Quantum Codes From Negacyclic Codes over Group Ring $\left(F_q + vF_q\right) G$ [1]

Mehmet E. Koroglu and Irfan Siap

Yıldız Technical University, Department of Mathematics, Faculty of Art and Sciences, 34220, Esenler, Istanbul-Turkey

E-mail: mkoroglu@yildiz.edu.tr, isiap@yildiz.edu.tr

Abstract. In this paper, we determine self dual and self orthogonal codes arising from negacyclic codes over the group ring $\left(F_q + vF_q\right) G$. By taking a suitable Gray image of these codes we obtain many good parameter quantum error-correcting codes over F_q.

1. Introduction and Preliminaries

Quantum error-correcting (QEC) codes play a crucial role in protecting quantum information. In recent years many researchers have been working to find quantum codes with good parameters over various fields. The construction of quantum codes via classical codes over F_2 was first introduced by Calderbank and Shor [4] and Steane [13] in 1996. This method, known as CSS construction, has received a lot of attention and it has allowed to find many good quantum stabilizer codes. Later, construction of quantum codes over larger alphabets from classical linear codes over F_q has shown by Ketkar et al. in [10]. One direction of the main research in quantum error correction codes is constructing quantum codes that have large minimum distances [9] for a given size and length. In [14], based on classical quaternary constacyclic linear codes, some parameters for quantum codes are obtained. In [8, 9], respectively based on classical negacyclic and constacyclic linear codes some parameters for quantum MDS codes are presented. In this work, we determine self-dual and self-orthogonal codes arising from constacyclic codes over the group ring $\left(F_q + vF_q\right) G$. Based on these codes we obtain some quantum codes with promising parameters.

$R = F_q + vF_q$ is a commutative, characteristic 3 ring with $v^2 = v$ or with a ring isomorphism $F_q\left[v\right] / \left\langle v^2 - v\right\rangle$. For a prime p and an integer k take $n = 2p^k$ then the set $G = 2\mathbb{Z}_n^*$ is a cyclic group of order $p^k - p^{k-1}$ and identity element $p^k + 1$. Then, the group ring RG is the set of all linear combinations in the form $u = \sum\limits_{g\in G} \alpha_g g$ such that $\alpha_g \in R$ and only finitely many of the α_g's are non-zero. This set is a commutative ring with respect to the following binary operations

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

[1] This research is supported by Yıldız Technical University Scientific Research Projects Coordination Department. Project Number: 2016-01-03-DOP01.

and

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

A non-zero element $u \in RG$ is a zero-divisor if and only if there exists a non-zero $v \in RG$ 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 $w = \sum\limits_{i=1}^{n}\alpha_{g_i}g_i \in RG$ is defined as

$$W = \begin{pmatrix} \alpha_{g_1^{-1}g_1} & \alpha_{g_1^{-1}g_2} & \cdots & \alpha_{g_1^{-1}g_n} \\ \alpha_{g_2^{-1}g_1} & \alpha_{g_2^{-1}g_2} & \cdots & \alpha_{g_2^{-1}g_n} \\ \vdots & \vdots & \vdots & \vdots \\ \alpha_{g_n^{-1}g_1} & \alpha_{g_n^{-1}g_2} & \cdots & \alpha_{g_n^{-1}g_n} \end{pmatrix}.$$

A group ring RG is isomorphic to a subring of the ring of $n \times n$ matrices over R [6].

The rank of an element $u = \sum\limits_{g\in G}\alpha_g g$ in RG is the rank of the matrix U. The transpose of an element $u = \sum\limits_{g\in G}\alpha_g g$ in RG is $u^T = \sum\limits_{g\in G}\alpha_g g^{-1}$ or equivalently $u^T = \sum\limits_{g\in G}\alpha_{g^{-1}}g$. Given an element $\alpha = \sum\limits_{g\in G}\alpha_g g \in RG$, its support is the set $supp\,(\alpha) = \{g \in G|\, \alpha_g \neq 0\}$. The Hamming weight of an element $\alpha \in RG$ is the number of nonzero coefficient group elements in its support i.e., $w\,(\alpha) = |supp\,(\alpha)|$. The minimum weight of a submodule M in RG is $w\,(M) = \min\{\,|supp\,(\alpha)||\,0 \neq \alpha \in M\}$. Let w_L denote the Lee weight and w_H denote the Hamming weight for the codes over $R = F_q + vF_q$. Then, we set

