www.combinatorics.ir

Transactions on Combinatorics
ISSN (print): 2251-8657, ISSN (on-line): 2251-8665
Vol. 2 No. 1 (2013), pp. 17-26.

www.ui.ac.ir

GRAY ISOMETRIES FOR FINITE p-GROUPS

REZA SOBHANI

Communicated by Leo Storme

Abstract. We construct two classes of Gray maps, called type-I Gray map and type-II Gray map, for a finite p-group G. Type-I Gray maps are constructed based on the existence of a Gray map for a maximal subgroup H of G. When G is a semidirect product of two finite p-groups H and K, both H and K admit Gray maps and the corresponding homomorphism $\psi : H \longrightarrow \mathrm{Aut}(K)$ is compatible with the Gray map of K in a sense which we will explain, we construct type-II Gray maps for G. Finally, we consider group codes over the dihedral group D_8 of order 8 given by the set of their generators, and derive a representation and an encoding procedure for such codes.

1. Introduction

The realization that many seemingly nonlinear binary codes are indeed Gray images of some extended cyclic codes over $\mathbb{Z}_4$, motivated the study of cyclic codes over rings rather than fields [1, 2]. After [1] and [2], many efforts have been made to obtain good binary codes from linear codes over rings. However, only a few of them had success. Among them we may refer to [3], [4], [5] and [6]. In [3] a binary $(64, 2^{37}, 12)$-code has been constructed using Galois extensions of the ring $\mathbb{Z}_4$. In [4], by introducing a Gray isometry for codes over finite chain rings, a ternary $(36, 3^{12}, 15)$-code has been constructed from the Gray image of the $\mathbb{Z}_9$-lift of the ternary Golay code. In a similar way, a binary $(96, 2^{37}, 24)$-code has been constructed from the Gray image of the $\mathbb{Z}_8$-lift of the binary Golay code in [5]. In [6], originally by a heuristic computer search and then by a geometric construction based on a hyperoval in the projective Hjelmslev plane over $\mathbb{Z}_4$, a new nonlinear binary code with parameters $(58, 2^7, 28)$, having twice as many codewords as the biggest linear binary codes of equal length and

MSC(2010): Primary: 94B25; Secondary: 05E15.

Keywords: Finite group, Code, Gray map, Isometry.

Received: 27 May 2012, Accepted: 13 April 2013.

minimum distance, has been constructed. The code also improves the known lower bound on the maximal size of binary block codes of that length and minimum distance.

In the code constructions of the above research papers, the key is the Gray isometry which acts as a distance-invariant map and connects linear codes over $\mathbb{Z}_4$, $\mathbb{Z}_9$ and $\mathbb{Z}_8$ to binary or ternary codes. In this regard, a weight function on the ring $\mathbb{Z}_m$, as a generalization of the Lee weight on $\mathbb{Z}_4$, was given in [7]. Also for the case $m = p^2$, a Gray map between spaces $\mathbb{Z}_{p^2}^n$ and $\mathbb{Z}_p^{pn}$, as a generalization of the usual Gray map between $\mathbb{Z}_4^n$ and $\mathbb{Z}_2^{2n}$, was introduced there. After this work, for various kinds of rings, some generalizations for the Gray map have been introduced in [4, 8–12].

Recall from coding theory that linear codes of length n over a finite commutative ring R with identity are defined as submodules of R^n. When $R = \mathbb{Z}_m$, linear codes of length n over $\mathbb{Z}_m$ become subgroups of the abelian group $\mathbb{Z}_m^n$. Therefore, in a general manner, a code of length n over an arbitrary group G is defined to be a subgroup of the group G^n.

Note that codes over general groups, treated as the Hamming spaces, were extensively studied in [13]. It was shown there that codes over non-abelian groups have poor minimum Hamming distances ([13, Sections III and IV]). Also it was proved there that codes over abelian groups can not have parameters better than those over elementary abelian groups ([13, Theorem 5]).

