# CODES OVER RINGS OF ALGEBRAIC INTEGERS

**Osvaldo Milaré Favareto, Trajano Pires da Nóbrega Neto, J. C. Interlando†, and Reginaldo Palazzo Jr.‡**
UNESP - Departamento de Matemática†
DT/FEEC/UNICAMP‡
palazzo@dt.fee.unicamp.br

**Resumo** - Neste trabalho códigos sobre os inteiros algébricos provenientes de duas extensões do conjunto dos números racionais $\mathbb{Q}$ isto é, $\mathbb{Q}(i)$ e $\mathbb{Q}(\sqrt{-3})$ são propostos. Estes códigos são projetados para a distância de Mannheim embora algumas propriedades com relação à distância de Hamming são também apresentadas, isto é, mostramos que estes são códigos com a máxima distância de sepração, ou equivalentemente, são códigos MDS. Eficientes algoritmos de decodificação são propostos para a decodificação destes códigos quando até duas coordenadas da palavra-código transmitida são alteradas por erros com peso de Mannheim arbitrário. O algoritmo de Berlekamp-Mussey é utilizado na correção de multiplos erros. O interesse prático destes códigos sob a métrica de Mannheim está relacionado com esquemas de modulação baseado em constelações do tipo QAM para as quais nem a métrica de Hamming nem a métrica de Lee são apropriadas.

**Abstract** - We propose codes over the algebraic integers of two quadratic extensions of $\mathbb{Q}$, namely, $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{-3})$. The codes being proposed are designed to the Mannheim distance, although some properties regarding their Hamming distances are also presented, e.g., we show that all presented codes are maximum distance separable MDS. Efficient decoding algorithms are proposed to decode the codes when when up to two coordinates of a transmitted code vector are affected by errors of arbitrary Mannheim weight. The Berlekamp-Massey algorithm is used for multiple error correction. The practical interest in such Mannheim-metric codes is for their use in coded modulation schemes based on QAM-type constellations, for which neither Hamming nor Lee metric is appropriate.

**Keywords:** Number fields, lattices, signal sets matched to groups, Mannheim distance, linear codes, algebraic decoding.

## 1. INTRODUCTION

In [1], Huber proposed codes over the ring $\mathbb{Z}[i]$, the algebraic integers of $\mathbb{Q}(\sqrt{-1})$. Two classes have been considered, viz., the one Mannheim error correcting codes, and the codes with minimum Mannheim distance greater than 3. In this work, we complete the results in [1] and present new ones. For example, all proposed codes are codes over the ring $\mathbb{A}$, the algebraic integers of $\mathbb{Q}(\sqrt{d})$, for $d=-1$ and $d=-3$. Such algebraic integers are $\mathbb{Z}[i]$ (Gaussian integers) and $\mathbb{Z}[\omega]$, where $\omega=(1+\sqrt{-3})/2$, respectively, and both will be denoted by $\mathbb{A}$.

The alphabets of the codes being proposed are actually subsets of the ring $\mathbb{A}$, having $p$ elements, where $p$ is a prime congruent to 1 modulo 4 if $d=-1$, and $p$ is congruent to 1 modulo 6 if $d=-3$. These alphabets are isomorphic to the field $GF(p)$, and both will be denoted by $\mathcal{A}$. Associated to any two elements of $GF(p)$, there is a distance, which is called Mannheim distance between the corresponding elements in $\mathcal{A}$. Four classes of codes are proposed. One class is designed to correct one Mannheim error, another to correct errors of any Mannheim weight affecting one coordinate of a code vector, another to correct errors of Mannheim weight 1 affecting two coordinates of a code vector, and another to correct errors of arbitrary Mannheim weight affecting two coordinates of a code vector. All codes in the present paper are constacyclic codes [2]. We present efficient syndrome decoding algorithms for each class being proposed. Finally, the Berlekamp-Massey algorithm is used when multiple Hamming errors occur.

## 2. ALGEBRAIC NUMBER FIELDS

In this section we review the background material on the theory of algebraic number fields that is necessary for understanding much of the remainder of this paper. The alphabets of the codes (proposed in Sections IV-A and IV-B), denoted by $\mathcal{A}$, are finite subsets of rings of algebraic integers $\mathbb{A}$ of a quadratic extension $\mathbb{K}=\mathbb{Q}(\sqrt{d})$ of $\mathbb{Q}$, where $d=-1$ and $d=-3$. In these cases, the ring $\mathbb{A}$ of the algebraic integers of $\mathbb{K}$ is $\mathbb{Z}[\omega]$, where $\omega=i$ if $d=-1$ and $\omega=(1+\sqrt{-3})/2$ if $d=-3$. In both cases, $\mathbb{A}$ is a principal ideal domain, and in particular its prime ideals have the form

$$p=<\pi>,$$

where $\pi=a+b\omega$, $a,b\in\mathbb{Z}$. The prime ideals of $\mathbb{Z}$ that we consider decompose completely in $\mathbb{A}$. As the nonzero prime ideals $\boldsymbol{p}$ of $\mathbb{A}$ are maximal, the quotients $\mathbb{A}/\boldsymbol{p}$ are fields of order $p$, where $p$ is a prime such that

$$p\equiv\begin{cases}1 \pmod 4 & \text{if } d=-1\\ 1 \pmod 6 & \text{if } d=-3.\end{cases} \tag{1}$$

From now on, $p=<a+b\omega>$ will denote a prime ideal in $\mathbb{A}$ containing $p\mathbb{Z}$, where $p$ is as in (1), and $N(a+b\omega)=p$. The function $N(\cdot)$ is the norm and $N(x+y\sqrt{d})=x^2-dy^2$, $\forall\, x,y\in\mathbb{Z}$. Since $\omega\in\mathbb{A}$, we have that $\omega$ belongs to some coset $\overline{s}\in\mathbb{A}/p$, where $0\le s\le p-1$. Thus $\overline{x+y\omega}=\overline{x}+\overline{y}\,\overline{\omega}=\overline{x}+\overline{y}\,\overline{s}=\overline{x+ys}=\overline{\ell}\in\{0,1,\ldots,p-1\}$. Now, $\overline{x+ys}=\overline{\ell}\Leftrightarrow x+ys-l\in p\cap\mathbb{Z}=p\mathbb{Z}$. In summary,

$$x+y\omega\equiv\ell \pmod p \Leftrightarrow x+ys\equiv\ell \pmod p, \tag{2}$$

where $s$ is a representative of the coset containing $\omega$. We define $\mathcal{A}$ as $\{\alpha_0,\alpha_1,\ldots,\alpha_{p-1}\}$, which is a complete set of

representatives of $p$ in $\mathbb{A}$, satisfying $\alpha_\ell \equiv \ell \pmod{p}$ and $N(\alpha_\ell)$ minimum. The fact that each $\alpha_\ell$ is unique is guaranteed by the next

**Theorem 1** *Let $p \in \mathbb{Z}$ be an odd prime, which factors into the product of two conjugate primes $\pi = a + \rho b$ and $\bar{\pi}$ (where $\rho$ can be either $\sqrt{-1}$ or $(1+\sqrt{-3})/2$)) in the ring $\mathbb{Z}[\rho]$, that is, $p = \pi\bar{\pi}$. Then in each coset $\ell + \mathfrak{p}$, where $\mathfrak{p} = \langle\pi\rangle$ and $\ell = 0, \ldots, p-1$, there is a unique element $\alpha_\ell = \ell + \mu\pi$ having minimum Euclidean norm.*

