Malaysian Journal of Mathematical Sciences 11(2): 289–301 (2017)

MALAYSIAN JOURNAL OF MATHEMATICAL SCIENCES
Journal homepage: http://einspem.upm.edu.my/journal

Quantum Codes from a Class of Constacyclic Codes over Group Algebras

Koroglu, M. E. *[1] and Siap, I. [2]

[1] *Yıldız Technical University, Department of Mathematics, Faculty of Art and Sciences, Turkey*
[2] *Jacodesmath Institute, Turkey*

E-mail: mkoroglu@yildiz.edu.tr
* *Corresponding author*

Received: 8th December 2016
Accepted: 8th May 2017

ABSTRACT

In this work, we determine self dual and self orthogonal codes arising from constacyclic codes over group algebras. Also, based on these codes we obtain some good parameters for quantum error-correcting codes.

Keywords: Group algebras, constacylic codes, linear codes, quantum codes.

1. Introduction

Quantum error-correcting (QEC) codes are crucial to protect 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 $\mathbb{F}_2$ was first introduced by Calderbank and Shor (1996) and Steane (1996). This method known as CSS construction has received a lot of attention and it has been a rich source for constructing many good quantum stabilizer codes. Later, construction of quantum codes over higher alphabets from classical linear codes over $\mathbb{F}_q$ was shown by Ketkar et al. (2006). One direction of the main research in quantum error correction codes is constructing quantum codes that have large minimum distances Kai et al. (2014).

In literature, dozens of papers have been devoted to obtaining good parameters for quantum codes derived from classical error correcting codes. A few of those papers uses constacylic codes to obtain quantum codes. In Xiaoyan (2004), based on classical quaternary constacyclic linear codes, some good parameters of quantum codes were obtained. In Kai and Zhu (2013) and Kai et al. (2014), respectively based on classical negacyclic and constacyclic linear codes some parameters for quantum MDS (maximum distance separable) codes were also presented. In Koroglu and Siap (2016), self dual and self orthogonal codes arising from negacyclic codes over the group ring $(\mathbb{F}_q + v\mathbb{F}_q)\,G$ were determined. Also, by taking a suitable Gray image of those codes they obtained many good parameters of quantum error-correcting codes over $\mathbb{F}_q$.

Let $\mathbb{F}_q$ be a finite field with q elements and m a positive integer. Cyclic codes of length m can be viewed as ideals in the group algebra $\mathbb{F}_q C_m$, where C_m is a cyclic group of order m. It is known that the quotient ring $\mathbb{F}_q[x]/\langle x^m - 1\rangle$ is isomorphic to the group algebra $\mathbb{F}_q C_m$ (Milies and Sehgal (2002)). Along this line of the research, construction of a group algebra $\mathbb{F}_q G$, which is isomorphic to the quotient ring $\mathbb{F}[x]_q/\langle x^m - e\rangle$, where $e \in \mathbb{F}_q$ and $e \neq 0, 1$, have been an open problem.

In this context, an e-constacyclic code of length m over $\mathbb{F}_q$ can be viewed as an ideal in the group algebra $\mathbb{F}_q G$, where G denotes a multiplicative cyclic group of order m with identity element $e \neq 1$. In Koroglu and Siap (2017), for $n = 2p^k$ (where p is an odd prime and k is an integer) it was shown 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 $e \neq 1$. In this paper, we studied self dual and self orthogonal $\left(p^k + 1\right)$-constacyclic codes of length $\varphi(n)$ over $\mathbb{F}_q$ by considering those codes as ideals in

the group algebra $\mathbb{F}_q G$. In this work, we determined self dual and self orthogonal $\left(p^k+1\right)-$constacyclic codes of length $\varphi(n)$ over $\mathbb{F}_q$ by considering these codes as ideals in the group algebra $\mathbb{F}_q G$. Further, based on these codes we obtained some quantum codes with promising parameters. Most of the obtained code parameters are near MDS quantum codes different from the parameters given in the Ezerman et al. (2013), Grassl and Rötteler (2015).

The rest of this paper is structured as follows. In the next section, we review some of the basics about linear codes, constacyclic codes, group rings and group ring encoding. In Section 3, we introduce the structure of e-constacyclic codes of length $\varphi(n)$ over group algebras. In Section 4, we determine self dual and self orthogonal codes arising from constacyclic codes over group algebras. In Section 5, we give some illustrative examples and tables which present some of the quantum codes obtained from self dual and self orthogonal codes arising from constacyclic codes over group algebras. The last section concludes this paper.

