Published by
NIGERIAN SOCIETY OF PHYSICAL SCIENCES
Available online @ https://asr.nsps.org.ng/index.php/asr

African Scientific Reports 2 (2023) 98

African Scientific Reports

Coding Matrices for Wreath Products of Groups

Enoch Suleiman[a,*], Ahmed A. Khammash[b]

[a] *Department of Mathematics, Federal University Gashua, Yobe State, Nigeria*
[b] *Department of Mathematical Sciences, Umm Al-Qura University, Makkah, Saudi Arabia*

Abstract

Wreath product, a powerful construction in group theory, has found extensive applications in various areas of mathematics and computer science. In this paper, we present a comprehensive analysis of coding matrices associated with wreath products. The coding matrices for the wreath product of two cyclic finite groups were given for the first time. It gives a generalization of the coding matrices for the semi-direct product. We found out that the coding matrix of wreath product really has the same shape as the one for semidirect product and gave the RW-matrix for the coding matrix. An example was showed to illustrate the assertions. Conditions were also given for different wreath products of cyclic groups and that gives different orders for the wreath products.

DOI:10.46481/asr.2023.2.2.114

Keywords: Code, Ring of matrices, Group ring, Wreath product, Semi direct product, Matrix

Article History :
Received: 21 April 2023
Received in revised form: 04 June 2023
Accepted for publication: 12 June 2023
Published: 11 July 2023

Communicated by: Tolulope Latunde

1. Introduction

Many people have work on coding matrices over the years, [1] showed that the group ring RG of a group G of order n over a ring R is isomorphic to a certain ring of $n \times n$ matrices over R. At the instance that the ring R has an identity element and no zero-divisors, the representation made it easier to describe the units and zero-divisors of the group ring in terms of properties of these matrices and where applicable in terms of the determinant of the matrices. Such rings of matrices which turn up as isomorphic to certain group rings include circulant matrices, Toeplitz matrices, Walsh-Toeplitz matrices, circulant or Toeplitz combined with Hankel matrices and block-type circulant matrices. Group rings thus can be considered to be a generalisation of these rings of matrices, which are useful in communications, signal

[*] Corresponding author tel. no: +234 7084701525
Email address: enochsuleiman@gmail.com (Enoch Suleiman)

processes, time series analysis and somewhere else. The new construction method for codes using encodings from group rings is described and presented in [2]. The new construction consisted mainly of two types: zero-divisor and unit-derived codes and previous codes from group rings focused on ideals. They focused on the encodings themselves, which only under very limited conditions result in ideals. They used the result that a group ring is isomorphic to a certain well-defined ring of matrices, and accordingly every group ring element has an associated matrix which allows matrix algebra to be used as needed in the production of codes, enabling the creation of standard generator and check matrices. [3] presented a general method for constructing convolutional codes from units in Laurent series over matrix rings. In the study [4], the algebra of groups ring and matrix rings is used for the construction and analysis of systems of zero-divisor and unit-derived codes which are more general than codes from ideals in group rings. They expanded the space of linear block codes, offering additional flexibility in terms of the desired properties as algebraic formulations, while having readily available generator and check matrices. It is further showed how the codes may be derived, showing particular cases such as self-dual codes and codes from dihedral group rings.

The BN-pair structure is used in [5] for the general linear group to write a suitable listing of the elements of the finite group GL(2,q) which they used to determine its ring of matrices. This method of identifying finite group ring with ring of matrices was used effectively to construct linear codes, furthering from the ring-theoretic structure of both group rings and the ring of matrices. The coding matrix of the semi-direct product group of two cyclic groups os determined in [6] in order to generalize the known result for the dihedral group, which is known to be a semi-direct of the two cyclic groups. in [7], a well-established isomorphism between a group ring and a ring of matrices and constructed certain self-dual and formally self-dual codes over a finite commutative Frobenius ring. He found out that there are interesting relationships between the Automorphism group of the code produced and the underlying group in the group ring. He further described all possible group algebras that can be used to construct the well-known binary extended Golay code.

The paper provides theoretical insights into the properties and relationships between coding matrices and wreath products. These insights deepen our theoretical understanding of coding matrices and their characterization in terms of wreath product parameter.

We give some basic definitions in the following section.

2. Basic Definition

Definition 2.1[1]: Let RG denote the group ring of the group G over the ring R. A non-zero element z in a ring W is said to be a zero-divisor in W if and only if there exists a non-zero element $r \in W$ with $z * r = 0$. When W has an identity 1_W say u is a unit in W if and only if there exists an element $w \in W$ with $u * w = 1_W$. The group of units of W is denoted by $U(W)$. We shall be particularly interested in zero-divisors and units in RG.

It is shown for example that over a field every element is either a unit or a zero-divisor;

This was known for finite fields.

