Discrete Mathematics 313 (2013) 704–714

Contents lists available at SciVerse ScienceDirect

Discrete Mathematics

journal homepage: www.elsevier.com/locate/disc

Codes over Hurwitz integers

Murat Güzeltepe

Department of Mathematics, Sakarya University, TR54187 Sakarya, Turkey

ARTICLE INFO

Article history:
Received 20 December 2011
Received in revised form 19 October 2012
Accepted 20 October 2012
Available online 10 November 2012

Keywords:
Block codes
Cyclic codes
Syndrome decoding
Hurwitz metric

ABSTRACT

In this study, we obtain new classes of linear codes over Hurwitz integers equipped with a new metric. We refer to the metric as the Hurwitz metric. Also, we define decoding algorithms for these codes when up to two coordinates of a transmitted code vector are affected by the error of arbitrary Hurwitz weight. The interest in the codes with respect to the Hurwitz metric is their use in coded modulation schemes based on quadrature amplitude modulation (QAM)-type constellations where the Hamming metric and the Lee metric are not appropriate.

1. Introduction

Hamming and Lee distances have been revealed to be inappropriate metrics to deal with quadrature amplitude modulation (QAM) signal sets and other related constellations [4]. 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 in terms of Gaussian integers, i.e., the integral points on the complex plane [5]. His original idea 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 minimal norm in each residue class, which represents each element of a finite field. Therefore, each element of a finite field can be represented by a Gaussian integer with the minimal Galois norm in the residue class; and the set of the selected Gaussian integers is called a 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 obtained linear codes which are of one Mannheim error-correcting capability. In [6], 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 [9]. Later, T.P. da Nobrega Neto et al. in [2] discussed the algebraic integer rings of quadratic fields which are Euclidean norm, and proposed a new class of linear codes. In [2], 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 [2] is inspired by the Mannheim metric.

On the other hand, C. Martinez et al. introduced a metric called the Lipschitz metric in [9] and obtained codes over Lipschitz integers with respect to this metric.

In this paper, we introduce the Hurwitz metric over Hurwitz integers and give codes over Hurwitz integers with respect to this metric. Also, we give decoding algorithms of these codes.

In what follows, we consider the following.

Definition 1 (*[3]*). The Hamilton Quaternion Algebra over the set of the real numbers $(\mathbb{R})$, denoted by $H(\mathbb{R})$, is the associative unital algebra given by the following representation:

E-mail address: mguzeltepe@sakarya.edu.tr.

0012-365X/$ – see front matter © 2012 Elsevier B.V. All rights reserved.
doi:10.1016/j.disc.2012.10.020

(i) $H(\mathbb{R})$ is the free $\mathbb{R}$ module over the symbols $1, \widehat{e}_1, \widehat{e}_2, \widehat{e}_3$, that is, $H(\mathbb{R}) = \{a_0 + a_1\widehat{e}_1 + a_2\widehat{e}_2 + a_3\widehat{e}_3 : a_0, a_1, a_2, a_3 \in \mathbb{R}\}$;
(ii) 1 is the multiplicative unit;
(iii) $\widehat{e}_1^2 = \widehat{e}_2^2 = \widehat{e}_3^2 = -1$;
(iv) $\widehat{e}_1\widehat{e}_2 = -\widehat{e}_2\widehat{e}_1 = \widehat{e}_3, \widehat{e}_3\widehat{e}_1 = -\widehat{e}_1\widehat{e}_3 = \widehat{e}_2, \widehat{e}_2\widehat{e}_3 = -\widehat{e}_3\widehat{e}_2 = \widehat{e}_1$.

If $q = a_0 + a_1\widehat{e}_1 + a_2\widehat{e}_2 + a_3\widehat{e}_3$ is a quaternion integer, its conjugate quaternion is $q^* = a_0 - (a_1\widehat{e}_1 + a_2\widehat{e}_2 + a_3\widehat{e}_3)$.

The ring of the integers of the quaternions, or Lipschitz integers is $H(\mathbb{Z}) = \{a_0 + a_1\widehat{e}_1 + a_2\widehat{e}_2 + a_3\widehat{e}_3 : a_0, a_1, a_2, a_3 \in \mathbb{Z}\}$, where $\mathbb{Z}$ is the set of all integers.

