CERTAIN BINARY MINIMAL CODES CONSTRUCTED USING SIMPLICIAL COMPLEXES

VIDYA SAGAR AND RITUMONI SARMA

ABSTRACT. In this article, we work over the non-chain ring $\mathcal{R} = \mathbb{Z}_2[u]/\langle u^3 - u\rangle$. Let $m \in \mathbb{N}$ and let $L, M, N \subseteq [m] := \{1, 2, \ldots, m\}$. For $X \subseteq [m]$, define $\Delta_X := \{v \in \mathbb{Z}_2^m : \mathrm{Supp}(v) \subseteq X\}$ and $D := (1+u^2)D_1 + u^2\big(D_2 + (u+u^2)D_3\big)$, a subset of $\mathcal{R}^m$, where $D_1 \in \{\Delta_L, \Delta_L^c\}, D_2 \in \{\Delta_M, \Delta_M^c\}, D_3 \in \{\Delta_N, \Delta_N^c\}$. The linear code C_D over $\mathcal{R}$ defined by $\{\big(v \cdot d\big)_{d\in D} : v \in \mathcal{R}^m\}$ is studied for each D. For instance, we obtain the Lee weight distribution of C_D. The Gray map $\Phi : \mathcal{R} \longrightarrow \mathbb{Z}_2^3$ given by $\Phi(a + ub + u^2d) = (a + b, b + d, d)$ is utilized to derive a binary linear code, namely, $\Phi(C_D)$ for each D. Sufficient conditions for each of these binary linear codes to be minimal are obtained. In fact, sufficient conditions for minimality are mild in nature, for example, $|L|, |M|, |N| < m - 2$ is a set of conditions for minimality of $\Phi(C_D)$ for each D. Moreover, these binary codes are self-orthogonal if each of L, M and N is nonempty.

1. INTRODUCTION

This article studies the linear code $C_D = \{\big(v \cdot d_1, v \cdot d_2, \ldots, v \cdot d_n\big) : v \in \mathcal{R}^m\}$ over $\mathcal{R} = \mathbb{Z}_2[u]/\langle u^3 - u\rangle$, where $D \subseteq \mathcal{R}^m$ and m is a positive integer. Ding et al. in [5] first considered the above construction of C_D. By using simplicial complexes, several interesting linear codes have been constructed in the recent past. The authors in [7] studied linear codes by using simplicial complexes and obtained a class of binary optimal linear codes. Zhu et al. in [21] studied minimal linear codes over $\mathbb{F}_4$. Yansheng et al. in [19] studied linear codes over $\mathbb{F}_4$ and produced two infinite classes of optimal codes; motivated by this work, the authors in [9] constructed linear codes over $\mathbb{F}_8$ using simplicial complexes and discussed optimal and minimal codes.

The study of minimal codes is an active research topic nowadays because of its applications in secure two-party computation and secret sharing schemes [3, 10]. Minimal codes are helpful to construct the access structure of secret sharing schemes [4, 8]. This special class of codes is also important as these can be decoded by using the minimum distance decoding rule [1]. Many researchers have studied linear codes over finite rings using simplicial complexes and produced minimal codes (see [11–14, 16, 17, 20]).

Motivated by the research in [14], a natural endeavor is to explore the construction of linear codes over other finite rings using simplicial complexes and obtain minimal codes. We, in this manuscript, study linear codes over $\mathcal{R}$ whose defining set is obtained from certain simplicial complexes. We also obtain their Lee-weight distributions. By considering a Gray map, we obtain certain binary linear codes and establish sufficient conditions for these codes to be minimal. Moreover, we show that these binary codes are self-orthogonal.

The remaining sections of this manuscript are arranged as follows. Preliminaries are presented in the next section. Section 3 studies construction of linear codes using simplicial complexes. In

2010 *Mathematics Subject Classification.* 94B05, 05E45.
Key words and phrases. linear code, simplicial complex, Lee weight distribution, minimal code.

