Erratum to ”Lattice constellation and codes from quadratic number fields” [IEEE Trans. Inform. Theory, vol. 47, No. 4, May. 2001]

Murat Güzeltepe
Department of Mathematics, Sakarya University, TR54187 Sakarya, Turkey

Abstract

We correct a partial mistake for a metric presented in the article ”Lattice constellation and codes from quadratic number fields” [IEEE Trans. Inform. Theory, vol. 47, No. 4, May. 2001]. We show that the metric defined in the article is not true, therefore, this brings about to destroy the encoding and decoding procedures. Also, we define a proper metric for some codes defined in the article and show that there exist some 1–error correcting perfect codes with respect to this new metric.

AMS Classification: 94B05, 94B60
Keywords: Block codes, Mannheim distance, Cyclic codes, Syndrome decoding

1 Introduction and preliminaries

In this Section, we show that the metric defined in [1] is not a true metric. Later, we define a proper Mannheim distance over $A_p[w]$. Note that the metric given in [1] is inspired by the Mannheim metric introduced in [2]. Unfortunately, it is proved that the Mannheim metric is incorrect in [3].

In [1], labeling procedure for the elements of $A_p[w]$ by elements of the Galois field of order $p$, $GF(p)$, has been given as follows:

i) Given a prime $p$ that splits completely over $Z[w]$, let $\pi = a + bw$ be a solution of $N(\pi) = a\overline{\pi} = p$, where $Z$ denotes the set of all integers, and $\overline{\pi}$ denotes the conjugate of $\pi$.

ii) Let $s \in Z$ be the only solution (in $r$) to the equation $a + br \equiv 0 \pmod{p}$, where $0 \leq r \leq p - 1$.

iii) The element $l \in GF(p)$ is the label of the point $\alpha = x + yw \in Z[w]$ if $x + sy \equiv l \pmod{p}$ and $N(\alpha)$ is minimum.

Example 1 Let $d = -3$ and $p = 7 \equiv 1 \pmod{6}$.

i) A solution to the equation $N(\alpha) = a^2 + ab + \frac{1-d}{4}b^2 = 7$ is given by $(a, b) = (1, 2)$. Thus, we can take $\pi = 1 + 2w$.

ii) The only solution to the equation $1 + 2r \equiv 0 \pmod{7}$, where $0 \leq r \leq 6$ is 3.
iii) The element \( l \) is the label of the point \( \alpha = x + yw \in \mathbb{Z}[w] \), if \( x + 3y \equiv l \pmod{7} \) and \( N(\alpha) \) is minimum. Hence, the set \( \mathcal{A}_7[w] \) is obtained as \( \{0, \pm 1, \pm w, \pm w^2 \equiv \pm \omega \} \). The set \( \mathcal{A}_7[w] \) is a finite field.

**Example 2** Let \( d = -3 \) and \( p = 193 \equiv 1 \pmod{6} \).

i) A solution to the equation \( N(\alpha) = a^2 + ab + \frac{1-d}{4}b^2 = 7 \) is given by \((a, b) = (7, 9)\). Thus, we can take \( \pi = 7 + 9w \).

ii) The only solution to the equation \( 7 + 9r \equiv 0 \pmod{193} \), where \( 0 \leq r \leq 192 \) is 85.

iii) The element \( l \) is the label of the point \( \alpha = x + yw \in \mathbb{Z}[w] \), if \( x + 85y \equiv l \pmod{193} \) and \( N(\alpha) \) is minimum. Some elements of the finite field \( \mathcal{A}_{193}[w] \) are \( 9 \equiv -7 + 7w, 94 \equiv 2 - 8w, 108 \equiv -w \pmod{(7 + 9w)} \).

**Definition 1** [\( \mathcal{E} \)] Given an element \( \gamma = x + yw \in \mathcal{A}_p[w] \), the Mannheim weight of \( \gamma \) is defined as

\[ W_M(\gamma) = |x| + |y|. \]

Also, the Mannheim distance between any two elements \( \alpha \) and \( \beta \) in \( \mathcal{A}_p[w] \) is defined as

\[ d_M(\alpha, \beta) = W_M(\delta), \]

where \( \delta \equiv \alpha - \beta \pmod{p} \), \( \delta \in \mathcal{A}_p[w] \) with \( N(\delta) \) minimum.

But, \( d_M(\alpha, \beta) = W_M(\delta) \) is not a true metric since it does not fulfill the triangular inequality.