2. Preliminaries

In this section, we present some of basic facts about linear codes, constacyclic codes, group rings and group ring encoding that are more relevant to our search. For further and more detailed theory reader can refer to Bosma et al. (1997), Hurley and Hurley (2009), Hurley (2006), Ling and Xing (2004), and Milies and Sehgal (2002).

A linear code C of length n over $\mathbb{F}_q$ is a vector subspace of $\mathbb{F}_q^n$. A linear code of length n, dimension k, and minimum (Hamming) distance d over $\mathbb{F}_q$ is termed as an $[n,k,d]_q$ code. For any $\mathbf{x}=(x_1,\ldots,x_n)$ and $\mathbf{y}=(y_1,\ldots,x_n)\in\mathbb{F}_q^n$, the inner product of $\mathbf{x}$ and $\mathbf{y}$ defined as $\mathbf{x}\cdot\mathbf{y}=x_1y_1+\ldots+x_ny_n$. Then, the dual code of C is denoted by $C^{\perp}$ and defined as $C^{\perp}=\left\{\mathbf{x}\in F_q^n \,\middle|\, \mathbf{x}\cdot\mathbf{y}=\mathbf{0}, \text{ for all } \mathbf{y}\in C\right\}$. If $C\subseteq C^{\perp}$, then C is called self-orthogonal. If $C=C^{\perp}$, then C is called self-dual. The class of constacyclic codes contains cyclic and negacyclic codes which have been studied for a long time by Berlekamp (2015). The algebraic structure of constacyclic codes was described in detail in Aydin et al. (2001), and Bosma et al. (1997). Here, we review only the definition of constacyclic codes which is enough for our purpose.

Let n be a positive integer and α be a non-zero element of $\mathbb{F}_q$. A linear code C of length n over $\mathbb{F}_q$ is said to be an $\alpha-$consta cyclic if for any codeword $(c_0,c_1,\ldots,c_{n-1})\in C$ we have that $(\alpha c_{n-1},c_0,c_1,\ldots,c_{n-2})\in C$.

Let R be a ring and G a group. 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 finitely many of the α_g's are non-zero. The addition and multiplication are defined as

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

and

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

respectively. RG is a ring with respect to the binary operations defined above. The commutativity of RG depends on the commutativity of the ring R and the group G. 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 $u = \sum_{i=1}^{n} \alpha_{g_i} g_i \in RG$ is in $R_{n\times n}$ (the ring of $n \times n$ matrices over R) and defined as

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

A group ring RG is isomorphic to a subring of $R_{n\times n}$ (Hurley (2006)).

The rank of an element $u = \sum_{g\in G} \alpha_g g$ in RG is the rank of the matrix U. The transpose 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 $u^T = \sum_{g\in G} \alpha_{g^{-1}} g$. Given an element $\alpha = \sum_{g\in G} \alpha_g g \in RG$, 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 $w(M) = \min\{ |supp(\alpha)| \, | \, 0 \neq \alpha \in M \}$. The map

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

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

Let W be a submodule of RG. For a fixed element $u \in RG$ the map $f : W \to RG$, such that $f(x) = xu$ or $f(x) = ux$ is called a group ring encoding (Hurley and Hurley (2009)). Here x is the information message and xu is the encoded message i.e., the codeword. Hence, the code is then the set

$$C = \{ ux | \, x \in W \} \text{ or } C = \{ xu | \, x \in W \}$$

where the former is a right group ring encoding and the latter is a left group ring encoding.

Definition 2.1. *(Hurley and Hurley (2009)). 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 $C = \{ xu | \, x \in W \} = Wu$.*

The code is thus constructed from a zero-divisor u, a submodule W and for an RG non-commutative group ring, a choice of direction i.e., right or left encoding. We say that u is a generator element of the code C relative to the submodule W if $C = Wu$.

