Fundamental Journal of Mathematics and Applications, 3 (2) (2020) 109-115
Research Article

Fundamental Journal of Mathematics and Applications

Journal Homepage: www.dergipark.gov.tr/fujma
ISSN: 2645-8845
doi: 10.33401/fujma.690424

Coding Matrices for the Semi-Direct Product Groups

Amnah A. Alkinani[1*] and Ahmed A. Khammash[1]

[1]*Departement of Mathematical Sciences, Umm Al-Qura University, Makkah, Saudi Arabia*
[*]*Corresponding author*

Article Info

Keywords: *Code, Group ring, Ring of matrices, Semi-direct product group*
2010 AMS: *15A30, 16S34, 20C05, 20C07, 94A30*
Received: *18 February 2020*
Accepted: *08 July 2020*
Available online: *15 December 2020*

Abstract

We shall determine the coding matrix of the semi-direct product group $G = C_n \rtimes_\phi C_m$; $\phi : C_m \longrightarrow Aut(C_n)$ of two cyclic groups in order to generalize the known result for the dihedral group D_{2n}, which is known to be a semi-direct of the two cyclic groups C_n , C_2.

1. Introduction

An (n,k)-linear code C of length n over the finite field of q elements $\mathbb{F}_q$ is a k-dimensional subspace of $\mathbb{F}_q^n$. It gained more attention from the work of W. Hamming in 1950 [1]. The first connection between codes and group rings of finite groups appeared in the work of F. G. MacWilliams (1969) [2]. In (2006) T. Hurley [3] (starting with a coding matrix of the finite group G based on an appropriate listing of its elements) proved that the group ring RG of a finite group of order n over a ring R is isomorphic to certain well-defined ring of matrices, and hence gave a construction of codes from certain elements of the group ring such as units and zero divisors [4]. The coding matrices were determined for several classes of finite groups such as cyclic [3], elementary-abelian [3], dihedral groups D_{2n} [3], direct product [5] and the general linear group $GL(2,\mathbb{F})$ [6].
In this paper, we shall generalize Hurley's theorem in [3] to $C_n \rtimes_\phi C_2$ as a special case of $C_n \rtimes_\phi C_m$ and we will decide the form of the coding matrices of $C_n \rtimes_\phi C_m$.

The paper is organized as follows in section 2, we present some definitions and basic results with examples about group rings, coding matrices of group rings and codes. In section 3, we determine the coding matrix of the semi-direct product group of two cyclic groups with illustrative examples.

2. Preliminaries

Let G be a finite group of order n, and $\{g_1, g_2, ..., g_n\}$ be a fixed listing of the element of G. Consider the matrix of G relative to its listing, $M(G)$, which has the following form:

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

Email addresses and ORCID numbers: **aaalkenane@uqu.edu.sa, https://orcid.org/0000-0001-8208-7995 (A. A. Alkinani), aakhammash@uqu.edu.sa, https://orcid.org/0000-0001-9404-1732 (A. A. Khammash)**

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

$$M(RG,u) = \begin{pmatrix} \alpha_{g_1^{-1}g_1} & \alpha_{g_1^{-1}g_2} & \dots & \alpha_{g_1^{-1}g_n} \\ \alpha_{g_2^{-1}g_1} & \alpha_{g_2^{-1}g_2} & \dots & \alpha_{g_2^{-1}g_n} \\ \vdots & \vdots & \vdots & \vdots \\ \alpha_{g_n^{-1}g_1} & \alpha_{g_n^{-1}g_2} & \dots & \alpha_{g_n^{-1}g_n} \end{pmatrix}_{n\times n}.$$

It is quite clear that the shape as well as the coefficients of the coding matrix $M(RG,u)$ depends on the listing of the group elements of the group G.
In [3], T. Hurley proved 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.

Theorem 2.1. *([3], Theorem 1)*
Let G be a group of order n with the given listing of the elements, then there is a bijective ring homomorphism is given by

$$\sigma : u \longrightarrow M(RG,u)$$

between RG and the ring of $(n \times n)$ G-matrices over R.

The coding matrices are known for several types of groups, for details see [3].