**Proof:** Let $N_l^* = \min\{N(\alpha); \alpha \in \ell + \mathfrak{p}\}$ be the minimum value of the norm of the elements in $\ell + \mathfrak{p}$. Since $\{-\frac{p-1}{2}, \ldots, -1, 0, 1, \ldots, \frac{p-1}{2}\}$ is a complete set of representatives of $\mathfrak{p}$ in $\mathbb{Z}[\rho]$, the Euclidean distance between any two coset representatives of minimum norm is always less than $p$. Now suppose that $\alpha_{l_1} = \ell + \mu_1\pi$ and $\alpha_{l_2} = \ell + \mu_2\pi$ are two elements in $\ell + \mathfrak{p}$ having the same minimum norm, that is, $N(\alpha_{l_1}) = N(\alpha_{l_2}) = N_l^*$. This implies that

$$\ell^2 + \ell[\mu_1\pi + \bar{\mu}_1\bar{\pi}] + \mu_1\bar{\mu}_1\pi\bar{\pi} = \ell^2 + \ell[\mu_2\pi + \bar{\mu}_2\bar{\pi}] + \mu_2\bar{\mu}_2\pi\bar{\pi},$$

and therefore,

$$\ell[(\bar{\mu}_1 - \bar{\mu}_2)\bar{\pi} + (\mu_1 - \mu_2)\pi] = [\mu_1\bar{\mu}_1 - \mu_2\bar{\mu}_2]\pi\bar{\pi}.$$

Since $\ell, \pi$, and $\bar{\pi}$ are coprimes, and $\langle\pi\rangle$ and $\langle\bar{\pi}\rangle$ are prime principal ideals, then $\mu_1 - \mu_2 \in \langle\bar{\pi}\rangle$, that is, $\alpha_{l_1} - \alpha_{l_2} = pt$, for some $t$ in $\mathbb{Z}[\rho]$. Now, $\alpha_{l_1}$ and $\alpha_{l_2}$ belong to the circle with radius $(p-1)/2$ and center at the origin. Hence $t = 0$, and therefore $\alpha_{l_1} = \alpha_{l_2}$, which completes the proof. □

In this way, we obtain a labeling of the elements of the set $\mathcal{A} = \{\alpha_0, \alpha_1, \ldots, \alpha_{p-1}\} \subset \mathbb{A}$ by the additive group of $GF(p)$. Therefore, the following procedure can be used to label each element of $\mathcal{A}$ by an element of the field $GF(p)$.

1. Given a prime number $p$ that decomposes completely in $\mathbb{A}$, let $\pi = a + b\omega$ be a solution of $N(\alpha) = p, \alpha \in \mathbb{A}$;
2. Let $s \in \mathbb{Z}$ be the only solution (in $r$) of the equation $a + br \equiv 0 \pmod{p}$, where $0 \le r \le p-1$;
3. The element $\ell \in GF(p)$ is the label of the point $\alpha = x + y\omega \in \mathbb{A}$ if $x + ys \equiv \ell \pmod{p}$ and $N(\alpha)$ is minimum.

We can improve the above algorithm if before starting it, the values of $N(\alpha)$ are sorted in increasing order, and next, to each point $\alpha = x + y\omega$ of $\mathcal{A}$, we assign the label $\ell$, where $\ell \equiv x + ys \pmod{p}$.

**Definition 1** *i) Given an element $\gamma = a + b\omega \in \mathcal{A}$, the* Mannheim weight *of $\gamma$ is*

$$w^M(\gamma) = |a| + |b|.$$

*ii) The Mannheim distance between any two elements $\alpha$ and $\beta$ in $\mathcal{A}$ is*

$$d^M(\alpha, \beta) = w_M(\delta),$$

*where $\delta \equiv \alpha - \beta \pmod{p}$, $\delta \in \mathcal{A}$.*

This definition for the Mannheim distance generalizes the one given by Huber in [1].

**Theorem 2** *[4] Let $\mathbb{A} = \mathbb{Z}[\omega]$ be the ring of algebraic integers of $\mathbb{Q}(\sqrt{-3})$ and $\pi = a + b\omega \in \mathbb{A}$, such that $N(\pi) = a^2 + ab + b^2$ is a prime $p \equiv 1 \pmod{6}$. Then the maximum Mannheim distance between any two elements of $\mathcal{A}$ is given by*

$$d^M_{\max}(\mathcal{A}) = \max\{|a|, |b|, |a+b|\} - 1.$$

**Theorem 3** *[1] Let $\mathbb{A} = \mathbb{Z}[i]$ be the ring of algebraic integers of $\mathbb{Q}(\sqrt{-1})$ and $\pi = a + bi \in \mathbb{A}$, such that $N(\pi) = a^2 + b^2$ is a prime $p \equiv 1 \pmod{4}$. The the maximum Mannheim distance between any two elements of $\mathcal{A}$ is given by $d^M_{\max}(\mathcal{A}) = \max\{|a|, |b|\} - 1$.*

To save space we omit the proof of Theorem 2, however it can be found in [4].

## 3. CODES OVER ALGEBRAIC INTEGERS: PRELIMINARIES

In this section our objective is to present some properties of codes over the rings of algebraic integers of $\mathbb{Q}(\sqrt{-3})$ and of $\mathbb{Q}(\sqrt{-1})$, from their parity-check matrices, as well as to present some of their basic properties. Initialy, we consider codes over $\mathbb{Z}[\omega]$, the ring of algebraic integers of $\mathbb{Q}(\sqrt{-3})$, where $\omega = (1+\sqrt{-3})/2$. Let $\beta \in \mathcal{A}$ be an element of order $6n = p - 1$, (where $p$ is a prime number, as in (1)), such that $\beta^n = \omega$. Let $C$ be the code defined by the parity-check matrix

$$H = \begin{bmatrix} 1 & \beta & \cdots & \beta^{n-1} \\ 1 & \beta^7 & \cdots & (\beta^7)^{n-1} \\ \vdots & \vdots & \cdots & \vdots \\ 1 & \beta^{6t+1} & \cdots & (\beta^{6t+1})^{n-1} \end{bmatrix}, \qquad (3)$$

where $0 \le t \le n-1$.

**Theorem 4** *The polynomial $g(x) = (x-\beta)(x-\beta^7)\cdots(x-\beta^{6t+1})$ is the generator of code $C$, which is a principal ideal of the ring $\mathcal{A}[x]/ < x^n - \omega >$.*

**Proof:** An $n$-tuple $\underline{c} = (c_0, c_1, \ldots, c_{n-1}) \in \mathcal{A}_p^n[\omega]$ is a codeword of $C$ if and only if $H\underline{c}^t = \underline{0}$. Hence, if $c(x) = \sum_{i=0}^{n-1} c_i x^i$ is the associated code polynomial, we have $c(\beta^{6k+1}) = 0$, for $k = 0, 1, \ldots, t$. Let $g(x) = (x-\beta)(x-\beta^7)\ldots(x-\beta^{6t+1})$. Then the degree of $g(x)$ is $\partial g = t + 1$. The elements in the set $S = \{\beta, \beta^7, \ldots, \beta^{6t+1}\}$ are all distinct elements of $\mathcal{A}_p[\omega]$, and they are roots of $c(x)$. Further, the set $S$ is exactly the set of all the roots of $g(x)$. Now, since $(\beta^{6k+1})^n - \omega = \beta^{6nk}\beta^n - \omega = \beta^n - \omega = 0$, for $k = 0, 1, \ldots, t$, then $g(x)$ divides $x^n - \omega$. □.

