Theory of Approximation and Applications, 2021, Volume 15, No. 1 : 1-7, DOR: 20.1001.1.25382217.2021.15.1.1.0

Constacyclic Codes over Group Ring $\left(Z_q[v]/\langle v^q - v\rangle\right)G$

Alireza Soleimani

Faculty of Mathematics, Tarbiat Modares University, Tehran, Iran

ARTICLE INFO

Keywords
Code, Ring, Group Ring, Constacyclic Codes

Article history
Received: 27 June 2020
Accepted: 11 July 2021

ABSTRACT

Recently, codes over some special finite rings especially chain rings have been studied. More recently, codes over finite non-chain rings have been also considered. Study on codes over such rings or rings in general is motivated by the existence of some special maps called Gray maps whose images give codes over fields. In this work, we determine self-dual and self-orthogonal codes arising from constacyclic codes over the group ring $\left(Z_q[v]/\langle v^q - v\rangle\right)G$.

1 Introduction and Preliminaries

$R = Z_q[v]/\langle v^q - v\rangle$ is a commutative, with $v^q = v$ (q is a prime number) . For a prime p and an integer k take $n = 2p^k$ then the set $G = 2Z_n^*$ is a cyclic group of orde $p^k - p^{k-1}$ and identity element $p^k + 1$. Then, the group ring RG is the set of all linear combinations in the form $u = \sum_{g\in G}\alpha_g g$ such that $\alpha_g \in R$ and only finitly many α_g is non zero. This set is commutative and operation of addition and multiplication is

$$u + v = \sum_{g\in G}\alpha_g g + \sum_{g\in G}\beta_g g = \sum_{g\in G}\left(\alpha_g + \beta_g\right)g$$

$$uv = \left(\sum_{g\in G}\alpha_g g\right)\left(u = \sum_{h\in G}\beta_h g\right)$$

A non-zero element u ∈ RG is a zero-divisor if and only if there exists a non-zero v ∈ RG such that uv = 0. For a fixed listing $\{g_1, g_2, \ldots., g_n\}$ of the elements of G the RG matrix of the element

*Corresponding author's E-mail: mr.soleymani25@yahoo.com

$w = \sum_{i=1}^{n} \alpha_{g_i} g_i \in RG$ is defined

$$w = \begin{pmatrix} \alpha g_1^{-1}g_1 & \alpha g_1^{-1}g_2 & \cdots & \alpha g_1^{-1}g_n \\ \alpha g_2^{-1}g_1 & \alpha g_2^{-1}g_2 & \cdots & \alpha g_2^{-1}g_n \\ \vdots & \vdots & \vdots & \vdots \\ \alpha g_n^{-1}g_1 & \alpha g_n^{-1}g_2 & \cdots & \alpha g_n^{-1}g_n \end{pmatrix}$$

A group ring RG is isomorphic to a subring of the ring of $n \times n$ matrices over R.

The teranspose of an element $u = \sum_{g \in G} \alpha_g g$ in RG is $u^T = \sum_{g \in G} \alpha_g g^{-1}$ or equivalently $u^T = \sum_{g \in G} \alpha_{g^{-1}} g$

.

The definition of the weight immediately leads to a Gray map from R to $Z_q{}^q$ which can be extended to $\left(Z_q + vZ_q + \ldots + v^{q-1}Z_q\right)^n$:

$$\phi : R \to Z_q{}^q$$

$$a = a_0 + a_1 v + \ldots + a_{q-1}v^{q-1} \to \phi(a) = \phi(a_0 + a_1 v + \ldots + a_{p-1}v^{q-1}) = (a(0), a(1), \ldots, a(q-1))$$

Where $a(i) = a_0 + a_1 i + \ldots + a_{q-1} i^{q-1} \pmod{q}$ for all $i \in \{0,1,\ldots,q-1\}$. this map is basically the natural one that gives the Chinese Remainder Theorem and hence this map relates the rings R and $Z_q{}^q$. Since ϕ is a isomorphism we have:

$$R \cong Z_q[v]/\langle v\rangle \oplus Z_q[v]/\langle v-1\rangle \oplus \ldots. \oplus Z_q[v]/\langle v-(q-1)\rangle \cong Z_q{}^q$$

Let $x = \sum_{g \in G} \alpha_g g$ and $y = \sum_{g \in G} \beta_g g$ be two elements in the group ring RG. Then, inner product of x and y is given by $\langle x, y\rangle = \sum_{g \in G} \alpha_g \beta_g$.

The map

$$\theta : \mathrm{RG} \to \mathrm{R}^n, \theta\left(\sum_{i=1}^{n} \alpha_i g_i\right) = (\alpha_1, \alpha_2, \ldots, \alpha_n)$$

is an isomorphism from RG to R^n. Thus every element in RG can be considered as an n-tuple in R^n.

