A note on alternant and BCH codes

A.A. Andrade and J.C. Interlando*, R. Palazzo Jr.†

Abstract - Alternant codes over arbitrary finite commutative local rings with identity are constructed in terms of parity-check matrices. The derivation is based on the factorization of $x^s - 1$ over the unit group of an appropriate extension of the finite ring. An efficient decoding procedure which makes use of the modified Berlekamp-Massey algorithm to correct errors is presented. Furtermore, we address the construction of BCH codes over $\mathbb{Z}_m$ under Lee metric.

1 Introduction

Alternant codes form a large and powerful family of codes. They can be obtained by a simple modification of the parity-check matrix of a BCH code. The most famous subclasses of alternant codes are BCH codes and (classical) Goppa codes, the former for their simple and easily instrumented decoding algorithm, and the latter for meeting the Gilbert-Varshamov bound. However, most of the work regarding construction and decoding of alternant codes has been done considering codes over finite fields. On the other hand, linear codes over integer rings have recently generated a great deal of interest because of their new role in algebraic coding theory and their successful application in combined coding and modulation. A remarkable paper by Hammons et al. [1] has shown that certain binary nonlinear codes with good error correcting capabilities can be viewed through a Gray mapping as linear codes over $\mathbb{Z}_4$. Moreover, Calderbank et al. [2] studied cyclic codes over $\mathbb{Z}_4$. Viewing many BCM (block coded modulation) schemes as group block codes over groups, in [3] it was shown that group block codes over abelian groups can be studied via linear codes over finite rings. Andrade and Palazzo [4] constructed BCH codes over finite commutative rings with identity. Also, Greferath and Vellbinger [5] have investigated codes over integer residue rings under the aspect of decoding. The Lee metric [6], [7] was developed as an alternative to the Hamming metric for transmission of nonbinary signals over certain noisy channels. Roth and Siegel [8] have constructed and decoded BCH codes over $GF(p)$ under Lee metric.

In this work we address the problems of constructing and decoding alternant codes over arbitrary finite commutative local rings with identity and the problems of construction BCH codes for the Lee metric. The core of the construction technique mimics that of alternant and BCH codes over a finite field, and is based on the factorization of $x^s - 1$ over an appropriate extension ring. Thus, this work is organized as follows. In Section 2, we describe a construction of alternant codes over a finite commutative local ring with identity, using the Galois theory of commutative rings [10], and using the modified Berlekamp-Massey algorithm

*Department of Mathematics - Ibilce - Unesp, 15054-000 - São José do Rio Preto - SP, Brazil, e-mail: andrade@mat.ibilce.unesp.br, carmelo@mat.ibilce.unesnp.br

†Department of Telematics, Feec - Unicamp, P.O. Box 6101,13081-970 Campinas - SP, Brazil, e-mail: palazzo@dt.fee.unicamp.br

an efficient decoding procedure is proposed. An example of the decoding method is given. In Section 3, we describe a construction of BCH codes over $\mathbb{Z}_q$, where q is a prime power, under Lee metric. The question of the existence of a simple decoding algorithm for these codes remains open.

2 Alternant Code

In this section we present a construction technique of alternant codes over finite commutative local rings with identity, in terms of parity-check matrices. First we collect basic definitions and facts from the Galois theory of commutative rings, those necessary to characterize such matrices. Throughout this section we assume that $\mathcal{A}$ is a finite commutative local ring with identity with maximal ideal $\mathcal{M}$ and residue field $\mathbb{K} = \frac{\mathcal{A}}{\mathcal{M}} \cong GF(p^m)$, where m is a positive integer and p is a prime. Let $f(x)$ be a monic polynomial of degree h in $\mathcal{A}[x]$, such that $\mu(f(x))$ is irreducible in $\mathbb{K}[x]$, where μ is the natural projection. Then by [10, Theorem XIII.7(a)], we have $f(x)$ also irreducible in $\mathcal{A}[x]$. Let $\mathcal{R}$ be the ring $\mathcal{A}[x]/\langle f(x)\rangle$. Then $\mathcal{R}$ is a finite commutative local ring with identity and is called a Galois extension of $\mathcal{A}$ of degree h. Its residue field is $\mathbb{K}_1 = \mathcal{R}/\overline{\mathcal{M}_1} \cong GF(p^{mh})$, where $\overline{\mathcal{M}_1}$ is the maximal ideal.

