Filomat 31:10 (2017), 2917–2923
https://doi.org/10.2298/FIL1710917K

Published by Faculty of Sciences and Mathematics,
University of Niš, Serbia
Available at: http://www.pmf.ni.ac.rs/filomat

A Class of Constacyclic Codes from Group Algebras

Mehmet E. Koroglu[a], Irfan Siap[b]

[a]*Yıldız Technical University, Department of Mathematics, Faculty of Art and Sciences, 34220, Istanbul, Turkey*
[b]*Jacodesmath Institute, 34040, Istanbul, Turkey*

Abstract. Constacyclic codes are preferred in engineering applications due to their efficient encoding process via shift registers. The class of constacyclic codes contains cyclic and negacyclic codes. The relation and presentation of cyclic codes as group algebras has been considered. Here for the first time, we establish a relation between constacyclic codes and group algebras and study their algebraic structures. Further, we give a method for constructing constacyclic codes by using zero-divisors in group algebras. Some good parameters for constacyclic codes which are derived from the proposed construction are also listed.

1. Introduction

A linear code C of length n over $\mathbb{F}_q$, the finite field with q elements, 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 [9]. A linear code C whose parameters satisfy $k+d=n+1$ is called maximum distance separable or MDS. Constacyclic codes are preferred in engineering due to their efficient encoding process via shift registers. The class of constacyclic codes contains cyclic and negacyclic codes which have been studied for a long time [2]. On the other hand, in the literature there exist a few papers which study group ring encodings [8].

Algebraic structures of constacyclic codes are described in detail in [1, 2]. Here, we review only the definition of constacyclic codes which is sufficient to serve for our purpose.

Let m be a positive integer and α be a non-zero element of $\mathbb{F}_q$. A linear code C of length m over $\mathbb{F}_q$ is said to be $\alpha-$constacyclic if for any codeword $(c_0,c_1,\ldots,c_{m-1})\in C$ we have that $(\alpha c_{m-1},c_0,c_1,\ldots,c_{m-2})\in C$. Let $\mathbb{F}_q$ be a finite field with q elements and m a positive integer. It is known that $\alpha-$constacyclic codes of length m are ideals of quotient ring $\mathbb{F}_q[x]/\langle x^m-\alpha\rangle$ where $0\neq\alpha\in\mathbb{F}_q$. In particularly, if we take $\alpha=1$, then the class of constacyclic codes are called cyclic codes.

There are many papers in the literature that studied the structure of constacyclic codes. The majority of these papers are devoted to obtain $\alpha-$constacyclic codes of length m over certain algebraic structures (fields, rings etc.) based on the factorization of $x^m-\alpha$ (for instance see [4, 5, 11]).

The cyclic codes of length m can be viewed as ideals in the group algebra $\mathbb{F}_qC_m$, 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 $\mathbb{F}_qC_m$ [10]. In the light of this fact, the problem of determining the structure of constacyclic codes as group

2010 *Mathematics Subject Classification*. Primary 94B05, 94B15
Keywords. group algebras, cyclic codes, constacyclic codes
Received: 24 July 2016; Accepted: 26 January 2017
Communicated by Miroslav Ćirić
This research is supported by Yıldız Technical University Scientific Research Projects Coordination Unit. Project Number: 2016-01-03-DOP01.
Email addresses: mkoroglu@yildiz.edu.tr (Mehmet E. Koroglu), irfan.siap@gmail.com (Irfan Siap)

algebras has been open one till this paper. In other words, constructing a group algebra $\mathbb{F}_q G$, which is isomorphic to the quotient ring $\mathbb{F}_q[x]/\langle x^m - e\rangle$, where $e \in \mathbb{F}_q$ and $e \neq 0, 1$ has not been addressed yet. In this paper we address this problem and show up to which extent this is possible with the method introduced here.

The rest of paper is organized as follows. In the next section, we review some of the basics about group rings and group ring encodings. In Section 3, we introduce the structure of $e-$constacyclic codes of length $\varphi(n)$ over group algebras. In Section 4, we give some illustrative examples. Further, some of the heretofore known the best parameter codes are tabulated. The last section, concludes this study.