A linear code C of length n over R, is a submodule of R^n. A linear code of length n, dimension k, and minimum (Hamming) distance d over R is termed as an $[n,k,d]_q$ code. Let n be a positive integer and α be a unit element of R. A linear code C of length n over R is said to be α−constacyclic if for any codeword $(c_0,c_1,\ldots,c_{n-1})\in C$ we have that $(\alpha c_{n-1},c_0,c_1,\ldots,c_{n-2})\in C$ If we take α as −1, then the code is called negacyclic.

It is not easy to find the structure of lattices of ideals of non-chain rings in general. Here by using the Gray map introduced above, we are able to give the structure of ideals of R and further count the number of ideals as follows:

Lemma 1.1 R has exactly 2^q ideals.

Proof. Since Z_q is a field (q is a prime number) then its ideals are exactly the zero ideal and Z_q itself, then the number of ideals of $Z_q{}^q$ is the product of the number of trivial ideals. Therefor the number of ideal of R is 2^q .

The cyclic codes of length m are ideals in the quotient ring $R[x]/\langle x^m - 1\rangle$. Further, for a cyclic group C_m of order m we have $R[x]/\langle x^m - 1\rangle \cong RC_m$.

Definition 1 Let u be a zero-divisor in RG, i.e. uv = 0 for some non-zero v ∈ RG. Let W be a submodule of RG with basis of group elements $S \subseteq G$. Then, a zero-divisor code is $C = \{ux|x\in W\} = uW$ or $C = \{xu|x\in W\} = Wu$.

Definition 2 A zero-divisor u with rank(U) = r is called a principal zero-divisor if and only if there exists a v ∈ RG such that uv = 0 and rank(V) = n−r.

Corollary 3 $C = \{xu|x\in W\} = Wu$ has a unique check element if and only if u is a principal zero divisor.

The dual of a code with respect to the standard inner product forms a group ring encoding as well where the dual is defined by

$$C^{\perp} = \{y\in RG|\langle ux,y\rangle = 0,\forall x\in W\}.$$

Proof. In [7].

Theorem 4 Let u,v ∈ RG such that uv = 0. Let U and V be the RG matrices of u and v respectively, such that rank(U) = r and rank(V) = n−r Let W be a submodule over a basis S ⊂ G of dimension r such that Su is linearly independent and $W^{\perp}$ denote the submodule over basis

G\S. Then, the dual code of $C = \{xu|x \in W\} = Wu$ is $C^{\perp} = \left\{xv^T|x \in W^{\perp}\right\} = \left\{y \in RG|yu^T = 0\right\}$.

Proof. Note that v^T is a zero-divisor and that rank v^T = n − r (because rankV = n − r), and that $W^{\perp}$ does not contain a zero-divisor of v^T. Thus, there is a 1-1 map between $W^{\perp}$ and $\{xv^T : x \in W^{\perp}\}$. It remains to show it is the dual.

Let z ≠ 0 be an element in RG. We need to prove that $\langle xu, z\rangle = 0$, ∀x ∈ W if and only if z = y v^T for some y $\in W^{\perp}$.

Suppose z = y, and let x,y ∈ RG

Recall that $x' = \zeta^{-1}(x), y' = \zeta^{-1}(y)$. are the vectors in R^n corresponding to x,y. Then $\langle xu, z\rangle = \langle xu, yv^T\rangle = x'U(V^Ty')^T = x'(UV)y'^T = 0$.

Conversely, suppose $\langle xu, z\rangle = 0 \ \forall x \in W$. Without loss of generality, assume 1 ∈ W. Then $\langle xu, z\rangle = 0$ implies $zu^T = 0$ and since u^T is the check element for the code generated by v^T, z = yv^T for some y ∈ $W^{\perp}$. □

2 Constacyclic Codes over Group Ring $\left(Z_q[v]/\langle v^q - v\rangle\right)G$

In this section, we extend the notion of cyclic group ring codes to constacyclic group ring codes. Throughout this section, we assume p is an odd prime, $R = Z_q[v]/\langle v^q - v\rangle$ and $n = 2p^k$ under the restrictions $\gcd\left(q, \varphi\left(2p^k\right)\right) = 1$ (φ is the Euler totient function) and $p^k + 1 \neq 0, 1 (\mathrm{mod}\, q)$.

Let Z_n be the set of integers modulo $n = 2p^k$. Let $G = 2Z_n^* \subset Z_n$ be the set of all double elements in Z_n^*.

Theorem 5 The set $G = 2Z_n^*$ all doubled elements in Z_n^* is a cyclic multiplicative group with identity element $e = p^k + 1$.

Corollary 6 Let p be an odd prime and n = 2p. Then, $G = 2Z_n^*$ the set of all doubled elements in Z_n^* is a cyclic multiplicative group with identity element $e = p + 1$.

Theorem 7 Let G be the cyclic group given in Theorem 5 and $R = Z_q[v]/\langle v^q - v\rangle$ such that

$\gcd(\varphi(p^k),q)=1$. Also, let u,v ∈ RG be principle zero divisors. Then, (RG)u is an e−constacyclic code of length $\varphi(p^k)$ and dimension rank(u).