Let $\mathcal{R}^*$ denote the multiplicative group of units of $\mathcal{R}$. It follows that $\mathcal{R}^*$ is an abelian group, and therefore it can be expressed as a direct product of cyclic groups. We are interested in the maximal cyclic group of $\mathcal{R}^*$, hereafter denoted by $\mathcal{G}_s$, whose elements are the roots of $x^s - 1$ for some positive integer s such that $\gcd(s,p) = 1$. From [10, Theorem XVIII.2], there is only one maximal cyclic subgroup of $\mathcal{R}^*$ having order relatively prime to p. This cyclic group has order $s = p^{mh} - 1$.

Definition 2.1 Let $\boldsymbol{\eta} = (\alpha_1, \alpha_2, \cdots, \alpha_n)$ be the *locator vector*, consisting of distinct elements of $\mathcal{G}_s$, and let $\boldsymbol{w} = (w_1, w_2, \cdots, w_n)$ be an arbitrary vector consisting of elements of $\mathcal{G}_s$. Now define matrix H as

$$H = \begin{bmatrix} w_1 & w_2 & \cdots & w_n \\ w_1\alpha_1 & w_2\alpha_2 & \cdots & w_n\alpha_n \\ w_1\alpha_1^2 & w_2\alpha_2^2 & \cdots & w_n\alpha_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ w_1\alpha_1^{r-1} & w_2\alpha_2^{r-1} & \cdots & w_n\alpha_n^{r-1} \end{bmatrix},$$

where r is a positive integer. Then H is the parity-check matrix of a *shortened alternant code* $\mathcal{C}(n, \boldsymbol{\eta}, \boldsymbol{w})$ of length $n \leq s$ over $\mathcal{A}$.

It is possible to obtain an estimate of the minimum Hamming distance d of $\mathcal{C}(n, \boldsymbol{\eta}, \boldsymbol{w})$ directly from the parity-check matrix. The next theorem provides such an estimate.

Lemma 2.1 *Let α be an element of $\mathcal{G}_s$ of order s. Then the difference $\alpha^{l_1} - \alpha^{l_2}$ is a unit in $\mathcal{R}$ if $0 \leq l_1 < l_2 \leq s - 1$.*

Theorem 2.1 *$\mathcal{C}(n, \boldsymbol{\eta}, \boldsymbol{w})$ has minimum Hamming distance $d \geq r + 1$.*

Example 2.1 The polynomial $f(x) = x^3 + x + 1$ is irreducible over $\mathbb{Z}_2$, and over the commutative local ring $\mathcal{A} = \mathbb{Z}_2[i]$, where $i^2 = -1$. Thus $\mathcal{R} = \frac{\mathcal{A}[x]}{\langle f(x)\rangle}$ is a Galois extension of $\mathcal{A}$. Let α be a root of $f(x)$. We have that α generates a cyclic group $\mathcal{G}_s$ of order $s = 2^3 - 1 = 7$ in $\mathcal{R}^*$. Letting $\boldsymbol{\eta} = (1, \alpha, \cdots, \alpha^6)$ and $\boldsymbol{w} = (1,1,1,1,1,1,1)$, then if $r = 2$, we have an alternant code $\mathcal{C}(7, \boldsymbol{\eta}, \boldsymbol{w})$ over $\mathbb{Z}_2[i]$ with minimum Hamming distance of at least 3.

2.1 Decoding Procedure

This section is devoted to developing a decoding method for an alternant code as defined in the previous section. Let $\mathcal{C}(n, \boldsymbol{\eta}, \boldsymbol{w})$ be an alternant code with minimum Hamming distance at least $r+1$, i.e., this code can correct up to $t = [(r+1)/2]$ errors, where $[n]$ denotes the largest integer less than or equal to n. Then $t = (r+1)/2$ when r is odd, and $t = r/2$ when r is even. The idea is to extend efficient standard decoding procedures for BCH codes which work well over fields (as described, for example, in [11], [12], [13], and [14]) to finite commutative local rings with identity. Note that these afore mentioned decoding procedures do not work over rings, in general. As an example, the original Berlekamp-Massey algorithm [11], [15], which is fundamental in the decoding process of a BCH code, cannot be applied directly if the elements of the sequence to be generated do not lie in a field.

