n(x)}$$

Hence the theorem is proved.

A simple example of theorem 2 for decoding a RS code in $GF(F_n)$ is now presented.

Example: Let $GF(2^{2^2} + 1)$ be the field of integers modulo the Fermat prime $F_2 = 17$. We consider a 2-error correcting 8-tuple RS in $GF(17)$. (Note that this example is the same example in Ref. 10.)

Assume the information symbols are $1,2,3,2 \epsilon GF(17)$; i.e., $I(x) = 1x^7 + 2x^6 + 3x^5 + 2x^4$. By the example in (Ref. 10), the encoding of $I(x)$ is the polynomial

$$b(x) = 1x^7 + 2x^6 + 3x^5 + 2x^4 + 15x^3 + 12x^2 + 2x + 5$$

Suppose that two errors occur in the received words, i.e.,

$$\gamma(x) = 5 + 2x + 9x^2 + 15x^3 + 2x^4 + 1x^5 + 2x^6 + 1x^7$$

By the example in (Ref. 10), the syndrome can be calculated, using a FFT over $GF(F_n)$. That is,

$$S_K = E_K = \sum_{n=0}^{8-1} \gamma_n 2^{nK} \qquad \text{for } k = 1,2,3,4$$

Hence,

$$S_1 = E_1 = -8$$
$$S_2 = E_2 = -5$$
$$S_3 = E_3 = 11$$
$$S_4 = E_4 = -1$$

By (6)

$$E(x) = -8x^{-1} - 5x^{-2} + 11x^{-3} - x^{-4} \underbrace{+ Xx^{-5} + \cdots}_{X(x)} = \frac{P(x)}{\sigma(x)} \qquad (27)$$

where

$$\sigma(x) = \prod_{i=1}^{2} (x - x_i) = x^2 - \sigma_1 x + \sigma_2,$$

and X denotes the first unknown coefficient of $X(x)$. Since the deg $X(x) < \deg \sigma(x) = -2t = -4$ in (27) then, by Theorem 2, $\sigma(x)$ can be determined by the use of a continued fraction which is given below in tabular form.

S	$R_{S-2}(x) = q_S(x)R_{S-1}(x) + R_S(x)$	$q_S(x)$	$R_S(x)$	$\sigma_S(x) = q_S(x)\sigma_{S-1}(x)$ $+ \sigma_{S-2}(x)$
-1				1
0				0
1	0 $1 \overline{)\, -8x^{-1} - 5x^{-2} + 11x^{-3} - x^{-4} + Xx^{-5} + \cdots}$ $0x^{-1} + 0x^{-2} + 0x^{-3} + 0x^{-4} + \cdots$ $\overline{-8x^{-1} - 5x^{-2} + 11x^{-3} - x^{-4} + Xx^{-5} + \cdots}$	0	$-8x^{-1} - 5x^{-2} + 11x^{-3}$ $- x^{-4} + Xx^{-5} + \cdots$	$\sigma_1(x) = 0 \cdot 0 + 1 = 1$
2	$2x + 3$ $-8x^{-1} - 5x^{-2} \overline{)\, 1}$ $+ 11x^{-3} - x^{-4} \quad 1 - 10x^{-1} + 5x^{-2} - 2x^{-3} + Xx^{-4} + \cdots$ $+ Xx^{-5} + \cdots \quad \overline{10x^{-1} - 5x^{-2} + 2x^{-3} + Xx^{-4} + \cdots}$ $10x^{-1} - 15x^{-2} - x^{-3} + \cdots$ $\overline{10x^{-2} + 3x^{-3} + Xx^{-4} + \cdots}$	$2x + 3$	$10x^{-2} + x^{-3}$ $+ Xx^{-4} + \cdots$	$\sigma_2(x) = (2x + 3) \cdot 1 + 0$ $= 2x + 3$
3	$6x - 4$ $-7x^{-2} + 3x^{-3} \overline{)\, -8x^{-1} - 5x^{-2} + 11x^{-3} - x^{-4} + Xx^{-5} + \cdots}$ $+ Xx^{-4} + \cdots \quad -8x^{-1} + x^{-2} + Xx^{-3} + \cdots$ $\overline{-6x^{-2} + Xx^{-3} + \cdots}$ $-6x^{-2}$ $\overline{-0x^{-2} + Xx^{-3}}$	$6x - 4$	$0 + Xx^{-3} + \cdots$	$\sigma_3 = (6x - 4)(2x + 3)$ $+ 1$ $= x^2 - 2x + 9$