**Definition 2** *$\omega$-cyclic codes (respectively $-\omega$-cyclic codes) are codes over $\mathcal{A}$, whose codewords are multiples of the generator polynomial $g(x) = \prod_{k=0}^{t} (x - \beta^{6t+1})$, that divides $f(x) = x^n - \omega$, (resp. $x^n + \omega$).*

Code $C$ defined by the matrix in (3) belong to the class of constacyclic codes, [2], or $\pm\omega$−cyclic codes. Codes over $\mathbb{Z}[i]$ are defined in a similar way [1].

## 4. CONSTRUTION OF CODES OVER ALGEBRAIC INTEGERS

In this section we present linear codes over algebraic integers in terms of parity-check matrices. The corresponding decoding algorithms follow from the proofs of Theorems 5, 6, 7, and 8 given next.

### 4.1. Codes over the Algebraic Integers of $\mathbb{Z}g[\omega]$

In this section we construct codes over the ring of algebraic integers of $\mathbb{Z}[\omega]$, where $\omega = (1+\sqrt{-3})/2$. Let $\beta \in \mathcal{A}$ be an element of order $6n = p-1$, such that $\beta^n = \omega$.

#### 4.1.1. Single-Error-Correcting Codes

**Theorem 5** *Let $C$ be the code defined by the parity-check matrix*

$$H = \begin{bmatrix} 1 & \beta & \cdots & \beta^{n-1} \end{bmatrix}.$$

*Then $C$ can correct every error pattern of the form $e(x) = e_i x^i$, where $w^M(e_i) = 1$ and the error patterns $e(x) = e_j x^j$, where $w^M(e_j) = 2$, if $e_j$ is a sixth root of unity.*

**Proof:** Recall that the elements of Mannheim weight 1 of the alphabet $\mathcal{A}_p[\omega]$ are $\pm 1$ and $\pm\omega$, where $\omega$ is a 6th root of unity. The other roots of unity, namely, $\pm\omega^2 = \pm(\omega - 1)$, have Mannheim weight 2. Now, notice that the set $\{\pm 1, \pm\omega, \pm\omega^2\}$ can be represented as $\{\beta^{nu},\ u = 1,2,\cdots,6\}$. Without loss of generality, we can suppose that the all zero codeword has been transmitted. Let $r = (0,\cdots,\beta^{nu},\cdots,0)$ denote the received vector. Then the syndrome $S = Hr^t$ is given by

$$S = \beta^{j+nu} = \beta^L, \text{ where } L, j \in \mathbb{Z}, \quad 0 \le L, j \le n-1.$$

By reducing $L$ modulo $n$, we determine $j$, and next $u$ is determined by $u = \frac{L-j}{n}$. Therefore, we have the location and the magnitude of the error. □

**Theorem 6** *Let $C$ be the code defined by the parity-check matrix*

$$H = \begin{bmatrix} 1 & \beta & \cdots & \beta^{n-1} \\ 1 & \beta^7 & \cdots & \beta^{7(n-1)} \end{bmatrix}.$$

*Then $C$ can correct every error pattern of the form $e(x) = e_i x^i$, where $1 \le w^M(e_i) \le d^M_{\max}(\mathcal{A})$, $0 \le i \le n-1$.*

**Proof:** Suppose that an error of magnitude $\beta^k$, $0 \le k \le 6n-1$, has occurred in location $j$, $0 \le j \le n-1$. Let $r = (0,0,\cdots,\beta^k,\cdots,0,0)$ be the received vector. Then the syndrome $S$ is given by

$$S = Hr^t = \begin{bmatrix} \beta^{j+k} \\ \beta^{7j+k} \end{bmatrix} = \begin{bmatrix} S_1 \\ S_7 \end{bmatrix}.$$

Letting $S_1 = \beta^{L_1}$ and $S_7 = \beta^{L_2}$, where $L_i$ is the logarithm of $S_i$ to the base $\beta$, $i = 1, 7$, we have

$$\beta^{j+k} = S_1 \Rightarrow j + k \equiv L_1 \pmod{p-1},$$

$$\beta^{7j+k} = S_7 \Rightarrow 7j + k \equiv L_2 \pmod{p-1}.$$

The linear system of equations

$$\begin{cases} j + k \equiv L_1 \pmod{p-1} \\ 7j + k \equiv L_2 \pmod{p-1} \end{cases},$$

has only one solution, namely,

$$\begin{cases} j \equiv \frac{L_2 - L_1}{6} \pmod{n} \\ k \equiv L_1 - j \pmod{p-1} \end{cases}$$

Thus we can conclude that one error has occurred in location $\frac{L_2-L_1}{6} \pmod{n}$ and its magnitude is $\beta^k$, where $k = L_1 - j \pmod{p-1}$. □

#### 4.1.2. Double-Error-Correcting Codes

**Theorem 7** *Let $C$ be the code defined by the parity-check matrix*

$$H = \begin{bmatrix} 1 & \beta & \cdots & \beta^{n-1} \\ 1 & \beta^7 & \cdots & \beta^{7(n-1)} \\ 1 & \beta^{13} & \cdots & \beta^{13(n-1)} \end{bmatrix}.$$

*Then $C$ can correct every error pattern of the form $e(x) = e_i x^i + e_j x^j$, where $w^M(e_i) = w^M(e_j) = 1$, $0 \le i \ne j \le n-1$.*

**Proof:** Let $v \in C$ be the transmitted codeword, and $e$ the error pattern introduced by the channel. Suppose that two errors each of Mannheim weight one, have occurred in locations $j$ and $k$, $0 \le j < k \le n-1$, and that their magnitudes are, respectively, $\beta^{un}$ and $\beta^{vn}$, $0 \le u < v \le 5$. Let

$$H = \begin{bmatrix} 1 & \beta & \cdots & \beta^j & \cdots & \beta^k & \cdots & \beta^{n-1} \\ 1 & \beta^7 & \cdots & \beta^{7j} & \cdots & \beta^{7k} & \cdots & \beta^{7(n-1)} \\ 1 & \beta^{13} & \cdots & \beta^{13j} & \cdots & \beta^{13k} & \cdots & \beta^{13(n-1)} \end{bmatrix}$$

be the parity-check matrix, and $r = (0,0,\cdots,\beta^{un},\cdots,\beta^{vn},\cdots,0)$ the received vector. Then,

$$S = Hr^t = \begin{bmatrix} \beta^{j+un} + \beta^{k+vn} \\ \beta^{7j+un} + \beta^{7k+vn} \\ \beta^{13j+un} + \beta^{13k+vn} \end{bmatrix} = \begin{bmatrix} S_1 \\ S_7 \\ S_{13} \end{bmatrix}$$

is the syndrome. Since $\beta^{6n} = 1$, then $\beta^{un} = \beta^{6un}\beta^{un} = \beta^{7un} = \beta^{12un}\beta^{un} = \beta^{13un}$ (similarly, $\beta^{vn} = \beta^{7vn} = \beta^{13vn}$). Therefore, we have the following linear system of equations

$$\begin{cases} \beta^{j+un} + \beta^{k+vn} = S_1 \\ \beta^{7(j+un)} + \beta^{7(k+vn)} = S_7 \\ \beta^{13(j+un)} + \beta^{13(k+vn)} = S_{13} \end{cases}.$$

Letting $\beta^{j+un} = x$, $\beta^{k+vn} = y$, $S_1 = a$, $S_7 = b$, and $S_{13} = c$, we have

$$\begin{cases} x + y = a \\ x^7 + y^7 = b \\ x^{13} + y^{13} = c \end{cases}. \tag{4}$$

Code $C$ is capable of correcting any error pattern of two Hamming errors, each of Mannheim weight one if and only if the system in (4) admits only two solutions.