Corollary 8 The dual code of the code given in the Theorem 7 is a e^{-1} −constacyclic code of length $\varphi(p^k)$ and dimension $\mathrm{rank}(v)$.

3 Self Dual and Self Orthogonal Constacyclic Codes over $(Z_q[v]/\langle v^q-v\rangle)G$

This section is devoted to determining self dual and self orthogonal codes arising from constacyclic codes over group algebras

Lemma 9 Let $C=(\theta(RG)u)$ be an e−constacyclic code of length $\varphi(p^k)$ given in Theorem 7 with dual code $C^{\perp}=\theta((RG)v^T)$. Then, the code $C^{\perp}=\theta((RG)v^T)$ is also an e^{-1} −constacyclic code of length $\varphi(p^k)$.

Theorem 10 Let $C=(\theta(RG)u)$ be an e−constacyclic code of length $\varphi(p^k)$ given in Theorem 7 with dual code $C^{\perp}=\theta((RG)v^T)$. Then, C is self dual if and only if $e^2=1(\mathrm{mod}\, q)$ and $u=v^T$.

Corollary 11 Let $C=(\theta(RG)u)$ be an e−constacyclic code of length $\varphi(p^k)$ given in Theorem 7 with dual code $C^{\perp}=\theta((RG)v^T)$. Then, $p^k\equiv 2(\mathrm{mod}\, q)$.

Theorem 12 11 Let $C=(\theta(RG)u)$ be an e−constacyclic code of length $\varphi(p^k)$ given in Theorem 7 with dual code $C^{\perp}=\theta((RG)v^T)$. Then, C is self orthogonal if and only if $e^2=1(\mathrm{mod}\, q)$ and for some w ∈ RG $w=uv^T$.

4 Quantum Codes Obtained from Negacyclic Codes over $(Z_q[v]/\langle v^q-v\rangle)G$

The construction of quantum codes via classical codes over F_2 was first introduced by Calderbank and Shor [4] and Steane [13] in 1996. Later, construction quantum codes over different alphabets obtained from classical linear codes over Fq has been shown by Ketkar et al. in [10]. A quantum error correcting code Q is defined as follows:

Definition 14 A q−ary quantum code Q, denoted by $[[n,k,d]]_q$ is a q^k dimensional subspace of the Hilbert space C^{q^n} and can correct all errors up to $\left[\frac{d-1}{2}\right]$.

The following lemma is a method to get quantum error correcting codes via classical linear codes over finite fields.

Lemma 15 (CSS Code Construction) [10] Let C_1 and C_2 denote two classical linear codes with parameters $[n,k_1,d_1]_q$ and $[n,k_2,d_2]_q$ such that $C_2^{\perp} \le C_1$. Then there exists a $[[n,k_1+k_2-n,d]]_q$ quantum code with minimum distance d = $\min\left\{wt(c) \middle| c \in \left(C_1 \setminus C_2^{\perp}\right) \subset \left(C_2 \setminus C_1^{\perp}\right)\right\}$.

Corollary 16 [10] If C is a classical linear $[n,k,d]_q$ code containing its dual, $C^{\perp} \subset C$ then there exists an $[[n,2k-n,\ge d]]_q$ quantum code.

5 Conclusion

In this work, we determine self dual and self orthogonal codes arising from constacyclic codes of length $\varphi(p^k)$ over group ring $\left(Z_q[v]/\langle v^q-v\rangle\right)G$. Further, we take look at a quantum codes.

References

[1] Aydin N Siap I and Ray-Chaudhuri D K 2001 Design Code Cryptogr 24 313-326

[2] Berlekamp E R 2015 World Scientific

[3] Bosma W Cannon J and Playoust C 1997 J. Symbolic Comput 24 235-265

[4] Calderbank A R and Shor P W 1996 Phys. Rev. A 54 1098

[5] Calderbank A R Rains E M Shor P W and Sloane N J A 1998 IEEE Trans. Inform. Theory 44 1369

[6] Hurley T 2006 Int. J. Pure Appl. Math 31 319-335

[7] Hurley P and Hurley T 2009 Int. J. of Inform. and Coding Theory 1 57-87

[8] Kai X and Zhu S 2013 IEEE Trans. Inform. Theory 59 1193-1197

[9] Kai X Zhu S and Li P 2014 IEEE Trans. Inform. Theory 60 2080-2086

[10] Ketkar A Klappenecker A Kumar S and Sarvepalli P K 2006 IEEE Trans. Inform. Theory

52 4892-4914
[11] Milies C P and Sehgal S K 2002 Springer
[12] Ling S and Xing C 2004 Cambridge University Press
[13] Steane A M 1996 Phys. Rev. A 54 4741
[14] Xiaoyan L 2004 IEEE Trans. Inform. Theory 50 547-549