IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 3 July 2023, accepted 19 August 2023, date of publication 28 August 2023, date of current version 5 September 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3309246

RESEARCH ARTICLE

Self-Dual Double Circulant, Self-Dual Double Negacirculant and LCD Double Negacirculant Codes Over the Ring $\frac{\mathbb{F}_q[u,v]}{\langle u^2-u,\ v^2-v,\ uv-vu\rangle}$

HAI Q. DINH[1], BHANU PRATAP YADAV[2], BAC T. NGUYEN[3,4], ASHISH KUMAR UPADHYAY[5], AND WORAPHON YAMAKA[6]

[1]Department of Mathematical Sciences, Kent State University, Kent, OH 44240, USA
[2]Department of Communications and Networking, Aalto University, 02150 Espoo, Finland
[3]Faculty of Natural Sciences, Duy Tan University, Da Nang 550000, Vietnam
[4]Institute of Fundamental and Applied Sciences, Duy Tan University, Ho Chi Minh City, Da Nang 550000, Vietnam
[5]Department of Mathematics, Banaras Hindu University, Varanasi 221005, India
[6]Centre of Excellence in Econometrics, Chiang Mai University, Chiang Mai 50200, Thailand

Corresponding author: Bhanu Pratap Yadav (bhanupratap.yadav@aalto.fi)

This work was supported in part by the Centre of Excellence in Econometrics, Faculty of Economics, Chiang Mai University, Thailand.

ABSTRACT In this paper, we investigate self-dual double circulant, and self-dual and linear complementary dual (LCD) double negacirculant codes over a finite ring $R = \mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q + uv\mathbb{F}_q$, where $u^2 = u$, $v^2 = v$, $uv = vu$ and $q = p^m$. We study the algebraic structure of double circulant codes over R. We provide necessary and sufficient conditions for a double circulant code to be a self-dual code. We give a formula to get the total number of self-dual double circulant codes over the ring R. We compute distance bounds for self-dual double circulant codes over R. In addition, by using a Gray map, we show that the families of self-dual double circulant codes under the Gray map are asymptotically good. Moreover, the algebraic structure of double negacirculant codes and necessary and sufficient conditions for a double negacirculant code to be a self-dual code and to be an LCD code are also given. We determine the total number of self-dual and LCD double negacirculant codes over R.

INDEX TERMS Double circulant codes, double negacirculant codes, self-dual codes, LCD codes, Gray map, Artin conjecture.

I. INTRODUCTION

Assume that $\mathcal{C}(n)$ is a family of codes over the finite field $\mathbb{F}_q$ and it has parameters $[n, k_n, d_n]$. The rate ρ and the relative distance of $\mathcal{C}(n)$ are expressed as $\rho = \limsup_{n\to\infty} \frac{k_n}{n}$ and $\delta = \liminf_{n\to\infty} \frac{d_n}{n}$, respectively. If there is a sequence of codes in $\mathcal{C}(n)$ satisfying ρ and δ are finite, then $\mathcal{C}(n)$ is called to be asymptotically good. It is not an easy process to compute the rate and relative distance for any class of linear codes. On other hand, for some special cases, we can find the rate and relative distance of particular families of linear codes. People want to discover asymptotically good cyclic codes or describe that all cyclic codes are asymptotically bad. (see [3], [22], [24]).

Let C be a linear code, I be an identity matrix and B be a circulant or a negacirculant matrix. Then C is a double circulant (briefly, DC) code or a double negacirculant (briefly, DN) code if C has a generator matrix of the form $G = [I, B]$. In 1969, [5] proved that binary DC codes are asymptotically good.

In 2006, [18] provided a class of cyclic codes over a finite field that is asymptotically good. In 1969, Chen et al. [5] showed that a class of quasi-cyclic codes over the finite fields meets the Gilbert-Varshamov bound. In 2001, [15] studied the algebraic structure of quasi-cyclic codes over finite fields and finite chain rings.

The associate editor coordinating the review of this manuscript and approving it for publication was Zesong Fei.

At the latest, DC codes and DN codes over finite fields are studied in [1] and [2]. In 2020, [21] used a Gray map and provided some self-dual double circulant (briefly, SDDC) and LCD double circulant codes over $\mathbb{Z}_4$. Reference [11] gave SDDC and LCD double circulant codes over $\mathbb{Z}_{p^2}$, for $p \equiv 1 \pmod 4$ and p is an odd prime. Exact enumeration formulas and asymptotic lower bounds on the minimum distance of p-ary Gray images of these codes are also presented in [11]. In addition, Yao et al. [23] discussed the asymptotic performance of SDDC and LCD double circulant codes over a non-chain ring. Furthermore, asymptotically good self-dual and LCD codes of length $6n$ over $\mathbb{F}_q$ are determined in [23].

SDDC codes, LCD double circulant codes and DN codes over $\mathbb{F}_q + u\mathbb{F}_q$ are given by Shi et al. [22]. However, in their enumeration formulas, there are some inaccuracies. After that, [24] studied LCD double circulant codes and DN codes over $\mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q$.