First, we establish some notation. Let $\mathcal{R}$ denote the ring defined in Section 2 and α be a primitive element of $\mathcal{G}_s$. Let $\boldsymbol{c} = (c_1, c_2, \cdots, c_n)$ be the transmitted codeword and $\boldsymbol{r} = (r_1, r_2, \cdots, r_n)$ be the received vector. The error vector is given by $\boldsymbol{e} = (e_1, e_2, \cdots, e_n) = \boldsymbol{r} - \boldsymbol{c}$. Given a locator vector $\boldsymbol{\eta} = (\alpha_1, \cdots, \alpha_n) = (\alpha^{k_1}, \cdots, \alpha^{k_n})$ in $\mathcal{G}_s^n$, we define the *syndrome values* $s_\ell \in \mathcal{G}_s$, of an error vector $\boldsymbol{e} = (e_1, \cdots, e_n)$, as $s_\ell = \sum_{j=1}^{n} e_j w_j \alpha_j^\ell, \quad \ell \geq 0$. Suppose that $\nu \leq t$ is the number of errors which occurred at locations $x_1 = \alpha_{i_1}, \cdots, x_\nu = \alpha_{i_\nu}$, with values $y_1 = e_{i_1}, \cdots, y_\nu = e_{i_\nu}$. Since $\boldsymbol{s} = \boldsymbol{r}H^T = \boldsymbol{e}H^T$, where $\boldsymbol{s} = (s_0, \cdots, s_{r-1})$, the first r syndrome values s_ℓ can be calculated from the received vector $\boldsymbol{r}$ as $s_\ell = \sum_{j=1}^{n} e_j w_j \alpha_j^\ell = \sum_{j=1}^{n} r_j w_j \alpha_j^\ell, \quad \ell = 0, 1, \cdots, r-1$. The elementary symmetric functions $\sigma_1, \sigma_2, \cdots, \sigma_\nu$ of the error-location numbers $x_1, x_2, \cdots, x_\nu$ are defined as the coefficients of the polynomial $\prod_{i=1}^{\nu}(x - x_i) = \sum_{i=0}^{\nu} \sigma_i x^{\nu-i}$, where $\sigma_0 = 1$. Thus, the decoding procedure being proposed consists of four major steps [4]:

Step 1 - Calculation of the syndrome vector from the received vector;

Step 2 - Calculation of the elementary symmetric functions $\sigma_1, \sigma_2, \cdots, \sigma_\nu$ from $\boldsymbol{s}$;

Step 3 - Calculation of the error-location numbers $x_1, x_2, \cdots, x_\nu$ from $\sigma_1, \sigma_2, \cdots, \sigma_\nu$;

Step 4 - Calculation of the error magnitude $y_1, y_2, \cdots, y_\nu$ from x_i and $\boldsymbol{s}$.

In *Step* 4, the calculation of the error magnitude is based on Forney's procedure [12]. The error magnitude $y_1, y_2, \cdots, y_\nu$ are given by

$$y_j = \frac{\sum_{\ell=0}^{\nu-1} \sigma_{j\ell} s_{\nu-1-\ell}}{E_j \sum_{l=0}^{\nu-1} \sigma_{j\ell} x_j^{\nu-1-\ell}}, \qquad j = 1, 2, \cdots, \nu, \quad (1)$$

where the coefficients $\sigma_{j\ell}$ are recursively defined by $\sigma_{j,i} = \sigma_i + x_j \sigma_{j,i-1}, \quad i = 0, 1, \cdots, \nu-1$, starting with $\sigma_{j,0} = \sigma_0 = 1$. The $E_j = w_{i_j}, \quad j = 1, 2, \cdots, \nu$ are the corresponding location of errors in the vector $\boldsymbol{w}$. Again making use of Lemma 2.1, it can be shown that the denominator in Eq. (1) is always a unit in $\mathcal{R}$.

