Global Journal of Pure and Applied Mathematics.
ISSN 0973-1768 Volume 7, Number 2 (2011), pp. 201-206

http://www.ripublication.com/gjpam.htm

Quantum Codes from Codes over Lipschitz Integers

Mehmet ÖZEN and Murat GÜZELTEPE

Department of Mathematics, Sakarya University, TR54187, Turkey
E-mail: ozen@sakarya.edu.tr, mguzeltepe@sakarya.edu.tr

Abstract

In this study, some nonbinary quantum codes using classical codes over Lipschitz integers are obtained. Also, the error bases over Lipschitz integers are defined.

AMS Classification: 94B05, 94B60, 81P99.

Keywords: Nonbinary quantum codes, CSS codes, Lipschitz integers.

Introduction

There has been a great deal of work on trying to create efficient codes since Shore [1] and Steane [2] showed that it was possible to create quantum error-correcting codes. The most successful technique to date for constructing binary quantum codes is the additive or stabilizer construction [3]. This construction takes a classical binary code, self-orthogonal under a certain symplectic inner product, and produces a quantum code, with the minimum distance determined from the classical code. On the other hand, CSS codes was presented in [4]. In fact, CSS codes are obtained from two classical codes such that one of these codes contains the other code. Moreover, the bit flip and phase flip error correcting capacities of a CSS code depends on the classical code that contains the other code and the dual code of the other classical code, respectively [5, pp. 450-451]. Later, some results were generalized to the case of nonbinary quantum codes [6-8], but the theory is not nearly as complete as in the binary case. In [8], comprehensive theory of nonbinary quantum codes was submitted.

The rest of this paper is organized as follows. In Section II, Lipschitz integers, classical codes over Lipschitz integers, and the error basis operators are defined. In Section III, some quantum CSS codes are constructed.

Classical Codes over Lipschitz Integers

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

a. $H(\mathbb{R})$ is the free $\mathbb{R}$ module over the symbols $1, i, j, k$, that is, $H(\mathbb{R}) = \{a_0 + a_1 i + a_2 j + a_3 k : a_0, a_1, a_2, \ a_3 \in \mathbb{R}\}$;
b. 1 is the multiplicative identity;
c. $i^2 = j^2 = k^2 = -1$;
d. $ij = -ji = k, \ jk = -kj = i, ik = -ki = j$ [9].

The set $H(\mathbb{Z})$, which is defined by $H(\mathbb{Z}) = \{a_0 + a_1 i + a_2 j \ + a_3 k : a_0, a_1, a_2, a_3 \in \mathbb{Z}\}$ is a subset of $H(\mathbb{R})$, where $\mathbb{Z}$ is the set of all integers. The set $H(\mathbb{Z})$ was called Lipschitz integers or quaternion integers ring. More information about the arithmetic properties of $H(\mathbb{Z})$ can be found in [9, pp. 57-71]. If $q = a_0 + a_1 i + a_2 j + a_3 k$ is a quaternion integer, its conjugate quaternion is $q = a_0 - a_1 i - a_2 j - a_3 k$. The norm of q is $N(q) = q\bar{q} = a_0^2 + a_1^2 + a_2^2 + a_3^2$.

Definition 2. Let $\pi \neq 0$ be a quaternion integer. If there exists $\beta \in H(\mathbb{Z})$ such that $q_1 - q_2 \equiv_r \beta\pi$ then $q_1, q_2 \in H(\mathbb{Z})$ are right congruent modulo π and it is denoted as $q_1 \equiv_r q_2$ [10].

Theorem 1. Let $\pi \in H(\mathbb{Z})$ be a prime quaternion integer. Then, $H(\mathbb{Z})_\pi$ has $N(\pi)^2$ elements [10].

Example 1. Let $\pi = 1 + i + j$. Then, $H(\mathbb{Z})_\pi = \{0, \pm 1, \pm i, \pm j, \ \pm k\}$.

