JOURNAL OF SCIENCE
SAKARYA UNIVERSITY

Sakarya University Journal of Science

ISSN 1301-4048 | e-ISSN 2147-835X | Period Bimonthly | Founded: 1997 | Publisher Sakarya University | http://www.saujs.sakarya.edu.tr/

Title: LCD codes and LCP of codes from units of group rings

Authors: Mehmet Emin Köroğlu
Recieved: 2018-09-11 00:00:00

Accepted: 2019-02-07 00:00:00

Article Type: Research Article
Volume: 23
Issue: 3
Month: June
Year: 2019
Pages: 486-492

How to cite
Mehmet Emin Köroğlu; (2019), LCD codes and LCP of codes from units of group rings . Sakarya University Journal of Science, 23(3), 486-492, DOI: 10.16984/saufenbilder.459123
Access link
http://www.saujs.sakarya.edu.tr/issue/41686/459123

Sakarya University Journal of Science 23(3), 486-492, 2019

LCD codes and LCP of codes from units of group rings

Mehmet E. KOROGLU*[1]

Abstract

A linear code with complementary dual (LCD) is a linear code such that $C \cap C^{\perp} = \{0\}$. LCD codes are of great importance due to their wide range of applications in consumer electronics, storage systems and cryptography. Group rings have a rich source of units. Also the well-known structural linear codes such as cyclic codes are within the family of group ring codes. Thus, group rings offer an affluent source for structural codes that may lead to linear codes with good properties. In this work, we derive a condition for codes obtained from units of group rings to be LCD. We show that a special decomposition of group rings meet the LCD condition. We also proposed a consruction of linear complementary pair (LCP) of codes.

Keywords: group rings, unit derived codes, linear complementary dual codes, linear complementary pair of codes

1. INTRODUCTION

A linear code is called a linear code with complementary-dual (for short LCD) if $C^{\perp} \cap C = \{0\}$. LCD codes were introduced by Massey in 1992 (see [1]). LCD codes have many applications such as in cryptography, communication systems, storage systems and consumer electronics. It is also shown that LCD codes provide an optimum linear coding solution for binary adder channel and asymptotically good LCD codes exist [1]. In [2], it was proved that LCD codes meet the asymptotic Gilbert-Varshamov bound. Carlet et al. have shown that LCD codes are used in counter measure to passive and active side channel analyses on embedded cryto-systems [3].

Group rings have a rich source of units. Also the well-known structural linear codes such as cyclic codes are within the family of group ring codes. Thus, group rings offer an affluent source for structural codes that may lead to linear codes with good properties.

In this study, we provide a condition for linear codes obtained from units of group rings to be LCD. Further, we give a special decomposition of group rings with two summands. In this obtained decomposition, we have shown that each component is treated as a linear code which is the

*Corresponding Author: mkoroglu@yildiz.edu.tr
[1] Department of Mathematics, Faculty of Art and Sciences, Yildiz Technical University, 34220, Istanbul, Turkey. ORCID: 0000-0002-9173-4944

dual of the other, and that the LCD condition is satisfied.

The rest of the paper is organized as follows. In Section 2, we present some definitions and basic results about linear codes and group rings. In Section 3, we remind some basics of unit derived codes from group rings. In Section 4, we give a condition for linear codes obtained from units of group rings to be LCD. In Section 5, we show that a special decomposition of group rings meet LCD condition by considering its components as linear codes. In Section 6, we proposed a consruction of linear complementary pair (LCP) of codes. The last section concludes the paper.

2. PRELIMINARIES

Let q be a prime power and F_q be the finite field with q elements. An $[n,k]_q$ linear code C of length n over F_q is a k-dimensional subspace of the vector space F_q^n. The elements of C are of the form $(c_0,c_1,\ldots,c_{n-1})$ and called codewords. The Hamming weight of any $c\in \mathrm{C}$ is the number of nonzero coordinates of c and denoted by $w(c)$. The minimum distance of C is defined as $d=\min\{w(c)\,|\,0\neq c\in \mathrm{C}\}$.