Section 4, we consider a Gray map and obtain a family of binary codes. Besides, we establish certain sufficient conditions for these binary codes to be minimal and self-orthogonal. Section 5 concludes this manuscript.

2. Definitions and Preliminaries

Throughout the manuscript, $\mathcal{R} = \mathbb{Z}_2[u]/\langle u^3 - u\rangle$, where $\mathbb{Z}_2$ is the binary field. Observe that $\mathcal{R}$ is a non-chain principal ideal ring. The ring $\mathcal{R}$ can be written as $(1+u^2)\mathbb{Z}_2 + u^2\big(\mathbb{Z}_2 + (u+u^2)\mathbb{Z}_2\big)$ uniquely (see [18]). Let $\Phi : \mathcal{R} \longrightarrow \mathbb{Z}_2^3$ be the *Gray map* given by $\Phi(a + ub + u^2d) = (a + b, b + d, d)$. This extends to $\Phi : \mathcal{R}^m \longrightarrow \mathbb{Z}_2^{3m}$ where $\Phi(r + us + u^2t) = (r + s, s + t, t)$. An $\mathcal{R}$-submodule C is $\mathcal{R}^n$ is a *linear code* over $\mathcal{R}$ and m is its length. Let $v, w \in \mathbb{Z}_2^m$. Then the *Hamming weight* of v denoted by $wt_H(v)$ is the number of nonzero entries in v.
Let $x = \alpha+u\beta+u^2\gamma \in \mathcal{R}^m$, where $\alpha, \beta, \gamma \in \mathbb{Z}_2^m$. Then the *Lee weight* of x is $wt_L(x) = wt_H(\Phi(x)) = wt_H(\alpha+\beta)+wt_H(\beta+\gamma)+wt_H(\gamma)$. Note that the image of a linear code over $\mathcal{R}$ under a Gray map is a binary linear code. Suppose C is a linear code over $\mathcal{R}$ of length n, where $n \in \mathbb{N}$. Let A_i be the cardinality of the set that contains all codewords of C having Lee weight i, $0 \le i \le 3n$. Then the string $(1, A_1, \ldots, A_n)$ is called the *Lee weight distribution* of C. In addition, if the total number of $i \ge 1$ such that $A_i \ne 0$ is l, then C is called an *l-weight linear code*.

3. Construction of linear codes using simplicial complexes

For $m \in \mathbb{N}$, we shall write $[m]$ to denote the set $\{1, 2, \ldots, m\}$. For any $n, m \in \mathbb{N}$, let $D = \{d_1 < d_2 < \cdots < d_n\}$ be an ordered subset of $\mathcal{R}^m$ of cardinality n. Define [6],

$$C_D = \{(v \cdot d_1, v \cdot d_2, \ldots, v \cdot d_n) : v \in \mathcal{R}^m\}, \tag{3.1}$$

where $x \cdot y = \sum_{i=1}^{m} x_i y_i$ for $x, y \in \mathcal{R}^m$. C_D forms a linear code of length $|D| = n$. The ordered set D is termed as the *defining set* of C_D. Note that on changing the ordering of D we will get a permutation equivalent code. If D is chosen appropriately, C_D may possess good parameters. For $w \in \mathbb{Z}_2^m$, the set $\mathrm{Supp}(w) = \{i \in [m] : w_i = 1\}$ is called the *support* of w. Note that the Hamming weight of $w \in \mathbb{Z}_q^m$ is $wt_H(w) = |\mathrm{Supp}(w)|$. For $v, w \in \mathbb{Z}_2^m$, one says that v covers w if $\mathrm{Supp}(w) \subseteq \mathrm{Supp}(v)$. If v covers w we write $w \preceq v$.
Consider the map $\psi : \mathbb{Z}_2^m \longrightarrow 2^{[m]}$ is defined as $\psi(w) = \mathrm{Supp}(w)$, where $2^{[m]}$ denotes the power set of $[m]$. Note that ψ is a bijective map. Now onwards, we will write w instead of $\mathrm{Supp}(w)$ whenever we require.
A subset Δ of $\mathbb{Z}_2^m$ is called a *simplicial complex* if $u \in \Delta$ then $w \in \mathbb{Z}_2^m \implies w \in \Delta$ whenever $w \preceq u$. $v \in \Delta$ is called *maximal* if for $w \in \Delta$, $v \preceq w$ imply $v = w$. Let $L \subseteq [m]$. The simplicial complex generated by $L \subseteq [m]$ is denoted by Δ_L and is defined as