Example 2.2 Let $\mathcal{G}_7$ be the cyclic group as in Example 2.1. Considering $\boldsymbol{\eta} = (\alpha^5, \alpha, \alpha^4, \alpha^2) = (\alpha^{k_1}, \cdots, \alpha^{k_4})$, $\boldsymbol{w} = (\alpha^4, \alpha, \alpha^4, \alpha)$ and $r = 2$, we have an alternant code over $\mathbb{Z}_2[i]$ of length 4 and minimum Hamming distance of at least 3. Let H be the parity-check matrix. Assume that the all-zero codeword $\boldsymbol{c} = (0, 0, 0, 0)$ is transmitted, and the vector $\boldsymbol{r} = (0, 0, i, 0)$ is received. Then the syndrome vector is $\boldsymbol{s} = \boldsymbol{r}H^T = (i\alpha^4, i\alpha)$. By the modified Berlekamp-Massey algorithm we obtain

$\sigma^{(2)}(z) = 1 + \alpha^4 z$. The root of $\rho(z) = z + \alpha^4$ (the reciprocal of $\sigma^{(2)}(z)$) is $z_1 = \alpha^4$. Among the elements $\alpha^0, \cdots, \alpha^6$, we have that $x_1 = \alpha^4$ satisfies $x_1 - z_1 = 0$ (zero divisor in $\mathcal{R}$). Therefore, x_1 is the correct error-location number since $k_3 = 4$ indicates that one error has occurred in the third coordinate of the codeword. The correct elementary symmetric function $\sigma_1 = \alpha^4$ is obtained from $x - x_1 = x - \sigma_1 = x - \alpha^4$. Finally, applying Forney's method to $\boldsymbol{s}$ and σ_1, gives $y_1 = i$. Therefore, the error pattern is $\boldsymbol{e} = (0, 0, i, 0)$.

3 BCH code

In this section we present a construction technique of BCH codes over commutative ring of integers modulo q, where q is a prime power, in terms of parity-check matrices under Lee metric. First we collect basic definitions and facts from Lee metric over $\mathbb{Z}_m$, where m is a positive integer.

Definition 3.1 *Let $\mathbb{Z}_m$ denote the commutative ring of integers modulo m, where m is a positive integer.*

- *The Lee value of an element $\alpha \in \mathbb{Z}_m$ is defined by*

$$| \alpha | = \begin{cases} \alpha, & for \quad 0 \leq \alpha \leq [\frac{m}{2}], \\ m - \alpha, & for \quad [\frac{m}{2}] < \alpha \leq m - 1. \end{cases},$$

  where $[\frac{m}{2}]$ is the greatest integer smaller than or equal to $\frac{m}{2}$.

- *The Lee distance between two vectors $\mathbf{a} = (a_1, a_2, \ldots, a_n)$ and $\mathbf{b} = (b_1, b_2, \ldots, b_n)$ over $\mathbb{Z}_m$ is defined by*

$$d_L(\mathbf{a}, \mathbf{b}) = \sum_{i=1}^{n} d_L(a_i, b_i),$$

  where $d_L(a_i, b_i) = min\{a_i - b_i, b_i - a_i\} (mod\ m)$, $i = 1, 2, \ldots, n$.

- *The Lee weight of a vector $\mathbf{a} = (a_1, a_2, \ldots, a_n)$ over $\mathbb{Z}_m$ is defined by*

$$w_L(\mathbf{a}) = d_L(\mathbf{a}, \mathbf{0}) = \sum_{i=1}^{n} | a_i | .$$

- *The* **minimum Lee distance**, *$d_L(X)$, of a subset X of $\mathbb{Z}_m^n$ is the minimum Lee distance between any pair of distinct vectors in X.*

Let $\mathbb{Z}_q[x]$ denote the ring of polynomials in the variable x over $\mathbb{Z}_q$, where q is a prime power p. Let $f(x)$ be a monic polynomial of degree h, irreducible over $\mathbb{Z}_p$. We have that $f(x)$ is also irreducible over $\mathbb{Z}_q$. Let $\mathcal{R} = \frac{\mathbb{Z}_m[x]}{\langle f(x) \rangle}$ denote the set of residue classes of polynomials in x over $\mathbb{Z}_q$, modulo the polynomial $f(x)$. This ring is a local commutative with identity and is called a Galois extension of $\mathbb{Z}_q$ of degree h. Let $\mathcal{G}_s$, where $s = p^h - 1$, be the maximal cyclic subgroup of $\mathcal{R}^*$ such that $gcd(s, p) = 1$.