Definition 2.2.
- *Let R be a ring, a non zero element $u = \sum_{g\in G} \alpha_g g \in RG$ is called a zero-divisor if and only if there exists a non zero element $v \in RG$ such that $uv = 0$ or $vu = 0$.*
- *Let R be a ring with identity $I_R \neq 0$, an element $u \in RG$ is called a unit if and only if there exists an element $v \in RG$, such that $uv = 1 = vu$.*

Definition 2.3.
- *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 $C^{\perp} = \{u \in \mathbb{F}_q^n \mid u.v = 0 \text{ for all } v \in C\}$.*

Definition 2.4. *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 $\{g_1, g_2, \dots, g_n\}$. Suppose W is a submodule of RG, $x \in W$ and $u \in RG$ is given. Then the group ring encoding is a mapping $f : W \longrightarrow RG$ such that $f(x) = xu$ or $f(x) = ux$. 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 $u \in RG$, either $C = \{ux : x \in W\}$ or $C = \{xu : x \in W\}$.
The map $\theta : RG \to R^n$, $\theta(\sum_{i=1}^{n} \alpha_{g_i} g_i) = (\alpha_1, \alpha_2, ..., \alpha_n)$ 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 2.5. *If $xu = ux$ for all x, then the code $C = \{xu : x \in W\}$ is said to be commutative, and otherwise non-commutative codes.*

When u 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 where done by P. Hurley and T. Hurley in [4] , [7].

Example 2.6. *Let $R = \mathbb{Z}_2 = \{0,1\}$ be the finite field of two elements and $G = S_3 = \prec a,b \mid a^3 = b^2 = 1, ba = a^2b \succ = \{1,a,a^2,b,ab,a^2b\}$ be the symmetric group of order 6. Then the coding matrices of S_3 is:*

$\times$	1	a	a^2	a^2b	ab	b
1	1	a	a^2	a^2b	ab	b
a^2	a^2	1	a	ab	b	a^2b
a	a	a^2	1	b	a^2b	ab
a^2b	a^2b	ab	b	1	a	a^2
ab	ab	b	a^2b	a^2	1	a
b	b	a^2b	ab	a	a^2	1

Thus,

$$M(S_3) = \begin{pmatrix} 1 & a & a^2 & a^2b & ab & b \\ a^2 & 1 & a & ab & b & a^2b \\ a & a^2 & 1 & b & a^2b & ab \\ a^2b & ab & b & 1 & a & a^2 \\ ab & b & a^2b & a^2 & 1 & a \\ b & a^2b & ab & a & a^2 & 1 \end{pmatrix}_{6\times 6}$$

And the group ring $RG=\mathbb{Z}_2S_3=\sum_{g\in S_3}\alpha_g g \mid \alpha_g\in\mathbb{Z}_2=\{c_0+c_1a+c_2a^2+c_3a^2b+c_4ab+c_5b\,;\,c_i\in\mathbb{Z}_2\}$, *Such that* $(\mathbb{Z}_2S_3,+,.)$ *is* $\mathbb{F}$*-algebra. From T. Hurley's theorem :* $\mathbb{Z}_2S_3\hookrightarrow M_{|S_3|\times|S_3|}(\mathbb{Z}_2)$. *So, if* $u\in\mathbb{Z}_2S_3$; $u=c_0+c_1a+c_2a^2+c_3a^2b+c_4ab+c_5b$, *then :*

$$M(\mathbb{Z}_2S_3,u)=\begin{pmatrix} c_0 & c_1 & c_2 & c_3 & c_4 & c_5\\ c_2 & c_0 & c_1 & c_4 & c_5 & c_3\\ c_1 & c_2 & c_0 & c_5 & c_3 & c_4\\ c_3 & c_4 & c_5 & c_0 & c_1 & c_2\\ c_4 & c_5 & c_3 & c_2 & c_0 & c_1\\ c_5 & c_3 & c_4 & c_1 & c_2 & c_0 \end{pmatrix}_{6\times 6}$$

For the unit element $u=1+a+a^2+ab+a^2b\in U(\mathbb{Z}_2S_3)$ *there exists* $u^{-1}=1+a+a^2+ab+a^2b$ *such that* $uu^{-1}=1$. *Then we have* $M(\mathbb{Z}_2S_3,u)$ *as follows :*

$$M(\mathbb{Z}_2S_3,u)=\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 0\\ 1 & 1 & 1 & 1 & 0 & 1\\ 1 & 1 & 1 & 0 & 1 & 1\\ 1 & 1 & 0 & 1 & 1 & 1\\ 1 & 0 & 1 & 1 & 1 & 1\\ 0 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}_{6\times 6}$$

