Hindawi Publishing Corporation
EURASIP Journal on Wireless Communications and Networking
Volume 2011, Article ID 212136, 6 pages
doi:10.1155/2011/212136

Review Article

List Decoding of Generalized Reed-Solomon Codes by Using a Modified Extended Key Equation Algorithm

Ta-Hsiang Hu[1] and Ming-Hua Chang[2]

[1] *Department of Electrical Engineering, Da-Yeh University, 168 University Road, Dacun, Changhua 51591, Taiwan*
[2] *Department of Electronic Engineering, Jinwen University of Science and Technology, No. 99 An-Chung Road, Hsin-Tien, Taipei 23154, Taiwan*

Correspondence should be addressed to Ming-Hua Chang, mhchang@just.edu.tw

Received 27 October 2010; Revised 31 December 2010; Accepted 7 January 2011

Academic Editor: Kwan L. Yeung

This work presents a modified extended key equation algorithm in list decoding of generalized Reed-Solomon (GRS) codes. A list decoding algorithm of generalized Reed-Solomon codes has two steps, interpolation and factorization. The extended key equation algorithm (EKE) is an interpolation-based approach with a lower complexity than Sudan's algorithm. To increase the decoding speed, this work proposes a modified EKE algorithm to perform codeword checking prior to such an interpolation process. Since the evaluation mapping is engaged in encoding, a codeword is not generated systematically. Thus, the transmission information is not directly obtained from a received codeword. Therefore, the proposed algorithm undertakes a matrix operation to obtain the transmission information once a received vector has been checked to be error-free. Simulation results demonstrate that the modified EKE algorithm in list decoding of a GRS code provides low complexity, particularly at high signal-to-noise ratios.

1. Introduction

Reed-Solomon (RS) codes are currently used in a wide variety of applications, ranging from data storage systems, mobile communications, to satellite communications. The third-generation (3G) wireless standard utilizes RS codes as outer codes. For CDMA2000 high-rate broadcast packet data air interface [1], they are expected to be adopted as outer codes in concatenated coding schemes for future fourth-generation (4G) wireless systems.

Algorithms for hard decision decoding of RS codes are typically classified into two well-known types, namely, syndrome-based decoding and interpolation-based decoding. Well-developed algorithms in the first category include the Peterson-Gorenstein-Zierler algorithm [2], Berlekamp-Massey algorithm [2, 3], Euclidean algorithm [2, 3], frequency domain algorithm [2, 3], and step-by-step algorithm [4–7]. Algorithms in the second category include the Welch-Berlekamp algorithms [8, 9] and list decoding algorithms [10–12], as Koetter-Vardy algorithm [13] is also a list decoding algorithm but with soft decision approaching.

Sudan's algorithm [10] decodes GRS codes in two steps involved, namely, interpolation and factorization. An interpolation is performed on a received word $\overline{r} = (r_0, r_1, \ldots, r_{n-1})$, producing a nonzero bivariate polynomial $Q(x, y) = \sum_{t=0}^{l} Q^{(t)}(x)y^t = \sum_{i=0}^{n} a_i\phi(x, y)$ with at least $n - \tau$ points (α^i, r_i), such that $Q(\alpha^i, r_i) = 0$ and $i \in [n-1] = \{0, 1, \ldots, n-1\}$. Factorization is then performed on $Q(x, y)$, yielding linear factors (or called y-root polynomials) $y - f(x)$. The codewords are then generated from these distinct factors $f(x)$ via an evaluation mapping. A decoded codeword $\overline{c}^*$ is chosen if the Hamming distance between $\overline{c}^*$ and $\overline{r}$ is τ or less.

Because solving these interpolation equations of Sudan's algorithm with a naïve Gaussian elimination requires the time complexity $O(n^3)$, an EKE algorithm has been presented to decrease this complexity [12]. The EKE algorithm employs generalized Berlekamp-Massy algorithm (or the Feng-Tzeng algorithm in [14]) that obtains the shortest recurrence that generates a given sequence, and the time complexity of EKE to solve these interpolation equations is $O(l(n-k)^2)$. l represents a design parameter, typically a small constant, which is an upper bound on the size of the list of decoded codewords.