$$\Delta_L = \{w \in \mathbb{Z}_2^m |\ \mathrm{Supp}(w) \subseteq L\}. \tag{3.2}$$

Note that $\psi^{-1}(L)$ is maximal in Δ_L and $|\Delta_L| = |2^L| = 2^{|L|}$.
The following result describes Lee weight distributions of C_D for various choices of D.

Theorem 3.1. *Suppose that $m \in \mathbb{N}$ and $L, M, N \subseteq [m]$.*

(1) *Let $D = (1 + u^2)\Delta_L + u^2(\Delta_M + (u + u^2)\Delta_N) \subset \mathcal{R}^m$. Then C_D is a 2-weight linear code of length $|D| = 2^{|L|+|M|+|N|}$ and size $2^{|L|+|M|+|M\cup N|}$. The Lee weight distribution of C_D is displayed in Table 1.*

Lee weight	*Frequency*
$3 \times 2^{\lvert L\rvert+\lvert M\rvert+\lvert N\rvert-1}$	$2^{3m} + 2^{3m-\lvert L\rvert-\lvert M\rvert-\lvert M\cup N\rvert+1} - 2^{3m-\lvert L\rvert-\lvert M\rvert} - 2^{3m-\lvert L\rvert-\lvert M\rvert-\lvert N\rvert+1}$
$2^{\lvert L\rvert+\lvert M\rvert+\lvert N\rvert}$	$2^{3m-\lvert L\rvert-\lvert M\rvert} + 2^{3m-\lvert L\rvert-\lvert M\rvert-\lvert N\rvert+1} - 3 \times 2^{3m-\lvert L\rvert-\lvert M\rvert-\lvert M\cup N\rvert}$
0	$2^{3m-\lvert L\rvert-\lvert M\rvert-\lvert M\cup N\rvert}$