An interesting field of research may now be introducing Gray isometries for an arbitrary finite p-group G and then searching for good codes from among Gray images of subgroups of G^n. In this paper, we construct two classes of Gray maps, called type-I Gray map and type-II Gray map, for an arbitrary finite p-group G. Type-I Gray maps are constructed based on the existence of a Gray map for a maximal subgroup H of G while type-II Gray maps are constructed when G is a semidirect product of two finite p-groups H and K, both H and K admit Gray maps, and the corresponding homomorphism $\psi : H \longrightarrow \mathrm{Aut}(K)$ is compatible with the Gray map of K in a sense which we will explain later. At the end, we consider group codes over the dihedral group D_8 of order 8 given by the set of their generators, and derive a representation and an encoding process for such codes.

The paper is organized as follows. In the next section, we present background information and preliminaries. Section 3 is devoted to the construction of two types of Gray isometries for finite p-groups. In Section 4, we deal with group codes over D_8.

2. Preliminaries and Background

Let R be a finite commutative ring with identity. A code C of length n over R is a subset of R^n. The code C is said to be linear if C is a submodule of R^n. For any two elements $\mathbf{u} = (u_1, u_2, \ldots, u_n)$ and $\mathbf{v} = (v_1, v_2, \ldots, v_n)$ of C, the Hamming distance between $\mathbf{u}$ and $\mathbf{v}$, denoted by $d_H(\mathbf{u}, \mathbf{v})$, is defined to be the number of positions i for which $u_i \neq v_i$. Also the Hamming weight of $\mathbf{u}$, denoted by $w_H(\mathbf{u})$, is defined to be the number of positions for which $u_i \neq 0$. The minimum distance of C, denoted by $d(C)$ or briefly d, is the minimum of the distances between different elements of C. If $|C| = M$ and $d(C) = d$ then C is said to be a (n, M, d)-code over R. When R is a finite field and $\dim_R C = k$ then C is said to be an $[n, k, d]$-code. It is worth mentioning that when C is a linear code, then the minimum

distance of C is equal to the minimum weight of nonzero elements of C. The latter is denoted by $w_H(C)$.

A linear code over the ring $\mathbb{Z}_4$ is called a quaternary code. It is well-known that any quaternary code is permutation-equivalent to a quaternary code C with generator matrix of the form

$$G = \begin{pmatrix} I_{k_1} & A & B \\ 0 & 2I_{k_2} & 2C \end{pmatrix}$$

where A and C are $\mathbb{Z}_2$-matrices and B is a $\mathbb{Z}_4$-matrix. The code is then an abelian group of type $4^{k_1}2^{k_2}$ with $2^{2k_1+k_2}$ codewords. In what follows we shall indicate this by saying that C has type (k_1, k_2).

3. **Constructions for Gray Isometries**

For a prime p, let G be an arbitrary finite p-group. We start the section with the definition of a Gray map.

Definition 3.1. *A map $\phi : G \longrightarrow \mathbb{Z}_p^n$ is said to be a Gray map, if the following properties hold:*

1: *The map $d_\phi : G \times G \longrightarrow \mathbb{N} \cup \{0\}$ defined by $d_\phi(a, b) = w_H(\phi(ab^{-1}))$ is a distance on G.*

2: *For all a, b in G we have $d_\phi(a, b) = d_H(\phi(a), \phi(b))$.*

The following lemma can be easily proved and hence we omit its proof.

Lemma 3.2. *Condition 1 in the definition of a Gray map, is equivalent to the following conditions:*

a: *For $g \in G$ we have $w_H(\phi(g)) = 0$ if and only if $g = id$, where id stands for the identity of G.*

b: *For all g in G we have $w_H(\phi(g)) = w_H(\phi(g^{-1}))$.*

c: *For all x, y in G we have $w_H(\phi(xy)) \leq w_H(\phi(x)) + w_H(\phi(y))$.*

□

Remark 3.3. *It can be verified from the definition of a Gray map $\phi : G \longrightarrow \mathbb{Z}_p^n$ that ϕ is an isometry between metric spaces (G, d_ϕ) and $(\mathbb{Z}_p^n, d_H)$. Therefore a Gray map is sometimes called a Gray isometry.*

Remark 3.4. *A metric d on a group G is said to be left (resp. right) invariant if*

$$d(a, b) = d(ag, bg) \ (resp.\ d(a, b) = d(ga, gb))$$

for all $a, b, g \in G$. For a Gray map ϕ on a group G, the metric d_ϕ is always a left invariant metric on G. Clearly, when G is abelian, any left invariant metric d on G is also right invariant. However, there are left invariant metrics on nonabelian groups, which are not right invariant.