Guruswami and Sudan (GS) presented an improvement on Sudan's algorithm [11], by introducing a multiplicity u at each interpolation point. A nonzero $Q(x,y)$ polynomial exists that interpolates the points (x_i, y_i), $i \in [n-1]$ with multiplicity u, and is formed by $Q(x,y) = \sum_{i=0}^{c} a_i \phi(x,y)$, where $c = n\binom{u+1}{2}$, and the expression of $\binom{I}{J}$ denotes the number of ways to choose J from I. In comparison with Sudan's work, the GS algorithm provides more $n\binom{u+1}{2} - n$ linear homogeneous equations in interpolation, thus improving the decoding correction distance. Increasing u improves the decoding performance but also increases the required complexity. The asymptotical decoding correction fraction is given by $1-\sqrt{R}$, and the code rate R is given by $R = k/n$. The increase in decoding capability is substantial, especially for low-rate GRS codes.

Koetter and Vardy [13] extended the GS algorithm by incorporating the soft information received from a channel into the interpolation process. With a complexity that is a polynomial of the code length, the Koetter-Vardy (KV) algorithm can achieve a substantial coding gain over the GS algorithm. For instance, at a frame-error-rate (FER) of 10^{-5}, the KV algorithm can achieve a coding gain of about 1 dB over the GS algorithm, for a (255, 144) GRS code transmitted over an additive white Gaussian noise (AWGN) channel using 256-QAM modulation [13].

However, those approaches have a drawback, that is codeword checking is absent during decoding. In other words, regardless of whether the received sequence is correct or not, the decoding algorithm proceeds to decode it. This work overcomes this drawback by presenting a modified EKE algorithm with codeword checking. Additionally, a matrix operation is also proposed to obtain the transmission information from the received codeword. As in syndrome-based decoding, if the syndrome vector is all-zero, then the decoding process is terminated and the received sequence is output as a decoded codeword. The rest of this paper is organized as follows. Section 2 introduces the EKE algorithm. Section 3 then presents the modified EKE algorithm with the proposed codeword checking method and the matrix operation to obtain the transmission information from the received codeword. Finally, simulations and conclusions are presented in Section 4.

2. Extended Key Equation Algorithm

Consider an evaluation mapping $f(x) = m_0 + m_1 x + \cdots + m_{k-1}x^{k-1}$ and $n = 2^m - 1$. A codeword in an $[n,k]$ GRS code over GF(2^m) is generated as

$$\begin{aligned}\overline{c} &= (c_0, c_1, \ldots, c_{n-1})\\ &= \left(f(\alpha^0), f(\alpha), \ldots, f(\alpha^{n-1})\right)\\ &= (m_0, m_1, \ldots, m_{k-1})\begin{pmatrix}1 & 1 & \cdots & 1\\ 1 & \alpha & \cdots & \alpha^{n-1}\\ \vdots & \vdots & \cdots & \vdots\\ 1 & \alpha^{k-1} & \cdots & \alpha^{(n-1)(k-1)}\end{pmatrix}\\ &= \overline{m}\cdot\mathbf{G},\end{aligned} \tag{1}$$

where the information vector is $\overline{m} = (m_0, m_1, \ldots, m_{k-1})$, the generator matrix is

$$\mathbf{G} = \begin{pmatrix}1 & 1 & \cdots & 1\\ 1 & \alpha & \cdots & \alpha^{n-1}\\ \vdots & \cdots & \cdots & \vdots\\ 1 & \alpha^{k-1} & \cdots & \alpha^{(n-1)(k-1)}\end{pmatrix}, \tag{2}$$

and α is a primitive element in GF(2^m).

The term l is the upper bound of the number of consistent codewords, which are at Hamming distance $\leq \tau$ from any received word. For an (n,k) GRS code, Sudan's algorithm corrects any error pattern of up to τ errors for

$$\tau = n - (h+1) - l(k-1), \tag{3}$$

where h denotes the smallest nonnegative integer holding the following equation:

$$(h+1)(l+1) + (k-1)\binom{l+1}{2} > n. \tag{4}$$

Assuming that $k \leq (n+1)/3$, the value of τ becomes

$$\tau = \left\lfloor \frac{2(n+1)}{3} \right\rfloor - k. \tag{5}$$

Let F be a field, and let $F_k[x]$ represent the set of all polynomials of degree $< k$ in the variable x over F. Sudan's algorithm consists of the following steps.