From the above tabular form, observe that $R_3 = 0 + Xx^{-3}$. Hence, $\sigma(x) = \sigma_3(x) = x^2 - 2x + 9$ where $\sigma_1 = 2$ and $\sigma_2 = 9$. By (7), one gets

$$E_{j+2} - 2E_{j+1} + 9E_j = 0 \qquad \text{for } j > 2 \qquad (28)$$

From (28), the rest of the transform E_j of the error pattern is $E_5 = 1$, $E_6 = 11$, $E_7 = 13$, $E_8 = E_0 = 12$. By example in Ref. 10, the inverse FFT over $GF(2^{2^2} + 1)$ of the E_j for $j = 0,1,\cdots,7$ is given by

$$(e_0,e_1,e_2,e_3,e_4,e_5,e_6,e_7) = (0,0,14,0,0,15,0,0)$$

The corrected code word is

$$b(x) = \gamma(x) - e(x) = (5,2,9,15,2,1,2,1)$$
$$- (0,0,14,0,0,15,0,0)$$
$$= (5,2,12,15,2,3,2,1)$$

Appendix

The Computation of Continued Fractions by Using Euclid's Algorithm

Let S be an irreducible rational element S in the field of real numbers. In this Appendix, it will be shown that a finite sequence of rational approximations to S can be constructed by using continued fractions.

Let $S = a/b$, where a and b are integers, be an irreducible rational element in the field of real numbers. Using Euclid's algorithm, one gets,

$$\begin{aligned}
a &= bq_1 + \gamma_1 \qquad \text{(A-1)}\\
b &= \gamma_1 q_2 + \gamma_2\\
\gamma_1 &= \gamma_2 q_3 + \gamma_3\\
&\vdots\\
\gamma_{k-2} &+ \gamma_{K-1} q_K + \gamma_K\\
&\vdots\\
\gamma_{n-3} &= \gamma_{n-2} q_{n-1} + \gamma_{n-1}\\
\gamma_{n-2} &= \gamma_{n-1} q_n + \gamma_n = \gamma_n q_n
\end{aligned}$$

or

$$\begin{aligned}
\frac{a}{b} &= q_1 + \frac{\gamma_1}{b}\\
\frac{b}{\gamma_2} &= q_2 + \frac{\gamma_2}{\gamma_1}\\
\frac{\gamma_1}{\gamma_2} &= q_3 + \frac{\gamma_3}{\gamma_2}\\
&\vdots\\
\frac{\gamma_{K-2}}{\gamma_{K-1}} &= q_K + \frac{\gamma_K}{\gamma_{K-1}}\\
&\vdots\\
\frac{\gamma_{n-3}}{\gamma_{n-2}} &= q_{n-1} + \frac{\gamma_{n-1}}{\gamma_{n-2}}\\
\frac{\gamma_{n-2}}{\gamma_{n-1}} &= q_n
\end{aligned}$$

By (A-1), $S = a/b$ can be developed by a continued fraction, as follows:

$$S = \frac{a}{b} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \ddots + \cfrac{1}{q_K + \alpha_K}}}, k < \mathrm{n} \qquad \text{(A-2)}$$

or

$$= q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \ddots + \cfrac{1}{q_n}}} \qquad \text{(A-3)}$$

where q_K for $k = 1,2,\cdots,n$ are called the partial quotients.

Let us define the convergents S_K for $k = 1,2,\cdots,n$ as follows

$$\begin{aligned}
S_1 &= q_1\\
S_2 &= q_1 + \frac{1}{q_2}\\
S_3 &= q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3}}\\
&\vdots\\
S_n &= \frac{a}{b} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \ddots + \cfrac{1}{q_n}}}
\end{aligned}$$

From (A-1), we observe that S_K is a finite sequence. In other words, S_1, S_2, $\cdots$, S_K, $\cdots$ will be terminated when $\gamma_n = 0$. Thus, $S_n = a/b$, where n is a finite number.

A recursive formula for convergents is generated as follows. Let $P_0 = 1$ and $Q_0 = 0$. Then set

$$S_1 = \frac{q_1}{1} = \frac{P_1}{Q_1}$$

$$S_2 = q_1 + \frac{1}{q_2} = \frac{q_2 q_1 + 1}{q_2 \cdot 1 + 0} = \frac{q_2 P_1 + P_0}{q_2 Q_1 + Q_0} = \frac{P_2}{Q_2}$$

$$S_3 = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3}} = \frac{\left(q_2 + \frac{1}{q_3}\right) P_1 + P_0}{\left(q_2 + \frac{1}{q_3}\right) Q_1 + Q_0}$$

$$= \frac{q_2 P_1 + P_0 \left(\frac{1}{q_3}\right) q_3}{(q_2 Q_1 + Q_0) + \frac{\mathrm{P}_1}{Q_1}} = \frac{q_3 P_2 + P_1}{q_3 Q_2 + Q_1} = \frac{P_3}{Q_3}$$