If $\phi : G \longrightarrow \mathbb{Z}_p^n$ is a Gray isometry then for any $g \in G$, the Hamming weight of $\phi(g)$, i.e. $w_H(\phi(g))$, is called the ϕ-weight of g and is denoted by $w_\phi(g)$. Also for elements g and h in G, the Hamming distance between $\phi(g)$ and $\phi(h)$, i.e. $d_H(\phi(g), \phi(h))$, is called the ϕ-distance of g and h and is denoted by $d_\phi(g, h)$.

3.1. **Type-I Gray Maps.** In this subsection, G is a finite p-group of order p^m, H is a maximal subgroup of G with $[G : H] = p$ and $G/H = \langle xH\rangle$. In this part, we construct a Gray map for G, called type-I Gray map, based on the existence of a Gray map for H. For $i \in \mathbb{Z}_p$, let us denote the all i vector in $\mathbb{Z}_p^n$ by $\mathbf{i}$. Also we denote the usual concatenation of vectors in $\mathbb{Z}_p^n$ by $|$. Suppose $\phi : H \longrightarrow \mathbb{Z}_p^n$ is a Gray isometry and define the map $\widehat{\phi} : G \longrightarrow \mathbb{Z}_p^{pn}$ by $\widehat{\phi}(x^i h) = \eta_i(\phi(h))$, where $\eta_i : \mathbb{Z}_p^n \longrightarrow \mathbb{Z}_p^{pn}$ is the map which sends $\mathbf{v}$ to $(\mathbf{v}|\mathbf{v}+\mathbf{i}|\mathbf{v}+2\mathbf{i}|\cdots|\mathbf{v}+(p-1)\mathbf{i})$.

Lemma 3.5. *For any $\mathbf{v} \in \mathbb{Z}_p^n$ we have $w_H(\eta_0(\mathbf{v})) = pw_H(\mathbf{v})$ and $w_H(\eta_i(\mathbf{v})) = (p-1)n$ for $i \neq 0$. Specially $w_H(\widehat{\phi}(x^i h)) = pw_H(\phi(h))$ if $i = 0$ and $w_H(\widehat{\phi}(x^i h)) = (p-1)n$ if $i \neq 0$.*

Proof. Let $i \neq 0$ and for $0 \leq t \leq p-1$ set $E_t^{\mathbf{v}} := \{1 \leq j \leq n | v_j = t\}$. We have $n = \sum_{t=0}^{p-1} |E_t^{\mathbf{v}}|$ and $|E_0^{\mathbf{v}}| = n - w_H(\mathbf{v})$. On the other hand

$$\begin{aligned} w_H(\eta_i(\mathbf{v})) &= (n - |E_0^{\mathbf{v}}|) + (n - |E_{-i}^{\mathbf{v}}|) + \cdots + (n - |E_{-(i(p-1))}^{\mathbf{v}}|) \\ &= pn - \textstyle\sum_{t=0}^{p-1} |E_{it}^{\mathbf{v}}| \\ &= \begin{cases} (p-1)n, & i \neq 0; \\ pw_H(\mathbf{v}), & i = 0. \end{cases} \end{aligned}$$

□

Lemma 3.6. *For all $g \in G$ we have $w_H(\widehat{\phi}(g)) = w_H(\widehat{\phi}(g^{-1}))$.*

Proof. Follows from previous lemma and the fact that $g \in H$ if and only if $g^{-1} \in H$. □

Lemma 3.7. *For all $a, b \in G$ we have $w_H(\widehat{\phi}(ab)) \leq w_H(\widehat{\phi}(a)) + w_H(\widehat{\phi}(b))$.*