Also , from Hurley's theorems : If R has an identity 1_R, *then* $u\in RG$ *is a unit if and only if* $\sigma(u)$ *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* $UV=1_6$ *in* $R_{6\times 6}$.
Taking any r rows of U as a generator matrix define an (n,r)*-code. Then we have*

$$A=\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 0\\ 1 & 1 & 1 & 1 & 0 & 1\\ 1 & 1 & 1 & 0 & 1 & 1 \end{pmatrix}_{3\times 6},\ B=\begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 1\\ 1 & 0 & 1 & 1 & 1 & 1\\ 0 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}_{3\times 6},$$

$$C=\begin{pmatrix} 1 & 1 & 1\\ 1 & 1 & 1\\ 1 & 1 & 1\\ 1 & 1 & 0\\ 1 & 0 & 1\\ 0 & 1 & 1 \end{pmatrix}_{6\times 3}\quad \textit{and } D=\begin{pmatrix} 1 & 1 & 0\\ 1 & 0 & 1\\ 0 & 1 & 1\\ 1 & 1 & 1\\ 1 & 1 & 1\\ 1 & 1 & 1 \end{pmatrix}_{6\times 3}.$$

Such that

$$AC=BD=\begin{pmatrix} 1 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & 1 \end{pmatrix}_{3\times 3}\quad \textit{and } AD=BC=\begin{pmatrix} 0 & 0 & 0\\ 0 & 0 & 0\\ 0 & 0 & 0 \end{pmatrix}_{3\times 3}.$$

Then,

$$UV=\begin{pmatrix}A\\B\end{pmatrix}.\begin{pmatrix}C & D\end{pmatrix}=\begin{pmatrix}AC & AD\\ BC & BD\end{pmatrix}=\begin{pmatrix}I_3 & O_3\\ O_3 & I_3\end{pmatrix}=I_{6\times 6}.$$

The linear code C of dimension $k=3$, *generated by the matrix*

$$A=\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 0\\ 1 & 1 & 1 & 1 & 0 & 1\\ 1 & 1 & 1 & 0 & 1 & 1 \end{pmatrix}_{3\times 6},$$

is the unit derived code $C=\{ux \mid x\in W\}$, *where* $S=\{a\}\subset G$ *and* $W=\prec a\succ=\{1,a,a^2\}$. *The dual code* $C^{\perp}$ *is the linear code generated by the matrix*

$$D^T=\begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 1\\ 1 & 0 & 1 & 1 & 1 & 1\\ 0 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}_{3\times 6},$$

with dimension $n-k=3$. *The dual code can be considered as the submodule* $C^{\perp}=\{(u^{-1})^T y \mid y\in W^{\perp}\}$, *where* $W^{\perp}=\prec G-S\succ=\{a^2b,ab,b\}$. *So,* $C=\{ux \mid x\in W\}=\{1+a+a^2+a^2b+ab,1+a+a^2+b+a^2b,1+a^2+a+ab+b\}$, $\theta(C)=$

$\{111110, 111101, 111011\}$, *and* $C^{\perp} = \{(u^{-1})^T y \mid y \in W^{\perp}\} = \{1+a^2b+ab+b+a, 1+ab+b+a^2b+a^2, b+a^2b+ab+b+a\}$, $\theta(C^{\perp}) = \{110111, 101111, 011111\}$. *Clearly, the matrix A is the generator matrix for an* $(6,3)$*-code, and* D^T *is the parity-check matrix for this code, since it is a generator matrix of* $C^{\perp}$ *as defined in (definition 2.3).*

3. Coding matrices of semi-direct product groups

Definition 3.1. *Let H and K be groups and let* ϕ *be a homomorphism,*

$$\phi : K \longrightarrow Aut(H)$$

Then the semi-direct product of H and K with respect the action ϕ *is the group G containing of ordered pairs* (h,k) *with* $h \in H$ *and* $k \in K$ *defined by:*

$$(h_1,k_1)(h_2,k_2) = (h_1\phi_{k_1}h_2, k_1k_2)$$

Where $\phi_k(h) = kh = khk^{-1}, \forall h \in H, k \in K$.

Denote of semi-direct product by $H \rtimes_{\phi} K$ (or simply, write $H \rtimes K$).