(1) Find a nonzero bivariate polynomial $Q(x,y)$ over F with at least $n-\tau$ points (α^i, r_i), such that $Q(\alpha^i, r_i) = 0$ and $i \in [n-1]$, for a received vector $\overline{r} = (r_0, r_1, \ldots, r_{n-1})$.

(2) Output all polynomials $f(x) \in F_k[x]$ for which $y - f(x)$ is a factor of $Q(x,y)$ and $f(\alpha^i) = r_i$ for at least $n-\tau$ locators α^i.

In [2, 3], for an (n,k) RS code, the error-locator polynomial $\Lambda(x)$ and the error-evaluator polynomial $\Omega(x)$ are computed in the following key equation (KE):

$$\Lambda(x)\cdot S(x) \equiv \Omega(x) \quad \left(\operatorname{mod} x^{n-k}\right). \tag{6}$$

In [12], based on the linear factors of bivariate polynomials $Q(x,y)$ where the polynomial arithmetic is carried out modulo a power of x in Sudan's algorithm, an EKE algorithm is derived as follows:

$$\sum_{t=1}^{l} \Lambda^{(t)}(x)x^{(t-1)(k-1)} \cdot S^{(t)}(x) \equiv \Omega(x) \quad \left(\operatorname{mod} x^{n-k}\right), \tag{7}$$

where $\Lambda^{(t)}(x)$, $t \in \{1,2,\ldots,l\}$, and $\Omega(x)$ are polynomials that satisfy certain degree constraints and $S^{(t)}(x)$ are syndrome polynomials computed as follows:

$$S^{(t)}(x) = \sum_{i=0}^{n-2-t(k-1)} S_i^{(t)}x^i, \qquad S_i^{(t)} = \sum_{j=0}^{n-1} r_j^t \eta_j \alpha^{i\cdot j}, \tag{8}$$

$$\eta_j^{-1} = \prod_{\gamma\in[n-1]\setminus\{j\}} \left(\alpha^j - \alpha^\gamma\right). \tag{9}$$

Furthermore, the above equation can be obtained as follows:

$$\sum_{t=1}^{l}\sum_{s=0}^{N_t-1} Q_s^{(t)}S_{i+s}^{(t)} = 0, \qquad 0 \leq i < \tau, \tag{10}$$

which is denoted as

$$\begin{pmatrix} S_0^{(1)} & \cdots & S_{N_l-1}^{(1)} & S_0^{(2)} & \cdots & S_{N_l-1}^{(l)} \\ S_1^{(1)} & \cdots & S_{N_l}^{(1)} & S_1^{(2)} & \cdots & S_{N_l}^{(l)} \\ \vdots & & \vdots & \vdots & & \vdots \\ S_\tau^{(1)} & \cdots & S_{N_l+\tau-1}^{(1)} & S_\tau^{(2)} & \cdots & S_{N_l+\tau-1}^{(l)} \end{pmatrix} \cdot \begin{pmatrix} Q_0^{(1)} \\ \vdots \\ Q_{N_l-1}^{(1)} \\ Q_0^{(2)} \\ \vdots \\ Q_{N_l-1}^{(l)} \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}. \tag{11}$$

Let

$$Q^{(t)}(x) = \sum_{s=0}^{N_t-1} Q_s^{(t)}x^s, \tag{12}$$

where $N_t = n - \tau - t(k-1)$ and $t \in \{1,2,\ldots,l\}$. After these polynomials $Q^{(t)}(x)$, $t \in \{1,2,\ldots,l\}$, have been computed in (11) by using the Feng-Tzeng algorithms [14] or a similar algorithm mentioned in [12], the polynomial $Q^{(0)}(x)$ is obtained as follows:

$$Q^{(0)}(x) + \sum_{t=1}^{l} Q^{(t)}(x)y^t = Q(x,y) \tag{13}$$

and satisfies

$$Q^{(0)}\left(\alpha^j\right) = -\sum_{t=1}^{l} Q^{(t)}\left(\alpha^j\right)r_j^t, \quad j \in [n-1]. \tag{14}$$