Let G be a finite group of order n, and let $\{g_1, g_2, \ldots, g_n\}$ be the elements of G, let $M(G)$ be of the form

$$M(G) = \begin{pmatrix} g_1^{-1}g_1 & g_1^{-1}g_2 & \cdots & g_1^{-1}g_n \\ g_2^{-1}g_1 & g_2^{-1}g_2 & \cdots & g_2^{-1}g_n \\ \vdots & \vdots & \ddots & \vdots \\ g_n^{-1}g_1 & g_n^{-1}g_2 & \cdots & g_n^{-1}g_n \end{pmatrix}_{n\times n} = \begin{pmatrix} 1 & g_1^{-1}g_2 & \cdots & g_1^{-1}g_n \\ g_2^{-1}g_1 & 1 & \cdots & g_2^{-1}g_n \\ \vdots & \vdots & \ddots & \vdots \\ g_n^{-1}g_1 & g_n^{-1}g_2 & \cdots & 1 \end{pmatrix}_{n\times n}$$

Then for each $u = \sum_{i=1}^{n} \alpha_{g_i} g_i \in RG$, define the matrix $M(RG, w) \in M_n(R)$ as follows:

$$M(RG, w) = \begin{pmatrix} \alpha_{g_1^{-1}g_1} & \alpha_{g_1^{-1}g_2} & \cdots & \alpha_{g_2^{-1}g_n} \\ \alpha_{g_2^{-1}g_1} & \alpha_{g_2^{-1}g_2} & \cdots & \alpha_{g_2^{-1}g_n} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{g_n^{-1}g_1} & \alpha_{g_n^{-1}g_2} & \cdots & \alpha_{g_n^{-1}g_n} \end{pmatrix}_{n\times n} = \begin{pmatrix} \alpha_1 & \alpha_{g_1^{-1}g_2} & \cdots & \alpha_{g_2^{-1}g_n} \\ \alpha_{g_2^{-1}g_1} & \alpha_1 & \cdots & \alpha_{g_2^{-1}g_n} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{g_n^{-1}g_1} & \alpha_{g_n^{-1}g_2} & \cdots & \alpha_1 \end{pmatrix}_{n\times n}$$

It is rather clear that the shape as well as the coefficients of the coding matrix $M(RG, u)$ depends on the group elements of the group G. The group ring RG of a group G of order n over a ring R is isomorphic to a certain ring of $(n \times n)$ matrices over R [1].

Theorem 2.2[1]: Given a listing of the elements of a group G of order n there is a bijective ring homomorphism between RG and the $(n \times n)$ G-matrices over R. This bijective ring homomorphism is given by $\sigma : w \longmapsto M(RG, w)$.

Theorem 2.3[1]: Suppose R has an identity. Then $w \in RG$ is a unit in RG if and only if $\sigma(w)$ is a unit in $R_{n\times n}$, where $R_{n\times n}$denotes the ring of $(n \times n)$ matrices with coefficients from R.

Definition 2.4[1,3]: Let C be an (n, k)-code and let G be a $(k \times n)$-matrix whose rows are the basis for C, then G is called a *generator matrix* for C.

A parity-check matrix H for an (n, k)-code C is a generator matrix of $C^{\perp}$, such that the dual code $C^{\perp}$ is defined by

$$C^{\perp} = \left\{ w \in \mathbb{F}_q^n | w.v = 0 \text{ for all } w \in W \right\}.$$

Definition 2.5[1,3]: Let RG be the group ring of the group G over the ring R, where the listing of the elements of G is given by$\{g_1, g_2, \ldots, g_n\}$. Suppose W is a submodule of RG, $x \in W$ and $w \in RG$ is given. Then the group ring encoding is a mapping $f : W \longrightarrow RG$ such that $f(x) = xw$ or $f(x) = wx$. In the first case, f is a right group ring encoding and in the letter case is a left group ring encoding.

Thus, a code C derived from a group ring encoding is the image of a group ring encoding, for a given $w \in RG$, either $C = \{wx : x \in W\}$ or $C = \{xw : x \in W\}$

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

In the group ring the multiplication is not necessary be commute, and this allows the construction of non-commutative.

Definition 2.6[1]: If $xw = wx$ for all x, then the code $C = \{xw : x \in W\}$ is said to be *commutative*, and otherwise *non-commutative* codes.

When w is a zero-divisor, it generates a zero-divisor code and when it is a unit, it generates a unit-derived code. The structure of codes from unit and zero-divisor in RG.

Example 2.7: Let $R = \mathbb{Z}_2 = \{0, 1\}$ be the finite field of two elements and $G = C_4 = \left\langle a | g^4 = 1 \right\rangle = \{1, g, g^2, g^3\}$ be the cyclic group of order 4. Then the coding matrices for C_4 is given by

	1	g	g^2	g^3
1	1	g	g^2	g^3
g^3	g^3	1	g	g^2
g^2	g^2	g^3	1	g
g	g	g^2	g^3	1

Thus,

$$M(C_4) = \begin{pmatrix} 1 & g & g^2 & g^3 \\ g^3 & 1 & g & g^2 \\ g^2 & g^3 & 1 & g \\ g & g^2 & g^3 & 1 \end{pmatrix}_{4\times 4}$$

And the group ring $RG = (\mathbb{Z}_2 C_4 = \sum_{x\in C_4} \alpha_x x | \alpha_x \in \mathbb{Z}_2 = \left\{ c_0 + c_1 g + c_2 g^2 + c_3 g^3 \;\middle|\; c_i \in \mathbb{Z}_2 \right\}$, such that $(\mathbb{Z}_2 C_4, +, \bullet)$ is $\mathbb{F}$-algebra. From Hurley's theorem, $\mathbb{Z}_2 C_4$ Is embedded in $M_{|C_4|\times|C_4|}(\mathbb{Z}_2)$. So if $w \in \mathbb{Z}_2 C_4$, that is , $w = c_0 + c_1 g + c_2 g^2 + c_3 g^3$, then

$$M(\mathbb{Z}_2 C_4, w) = \begin{pmatrix} c_0 & c_1 & c_2 & c_3 \\ c_3 & c_0 & c_1 & c_2 \\ c_2 & c_3 & c_0 & c_1 \\ c_1 & c_2 & c_3 & c_0 \end{pmatrix}_{4\times 4}$$