2. Group Rings and Encodings

In this section, we present some of basic facts about group rings and group ring encodings that are more relevant to our research. For further and detailed theory readers can refer to the references in [7, 8, 10].

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

$$u + v = \sum_{g\in G} \alpha_g g + \sum_{g\in G} \beta_g g = \sum_{g\in G} \left(\alpha_g + \beta_g\right) g \quad \text{and} \quad uv = \left(\sum_{g\in G} \alpha_g g\right)\left(\sum_{h\in G} \beta_h h\right) = \sum_{g,h\in G} \alpha_g \beta_h gh. \tag{1}$$

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. If the ring R is chosen as a field then the group ring RG is called a group algebra. 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 an element of $R_{n\times n}$ (the ring of $n \times n$ matrices over R) and defined as

$$U = \begin{pmatrix} \alpha_{g_1^{-1}g_1} & \alpha_{g_1^{-1}g_2} & \ldots & \alpha_{g_1^{-1}g_n} \\ \alpha_{g_2^{-1}g_1} & \alpha_{g_2^{-1}g_2} & \ldots & \alpha_{g_2^{-1}g_n} \\ \vdots & \vdots & \vdots & \vdots \\ \alpha_{g_n^{-1}g_1} & \alpha_{g_n^{-1}g_2} & \ldots & \alpha_{g_n^{-1}g_n} \end{pmatrix}. \tag{2}$$

A group ring RG is isomorphic to a subring of $R_{n\times n}$[7].

Example 2.1. *Let $R = \mathbb{Z}_2 = \{0, 1\}$ be the finite field of two elements, and $G = C_3$ be a cyclic group of order 3. Then the RG matrix of the element $u = g + g^2$ in the group ring $\mathbb{Z}_2 C_3$ is $U = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$.*

The rank of an element $u = \sum_{g\in G} \alpha_g g$ in RG is the rank of the RG matrix U i.e., $rank(u) = rank(U)$. 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 $supp(\alpha) = \left\{ g \in G \middle| \alpha_g \neq 0 \right\}$. The Hamming weight of an element $\alpha \in RG$ is the number of nonzero coefficient group elements in its support of α i.e. $w(\alpha) = \left|supp(\alpha)\right|$. The minimum weight of a submodule M in RG is $w(M) = \min\left\{ \left|supp(\alpha)\right| \middle| 0 \neq \alpha \in M \right\}$. The map

$$\theta : RG \to R^n,\ \theta\left(\sum_{i=1}^{n} \alpha_i g_i\right) = (\alpha_1, \alpha_2, \ldots, \alpha_n) \tag{3}$$

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 [8]. Here x is the information message and xu is the encoded message i.e. the codeword. Hence, the code is then the set

$$C = \{ux | x \in W\} \text{ or } C = \{xu | x \in W\} \tag{4}$$

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

Definition 2.2. *[8] 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 and a submodule W. The element u is called a generator element of the code $C = Wu$ relative to the submodule W.

A set of group ring elements $T \subset RG$ is linearly independent if, for $\alpha_x \in R$, $\sum_{x \in T} \alpha_x x = 0$ only when $\alpha_x = 0$ for all $x \in T$. Otherwise T is linearly dependent. The rank (T) is defined as the maximum number of linearly independent elements of T.

Note that a zero-divisor code $C = Wu$, where W is generated by S, is the submodule of RG consisting of all elements of the form $\sum_{g \in S} \alpha_g gu$. The dimension of this submodule is thus the rank of Su, and denoted as $rank\,(Su)$.

Example 2.3. *Let $RG = \mathbb{Z}_2C_3 = \left\{0, 1, g, g^2, 1+g, 1+g^2, g+g^2, 1+g+g^2\right\}$, $u = 1+g$ and $v = 1+g+g^2$. Also, let W be the submodule of $\mathbb{Z}_2C_3$ generated by $S = \{1, g\}$ i.e. $W = \langle S \rangle = \{0, 1, g, 1+g\}$. Then $(Su) = \{1, g\}(1+g) = \left\{1+g, g+g^2\right\}$ and so rank $(Su) = 2$. Moreover, the zero-divisor code generated by u with respect to the submodule W is $C = Wu = \left\{0, 1+g, g+g^2, 1+g^2\right\}$. By using the map given in (3) we get C as $\theta(C) = \{000, 110, 011, 101\}$. Thus, $\theta(C)$ is a $[3, 2, 2]$ binary cyclic linear code.*