**Example 3** Let \( d = -3 \) and \( p = 193 \equiv 1 \pmod{6} \). Then, \( \pi = 7 + 9w \) and \( r = 85 \). Consider \( \mathcal{A}_{193}[w] \) and the elements \( x = -6 + 7w, y = 1, \) and \( z = 1 - w \). The inequality

\[ d_M(x, y) \leq d_M(x, z) + d_M(z, y) \]

should be verified, but this is not true:

- \( d_M(x, y) = 14 \) since \( x - y = -7 + 7w \) with minimum norm \( N(-7 + 7w) = 49 \);
- \( d_M(x, z) = 10 \) since \( x - z = 2 - 8w \) with minimum norm \( N(2 - 8w) = 52 \);
- \( d_M(z, y) = 1 \) since \( z - y = -w \) with minimum norm \( N(-w) = 1 \).

Now, we define a Mannheim metric over \( \mathcal{A}_p[w] \).

We denote the set of units in \( \mathcal{A}_p[w] \) by \( \mathcal{E} \). It is easy to check that \( \mathcal{E} \) is the union of a set as indicated below:

\[ \mathcal{E} = \{ \mp 1, \mp \omega, \mp \omega^2 \}. \]

We note that for any two distinct elements \( e_1 \) and \( e_2 \) in \( \mathcal{E} \)

\[ N(e_1 - e_2) \in \{1, 2, 3, 4\}. \]

Hence, if \( \pi \pi \) is equal to a prime number \( p \geq 7, p \equiv 1 \pmod{6} \) we may conclude that the elements in \( \mathcal{E} \) represent 6 distinct elements in \( \mathcal{A}_p[w] \).
Consider the direct product $S = A_p[w]^n$ of $n$ copies of $A_p[w]$. We say that two elements, or words, $\bar{x}$ and $\bar{y}$ in $A_p[w]^n$ have distance one, $d_m(\bar{x}, \bar{y}) = 1$, if there is a word $\bar{e} = (0, \ldots, 0, e, 0, \ldots, 0)$, with just one non-zero entry such that 

$$\bar{y} = \bar{x} + \bar{e},$$

for a unique element $e$ in a set $E$.

With terminology from graph theory, it is now easy to explain how we can define a metric in $A_p[w]^n$. Consider the words of $S$ as vertices in a graph, where there is an edge between two vertices $\bar{x}$ and $\bar{y}$ if $d_m(\bar{x}, \bar{y}) = 1$. The distance $d_m(a, b)$ between any two vertices $a$ and $b$ is the length of the shortest path between these two vertices. General results from graph theory give that this distance function defines a metric in $S$.

If $E$ is defined as in Eq. (1), then the metric obtained in $A_p[w]^n$ is called the Mannheim metric.

We can give an alternative Mannheim metric which is equivalent to above definition.

For this, we first give a modulo function from the Galois field $GF(p)$ to the $A_p[w]$.

**Definition 2** Let $\pi = a + bw$ such that $\pi \pi = p = a^2 + ab + b^2 \equiv 1 \pmod{(6)}$, where $p$ is a prime and $a, b \in \mathbb{Z}$. We define the modulo function $\mu : GF(p) \rightarrow A_p[w]$ as

$$\mu(l) = \begin{cases} x + yw, & |x| + |y| \leq |x'| + |y'| \\ x' + y\overline{w}, & |x| + |y| > |x'| + |y'| \end{cases}.$$

Here, $x + ry \equiv l \pmod{p}$ and $x + yw = x' + y\overline{w}$, where $a + br \equiv 0 \pmod{p}$, $0 \leq r \leq p - 1$.

For example, $w^2 = -1 + w = -\overline{w}$. So, $x, y, x', y'$ are $-1, 1, 0, -1$, respectively.

**Example 4** Let $p = 7 \equiv 1 \pmod{(6)}$. Then, $\pi = 1 + 2w$. The only solution to the equation $1 + 2r \equiv 0 \pmod{(7)}$, where $0 \leq r \leq 6$ is 3. Thus, we obtain the elements of $A_7[w]$ using by the modulo function $\mu$ as

$$\mu(0) = 0; \quad \mu(1) = 1; \quad \mu(2) = -\overline{w}; \quad \mu(3) = w; \quad \mu(4) = -w; \quad \mu(5) = \overline{w}; \quad \mu(6) = -1.$$

Hence, we obtain $A_7[w] = \{0, \pm 1, \pm w, \pm \overline{w}\}$.

**Definition 3** Given an element $\gamma = x + yw = x' + y'\overline{w}$ in $A_p[w]$, we define the Mannheim weight of $\gamma$ as

$$W_m(\gamma) = \begin{cases} |x| + |y|, & |x| + |y| \leq |x'| + |y'| \\ |x'| + |y'|, & |x| + |y| > |x'| + |y'| \end{cases}.$$
We also define the Mannheim distance between any two elements \( \alpha \) and \( \beta \) in \( A_p[w] \) as

\[
d_m(\alpha, \beta) = W_m(\delta),
\]

where \( \delta \equiv \alpha - \beta \pmod{\pi} \), \( \delta \in A_p[w] \).

