Available online at www.sciencedirect.com
ScienceDirect
Journal of the Franklin Institute 348 (2011) 1312–1317
Journal of The Franklin Institute
www.elsevier.com/locate/jfranklin

Cyclic codes over some finite quaternion integer rings

Mehmet Özen*, Murat Güzeltepe

Department of Mathematics, Sakarya University, TR54187 Sakarya, Turkey

Received 18 May 2009; received in revised form 11 February 2010; accepted 15 February 2010
Available online 6 March 2010

Abstract

In this paper, cyclic codes are studied over some finite quaternion integer rings with respect to the quaternion Mannheim distance.

Keywords: Block codes; Mannheim distance; Cyclic codes; Syndrome decoding

1. Introduction

Mannheim distance, which is much better suited for coding over two dimensional signal space than the Hamming distance, was introduced by Huber [1]. Moreover, Huber constructed one Mannheim error correcting codes, which are suitable for quadrature amplitude modulation (QAM)-type modulations [1]. Cyclic codes over some finite rings with respect to the Mannheim metric were obtained by using Gaussian integers in [2]. Later, in [3], using quaternion Mannheim metric perfect codes over some finite quaternion integer rings were obtained and these codes were decoded.

The rest of this paper is organized as follows. In Section 2, quaternion integers and some fundamental algebraic concepts have been considered. In Section 3, we construct cyclic codes over some quaternion integer rings with respect to quaternion Mannheim metric. In Theorem 3, it is shown how to obtain cyclic codes by utilizing Theorem 2 and Proposition 1. In Proposition 3, the algebraic background, which is essential for obtaining cyclic codes over the other finite rings, is arranged and in Theorem 4, it is shown how to obtain cyclic codes over the other finite rings.

*Corresponding author.
E-mail addresses: ozen@sakarya.edu.tr (M. Özen), mguzeltepe@sakarya.edu.tr (M. Güzeltepe).

0016-0032/$32.00
doi:10.1016/j.jfranklin.2010.02.008

2. Quaternion integers

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

(i) $H(\mathcal{R})$ is the free $\mathcal{R}$ module over the symbols $1, i, j, k$, that is, $H(R) = \{a_0 + a_1 i + a_2 j + a_3 k : a_0, a_1, a_2, a_3 \in R\}$;
(ii) 1 is the multiplicative unit;
(iii) $i^2 = j^2 = k^2 = -1$;
(iv) $ij = -ji = k$, $ik = -ki = j$, $jk = -kj = i$ [4].

The set $H(\mathcal{Z})$, $H(\mathcal{Z}) = \{a_0 + a_1 i + a_2 j + a_3 k : a_0, a_1, a_2, a_3 \in \mathcal{Z}\}$, is a subset of $H(\mathcal{R})$, where $\mathcal{Z}$ is the set of all integers. If $q = a_0 + a_1 i + a_2 j + a_3 k$ is a quaternion integer, its conjugate quaternion is $\overline{q} = a_0 - (a_1 i + a_2 j + a_3 k)$. The norm of q is $N(q) = q.\overline{q} = a_0^2 + a_1^2 + a_2^2 + a_3^2$. A quaternion integer consists of two parts which are the complete part and the vector part. Let $q = a_0 + a_1 i + a_2 j + a_3 k$ be a quaternion integer. Then its complete part is a_0 and its vector part is $a_1 i + a_2 j + a_3 k$. The commutative property of multiplication does not hold for quaternion integers. However, if the vector parts of quaternion integers are parallel to each other, then their product is commutative. Define $H(K_1)$ as follows:

$$H(K_1) = \{a_0 + a_1(i + j + k) : a_0, a_1 \in Z\},$$

which is a subset of quaternion integers. The commutative property of multiplication holds over $H(K_1)$.

Theorem 1. *For every odd, rational prime $p \in \mathcal{N}$, there exists a prime $\pi \in H(\mathcal{Z})$, such that $N(\pi) = p = \pi\overline{\pi}$. In particular, p is not prime in $H(Z)$* [4].

Corollary 1. *$\pi \in H(\mathcal{Z})$ is prime in $H(\mathcal{Z})$ if and only if $N(\pi)$ is prime in $\mathcal{Z}$* [4].

Theorem 2. *If a and b are relatively prime integers then $H(K_1)/\langle a + b(i + j + k)\rangle$ is isomorphic to $Z_{a^2+3b^2}$.*

Proof. We can assume without loss of generality that a and b are both positive. Observe that b is relatively prime to $a^2 + 3b^2$, so b^{-1} exists in $\mathcal{Z}_{a^2+3b^2}$. Since $a^2 + 3b^2 \equiv 0 \pmod{a^2 + 3b^2}$, $a^2 \equiv -3b^2 \pmod{a^2 + 3b^2}$, implying that $(ab^{-1})^2 \equiv -3$. Define $H(K_1) \to \mathcal{Z}_{a^2+3b^2}$ by $\varphi(x + y(i + j + k)) = x - (ab^{-1})y \pmod{a^2 + 3b^2}$. Clearly φ is surjective and preserves addition.

Let $\alpha_1 = x_1 + y_1(i + j + k)$ and $\alpha_2 = x_2 + y_2(i + j + k)$ be in $H(K_1)$. Since

$$\begin{aligned}
\varphi(\alpha_1)\varphi(\alpha_2) &= (x_1 - (ab^{-1})y_1)(x_2 - (ab^{-1})y_2) \\
&\equiv (x_1x_2 + (ab^{-1})^2 y_1y_2) - (ab^{-1})(y_1x_2 + y_2x_1) \\
&\equiv (x_1x_2 - 3y_1y_2) - (ab^{-1})(y_1x_2 + y_2x_1) \\
&= \varphi[(x_1x_2 - 3y_1y_2) + (y_1x_2 + y_2x_1)(i + j + k)] \\
&= \varphi[(x_1 + y_1(i + j + k))(x_2 + y_2(i + j + k))] = \varphi(\alpha_1\alpha_2),
\end{aligned}$$

φ observes multiplication. Moreover, because $\varphi(a + b(i + j + k)) = a - (ab^{-1})b \equiv 0$, $\langle a + b(i + j + k)\rangle \subseteq \ker(\varphi)$, where $\langle \cdot \rangle$ denotes an ideal generated by the element