For the unit element $w = 1 + g + g^3 \in U(C_4, w)$ there exists $w^{-1} = 1 + g + g^3$ such that $ww^{-1} = 1$. Then we have

$M(\mathbb{Z}_2C_4, w)$ as follows

$$M(\mathbb{Z}_2C_4, w) = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix}_{4\times 4}$$

Also, from Hurley's theorems : If R has an identity 1_R, then $w \in RG$ is a unit if and only if $\sigma(w)$ is a unit in $R_{n\times n}$. Hence we have the invertible matrix as follows:

$U = \begin{pmatrix} A \\ B \end{pmatrix}$ and $V = \begin{pmatrix} C & D \end{pmatrix}$ such that $UV = 1_{4\times 4}$ in $R_{4\times 4}$.

Taking any r rows of U as a generator matrix to define an (n, r)-code. Then we have:

$$A = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}_{2\times 4}, B = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix}_{2\times 4}, C = \begin{pmatrix} 1 & 1 \\ 1 & 1 \\ 0 & 1 \\ 1 & 0 \end{pmatrix}_{4\times 2}, D = \begin{pmatrix} 0 & 1 \\ 1 & 0 \\ 1 & 1 \\ 1 & 1 \end{pmatrix}_{4\times 2}$$

Such that

$AC = BD = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}_{2\times 2}$ and $= BC = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}_{2\times 2}$. Then,

$$UV = \begin{pmatrix} A \\ B \end{pmatrix} \bullet \begin{pmatrix} C & D \end{pmatrix} = \begin{pmatrix} AC & AD \\ BC & BD \end{pmatrix} = \begin{pmatrix} I_2 & 0_2 \\ 0_2 & I_2 \end{pmatrix} = I_{4\times 4}.$$

The linear code C of dimension $k = 2$, generated by the matrix

$$A = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}_{2\times 4},$$

is the unit derived code $\mathbb{C} = \{wx \mid x \in W\}$, *where* $S = \{g\} \subset G$ and $W = \left\langle g^2 \right\rangle = \{1, g^2\}$. The dual code $\mathbb{C}^{\perp}$ generated by the matrix

$$D^T = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix}_{2\times 4}$$

With dimension $n - k = 2$. The dual code is considered as the submodule $\mathbb{C}^{\perp} = \{(u^{-1})^T y | y \in W^{\perp}\}$ where $W^{\perp} = G - S = \left\{g, g^3\right\}$. So, $\mathbb{C} = \{wx \mid x \in W\} = \{1 + g^2 + g^3,\ 1 + g + g^2\}$, $\theta\left(\mathbb{C}\right) = \{1011,\ 1101\}$, $\mathbb{C}^{\perp} = \left\{\left(u^{-1}\right)^T y | y \in W^{\perp}\right\} = \{1 + g + g^3, g + g^2 + g^3\}$ $\theta\left(\mathbb{C}^{\perp}\right) = \{1101,\ 0111\}$. Clearly, the matrix A is the generated matrix for an $(4, 2)$-code, and D^T is the parity-check matrix for this code, since this code is a generator matrix for $\mathbb{C}^{\perp}$ as defined above.

Definition 2.8[11]: Let R be a ring. A subset M with two binary operations + and • are called an $R - module$ if M is an abelian group under the operation + and •, and the following axioms hold:

1. $rm \in M$,
2. $(r + s)m = rm + sm$,
3. $r(m + m_1) = rm + rm_1$,
4. $r(sm) = (rs)m$,
5. $1m = m$,

For all $r, s \in R$, and $m, m_1 \in M$.

Definition 2.9[11]: A non-empty subset N of an $R-$module M is known as an $R - submodule$ of M if for all $r \in R$, and $n, n_1 \in N$

1. $rn \in N$
2. $n + n_1 \in N$.

It is known that the group ring RG is an $R-$module with scalar multiplication defined as

$$r\sum_{g\in G}\alpha_g g = \sum_{g\in G}\left(r\alpha_g\right)g$$

For all $r \in R$ and $\sum_{g\in G}\alpha_g g \in RG$.

Definition 2.10[11]: Given two $R-$submodule M and N. A mapping $T : M \longrightarrow N$ is called an $R-$ *linear map* if for all $r \in R$ and $m, m_1 \in M$,

1. $T(m + m_1) = T(m) + T(m_1)$
2. $T(rm) = rT(m)$

A bijective $R-$linear map T is known as an isomorphism. The modules M and N are said to be isomorphic if there exists an isomorphism T between them.

Definition 2.11[11]: The kernel and the image of the $R-$linear map $T : M \longrightarrow N$ are defined by
$\ker(T) = \{m \in M\,|T(m) = 0\}$, $Im(T) = \{T(m) \in N|\, m \in M\}$are $R-$submodules of M and N , respectively. Also, T is one-to-one if and only if $\ker\{T\} = \{0\}$.

Proposition 2.12[11]: Let $\gamma : g_1 < g_2 < \cdots < g_n$ be an ordering on G. The $R-linear$ map $T_\gamma : RG \longrightarrow R^n$ with respect to γ is defined by

$$T_\gamma\left(\alpha_{g_1}g_1 + \alpha_{g_2}g_2 + \cdots + \alpha_{g_n}g_n\right) = \alpha_{g_1}\alpha_{g_2}\ldots\alpha_{g_n}$$

Is a module isomorphism and thus RG and R^n are isomorphic.