Proof. Assume that $a = x^i h_1$, $b = x^j h_2$ and $ab = x^{i+j} h_3$ for some $h_1, h_2, h_3 \in H$. If $i + j \neq 0$ then we have $w_H(\widehat{\phi}(ab)) = (p-1)n$ while $w_H(\widehat{\phi}(a)) + w_H(\widehat{\phi}(b))$ is equal to $(p-1)n + pw_H(h_1)$ or $(p-1)n + pw_H(h_2)$ or $2(p-1)n$. In each of the above cases the claim is true. If $i + j = 0$ then we have $i = j = 0$ or $i = -j$ are nonzero. In the first case, the claim is true due to the fact that ϕ is an isometry. In the second case we have $w_H(\widehat{\phi}(ab)) = pw_H(\phi(h_3)) \leq pn \leq 2(p-1)n = w_H(\widehat{\phi}(a)) + w_H(\widehat{\phi}(b))$. The proof is now completed. □

Theorem 3.8. *With notation as above, the map $\widehat{\phi}$ is a Gray isometry.*

Proof. Clearly, Lemmas 3.2, 3.5, 3.6 and 3.7 imply that $d_{\widehat{\phi}} : G \times G \longrightarrow \mathbb{N} \cup \{0\}$ defined by $d_{\widehat{\phi}}(a, b) = w_H(\widehat{\phi}(ab^{-1}))$ is a distance on G. Now we must prove that $d_{\widehat{\phi}}(a, b) = d_H(\widehat{\phi}(a), \widehat{\phi}(b))$ or equivalently $w_H(\widehat{\phi}(ab^{-1})) = w_H(\widehat{\phi}(a) - \widehat{\phi}(b))$. To see this, assume that $a = x^i h_1$, $b = x^j h_2$. Since $ab^{-1} \in H$ if and only if a and b belong to the same coset of H and this is equivalent to $i = j$, according to Lemma 3.5 we have

$$w_H(\widehat{\phi}(ab^{-1})) = \begin{cases} (p-1)n, & i \neq j; \\ pw_H(\phi(h_1 h_2^{-1})), & i = j. \end{cases}$$

On the other hand

$$\begin{aligned} w_H(\widehat{\phi}(a)-\widehat{\phi}(b)) &= w_H(\widehat{\phi}(x^ih_1)-\widehat{\phi}(x^jh_2)) \\ &= w_H(\eta_i(\phi(h_1))-\eta_j(\phi(h_2))) \\ &= w_H(\eta_{i-j}(\phi(h_1)-\phi(h_2))) \\ &= \begin{cases} (p-1)n, & i\neq j; \\ pw_H(\phi(h_1)-\phi(h_2)), & i=j. \end{cases} \end{aligned}$$

Since ϕ is a Gray isometry, we have $w_H(\phi(h_1h_2^{-1})) = w_H(\phi(h_1)-\phi(h_2))$ and the proof is now completed. □

Corollary 3.9. *The group G admits a type-I Gray map $\phi : G \longrightarrow \mathbb{Z}_p^{p^{m-1}}$.*

Proof. Let $\{1\} = G_0 \leq G_1 \leq \cdots \leq G_m = G$ be a sequence of subgroups of G where $[G_i : G_{i-1}] = p$. We proceed by induction on m. If $m = 1$ then G has size p and hence is isomorphic to $\mathbb{Z}_p$. In this case the identity map is the desired Gray map. Now if G_i, $i \geq 1$, admits a Gray map $\phi_i : G_i \longrightarrow \mathbb{Z}_p^{p^{i-1}}$ then by Theorem 3.8, G_{i+1} also admits a Gray map $\phi_{i+1} : G_{i+1} \longrightarrow \mathbb{Z}_p^{p^i}$. Therefore, $G_m = G$ admits the desired Gray map and the proof is completed. □