Definition 2.2. *(Hurley and Hurley (2009)). A zero-divisor u with $rankU = r$ is called a principal zero-divisor if and only if there exists a $v \in RG$ such that $uv = 0$ and $rankV = n - r$.*

Corollary 2.1 (Hurley and Hurley (2009))**.** *. $C = \{ xu | \, x \in W \}$ has a unique check element if and only if u is a principal zero divisor.*

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, the inner product of x and y is given by term-by-term multiplication of the coefficients of x and y, namely $\langle x, y \rangle = \sum_{g \in G} \alpha_g \beta_g$ where $x = \sum_{g \in G} \alpha_g g$ and $y = \sum_{g \in G} \beta_g g$. Thus, the dual of a code forms a group ring encoding as

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

Theorem 2.1. *(Hurley and Hurley (2009)). 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 $C^{\perp} = \left\{ xv^T \middle| \, x \in W^{\perp} \right\} = \left\{ y \in RG | \, yu^T = 0 \right\}$.*

3. Constacyclic Codes over Group Algebras

The structure of constacyclic codes over group algebras was introduced in Koroglu and Siap (2017). In this section, we review some of the theory about constacyclic codes from group algebras, which are necessary for the rest of this paper. Throughout this section, we assume p is an odd prime, $\mathbb{F}_q$ is a finite field of q elements, and $n = 2p^k$ with 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,where $n = 2p^k$, p is an odd prime and k is a positive integer. Let $G = 2\mathbb{Z}_n^* \subset \mathbb{Z}_n$ be the set of all doubled elements in $\mathbb{Z}_n^*$. As shown in the illustrative example above, the choice of n for which doubled elements of $\mathbb{Z}_n^*$ form a group is crucial. The answer to this fact is given in Theorem 3.1.

Theorem 3.1. *(Koroglu and Siap (2017)). 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 3.1. *(Koroglu and Siap (2017)). Let p be an odd prime and $n = 2p$. Then, the set of all doubled elements $G = 2\mathbb{Z}_n^*$ in $\mathbb{Z}_n^*$ is a cyclic multiplicative group with identity element $e \equiv p + 1$.*

An e-consta cyclic code of length $\varphi\left(p^k\right)$ over $\mathbb{F}_q$ can be viewed as an ideal in the group algebra $\mathbb{F}_q G$, where G denotes the cyclic group of order $\varphi\left(p^k\right)$ in Theorem 3.1 with identity element e and where $e = p^k + 1 \ (mod\ q)$.

Theorem 3.2. *(Koroglu and Siap (2017)). Let $\mathbb{F}_q$ be the finite field of q elements and G be the cyclic group given in Theorem 3.1 such that* $\gcd\left(\varphi\left(p^k\right), q\right) = 1$. *Also, let $u, v \in \mathbb{F}_q G$ be principle zero divisors. Then $(\mathbb{F}_q G)\, u$ is an $e-$constacyclic code of length $\varphi\left(p^k\right)$ and dimension rank (u).*

Corollary 3.2. *The dual code of the code given in the Theorem 3.2 is an e^{-1}-constacyclic code of length $\varphi\left(p^k\right)$ and dimension rank (v).*

4. Self Dual and Self Orthogonal Constacyclic Codes over Group Algebras

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

Lemma 4.1. *Let $C = \theta\left((\mathbb{F}_q G)\, u\right)$ be an e-constacyclic code of length $\varphi\left(p^k\right)$ given in Theorem 3.2 with its dual code $C^{\perp} = \theta\left((\mathbb{F}_q G)\, v^T\right)$. Then, the code $C^{\perp} = \theta\left((\mathbb{F}_q G)\, v^T\right)$ is also an e^{-1}-constacyclic code of length $\varphi\left(p^k\right)$.*

Proof. The proof follows from Corollary 3.2. □

Theorem 4.1. *Let $C = \theta((\mathbb{F}_q G)\, u)$ be an e-constacyclic code of length $\varphi(p^k)$ given in Theorem 3.2 with its dual code $C^{\perp} = \theta\left((\mathbb{F}_q G)\, v^T\right)$. Then, C is self dual if and only if $e^2 = 1\,(mod\ q)$ and $u = v^T$.*

Proof. The proof directly follows from the definition of self dual codes, Theorem 3.2 and Corollary 3.2. □

Corollary 4.1. *Let $C = \theta((\mathbb{F}_q G)\, u)$ be an e-constacyclic code of length $\varphi(p^k)$ given in Theorem 3.2 with dual code $C^{\perp} = \theta\left((\mathbb{F}_q G)\, v^T\right)$. Then, $p^k \equiv 2\,(mod\ q)$.*

Proof. By the Theorem 3.1 we have $e = p^k + 1$. Also, from Theorem 4.1 $e^2 = 1\,(mod\ q)$. So, we have $\left(p^k + 1\right)^2 = p^{2k} + 2p^k + 1 = 1\,(mod\ q)$. This means that $p^k = 0\,(mod\ q)$ or $p^k = 2\,(mod\ q)$. □