The recursive convergents are defined as

$$S_K = \frac{q_K P_{K-1} + P_{K-2}}{q_K Q_{K-1} + Q_{K-2}} = \frac{P_K}{Q_K} \qquad \text{(A-4)}$$

where $P_1 = q_1$, $P_0 = 1$, $Q_0 = 0$, $Q_1 = 1$, for $k = 2,3,\cdots,n$. (A-4)

In order to calculate Eq. (A-4), it is necessary to compute the partial quotients. To do this, by the same procedure used in the derivation of (A-4), we can show first that S in (A-2) can be expressed in the following form:

$$S = \frac{(q_K + \alpha_K)P_{K-1} + P_{K-2}}{(q_K + \alpha_K)Q_{K-1} + Q_{K-2}}, \text{ where } \alpha_K \text{ is defined in (A-2)}$$

If S has this form, then

$$(q_K + \alpha_K)(P_{K-1} - SQ_{K-1}) = S\,Q_{K-2} - P_{K-2}$$

and,

$$\frac{1}{\alpha_{K-1}} = q_K + \alpha_K = -\frac{P_{K-2} - Q_{K-2}S}{P_{K-1} - Q_{K-1}S} = -\frac{R'_{K-2}}{R'_{K-1}} \qquad \text{(A-5)}$$

where $R'_K = P_K - Q_K S$. It follows that

$$q_K R'_{K-1} + R'_{K-2} = -\alpha_K R_{K-1} = -\left(-\frac{R'_K}{R'_{K-1}}\right)\cdot R'_{K-1} = R'_K$$

Finally,

$$R'_K = q_K R'_{K-1} + R'_{K-2} \qquad \text{(A-6)}$$

By (5-A), the initial condition of R'_K for $K = 0,1$, is given by

$$R'_{-1} = P_{-1} - Q_{-1}S = -S$$

$$R'_0 = P_0 - Q_0 S = 1 - 0\cdot S = 1$$

Define a new function R_K in forms of R'_K by $R'_K = (-1)^K R_K$. Then (A-6) becomes

$$-(-1)^{K-2}R_{K-2} = q_K(-1)^{K-1}R_{K-1} - (-1)^K R_K$$

It is evident that

$$R_{K-2} = q_K R_{K-1} + R_K \text{ for both even and odd } k$$

Hence

$$R_{K-2} = q_K R_{K-1} + R_K \qquad \text{(A-7)}$$

with

$$R_{-1} = (-1)^{-1}R'_{-1} = S$$

$$R_0 = (-1)^0 R'_0 = 1$$

and by (A-5)

$$(-1)^K R_K = Q_K S = P_K \qquad \text{(A-8)}$$

To show that $S_K = (P_K/Q_K)$, which is computed by using a continued fraction, is an irreducible fraction, i.e., $(P_K,Q_K) = 1$, consider the difference between S_K and S_{K-1} for $K > 1$. That is,

$$S_K - S_{K-1} = \frac{P_K}{Q_K} - \frac{P_K}{Q_{K-1}} = \frac{P_K Q_{K-1} - Q_K P_{K-1}}{Q_K Q_{K-1}} \qquad \text{(A-9)}$$

Let $I_K = P_K Q_{K-1} - Q_K P_{K-1}$. By (A-4),

$$\begin{aligned} I_K = P_K Q_{K-1} - Q_K P_{K-1} &= (q_K P_{K-1} + P_{K-2})Q_{K-1} \\ &\quad - (q_K Q_{K-1} + Q_{K-2})P_{K-1} \\ &= -(P_{K-1}Q_{K-2} - Q_{K-1}P_{K-2}) \\ &= -I_{K-1} \qquad \text{(A-10)} \end{aligned}$$

Since $I_1 = P_1 Q_0 - Q_1 P_0 = q_1 \cdot 0 - 1 \cdot 1 = -1$, one has, by (A-10), $I_2 = -I_1 = 1$. With the above result, one has $I_K = (-1)^K$. It follows that

$$S_K - S_{K-1} = \frac{P_K}{Q_K} - \frac{P_{K-1}}{Q_{K-1}} = \frac{(-1)^K}{Q_K Q_{K-1}} \qquad \text{for } k > 1$$

or

$$P_K Q_{K-1} - Q_K P_{K-1} = (-1)^K \qquad \text{for } k > 1 \qquad \text{(A-11)}$$

If $(P_K,Q_K) = d_K$, then, by (A-11), $d_K | (-1)^K$. This implies that $d_K = 1$. Hence $(P_K,Q_K) = 1$.