Example 3.10. Let G be the cyclic group of order 4, namely the group $\mathbb{Z}_4 = \{0, 1, 2, 3\}$. Assume that $H = \{0, 2\} \leq G$ be the maximal subgroup of G which is isomorphic to $\mathbb{Z}_2$. Let $\phi_0 : H \longrightarrow \mathbb{Z}_2$ be the identity map which sends 0 to 0 and 2 to 1. Clearly ϕ_0 is a Gray isometry. Set $\psi_1 := \widehat{\phi_0}$. We have $\phi_1(0) = \phi_0(0)|\phi_0(0) = 00$, $\phi_1(2) = \phi_0(1)|\phi_0(1) = 11$, $\phi_1(1) = \phi_0(0)|(\phi_0(0)+1) = 01$ and $\phi_1(3) = \phi_0(1)|(\phi(1)+1) = 10$. This is the well-known Gray map on $\mathbb{Z}_4$. Now let G be the cyclic group of order 8, namely the group $\mathbb{Z}_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$. Assume that $H = \{0, 2, 4, 6\} \leq G$ be the maximal subgroup of G which is isomorphic to $\mathbb{Z}_4$. Let $\phi_1 : H \longrightarrow \mathbb{Z}_2^2$ be the previously constructed Gray map for $\mathbb{Z}_4$. Set $\phi_2 := \widehat{\phi_1}$. We have

$$\begin{aligned} &\phi_2(0) = \phi_1(0)|\phi_1(0) = 0000, \\ &\phi_2(2) = \phi_1(1)|\phi_1(1) = 0101, \\ &\phi_2(4) = \phi_1(2)|\phi_1(2) = 1111, \\ &\phi_2(6) = \phi_1(3)|\phi_1(3) = 1010, \\ &\phi_2(1) = \phi_1(0)|(\phi_1(0)+11) = 0011, \\ &\phi_2(3) = \phi_1(1)|(\phi_1(1)+11) = 0110, \\ &\phi_2(5) = \phi_1(2)|(\phi_1(2)+11) = 1100, \\ &\phi_2(7) = \phi_1(3)|(\phi_1(3)+11) = 1001. \end{aligned}$$

If one construct a Gray map for $\mathbb{Z}_{p^m}$ by generalizing the method of this example, it can be verified that this Gray map is an alternative for the one given in [9].

Example 3.11. Let G be the dihedral group $D_8 = \langle \epsilon, \rho | \epsilon^2 = \rho^4 = 1, \epsilon\rho = \rho^3\epsilon \rangle$ of size 8. Clearly $\langle \rho \rangle \cong \mathbb{Z}_4$ is a cyclic maximal subgroup of D_8 equipped with the Gray map $\phi_1 : \mathbb{Z}_4 \longrightarrow \mathbb{Z}_2^2$ described

in the previous example. Now we can construct a Gray map ϕ from D_8 to $\mathbb{Z}_2^4$ as follows:

$$\begin{aligned}
&\phi(1) = \phi_1(0)|\phi_1(0) = 0000,\\
&\phi(\rho) = \phi_1(1)|\phi_1(1) = 0101,\\
&\phi(\rho^2) = \phi_1(2)|\phi_1(2) = 1111,\\
&\phi(\rho^3) = \phi_1(3)|\phi_1(3) = 1010,\\
&\phi(\epsilon) = \phi_1(0)|(\phi_1(0) + 11) = 0011,\\
&\phi(\epsilon\rho) = \phi_1(1)|(\phi_1(1) + 11) = 0110,\\
&\phi(\epsilon\rho^2) = \phi_1(2)|(\phi_1(2) + 11) = 1100,\\
&\phi(\epsilon\rho^3) = \phi_1(3)|(\phi_1(3) + 11) = 1001.
\end{aligned}$$

3.2. **Type-II Gray Maps.** In this subsection we assume that G is a finite p-group of order p^m which is isomorphic to the semidirect product of two finite p-groups H and K of orders p^a and p^b respectively, i.e. $G = H \ltimes_\psi K$ where $\psi : H \longrightarrow \mathrm{Aut}(K)$ is a group homomorphism. Let $\phi_1 : H \longrightarrow \mathbb{Z}_p^{n_1}$ and $\phi_2 : K \longrightarrow \mathbb{Z}_p^{n_2}$ be Gray maps, where ϕ_2 is compatible with ψ in the sense that for all $h \in H$ we have

$$w_H(\phi_2(k)) = w_H(\phi_2(\psi_h(k))),$$

then in the next theorem we show that $\phi : G \longrightarrow \mathbb{Z}_p^{n_1+n_2}$ with $\phi(hk) = (\phi_1(h), \phi_2(k))$ is a Gray map which we call type-II Gray map.