Definition 2.4. *[8] 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 $rank(v) = n - r$.*

Example 2.5. *The elements $u = 1+g$ and $v = 1+g+g^2$ in $\mathbb{Z}_2C_3$ are principal zero-divisors because*

$$U = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} \quad \text{and} \quad V = \begin{pmatrix} 1 & 1 & 1 \end{pmatrix}. \tag{5}$$

Theorem 2.6. *[8] Let $C = \{xu | x \in W\}$ where W is generated by S such that Su is linearly independent and $|S| = rank(u) = r$. Suppose further that $uv = 0$ in the group ring RG so that $rank(v) = n - r$. Then, y is a codeword if and only if $yv = 0$.*

The element $v \in RG$ is called the check element of the code C.

Corollary 2.7. *[8] $C = \{xu | x \in W\}$ 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 the term-by-term multiplication of the coefficients of x and y, namely $\langle x, y \rangle = \sum_{g \in G} \alpha_g \beta_g$. Thus, the dual of a code forms a group ring encoding as $C^{\perp} = \left\{ y \in RG \middle| \langle ux, y \rangle = 0, \forall x \in W \right\}$.

Theorem 2.8. *[8] Let $u, v \in RG$ such that $uv = 0$. Let $rank(u) = r$ 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 of the code $C = \{xu | x \in W\}$ is $C^{\perp} = \left\{ xv^T \middle| x \in W^{\perp} \right\} = \left\{ y \in RG \middle| yu^T = 0 \right\}$.*

3. Constacyclic Codes over Group Algebras

Here we extend the notion of cyclic group ring codes to constacyclic group ring codes. Throughout this section we assume that p is an odd prime, $\mathbb{F}_q$ is a finite field of q elements, $n = 2p^k$ and $\gcd\left(q, \varphi\left(2p^k\right)\right) = 1, p^k + 1 \neq 0, 1 \,(mod\ q)$. Moreover, $\varphi(.)$ is the Euler totient function.

Prior giving the definitions and the results, we present a concrete and illustrative construction over an example.

Let $\mathbb{Z}_{10} = \{0,1,2,3,4,5,6,7,8,9\}$ be the set of integers modulo 10 and $G = 2\mathbb{Z}_{10}^* = \{2,4,6,8\} \subset \mathbb{Z}_{10}$ be the set of all doubled elements in $\mathbb{Z}_{10}^*$. The set G is a cyclic multiplicative group with identity element 6. Thus, there exists an element $g \in G$ such that $g^4 = e$ and $g^i \neq e$ for $i = 1,2,3$. Let $\mathbb{F}_7$ be the finite field of characteristic 7. Then the group algebra $\mathbb{F}_7 G$ is the set of all elements of the form $\sum_{i=0}^{3} \alpha_i g^i$, where $\alpha_i \in \mathbb{F}_7$ for $i = 0,1,2,3$. Let $u = 1 + 3g + g^2$ and $v = 1 + 4g + g^2$ be principle zero-divisors in $\mathbb{F}_7 G$. Then $uv = 0$ and $rank(u) + rank(v) = 2 + 2 = 4$. The set $(\mathbb{F}_7 G)u = \{xu | x \in \mathbb{F}_7 G\} \subset \mathbb{F}_7 G$ is an ideal of $\mathbb{F}_7 G$ with dimension 2. $\theta((\mathbb{F}_7 G)u)$ is a two dimensional subspace of the vector space $\mathbb{F}_7^4$. We see that the set $\theta((\mathbb{F}_7 G)u)$ is a 6−constacyclic code generated by the matrix $G' = \begin{pmatrix} 1 & 0 & 6 & 4 \\ 0 & 1 & 3 & 1 \end{pmatrix}$ with the parameters $[4,2,3]_7$. The dual code of this code is the two sided ideal $(\mathbb{F}_7 G)v^T = \left\{xv^T \middle| x \in \mathbb{F}_7 G\right\} \subset \mathbb{F}_7 G$ with parameters $[4,2,3]_7$ and the generator matrix $H = \begin{pmatrix} 1 & 0 & 6 & 3 \\ 0 & 1 & 4 & 1 \end{pmatrix}$. Both the code and its dual are MDS.