Let $\mathbb{F}_q$ be a finite field or order q.

Definition 2.13[11]: Let RG be a group ring where R is an integral domain, G a group. Let W be a submodule of RG and $u \in RG - \{0\}$. The map $f_u : W \longrightarrow RG$ defined by $f_u(x) = xu$, where

1. $f_u(x + y) = (x + y)u = xu + yu = f_u(x) + f_u(y)$
2. $f_u(\alpha x) = (\alpha x)u = \alpha(xu) = \alpha f_u(x)$, for all $x, y \in RG$ and $\alpha \in R$ is called an $R-$*linear map.*

Definition 2.14[11]: Let RG be a group ring. Suppose W is a R-submodule of RG and $u \in RG - \{0\}$. A one-to-one mapping $f_u : W \longrightarrow RG$ given by $f_u(u) = xu$ is known as a *group ring encoding function*. The RG -code with generator u comparative to the submodule W, denoted $C_G(W, u)$, is the image of f_u , that is

$$C_G(W, u) = f_u[W] = Wx$$

Note that $C_G(W, u)$ is an R -submodule of RG. Clearly, W is isomorphic to $C_G(W, u)$ under f_u and thus $rank(W) = rank(C_G(W, u))$ Suppose N is a basis of W. It can be verified easily that $C_G(W, u) = Wu = L_R(Nu)$. Since f_u is one-to-one, the linear independency of N over R guarantees the linear independency of Nu over R. Hence, Nu is a basis of $C_G(W, u)$ and $rank(C_G(W, u)) = |Nu| = |N|$.

Let the RG code $C_G(W, u) = C_G(L_R(N), u)$ be represented as $C_G(N, u)$.

Definition 2.15[11]: Let $u \in RG - \{0\}$ and $N \subseteq G$ with Nu as linearly independent. The RG-code $C_G(N, u)$ is known as a *zero-divisor* code if u is a zero-divisor.

Otherwise, $C_G(N, u)$ is known as a unit-derived code when $u \in RG$ is a unit.

Since $C_G(N,u)$ over $\mathbb{F}_q$ is the image of an injective linear transformation. Let $\gamma : g_1 < g_2 < \cdots < g_n$ be an ordering on G. The isomorphism $T_\gamma : \mathbb{F}_qG \longrightarrow \mathbb{F}_q^n$ with respect to γ is defined by

$$T_\gamma(\alpha_1 g_1 + \alpha_2 g_2 + \cdots + \alpha_n g_n) = \alpha_1\alpha_2 \ldots \alpha_n$$

Hence, each codeword in each $\mathbb{F}_qG$ -code $C_G(N,u)$ will be related to its isomorphic image under T_γ and $C_G(N,u)$ will be allied to $T_\gamma[C_G(N,u)] = Im\left(T_\gamma|_{C_G(N,u)}\right)$, which is a linear code of length n.

Nu is a basis of $C_G(N,u)$. Thus, $T_\gamma[Nu]$ is a basis for the linear code $T_\gamma[C_G(N,u)]$.

Example 2.16: Consider the group ring $\mathbb{F}_2[C_2wrC_2]$ where $C_2wrC_2 = \{1, x, y, xy, z, xz, yz, xyz\}$ (see Definition 3.1)

Let $\gamma : 1 < x < y < xy < z < xz < yz < xyz$ and let $u = 1 + y$, $N = \{1, x\}$, $N_1 = \{1, z\}$ and $N_3 = \{1, y\}$, then

$$C_{C_2wrC_2}(N,u) = L_{\mathbb{F}_2}(\{1+y, x+xy\}) = \{0, 1+y, x+xy, 1+x+y+xy\}$$

$$T_\gamma[C_{C_2wrC_2}(N,u)] = \{00000000, 10100000, 01010000, 11110000\}$$

$$C_{C_2wrC_2}(N_1,u) = L_{\mathbb{F}_2}(\{1+y, z+yz\}) = \{0, 1+y, z+yz, 1+y+z+yz\}$$

$$T_\gamma[C_{C_2wrC_2}(N_1,u)] = \{00000000, 10100000, 00001010, 10101010\}$$

$$C_{C_2wrC_2}(N_2,u) = L_{\mathbb{F}_2}(\{1+y, 1+y\}) = \{0, 1+y, 1+y, 0\}$$

$$T_\gamma[C_{C_2wrC_2}(N_2,u)] = \{00000000, 10100000, 10100000, 00000000\}$$

Section 3 gives the definition of wreath products and lists the elements of the wreath products of two finite cyclic groups (see [8,9,10]).

3. Coding Matrices of Wreath Product of Groups

Definition 3.1[10]: Let C and D be groups and suppose D acts on the nonempty set Δ. Then the *wreath product* of C by D is defined with respect to this action; it is defined to be the semidirect product $C^\Delta \rtimes D$, where D acts on the group C^Δ via

$$f^d(\gamma) := f(\gamma^{d^{-1}})$$

for all $f \in C^\Delta$,$\gamma \in \Delta$ and $d \in D$.

We denote this group by $CwrD$, and call the subgroup $B := \{(f,1)|f\in C^\Delta \cong C^\Delta\}$ the *base group* of the wreath product.

Again, it is helpful to look at the case where Δ is finite, say $\Delta = \{1, 2, \ldots, n\}$. In this case we can identify the base group B with the direct product $C \times C \times \cdots \times C$ (n factors).

Obviously, $|CwrD| = |C|^n\,|D|$.