Let $\langle \mathbf{x},\mathbf{y}\rangle=\sum_{i=0}^{n-1}x_iy_i$ be the Euclidean inner product of the vectors $\mathbf{x}$ and $\mathbf{y}\in \mathrm{F}_q^n$ and C be a code of length n over F_q. Then the Euclidean dual code of C is defined to be

$$\mathrm{C}^{\perp}=\left\{\mathbf{x}\in \mathrm{F}_q^n\,\middle|\,\sum_{i=0}^{n-1}x_iy_i=0,\forall \mathbf{y}\in \mathrm{C}\right\}. \qquad (1)$$

Let R be a ring and G be a group. Then the set of all linear combinations in the form $\omega=\sum_{g\in G}\alpha_g g$ is a ring with respect to the following binary operations:

$$u+v=\sum_{g\in G}\alpha_g g+\sum_{g\in G}\beta_g g=\sum_{g\in G}(\alpha_g+\beta_g)g \qquad (2)$$

$$uv=\left(\sum_{g\in G}\alpha_g g\right)\left(\sum_{h\in G}\beta_h h\right)=\sum_{g,h\in G}\alpha_g\beta_h gh \qquad (3)$$

where $\alpha_g,\beta_g,\beta_h\in R$.

Definition 2.1. (see [4]) A non-zero element $u\in RG$ is a unit if and only if there exists a non-zero $v\in RG$ such that $uv=1$.

Definition 2.2. (see [4]) 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 $u^T=\sum_{g\in G}\alpha_{g^{-1}}g$.

Definition 2.3. (see [4]) The support of a given element $u=\sum_{g\in G}\alpha_g g\in RG$ is the set $supp(u)=\{g\in G\,|\,\alpha_g\neq 0\}$.

Example 2.1. Let G be the cyclic group $C_3=\langle g\rangle=\{1,g,g^2\}$ and R be the finite field $\mathbf{Z}_5=\{0,1,2,3,4\}$. Then the transpose of the element $u=3+g+2g^2\in \mathbf{Z}_5C_3$ is $u^T=3+2g+g^2$. The support of u is $supp(u)=\{1,g,g^2\}$.

The Hamming weight of an element $u\in RG$ is the number of nonzero coefficient of group elements in its support i.e., $w(u)=|supp(u)|$.

Example 2.2. The Hamming weight of the element $u=3+g+2g^2\in \mathbf{Z}_5C_3$ is 3.

The minimum weight of a submodule M in RG is $w(M)=\min\{|supp(u)|\,\|\,0\neq u\in M\}$.

The map

$\theta: RG\to R^n$, $\theta\left(\sum_{i=1}^{n}\alpha_i g_i\right)=(\alpha_1,\alpha_2,\ldots,\alpha_n)$ is a ring isomorphism from RG to R^n. Thus, every element in RG can be considered as an n-tuple in R^n.

Example 2.3. For instance, the element $u = 3 + g + 2g^2 \in \mathbf{Z}_5 C_3$ can be mapped as $\theta(u) = (3,1,2)$.

3. OVERVIEW OF UNIT DERIVED CODES FROM GROUP RINGS

In this section, we remind some basics of unit derived codes obtained from group rings. For further and detailed information readers may refer to [5].

Definition 3.1. Let u be a unit element in RG, i.e., $uv = vu = 1$ for some non-zero $v \in RG$. Let W be a submodule of RG with basis of group elements $S \subseteq G$. Then a unit derived code is $\mathrm{C} = \{ux \mid x \in W\}$.

In the following, we give an example of unit derived codes from group ring $\mathbf{Z}_2 C_4$.

Example 3.1. Let G be the cyclic group $C_4 = \langle g \rangle = \{1, g, g^2, g^3\}$ and R be the finite field $\mathbf{Z}_2 = \{0,1\}$. Then

$$\mathbf{Z}_2 C_4 = \begin{Bmatrix} 0,1,g,g^2,g^3,1+g,1+g^2,g+g^2, \\ 1+g+g^2,1+g^3,g+g^3,1+g+g^3, \\ g^2+g^3,1+g^2+g^3,g+g^2+g^3, \\ 1+g+g^2+g^3 \end{Bmatrix}$$

and the set of units of $\mathbf{Z}_2 C_4$ is

$$U(\mathbf{Z}_2 C_4) = \begin{Bmatrix} 1,g,g^2,g^3,1+g+g^2, \\ 1+g+g^3,1+g^2+g^3,g+g^2+g^3 \end{Bmatrix}$$