Theorem 4.2. *Let $C = \theta((\mathbb{F}_q G)\, u)$ be an e-consta cyclic code of length $\varphi(p^k)$ given in Theorem 3.2 with its dual code $C^{\perp} = \theta\left((\mathbb{F}_q G)\, v^T\right)$. Then, C is self orthogonal if and only if $e^2 = 1\,(mod\ q)$ and for some $w \in \mathbb{F}_q G$ $u = wv^T$.*

5. Quantum Codes Obtained from Constacyclic Codes over Group Algebras

The construction of quantum codes via classical codes over $\mathbb{F}_2$ was first introduced by Calderbank and Shor (1996) and Steane (1996). Later, construction stabilizer quantum codes over different alphabets obtained from classical linear codes over $\mathbb{F}_q$ was shown by Ketkar et al. (2006). A quantum error correcting code Q is defined as follows:

Definition 5.1. *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 type (both bit flip and phase shift) errors up to $\lfloor \frac{d-1}{2} \rfloor$.*

Any quantum code with parameters $[[n, k, d]]_q$ must satisfy the quantum Singleton bound: $k \leq n - 2d + 2$ (see Ketkar et al. (2006)). A quantum code attaining this bound is called a quantum maximum-distance-separable (MDS) code.

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

Lemma 5.1. *(Ketkar et al. (2006)). 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 $C_2^{\perp} \subseteq C_1$. Then there exists a $[[n, k_1 + k_2 - n, d]]_q$ quantum code with minimum distance $d = min\{wt(c)|c \in (C_1 \backslash C_2^{\perp}) \cup (C_2 \backslash C_1^{\perp})\}$.*

Corollary 5.1. *(Ketkar et al. (2006)). If C is a classical linear $[n, k, d]_q$ code containing its dual, $C^{\perp} \subseteq C$, then there exists an $[[n, 2k - n, \geq d]]_q$ quantum code.*

For further and detailed information readers can refer to the references Calderbank et al. (1998), Calderbank and Shor (1996), Steane (1996).

We will use Corollary 5.1 to derive quantum error-correcting codes based on self dual and self orthogonal constacyclic codes over group algebras given in Theorem 4.1 and 4.2. Most of the obtaining code parameters are near MDS quantum codes different from the parameters were given in the Ezerman et al. (2013), Grassl and Rötteler (2015). In Table 1 and Table 4, the generator elements are given in vectorial form. For example, the group ring element $2g^2 + 2g + 1$ denoted by 122. All the computations are done using MAGMA (Bosma et al. (1997)).

Table 1: A new quantum code of length 20 over $\mathbb{F}_3$.

v^T	u	$C^{\perp}$	C	Q
11021100212101201	10121	$[20, 4, 12]_3$	$[20, 16, 3]_3$	$[[20, 12, 3]]_3$

Example 5.1. *Let $\mathbb{F}_3$ be the finite field with characteristic 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 3.1. 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 principle zero divisors in the group algebra $\mathbb{F}_3 G$ such that $rank\,(u) = 2$ and $rank\,(v) = 18$. Then, the two sided ideal $(\mathbb{F}_3 G)\, u = \{\, xu |\, x \in \mathbb{F}_3 G\} \subset \mathbb{F}_3 G$ is a $2-$constacyclic code (negacyclic code) of parameters $[20, 2, 15]_3$. The generator matrix of this code can be computed as

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

The dual code of this code is the two sided ideal $(\mathbb{F}_3 G)\, v^T = \left\{\, xv^T \middle|\, x \in \mathbb{F}_3 G\right\} \subset \mathbb{F}_3 G$ with parameters $[20, 18, 2]_3$. From Corollary 5.1 we have a quantum code Q of parameters $[[20, 16, \geq 2]]_3$.

Table 2: A new of quantum code of length 42 over $\mathbb{F}_5$.

$C^{\perp}$	C	Q
$[42, 19, 12]_5$	$[42, 23, 10]_5$	$[[42, 4, 10]]_5$

Table 3: Some new parameters of quantum codes obtained from self dual 4−constacyclic codes of length 52 over $\mathbb{F}_5$.