Assuming that two Hamming errors have occurred, we will show that:

a) $a \ne 0$;

b) The system in (4) admits at least two solutions.

a) If $a = 0$, then $\beta^{j+un} = -\beta^{k+vn}$. This implies that $b = \beta^{7(j+un)} + \beta^{7(k+vn)} = -\beta^{7(k+vn)} + \beta^{7(k+vn)} = 0$. Similarly, $c = 0$. Hence, $a = b = c = 0$. Therefore, no errors have occurred, which contradicts our hypothesis. So, $a \neq 0$;

b) Let $(x_0, y_0)$ be a solution of (4); we shall show that $x_0 \neq y_0$. If $x_0 = \beta^{j+un} = \beta^{k+vn} = y_0$, then $\beta^{k-j+n(v-u)} = 1$; however, $k - j + n(v-u) \leq n - 1 + n \cdot 5 = 6n - 1 < 6n = o(\beta)$, a contradiction. Thus, $x_0 \neq y_0$. Since the system in (4) is symmetric in $x$ and $y$, we have that $(y_0, x_0)$ is also a solution. We can conclude, therefore, that the solutions of (4) occur always in pairs. Now, we proceed to indicate how to find them.

In (4), we have $y = a - x$; thus we can consider the polynomials

$$f(x) = x^{13} + (a-x)^{13} - c,$$

and

$$g(x) = x^7 + (a-x)^7 - b,$$

where $f(x), g(x) \in \mathcal{A}_p[\omega][x]$. Let $x_0$ be a root of $f(x)$, that is, $f(x_0) = 0$. Now, $f(a-x_0) = (a-x_0)^{13} + (a-a+x_0)^{13} - c = x_0^{13} + (a-x_0)^{13} - c = f(x_0) = 0$. Therefore, $f(x_0) = 0$ if and only if $f(a-x_0) = f(y_0) = 0$. Similarly, the same result holds for $g(x)$ (notice that since we are assuming that two coordinates of $r$ are in error, $f(x)$ and $g(x)$ have at least two common roots). Considering then the polynomials $f(x)$ and $g(x)$, and using Euclid's Algorithm, it follows that

$$\exists\ q(x), h(x) \in \mathcal{A}_p[\omega][x]$$

such that $f(x) = q(x)\,g(x) + h(x)$, with $\partial h \leq 5$

(here and thereafter $\partial p$ denotes the degree of polynomial $p(x)$). After some calculations, we obtain

$$h(x) = \frac{a^2}{7}(b - a^7)(39x^4 - 78ax^3 + 65a^2x^2 - 26a^3x)$$

$$+\frac{1}{49a}(-29a^{14} + 65a^7b + 13b^2 - 49ac),$$

($a \neq 0$, by a)). Thus either $\partial h = 0$ or $\partial h = 4$. Notice that the common roots to $f(x)$ and $g(x)$ are also roots of $h(x)$.

1. If $\partial h = 0$, then $h(x)$ must be the null polynomial (since $f(x)$ and $g(x)$ admit at least two solutions). However, $h(x) = 0$ if and only if $b = a^7$ and $c = a^{13}$. Now, if $b = a^7$ and $c = a^{13}$, we have

$$g(x) =$$

$$= x(x-a)\left(x - \frac{a(1-i\sqrt{3})}{2}\right)^2\left(x - \frac{a(1+i\sqrt{3})}{2}\right)^2$$

$$= x(x-a)(x-a\omega)^2(x+a\omega^2)^2.$$

So, the distinct roots of $g(x)$ are $x = 0$, $x = a$, $x = \frac{a(1+i\sqrt{3})}{2} = a\omega$, and $x = \frac{a(1-i\sqrt{3})}{2} = -a\omega^2$. However, $x = 0$ implies that $\beta^{j+un} = 0$, which is impossible. Similarly, $x = a$ implies that $y = 0$, that is, $\beta^{k+vn} = 0$, which is impossible too. It is easy to check that $a\omega$ and $-a\omega^2$ are also roots of $f(x)$. Thus $f(x)$ and $g(x)$ have only two distinct common roots, namely, $x_1 = a\omega$, and $x_2 = a(1-\omega)$;

2. If $\partial h = 4$, then applying Euclid's algorithm to the polynomials $g(x)$ and $h(x)$, we have

$$\exists\ s(x), k(x) \in \mathcal{A}_p[\omega][x]$$

such that $g(x) = s(x)\,h(x) + k(x)$, with $\partial k \leq 3$.

Now, since the roots of $f(x)$ and $g(x)$ (and consequently, the roots $h(x)$ and $k(x)$) occur in pairs, we have either $\partial k = 0$ or $\partial k = 2$ (the polynomial expression for $k(x)$ is of the form $k(x) = k_0 + k_1x + k_2x^2$; for the sake of brevity, we omit the rather long expressions for the coefficients $k_0, k_1$, and $k_2$).

(a) If $\partial k = 2$, then $g(x)$ and $h(x)$ (and also $f(x)$) have two common roots, which are exactly the two roots of $k(x)$.

(b) If $\partial k = 0$, then $k(x)$ is identically null. Since $k(x) = k_0 + k_1x + k_2x^2$, we have

$$k_0 = 0 \Rightarrow c = \frac{a^{14} + 26a^7b + 169b^2}{196a}, \quad (5)$$

$$k_1 = 0 \Rightarrow c = \frac{4a^{14} + 104a^7b + 39b^2}{147a}, \quad (6)$$

$$k_2 = 0 \Rightarrow c = \frac{4a^{14} + 104a^7b + 39b^2}{147a}. \quad (7)$$

Upon equating (5) and (6), we get the following 2nd degree equation in $b$

$$m(b) = -17199b^2 + 16562a^7b + 637a^{14}$$

Now, solving the equation $m(b) = 0$, we obtain the roots $b = a^7$ and $b = \frac{-a^7}{27}$. The case $b = a^7$ has already been analysed in 1. If $b = \frac{-a^7}{27}$, then $c = \frac{a^{13}}{729}$, and in this case the only common roots to $f(x)$ and $g(x)$ are $x_1 = \frac{a(3+i\sqrt{3})}{6} = \frac{a}{3}(1+\omega)$ and $x_2 = \frac{a(3-i\sqrt{3})}{6} = \frac{a}{3}(2-\omega)$. Actually, in this case,

$$g(x) =$$

$$\left(x - \frac{a(3-i\sqrt{3})}{6}\right)^2\left(x - \frac{a(3+i\sqrt{3})}{6}\right)^2 \cdot$$

$$\cdot\left(x - \frac{a(3-i\sqrt{39})}{6}\right)\left(x - \frac{a(3+i\sqrt{39})}{6}\right),$$

and

$$f\left(\frac{a(3 \pm i\sqrt{39})}{6}\right) \neq 0,$$

since

$$f\left(\frac{a(3 \pm i\sqrt{39})}{6}\right) = \frac{-a^{13}}{729} + 2\left[\frac{a(3 \pm i\sqrt{39})}{6}\right]^{13}$$

$$= a^{13}\left\{\frac{-1}{729} + 2\left[\frac{(3 \pm i\sqrt{39})}{6}\right]^{13}\right\} = 0 \Leftrightarrow a = 0,$$

$$(\beta^{12i}+\beta^{6i}\beta^{6j}+\beta^{12j})(S_7-\beta^{6j}S_1)=S_{19}-\beta^{18j}S_1. \quad (13)$$