If we take $u = 1+g+g^2$, then $u^{-1} = 1+g^2+g^3$ and $(u^{-1})^T = 1+g+g^2$. For the submodule $W = \langle \{1,g\} \rangle = \{0,1,g,1+g\}$ we have a $[4,2,2]_2$ unit derived code

$$\mathrm{C} = \{ux \mid x \in W_1\} = \{0,1+g+g^2,g+g^2+g^3,1+g^3\}$$

and

$$\theta(\mathrm{C}) = \{0000,1110,0111,1001\}.$$

In Theorem 3.1 we give the relation between a unit derived code and its dual.

Theorem 3.1. (see [5]) Let W be a submodule with basis of group elements $S \subset G$ and $W^\perp$ be the submodule with the basis $G - S$. Let $u \in RG$ be a unit such that $u.u^{-1} = u^{-1}u = 1$. Then the dual code of $\mathrm{C} = \{xu \mid x \in W\}$ is $\mathrm{C}^\perp = \left\{ x\left(u^{-1}\right)^T \,\middle|\, x \in W^\perp \right\}$.

4. LCD CODES FROM GROUP RINGS

In this section, we provide a condition for linear codes obtained from units of group rings to be LCD.

In Theorem 4.1 we give a condition for unit derived codes to be LCD.

Theorem 4.1. Let R be a ring and $G = \{g_1, g_2, \ldots, g_n\}$ be a cyclic group of order n. Also let $S \subseteq G$ such that $W = \langle S \rangle$ and $W^\perp = \langle G - S \rangle$ be R-submodules of the group ring RG. For a given unit element $u \in RG$ let the unit derived code and its dual be $\mathrm{C} = \{ux \mid x \in W\}$ and $\mathrm{C}^\perp = \left\{ \left(u^{-1}\right)^T y \,\middle|\, y \in W^\perp \right\}$ respectively. Then $\mathrm{C} \cap \mathrm{C}^\perp = \{0\}$ if and only if $u^{-1} = u^T$.

Proof: Let $u^{-1} = u^T$ and assume that $\mathrm{C} \cap \mathrm{C}^\perp \neq \{\mathbf{0}\}$. Then, there exists at least one element $0 \neq z \in \mathrm{C} \cap \mathrm{C}^\perp$ such that $z = ux = \left(u^{-1}\right)^T y$. Since $u^{-1} = u^T$ we have $z = ux = \left(u^T\right)^T y \Rightarrow ux = uy$. Hence, we have $0 \neq x = y$. This is a contradiction, because $W \cap W^\perp = \{\mathbf{0}\}$.

On the other hand, let $\mathrm{C} \cap \mathrm{C}^\perp = \{\mathbf{0}\}$ be. Then, for $0 \neq x \in W$, $0 \neq y \in W^\perp$ there exists $ux \in \mathrm{C}$, $\left(u^{-1}\right)^T y \in \mathrm{C}^\perp$. If ux and $\left(u^{-1}\right)^T y \in \mathrm{C} \cap \mathrm{C}^\perp$, then $ux = \left(u^{-1}\right)^T y = 0$. Therefore, it can be seen that

$uxy = 0$ and $\left(u^{-1}\right)^T xy = 0$. This means that $uxy - \left(u^{-1}\right)^T xy = xy\left(u - \left(u^{-1}\right)^T\right) = 0$. As a result, $u - \left(u^{-1}\right)^T = 0$ and then $u = \left(u^{-1}\right)^T$. By taking the transpose of both sides we can get $u^{-1} = u^T$.

In Example 4.1, we provide an example of LCD unit derived codes.

Example 4.1. Let G be the cyclic group $C_6 = \langle g \rangle = \{1, g, g^2, g^3, g^4, g^5\}$ and R be the finite field $\mathbf{Z}_2 = \{0,1\}$. If we take the unit element $u = 1 + g + g^2 + g^4 + g^5 \in \mathrm{F}_2 C_6$, then $u^T = u = u^{-1}$. For the submodule $W = \langle \{1, g^2, g^4\} \rangle$