Example 3.2: The wreath product of $C_3wrC_2 = C_3^2 \rtimes C_2$; $C_3^2 = \left\langle x \mid x^3 = 1\right\rangle \times \left\langle y \mid y^3 = 1\right\rangle$ and $C_2 = \left\langle z \mid z^2 = 1\right\rangle$. The listing of elements of C_3wrC_2 are: $1, x, x^2, y, xy, x^2y, y^2, xy^2, x^2y^2, z, xz, x^2z, yz, xyz, x^2yz, y^2z, xy^2z, x^2y^2z$. The action of C_2 on C_3^2 given by $\phi : C_2 \longrightarrow Aut\left(C_3^2\right)$ such that $Aut(C_3^2)$ is defined as

$$Aut\left(C_3^2\right) = \{\phi\ : x \longrightarrow x^2, y \longrightarrow y^2\}$$

This gives the Wreath products with the presentation

$$\left\langle x, y, z \mid x^3 = y^3 = z^2 = 1, zxz^{-1} = x^2,\ zyz^{-1} = y^2\right\rangle$$

wr	1	x	x^2	y	xy	x^2y	y^2	xy^2	x^2y^2	z	xz	x^2z	yz	xyz	x^2yz	y^2z	xy^2z	x^2y^2z
1	1	x	x^2	y	xy	x^2y	y^2	xy^2	x^2y^2	z	xz	x^2z	yz	xyz	x^2yz	y^2z	xy^2z	x^2y^2z
x^2	x^2	1	x	x^2y	y	xy	x^2y^2	y^2	xy^2	x^2z	z	xz	x^2yz	yz	xyz	x^2y^2z	y^2z	xy^2zz
x	x	x^2	1	xy	x^2y	y	xy^2	x^2y^2	y^2	xz	x^2z	z	xyz	x^2yz	yz	xy^2z	x^2y^2z	y^2z
y^2	y^2	xy^2	x^2y^2	1	x	x^2	y	xy	x^2y	y^2z	xy^2z	x^2y^2z	z	xz	x^2z	yz	xyz	x^2yz
x^2y^2	x^2y^2	y^2	xy^2	x^2	1	x	x^2y	y	xy	x^2y^2z	y^2z	xy^2zz	x^2z	z	xz	x^2yz	yz	xyz
xy^2	xy^2	x^2y^2	y^2	x	x^2	1	xy	x^2y	y	xy^2z	x^2y^2z	y^2z	xz	x^2z	z	xyz	x^2yz	yz
y	y	xy	x^2y	y^2	xy^2	x^2y^2	1	x	x^2	yz	xyz	x^2yz	y^2z	xy^2z	x^2y^2z	z	xz	x^2z
x^2y	x^2y	y	xy	x^2y^2	y^2	xy^2	x^2	1	x	x^2yz	yz	xyz	x^2y^2z	y^2z	xy^2zz	x^2z	z	xz
xy	xy	x^2y	y	xy^2	x^2y^2	y^2	x	x^2	1	xyz	x^2yz	yz	xy^2z	x^2y^2z	y^2z	xz	x^2z	z
z	z	x^2z	xz	y^2z	x^2y^2z	xy^2z	yz	x^2yz	xyz	1	x^2	x	y^2	x^2y^2	xy^2	y	x^2y	xy
xz	xz	z	x^2z	xy^2z	y^2z	x^2y^2z	xyz	yz	x^2yz	x	1	x^2	xy^2	y^2	x^2y^2	xy	y	x^2y
x^2z	x^2z	xz	z	x^2y^2z	xy^2z	y^2z	x^2yz	xyz	yz	x^2	x	1	x^2y^2	xy^2	y^2	x^2y	xy	y
yz	yz	x^2yz	xyz	z	x^2z	xz	y^2z	x^2y^2z	xy^2z	y	x^2y	xy	1	x^2	x	y^2	x^2y^2	xy^2
xyz	xyz	yz	x^2yz	xz	z	x^2z	xy^2z	y^2z	x^2y^2z	xy	y	x^2y	x	1	x^2	xy^2	y^2	x^2y^2
x^2yz	x^2yz	xyz	yz	x^2z	xz	z	x^2y^2z	xy^2z	y^2z	x^2y	xy	y	x^2	x	1	x^2y^2	xy^2	y^2
y^2z	y^2z	x^2y^2z	xy^2z	yz	x^2yz	xyz	z	x^2z	xz	y^2	x^2y^2	xy^2	y	x^2y	xy	1	x^2	x
xy^2z	xy^2z	y^2z	x^2y^2z	xyz	yz	x^2yz	xz	z	x^2z	xy^2	y^2	x^2y^2	xy	y	x^2y	x	1	x^2
x^2y^2z	x^2y^2z	xy^2z	y^2z	x^2yz	xyz	yz	x^2z	xz	z	x^2y^2	xy^2	y^2	x^2y	xy	y	x^2	x	1

It follows that the coding matrix

$$M\left(C_3wrC_2\right) = \begin{pmatrix} T_0 & H_2 \\ H_3 & T_1 \end{pmatrix}_{18\times 18}$$

Is a block matrix consisting of $4 = 2\times 2$ matrices of size $\left(3^2 \times 3^2\right)-$matrices from which $2 = (2-1)^2 + 1$ are circulant (Toeplitz) matrices and $2 = 2(2-1)$ Hankel-type matrices.

Group codes

Definition 3.3[2]: A unit $w \in RG$ is *orthogonal* if and only if its inverse is w^T(i.e. $ww^T = 1$).