Example 3.2. *Let* $G = S_3$*, let N be the normal subgroup of order* 3 *generated by a* 3*-cycle, and let H be a subgroup of order* 2 *generated by a* 2*-cycle. Then* $G = N \rtimes H$*. This example generalizes a long two different lines:*

1 • *Let* $G = S_n$ *,* $N = A_n$ *and H a subgroup of order* 2 *generated by a* 2*-cycle. Then* $G = N \rtimes H$*.*
2 • *Let* $G = D_{2n}$*, the dihedral group of order* $2n$*. Then let* $N = C_n$ *and* $H = C_2$*. Then* $D_{2n} \cong C_n \rtimes C_2$*.*

We will decide the coding matrices of the semi-direct product groups $C_n \rtimes C_m$ as following:
Consider $G = C_n \rtimes C_m$; $C_n \lhd G$ of two groups $C_n =< x >= \{x \mid x^n = 1\}$ and $C_m =< y >= \{y \mid y^m = 1\}$. We may list the elements of the semi-direct product $C_n \rtimes C_m$ as follows: $x^i y^j$; $0 \leqslant i \leqslant n-1$, $0 \leqslant j \leqslant m-1$:

$$1, x, x^2, \ldots, x^{n-1} \ , \ y, xy, x^2y, \ldots, x^{n-1}y \ , \ y^2, xy^2, x^2y^2, \ldots, x^{n-1}y^2 \ , \ \ldots\ldots\ldots \ , y^{m-1}, xy^{m-1}, x^2y^{m-1}, \ldots \ , \ x^{n-1}y^{m-1} \ . \qquad (3.1)$$

(m blocks each with n elements).
This product defined by the action of C_m on C_n (or group homomorphism) given by $\phi : C_m \longrightarrow Aut(C_n)$; $C_n \rtimes C_m = \{x^i y^j : x^i \in C_n \ , \ y^j \in C_m \mid x^i y^j . x^s y^t = x^i \phi_{y^j} x^s . y^j y^t\}$. The inverse of the element $x^i y^j$ in $C_n \rtimes C_m$ is $\phi_{(m-j)} x^{n-i} . y^{m-j}$.
In fact, the automorphism group $Aut(C_n)$ is one to one correspondence with the set $\{x^r \mid hcf(n,r) = 1\}$ of generators of C_n, so $|Aut(C_n)| = \varphi(n)$, where φ is the Euler function.

Definition 3.3. *The Euler* φ*-function is defined as: for* $n \in Z^+$*, let* $\varphi(n)$ *be the number of positive integers* $a \leqslant n$ *with* $(a,n) = 1$.

Here, the non-identity element of C_2 acts on C_n by inverting elements; this is an automorphisms since C_n is an abelian, and the presentation for this group is: $< xy | x^n = y^m = 1, yxy^{-1} = x^{-1} >$.
More generally, a semi-direct product of any two cyclic groups C_n with generator x and C_m with generator y is given by one extra relation, $yxy^{-1} = x^k$, with $(k,n) = 1$, where $Aut(C_n) : x \longrightarrow x^k$ for some k; that is, the presentation: $< xy | x^n = y^m = 1, yxy^{-1} = x^k >$.
If y^r is a generator of C_m and $(r,m) = 1$, hence we have the presentation: $< xy | x^n = y^m = 1, y^r x y^{r^{-1}} = x^{k^r} >$.

Now, taking the trivial homomorphism $\phi : C_m \longrightarrow Aut(C_n); C_m \mapsto I_{C_n}$ gives the direct product $G = C_n \rtimes C_m = C_n \times C_m$.
And consider $G = C_n \rtimes C_m$, we need to know when there is a non-trivial homomorphism $\phi : C_m \longrightarrow Aut(C_n)$ but since $Aut(C_n) \cong C_{\varphi(n)}$ and since $Hom(C_m, C_{\varphi(n)}) \cong C_{hcf(m,\varphi(n))}$ we have the following:

Lemma 3.4. *There is a non-trivial homomorphism* $\phi : C_m \longrightarrow Aut(C_n)$ *iff* $hcf(m, \varphi(n)) \neq 1$.