$= \{0, 1, g^2, 1+g^2, g^4, 1+g^4, g^2+g^4, 1+g^2+g^4\}$,

we have a $[6,3,2]_2$ unit derived code

$$\mathrm{C} = \{ux \mid x \in W\} = \begin{Bmatrix} 0, g+g^3, 1+g^2+g^4, \\ 1+g+g^2+g^3+g^4, \\ g+g^5, g^3+g^5, \\ 1+g+g^2+g^4+g^5, \\ 1+g^2+g^3+g^4+g^5 \end{Bmatrix}$$

and

$$\theta(\mathrm{C}) = \begin{Bmatrix} 000000, 010100, 101010, 111110, \\ 010001, 000101, 111011, 101111 \end{Bmatrix}.$$

For

$$W^{\perp} = \langle \{g, g^3, g^5\} \rangle = \begin{Bmatrix} 0, g, g^3, g+g^3, g^5, g+g^5, \\ g^3+g^5, g+g^3+g^5 \end{Bmatrix}$$

the dual code $\mathrm{C}^{\perp}$ is

$$\mathrm{C}^{\perp} = \left\{ \left(u^{-1}\right)^T x \,\middle|\, x \in W^{\perp} \right\} = \begin{Bmatrix} 0, 1+g^2, 1+g^4, g^2+g^4, \\ g+g^3+g^5, 1+g+g^2+g^3+g^5, \\ 1+g+g^3+g^4+g^5, \\ g+g^2+g^3+g^4+g^5 \end{Bmatrix}$$

and

$$\theta\left(\mathrm{C}^{\perp}\right) = \begin{Bmatrix} 000000, 101000, 100010, 010010, \\ 010101, 111101, 110111, 011111 \end{Bmatrix}.$$

Notice that $\mathrm{C} \cap \mathrm{C}^{\perp} = \{000000\}$ and so C is an LCD code.

5. LCD CODES FROM A DECOMPOSITION OF GROUP RINGS

In this section, we give a decomposition of group rings with two summands and then we have shown that each summand is treated as a linear code which is the dual of the other, and that the LCD condition is satisfied.

Let RG be a group ring and $\alpha = \sum_{g \in G} \alpha_g g \in RG$ then the involution of the element α is defined as $\alpha^* = \sum_{g \in G} \overline{\alpha}_g g^{-1}$, where α_g and $\overline{\alpha}_g \in R$.

Theorem 5.1. Let RG be a group ring. Define the sets

$$RG^+ = \left\{ \alpha = \sum_{g \in G} \alpha_g g \,\middle|\, \alpha^* = \alpha \right\}$$

and

$$RG^- = \left\{ \alpha = \sum_{g \in G} \alpha_g g \,\middle|\, \alpha^* = -\alpha \right\}.$$

Then $RG = RG^+ \oplus RG^-$ and $RG^+ \cap RG^- = \{0\}$. Further, for all $x \in RG^+$ and $y \in RG^-$ $\langle x, y \rangle = 0$.

Proof: Let $\alpha = \sum_{g \in G} \alpha_g g$ and $\beta = \sum_{g \in G} \beta_g g \in RG^+$. Since $(\alpha + \beta)^* = \alpha^* + \beta^* = \alpha + \beta$ and $(\alpha\beta)^* = \alpha^* \beta^*$ we have $\alpha + \beta$ and $\alpha\beta \in RG^+$.

This shows that the set RG^+ is a subring of RG. Also, for $\alpha=\sum_{g\in G}\alpha_g g\in RG^+\cap RG^-$ we have $\alpha^*=\alpha=-\alpha$ i.e., $\sum_{g\in G}\alpha_g g=-\sum_{g\in G}\alpha_g g$ $\Rightarrow \alpha_g=-\alpha_g\ (\forall g\in G)$. This is possible only when $\alpha=\sum_{g\in G}\alpha_g g=0$. This shows that $RG^+\cap RG^-=\{0\}$.

On the other hand, let $x\in RG^+$ and $y\in RG^-$. Since $RG=RG^+\oplus RG^-$ and $RG^+\cap RG^-=\{0\}$ we have $\langle x,y\rangle=0$.

Corollary 5.1. Let $\mathrm{C}=RG^+$ and $\mathrm{C}^{\perp}=RG^-$. Then C is an LCD code.

