Journal of Applied Mathematics and Computation (JAMC), 2017, 1(1), 8-12
http://www.hillpublisher.org/journal/jamc
ISSN Online:2576-0645
ISSN Print:2576-0653

On Perfect Codes Over $A_p[w]$

Murat Güzeltepe

Department of Mathematics, Sakarya University, TR54187 Sakarya, TURKEY

How to cite this paper: Murat Güzeltepe (2017) ON PERFECT CODES OVER $A_p[w]$. *Journal of Applied Mathematics and Computation*, **1(1)**, 8-12.
http://dx.doi.org/10.26855/jamc.2017.01.002

Corresponding author: Murat Güzeltepe, Department of Mathematics, Sakarya University, TR54187 Sakarya, TURKEY

Abstract

In this paper, we study on error correcting perfect codes over $A_p[w]$ with respect to the Mannheim metric.

Keywords

Block codes, Mannheim distance, Cyclic codes, Syndrome decoding.

1. Introduction

Coding theorists and mathematicians have always been fascinated perfect codes since they are important in coding theory for theoretical and practical reasons. Some perfect codes in the Hamming metric are known [8]. Some perfect codes in the Lee metric was given in [9]. A survey of perfect binary codes can be found in [10]. A kind of classification of all perfect $1-$error-correcting $q-$ary codes can be found in [11]. More recent perfect codes can be found in[12, 13, 14, 15].

On the other hand, Hamming and Lee's distances have been revealed to be inappropriate metrics to deal with quadrature amplitude modulation (QAM) signal sets and other related constellations. To solve this problem, different authors have constructed new error−correcting codes over fields or rings. For example, Huber discovered a new way to construct codes for two−dimensional signals over Gaussian integers [2]. Huber's method is to regard a finite field as a residue field of the Gaussian integer ring modulo a Gaussian prime and, by Euclidean division to get a unique element of the minimal norm in each residue class, which represents each element of the finite field. So, each element of these fields can be represented by a Gaussian integer with the minimal Euclidean norm in the residue class. These sets constructed by Gaussian integers are called constellation. Since the Galois norm of integral points on the complex plane coincides with the Euclidean metric, Huber's constellation is of minimal energy. Moreover, Huber introduced the Mannheim weight by means of the Manhattan metric of the constellation, and defined one error correcting Mannheim codes. In [3], Huber developed his wonderful idea further to the Eisenstein integers, i.e., the algebraic integers of the cyclotomic field generated by the sixth roots of unity. Although Huber's work constitutes a relevant contribution, unfortunately, the Mannheim distance is not a true metric as was proved in [5]. C. Martinez *et al.* obtained perfect codes for metrics induced by circulant graphs in [4]. Later, T. P. da Nobrega Neto *et al.* in [1] discussed the algebraic integer rings of quadratic fields which are the Euclidean norm, and proposed a new class of linear codes. In [1], codes over the ring $\mathbb{Z}[i]$ of Gaussian integers and codes over the ring $A_p[\rho]$ of Eisenstein-Jacobi integers were presented. The metric used in [1] is inspired by Mannheim metric. In this study, we show that the metric defined in [1] is not a true metric. Also, we define a proper Mannheim metric and we obtain perfect codes over the finite fields $A_p[w]$ with respect to this metric. One error correcting perfect code was not obtained in [1]. In this study, we obtain perfect codes over $A_p[w]$ with respect to the Mannheim metric.

2. Mannheim Distance over $A_p[w]$

In this Section, we show that the metric defined in [1] is not a true metric. Later, we define a proper Mannheim distance over $A_p[w]$. Here and there after w will denote $\frac{1+i\sqrt{3}}{2}$, $i^2=-1$.

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

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

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

iii) The element $l\in GF(p)$ is the label of the point $\alpha=x+yw\in\mathbb{Z}[w]$ 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 $1+2r\equiv 0 \pmod{7}$ is 3, where $0\le r\le 6$.