The norm of q is $N(q) = qq^* = a_0^2 + a_1^2 + a_2^2 + a_3^2$. The units of $H(\mathbb{Z})$ are $\pm 1, \pm\widehat{e}_1, \pm\widehat{e}_2, \pm\widehat{e}_3$.

Definition 2 (*[9]*). Let π be an odd integer quaternion. If there exists $\delta \in H(\mathbb{Z})$ such that $q_1 - q_2 = \delta\pi$ then $q_1, q_2 \in H(\mathbb{Z})$ are right congruent modulo π and it is denoted as $q_1 \equiv_r q_2$.

This equivalence relation is well-defined. Hence, it can be considered as the quotient ring of the quaternion integers modulo this equivalence relation, which is denoted by

$$H(\mathbb{Z})_\pi = \{q \pmod{\pi} | q \in H(\mathbb{Z})\}.$$

This set coincides with the quotient ring of the integer quaternions over the left ideal generated by π, which is denoted by $\langle\pi\rangle$; see [9].

Definition 3 (*[9]*). Let $\pi \neq 0$ be a Lipschitz integer. Then, the Lipschitz weight of γ is defined as

$$w_L(\gamma) = |a_0| + |a_1| + |a_2| + |a_3|,$$

where

$$\gamma = \alpha - \beta \equiv_r a_0 + a_1\widehat{e}_1 + a_2\widehat{e}_2 + a_3\widehat{e}_3 \pmod{\pi}$$

with $|a_0| + |a_1| + |a_2| + |a_3|$ minimum. Then, the Lipschitz distance d_L between α and β is defined as

$$d_L(\alpha, \beta) = w_L(\gamma).$$

More information related with the arithmetic properties of $H(\mathbb{Z})$ can be found in [8,9,3].

Theorem 1 (*[9]*). *Let $\pi \in H(\mathbb{Z})$. Then $H(\mathbb{Z})_\pi$ has $N(\pi)^2$ elements.*

Definition 4 (*[1]*). The set of all Hurwitz integers is

$$\begin{aligned}\mathcal{H} &= \left\{a_0 + a_1\widehat{e}_1 + a_2\widehat{e}_2 + a_3\widehat{e}_3 \in H(\mathbb{R}) : a_0, a_1, a_2, a_3 \in \mathbb{Z} \text{ or } a_0, a_1, a_2, a_3 \in \mathbb{Z} + \frac{1}{2}\right\}\\ &= H(\mathbb{Z}) \cup H\left(\mathbb{Z} + \frac{1}{2}\right).\end{aligned}$$

It can be checked that $\mathcal{H}$ is closed under quaternion multiplication and addition, so that it forms a subring of the ring of all quaternions.

Definition 5. We define the set $\mathcal{R}$ as

$$\mathcal{R} = \{a + bw : a, b \in \mathbb{Z}\}.$$

Here and thereafter, w will denote $\frac{1}{2}(1 + \widehat{e}_1 + \widehat{e}_2 + \widehat{e}_3)$. Let π be a prime in $\mathcal{R}$. If there exists $\delta \in \mathcal{R}$ such that $q_1 - q_2 = \delta\pi$ then $q_1, q_2 \in \mathcal{R}$ are congruent modulo π. We will denote it as $q_1 \equiv q_2 \pmod{\pi}$.

Remark 1. $\pi \in \mathcal{R}$ is a prime in $\mathcal{R}$ if and only if $N(\pi)$ is a prime in $\mathbb{Z}$ [1].

The commutative property of multiplication holds over $\mathcal{R}$ since the vector parts of quaternion integers are parallel to each other, then their product is commutative. This equivalence relation is well-defined. We can consider the ring of $\mathcal{R}$ modulo this equivalence relation, which we denote as

$$\mathcal{R}_\pi = \{q \pmod{\pi} | q \in \mathcal{R}\}.$$

Theorem 2. *Let $\pi = a + bw \in \mathcal{R}$ be such that $\gcd(a, b) = 1$. It is obtained that $\mathbb{Z}_{N(\pi)}$ and $\mathcal{R}_\pi$ are isomorphic rings.*

The proof is straightforward from the proof of Theorem 11 in [8].