TABLE 1

(2) *Let* $D = (1+u^2)\Delta_L^c + u^2(\Delta_M + (u+u^2)\Delta_N) \subset \mathcal{R}^m$. *Then* C_D *is a* 4*-weight linear code of length* $|D| = (2^m - 2^{|L|}) \times 2^{|M|+|N|}$ *and size* $2^{m+|M|+|M\cup N|}$. *The Lee weight distribution of* C_D *is displayed in a Table (omitted for brevity).*
(3) *Let* $D = (1+u^2)\Delta_L + u^2(\Delta_M^c + (u+u^2)\Delta_N) \subset \mathcal{R}^m$. *Then* C_D *is* 5*-weight linear code of length* $|D| = (2^m - 2^{|M|}) \times 2^{|L|+|N|}$ *and size* $2^{2m+|L|}$. *The Lee weight distribution of* C_D *is displayed in a Table (omitted for brevity).*
(4) *Let* $D = (1+u^2)\Delta_L + u^2(\Delta_M + (u+u^2)\Delta_N^c) \subset \mathcal{R}^m$. *Then* C_D *is a* 4*-weight linear code of length* $|D| = (2^m - 2^{|N|}) \times 2^{|L|+|M|}$ *and size* $2^{m+|L|+|M|}$. *The Lee weight distribution of* C_D *is displayed in a Table (omitted for brevity).*
(5) *Let* $D = (1+u^2)\Delta_L^c + u^2(\Delta_M^c + (u+u^2)\Delta_N) \subset \mathcal{R}^m$. *Then* C_D *is* 10*-weight linear code of length* $|D| = (2^m - 2^{|L|})(2^m - 2^{|M|}) \times 2^{|N|}$ *and size* 2^{3m}. *The Lee weight distribution of* C_D *is displayed in a Table (omitted for brevity).*
(6) *Let* $D = (1+u^2)\Delta_L^c + u^2(\Delta_M + (u+u^2)\Delta_N^c) \subset \mathcal{R}^m$. *Then* C_D *is* 8*-weight linear code of length* $|D| = (2^m - 2^{|L|})(2^m - 2^{|N|}) \times 2^{|M|}$ *and size* $2^{2m+|M|}$. *The Lee weight distribution of* C_D *is displayed in a Table (omitted for brevity).*
(7) *Let* $D = (1+u^2)\Delta_L + u^2(\Delta_M^c + (u+u^2)\Delta_N^c) \subset \mathcal{R}^m$. *Then* C_D *is* 8*-weight linear code of length* $|D| = (2^m - 2^{|M|})(2^m - 2^{|N|}) \times 2^{|L|}$ *and size* $2^{2m+|L|}$. *The Lee weight distribution of* C_D *is displayed in a Table (omitted for brevity).*
(8) *Let* $D = (1+u^2)\Delta_L^c + u^2(\Delta_M^c + (u+u^2)\Delta_N^c) \subset \mathcal{R}^m$. *Then* C_D *is* 16*-weight linear code of length* $|D| = (2^m - 2^{|L|})(2^m - 2^{|M|})(2^m - 2^{|N|})$ *and size* 2^{3m}. *The Lee weight distribution of* C_D *is displayed in a Table (omitted for brevity).*

Remark 3.2. The tables omitted in Theorem 3.1 are ready and we can provide when needed.

4. Gray images and minimal linear codes

Here we discuss minimality and self-orthogonality of the binary codes derived from C_D through the Gray map Φ. Let C be a linear code over $\mathbb{Z}_2$. An element $v_0 \in C \setminus \{0\}$ is called *minimal* if $v \preceq v_0$ and $v \in C \setminus \{0\}$ imply $v = v_0$. If every codeword of $C \setminus \{0\}$ is minimal then we say that C is a *minimal code.*

Proposition 4.1. *Assume that* C_D *as in Theorem 3.1. Then the Gray image* $\Phi(C_D)$ *is binary self-orthogonal code provided* L, M, N *are nonempty subsets of* $[m]$.

The following result describes the minimality condition for the binary code $\Phi(C_D)$ for each D in Theorem 3.1.

Theorem 4.2. *Let $m \in \mathbb{N}$ and let $L, M, N \subseteq [m]$. Assume that C_D as in Theorem 3.1. Let $w_0 = \min\{wt_H(c) : (0 \neq)c \in \Phi(C_D)\}$ and $w_\infty = \max\{wt_H(c) : c \in \Phi(C_D)\}$. Then the sufficient conditions for the Gray image $\Phi(C_D)$ to be a minimal code is given in Table 2 for each D.*