We now define a block code C of length n over $H(\mathbb{Z})_\pi$ as a set of codewords $c = (c_0, c_1, \cdots, c_{n-1})$ with coefficients $c_i \in H(\mathbb{Z})_\pi$. Let $\pi \in H(\mathbb{Z})$ be a prime quaternion integer and let $\alpha_1, \alpha_2 \in H(\mathbb{Z})_\pi$ be two different elements of orders $p-1$ and $(p-1)/2$, respectively. Hence, $x^{(p-1)/2} + 1$ and $x^{(p-1)/2} - 1$ are factored as

$$x^{(p-1)/2} + 1 = (x - \alpha_1)(x - \alpha_1^3) \cdots (x - \alpha_1^{p-2}),$$

$$x^{(p-1)/2} - 1 = (x - \alpha_2)(x - \alpha_2^3) \cdots (x - \alpha_2^{p-2}).$$

Also,

$$x^{p-1} - 1 = (x - \alpha_1)(x - \alpha_1^3) \cdots (x - \alpha_1^{p-2})(x - \alpha_2)(x - \alpha_2^3) \cdots (x - \alpha_2^{p-2}). \quad (1)$$

A monic polynomial $g(x)$ in $H(\mathbb{Z})_\pi[x]$ is the generator polynomial for a cyclic

code if and only if $g(x)\big|x^n-1$, where $H(\mathbb{Z})_\pi[x]$ is the set of all polynomials with coefficients in $H(\mathbb{Z})_\pi$ [11]. Using (1), we can construct two codes C_1, C_2 of length $n=p-1$ over $H(\mathbb{Z})_\pi$ such that $C_2 \subset C_1$. More information of cyclic codes over Lipschitz integer can be found [10-12].

Error Bases

Let $\pi \in H(\mathbb{Z})$ be a prime quaternion integer, let $p(x)$ be a monic irreducible polynomial of degree 2 in $\mathbb{Z}_{N(\pi)}[x]$. Then there exist a function $f: H(\mathbb{Z})_\pi \to \mathbb{Z}_{N(\pi)}[x]/(p(x))$. The function f defines a bijective mapping from $H(\mathbb{Z})_\pi$ to $\mathbb{Z}_{N(\pi)}[x]/(p(x))$ such that $f(b)=a_1+a_2\beta$, where $b \in H(\mathbb{Z})_\pi$, $a_1, a_2 \in \mathbb{Z}_{N(\pi)}$, and β is the root of the polynomial $p(x)$. We define the error operators over $\mathbb{Z}_{N(\pi)}$ as

$$(X_a)_{s,t} = \delta_{t,s+a(\mathrm{mod}(N(\pi)))} \text{ and } (Z_a)_{s,t} = \xi^{as(\mathrm{mod}(N(\pi)))}\delta_{s,t}, \tag{2}$$

where $s,t \in N(\pi)$, $a \in \mathbb{Z}_{N(\pi)}$, ξ denotes $N(\pi)-th$ root of unity, and δ denotes the kronecker delta function. Using (2), we define the error operators over $H(\mathbb{Z})_\pi$ as follows:

$$X_b^L = X_{a_1} \otimes X_{a_2} \text{ and } Z_b^L = Z_{N(\pi)-a_1} \otimes Z_{N(\pi)-a_2},$$

where $b \in H(\mathbb{Z})_\pi$, $f(b)=a_1+a_2\beta$, and the symbol "$\otimes$" denotes the tensor product. These error operators X_b^L, Z_b^L act on the quantum state $|u\rangle$ as

$$X_b^L|u\rangle = |(u+b)(\mathrm{mod}\,\pi)\rangle, Z_b^L|u\rangle = \xi^{(a_1a_3+a_2a_4)(\mathrm{mod}\,N(\pi))}|u\rangle,$$

where $f(b)=a_1+a_2\beta,\ f(u)=a_3+a_4\beta$.

CSS Code Construction

A $p-$ary quantum code Q of length n and size K is a $K-$dimensional subspace of a p^n-dimensional Hilbert space. This Hilbert space is identified with the $n-$fold tensor product of $p-$dimensional Hibert space. We denote by $|u\rangle$ the vectors of distinguished orthonormal bases of the Hilbert space, where the labels u range over the elements of the finite skew field $H(\mathbb{Z})_\pi$. For $u=(u_0,u_1,\cdots,u_{n-1})$, $v=(v_0,v_1,\cdots,v_{n-1}) \in H(\mathbb{Z})_\pi^n$, let $u.v=\sum u_i v_i$ be the usual inner product on $H(\mathbb{Z})_\pi^n$. For $(u|v),(u'|v') \in H(\mathbb{Z})_\pi^{2n}$, set $(u|v)*(u'|v') = Tr(v.u' - u.v')$, where $Tr: \mathbb{Z}_{N(x)}[x]/(p(x)) \to \mathbb{Z}_p$, $a_1+a_2\beta \mapsto a_1$ is the trace map. The weight of the vector $x=(u|v)$ is defined as

$$wt((u\,|\,v)) = \left|\{i:(u_i\,|\,v_i) \neq (0\,|\,0)\}\right|.$$

Also, the distance between the vectors $x=(u|v)$ and $y=(u'|v')$ is defined as $d(x,y)=wt(x-y)$. The minimum distance of the code C is $d(C)=\min\{wt(x):x\neq 0, x\in C\}$.