Self-dual codes: Some self-dual codes in RG can be formed as follows: suppose that $|G| = n = 2m$ and $G = \{g_1, g_2, \ldots, g_n\}$. Let $w \in RG$ satisfy:

1. $w^2 = 0$,
2. $w = w^T$ so that $ww^T = 0$,
3. u and its corresponding matrix U have rank m.

Then w generates a self-dual code.

From Example 3.2, $W = C_3wrC_2 = \left\{1, x, x^2, y, xy, x^2y, y^2, xy^2, x^2y^2, z, xz, x^2z, yz, xyz, x^2yz, y^2z, xy^2z, x^2y^2z\right\}$. We then form the group ring $\mathbb{Z}_2W$. Consider $w = y + yz\left(1 + xy + x^2y^2\right) \in \mathbb{Z}_2W$. Then $w^2 = 0$. Thus *rank* $u \leq 9$. The RW-matrix of u is

$$U = \begin{pmatrix} I & B \\ B & I \end{pmatrix}$$

From which it follows that the *rank* $u = 9$. We found the distance to be ...

Example of unit derived codes. If $w^2 = 0$, then $(1 + w)^2 = 1$ over $\mathbb{Z}_2$. Thus $a = 1 + w$ satisfies $a^2 = aa^T = 1$, and this gives a series of orthogonal units.

An element $w \in \mathbb{Z}_2W$ can be written as

$$w = \alpha_0+\alpha_1x+\alpha_2x^2+\alpha_3y+\alpha_4xy+\alpha_5x^2y+\alpha_6y^2+\alpha_7xy^2+\alpha_8x^2y^2+\beta_0z+\beta_1xz+\beta_2x^2z+\beta_3yz+\beta_4xyz+\beta_5x^2yz+\beta_6y^2z+\beta_7xy^2z+\beta_8x^2y^2z$$

The associated RW-matrix $\boldsymbol{W}$ is then

$$U = \left(\begin{array}{cccccccccccccccccc}
\alpha_0 & \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 & \alpha_5 & \alpha_6 & \alpha_7 & \alpha_8 & \beta_0 & \beta_1 & \beta_2 & \beta_3 & \beta_4 & \beta_5 & \beta_6 & \beta_7 & \beta_8 \\
\alpha_2 & \alpha_0 & \alpha_1 & \alpha_5 & \alpha_3 & \alpha_4 & \alpha_8 & \alpha_6 & \alpha_7 & \beta_2 & \beta_0 & \beta_1 & \beta_5 & \beta_3 & \beta_4 & \beta_8 & \beta_6 & \beta_7 \\
\alpha_1 & \alpha_2 & \alpha_0 & \alpha_4 & \alpha_5 & \alpha_3 & \alpha_7 & \alpha_8 & \alpha_6 & \beta_1 & \beta_2 & \beta_0 & \beta_4 & \beta_5 & \beta_3 & \beta_7 & \beta_8 & \beta_6 \\
\alpha_6 & \alpha_7 & \alpha_8 & \alpha_0 & \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 & \alpha_5 & \beta_6 & \beta_7 & \beta_8 & \beta_0 & \beta_1 & \beta_2 & \beta_3 & \beta_4 & \beta_5 \\
\alpha_8 & \alpha_6 & \alpha_7 & \alpha_2 & \alpha_0 & \alpha_1 & \alpha_5 & \alpha_3 & \alpha_4 & \beta_8 & \beta_6 & \beta_7 & \beta_2 & \beta_0 & \beta_1 & \beta_5 & \beta_3 & \beta_4 \\
\alpha_7 & \alpha_8 & \alpha_6 & \alpha_1 & \alpha_2 & \alpha_0 & \alpha_4 & \alpha_5 & \alpha_3 & \beta_7 & \beta_8 & \beta_6 & \beta_1 & \beta_2 & \beta_0 & \beta_4 & \beta_5 & \beta_3 \\
\alpha_3 & \alpha_4 & \alpha_5 & \alpha_6 & \alpha_7 & \alpha_8 & \alpha_0 & \alpha_1 & \alpha_2 & \beta_3 & \beta_4 & \beta_5 & \beta_6 & \beta_7 & \beta_8 & \beta_0 & \beta_1 & \beta_2 \\
\alpha_5 & \alpha_3 & \alpha_4 & \alpha_8 & \alpha_6 & \alpha_7 & \alpha_2 & \alpha_0 & \alpha_1 & \beta_5 & \beta_3 & \beta_4 & \beta_8 & \beta_6 & \beta_7 & \beta_2 & \beta_0 & \beta_1 \\
\alpha_4 & \alpha_5 & \alpha_3 & \alpha_7 & \alpha_8 & \alpha_6 & \alpha_1 & \alpha_2 & \alpha_0 & \beta_4 & \beta_5 & \beta_3 & \beta_7 & \beta_8 & \beta_6 & \beta_1 & \beta_2 & \beta_0 \\
\beta_0 & \beta_2 & \beta_1 & \beta_6 & \beta_8 & \beta_7 & \beta_3 & \beta_5 & \beta_4 & \alpha_0 & \alpha_2 & \alpha_1 & \alpha_6 & \alpha_8 & \alpha_7 & \alpha_3 & \alpha_5 & \alpha_4 \\
\beta_1 & \beta_0 & \beta_2 & \beta_7 & \beta_6 & \beta_8 & \beta_4 & \beta_3 & \beta_5 & \alpha_1 & \alpha_0 & \alpha_2 & \alpha_7 & \alpha_6 & \alpha_8 & \alpha_4 & \alpha_3 & \alpha_5 \\
\beta_2 & \beta_1 & \beta_0 & \beta_8 & \beta_7 & \beta_6 & \beta_5 & \beta_4 & \beta_3 & \alpha_2 & \alpha_1 & \alpha_0 & \alpha_8 & \alpha_7 & \alpha_6 & \alpha_5 & \alpha_4 & \alpha_3 \\
\beta_3 & \beta_5 & \beta_4 & \beta_0 & \beta_2 & \beta_1 & \beta_6 & \beta_8 & \beta_7 & \alpha_3 & \alpha_5 & \alpha_4 & \alpha_0 & \alpha_2 & \alpha_1 & \alpha_6 & \alpha_8 & \alpha_7 \\
\beta_4 & \beta_3 & \beta_5 & \beta_1 & \beta_0 & \beta_2 & \beta_7 & \beta_6 & \beta_8 & \alpha_4 & \alpha_3 & \alpha_5 & \alpha_1 & \alpha_0 & \alpha_2 & \alpha_7 & \alpha_6 & \alpha_8 \\
\beta_5 & \beta_4 & \beta_3 & \beta_2 & \beta_1 & \beta_0 & \beta_8 & \beta_7 & \beta_6 & \alpha_5 & \alpha_4 & \alpha_3 & \alpha_2 & \alpha_1 & \alpha_0 & \alpha_8 & \alpha_7 & \alpha_6 \\
\beta_6 & \beta_8 & \beta_7 & \beta_3 & \beta_5 & \beta_4 & \beta_0 & \beta_2 & \beta_1 & \alpha_6 & \alpha_8 & \alpha_7 & \alpha_3 & \alpha_5 & \alpha_4 & \alpha_0 & \alpha_2 & \alpha_1 \\
\beta_7 & \beta_6 & \beta_8 & \beta_4 & \beta_3 & \beta_5 & \beta_1 & \beta_0 & \beta_2 & \alpha_7 & \alpha_6 & \alpha_8 & \alpha_4 & \alpha_3 & \alpha_5 & \alpha_1 & \alpha_0 & \alpha_2 \\
\beta_8 & \beta_7 & \beta_6 & \beta_5 & \beta_4 & \beta_3 & \beta_2 & \beta_1 & \beta_0 & \alpha_8 & \alpha_7 & \alpha_6 & \alpha_5 & \alpha_4 & \alpha_3 & \alpha_2 & \alpha_1 & \alpha_0
\end{array} \right)$$