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 $A_7[w]$ is obtained as $\{0,\pm 1,\pm w,\pm w^2\}$. The set $A_7[w]$ is a finite field.

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

i) A solution to the equation $N(\alpha)=a^2+ab+\frac{1-d}{4}b^2=193$ is given by $(a,b)=(7,9)$. Thus, we can take $\pi=7+9w$.

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

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 $A_{193}[w]$ are $9\equiv -7+7w, 94\equiv 2-8w, 108\equiv -w \pmod{(7+9w)}$.

Definition1. [1] Given an element $\gamma=x+yw\in A_p[w]$, the Mannheim weight of γ is defined as

$W_M(\gamma)=|x|+|y|$.

Also, the Mannheim distance between any two elements α and β in $A_p[w]$ is defined as

$d_M(\alpha,\beta)=W_M(\delta)$,

where $\delta\equiv\alpha-\beta \pmod{\langle\pi\rangle}, \delta\in A_p[w]$ 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 $A_{193}[w]$ and the elements $x=-6+7w, y=1,$ and $z=1-w$. It should be verify that

$d_M(x,y)\le d_M(x,z)+d_M(z,y)$.

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 the Mannheim metric over $A_p[w]$. 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 $\pi\bar{\pi}=p=a^2+ab+b^2\equiv 1(\bmod 6)$, where p is a prime and $a,b\in\mathbb{Z}$. We define the modulo function $\mu: GF(p)\to A_p[w]$ by

$$\mu(l)=\begin{cases} x+yw, & |x|+|y|\le|x'|+|y'| \\ x'+y'\bar{w}, & |x'|+|y'|<|x|+|y|. \end{cases}$$

Here, $x+ry\equiv l\ (mod\ p)$ and $x+yw=x'+y'\bar{w}$, where $a+br\equiv 0\ (mod\ p)$, $0\le r\le p-1$.

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

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

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

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

$$W_m(\gamma)=|x|+|y|$$

with $|x|+|y|$ minimum. Also, we define the Mannheim distance between any two elements α and β in $A_p[w]$, as

$$d_m(\alpha,\beta)=W_m(\delta),$$

where $\delta\equiv\alpha-\beta\ (mod\ \pi)$, $\delta\in A_p[w]$.

It should be noted that our Mannheim distance d_m is not the same as the Mannheim distance d_M defined in [1]. To see this, consider the elements $\pm w^2$. The Mannheim weight defined in [1] of the elements $\pm w^2$ are

$$d_M(\pm w^2)=2.$$

The Mannheim weight of the same elements are $d_m(\pm w^2)=1$ since $w^2=-\bar{w}$ and $-w^2=\bar{w}$.

3. Single-Error-Correcting Perfect Codes

In this section, β will denote an element of order $6n = p-1$ such that $\beta^n = w$. Thus, β 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 $\pi\bar{\pi}$, where π is a prime in $\mathbb{Z}[w]$. Let β denotes an element of

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

of order $6n$. Hence $\beta^n = w$, and since β is a primitive element of $A_p[w]$, it can written $A_p[w] = \langle \beta \rangle \cup \{0\}$.

Now let C be the code defined by the parity-check matrix

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

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 $A_p[w][x] \big/ \langle x^n - w \rangle$. If multiplying a code polynomial $c(x)$ by $x \ (\mathrm{mod}\,(x^n - w))$, 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 $x(\mathrm{mod}(x^n - w))$ means the following:

- Shifting $c(x)$ cyclically one position to the right;
- 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 an $w-$ cyclic codes by considering a primitive root β such that $\beta^n = w$.