Proof. We have $Hom(C_m, C_{\varphi(n)}) \cong C_{hcf(m,\varphi(n))}$. If $hcf(\ m, \varphi(n)\ ) = 1$ then $Hom(C_m, C_{\varphi(n)}) \cong C_1$ the trivial subgroup and so the only element $\phi \in Hom(C_m, C_{\varphi(n)})$ is the trivial one given by $\phi(y) = I_{C_n}$. Conversely, suppose that $hcf(m, \varphi(n)) \neq 1$, to define $\phi \in Hom(C_m, C_{\varphi(n)})$ by $\phi(y) : x \longmapsto x^t$ (where $1 \leq t < \varphi(n)$ with $hcf(t, \varphi(n)) \neq 1$ in order for x^t to be a generator for $C_{\varphi(n)}$), we must have $order(\phi(y)) \mid m$ (as $y^m = 1$) and $order(\phi(y)) \mid \varphi(n)$ (as $\phi(y) \in C_{\varphi(n)}$). But this is possible since $hcf(m, \varphi(n)) \neq 1$. □

So for example there will be no non-trivial semi-direct product $C_n \rtimes C_m$ (i.e. different from the direct product $C_n \times C_m$) if $hcf(m, \varphi(n)) = 1$, for instance $C_4 \rtimes C_3$ the only homomorphism $\phi : C_3 \longrightarrow Aut(C_4)$ is the one which takes $y \in C_m =< y >$ to the identity $I_{C_4} \in Aut(C_4) =< \theta_3 >= \{I_{C_4}, \theta_3\}; \theta_3 : x \longmapsto x^3 = x^{-1}$, therefore the only semi-direct product $C_4 \rtimes C_3$ is the direct product $C_4 \times C_3$.

Definition 3.5.
- *A circulant matrix is special type of Toeplitz matrix, which is one that is constant a long any diagonal running from upper left to lower right.*
- *A (general) Hankel matrix is one which is constant on any diagonal from upper right to lower left.*

In the following examples, we will clarify the coding matrices of $C_n \rtimes C_m$.

Example 3.6. *The semi-direct product of* $C_3 \rtimes C_4$ *;* $C_3 =\prec x \mid x^3 = 1 \succ= \{1,x,x^2\}$ *and* $C_4 =\prec y \mid y^4 = 1 \succ= \{1,y,y^2,y^3\}$. *The listing of elements of* $C_3 \rtimes C_4$ *are :* $1,x,x^2,y,xy,x^2y,y^2,xy^2,x^2y^2,y^3,xy^3,x^2y^3$. *And it has non-trivial homomorphism since* $(4,\varphi(3)\,) = (4,2) = 2 \neq 1$, *the action of* C_4 *on* C_3 *given by* $\phi : C_4 \to Aut(C_3)$, *such that* $Aut(C_3)$ *is* $\phi : C_3 \longrightarrow C_3$ *;* $\mid Aut(C_3) \mid= \varphi(3) = 2$, *hence it has* $Aut(C_3) = \{\phi_1 : x \longrightarrow x \ , \ \phi_2 : x \longrightarrow x^2\}$. *At* ϕ_1 *give us the semi-direct product as a direct product, but at* ϕ_2 *give us the semi-direct product with the presentation* $< xy|x^3 = y^4 = 1, yxy^{-1} = x^2 >$ *;* $C_3 \rtimes C_4 = \{\ xy \ : \ x \in C_3 \ , \ y \in C_4 \ : \ x_1y_1.x_2y_2 = x_1\phi_{y_1}(x_2).y_1y_2 \ \}$ *and the inverse of the element xy is* $(\phi_{y^{-1}}(x^{-1}).y^{-1})$ *as following:*