This can be written as $U = \begin{pmatrix} A & B \\ B^T & A^T \end{pmatrix}$, where A is a circulant matrix,

Example 3.4: The wreath product of $C_mwrC_n = C_m^n \rtimes C_n$;

$C_m^n = \left\langle x_1 \mid x_1^m = 1 \right\rangle \times \left\langle x_2 \mid x_2^m = 1 \right\rangle \times \cdots \times \langle x_n \mid x_n^m = 1 \rangle$ and $C_n = \langle z \mid z^n = 1 \rangle$. The listing of elements of C_mwrC_n are: $1, x_1, \ldots, x_1^{m-1}, x_2, x_1x_2, \ldots, x_1^{m-1}x_2, x_2^2, x_1x_2^2, \ldots, x_1^{m-1}x_2^2, \ldots, x_2^{m-1}, x_1x_2^{m-1}, \ldots, x_1^{m-1}x_2^{m-1}, \ldots$

$$, x_n, x_1x_n, \ldots, x_1^{m-1}x_n, x_2x_n, \ldots, x_2^{m-1}x_n, x_1x_2^{m-1}x_n, \ldots, x_1^{m-1}x_2^{m-1}x_n, x_n^2, \ldots, x_1^{m-1}x_2^{m-1}x_n^{n-1}, \ldots,$$

$$x_1x_2\ldots x_n, \ldots, x_1^{m-1}x_2^{m-1}\ldots x_n^{n-1}, z, x_1z, \ldots, x_1^{m-1}z, x_2z, x_1x_2z, \ldots, x_1^{m-1}x_2z, x_2^2z, x_1x_2^2z, \ldots,$$

$$x_1^{m-1}x_2^2z, \ldots, x_2^{m-1}z, x_1x_2^{m-1}z, \ldots, x_1^{m-1}x_2^{m-1}z, \ldots, x_nz, x_1x_nz, \ldots, x_1^{m-1}x_nz, x_2x_nz, \ldots,$$

$$x_2^{m-1}x_nz, x_1x_2^{m-1}x_nz, \ldots, x_1^{m-1}x_2^{m-1}x_nz, x_n^2z, \ldots, x_1^{m-1}x_2^{m-1}x_n^{n-1}z, \ldots, x_1x_2\ldots x_nz, \ldots, x_1^{m-1}x_2^{m-1}\ldots x_n^{n-1}z,$$

$$\ldots, z^{n-1}, x_1z^{n-1}, \ldots, x_1^{m-1}z^{n-1}, x_2z^{n-1}, x_1x_2z^{n-1}, \ldots, x_1^{m-1}x_2z^{n-1}, x_2^2z^{n-1}, x_1x_2^2z^{n-1}, \ldots, x_1^{m-1}x_2^2z^{n-1},$$

$$\ldots, x_2^{m-1}z^{n-1}, x_1x_2^{m-1}z^{n-1}, \ldots, x_1^{m-1}x_2^{m-1}z^{n-1}, \ldots, x_nz^{n-1}, x_1x_nz^{n-1}, \ldots, x_1^{m-1}x_nz^{n-1}, x_2x_nz^{n-1}, \ldots$$

$$, x_2^{m-1}x_nz^{n-1}, x_1x_2^{m-1}x_nz^{n-1}, \ldots, x_1^{m-1}x_2^{m-1}x_nz^{n-1}, x_n^2z^{n-1}, \ldots, x_1^{m-1}x_2^{m-1}x_n^{n-1}z^{n-1}, \ldots,$$