Let $\mathbb{Z}_n$ be the set of integers modulo n, where $n = 2p^k$, p is an odd prime and k be 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 by the following series of lemmas.

Lemma 3.1. *The set $G = 2\mathbb{Z}_n^*$ is closed under multiplication.*

Proof. Let p be an odd prime and $n = 2p^k$. By the Gauss Theorem we know that the multiplicative group $\mathbb{Z}_n^*$ of integer modulo n, $\mathbb{Z}_n$ is cyclic if $n = 2, 4, p^k$ and $2p^k$. Therefore, for $n = 2p^k$ there exists an element $g \in \mathbb{Z}_n^*$ such that $g^{\varphi(2p^k)} \equiv 1\left(mod\ 2p^k\right)$ and so we have $\langle g \rangle = \mathbb{Z}_n^* = \left\{1, g, g^2, \ldots, g^{\varphi(p^k)-1}\right\}$. We can rewrite the set G as $2\mathbb{Z}_n^* = \left\{a \in \mathbb{Z}_n | \gcd\left(a, 2p^k\right) = 2\right\} = \left\{2, 2g, 2g^2, \ldots, 2g^{\varphi(p^k)-1}\right\}$. Let x, y be any two elements in $2\mathbb{Z}_n^*$. Then, for some integer i, j such that $0 \leq i, j \leq \varphi\left(2p^k\right)$, we have $x = 2g^i$ and $y = 2g^j$. By multiplying these elements we get $xy = 2g^i 2g^j = 4g^i g^j$. If $xy = 2g^i 2g^j = 4g^i g^j \notin 2\mathbb{Z}_n^*$, then $p \Big| 4g^i g^j$. But this is a contradiction, since $(p, 4) = 1$ and $\left(p, g^i g^j\right) = 1$. Thus, we have $p \nmid 4g^i g^j$ and whence for some integer t, such that $0 \leq t \leq \varphi\left(2p^k\right)$, we have that $xy = 2g^t \in 2\mathbb{Z}_n^*$. This shows that the set $2\mathbb{Z}_n^*$ is closed under multiplication. □

Lemma 3.2. *The multiplicative identity of the set $G = 2\mathbb{Z}_n^*$ is $e = p^k + 1$.*

Proof. Let $G = \left\{a \in \mathbb{Z}_n | \gcd\left(a, 2p^k\right) = 2\right\}$. Choose an arbitrary element $x \in G$. Then, for some integer i, such that $0 \leq i \leq \varphi\left(2p^k\right)$, we have that $x = 2g^i$. Multiply the element x by e to get $xe = 2g^i\left(p^k + 1\right) = 2g^i p^k + 2g^i \equiv 2g^i\left(mod\ 2p^k\right)$. Therefore, $e = p^k + 1$ is the multiplicative identity of the set $G = 2\mathbb{Z}_n^*$. □

The following corollary is a direct result of Lemma 3.2.

Corollary 3.3. $e \equiv 1 \,(mod\ p)$.

Lemma 3.4. *Let p be an odd prime and $n = 2p^k$, where k is a positive integer. Then, for some positive integer r such that $r | \varphi\left(p^k\right)$ the congruence $2^r \equiv p^k + 1\left(mod\ 2p^k\right)$ holds.*

Proof. By the definition of G clearly 2 is an element in G. If 2 is a primitive element in $G = 2\mathbb{Z}_n^*$, then $2^{\varphi(p^k)} \equiv p^k + 1 \left(mod\ 2p^k\right)$. On the other hand, if 2 is not a primitive element in $G = 2\mathbb{Z}_n^*$, then for some positive integer r such that $r|\varphi\left(p^k\right)$ we have $2^r \equiv p^k + 1 \left(mod\ 2p^k\right)$. □

Lemma 3.5. *Every element in $G = 2\mathbb{Z}_n^*$ has a multiplicative inverse.*