at ϕ_2

$\rtimes$	1	x	x^2	x^2y	xy	y	x^2y^2	xy^2	y^2	x^2y^3	xy^3	y^3
1	1	x	x^2	x^2y	xy	y	x^2y^2	xy^2	y^2	x^2y^3	xy^3	y^3
x^2	x^2	1	x	xy	y	x^2y	xy^2	y^2	x^2y^2	xy^3	y^3	x^2y^3
x	x	x^2	1	y	x^2y	xy	y^2	x^2y^2	xy^2	y^3	x^2y^3	xy^3
x^2y^3	x^2y^3	xy^3	y^3	1	x	x^2	y	xy	x^2y	y^2	xy^2	x^2y^2
xy^3	xy^3	y^3	x^2y^3	x^2	1	x	x^2y	y	xy	x^2y^2	y^2	xy^2
y^3	y^3	x^2y^3	xy^3	x	x^2	1	xy	x^2y	y	xy^2	x^2y^2	y^2
xy^2	xy^2	x^2y^2	y^2	y^3	x^2y^3	xy^3	1	x^2	x	y	x^2y	xy
x^2y^2	x^2y^2	y^2	xy^2	xy^3	y^3	x^2y^3	x	1	x^2	xy	y	x^2y
y^2	y^2	xy^2	x^2y^2	x^2y^3	xy^3	y^3	x^2	x	1	x^2y	xy	y
x^2y	x^2y	xy	y	y^2	xy^2	x^2y^2	y^3	xy^3	x^2y^3	1	x	x^2
xy	xy	y	x^2y	x^2y^2	y^2	xy^2	x^2y^3	y^3	xy^3	x^2	1	x
y	y	x^2y	xy	xy^2	x^2y^2	y^2	xy^3	x^2y^3	y^3	x	x^2	1

It follows that the coding matrix

$$M(C_3 \rtimes C_4) = \begin{pmatrix} T_0 & H_1 & H_2 & H_3 \\ H_4 & T_1 & T_2 & T_3 \\ H_5 & T_4 & T_5 & T_6 \\ H_6 & T_7 & T_8 & T_9 \end{pmatrix}_{12\times 12} ,$$

is a block matrix consisting of $16 = 4 \times 4$ matrices all are of size (3×3)-matrices from which $10 = (4-1)^2 + 1$ are circulant (Toeplitz) matrices and $6 = 2(4-1)$ Hankel-type-matrices.

Example 3.7. *Consider the semi-direct product* $C_7 \rtimes C_3$, $C_7 =\prec x \mid x^7 = 1 \succ= \{1,x,x^2,x^3,x^4,x^5,x^6\}$ *and* $C_3 =\prec y \mid y^3 = 1 \succ= \{1,y,y^2\}$, *where* $\phi : C_3 \longrightarrow Aut(C_7) \cong C_6$. *In fact* $Aut(C_7) = \{\theta_i | i = 1,2,3,4,5,6\} =< \theta_3 >=< \theta_5 > \cong C_6$ *; i.e.* $order(\theta_3) = order(\theta_5) = 6$, *while* $order(\theta_2) = order(\theta_4) = 3$ *and* $order(\theta_6) = 2$. *Therefore we may take* $\phi_i : C_3 \longrightarrow Aut(C_7)$ *to be the group homomorphism (or the action of* C_3 *on* C_7*) defined as* $(\phi_i(y) = \theta_i; i = 1,2,4)$, *since* $order(\theta_i); i = 1,2,4 \mid order(y) = 3$. *Clearly* $\phi_1(y) = \theta_1 = I_{C_7}$ *will induce the direct product* $C_7 \times C_3$. *(In fact it is easy to prove from the relations that* $C_7 \rtimes_{\phi_4} C_3 \cong C_7 \rtimes_{\phi_2} C_3$*). So we take* $\phi_2(y) = \theta_2 : x \longmapsto x^2$ *and consider* $C_7 \rtimes_{\phi_2} C_3 =< xy \mid x^7 = y^3 = 1, yxy^{-1} = x^2 >$, *generally* $G = C_7 \rtimes_{\phi_i} C_3 =< xy \mid x^7 = y^3 = 1, yxy^{-1} = x^i; i = 1,2,4 >$. *Therefore* $C_7 \rtimes C_3$ *has the listing:* $1,x,x^2,x^3,x^4,x^5,x^6,y,xy,x^2y,x^3y,x^4y,x^5y,$ $x^6y,y^2,xy^2,x^2y^2,x^3y^2,x^4y^2,x^5y^2,x^6y^2$ *subject to the above relations. From it we may deduce the product of different elements as* $\{\ xy \ : \ x \in C_7 \ , \ y \in C_3 \ : \ x_1y_1.x_2y_2 = x_1\phi_{y_1}(x_2).y_1y_2 \ \}$ *and the inverse of the element yx is* $(\phi_{y^{-1}}(x^{-1}).y^{-1})$ *as following:*