S.N.	*D as in*	w_0	w_∞	*minimality condition*
1	*Theorem 3.1(1)*	$2^{\lvert L\rvert+\lvert M\rvert+\lvert N\rvert}$	$3 \times 2^{\lvert L\rvert+\lvert M\rvert+\lvert N\rvert-1}$	*no conditions*
2	*Theorem 3.1(2)*	$(2^m - 2^{\lvert L\rvert}) \times 2^{\lvert M\rvert+\lvert N\rvert}$	$3 \times 2^{m+\lvert M\rvert+\lvert N\rvert-1}$	$\lvert L\rvert \leq m-2$
3	*Theorem 3.1(3)*	$(2^m - 2^{\lvert M\rvert}) \times 2^{\lvert L\rvert+\lvert N\rvert}$	$3 \times 2^{m+\lvert L\rvert+\lvert N\rvert-1}$	$\lvert M\rvert \leq m-3$
4	*Theorem 3.1(4)*	$(2^m - 2^{\lvert N\rvert}) \times 2^{\lvert L\rvert+\lvert M\rvert}$	$2^{\lvert L\rvert+\lvert M\rvert-1} \times (3 \times 2^m - 2^{\lvert N\rvert+1})$	$\lvert N\rvert \leq m-2$
5	*Theorem 3.1(5)*	$(2^m - 2^{\lvert L\rvert})(2^m - 2^{\lvert M\rvert}) \times 2^{\lvert N\rvert}$	$3 \times (2^m - 2^{\lvert L\rvert}) \times 2^{m+\lvert N\rvert-1}$, *if* $\lvert L\rvert \leq \lvert M\rvert$	$\lvert M\rvert \leq m-3$
			$3 \times (2^m - 2^{\lvert M\rvert}) \times 2^{m+\lvert N\rvert-1}$, *if* $\lvert L\rvert \geq \lvert M\rvert+1$	$\lvert L\rvert \leq m-3$
6	*Theorem 3.1(6)*	$(2^m - 2^{\lvert L\rvert})(2^m - 2^{\lvert N\rvert}) \times 2^{\lvert M\rvert}$	$3 \times (2^m - 2^{\lvert N\rvert}) \times 2^{m+\lvert M\rvert-1}$, *if* $\lvert N\rvert \leq \lvert L\rvert+1$	$\lvert L\rvert \leq m-3$
			$(2^m - 2^{\lvert L\rvert})(3 \times 2^m - 2^{\lvert N\rvert+1}) \times 2^{\lvert M\rvert-1}$, *if* $\lvert N\rvert \geq \lvert L\rvert+2$	$\lvert N\rvert \leq m-2$
7	*Theorem 3.1(7)*	$(2^m - 2^{\lvert M\rvert})(2^m - 2^{\lvert N\rvert}) \times 2^{\lvert L\rvert}$	$(2^m - 2^{\lvert M\rvert})(3 \times 2^m - 2^{\lvert N\rvert+1}) \times 2^{\lvert L\rvert-1} + (2^m - 2^{\lvert N\rvert}) \times 2^{\lvert L\rvert+\lvert M\rvert-1}$ $-2^{\lvert L\rvert+\lvert M\rvert+\lvert N\rvert-1}$, *if* $\lvert M\rvert \leq m-2, \lvert N\rvert \leq m-2$	*no conditions*
8	*Theorem 3.1(8)*	$(2^m - 2^{\lvert L\rvert})(2^m - 2^{\lvert M\rvert})(2^m - 2^{\lvert N\rvert})$	$(2^m - 2^{\lvert L\rvert})(2^m - 2^{\lvert M\rvert})(3 \times 2^{m-1} - 2^{\lvert N\rvert})$ $+(2^m - 2^{\lvert L\rvert})(2^m - 2^{\lvert N\rvert+1}) \times 2^{\lvert M\rvert-1}$	$\lvert M\rvert \leq m-2, \lvert N\rvert \leq m-2$
			$3 \times (2^m - 2^{\lvert M\rvert})(2^m - 2^{\lvert N\rvert}) \times 2^{m-1}$	$\lvert L\rvert \leq m-3$

Table 2. Minimality conditions in Theorem 4.2

5. Conclusion

In this article, simplicial complexes are used to construct certain linear codes over $\mathcal{R}$. Binary codes which are obtained as Gray images of these linear codes, are minimal and self-orthogonal under certain conditions that are mild in nature.