Definition 3.2 *Let $\eta = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ be the locator vector consisting of distinct elements of $\mathcal{G}_s$. Now define matrix H as*

$$H = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \cdots & \alpha_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{r-1} & \alpha_2^{r-1} & \cdots & \alpha_n^{r-1} \end{bmatrix},$$

where r is a positive integer. Then H is the parity-check matrix of a shortened BCH code $\mathcal{C}(n, \eta)$ of length $n \leq s$ over $\mathbb{Z}_q$.

Thus, a word $\mathbf{c} = (c_1, c_2, \cdots, c_n) \in \mathbb{Z}_q^n$ is in $\mathcal{C}(n, \eta)$ if and only if it satisfies the following r parity-check equations over $\mathcal{R}$:

$$\sum_{j=1}^{n} c_j \alpha_j^l = 0, \quad l = 0, 1, \ldots, r - 1.$$

The codes $\mathcal{C}(n,\eta)$ for which $n = p^h - 1$ will be called *primitive*. In this case, η is unique, up to permutation of coordinates.

Given a transmitted word $\mathbf{c} = (c_1, c_2, \ldots, c_n) \in \mathcal{C}(n,\eta)$ and a received word $\mathbf{b} \in \mathbb{Z}_q^n$, the error vector is defined by $\mathbf{e} = \mathbf{b} - \mathbf{c}$. The number of *Lee errors* is given by $w_L(\mathbf{e})$, that is, the number of Lee errors is the smallest number of additions of ± 1 to the coordenates of the transmitted codeword $\mathbf{c}$ which yields the received word $\mathbf{b}$. Since the Lee weight satisfies the triangle inequality, using a code of minimum Lee distance d_L allows one to correct any pattern of up to $(d_L - 1)/2$ Lee errors.

Given a locator vector $\eta = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ of a code $\mathcal{C}(n,\eta)$ and a word $\mathbf{b} = (b_1, b_2, \ldots, b_n) \in \mathbb{Z}_q^n$, we define the *locator polynomial* associated with $\mathbf{b}$ as the polynomial

$$\sigma(x) = \prod_{j=1}^{n} (1 - \alpha_j x)^{w_L(c_j)}.$$

We define the syndrome values s_l of an error vector $\mathbf{e} = (e_1, e_2, \ldots, e_n)$ by

$$s_l = \sum_{j=1}^{n} e_j \alpha_j^l, \quad l \geq 0.$$

The formal syndrome series $S(x)$ is defined as

$$s(x) = \sum_{j=1}^{\infty} s_l x^l.$$

Given a codeword $\mathbf{c} \in \mathcal{C}(n,\eta)$ we define the word $\mathbf{c}^+ = (c_1^+, c_2^+, \ldots, c_n^+)$ as

$$c_j^+ = \begin{cases} c_j & \text{if } c_j \in \{1, 2, \ldots, [\frac{q}{2}]\} \\ 0 & \text{otherwise,} \end{cases},$$

and let $\mathbf{c}^- = \mathbf{c}^+ - \mathbf{c}$. That is, $\mathbf{c}^+$ is equal to $\mathbf{c}$ at the latter's positive entries, and is zero otherwise, whereas the entries of $\mathbf{c}^-$ take the Lee values of the negative entries of $\mathbf{c}$, leaving the others locations zero. We define the *positive syndrome values* s_l^+ and the *negative syndrome values* s_l^- of the error vector $\mathbf{e}$ by

$$s_l^+ = \sum_{j=1}^{n} e_j^+ \alpha_j^l \quad \text{and} \quad s_l^- = \sum_{j=1}^{n} e_j^- \alpha_j^l, \quad l \geq 0$$

with the associated formal syndromes series

$$s^+(x) = \sum_{l=1}^{\infty} s_l^+ x^l \quad \text{and} \quad s^-(x) = \sum_{l=1}^{\infty} s_l^- x^l.$$