Example 5.1. Let R be the ternary field $\mathbf{Z}_3=\{0,1,2\}$ and G be the cyclic group $C_3=\{1,g,g^2\}$ of order 3. Then we have the group ring

$$RG=\begin{Bmatrix}0,1,2,g,2g,g^2,2g^2,1+g,2+g,\\1+2g,2+2g,1+g^2,2+g^2,\\g+g^2,1+g+g^2,2+g+g^2,\\2g+g^2,1+2g+g^2,2+2g+g^2,\\1+2g^2,2+2g^2,g+2g^2,\\1+g+2g^2,2+g+2g^2,2g+2g^2,\\1+2g+2g^2,2+2g+2g^2\end{Bmatrix}.$$

From Theorem 5.1, we also have

$$RG^+=\begin{Bmatrix}0,1,2,1+g+g^2,2+g+g^2,\\2g+2g^2,1+2g+2g^2,2+2g+2g^2\end{Bmatrix}$$

$$RG^-=\{0,2g+g^2,g+2g^2\}$$

and

$$\theta(RG^+)=\{000,100,200,111,211,022,122,222\}=\mathrm{C}$$

$$\theta(RG^-)=\{000,021,012\}=\mathrm{C}'.$$

It can be easily seen that the dual code of C is C' and $\mathrm{C}\cap\mathrm{C}'=\{\mathbf{0}\}$. This shows that C is LCD.

6. LCP OF CODES FROM UNIT OF GROUP RINGS

Recently, Carlet et al., have generalized the concept of LCD codes to the linear complementary pair (LCP) of codes [6]. Let C and $\overline{\mathrm{C}}$ be two linear codes of length n over finite field F_q. The pair of linear codes $(\mathrm{C},\overline{\mathrm{C}})$ is called a linear complementary pair (LCP) of codes if $\mathrm{C}\cap\overline{\mathrm{C}}=\{\mathbf{0}\}$ or equivalently $\mathrm{F}_q^n=\mathrm{C}\oplus\overline{\mathrm{C}}$. Notice that, if $\overline{\mathrm{C}}=\mathrm{C}^{\perp}$, then C is an LCD code [6].

Let R be a ring and $G=\{g_1,g_2,\ldots,g_n\}$ be a group. For the unit element $u\in RG$ there exists $u^{-1}\in RG$ such that $uu^{-1}=u^{-1}u=1$. For any $u=\sum_{i=1}^{n}a_ig_i\in RG$, where $a_i\in R$ and $g_i\in G$, define $\varphi: RG\to M_n(R)$ such that

$$\varphi(u)=\begin{pmatrix}a_{g_1^{-1}g_1} & a_{g_1^{-1}g_2} & \cdots & a_{g_1^{-1}g_n}\\ a_{g_2^{-1}g_1} & a_{g_2^{-1}g_2} & \cdots & a_{g_2^{-1}g_n}\\ \vdots & \vdots & \vdots & \vdots\\ a_{g_n^{-1}g_1} & a_{g_n^{-1}g_2} & \cdots & a_{g_n^{-1}g_n}\end{pmatrix}.$$

Clearly φ is an isomorphism from RG to a subset of $M_n(R)$. This enables us to write $\varphi(u)\varphi(u^{-1})=I_n$. Let $\varphi(u)=U=\begin{pmatrix}A\\B\end{pmatrix}$ and $\varphi(u^{-1})=U^{-1}=(E\quad D)$, where A,B,E,D are matrices of the form $k\times n$, $(n-k)\times n$, $n\times k$ and $n\times(n-k)$ respectively. Since $\varphi(u)\varphi(u^{-1})=I_n$ we have $\begin{pmatrix}A\\B\end{pmatrix}(E\quad D)=\begin{pmatrix}AE & AD\\BE & BD\end{pmatrix}=I_n$. Thus

$AD = 0_k$ and $BE = 0_{n-k}$, where 0_k is $k \times k$ all zero matrix.

The linear code C of dimension k, generated by the matrix A is the unit derived code $\mathrm{C} = \{ux \mid x \in W\}$, where $S \subseteq G$ and $W = \langle S \rangle$. The dual code $\mathrm{C}^{\perp}$ is the linear code generated by the matrix D^T with dimension $(n-k)$. The dual code can be considered as the submodule $\mathrm{C}^{\perp} = \left\{ \left(u^{-1}\right)^T y \,\middle|\, y \in W^{\perp} \right\}$ where $W^{\perp} = \langle G - S \rangle$.