A simple example, showing how to compute the rational approximations to an irreducible rational number, is presented in the following tabular form. For this example, S is the fraction 38/105.

s	$R_{S-2} = q_S R_{S-1} + R_S$	q_S	R_S	$P_S = q_S P_{S-1} + P_{S-2}$	$Q_S = q_S Q_{S-1} + Q_{S-2}$	$S_S = \dfrac{P_S}{Q_S}$
-1				0	1	
0				1	0	
1	$\dfrac{38}{105} = 0 \cdot 1 + \dfrac{38}{105}$	0	$\dfrac{38}{105}$	$P_1 = 0 \cdot 1 + 0 = 0 = q_1$	$Q_1 = 0 \cdot 0 + 1 = 1$	$S_1 = 1$
2	$1 = 2 \cdot \dfrac{38}{105} + \dfrac{29}{105}$	2	$\dfrac{29}{105}$	$P_2 = 2 \cdot 0 + 1 = 1$	$Q_2 = 2 \cdot 1 + 0 = 2$	$S_2 = \dfrac{1}{2}$
3	$\dfrac{38}{105} = 1 \cdot \dfrac{29}{105} + \dfrac{9}{105}$	1	$\dfrac{9}{105}$	$P_3 = 1 \cdot 1 + 0 = 1$	$Q_3 = 1 \cdot 2 + 1 = 3$	$S_3 = \dfrac{1}{3}$
4	$\dfrac{29}{105} = 3 \cdot \dfrac{9}{105} + \dfrac{2}{105}$	3	$\dfrac{2}{105}$	$P_4 = 3 \cdot 1 + 1 = 4$	$Q_4 = 3 \cdot 3 + 2 = 11$	$S_4 = \dfrac{4}{11}$
5	$\dfrac{9}{105} = 4 \cdot \dfrac{2}{105} + \dfrac{1}{105}$	4	$\dfrac{1}{105}$	$P_5 = 4 \cdot 4 + 1 = 17$	$Q_5 = 4 \cdot 11 + 3 = 47$	$S_5 = \dfrac{17}{47}$
6	$\dfrac{2}{105} = 2 \cdot \dfrac{1}{105} + 0$	2	0	$P_6 = 2 \cdot 17 + 4 = 38$	$Q_4 = 2 \cdot 47 + 11 = 105$	$S_6 = \dfrac{38}{105}$

From the tabular form when $s = n = 6$, one observes $R_6 = 0$. By (A-8),

$$S = S_6 = \frac{P_6}{Q_6} = \frac{38}{105}$$

For a more detailed discussion of the relation of Euclid's algorithm to the continued fraction associated with a rational element in the field of real numbers, see Ref. 12.

Acknowledgment

The authors wish to thank Mr. B. Mulhall and Dr. B. Benjauthrit of JPL for supporting and encouraging the research that led to this paper. The authors also wish to thank Prof. R. Scholtz of USC for many helpful suggestions and for providing his class notes on algebraic coding.

References

1. Gore, W. C., "Transmitting Binary Symbols with Reed–Solomon Code," Johns Hopkins EE Report No. 73-5, Apr. 1973.

2. Michelson, A., "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, Aug. 1975.

3. Mandelbaum, D., "On Decoding Reed–Solomon Codes," *IEEE Trans. Inform. Th.*, Vol. IT-17, No. 6, pp. 707-712, Nov. 1971.

4. Peterson, W. W., *Error-Correcting Codes*, MIT Press, Cambridge, Mass., 1961, pp. 168–169.

5. Rader, C. M., "Discrete Convolution Via Mersenne Transforms," *IEEE Trans. Comput.*, Vol. C-21, No. 12, Dec. 1972, pp. 1269–1273.

6. Agarwal, R. C., and Burrus, C. S., "Number Theoretic Transform to Implement Fast Digital Convolution," *Proc. IEEE*, Vol. 63, No. 4, Apr. 1975.

7. Reed, I. S., and Truong, T. K., "Convolutions over Residue Classes of Quadratic Integers," *IEEE Trans. Inform. Th.*, July 1976.

8. McClellan, J. H., "Hardware Realization of a Fermat Number Transform," *IEEE Trans. Acoustics, Speech, and Signal Processing*, Vol. Assp. 24, No. 3, June 1976, pp. 216–225.

9. Justesen, J., "On the Complexity of Decoding of Reed–Solomon Codes," *IEEE Trans. Inform. Th.*, Vol. IT-22, Mar. 1976, pp. 237–238.

10. Reed, I. S., Truong, T. K., and Welch, L. R., "The Fast Decoding of Reed–Solomon Codes Using Number Theoretic Transforms," to *The Deep Space Network Progress Report 42-35*, pp. 64–78, Jet Propulsion Laboratory, Pasadena, Calif., Oct. 15, 1976.

11. Berlekamp, E. R., *Algebraic Coding Theory*, McGraw-Hill, New York, 1968, Chapter 7.

12. Vinogrodov, I. M., *Elements of Number Theory*, Dover Publications, New York, 1954, Chapter 1.