$x_1x_2\ldots x_nz^{n-1}, \ldots, x_1^{m-1}x_2^{m-1}\ldots x_n^{n-1}z^{n-1}$. The action of C_n on C_m^n given by $\phi : C_n \longrightarrow Aut\,(C_m^n)$ such that $Aut(C_m^n)$ is defined as

$$Aut\,(C_m^n) = \left\{\phi\ : x_1 \longrightarrow x_1^{m-1}, x_2 \longrightarrow x_2^{m-1}, \ldots, x_n \longrightarrow x_n^{m-1}\right\}$$

Which gives the Wreath products with the presentation

$$\left\langle x_1, x_2, \ldots, x_n, z \mid x_1^m = x_2^m = \cdots = x_n^m = z^m = 1, zx_1z^{-1} = x_1^{m-1},\ zx_2z^{-1} = x_2^{m-1}, \ldots, zx_nz^{-1} = x_n^{m-1}\right\rangle$$

Proposition 3.5: The wreath product
$C_mwrC_n = C_m^n \rtimes C_n = \left\langle x_1, x_2, \ldots, x_n, z \mid x_1^m = x_2^m = \cdots = x_n^m = z^m = 1, zx_1z^{-1} = x_1^{m-1},\ zx_2z^{-1} = x_2^{m-1}, \ldots, zx_nz^{-1} = x_n^{m-1}\right\rangle$

has the coding matrix of the form

$$\begin{pmatrix} T_0 & H_1 & \cdots & H_{n-1} \\ H_n & T_1 & \cdots & T_{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ H_{2(n-1)} & T_{(n-2)(n-1)} & \cdots & T_{(n-1)^2} \end{pmatrix}_{m^n n \times m^n n}$$

Consisting of n^2 matrices all of size $(m^n \times m^n)$ from which the $(n-1)^2 + 1$ matrices $T_0, T_1, \ldots, T_{(n-1)^2}$ are Circulant (Toepltz) and the $2(n-1)$ marices $H_1, H_2, \ldots, H_{2(n-1)}$ are Hankel-type matrices.

So the coding matrix of wreath product really has the same shape as the one for semidirect product.

4. Structures of $C_m wr C_n$ for the pair (m, n)

1. If $m = n$, then $C_m wr C_m = C_m^{m+1}$ with $|C_m wr C_m| = m^{m+1}$.
2. If $gcd\,(m, n) = 1$ and $gcd\,(m, n) \neq 1$, then $|C_m wr C_n| = m^n n$.
3. If $gcd\,(p, n) = 1$ where p is a prime number, then $\left|C_p wr C_n\right| = p^n n$.
4. If $gcd\,(m, p) = 1$ where p is a prime number, then $\left|C_m wr C_p\right| = m^p p$

5. Conclusion

In conclusion, we were able to give the coding matrix of wreath product of two cyclic finite groups which is a generalization of the semi-direct product proved in [6] with examples. We found out that the coding matrix of wreath products of group has the same shape with that of semi-direct product.

Acknowledgements

The authors gratefully acknowledge the financial support of Hector Luis Avila Pisetta.

References

[1] T. Hurley, “Group Rings and Rings of Matrices”, International Journal of Pure and Applied Mathematics **31** (2006) 319.

[2] P. Hurley & T. Hurley, “Codes from Zero-divisors and Units in Group Rings” *arXiv:0710.5893v1 [cs.IT]* (2007) 1.

[3] T. Hurley, “Convolutional codes from units in matrix and group rings”, *arXiv:0711.3629v1 [cs.IT]* (2007) 1.

[4] P. Hurley & T. Hurley, “Block codes from matrix and group rings”, In P. Hurley, & T. Hurley, *Chapter 5, in Selected topics in information and coding theory,* (2010) 159.

[5] M. M. Hamed & A. A. Khammash, “Coding Matrices for GL(2,q)”, Fundamental Journal of Mathematics and Applications **1** (2018) 118.

[6] A. A. Alkinani & A. A. Khammash, “Coding Matrices for the Semi-Direct Product Groups”, Fundamental Journal of Mathematics and Applications **3** (2020) 109. https://doi.org/10.33401/fujma.690424

[7] T. Rhian, *Group rings: Units and their applications in self-dual codes*, PhD Thesis, University of Chester (2022).

[8] J. D. Dixon, & B. Mortimer, *Permutation Groups*, Springer, Berlin, New York (1996).

[9] B. Sury, “Wreath Products, Sylow’s Theorem and Fermat’s Little Theorem”, European Journal of Pure and Applied Mathematics **3** (2010) 13.

[10] E. Suleiman & M. S. Audu, “Some Embedment of Groups into Wreath Products”, International Journal of Algebra and Statistics **9** (2020) 1. https://doi.org/10.20454/ijas.2020.1630

[11] Z. S.Tan, Cyclic And Dihedral Group Ring Codes, MSc Thesis, Universiti Sains Malaysia (USM) (2016).