at ϕ_2

$\rtimes$	1	x	$\cdots$	x^5	x^6	x^6y	x^5y	$\cdots$	xy	y	x^6y^2	x^5y^2	$\cdots$	xy^2	y^2
1	1	x	$\cdots$	x^5	x^6	x^6y	x^5y	$\cdots$	xy	y	x^6y^2	x^5y^2	$\cdots$	xy^2	y^2
x^6	x^6	1	$\cdots$	x^4	x^5	x^5y	x^4y	$\cdots$	y	x^6y	x^5y^2	x^4y^2	$\cdots$	y^2	x^6y^2
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$
x^2	x^2	x^3	$\cdots$	1	x	xy	y	$\cdots$	x^3y	x^2y	xy^2	y^2	$\cdots$	x^3y^2	x^2y^2
x	x	x^2	$\cdots$	x^6	1	y	x^6y	$\cdots$	x^2y	xy	y^2	x^6y^2	$\cdots$	x^2y^2	xy^2
x^4y^2	x^4y^2	xy^2	$\cdots$	x^3y^2	y^2	1	x^3	$\cdots$	x	x^4	y	x^3y	$\cdots$	xy	x^4y
xy^2	xy^2	x^5y^2	$\cdots$	y^2	x^4y^2	x^4	1	$\cdots$	x^5	x	x^4y	y	$\cdots$	x^5y	xy
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$
x^3y^2	x^3y^2	y^2	$\cdots$	x^2y^2	x^6y^2	x^6	x^2	$\cdots$	1	x^3	x^6y	x^2y	$\cdots$	y	x^3y
y^2	y^2	x^4y^2	$\cdots$	x^6y^2	x^3y^2	x^3	x^6	$\cdots$	x^4	1	x^3y	x^6y	$\cdots$	x^4y	y
x^2y	x^2y	x^4y	$\cdots$	x^5y	y	y^2	x^5y^2	$\cdots$	x^4y^2	x^2y^2	1	x^5	$\cdots$	x^4	x^2
x^4y	x^4y	x^6y	$\cdots$	y	x^2y	x^2y^2	y^2	$\cdots$	x^6y^2	x^4y^2	x^2	1	$\cdots$	x^6	x^4
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$
x^5y	x^5y	y	$\cdots$	xy	x^3y	x^3y^2	xy^2	$\cdots$	y^2	x^5y^2	x^3	x	$\cdots$	1	x^5
y	y	x^2y	$\cdots$	x^3y	x^5y	x^5y^2	x^3y^2	$\cdots$	x^2y^2	y^2	x^5	x^3	$\cdots$	x^2	1

It follows that the coding matrix

$$M(C_7 \rtimes C_3) = \begin{pmatrix} T_0 & H_1 & H_2 \\ H_3 & T_1 & T_2 \\ H_4 & T_3 & T_4 \end{pmatrix}_{21\times 21},$$

is a block matrix consisting of $9 = 3\times 3$ matrices all are of size (7×7)-matrices from which $5 = (3-1)^2+1$ are circulant (Toeplitz) matrices and $4 = 2(3-1)$ Hankel-type-matrices.

In general, we take $G = C_n \rtimes_\phi C_m$ with respect the action ϕ as previously and it has the elements listing (3.1). By inspecting each block sub-matrix provided by each sub-list in $(1)-(m)$ and there corresponding inverse elements, we conclude the following theorem:

Theorem 3.8. *With respect to the above elements listing (3.1) for the semi-direct product groups*

$$G = C_n \rtimes_\phi C_m = < xy | x^n = y^m = 1, yxy^{-1} = x^k >,$$

the coding matrix of this group is a block matrix

$$\begin{pmatrix} T_0 & H_1 & \dots & H_{m-1} \\ H_m & T_1 & \dots & T_{m-1} \\ \vdots & \vdots & \vdots & \vdots \\ H_{2(m-1)} & T_{(m-2)(m-1)} & \cdots & T_{(m-1)^2} \end{pmatrix}_{nm\times nm},$$

consisting of m^2 matrices all are of size $(n\times n)$ from which the $(m-1)^2+1$ matrices $T_0, T_1, \dots, T_{(m-1)^2}$ are circulant (Toeplitz) and the $2(m-1)$ matrices $H_1, H_2, \dots, H_{2(m-1)}$ are Hankel-type-matrices.

As a special case of this theorem, we deduce the coding matrices for the dihedral group $D_{2n} \cong C_n \rtimes C_2$ which was determined in [3].