Theorem 6.1. Let $u, u^{-1} \in RG$, $uu^{-1} = u^{-1}u = 1$ and $\varphi(u) = \begin{pmatrix} A \\ B \end{pmatrix}$ and $\varphi\left(u^{-1}\right) = \begin{pmatrix} E & D \end{pmatrix}$, where A, B, E, D are matrices of the form $k \times n$, $(n-k) \times n$, $n \times k$ and $n \times (n-k)$ respectively. Further, let C and $\overline{\mathrm{C}}$ be codes generated by the matrices A and B of dimension k and $n-k$, respectively. Then the pair $(\mathrm{C}, \overline{\mathrm{C}})$ is an LCP of codes.

Proof: We know that C and $\overline{\mathrm{C}}$ are linear codes of dimension k and $n-k$ respectively. It is obvious from the genetator matrices of C and $\overline{\mathrm{C}}$ we have $\mathrm{C} \cap \overline{\mathrm{C}} = \{\mathbf{0}\}$. This means that $\mathrm{C} \oplus \overline{\mathrm{C}}$ has dimension n and so we get $\mathrm{F}_q^n = \mathrm{C} \oplus \overline{\mathrm{C}}$. This shows that the pair $(\mathrm{C}, \overline{\mathrm{C}})$ of codes is an LCP of codes.

Corollary 6.1. The pair of linear codes $\left(\mathrm{C}^{\perp}, \overline{\mathrm{C}}^{\perp}\right)$ is also an LCP of codes.

Exaple 6.1. Let $u = g + g^2 + g^6 + g^7 + g^8 \in \mathbf{Z}_2 C_9$ where C_9 is the cyclic group of order 9. Then, $u^{-1} = 1 + g^2 + g^5$ and $\varphi(u) = circ(0,1,1,0,0,0,1,1,1)$, where $circ(.)$ is the circulant matrix with the first row $(0,1,1,0,0,0,1,1,1)$ and $\varphi\left(u^{-1}\right) = circ(1,0,1,0,0,1,0,0,0)$.

Then $\varphi(u)\varphi\left(u^{-1}\right) = I_9 = \begin{pmatrix} AE & AD \\ BE & BD \end{pmatrix}$, where

$$A = \begin{pmatrix} 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \end{pmatrix},$$

$$B = \begin{pmatrix} 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix},$$

Then C is a $[9,\ 4,\ 3]_2$ code and $\overline{\mathrm{C}}$ is a $[9,\ 4,\ 3]_2$ code. Thus, the pair $(\mathrm{C}, \overline{\mathrm{C}})$ of codes is an LCP of codes.

7. CONCLUSION AND FUTURE REMARKS

In this paper, we give a condition for linear codes obtained from units of group rings to be LCD. Additionally, we give a special decomposition of group rings with two summands. Then we have shown that each component of the obtained decomposition is treated as a linear code, which is the dual of the other, and that the LCD condition is satisfied. Further, we have proposed a construction method to obtain LCP of codes. The results obtained are also valid for non-commutative group rings. This provides a very convenient way to search for parameters of new LCD codes and LCP of codes.

REFERENCES

[1] J. L. Massey, "Linear codes with complementary duals," *Discrete Math,* vol. 106, pp. 337–342, 1992.

[2] N. Sendrier, "Linear codes with complementary duals meet the Gilbert-

Varshamov bound," *Discrete Math,* vol. 285, pp. 345-347, 2004.

[3] C. Carlet and S. Guilley, S. (2016). "Complementary dual codes for counter-measures to side-channel attacks," *Adv. Math. Commun,* vol. 10, pp. 131-150, 2016.

[4] C.P. Milies, K.S. Sudarshan, "An introduction to group rings," vol.1. Springer, Nedherlands, 2002.

[5] P. Hurley, T. Hurley, "Codes from zero-divisors and units in group rings," *Int. J. Inf. Coding Theory* vol. 1 pp. 57-87, 2009.

[6] C. Carlet, C. Güneri, F. Özbudak, B. Özkaya, P. Solé, "On linear complementary pairs of codes". *IEEE Trans. Inform. Theory*, vol. 64, pp. 6583-6589, 2018.