Proof. Let $G = 2\mathbb{Z}_n^* = \left\{2, 2g, 2g^2, \ldots, 2g^{\varphi(p^k)-1}\right\}$. Then, every one of the element y in G is of the form $y = 2g^j$ for $0 \leq j \leq \varphi\left(2p^k\right)$. By multiplying all elements of $2\mathbb{Z}_n^*$ with $x = 2g^i$ we get $\left\{2 \cdot 2g^i, 2g \cdot 2g^i, \ldots, 2g^{\varphi(p^k)-1} \cdot 2g^i\right\}$. Choose an element $z = xy = 2g^j 2g^i$ in G such that $0 \leq j \leq \varphi\left(2p^k\right)$. Since G is closed under multiplication, for some integer l, such that $0 \leq l \leq \varphi\left(2p^k\right)$ we have that $z = 2g^l$ or $z = p^k + 1 = e$. The last case shows that every element y in $G = 2\mathbb{Z}_n^*$ has a multiplicative inverse. □

Corollary 3.6. *Let $x = 2g^i$ and $y = 2g^j, 0 \leq i, j \leq \varphi\left(2p^k\right)$ such that $xy \equiv p^k + 1 \left(mod\ 2p^k\right)$. Then the multiplicative inverse of $x = 2g^i$ is y and $y = 2^{r-1} g^{\varphi(p^k)-i-1}$, where $r|\varphi\left(p^k\right)$ and $2^r \equiv p^k + 1 \left(mod\ 2p^k\right)$.*

Theorem 3.7. *The set $G = 2\mathbb{Z}_n^*$ is a cyclic multiplicative group with identity element e such that $e \equiv 1\,(mod\ p)$.*

Proof. By Lemma 3.1, 3.2, 3.4 and 3.5 we know that the set $G = 2\mathbb{Z}_n^*$ is a multiplicative group with identity element e. Now, it is enough to show that the group G has a generator element. By the Gauss Theorem we know that $\mathbb{Z}_n^*$ is cyclic if $n = 2, 4, p^k$ and $2p^k$. Therefore, for $n = 2p^k$ there exists an element $g \in \mathbb{Z}_n^*$ such that $g^{\varphi(2p^k)} \equiv 1 \left(mod\ 2p^k\right)$ and so we have $\langle g \rangle = \mathbb{Z}_n^*$. Additionally, since $(2, p) = 1$ we have $2^{\varphi(p^k)} \equiv 1 \left(mod\ p^k\right)$. Further, since $(g, 2) = 1$ for some $h \in 2\mathbb{Z}_n^*$ we have $\langle h \rangle = 2\mathbb{Z}_n^* = G$. □

The following corollary is an immediate result of Theorem 3.7.

Corollary 3.8. *$G = 2\mathbb{Z}_n^*$ is a cyclic multiplicative group with identity element e such that $e \equiv 1\,(mod\ p)$.*

Hence, an $e-$constacyclic 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 3.7 with identity element e and where $e = p^k + 1\ (mod\ q)$.

Theorem 3.9. *Let $\mathbb{F}_q$ be the finite field of q elements and G the cyclic group given in Theorem 3.7 such that $\gcd\left(\varphi\left(p^k\right), q\right) = 1$. Let $u, v \in \mathbb{F}_q G$ be principle zero divisors. Then $\left(\mathbb{F}_q G\right) u$ is an $e-$constacyclic code of length $\varphi\left(p^k\right)$ and dimension rank (u).*

Proof. The proof follows from Theorem 3.7 and Definition 2.2. □

Corollary 3.10. *The dual code of the code given in the Theorem 3.9 is an $e^{-1}-$constacyclic code of length $\varphi\left(p^k\right)$ and dimension rank (v).*

Now, for a given $\varphi\left(p^k\right)$ positive integer, we can construct an $e-$constacyclic code of length s over $\mathbb{F}_q$ where s is a divisor of $\varphi\left(p^k\right)$ and $e = p^k + 1\ (mod\ q)$. The following corollary states this fact.