A design parameter l in [12] is an upper bound on the size of the list of decoded codewords. For code rate $R \leq 1/3$, from (4), the value of l is determined by the following range:

$$\begin{aligned} &\frac{2n-2\tau-k+1-\sqrt{(2n-2\tau-k+1)^2-8\tau(k-1)}}{2(k-1)} < l \\ &\quad < \frac{2n-2\tau-k+1+\sqrt{(2n-2\tau-k+1)^2-8\tau(k-1)}}{2(k-1)}. \end{aligned} \tag{15}$$

The EKE algorithm employs the Feng-Tzeng algorithm [14] to decode GRS codes. The dimensions of the S-matrix in (11) are τ by $l(n-\tau-(k-1)(l+1)/2)$. Since the Feng-Tzeng algorithm is run column by column in a matrix, therefore the column length dominates the decoding complexity. Reducing the column length lowers the complexity of locating the smallest set of linear dependent coefficients. The algorithm of [12] requires the solving of τ homogeneous linear equations in (11) and then finding the corresponding coefficients of $Q^{(0)}(x)$ in (14). Hence, the time complexity is $O(l(n-k)^2)$, which is less than the time complexity of $O(n^3)$ of Sudan's algorithm. Consequently, the EKE algorithm is more attractive than the algorithm of [10].

3. Modified Extended Key Equation Algorithm

Since the polynomial $f(x) = \sum_{i=0}^{n-1} m_i x^i$ is associated with a codeword $\overline{c} \in C$, which has zeros $1, \alpha, \alpha^2, \ldots, \alpha^{n-k}$ [15], a parity-check matrix for C is given by [16, 17]

$$\mathbf{H} = \begin{pmatrix} 1 & \alpha & \cdots & \alpha^{n-1} \\ 1 & \alpha^2 & \cdots & \alpha^{2(n-1)} \\ \vdots & & \cdots & \vdots \\ 1 & \alpha^{n-k} & \cdots & \alpha^{(n-k)(n-1)} \end{pmatrix}. \tag{16}$$

Theorem 1. *For a received vector $\overline{r} = (r_0, r_1, \ldots, r_{n-1})$, codeword checking $\overline{w}$ is equal to the computation of $\overline{S}^{(1)}$, which is*

$$\begin{aligned} \overline{w} &= (w_0, w_1, \ldots, w_{n-k-1}) \\ &= \overline{r} \cdot \mathbf{H}^T \\ &= \overline{S}^{(1)}, \end{aligned} \tag{17}$$

where T denotes the matrix transpose.

Proof. For computing the value of η_j in (9), a different element $\gamma \in [n-1]\setminus\{j\}$ should yield a different result for $\alpha^j - \alpha^\gamma$. Consequently, the value of $\prod_{\gamma\in[n-1]\setminus\{j\}}(\alpha^j - \alpha^\gamma)$ can be simplified as

$$\begin{aligned} \prod_{\gamma\in[n-1]\setminus\{j\}} \left(\alpha^j - \alpha^\gamma\right) &= \frac{\prod_{s\in[n-1]\setminus\{j\}}\alpha^s}{\alpha^j} \\ &= \alpha^{n(n-1)/2-j} \\ &= \alpha^{-j}. \end{aligned} \tag{18}$$

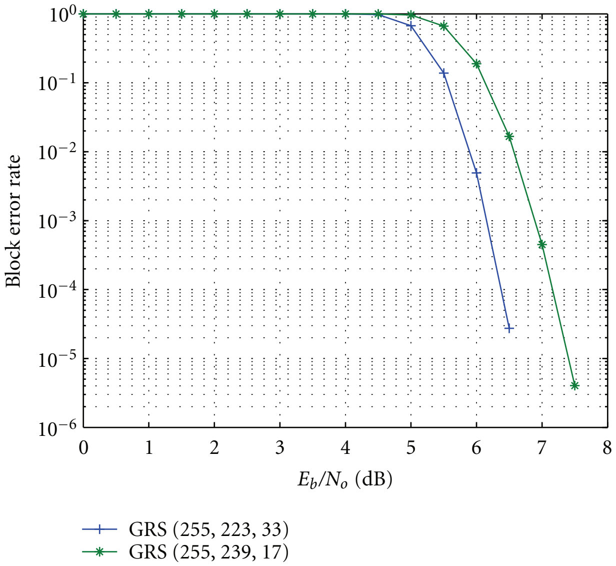

Figure 1: Performance of listing decoding with the modified EKE algorithm, when a (255, 233, 33) GRS code and a (255, 239, 17) GRS code are transmitted with BPSK signaling over AWQN channels.