Proposition 1. Suppose $C\subset H(\mathbb{Z})_\pi^{2n}$ is a $H(\mathbb{Z})_\pi-$ linear code of length $2n$. Let $C^{\perp_*}$ be the dual code of C with respect to the inner product "$*$". If $C\subset C^{\perp_*}$, then there is a $p-$ary $[[n,k,d]]_p$ quantum code with $d=d(C^{\perp_*}-C)$ [7].

Theorem 1. Let C_1 and C_2 denote two classical linear codes over $H(\mathbb{Z})_\pi$ with parameters $[n,k_1,d_1]_\pi$, $[n,k_2,d_2]_\pi$, respectively such that $C_2\subset C_1$. Then, there exist an $[[n,k_1-k_2,d]]_\pi$ quantum code with minimum distance $d=min\{wt(u)|u\in(C_1\setminus C_2)\cup(C_2^{\perp}\setminus C_1^{\perp}\}$.

Proof. Set $C=C_2\times C_1^{\perp}$. For $(u\,|\,v)\in C$ and $(u'\,|\,v')\in C^{\perp_*}$ it is obtained $(u\,|\,v)*(u'\,|\,v')=0$ since $C_2\subset C_1$, $C_1^{\perp}\subset C_2^{\perp}$. Note that C is a $H(\mathbb{Z})_\pi-$ linear code in a $H(\mathbb{Z})_\pi^{2n}$.

Example 2. Let $\pi=1+i+j+k, p(x)=x^2+x+1.$ Then, $N(\pi)=3, H(\mathbb{Z})_\pi=\{0,\pm1,\pm i,\pm j,\pm k\}$, $\mathbb{Z}_\pi[x]/(p(x))=\{0,1,2,\beta,2\beta,1+\beta,2+2\beta,2+\beta,1+2\beta\}$. The error bases over $\mathbb{Z}_3$ are obtained as

$$X_0=Z_0=I_3,$$
$$X_1=\begin{pmatrix}0&1&0\\0&0&1\\1&0&0\end{pmatrix}, X_2=\begin{pmatrix}0&0&1\\1&0&0\\0&1&0\end{pmatrix}, Z_1\begin{pmatrix}1&0&0\\0&\xi&0\\0&0&\xi^2\end{pmatrix},$$
$$Z_2=\begin{pmatrix}1&0&0\\0&\xi^2&0\\0&0&\xi\end{pmatrix},$$

where ξ is the $3rd$ root of unity. Hence, the error bases over $H(\mathbb{Z})_{1+i+j}$ are constructed as follows:

$$X_0^L=Z_0^L=I_3\otimes I_3,\ X_{-1}^L=X_2\otimes I_3,\ X_i^L=I_3\otimes X_1,$$
$$X_{-i}^L=I_3\otimes X_2,\ X_j^L=X_2\otimes X_2,\ X_{-j}^L=X_1\otimes X_1,$$
$$X_k^L=X_1\otimes X_2,\ X_{-k}^L=X_2\otimes X_1,\ X_1^L=X_1\otimes I_3$$

and

$$Z_1^L=Z_2\otimes I_3,\ Z_{-1}^L=Z_1\otimes I_3,\ Z_i^L=I_3\otimes Z_2,\ Z_{-i}^L=I_3\otimes Z_1,$$
$$Z_j^L=Z_1\otimes Z_1,\ Z_{-j}^L=Z_2\otimes Z_2,\ Z_k^L=Z_2\otimes Z_1,\ Z_{-k}^L=Z_1\otimes Z_2.$$

Some of these bases, for instance, act on the quantum state $|-i\rangle$ as

$$X_{-1}^{L}|-i\rangle = \left|(-1-i)\left(\bmod(1+i+j)\right)\right\rangle = |j\rangle,$$

$$Z_{-k}^{L}|-i\rangle = \xi^{2}|-i\rangle,\ \left(f(-i)=2\beta,\ f(-k)=2+\beta\right)$$

where the function $f: H(\mathbb{Z})_{\pi} \to \mathbb{Z}_{\pi}[x]/(p(x))$ is given in Table I.