Let $\beta^{6i}+\beta^{6j}=S$, and $\beta^{6i}\beta^{6j}=P$. Then we have

$$SS_7-\beta^{6j}\beta^{6i}S_1-\beta^{12j}S_1=S_{13}-\beta^{12j}S_1, \quad (14)$$

$$(S^2-P)(S_7-\beta^{6j}S_1)=S_{19}-\beta^{18j}S_1. \quad (15)$$

From (14), we conclude that

$$P=\frac{SS_7-S_{13}}{S_1}. \quad (16)$$

($S_1\neq 0$, since we are assuming that two coordinates of $r$ are in error). From (15), we obtain

$$S_7(S^2-P)-PSS_1=S_{19}. \quad (17)$$

Substituting (16) in (17), we get

$$S_7(S^2-\frac{SS_7-S_{13}}{S_1})-S_1S\frac{SS_7-S_{13}}{S_1}=S_{19},$$

which implies that

$$S=\frac{S_1S_{19}-S_7S_{13}}{S_1S_{13}-S_7^2}. \quad (18)$$

The term $S_1S_{13}-S_7^2\neq 0$, unless only one coordinate of $r$ is in error [4]. Substituting (18) in (16), we obtain

$$P=\frac{S_7S_{19}-S_{13}^2}{S_1S_{13}-S_7^2}.$$

After calculating the roots of the equation $X^2-SX+P=0$, namely,

$$X_1=\beta^{6i}, \qquad X_2=\beta^{6j},$$

we can find $i$ and $j$, the error locations. Now, using the first two equations of (8), we get

$$x=\frac{S_7-\beta^{6j}S_1}{\beta^{6i}-\beta^{6j}}, \text{ and } y=\frac{S_7-\beta^{6i}S_1}{\beta^{6j}-\beta^{6i}}.$$

In this way, we are able to determine $k$ and $l$, since $x=\beta^{i+k}$ and $y=\beta^{j+l}$. □

Next, we outline an error correction procedure for the codes defined in Theorem 8.

- **Decoding Procedure for the Codes Defined in Theorem 8**

1. If $S_1=0$, then no errors have occurred; set $v=r$.
2. If $S_1S_{13}-S_7^2=0$, then only one error of magnitude $\beta^k$ has occurred at location $i$. We determine $i$ and $k$ as in the decoding procedure for the codes in Theorem 8.
3. If $S_1S_{13}-S_7^2\neq 0$, then two errors have occurred, and we must proceed as follows:
   *a*) Solve the equation $X^2-SX+P=0$, where $S=\frac{S_1S_{19}-S_7S_{13}}{S_1S_{13}-S_7^2}$ and $P=\frac{S_7S_{19}-S_{13}^2}{S_1S_{13}-S_7^2}$, whose roots are $X_1=\beta^{6i}$ and $X_2=\beta^{6j}$. This yields the error locations $i$ and $j$.
   *b*) Using the first two equations of (8), we get

$$\begin{cases} x+y=S_1 \\ \beta^{6i}x+\beta^{6j}y=S_7 \end{cases},$$

   which yields

$$x=\frac{S_7-\beta^{6j}S_1}{\beta^{6i}-\beta^{6j}}, \text{ and } y=\frac{S_7-\beta^{6i}S_1}{\beta^{6j}-\beta^{6i}}.$$

   From $x$ and $y$, we are able to determine $k$ and $l$, since $x=\beta^{i+k}$ and $y=\beta^{j+l}$.
4. The transmitted codeword $v\in C$ is obtained by calculating the difference $v=r-e$.

## 4.2. Codes over the Gaussian Integers

For codes defined over the Gaussian integers $\mathbb{Z}[i]$, analogous theorems to the case $\mathbb{Z}[\omega]$ hold with appropriate modifications.

# 5. SOME HAMMING DISTANCE PROPERTIES OF CODES OVER ALGEBRAIC INTEGERS

Let $p\equiv 1 \pmod 6$ and $n=(p-1)/6$. Suppose $r,t\in\mathbb{Z}$ such that $0\leq r<n, t<p-1$ and $(t,p-1)\leq 6$. Consider the matrix

$$H=\begin{bmatrix} 1 & \beta & \cdots & \beta^{n-1} \\ 1 & \beta^{t+1} & \cdots & (\beta^{t+1})^{n-1} \\ \vdots & \vdots & \cdots & \vdots \\ 1 & \beta^{rt+1} & \cdots & (\beta^{rt+1})^{n-1} \end{bmatrix},$$

where $\beta$ is a primitive element of $\mathcal{A}$, as defined previously. Then we have the following

**Proposition 1** *Any $r+2$ columns of $H$ are linearly dependent.*

**Proof:** Straightforward.

**Proposition 2** *Any $r+1$ columns of $H$ are linearly independent.*

**Proof:** Let $h_{i_j}$ denote the $j$-th column of $H$, that is,

$$h_{i_j}=[\ \beta^{i_j} \quad (\beta^{t+1})^{i_j} \quad \cdots \quad (\beta^{rt+1})^{i_j}\ ]^T,$$

$j=1,2,\ldots,r+1$. Further, let $L$ be the matrix formed by the columns $i_1,\ldots,i_{r+1}$ of $H$, that is,

$$L=\begin{bmatrix} \beta^{i_1} & \beta^{i_2} & \cdots & \beta^{i_{r+1}} \\ (\beta^{t+1})^{i_1} & (\beta^{t+1})^{i_2} & \cdots & (\beta^{t+1})^{i_{r+1}} \\ \vdots & \vdots & \cdots & \vdots \\ (\beta^{rt+1})^{i_1} & (\beta^{rt+1})^{i_2} & \cdots & (\beta^{rt+1})^{i_{r+1}} \end{bmatrix},$$

Proving that the $r+1$ columns of $H$ are linearly independent is equivalent to proving that $\det L\neq 0$. Now,

$$\det L=\beta^{i_1}\beta^{i_2}\ldots\beta^{i_{r+1}}\det L_1=\beta^{\sum_{j=1}^{r+1}i_j}\det L_1,$$

which is impossible.

Now suppose that an error pattern of the form $e(x) = e_j x^j$, where $w^M(e_j) = 1$, and $0 \leq j \leq n-1$, has occurred. Thus, $S_1 \neq 0$. Then from (4), we have

$$\begin{cases} x = \beta^{j+un} = a \\ x^7 = \beta^{7(j+un)} = b = a^7 \\ x^{13} = \beta^{13(j+un)} = c = a^{13} \end{cases},$$

From $b = a^7$ and $c = a^{13}$, we have that $h(x)$ is identically null. Then, as in Case 1., the common roots of $f(x)$ and $g(x)$ are $x = 0, x = a, x = a\omega, x = a(1-\omega) = -a\omega^2$. Therefore, the solutions of (4) are $(a, 0)$, $(0, a)$, $(a\omega, -a\omega^2)$, and $(-a\omega^2, a\omega)$.

a) If $x = 0$, then $y = a = \beta^{j+un} = \beta^{L_1}$; therefore, $j + un = L_1 \equiv j \pmod{n}$. Thus one error has occurred at location $j$.

b) If $x = a$, then $y = 0$; therefore, $x = \beta^{j+un} = \beta^{L_1}$. Hence, $j + un = L_1 \equiv j \pmod{n}$. Thus one error has occurred at location $j$.

c) If $x = a\omega$, then $x = \beta^{j+un}\beta^n = \beta^{j+n(u+1)} = \beta^{L_2}$, hence $j + n(u+1) = L_2 \equiv j \pmod{n}$. Thus one error has occurred at location $j$.

d) If $x = -a\omega^2$, we have that $x = \beta^{3n}\beta^{j+un}\beta^{2n} = \beta^{j+n(u+5)} = \beta^{L_3}$; hence $j + n(u+5) = L_3 \equiv j \pmod{n}$. Thus one error has occurred at position $j$.