$$w_L\,(a + bv) = w_H\,(a, a + b)\,.$$

The definition of the weight immediately leads to a Gray map from R to F_q^2 which can be extended to $(F_q + vF_q)^n$:

$$\phi : R \to F_q^2,\ \phi\,(a + bv) = (a, a + b)\,.$$

This map is a distance preserving map from R to F_q^2. Let $x = \sum\limits_{g\in G}\alpha_g g$, and $y = \sum\limits_{g\in G}\beta_g g$ be two elements in the group ring RG. Then, the inner product of x and y is given by term-by-term multiplication of the coefficients of x and y, namely $\langle x, y\rangle = \sum\limits_{g\in G}\alpha_g\beta_g$.

Let $a_1 + b_1v$ and $a_2 + b_2v$ be any two elements in R. Then, we have

$$\begin{aligned} & (a_1 + b_1v)\,(a_2 + b_2v) \\ = \;& a_1a_2 + (a_1b_2 + b_1a_2 + b_1b_2)\,v = 0 \\ \Leftrightarrow \;& a_1a_2 = 0 \text{ and } a_1b_2 + b_1a_2 + b_1b_2 = 0. \end{aligned}$$

Hence, the following relation is valid.

$$\begin{aligned} & (a_1, a_1{+}b_1)\,(a_2, a_2{+}b_2) \\ = \;& a_1a_2 + a_1a_2 + a_1b_2 + b_1a_2 + b_1b_2 = 0. \end{aligned}$$

As a result of this fact, the map ϕ is a orthogonality preserving map. The map

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

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 [12]. The algebraic structure of constacyclic codes is described in detail in [3, 1]. 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 $\alpha-$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.

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 $R[x]/\langle x^m - 1\rangle \cong RC_m$. Similar to the cyclic codes $e-$constacylic codes of length m can be viewed as ideals in the quotient ring $R[x]/\langle x^m - e\rangle$. Our aim is to construct a group G such that the isomorphism $R[x]/\langle x^m - e\rangle \cong RG$ exist, where $e \in F_q$ and $e \neq 0, 1$. For $n = 2p^k$, where p is an odd prime and k is an integer we show that the set of all doubled elements $G = 2\mathbb{Z}_n^*$ in $\mathbb{Z}_n^*$, is a multiplicative cyclic group of order $m = \varphi(n)$ (φ is the Euler totient function) with identity element $e = p^k + 1$, such that $e \neq 1$. Afterwards, we obtain self dual and self orthogonal $\left(p^k + 1\right)-$constacyclic codes of length $\varphi(n)$ over $(F_q + vF_q)$ by considering these codes as ideals in the group ring $(F_q + vF_q)\, G$.

Definition 1 *[7] Let u be a zero-divisor in RG, i.e. $uv = 0$ for some non-zero $v \in RG$. 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 *[7] A zero-divisor u with rank$(U) = r$ is called a principal zero-divisor if and only if there exists a $v \in RG$ such that $uv = 0$ and rank$(V) = n - r$.*

Corollary 3 *[7] $C = \{xu|\, x \in W\}$ 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

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

Theorem 4 *[7] Let $u, v \in RG$ 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 $S \subset G$ of dimension r such that Su is linearly independent and $W^{\perp}$ denote the submodule over basis $G \backslash S$. Then, the dual code of $C = \{xu|\, x \in W\}$ is $C^{\perp} = \left\{xv^T\middle|\, x \in W^{\perp}\right\} = \left\{y \in RG|\, yu^T = 0\right\}$.*

2. Constacyclic Codes over Group Ring $(F_q + vF_q)\, G$

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, $R = F_q + vF_q$ and $n = 2p^k$ under the restrictions $\gcd\left(q, \varphi\left(2p^k\right)\right) = 1$, and $p^k + 1 \neq 0, 1\, (mod\ q)$.

Let $\mathbb{Z}_n$ be the set of integers modulo $n = 2p^k$. Let $G = 2\mathbb{Z}_n^* \subset \mathbb{Z}_n$ be the set of all doubled elements in $\mathbb{Z}_n^*$.