It should be noted that, in general, the Mannheim distance \( d_M \) defined in \( \Pi \) and the Mannheim distance \( d_m \) given here are not isomorphic, as shown in the next example.

**Example 5** Consider \( A_p[w]^1 \) and the elements \( 1 \) and \( \pm w^2 \). We note that

\[
d_M(1, 0) = W_M(1) = 1 = d_m(1, 0) = W_m(1)
\]

while

\[
d_M(\pm w^2, 0) = W_M(\pm w^2) = 2 \neq 1 = d_m(\pm w^2, 0) = W_m(\pm w^2).
\]

## 2 1–Error-Correcting Perfect Codes

In this section, \( \beta \) will denote an element of order \( 6n = p - 1 \) such that \( \beta^n = w \). Thus, \( \beta \) is a primitive element of \( A_p[w] \).

Let \( p = 6n + 1 \) be a prime in \( \mathbb{Z} \) which factors in \( \mathbb{Z}[w] \) as \( \pi \overline{\pi} \), where \( \pi \) is a prime in \( \mathbb{Z}[w] \). Let \( \beta \) denote an element of

\[
A_p[w] \cong \mathbb{Z}[w]/\langle \pi \rangle
\]

of order \( 6n \). Hence \( \beta^n = w \), and since \( \beta \) is a primitive element of \( A_p[w] \), it can written \( A_p[w] = \langle \beta \rangle \cup \{0\} \). Now let \( C \) be the null-space of the matrix

\[
H = \begin{pmatrix}
1 & \beta & \beta^2 & \cdots & \beta^{n-1} \\
1 & \beta^7 & \beta^{14} & \cdots & \beta^{7(n-1)} \\
\vdots & \vdots & \vdots & \cdots & \vdots \\
1 & \beta^{6t+1} & (\beta^{6t+1})^2 & \cdots & (\beta^{6t+1})^{(n-1)}
\end{pmatrix}
\]

where \( t < n \). An \( n \)-tuple

\[
c = (c_0, c_1, \cdots, c_{n-1}) \in A_p^n[w]
\]

is a codeword of \( C \) if and only if \( Hc^t = 0 \), where \( c^t \) denotes the transpose of \( c \). If \( c(x) = \sum_{i=0}^{n-1} c_i x^i \) is the associated code polynomial, we get

\[
c(\beta^{6j+1}) = 0, \text{for } j = 0, 1, \cdots, t.
\]

The polynomial \( g(x) = (x-\beta)(x-\beta^7) \cdots (x-\beta^{6t+1}) \) is the generator polynomial of \( C \), and \( C = \langle g(x) \rangle \) is an ideal of \( A_p[w][x]/(x^n - w) \). If multiplying a code polynomial \( c(x) \) by \( x \pmod{x^n - w} \), we get

\[
xc(x) = c_0 x + c_1 x^2 + \cdots + c_{n-1} x^n,
\]

which belongs to \( C \). We know that \( x^n = w \). Therefore, if \( c(x) \in C \), then \( xc(x) \in C \). Thus, multiplying \( c(x) \) by \( x \pmod{x^n - w} \) means the following:
1. Shifting $c(x)$ cyclically one position to the right;

2. Rotating the coefficient $c_{n-1}$ by $\pi/3$ radians in the complex plane and substituting it for the first symbol of the new codeword.

Therefore, code $C$ defined by the parity check matrix in (1) is a $w$-cyclic codes by considering a primitive root $\beta$ such that $\beta^n = w$.

**Theorem 1** Let $C$ be the null-space of the matrix

$$H = \begin{pmatrix} 1 & \beta & \beta^7 & \cdots & \beta^{n-1} \end{pmatrix}.$$  \hspace{1cm} (4)

Then $C$ is able to correct any error pattern of the form $e(x) = e_ix^i$, where $W_m(e_i) = 1$.

The proof of Thm. 1 is the same as the proof of Thm. 7 in [1].

Recall that the elements of Mannheim weight 1 of the alphabet $A_p[w]$ are $\pm 1$, $\pm w$, $\pm \overline{w}$. By the sphere-packing we get

$$p^{n-1}(6n+1) = p^{n-1}p = p^n.$$  

Hence, the codes defined by the parity check matrix in (4) are perfect.

**References**

[1] T. P. da N. Neto, J. C. Interlando., "Lattice constellation and codes from quadratic number fields," IEEE Trans. Inform. Theory, vol. 47, No. 4, May. 2001.

[2] K. Huber., "Codes Over Gaussian integers," IEEE Trans. Inform. Theory, vol. 40, pp. 207-216, Jan. 1994.

[3] C. Martinez, R. Beivide and E. Gabidulin., "Perfect codes for metrics induced by circulant graphs," IEEE Trans. Inform. Theory, vol. 53, No. 9, Sep. 2007.