So, if $b = a^7$, then one error has occurred at position $j$. □

*Remark*: Code $C$ defined by the parity-check matrix $H$ of Theorem 7 can also correct every error pattern of the form $e(x) = e_i x^i + e_j x^j$, where $w^M(e_i) \leq 2$, $w^M(e_j) \leq 2$, $0 \leq i < j \leq n-1$, and $e_i$ and $e_j$ are 6th roots of unity.

Next, we outline an error correction procedure for the codes defined in Theorem 7.

- **Decoding Procedure for the Codes Defined in Theorem 7**

1. If $a = 0$, then no errors have occurred; set $r = v$.
2. If $b = a^7$, and $c = a^{13}$, then only one error has occurred, and we proceed as follows. The location $j$ of the error is $j = L_1 \pmod{n}$, where $L_1$ is such that $S_1 = \beta^{L_1}$, and its magnitude is $Y = \beta^{L_1 - j}$.
3. If $b \neq a^7$ or $c \neq a^{13}$, then two coordinates are affected, each one by a Mannheim error of weight one. Then we must proceed as follows.
   - Solving $k(x) = 0$ (or $h(x) = 0$, or $g(x) = 0$), we get the roots $x_1 = \beta^{L_1}$, and $x_2 = \beta^{L_2}$. Since $x_1 = \beta^{j+un}$ and $x_2 = \beta^{k+vn}$, we have
   $$\begin{cases} j \equiv L_1 \pmod{n} \\ k \equiv L_2 \pmod{n} \end{cases}$$
   and this gives the error locations.
4. The error magnitudes are given by
   $$\begin{cases} Y_1 = \beta^{L_1 - j} \\ Y_2 = \beta^{L_2 - j} \end{cases}.$$
5. The transmitted codeword $v \in C$ is obtained by calculating the difference $v = r - e$.

**Theorem 8** *Let $C$ be the code defined by the parity-check matrix*

$$H = \begin{bmatrix} 1 & \beta & \cdots & \beta^{n-1} \\ 1 & \beta^7 & \cdots & (\beta^7)^{n-1} \\ 1 & \beta^{13} & \cdots & (\beta^{13})^{n-1} \\ 1 & \beta^{19} & \cdots & (\beta^{19})^{n-1} \end{bmatrix}.$$

*Then $C$ can correct every error pattern of the form $e(x) = e_i x^i + e_j x^j$, where $1 \leq w^M(e_i)$, $w^M(e_j) \leq d^M_{\max}(\mathcal{A})$, $0 \leq i \neq j \leq n-1$.*

**Proof**: Let $v \in C$ be the transmitted codeword, and $e$ the error pattern introduced by the channel. Suppose that two errors have occurred in locations $i$ and $j$, $0 \leq i < j \leq n-1$, and that their magnitudes are, respectively, $\beta^k$ and $\beta^l$, where $0 \leq k \leq p-1$, and $0 \leq l \leq p-1 = 6n$. Let

$$H = \begin{bmatrix} 1 & \beta & .. & \beta^i & .. & \beta^j & .. & \beta^{n-1} \\ 1 & \beta^7 & .. & (\beta^7)^i & .. & (\beta^7)^j & .. & (\beta^7)^{n-1} \\ 1 & \beta^{13} & .. & (\beta^{13})^i & .. & (\beta^{13})^j & .. & (\beta^{13})^{n-1} \\ 1 & \beta^{19} & .. & (\beta^{19})^i & .. & (\beta^{19})^j & .. & (\beta^{19})^{n-1} \end{bmatrix}$$

be the parity check matrix, and $r = (0, 0, \cdots, \beta^k, \cdots, \beta^l, \cdots, 0)$ the received vector. Then,

$$S = Hr^t = \begin{bmatrix} \beta^{i+k} + \beta^{j+l} \\ \beta^{7i+k} + \beta^{7j+l} \\ \beta^{13i+k} + \beta^{13j+l} \\ \beta^{19i+k} + \beta^{19j+l} \end{bmatrix} = \begin{bmatrix} S_1 \\ S_7 \\ S_{13} \\ S_{19} \end{bmatrix}$$

is the syndrome. Letting $x = \beta^{i+k}$ and $y = \beta^{j+l}$, we obtain the following linear system of equations

$$\begin{cases} x + y = S_1 \\ \beta^{6i}x + \beta^{6j}y = S_7 \\ \beta^{12i}x + \beta^{12j}y = S_{13} \\ \beta^{18i}x + \beta^{18j}y = S_{19} \end{cases} \tag{8}$$

Code $C$ can correct two errors if and only if the system in (8) admits only one solution. Since we are assuming that two coordinates of $r$ are in error, the system in (8) admits at least one solution. We will show that there is exactly one solution. From $x + y = S_1$, the system in (8) becomes

$$\begin{cases} (\beta^{6i} - \beta^{6j})x = S_7 - \beta^{6j}S_1 \\ (\beta^{12i} - \beta^{12j})x = S_{13} - \beta^{12j}S_1 \\ (\beta^{18i} - \beta^{18j})x = S_{19} - \beta^{18j}S_1 \end{cases},$$

which implies that

$$(\beta^{6i} - \beta^{6j})x = S_7 - \beta^{6j}S_1, \tag{9}$$

$$(\beta^{6i} - \beta^{6j})(\beta^{6i} + \beta^{6j})x = S_{13} - \beta^{12j}S_1, \tag{10}$$

$$(\beta^{6i} - \beta^{6j})\left(\beta^{12i} + \beta^{6i}\beta^{6j} + \beta^{12j}\right)x = S_{19} - \beta^{18j}S_1. \tag{11}$$

Now, substituting (9) in (10), and in (11), we get:

$$(\beta^{6i} + \beta^{6j})(S_7 - \beta^{6j}S_1) = S_{13} - \beta^{12j}S_1, \tag{12}$$

where

$$L_1 = \begin{bmatrix} 1 & 1 & \dots & 1 \\ \beta^{ti_1} & \beta^{ti_2} & \dots & \beta^{ti_r} \\ \vdots & \vdots & \dots & \vdots \\ \beta^{rti_1} & \beta^{rti_2} & \dots & \beta^{rti_r} \end{bmatrix}.$$

Thus $\det L = 0$ if and only if $\det L_1 = 0$. Since $\det L_1$ is a Vandermonde determinant, it follows that

$$\det L_1 = \pm \prod_{0 \le j < k \le r+1} (\beta^{ti_j} - \beta^{ti_k}).$$

Hence, $\det L_1 = 0$ if and only if there exists $j, k \in \mathbb{Z}$ with $j < k$ such that $\beta^{ti_j} = \beta^{ti_k}$. Now,

$$\beta^{ti_j} = \beta^{ti_k} \leftrightarrow \beta^{t(i_j - i_k)} = 1 \leftrightarrow t(i_j - i_k) \equiv 0 \pmod{6n}.$$