Theorem 5 *The set $G = 2\mathbb{Z}_n^*$, all doubled elements in $\mathbb{Z}_n^*$, is a cyclic multiplicative group with identity element $e = p^k + 1$.*

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

Theorem 7 *Let G be the cyclic group given in Theorem 5 and $R = F_q + vF_q$ such that $\gcd\left(\varphi\left(p^k\right), q\right) = 1$. Also, let $u, v \in RG$ be principle zero divisors. Then, $(RG)\, u$ is an $e-$constacyclic code of length $\varphi\left(p^k\right)$ 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* $\varphi\left(p^k\right)$ *and dimension* $rank\left(v\right).$

3. Self Dual and Self Orthogonal Constacyclic Codes over $\left(F_q+vF_q\right)G$

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

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

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

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

Theorem 12 *Let* $C=\theta\left(\left(RG\right)u\right)$ *be an* $e-$*consta cyclic code of length* $\varphi\left(p^k\right)$ *given in Theorem 7 with dual code* $C^{\perp}=\theta\left(\left(RG\right)v^T\right).$ *Then,* C *is self orthogonal if and only if* $e^2=1\left(mod\ q\right)$ *and for some* $w\in RG$ $u=wv^T.$

Corollary 13 *If* $C=\theta\left(\left(RG\right)u\right)$ *is an* $e-$*constacyclic code with parameters* $\left[\varphi\left(p^k\right),rank\left(u\right),d\right]_q$ *then,* $\phi\left(C\right)$ *is an* $e-$*constacyclic code with parameters* $\left[2\varphi\left(p^k\right),2rank\left(u\right),d\right]_q.$

4. Quantum Codes Obtained from Negacyclic Codes over $\left(F_q+vF_q\right)G$

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 F_q 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* $\mathbb{C}^{q^n}$ *and can correct all errors up to* $\lfloor\frac{d-1}{2}\rfloor.$

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* $C_2^{\perp}\leq C_1$*. Then there exists a* $[[n,k_1+k_2-n,d]]q$ *quantum code with minimum distance* $d=min\{wt(c)|c\in(C_1\backslash C_2^{\perp})\subset(C_2\backslash C_1^{\perp})\}.$

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* $[[n,2k-n,\geq d]]_q$ *quantum code.*

For further and detailed information readers can refer to the references [4, 5, 13]. We will use Corollary 16 to derive quantum error-correcting codes based on self dual and self orthogonal constacyclic codes over group algebras given in Theorem 10 and 12. All the computations are done using MAGMA [3].

Table 1. Some parameters of quantum codes obtained from self dual (self orthogonal) $2-$constacyclic codes of length 40 over $\mathbb{F}_3$.

v^T	u	$\phi(C^{\perp})$	$\phi(C)$	Q
$g^{10}+2g^9+g^8+g^7+$ $g^6+g^4+2g^3+2g+2$	$2g^{10}+g^9+2g^8+2g^7+$ $2g^6+2g^4+g^3+g+1$	$[40,20,6]_3$	$[40,20,6]_3$	$[[40,0,\geq 6]]_3$
$g^{12}+g^{10}+g^8$ $+g^4+2g^2+1$	$g^8+g^6+2g^2+1$	$[40,16,6]_3$	$[40,24,4]_3$	$[[40,8,\geq 4]]_3$
$g^{14}+2g^{13}+g^{11}+2g^{10}$ $+g^9+g^7+2g^5+g^4$ $+g^3+2g^2+g+2$	$2g^6+2g^5+g^2+g+1$	$[40,12,9]_3$	$[40,28,4]_3$	$[[40,16,\geq 4]]_3$
$g^{16}+2g^{14}+g^{13}+g^{11}$ $+2g^{10}+g^9+2g^8+g^5$ $+g^4+2g^3+g+1$	$g^4+2g^3+g^2+1$	$[40,8,12]_3$	$[40,32,3]_3$	$[[40,24,\geq 3]]_3$
$g^{18}+2g^{17}+2g^{16}+$ $2g^{14}+g^{13}+g^{12}+g^{10}$ $+2g^9+2g^8+2g^6+g^5$ $+g^4+g^2+2g+2$	$2g^2+g+1$	$[40,4,15]_3$	$[40,36,2]_3$	$[[40,32,\geq 2]]_3$

Table 2. Some parameters of quantum codes obtained from self dual (self orthogonal) $4-$constacyclic codes of length 44 over $\mathbb{F}_5$.