Theorem 3.12. *With notation as above, if ϕ_2 is compatible with ψ then the map ϕ is a Gray isometry.*

Proof. First we show that conditions (a), (b) and (c) in Lemma 3.2 hold. Condition (a) is trivially satisfied. For (b), assume $hk \in G$. We have

$$\begin{aligned}
w_H(\phi((hk)^{-1})) &= w_H(\phi((h^{-1}\psi_{h^{-1}}(k^{-1})))\\
&= w_H(\phi_1(h^{-1})) + w_H(\phi_2(\psi_{h^{-1}}(k^{-1})))\\
&= w_H(\phi_1(h)) + w_H(\phi_2(\psi_{h^{-1}}(k)^{-1}))\\
&= w_H(\phi_1(h)) + w_H(\phi_2(\psi_{h^{-1}}(k)))\\
&= w_H(\phi_1(h)) + w_H(\phi_2(k))\\
&= w_H(\phi(hk))
\end{aligned}$$

where, 5th equality follows from the fact that ϕ_2 is compatible with ψ. With a similar proof, one can check that Condition (c) of Lemma 3.2 and Condition (2) in the definition of a Gray map hold for ϕ. Therefore ϕ is a Gray isometry and the proof is now completed. □

Example 3.13. Again, let G be the dihedral group $D_8 = \langle \epsilon, \rho | \epsilon^2 = \rho^4 = 1, \epsilon\rho = \rho^3\epsilon \rangle$ of size 8. We have $D_8 \cong \mathbb{Z}_2 \ltimes_\psi \mathbb{Z}_4$, where $\psi : \mathbb{Z}_2 \longrightarrow \mathrm{Aut}(\mathbb{Z}_4)$ is a homomorphism which sends $a \in \mathbb{Z}_2$ to $f_a : \mathbb{Z}_4 \longrightarrow \mathbb{Z}_4$ with $f_a(b) = (-1)^a b$ for all $b \in \mathbb{Z}_4$. Consider the identity Gray map $\phi_1 : \mathbb{Z}_2 \longrightarrow \mathbb{Z}_2$ and the Gray map

$\phi_2 : \mathbb{Z}_4 \longrightarrow \mathbb{Z}_2^2$ described in the example 3.10. Now we can construct a type-II Gray map θ from D_8 to $\mathbb{Z}_2^3$ as follows:

$$\begin{aligned}
&\theta(1) = \phi_1(0)|\phi_2(0) = 000,\\
&\theta(\rho) = \phi_1(0)|\phi_2(1) = 001,\\
&\theta(\rho^2) = \phi_1(0)|\phi_2(2) = 011,\\
&\theta(\rho^3) = \phi_1(0)|\phi_2(3) = 010,\\
&\theta(\epsilon) = \phi_1(1)|\phi_2(0) = 100,\\
&\theta(\epsilon\rho) = \phi_1(1)|\phi_2(1) = 101,\\
&\theta(\epsilon\rho^2) = \phi_1(1)|\phi_2(2) = 111,\\
&\theta(\epsilon\rho^3) = \phi_1(1)|\phi_2(3) = 110.
\end{aligned}$$

4. **Group Codes over** D_8

By a group code of length n over a finite group G we mean a subgroup of G^n. In this section we consider group codes over the dihedral group D_8 which are given by the set of their generators, and derive a representation and an encoding procedure for such codes.

For $\mathrm{a} = (a_1, a_2, \cdots, a_n) \in \mathbb{Z}_2^n$, let $(-1)^{\mathrm{a}}$ be the vector of length n whose i-th entry is $(-1)^{a_i}$. Also let $*$ denotes the componentwise multiplication of two vectors. Note that $D_8^n \cong \mathbb{Z}_2^n \ltimes_\psi \mathbb{Z}_4^n$, where $\psi : \mathbb{Z}_2^n \longrightarrow \mathrm{Aut}(\mathbb{Z}_4^n)$ is a homomorphism given by $\psi(\mathbf{a}) = f_{\mathrm{a}}$ and $f_{\mathrm{a}} : \mathbb{Z}_4^n \longrightarrow \mathbb{Z}_4^n$ is an automorphism of $\mathbb{Z}_4^n$ with the role $f_{\mathrm{a}}(\mathrm{b}) = (-1)^{\mathrm{a}} * \mathrm{b}$. In what follows, we analyze the structure of subgroups of D_8^n. We identify an element of D_8^n with its image in the group $\mathbb{Z}_2^n \ltimes_\psi \mathbb{Z}_4^n$. For example, the element $(\epsilon, \epsilon\rho^2) \in D_8^2$ corresponds to the element $(1, 1, 0, 2)$ of $\mathbb{Z}_2^2 \ltimes_\psi \mathbb{Z}_4^2$.