Theorem 1. Let C be the code defined by the parity check matrix

$$H = \begin{pmatrix} 1 & \beta & \beta^7 & \cdots & \beta^{n-1} \end{pmatrix}. \tag{2}$$

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

Proof: Let $r(x) = c(x) + e(x)$ be the received polynomial, where $c(x)$ denotes the codeword polynomial $e(x) = e_l x^l$ denotes the error polynomial with $e_l = \beta^{an}$. The vector corresponding to the polynomial $r(x)$ is $r = c + e$. Then, the syndrome S of r is

$S = Hr^T = \beta^{l+an} = \beta^L$,

where $L, l \in \mathbb{Z}, 0 \le l \le n-1$. By reducing L modulo n, we determine the location l of the error, and next a is determined by $a = (L-l)/n$. Hence, we have the location and the value of the error.

Recall that the elements of Mannheim weight 1 of the alphabet $A_p[w]$ are $\pm 1, \pm w, \pm \bar{w}$. By 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 (2) are perfect.

Example 5. Let $p = 13$. Then, $\pi = 3 + w$, $r = 10$. Using the procedure given in Def.2, we obtain the set $A_{13}[w]$ as $\{0, \mp 1, \mp w, \mp \bar{w}, \mp 2w, \mp(1+w), \mp(1+\bar{w})\}$.
If we take $\beta = 2w$, since $\beta^{(p-1)/6} = \beta^2 = w$, the code C of the null space of the parity check matrix
$H = (1, \quad \beta) = (1, \quad 2w)$
defines a single-error-correcting perfect code over $A_{13}[w]$. The code C has 13 codewords. The number of the all words in the vector space $A_{13}^2[w]$ is 13^2. The elements of Mannheim weight 1 of the alphabet $A_p[w]$ are $\pm 1, \pm w, \pm \bar{w}$. By sphere-packing we get
$13^{2-1}(12+1) = 13^2$.

Acknowledgement

The work was supported by TUBİTAK (The Scientific and Technical Research Council of TURKEY) with project number 116F318. 2000 Mathematics Subject Classification. 94B05, 94B60.

4. 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] K. Huber., "Codes Over Eisenstein-Jacobi integers," AMS. Contemp. Math., vol. 158, pp.165-179, 2004.
[4] 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.
[5] C. Martinez, R. Beivide and E. Gabidulin, "Perfect Codes from Cayley Graphs over Lipschitz Integers," IEEE Trans. Inf. Theory, Vol. 55, No. 8, Aug. 2009.
[6] G. Davidoff, P. Sarnak, and A. Valette., Elementary Number Theory, Group Theory, and Ramanujan Graphs, Cambridge University Pres, 2003.
[7] J. H. Conway, D. A. Smith, On Quaternions and Octonions, A K Peters, 2003.
[8] R. W. Hamming, Error Detecting and Error Correcting Codes, Bell System Technical Journal 29(1950), 147160.
[9] C.Y. Lee, "Some properties of non-binary error correcting codes," IEEE Trans. Inform. Theory, vol. 4, pp. 7782, 1958.
[10] O. Heden, "A survey of perfect codes," Advances in Mathematics of Communications, Vol. 2, No. 2, pp. 223 - 247, 2008.
[11] O. Heden, and D. Krotov, "On the structure of non-full-rank perfect $q-$ary codes, "Advances in Mathematics of Communications, Vol. 5, No. 2, pp.149 - 156, 2011.
[12] M. Guzeltepe, O. Heden., "Perfect Mannheim, Lipschitz and Hurwitz weight codes,"Math. Commun. Vol.19, No. 1, pp. 253276, 2014
[13] O. Heden, M. Guzeltepe, "On perfect $1-\varepsilon-$error-correcting codes," Math. Commun. Vol. 20, No. 2, pp. 2335, 2015.
[14] O. Heden, M. Guzeltepe, "Perfect $1-$error-correcting Lipschitz weight codes," Math. Commun. Vol. 21, No. 1, pp. 2330, 2016.
[15] M. Guzeltepe, A. Altinel, "Perfect $1-$error-correcting Hurwitz weight codes", Math. Commun. Vol. 22, No. 2, pp. 265-272, 2017.