$C^{\perp}$	C	Q
$[52, 26, 14]_5$	$[52, 26, 14]_5$	$[[52, 0, 14]]_5$
$[52, 22, 18]_5$	$[52, 30, 12]_5$	$[[52, 8, 12]]_5$
$[52, 18, 20]_5$	$[52, 34, 10]_5$	$[[52, 16, 10]]_5$
$[52, 14, 25]_5$	$[52, 38, 8]_5$	$[[52, 24, 8]]_5$
$[52, 12, 26]_5$	$[52, 40, 7]_5$	$[[52, 28, 7]]_5$
$[52, 10, 26]_5$	$[52, 42, 6]_5$	$[[52, 32, 6]]_5$
$[52, 6, 26]_5$	$[52, 46, 4]_5$	$[[52, 40, 4]]_5$

Table 4: A new quantum code obtained from self dual 6−constacyclic codes of length 18 over $\mathbb{F}_7$.

u	v^T	$C^{\perp}$	C	Q
10302040501	102000401	$[18, 8, 3]_7$	$[18, 10, 3]_7$	$[[18, 2, 3]]_7$

Table 5: Some new parameters of quantum codes obtained from self dual 10−constacyclic codes of length 30 and 52 over $\mathbb{F}_{11}$.

$C^{\perp}$	C	Q
$[30, 10, 15]_{11}$	$[30, 20, 5]_{11}$	$[[30, 10, 5]]_{11}$
$[52, 26, 10]_{11}$	$[52, 26, 10]_{11}$	$[[52, 0, 10]]_{11}$
$[52, 24, 10]_{11}$	$[52, 28, 8]_{11}$	$[[52, 4, 8]]_{11}$
$[52, 14, 24]_{11}$	$[52, 38, 6]_{11}$	$[[52, 24, 6]]_{11}$
$[52, 12, 24]_{11}$	$[52, 40, 3]_{11}$	$[[52, 28, 3]]_{11}$

Table 6: Some new parameters of quantum codes obtained from self dual 12−constacyclic codes of length 36 over $\mathbb{F}_{13}$.

$C^{\perp}$	C	Q
$[36,14,4]_{13}$	$[36,22,4]_{13}$	$[[36,8,4]]_{13}$
$[36,8,6]_{13}$	$[36,28,3]_{13}$	$[[36,20,3]]_{13}$

Example 5.2. *Let* $\mathbb{F}_5$ *be the finite field of characteristic* 5 *and*

$$G = \{2,4,6,8,10,12,14,16,18,20,22,24\} \subset \mathbb{Z}_{26},$$

be the multiplicative cyclic group given in Corollary 3.1. Also, let $u = g^8 + 2g^7 + 4g^6 + 2g^5 + g^4 + g^3 + g^2 + 4g + 1$ *and* $v^T = g^4 + g^3 + 3g + 1$ *be two principle zero divisors in the group algebra* $\mathbb{F}_5 G$ *such that* $rank\,(u) = 4$ *and* $rank\,(v) = 8$. *Then, the two sided ideal* $(\mathbb{F}_5 G)\,u = \{\, xu |\, x \in \mathbb{F}_5 G\} \subset \mathbb{F}_5 G$ *is a* $4-$*constacyclic code (negacyclic code) of parameters* $[12,4,6]_5$. *The generator matrix of this code can be computed as*

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 4 & 1 & 4 & 4 & 4 & 3 & 1 & 3 \\ 0 & 1 & 0 & 0 & 2 & 2 & 3 & 1 & 1 & 3 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 2 & 2 & 3 & 1 & 1 & 3 & 1 \\ 0 & 0 & 0 & 1 & 4 & 1 & 1 & 1 & 2 & 4 & 2 & 1 \end{pmatrix}.$$

The dual code of this code is the two sided ideal $(\mathbb{F}_5 G)\,v^T = \left\{\, xv^T \middle|\, x \in \mathbb{F}_5 G\right\} \subset \mathbb{F}_5 G$ *with parameters* $[12,8,4]_5$ *and generator matrix*

$$H = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 2 & 0 & 4 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 2 & 2 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 4 & 3 & 2 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 4 & 1 & 3 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 4 & 1 & 1 & 2 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 3 & 3 & 1 & 4 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 3 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 3 & 0 & 1 & 1 \end{pmatrix}.$$

By Corollary 5.1 we have a quantum code Q *of parameters* $[[12,4,\geq 4]]_5$.

Table 7: Some new parameters of quantum codes obtained from self dual 16−constacyclic codes of length 42 over $\mathbb{F}_{17}$.