However, $\gcd(t, 6n) = s \le 6$ implies that $\gcd(\frac{t}{s}, \frac{6n}{s}) = 1$. Suppose that $t(i_j - i_k) \equiv 0 \pmod{6n}$. Thus $6n \mid t(i_j - i_k)$. Hence, $\frac{6n}{s} \mid \frac{t}{s}(i_j - i_k)$, and then, $\frac{6n}{s} \mid (i_j - i_k)$, because $\gcd(\frac{t}{s}, \frac{6n}{s}) = 1$. Since $6 \ge s$ and $(i_j - i_k) \le n-1$, then $\frac{6n}{s} \ge n$, and therefore $\frac{6n}{s} > (i_j - i_k)$, that is, $\frac{6n}{s}$ cannot divide $(i_j - i_k)$. Hence, $t(i_j - i_k) \not\equiv 0 \pmod{6n}$, which implies that $\beta^{ti_j} \neq \beta^{ti_k}$, for $i < k$. Thus $\det L_1 \neq 0$, and consequently, the $r+1$ columns of $H$ are linearly independent. □

The following two corollaries are immediate consequences of Propositions 1 and 2.

**Corollary 1** *Let $C$ be the code defined by the parity-check matrix*

$$H = \begin{bmatrix} 1 & \beta & \dots & \beta^{n-1} \\ 1 & \beta^{t+1} & \dots & (\beta^{t+1})^{n-1} \\ \vdots & \vdots & \dots & \vdots \\ 1 & \beta^{rt+1} & \dots & (\beta^{rt+1})^{n-1} \end{bmatrix}, \quad (19)$$

*with $(t, p-1) \le 6$, $0 \le r < (p-1)/6$, $t < p-1$. Then the minimum Hamming distance of $C$ is $d^H(C) = r+2$. Therefore code $C$ can correct up to $\lfloor (r+1)/2 \rfloor$ (Hamming) errors.*

**Corollary 2** *Code $C$ defined by the parity-check matrix $H$ in 5, under the hypotheses of Corollary 1, are MDS with respect to the Hamming distance.*

All the results in this section hold if we consider the prime number $p \equiv 1 \pmod 4$, $n = (p-1)/4$, $(t, p-1) \le 4$ and $\beta$ replaced by $\alpha$, where $\alpha$ is an element of $\mathcal{A}$ of order $4n = p-1$, such that $\alpha^n = i$ and $\mathbb{A} = \mathbb{Z}[i]$.

## 6. MULTIPLE ERROR CORRECTION

The purpose of this section is to show how to make use of the Berlekamp-Massey algorithm [2], [7], and of Forney's procedure [5] to decode codes over algebraic integers when multiple Hamming errors occur. We focus mainly on codes over the algebraic integers of $\mathbb{Q}(\sqrt{-3})$. However, it is straightforward to adapt the results to $\mathbb{Q}(\sqrt{-1})$.

Let $C$ be the code defined by the parity-check matrix,

$$H = \begin{bmatrix} 1 & \beta & \beta^2 & \dots & \beta^{n-1} \\ 1 & \beta^7 & \beta^{14} & \dots & (\beta^7)^{n-1} \\ \vdots & \vdots & \vdots & \dots & \vdots \\ 1 & \beta^{6t+1} & \beta^{2(6t+1)} & \dots & \beta^{(n-1)(6t+1)} \end{bmatrix},$$

where $\beta \in \mathcal{A} \cong GF(p)$, $p \equiv 1 \pmod 6$ is a prime number, $o(\beta) = 6n$, and $t < n$.

Let $e(x) = e_{j_1}x^{j_1} + e_{j_2}x^{j_2} + \dots + e_{j_\nu}x^{j_\nu}$ be the error pattern, where $\nu \le \lfloor (t+1)/2 \rfloor$ represents the number of symbols in error in the received codeword. The syndromes $T_i$ are given by

$$T_i = S_{6i-5} = e(\beta^{6i-5}) \quad (20)$$

$$= e_{j_1}(\beta^{6i-5})^{j_1} + e_{j_2}(\beta^{6i-5})^{j_2} + \dots + e_{j_\nu}(\beta^{6i-5})^{j_\nu}, \quad (21)$$

for $i = 1, 2, \dots, t+1$.

Let

$$Y_i = e_{j_i}, \quad i = 1, 2, \cdots, \nu,$$

and

$$X_i = \beta^{j_i}, \quad i = 1, 2, \cdots, \nu.$$

Then

$$T_i = \sum_{j=1}^{\nu} Y_j \cdot X_j^{6i-5}, \quad i = 1, 2, \dots, t+1. \quad (22)$$

Now let $\sigma(X)$ be the error locator polynomial, defined by

$$\sigma(X) = \prod_{j=1}^{\nu}(X - X_j^6) = X^\nu + \sigma_1 X^{\nu-1} + \dots + \sigma_{\nu-1}X + \sigma_\nu, \quad (23)$$

where $\sigma_1, \sigma_2, \dots, \sigma_\nu$ are the elementary symmetric functions of the error location numbers $X_1^6, X_2^6, \dots, X_\nu^6$.

Multiplying the equation in (23) by $Y_j X_j^{6i-5}$ and substituting $X_j^6$ for $X$ in the same equation, we get

$$Y_j X_j^{6(i+\nu)-5} + \sigma_1 Y_j X_j^{6(i+\nu-1)-5} + \dots \quad (24)$$

$$+ \sigma_{\nu-1} Y_j X_j^{6(i+1)-5} + \sigma_\nu Y_j X_j^{6i-5}, \quad 1 \le j \le \nu. \quad (25)$$

Now summing the equations in (24) for $1 \le j \le \nu$ and making use of equation (22) yield

$$T_{i+\nu} + \sigma_1 T_{i+\nu-1} + \dots + \sigma_{\nu-1} T_{i+1} + \sigma_\nu T_i = 0, \quad i = 1, \dots, t+1.$$

This is a set of linear equations that relates the syndromes to the coefficients of $\sigma(X)$. The first $\nu$ equations can be written in matrix form as

$$\begin{bmatrix} T_1 & T_2 & \cdots & T_\nu \\ T_2 & T_3 & \cdots & T_{\nu+1} \\ \vdots & \vdots & \dots & \vdots \\ T_\nu & T_{\nu+1} & \cdots & T_{2\nu-1} \end{bmatrix} \begin{bmatrix} \sigma_\nu \\ \sigma_{\nu-1} \\ \vdots \\ \sigma_1 \end{bmatrix} = \begin{bmatrix} -T_{\nu+1} \\ -T_{\nu+2} \\ \vdots \\ -T_{2\nu} \end{bmatrix}, \quad (26)$$

where $T_i = S_{6i-5}$

This equation has a unique solution if and only if the syndrome matrix $(T_j)_{\nu \times \nu}$ is nonsingular.