Similarly, we define the positive and negative error-locator polynomials $\sigma^+(x)$ and $\sigma^-(x)$ by

$$\sigma^+(x) = \prod_{j=1}^{n} (1 - \alpha_j x)^{w_L(e_j^+)} \quad \text{and}$$

$$\sigma^-(x) = \prod_{j=1}^{n} (1 - \alpha_j x)^{w_L(e_j^-)}.$$

Now we assume that $\mathbf{c}$ is a codeword of $\mathcal{C}(n,\eta)$ of Lee weight $< 2r$. Let $\sigma^+(x)$ and $\sigma^-(x)$ denote the locator polynomials of $\mathbf{c}^+$ and $\mathbf{c}^-$, respectively, and let $s^+(x)$ and $s^-(x)$ be the formal power-sum series over $\mathcal{R}$ associated with $\sigma^+(x)$ and $\sigma^-(x)$. Since $H\mathbf{c} = 0$, we have that $H\mathbf{c}^+ = H\mathbf{c}^-$. The first equation in this last equality reads $w_L(\mathbf{c}^+) = w_L(\mathbf{c}^-) (mod\ q)$, that is, $w_L(\mathbf{c}^+) = w_L(\mathbf{c}^-) \pm lq$, for some integer l, whereas the other $r-1$ equations can be rewritten as $s_l^+ = s_l^-$, $l = 1, 2, \ldots, r-1$, or equivalently $s^+(x) \equiv s^-(x) (mod\ x^r)$.

Lemma 3.1 *If $w_L(\mathbf{c}^+) \neq w_L(\mathbf{c}^-)$ then $w_L(\mathbf{c}) \geq q$.*

Theorem 3.1 *Let $\mathcal{C}(n,\eta)$ be the a code with minimum Lee distance $d_L(\mathcal{C})$. Then the Lee metric $d_L(\mathcal{C})$ satisties $d_L(\mathcal{C}) \geq$*

$$\begin{cases} 2r, & \text{for } 1 \leq r \leq [\frac{q}{2}] \\ q, & \text{for } [\frac{q}{2}] < r \leq q-1. \end{cases}$$

References

[1] A.R. Hammons, Jr., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Solé, *The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals and related codes*, IEEE Trans. Inform. Theory, IT-40 (1994), pp. 301-319.

[2] A.R. Calderbank, G. McGuire, P.V. Kumar and T. Helleseth, *Cyclic codes over $\mathbb{Z}_4$, locator polynomials, and Newton' identities, IEEE Trans. on Inform. Theory*, 42 (1996), pp. 217-226.

[3] E. Biglieri and M. Elia, *On the construction of group block codes*, Annales des Telecommunications, Tome 50, No. 9-10 (1995), pp. 817-823.

[4] A.A. Andrade and R. Palazzo Jr., *Construction and decoding of BCH codes over finite commutative rings*, Linear Algebra and its Applications, 286 (1999), pp. 69-85.

[5] M. Greferath and U. Vellbinger, *Efficient decoding of $\mathbb{Z}_{p^k}$-linear codes*, IEEE Trans. Inform. Theory, 44 (1998), pp. 1288-1291.

[6] C.Y.Lee, *Some properties of nonbinary error-correcting codes*, IRE Trans. Inform. Theory, vol. 4, no. 4 (1958), pp. 77-82.

[7] W. Ulrich, *Non-binary error correction codes*, Bell Sys. Tech. J., vol. 36, no. 6 (1957), pp. 1341-1387.

[8] Ron M. Roth and p. H. Siegel, *Lee-metric BCH codes and their application to constrained and partial-reponse channels*, IEEE Trans. Inform. Theory, vol. 40, no. 4 (1994), pp. 1083-1096.

[9] G.D. Forney, Jr., *Generalized minimum distance decoding*, IEEE Trans. Inform. Theory, IT-12 (1966) 125-131.

[10] B.R. McDonald, *Finite Rings with Identity*, Marcel Dekker, Inc., New York, (1974).

[11] E.R. Berlekamp, *Algebraic Coding Theory*, McGraw-Hill, New York, (1968).

[12] G.D. Forney, Jr., *On decoding BCH codes*, IEEE Trans. Inform. Theory, IT-11 (1965), pp. 549-557.

[13] F.J. MacWilliams and N.J.A. Sloane, *The Theory of Error Correcting Codes*, North-Holland, Amsterdam, (1977).

[14] W.W. Peterson and E.J. Weldon, Jr., *Error Correcting Codes*, MIT Press, Cambridge, Mass., (1972).

[15] J.L. Massey, *Shift-register synthesis and BCH decoding*, IEEE Trans. Inform. Theory, IT-15 (1969), pp. 122-127.