Equation (9) becomes

$$\eta_j = \alpha^j. \tag{19}$$

For the vector $\overline{S}^{(1)} = (S_0^{(1)}, S_1^{(1)}, \ldots, S_{n-k-1}^{(1)})$, the calculation of each $S_i^{(1)}$ can be denoted as follows:

$$S_i^{(1)} = \sum_{j=0}^{n-1} r_j \alpha^{(i+1)\cdot j}, \tag{20}$$

and the vector $\overline{S}^{(1)}$ becomes

$$\begin{aligned}\overline{S}^{(1)} &= \left(S_0^{(1)}, S_1^{(1)}, \ldots, S_{n-k-1}^{(1)}\right)\\ &= (r_0, r_1, \ldots, r_{n-1}) \cdot \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \alpha & \alpha^2 & \cdots & \alpha^{n-k} \\ \vdots & \cdots & \vdots & \\ \alpha^{n-1} & \alpha^{2(n-1)} & \cdots & \alpha^{(n-k)(n-1)} \end{pmatrix}\\ &= \overline{r} \cdot \mathbf{H}^T.\end{aligned} \tag{21}$$

□

Theorem 2. *The codeword checking $\overline{w}$ is checked to be all-zero, and then the transmission message is given by*

$$\overline{m} = \overline{m}' \cdot \mathbf{M}, \tag{22}$$

where $\overline{m}'$ is the last k-tuple of $\overline{r}$ and $\mathbf{M}$ is a $k \times k$ matrix such that $\mathbf{G}' = \mathbf{M} \cdot \mathbf{G}$ is a systematical matrix.

Proof. The proof is quite trivial. In the expression of (1),

$$\begin{aligned}\overline{c} &= \overline{m} \cdot \mathbf{G}\\ &= \overline{m}\mathbf{M}^{-1} \cdot \mathbf{MG}\\ &= \overline{m}' \cdot \mathbf{G}'.\end{aligned} \tag{23}$$

Then,

$$\overline{m} = \overline{m}' \cdot \mathbf{M}. \tag{24}$$

□

Example 1. For a (7, 3) GRS code over GF(2^3) generated by the polynomial $p(X) = 1 + X + X^3$, a codeword $\overline{v} = (1, \alpha^6, \alpha^5, \alpha^5, 1, \alpha^3, \alpha^6)$ is given by the evaluation mapping provided as the transmission message $\overline{m} = (\alpha^3, \alpha^2, \alpha^4)$. If the codeword is transmitted over an error-free channel, then $\overline{S}^{(1)}$ is checked to be all-zero by (17) and the transmission message is computed by (22) as follows:

$$\begin{aligned}\overline{m} &= \overline{m}'\mathbf{M}\\ &= (1 \quad \alpha^3 \quad \alpha^6) \cdot \begin{pmatrix} \alpha & \alpha^5 & \alpha^4 \\ \alpha^2 & \alpha^2 & \alpha^6 \\ \alpha^5 & \alpha^3 & \alpha^3 \end{pmatrix}\\ &= (\alpha^3 \quad \alpha^2 \quad \alpha^4),\end{aligned} \tag{25}$$

where

$$\mathbf{M} = \begin{pmatrix} \alpha & \alpha^5 & \alpha^4 \\ \alpha^2 & \alpha^2 & \alpha^6 \\ \alpha^5 & \alpha^3 & \alpha^3 \end{pmatrix},$$

$$\mathbf{G} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha & \alpha^3 & \alpha^5 \end{pmatrix}, \tag{26}$$

$$\mathbf{G}' = \mathbf{M} \cdot \mathbf{G} = \begin{pmatrix} \alpha^3 & \alpha & 1 & \alpha^3 & 1 & 0 & 0 \\ \alpha^6 & \alpha^6 & 1 & \alpha^2 & 0 & 1 & 0 \\ \alpha^5 & \alpha^4 & 1 & \alpha^4 & 0 & 0 & 1 \end{pmatrix}.$$

With the above theorems, the list decoding algorithm [12] of an $[n, k]$ GRS code is adjusted as follows.