Corollary 3.9. *The coding matrices for $C_n \rtimes C_2 \cong D_{2n}$ have the following form*

$$\begin{pmatrix} T_1 & H_1 \\ H_2 & T_2 \end{pmatrix}_{2n\times 2n},$$

where T_i, H_i ; $i = 1,2$ are circulant, Hankel-type $(n\times n)$-matrices, respectively.

Proof. Consider $C_n \rtimes C_2 \cong D_{2n}$ such that $C_n = \prec x \mid x^n = 1 \succ = \{1, x, x^2, \dots, x^{n-1}\}$, $C_2 = \prec y \mid y^2 = 1 \succ = \{1, y\}$, the listing of elements of $C_n \rtimes C_2$ are : $1, x, x^2, ..., x^{n-1}, y, xy, x^2y, ..., x^{n-1}y$. And there is a non-trivial homomorphism since $(2, \varphi(n)) \neq 1$, so the action of C_2 on C_n given by $\phi : C_2 \longrightarrow Aut(C_n)$; $Aut(C_n) : \phi : C_n \longrightarrow C_n, | Aut(C_n) | = \varphi(n)$, hence we have $Aut(C_n) = \{\phi_1 : x \longrightarrow x$, $\phi_{n-1} : x \longrightarrow x^{n-1}\}$.

$C_n \rtimes C_2 = \{\ xy\ :\ x \in C_n\ ,\ y \in C_2\ :\ x_1y_1.x_2y_2 = x_1\phi_{y_1}(x_2).y_1y_2\ \}$, and the inverse of the element yx is $(\phi_{y^{-1}}(x^{-1}).y^{-1})$. At ϕ_1 give us the semi-direct product as a direct product, but at ϕ_{n-1} give us the semi-direct product groups as following:

at ϕ_{n-1}

$\rtimes$	1	x	x^2	..	x^{n-1}	$x^{n-1}y$	..	x^2y	xy	y
1	1	x	x^2	..	x^{n-1}	$x^{n-1}y$	..	x^2y	xy	y
x^{n-1}	x^{n-1}	1	x	..	x^{n-2}	$x^{n-2}y$	..	xy	y	$x^{n-1}y$
x^{n-2}	x^{n-2}	x^{n-1}	1	..	x^{n-3}	$x^{n-3}y$	..	y	$x^{n-1}y$	$x^{n-2}y$
:	:	:	:	:	:	:	:	:	:	:
x	x	x^2	x^3	..	1	y	..	x^3y	x^2y	xy
$x^{n-1}y$	$x^{n-1}y$	$x^{n-2}y$	$x^{n-3}y$	..	y	1	..	x^{n-3}	x^{n-2}	x^{n-1}
:	:	:	:	:	:	:	:	:	:	:
x^2	x^2	xy	y	..	x^3y	x^3	..	1	x	x^2
xy	xy	y	$x^{n-1}y$	..	x^2y	x^2	..	x^{n-1}	1	x
y	y	$x^{n-1}y$	x^2y	..	xy	x	..	x^{n-2}	x^{n-1}	1

□

Acknowledgement

This work is a part of a dissertation written by the first author and submitted to Umm Al-Qura University as a partial fulfillment for the master degree in mathematics. The first author would like to thank her supervisor Prof. Ahmed A. Khammash for his support and encouragement.

References

[1] R. Hamming, *Error detecting and error correcting codes*, The Bell Syst. Tech. J., **29** (1950), 147-160.
[2] F. J. MacWilliams, *Codes and ideals in group algebra*, Comb. Math. Appl., (1969), 317-328.
[3] T. Hurley, *Group rings and rings of matrices*, Int. J. Pure Appl. Math, **31**(3) (2006), 319-335.
[4] P. Hurley, T. Hurley, *Codes from zero-divisors and units in group rings*, (2007), arXiv:0710.5893v1 [cs.IT].
[5] M. Hamed, *Constructing codes from group rings*, Msc dissertation, Umm Al-Qura University, 2018.
[6] M. Hamed, A. Khammash, *Coding matrices for GL (2, q)*, Fundam. J. Math. Appl., 1(2) (2018), 118-130.
[7] P. Hurley, T. Hurley, *Block codes from matrix and group rings*, Chapter 5, in *Selected topics in information and coding theory*, I. Woungang, S. Misra, (Eds.), World Scientific, (2010), 159-194.