References

[1] Ashikhmin, A. and Barg, A.: Minimal vectors in linear codes. IEEE Trans. Inf. Theory, **44**(5), 2010-2017, (1998)

[2] Chang, S. and Hyun, J. Y.: Linear codes from simplicial complexes. Des. Codes Cryptogr., **86**(10), 2167-2181, (2018)

[3] Chabanne, H., Cohen, G. and Patey, A.: Towards secure two-party computation from the wire-tap channel. in: Proceeding of ICISC 2013 (Lecture Notes in Computer Science, vol. 8565), H.-S. Lee and D.-G. Han Eds. Berlin: Springer-Verlag, 34-46, (2014)

[4] Ding, K. and Ding, C.: A class of two-weight and three-weight codes and their applications in secret sharing. IEEE Trans. Inf. Theory, **61**(11), 5835-5842, (2015)

[5] Ding, C., Helleseth, T., Klove, T. and Wang, X.: A generic construction of Cartesian authentication codes. IEEE Trans. Inf. Theory, **53**(6), 2229-2235, (2007)

[6] Huffman W. C. and Pless, V.: Fundamentals of Error-Correcting Codes. Cambridge University Press, Cambridge, (2003)

[7] Hyun, J. Y., Lee, J. and Lee, Y.: Infinite families of optimal linear codes constructed from simplicial complexes. IEEE Trans. Inf. Theory, **66**(11), 6762-6775, (2020)

[8] Massey, J. L.: Minimal codewords and secret sharing., In Proc. 6th Joint Swedish-Russian Int. Workshop on Info. Theory, 276-279, (1993)

[9] Sagar, V. and Sarma, R.: Linear codes using simplicial complexes. Cryptogr. Commun., (to appear), (2022)
[10] Shamir, A.: How to share a secret. Commun. ACM, **22**(11), 612-613, (1979)
[11] Shi, M. and Li, X.: A new family of optimal binary few-weight codes from simplicial complexes. IEEE Communications Letters, **25**(4), 1048-1051, (2021)
[12] Shi, M., Guan, Y., Wang, C. and Solé, P.: Few-weight codes from trace codes over Rk. Bulletin of the Australian Mathematical Society, **98**(1), 167-174, (2018)
[13] Shi, M., Qian, L., Helleseth, T. and Solé, P.: Five-weight codes from three-valued correlation of M-sequences. Advances in Mathematics of Communications, doi:10.3934/amc.2021022, (2021)
[14] Shi, M. and Li, X. Few-weight codes over a non-chain ring associated with simplicial complexes and their distance optimal Gray image. Finite Fields and Their Applications, **80**, 101994, (2022)
[15] Shi, M. and Li, X.: Few-weight codes over a non-chain ring associated with simplicial complexes and their distance optimal Gray image. Finite Fields Their Appl., **80**, 101994, (2022)
[16] Shi, M. and Li, X.: New classes of binary few weight codes from trace codes over a chain ring. Journal of Applied Mathematics and Computing, **68**(3), 1869-1880, (2022)
[17] Shi, M., Xuan, W. and Solé, P.: Two families of two-weight codes over Z4. Designs, Codes and Cryptography, **88**(12), 2493-2505, (2020)
[18] Kaya, A., Yildiz, B. and Siap, I.: New extremal binary self-dual codes of length 68 from quadratic residue codes over $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2$. Finite Fields and Their Applications, **29**, 160-177, (2014)
[19] Wu, Y., Li, C. and Xiao, F.: Quaternary linear codes and related binary subfield codes. IEEE Transactions on Information Theory, **68**(5), 3070-3080, (2022)
[20] Wu, Y., Zhu, X. and Yue, Q.: Optimal few-weight codes from simplicial complexes. IEEE Transactions on Information Theory, **66**(6), 3657-3663, (2020)
[21] Zhu, X. and Wei, Y.: Few-weight quaternary codes via simplicial complexes. AIMS Math., **6**(5), 5124-5132, (2021)

(V. Sagar) Department of Mathematics, IIT Delhi, New Delhi, India 110016
Email address: `vsagariitd@gmail.com`

(R. Sarma) Department of Mathematics, IIT Delhi, New Delhi, India 110016
Email address: `ritumoni407@gmail.com`