**Proposition 3** *The syndrome matrix*

$$M = \begin{bmatrix} T_1 & T_2 & \cdots & T_\mu \\ T_2 & T_3 & \cdots & T_{\mu+1} \\ \vdots & \vdots & \dots & \vdots \\ T_\mu & T_{\mu+1} & \cdots & T_{2\mu-1} \end{bmatrix}$$

*equivalently,*

$$\begin{bmatrix} S_1 & S_7 & \cdots & S_{6\mu-5} \\ S_7 & S_{13} & \cdots & S_{6\mu+1} \\ \vdots & \vdots & \cdots & \vdots \\ S_{6\mu-5} & S_{6\mu+1} & \cdots & S_{12\mu-11} \end{bmatrix},$$

*is nonsingular if $\mu = \nu$. If $\mu > \nu$ then $M$ is singular.*

**Proof**: Consider the matrices

$$A = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ X_1^6 & X_2^6 & \cdots & X_\mu^6 \\ \vdots & \vdots & \cdots & \vdots \\ X_1^{6\mu-6} & X_2^{6\mu-6} & \cdots & X_\mu^{6\mu-6} \end{bmatrix},$$

and

$$B = \begin{bmatrix} Y_1X_1 & 0 & \cdots & 0 \\ 0 & Y_2X_2 & \cdots & 0 \\ \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & Y_\mu X_\mu \end{bmatrix},$$

where $Y_j = X_j = 0$ if $j > \nu$. Using the equations in (22), it is easy to verify that $M = ABA^t$, where $A^t$ denotes transpose of $A$. Thus

$$\det M = \det A \cdot \det B \cdot \det A^t.$$

If $\mu = \nu$, then $\det B = \prod_{i=1}^{\nu} Y_iX_i$ is nonzero for the elements $Y_i$ and $X_i$, $i = 1, 2, \ldots, \nu$, are nonzero. Also, $\det A$ is nonzero for $A$ is a Vandermonde matrix and the elements $X_i, i = 1, 2, \ldots, \nu$, are distinct pairwise. Hence, $\det M \neq 0$, and therefore, $M$ is nonsingular. On the other hand, if $\mu > \nu$, then $\det B = 0$, which implies that $\det M = 0$, and therefore $M$ is singular. □

Thus, whenever the Hamming weight of the error pattern is less than or equal to $\nu$, it is possible to determine the positions in error in the received vector, by solving the linear system of equations in (26). This set of equations can be efficiently solved in the unknowns $\sigma_1, \ldots, \sigma_\nu$ by the Berlekamp-Massey algorithm [2],[7]. Then, knowing $\sigma_1, \ldots, \sigma_\nu$ enables us to determine the error locator polynomial whose roots are $X_1^6, X_2^6, \cdots, X_\nu^6$ (where $X_i = \beta^{j_i}, i = 1, 2, \cdots, \nu$ are the error locator numbers), and they can be found by Chien search [3]. From these roots, the error positions are easily determined.

Finally, the error values are determined from the equations in (20), which can be solved by Forney's procedure [5]. By using standard methods, see for example, [5], [6], it is not difficult to show that each error magnitude $Y_j$, $1 \leq j \leq \nu$, can be determined by

$$Y_j = \frac{\sum_{l=0}^{\nu-1} \sigma_{jl} \cdot T_{\nu-l}}{X_j^{-5} \cdot \sum_{l=0}^{\nu-1} \sigma_{jl} \cdot X_j^{6(\nu-l)}}, \qquad (27)$$

where $1 \leq j \leq \nu$, and the coefficients $\sigma_{jl}$ can be recursively calculated by

$$\sigma_{ji} = \sigma_i + X_j^6 \cdot \sigma_{j,i-1}.$$

## REFERENCES

[1] K. Huber, "Codes over Gaussian integers," *IEEE Trans. Inform. Theory*, vol. 40, No. 1, pp. 207-216, Jan. 1994.

[2] E.R. Berlekamp, *Algebraic Coding Theory*, Aegean Park Press, 1984.

[3] R.T. Chien, "Cyclic decoding procedure for the Bose-Chaudhuri-Hocquenghem codes," *IEEE Trans. Inform. Theory*, vol. IT-10, pp. 357-363, 1964.

[4] O.M. Favareto, "Linear block codes over rings of algebraic integers with alphabet matched to $GF(p)$" (in Portuguese), Ph.D. dissertation, Universidade Estadual de Campinas (UNICAMP), Campinas, Brazil, 1996.

[5] G.D. Forney, Jr., "On decoding BCH codes," *IEEE Trans. Inform. Theory*, vol. IT-11, pp. 549-557, October 1965.

[6] W.W. Peterson and E.J. Weldon, Jr., *Error Correcting Codes*, 2nd. edition, MIT Press, Cambridge, MA, 1972.

[7] J.L. Massey, "Shift-register synthesis and BCH decoding," *IEEE Trans. Inform. Theory*, vol. 15, No. 1, pp. 122-127, January 1969.

[8] P. Samuel, *Algebraic Theory of Numbers*, Paris, France: Hermann, 1971.

**Osvaldo Milaré Favareto** formou-se em Matemática é pelo IBILCE, São José do Rio Preto em 1972,concluiu seu mestrado em Matemática pelo Departamento de Matemática da Universidade de Brasília em 1975, e após o que foi professor do Departamento de Matemática da UFPB, campus João Pessoa, PB., até julho de 1998. Em dezembro de 1996 concluiu seu doutorado na Faculdade de Engenharia Elétrica e de Computação da UNICAMP apresentando a tese Códigos de Bloco Lineares sobre Anéis de Inteiros Algébricos Casado a GF(p). Atualmente é professor no Departamento de Matemática e Estatística da Universidade Federal da Paraíba em Campina Grande.

**Trajano Nóbrega Neto** was born in Malta, Brazil, on April 28, 1957. He received his B.S. degree in mathematics in 1980, MS and the Ph.D. degree in mathematics in 1984 and 1991, respectively, both from the State University of Campinas (UNICAMP), Campinas, Brazil. Since July of 1984 he has been with the Department of Mathematics at the State University of São Paulo (UNESP), campus of São José do Rio Preto, as an assistant professor. He has advised one PH.D. thesis and two M.S. dissertations. Dr. Trajano is a member of the SBM(Sociedade Brasileira de Matemática) and his reserach interests include Number Theory, error-correcting codes over rings and groups, lattices, algebraic decoding of block codes.

**J. Carmelo Interlando** was born in Campo Grande, Brazil, on June 10, 1969. He received his B.S. degree in applied mathematics in 1990, and the Ph.D. degree in eletrical engineering in 1994, both from the State University of Campinas (UNICAMP), Campinas, Brazil.

He spent one yer (1993) as a visiting scholar at the University of Notre Dame, IN, USA. doing research toward his doctorate. From January of 1995 to June of 1996, he was an associate research at the State University of Campinas (UNICAMP), where he co-advised two Ph.D. candidates, taught a graduate course, and worked on several of his now published papers. Since July of 1996 he has been with the Department of Mathematics at the State University of São Paulo (UNESP), campus of São José do Rio Preto, as an assistant professor. Dr. Interlando is a member of the IEEE and his research interests include error-correcting codes over rings and groups, Z4-linear codes, algebraic-geometry codes, coded modulation, lattices, algebraic decoding of block codes.

**Reginaldo Palazzo JR.** received the Electrical Engineering and MSEE degrees from University Estadual de Campinas - UNICAMP, SP, Brazil, in 1975 and 1977 respectively, and the Engineer and PH.D. degrees from the University of California,Los Angeles, CA, USA, in 1981 and 1984, respectively,. In May 1985 he joined the Faculty of Eletrical and Computing Engineering, UNICAMP, where he received the Livre-Docência degree in 1987. Since 1996 he is a Professor and Chair of the Algebraic and Geometric Coding Group. His research interests are in coding, information, and communication theory.