Corollary 3.11. *Let p be an odd prime $n = 2p^k$, where k is a positive integer such that $\gcd\left(\varphi\left(p^k\right), q\right) = 1$. Then, for each positive divisors of $\varphi\left(p^k\right)$, we have an $e-$constacyclic code.*

Example 3.12. *Let $p = 3, k = 6$, and $q = 7$ be. Then $e = p^k + 1 = 730 \equiv 2\,(mod\ 7)$, and so we have $2-$constacyclic codes of lengths*

$$1, 2, 3, 6, 9, 18, 27, 54, 81, 162, 243 \text{ and } 486. \tag{6}$$

If, we pick $p = 5, k = 5$, and $q = 7$, then $e = p^k + 1 = 3126 \equiv 4\,(mod\ 7)$, and so we get $4-$constacyclic codes of lengths

$$1, 2, 4, 5, 10, 20, 25, 50, 100, 125, 250, 500, 625, 1250 \text{ and } 2500. \tag{7}$$

4. An Example

Most of the code parameters given in Table 1 and Table 2 are the heretofore known best parameter codes in the Grassl's online table [6]. All of them are obtained directly via the construction method presented above. Though most of the results presented in Grassl's online table are obtained indirectly by shortening, puncturing, etc., here we have a direct construction. The computations for searching and computing the parameters is carried by MAGMA [3]. In Table 1 and 2 we prefer to represent a group element via a row matrix in order to save space. For instance, $g^2 + 10g + 2$ is presented only by the ordered coefficients such as $1\underline{1}02$. In all tables the parameters marked with $''*''$ are MDS.

Table 1: Some parameters of 3−constacyclic codes of length 12 over $\mathbb{F}_{11}$.

u	v	C	$C^{\perp}$
186290643$\underline{1}$0	133	$[12, 2, 10]$	$[12, 10, 2]$
1956169662	12$\underline{1}$04	$^{*}[12, 3, 10]$	$^{*}[12, 9, 4]$
1925074$\underline{1}$07	12269	$[12, 4, 8]$	$[12, 8, 3]$
168509537	15649	$[12, 4, 6]$	$[12, 8, 4]$
1167005582	1$\underline{1}$064	$[12, 3, 8]$	$[12, 9, 2]$
183000647	13699	$[12, 4, 6]$	$[12, 8, 2]$
18691038	133411	$[12, 5, 4]$	$[12, 7, 4]$
15302$\underline{1}$06	16040$\underline{1}$05	$[12, 6, 4]$	$[12, 6, 4]$
19984828	126881	$^{*}[12, 5, 8]$	$^{*}[12, 7, 6]$
13$\underline{1}$0558488	18$\underline{1}$06$\underline{1}$01	$[12, 5, 6]$	$[12, 7, 4]$
12$\underline{1}\underline{0}$0346	19$\underline{1}\underline{0}$445	$[12, 6, 6]$	$[12, 6, 4]$

Table 2: Some parameters of e−constacyclic codes obtained from $\mathbb{F}_q G$.

q	p	k	e	u	v	C	$C^{\perp}$
7	5	1	6	131	141	$^{*}[4, 2, 3]_7$	$^{*}[4, 2, 3]_7$
11	5	1	6	157	167	$^{*}[4, 2, 3]_{11}$	$^{*}[4, 2, 3]_{11}$
5	7	1	8	123	13144	$^{*}[6, 4, 3]_5$	$^{*}[6, 2, 5]_5$
11	7	1	8	149	17784	$^{*}[6, 4, 3]_{11}$	$^{*}[6, 2, 5]_{11}$
13	7	1	8	17	16$\underline{1}$0	$[6, 4, 2]_{13}$	$[6, 2, 3]_{13}$
7	11	1	12	11232	1660321	$[10, 6, 4]_7$	$[10, 4, 6]_7$
13	11	1	12	18$\underline{1}$2$\underline{5}$1	1500081	$[10, 6, 2]_{13}$	$[10, 4, 4]_{13}$
11	3	2	10	161	15251	$^{*}[6, 4, 3]_{11}$	$^{*}[6, 2, 5]_{11}$
13	3	2	10	1007	1006	$[6, 3, 2]_{13}$	$[6, 3, 2]_{13}$
3	13	1	14	112	11202210112	$[12, 10, 2]_3$	$[12, 2, 9]_3$
11	13	1	14	133	186290643$\underline{1}$0	$[12, 10, 2]_{11}$	$[12, 2, 10]_{11}$
11	17	1	18	100020002	100090002	$[16, 8, 3]_{11}$	$[16, 8, 3]_{11}$
7	5	2	26	1003005	1004004003006002006	$[24, 18, 3]_7$	$[24, 6, 7]_7$

Below we present an example constructed in Table 1 and 2 explicitly.