u	v^T	$\phi(C^{\perp})$	$\phi(C)$	Q
$g^{11}+3g^{10}+3g^9+4g^8$ $+4g^7+2g^6+4g^5+2g^4$ $+g^3+3g^2+g+3$	$g^{11}+3g^{10}+3g^9+4g^8$ $+4g^7+2g^6+4g^5+2g^4$ $+g^3+3g^2+g+3$	$[44,22,6]_5$	$[44,22,6]_5$	$[[44,0,6]]_5$
$g^{16}+g^{15}+2g^{14}+$ $3g^{13}+3g^{12}+4g^{11}+$ $2g^{10}+4g^9+3g^8+$ $g^7+2g^6+g^5+3g^2+1$	$g^6+2g^4+4g^2+4g+1$	$[44,12,12]_5$	$[44,32,4]_5$	$[[44,20,\geq 4]]_5$
$g^{12}+2g^{10}+3g^6$ $+2g^4+4g^2+1$	$g^{10}+g^8+4g^6$ $+4g^4+3g^2+1$	$[44,20,6]_5$	$[44,24,5]_5$	$[[44,4,\geq 5]]_5$
$g^{17}+g^{16}+g^{14}+2g^{13}+$ $2g^{12}+4g^{11}+3g^6+3g^5$ $+3g^3+g^2+g+2$	$3g^5+g^4+3g^3$ $+g^2+4g+1$	$[44,10,12]_5$	$[44,34,2]_5$	$[[44,24,\geq 2]]_5$

Example 17 *Let* $R=F_3+vF_3$ *and*

$$G=\{2,4,6,8,12,14,16,18,22,24,26,28,32,34,36,38,42,44,46,48\}\subset\mathbb{Z}_{50},$$

be the multiplicative cyclic group mentioned in Corollary 6. Also, let $u=g^{18}+g^{17}+2g^{16}+2g^{14}+2g^{13}+g^{12}+g^{10}+g^9+2g^8+2g^6+2g^5+g^4+g^2+g+2$ *and* $v^T=2g^2+2g+1$ *be two zero divisors in the group algebra* R *such that* $rank\,(u)=2$ *and* $rank\,(v)=18$*. Then, the two sided ideal* $(RG)\,u=\{xu|\,x\in RG\}\subset RG$ *is a* $2-$*constacyclic code (negacyclic code) of parameters* $[20,2,15]_3$*. The generator matrix of this code can be computed as*

$$G=\begin{pmatrix} 1 & 0 & 1 & 2 & 2 & 0 & 2 & 1 & 1 & 0 & 1 & 2 & 2 & 0 & 2 & 1 & 1 & 0 & 1 & 2 \\ 0 & 1 & 2 & 2 & 0 & 2 & 1 & 1 & 0 & 1 & 2 & 2 & 0 & 2 & 1 & 1 & 0 & 1 & 2 & 2 \end{pmatrix}.$$

So, $\phi\left(\theta\left((RG)\,u\right)\right)$ *is a* $2-$*constacyclic code (negacyclic code) of parameters* $[40,4,15]_3$*. The dual code of this code is the two sided ideal* $(RG)\,v^T=\left\{xv^T\middle|\,x\in RG\right\}\subset RG$ *with parameters* $[20,18,2]_3$*. Further,* $\phi\left(\theta\left((RG)\,v^T\right)\right)$ *is a* $2-$*constacyclic code (negacyclic code) of parameters* $[40,36,2]_3$*. By using Corollary 16 we have quantum code* Q *of parameters* $[[40,32,\geq 2]]_3$.

5. Conclusion

In this work, we determine self dual and self orthogonal codes arising from constacyclic codes of length $\varphi\left(p^k\right)$ over group ring $\left(F_q+vF_q\right)G$. Further, we obtained some parameters for quantum

Table 3. Some parameters of quantum codes obtained from self dual (self orthogonal) 6−constacyclic codes of length 36 over $\mathbb{F}_7$.

u	v^T	$\phi(C^{\perp})$	$\phi(C)$	Q
$g^{10}+5g^8+4g^6+2g^4+3g^2+1$	$g^8+4g^6+2g^2+1$	$[36,16,3]_7$	$[36,20,3]_7$	$[[36,4,\geq 3]]_7$
$g^{16}+3g^{14}+2g^{12}+6g^{10}$ $+4g^8+5g^6+g^4+3g^2+2$	$4g^2+1$	$[36,4,9]_7$	$[36,32,2]_7$	$[[36,28,\geq 2]]_7$
$g^{12}+3g^6+2$	$4g^6+1$	$[36,12,3]_7$	$[36,24,2]_7$	$[[36,12,\geq 2]]_7$

codes derived from self dual and self orthogonal codes arising from these codes. This family of codes awaits further studies since most of obtained codes are near optimal 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