(1) Perform codeword-checking, $\overline{S}^{(1)} = \overline{r}\mathbf{H}^T$, for a received vector $\overline{r} = (r_0, r_1, \ldots, r_{n-1})$. If $\overline{S}^{(1)}$ is an all-zero vector, then output the corresponding message vector $\overline{m}$ determined as $\overline{m} = \overline{m}' \cdot \mathbf{M}$, where a vector $\overline{m}'$ is the last k-tuple of $\overline{r}$. Then, go to step 5.

(2) Perform the EKE interpolation:

(a) compute the syndrome polynomials in parallel: $S^{(t)}(x) = \sum_{i=0}^{n-2-t(k-1)} S_i^{(t)} x^i$ and $S_i^{(t)} = \sum_{j=0}^{n-1} r_j^t \alpha^{(i+1)j}$ and $t \in \{2, \ldots, l\}$,

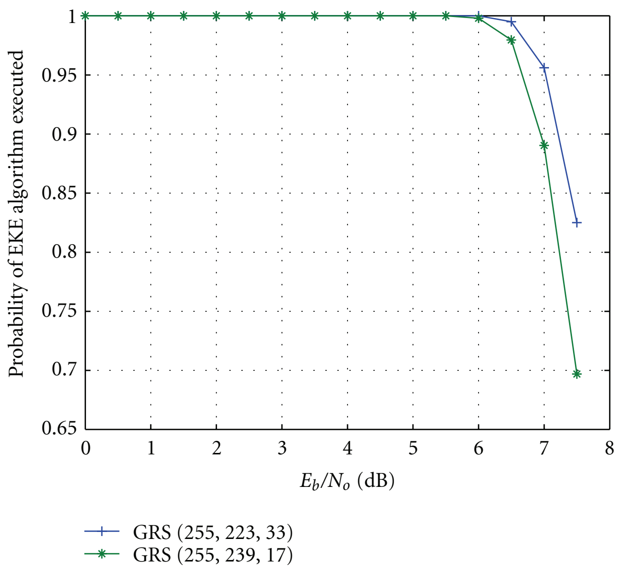

Figure 2: Probability of the EKE algorithm in listing decoding, when a (255, 233, 33) GRS code and a (255, 239, 17) GRS code are transmitted with BPSK signaling over AWQN channels.

(b) find polynomial polynomials $Q^{(t)}(x) = \sum_{s=0}^{N_t-1} Q_s^{(t)} x^s$, where $t \in \{1, \ldots, l\}$, by the Feng-Tzeng algorithm such that $\sum_{s=0}^{N_t-1} Q_s^{(t)} S_{i+s}^{(t)} = 0$, $0 \le i < \tau$,

(c) form the bivariate polynomial $Q(x, y) = \sum_{t=0}^{l} Q^{(t)}(x) y^t$, and then obtain the polynomial $Q^{(0)}(x)$ satisfying $Q^{(0)}(\alpha^j) = -\sum_{t=1}^{l} Q^{(t)}(\alpha^j) r_j^t$, $j \in [n-1]$.

(3) Perform the factorization on the bivariate polynomial $Q(x, y) = \sum_{t=0}^{l} Q^{(t)}(x) y^t$ by employing the reconstruction algorithm [12] to find the y-root polynomials $f(x) = m_0 + m_1 x + \cdots + m_{k-1} x^{k-1}$.

(4) Generate the corresponding codeword $\overline{c} = (f(1), f(\alpha), \ldots, f(\alpha^{n-1}))$ for each polynomial $f(x)$. Output the message vectors $\overline{m}^* = (m_0^*, m_1^*, \ldots, m_{k-1}^*)$ of the codewords $\overline{c}^*$ with the Hamming distance to $\overline{r}$ equal to τ or less.