Example 4.1. *Let $\mathbb{F}_{11}$ be the finite field of characteristic 11 and $G = \{2, 4, 6, 8, 10, 12\} \subset \mathbb{Z}_{14}$ be the multiplicative cyclic group stated in Corollary 3.8. Let $u = 4 + 3g + 7g^2 + 4g^3 + g^4$ and $v = 9 + 7g + g^2$ be two principal zero divisors in the group algebra $\mathbb{F}_{11}G$ such that $rank(u) + rank(v) = 6$. Then the two sided ideal $(\mathbb{F}_{11}G)\,u = \{xu | x \in \mathbb{F}_{11}G\} \subset \mathbb{F}_{11}G$ is a 8−constacyclic code of parameters $[6, 2, 5]_{11}$. The generator matrix of this code can be found as $G' =$*

$\begin{pmatrix} 1 & 0 & 6 & 10 & 5 & 6 \\ 0 & 1 & 9 & 10 & 1 & 3 \end{pmatrix}$. *The dual code of this code is the two sided ideal* $(\mathbb{F}_{11}G)\,v^T = \left\{xv^T \middle| x \in \mathbb{F}_{11}G\right\} \subset \mathbb{F}_{11}G$ *with parameters* $[6,4,3]_{11}$ *and its generator matrix is* $H = \begin{pmatrix} 1 & 0 & 0 & 0 & 8 & 5 \\ 0 & 1 & 0 & 0 & 0 & 6 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 2 & 5 \end{pmatrix}$. *Both the code and its dual are MDS.*

5. Conclusion

In this work, we introduce the structure of a class of constacyclic codes of length $\varphi\left(p^k\right)$ over group algebras. We give a method to construct $e-$constacyclic codes from zero-divisors in group algebras. Some of the heretofore known best parameter codes in the Grassl's online table ([6]) can be directly obtained by using our construction method. The given construction can be generalized to the group rings RG for a given ring R. Further, this method allows us to construct constacyclic codes over some specific lengths. A further study on non restricted length constacyclic codes over group rings awaits attention from the researchers.

6. Acknowledgment

The authors are grateful to the anonymous referees for their through review of the paper and for their useful suggestions.

References

[1] N. Aydin, I. Siap, D. K. Ray-Chaudhuri, The structure of 1-generator quasi-twisted codes and new linear codes, Designs, Codes and Cryptography 24 (2001) 313–326.
[2] E. R. Berlekamp, Algebraic Coding Theory (Revised Edition),World Scientific, New York, 2015
[3] W. Bosma, J. Cannon, C. Playoust, The Magma algebra system I, The user language, Journal of Symbolic Computation 24 (1997) 235–265.
[4] B. Chen, H. Q. Dinh, H. Liu, L. Wang, Constacyclic codes of length $2p^s$ over $\mathbb{F}_{p^m} + \mathbb{F}_{p^m}$, Finite Fields Their Applications 37 (2016) 108–130.
[5] B. Chen, H. Q. Dinh, H. Liu, Repeated-root constacyclic codes of length $2l^m p^n$. Finite Fields Their Applications 33 (2015) 137–159.
[6] M. Grassl, Bounds on the minimum distance of linear codes, Available at: ⟨*http* : *//www.codetables.de*⟩, Accessed on 2016-02-15.
[7] T. Hurley, Group rings and rings of matrices International Journal of Pure and Applied Mathematics 31 (2006) 319–335.
[8] P. Hurley, T. Hurley, Codes from zero-divisors and units in group rings International Journal of Information and Coding Theory 1 (2009) 57–87.
[9] S. Ling, X. Chaoping, Coding theory: A first course, Cambridge University Press, Cambridge, 2004.
[10] C. P. Milies, K. S. Sudarshan, An introduction to group rings, Springer, The Nedherlands, 2002.
[11] A. Sharma, R. Saroj, Repeated-root constacyclic codes of length $4l^m p^n$ Finite Fields Their Applications 40 (2016) 163–200.