Example 3. Let $\pi = 2+i+j+k, \beta_1 = 1-i-j-k, \beta_2 = -1+\ \ i+j+k \in H(\mathbb{Z})_{\pi}$. Using (1), the polynomial x^6-1 is factored as

$$x^6-1 = (x-\alpha_1)(x-\alpha_1^3)(x-\alpha_1^5)(x-\alpha_2)(x-\alpha_2^3)(x-\alpha_2^5).$$

If we select the generator polynomial of the cyclic code C_1, C_2 as $g_1(x) = x-(1-i-j-k), g_2(x) = x^5+(i+j+k)x^4+(-1+i+j+k)x^3-x^2-(i+j+k)x+(1-i-j-k)$, respectively, according to Theorem 2, we obtain $[[6,4,2]]_{2+i+j+k}$ quantum code. This quantum code has 49^4 codewords.

Conclusion

In this study, we obtain CSS codes from cyclic codes over Lipschitz integers, and give the error bases for these CSS codes. The CSS codes obtained in this paper have more codewords than the CSS codes which are constructed up to now. So, regarding to coding theory these quantum codes are more important than the ones constructed at present.

Table I: The function $f: H(\mathbb{Z})_{\pi} \to \mathbb{Z}_{\pi}[x]/(p(x))$, where $p(x) = x^2+x+1, \beta$ is the root of $p(x)$.

$H(\mathbb{Z})_{\pi}$	$\mathbb{Z}_{\pi}[x]/(p(x))$	$H(\mathbb{Z})_{\pi}$	$\mathbb{Z}_{\pi}[x]/(p(x))$	$H(\mathbb{Z})_{\pi}$	$\mathbb{Z}_{\pi}[x]/(p(x))$
0	0	i	β	$-j$	$1+\beta$
1	1	$-i$	2β	k	$1+2\beta$
-1	2	j	$2+2\beta$	$-k$	$2+\beta$

References

[1] Shor, P. W. (1995). Scheme for reducing decoherence in quantum memory, Phys. Rev. A, vol.2 pp. 2493-2496.

[2] Steane, A. M. (1996). Multiple-particle interference and quantum error correction, in Proc. Roy. Soc., London A, vol. 452, pp. 1551-2577.

[3] Calderbank A. R., Rains, E. M., Shor, P. W., Sloane, N. J. A. (1998). Quantum error correction via codes over $GF(4)$, IEEE Trans. Inform. Theory, 44: 1369-1387.
[4] Calderbank A. R., Shor, P. W. (1996). Good quantum error-correcting codes exist, Phys. Rev. A., 54: 1098-1105.
[5] Nielsen, M. A., Chuang, I. L. (2000). Quantum Computation and Quantum Information, Cambridge: Cambridge University Press.
[6] Rains. E. (1999). Nonbinary quantum codes, IEEE Trans. Inform. Theory, vol. 45, no. 6, pp. 1827- 1832.
[7] Knill, E. (1996). Non-binary unitary error bases and quantum codes, Los Alamos National Laboratory Report LAUR-96-2717.
[8] Ketkar, A., Klappenecker, A., Kumar, S., Sarvepalli, P. (2006). Nonbinary stabilizer codes over finite fields, IEEE Trans. Inform. Theory, vol. 52, no. 11, pp. 4892-4914.
[9] Davidoff, G., Sarnak, P., Valette, A. (2003). Elementary number theory, group theory, and Ramanujan graphs, Cambridge University Pres.
[10] Martinez, C., Stafford, E., Beivide, R., Gabidulin, E. (2007). Perfect Codes over Lipschitz Integers". IEEE Int. Symposium on Information Theory, ISIT'07.
[11] Roman, S. (1992). Conding and Information Theory, Graduate Texts in Mathematics, Springer Verlag.
[12] Özen, M., Güzeltepe, M. (2010). Cyclic codes over some finite quaternion integer rings, Journal of the Franklin Ins., (In press DOI: 10.1016/j.jfranklin.2010.02.008)