(5) Terminate decoding

4. Simulations and Conclusions

Figure 1 displays the decoding performance of listing decoding [12] with the modified EKE algorithm as a (255, 223, 33) GRS code and a (255, 239, 17) GRS code are transmitted with BPSK signaling over AWGN channels. Figure 2 illustrates the probability of the EKE algorithm being executed in such a listing decoding. Those simulations demonstrate that codeword checking has little effect on decoding at low signal-to-noise ratios. However, the modified EKE algorithm provides lower decoding complexity when the signal-to-noise is high. At a block error rate (BER) of 10^{-5}, the probabilities of the EKE algorithm being utilized in list decoding of these two GRS codes are 0.98 and 0.75, respectively. This work presents a modified EKE algorithm, incorporating codeword checking and a matrix operation, which obtains the transmission information from the received codeword. The computation of codeword checking does not increase the complexity of the original EKE algorithm, because it is an item in the original decoding process. The proposed EKE algorithm is beneficial when the signal-to-noise ratio is high.

Acknowledgment

The authors would like to thank the National Science Council of the Republic of China, Taiwan, for financially supporting this research under Contract no. NSC 97-2221-E-212-005.

References

[1] P. Agashe, R. Rezaiifar, and P. Bender, “CDMA2000 high rate broadcast packet data air interface design,” *IEEE Communications Magazine*, vol. 42, no. 2, pp. 83–90, 2004.

[2] S. B. Wicker, *Error Control Systems for Digital Communication and Storage*, Prentice Hall, New York, NY, USA, 1995.

[3] S. Lin and D. J. Costello Jr., *Error Control Coding*, Prentice Hall, New York, NY, USA, 2nd edition, 2004.

[4] W. W. Peterson and E. J. Weldon, *Error-Control Codes*, MIT Press, Cambridge, Mass, USA, 2nd edition, 1972.

[5] J. L. Massy, “Step-by-step decoding of Bose-Chauhuri-Hocquenghem codes,” *IEEE Transactions on Information Theory*, vol. 11, no. 4, pp. 580–585, 1965.

[6] S. W. Wei and C. H. Wei, “High-speed decoder of Reed-Solomon codes,” *IEEE Transactions on Communications*, vol. 41, no. 11, pp. 1588–1593, 1993.

[7] T. C. Chen, C. H. Wei, and S. W. Wei, “Step-by-step decoding algorithm for Reed-Solomon codes,” *IEE Proceedings Communications*, vol. 147, no. 1, pp. 8–12, 2000.

[8] L. Welch and E. R. Berlekamp, “Error correction for algebraic block codes,” U.S. Patent 4 633 470, 1983.

[9] S. V. Fedorenko, “A simple algorithm for decoding Reed-Solomon codes and its relation to the Welch-Berlekamp algorithm,” *IEEE Transactions on Information Theory*, vol. 51, no. 3, pp. 1196–1198, 2005.

[10] M. Sudan, “Decoding of Reed Solomon codes beyond the error-correction bound,” *Journal of Complexity*, vol. 13, no. 1, pp. 180–193, 1997.

[11] V. Guruswami and M. Sudan, “Improved decoding of reed-solomon and algebraic-geometry codes,” *IEEE Transactions on Information Theory*, vol. 45, no. 6, pp. 1757–1767, 1999.

[12] R. M. Roth and G. Ruckenstein, “Efficient decoding of Reed-Solomon codes beyond half the minimum distance,” *IEEE Transactions on Information Theory*, vol. 46, no. 1, pp. 246–257, 2000.

[13] R. Koetter and A. Vardy, “Algebraic soft-decision decoding of Reed-Solomon codes,” *IEEE Transactions on Information Theory*, vol. 49, no. 11, pp. 2809–2825, 2003.

[14] G. L. Feng and K. K. Tzeng, “A generalization of the Berlekamp-Massey algorithm for multisequence shift-register synthesis with applications to decoding cyclic codes,” *IEEE Transactions on Information Theory*, vol. 37, no. 5, pp. 1274–1287, 1991.

[15] F. J. MacWilliams and N. J. Sloane, *The Theory of Error Correcting Codes*, North Holland, Amsterdam, The Netherlands, 1977.

[16] R. J. McEliece, *The Theory of Information and Coding*, Cambridge University Press, Cambridge, UK, 2nd edition, 2002.

[17] R. Pellikaan and X. W. Wu, "List decoding of q-ary Reed-Muller codes," *IEEE Transactions on Information Theory*, vol. 50, no. 4, pp. 679–682, 2004.