Let $H = \langle (x_1, y_1), \cdots, (x_l, y_l) \rangle$ be a subgroup of D_8^n, where $x_i \in \mathbb{Z}_2^n$ and $y_i \in \mathbb{Z}_4^n$ for $1 \leq i \leq n$. We put these generators of H in a matrix M, called a generator matrix of H, as follows:

$$M = \begin{pmatrix} x_1 & y_1 \\ x_2 & y_2 \\ \vdots & \vdots \\ x_l & y_l \end{pmatrix}.$$

Since

$$(x_i, y_i)(x_j, y_j) = (x_i + x_j, (-1)^{x_j} * y_i + y_j), \tag{4.1}$$

we may perform row-column operations to obtain the following equivalent form for M:

$$M = \begin{pmatrix} I_{k_1} & \mathbf{0} & A & B \\ \mathbf{0} & I_{k_2} & C & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & D \end{pmatrix},$$

where A and C are binary matrices while B and D are quaternary matrices. The matrix D also can be put in the form

$$D = \begin{pmatrix} I_{k_3} & D_1 & D_2 \\ \mathbf{0} & 2I_{k_4} & 2D_3 \end{pmatrix},$$

and therefore M can be written in the form

$$M = \begin{pmatrix} I_{k_1} & \mathbf{0} & A & B_1 & B_2 & B_3 \\ \mathbf{0} & I_{k_2} & C & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & I_{k_3} & D_1 & D_2 \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & 2I_{k_4} & 2D_3 \end{pmatrix}. \tag{4.2}$$

On the other hand, we have $H' \leq Z(H)$, where H' is the commutator subgroup of H and $Z(H)$ is the center of H. Hence we have $H' = \langle [(x_i, y_i), (x_j, y_j)] \mid 1 \leq i < j \leq l \rangle$. Setting $H^2 = \{h^2 \mid h \in H\}$ we have $H'H^2 = \mathrm{Fratt}(H) \leq 2\mathbb{Z}_4^n$, where $\mathrm{Fratt}(H)$ is the Frattini subgroup of H. We may now assume that $\mathrm{Fratt}(H)$ is contained in the quaternary code generated by D, since otherwise we may add it to D and then write down D in its standard form. The form of M which is given in 4.2, is referred to as the *standard form* of M.

The next theorem now describes the structure of H, when M has been written in the standard form. Note that for $t \in \mathbb{Z}_4$ and a row $\mathbf{v}$ of M, by $t.\mathbf{v}$ we mean $\mathbf{v}^t$ where the multiplication is that given in 4.1.

Theorem 4.1. *Let H be a group code of length n over D_8 with a generator matrix M in the standard form given by 4.2. Then we have $|H| = 4^{k_3} 2^{(k_1+k_2+k_4)}$. Moreover, any codeword in H is of the form $\mathbf{v}M$ where $\mathbf{v} = (\mathbf{r}, \mathbf{s}, \mathbf{t}, \mathbf{u})$, $\mathbf{r} \in \mathbb{Z}_2^{k_1}$, $\mathbf{s} \in \mathbb{Z}_2^{k_2}$, $\mathbf{t} \in \mathbb{Z}_4^{k_3}$ and $\mathbf{u} \in \mathbb{Z}_2^{k_4}$.*

Proof. The proof follows from the following facts:

1) for any two rows $\mathbf{u}$ and $\mathbf{v}$ of M we have $\mathbf{uv} = [\mathbf{u}, \mathbf{v}]\mathbf{vu}$, where $[\mathbf{u}, \mathbf{v}]$ stands for the commutator of two group elements $\mathbf{u}$ and $\mathbf{v}$.
2) $H' \leq Z(H)$.
3) $\mathrm{Fratt}(H) = H'H^2$ is a subgroup of the quaternary code generated by D.