$C^{\perp}$	C	Q
$[42, 21, 12]_{17}$	$[42, 21, 12]_{17}$	$[[42, 0, 12]]_{17}$
$[42, 19, 12]_{17}$	$[42, 23, 10]_{17}$	$[[42, 4, 10]]_{17}$
$[42, 15, 12]_{17}$	$[42, 27, 8]_{17}$	$[[42, 12, 8]]_{17}$
$[42, 13, 16]_{17}$	$[42, 29, 6]_{17}$	$[[42, 16, 6]]_{17}$
$[42, 7, 24]_{17}$	$[42, 35, 4]_{17}$	$[[42, 28, 4]]_{17}$

Table 8: A new quantum code obtained from self dual 28−constacyclic codes of length 18 over $\mathbb{F}_{29}$.

$C^{\perp}$	C	Q
$[18, 7, 4]_{29}$	$[18, 11, 4]_{29}$	$[[18, 4, 4]]_{29}$

6. Conclusion

In the present paper, we have determined self dual and self orthogonal codes arising from constacyclic codes of length $\varphi\left(p^k\right)$ over group algebras. Further, we obtained some parameters for quantum codes which are derived from self dual and self orthogonal codes arising from constacyclic codes over these group algebras. This family of codes awaits further studies since most of the obtained codes are near optimal codes.

Acknowledgement

The research was supported by Yıldız Technical University Scientific Research Projects Coordination Department (Project Number: 2016-01-03-DOP01). The authors would like to thank the editors and the referees for their constructive comments for improvement of the paper.

References

Aydin, N., Siap, I., and Ray-Chaudhuri, D. K. (2001). The structure of 1-generator quasi-twisted codes and new linear codes. *Designs, Codes and Cryptography*, 24(3):313–326.

Berlekamp, E. R. (2015). *Algebraic Coding Theory: Revised Edition*. World Scientific.

Bosma, W., Cannon, J., and Playoust, C. (1997). The magma algebra system i: The user language. *Journal of Symbolic Computation*, 24(3-4):235–265.

Calderbank, A. R., Rains, E. M., Shor, P. M., and Sloane, N. J. A. (1998). Quantum error correction via codes over gf (4). *IEEE Transactions on Information Theory*, 44(4):1369–1387.

Calderbank, A. R. and Shor, P. W. (1996). Good quantum error-correcting codes exist. *Physical Review A*, 54(2):1098–1105.

Ezerman, M. F., Jitman, S., Kiah, H. M., and Ling, S. (2013). Pure asymmetric quantum mds codes from css construction: A complete characterization. *International Journal of Quantum Information*, 11(03):1350027.

Grassl, M. and Rötteler, M. (2015). Quantum mds codes over small fields. In *2015 IEEE International Symposium on Information Theory (ISIT)*, pages 1104–1108.

Hurley, P. and Hurley, T. (2009). Codes from zero-divisors and units in group rings. *International Journal of Information and Coding Theory*, 1(1):57–87.

Hurley, T. (2006). Group rings and rings of matrices. *Int. J. Pure Appl. Math*, 31(3):319–335.

Kai, X. and Zhu, S. (2013). New quantum mds codes from negacyclic codes. *IEEE Transactions on Information Theory*, 59(2):1193–1197.

Kai, X., Zhu, S., and Li, P. (2014). Constacyclic codes and some new quantum mds codes. *IEEE Transactions on Information Theory*, 60(4):2080–2086.

Ketkar, A., Klappenecker, A., Kumar, S., and Sarvepalli, P. K. (2006). Nonbinary stabilizer codes over finite fields. *IEEE Transactions on Information Theory*, 52(11):4892–4914.

Koroglu, M. E. and Siap, I. (2016). Quantum codes from negacyclic codes over group ring $(F_q + vF_q)\,G$. In *Journal of Physics: Conference Series*, volume 766. Article ID: 012019.

Koroglu, M. E. and Siap, I. (2017). A class of constacyclic codes from group algebras. *Filomat*, 31(10):2917–2923.

Ling, S. and Xing, C. (2004). *Coding theory: A first course*. Cambridge University Press.

Milies, C. P. and Sehgal, S. K. (2002). *An introduction to group rings*, volume 1. Springer Science and Business Media.

Steane, A. M. (1996). Simple quantum error-correcting codes. *Physical Review A*, 54(6):4741–4751.

Xiaoyan, L. (2004). Quantum cyclic and constacyclic codes. *IEEE Transactions on Information Theory*, 50(3):547–549.