□

Example 4.2. Let H be the subgroup of D_8^4 with the set of generators

$$M = \{(\epsilon, \epsilon\rho, \rho, \rho^3), (\epsilon\rho^2, \epsilon\rho^3, \rho^3, \rho), (\rho, \rho, \rho, \rho), (1, \rho^2, 1, \rho^2)\}.$$

In the matrix representation we have

$$M = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 1 & 1 & 3 \\ 1 & 1 & 0 & 0 & 2 & 3 & 3 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 2 & 0 & 2 \end{pmatrix}$$

It can be easily verified that the standard for of M is shore

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

Hence we have $|H| = 2^5$. Let ϕ and θ be type-I and type-II Gray maps for D_8. It can be seen that $\phi(H)$ is a binary $(16, 2^5, 8)$ code while $\theta(C)$ is a binary $(12, 2^5, 4)$ code.

Acknowledgments

The author would like to thank the referee for his/her constructive and invaluable comments which greatly improved the presentation and results of this paper. This work was partially supported by the Center of Excellence for Mathematics, University of Isfahan.

References

[1] A. A. Nechaev, Kerdock code in a cyclic form, *Discrete Math. Appl.*, **1** (1991) 365-384.

[2] A. R. Hammons, P. V. Kummar, A. R. Calderbank, N. J. A. Sloane and P. Sole, The $\mathbb{Z}_4$ linearity of Kerdock, Preparata, Goethals, and related codes, *IEEE Trans. Inform. Theory*, **40** (1994) 301–319.

[3] A. R. Calderbank and G. McGuire, Construction of a $(64, 2^{37}, 12)$ code via Galois rings, *Des. Codes Cryptogr.*, **10** (1997) 157–165.

[4] M. Greferath and S. E. Schmidt, Gray isometries for finite chain rings and a nonlinear ternary $(36, 3^{12}, 15)$-code, *IEEE Trans. Inform. Theory*, **45** (1999) 2522–2524.

[5] I. M. Duursma, M. Greferath, S. Litsyn and S. E. Schmidt, A $\mathbb{Z}_8$-linear lift of the binary Golay code and a non-linear binary $(96, 2^{37}, 24)$-code, *IEEE Trans. Inform. Theory*, **47** (2001) 1596-1598.

[6] M. Kiermaier and J. Zwanzger, A $\mathbb{Z}_4$-linear code of high minimum Lee distance derived from a hyperoval, *Adv. Math. Commun.*, **5** (2011) 275–286.

[7] I. Constantinescu and W. Heise, A metric for codes over residue class rings, *Problems Inform. Transmission*, **33** (1997) 208–213.

[8] H. Tapia-Recillas and G. Vega, Some constacyclic codes over $\mathbb{Z}_{2^k}$ and binary quasi-cyclic codes, *Discrete Appl. Math.*, **128** (2003) 305–316.

[9] S. Ling and T. Blackford, $\mathbb{Z}_{p^{k+1}}$-linear codes, *IEEE Trans. Inform. Theory*, **48** (2002) 2592–2605.

[10] J. F. Qian, L. N. Zhang and S. X. Zhu, $(1 + u)$ Constacyclic and cyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2$, *Appl. Math. Lett.*, **19** (2006) 820–823.

[11] J. F. Qian, L. N. Zhang and S. X. Zhu, Constacyclic and cyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2$, *IEICE Trans. Fundamentals*, **E89-A** (2006) 1863–1865.

[12] R. Sobhani and M. Esmaeili, Some Constacyclic and cyclic codes over $\mathbb{F}_q[u]/\langle u^{t+1}\rangle$, *IEICE Trans. Fundamentals*, **E93-A** (2010) 808–813.

[13] G. D. Forney, On the Hamming distance properties of group codes, *IEEE Trans. Inform. Theory*, **38** (1992) 1797–1801.

Reza Sobhani
Department of Mathematics, University of Isfahan, P.O.Box 81746-73441, Isfahan, Iran
Email: r.sobhani@sci.ui.ac.ir