Motivated by these, in this paper, we study on the SDDC codes, self-dual double negacirculant (briefly, SDDN) codes and LCD double negacirculant codes over R. We prove that the families of SDDC codes and LCD double circulant codes over R under a Gray map are asymptotically good.

The rest of our paper is organized as follows. In Section II, the algebraic structures of R are provided. We prove that the Gray image of a self-dual code is also a self-dual code. Some examples of Gray images of DC codes are given. In Section III, we provide the structures of DC codes and the conditions for a DC code to be self-dual. The SDDC codes over R are also presented in this section. In Section IV, we enumerate the distance bounds of SDDC codes. On the assumption that the Artin's conjecture on primitive roots holds true, the families of SDDC codes over R under the Gray map are asymptotically good. In Section V, the structures of DN codes and conditions for a DN code to be a self-dual or LCD code are given. The SDDN codes and LCD double negacirculant codes over R are listed in Section V. Finally, Section VI concludes the paper with some open directions for future work.

II. PRELIMINARIES

Let $\mathbb{F}_q$ be the finite field where $q = p^m$. We consider the finite commutative ring R. It implies that R has q^4 elements including $(q-1)^4$ units, $q^4-(q-1)^4$ non units. We see that R has four maximal ideals. Let $\zeta_0 = (1-u-v+uv)$, $\zeta_1 = (uv)$, $\zeta_2 = (u-uv)$ and $\zeta_3 = (v-uv)$. We see that $\zeta_0+\zeta_1+\zeta_2+\zeta_3 = 1$, $\zeta_i^2 = \zeta_i$ and $\zeta_i\zeta_j = 0$ where $i, j = 0, 1, 2, 3$ and $i \neq j$. Then $\{\zeta_0, \zeta_1, \zeta_2, \zeta_3\}$ forms a nonzero pairwise orthogonal idempotent set of R. Therefore, $R = \zeta_0 R \oplus \zeta_1 R \oplus \zeta_2 R \oplus \zeta_3 R \cong \zeta_0\mathbb{F}_q \oplus \zeta_1\mathbb{F}_q \oplus \zeta_2\mathbb{F}_q \oplus \zeta_3\mathbb{F}_q$. Let us suppose that $r \in R$. Then r is of the form $a_0 + ua_1 + va_2 + uva_3$. We see that

$$\begin{aligned} r &= (1-u-v+uv)b_0 + uvb_1 + (u-uv)b_2 + (v-uv)b_3 \\ &= b_0 + u(b_2-b_o) + v(b_3-b_0) + uv(b_0+b_1-b_2-b_3) \\ &= a_0 + ua_1 + va_2 + uva_3 \end{aligned}$$

where $a_0 = b_0$, $a_1 = (b_2 - b_o)$, $a_2 = (b_3 - b_o)$, $a_3 = (b_0 + b_1 - b_2 - b_3)$. Hence, $r = \zeta_0 b_0 + \zeta_1 b_1 + \zeta_2 b_2 + \zeta_3 b_3$.

Let

$$A = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}.$$

Define a Gray map $\psi : R \longmapsto \mathbb{F}_q^4$ given by $\psi(r) = (b_0, b_3, b_2, b_1)A$, where $b_0, b_1, b_2, b_3 \in \mathbb{F}_q$. It can also extend component-wise from R^n to $\mathbb{F}_q^{4n}$.

A nonempty subset $\mathcal{C}$ of R^n is a code of length n. Throughout this paper, $\mathcal{C}$ is a linear code of length n over R, i.e., $\mathcal{C}$ is a linear code if the subset $\mathcal{C}$ of R^n is an R-submodule of R^n. Let $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1})$ and $\mathbf{c}' = (c_0', c_1', \ldots, c_{n-1}') \in \mathcal{C}$ be codewords. The minimum Hamming weight $wt_H(\mathcal{C})$ of $\mathcal{C}$ is defined as $wt_H(\mathcal{C}) = \min\{wt_H(\mathbf{c}) \mid \mathbf{c} \in \mathcal{C}, \mathbf{c} \neq 0\}$, where $wt_H(\mathbf{c})$ is the Hamming weight of $\mathbf{c}$ and $wt_H(\mathbf{c})$ is determined by the number of nonzero coordinates of the codeword $\mathbf{c}$. The Hamming distance between $\mathbf{c}$ and $\mathbf{c}'$ is defined as $d_H(\mathbf{c}, \mathbf{c}') = |\{i \mid c_i \neq c_i'\}| = wt_H(\mathbf{c} - \mathbf{c}')$. The minimum Hamming distance $d_H(\mathcal{C})$ of $\mathcal{C}$ is defined as $d_H(\mathcal{C}) = \min\{d_H(\mathbf{c}, \mathbf{c}') | \mathbf{c} \neq \mathbf{c}'\} = d_H$. Let k be the dimension of $\psi(\mathcal{C})$. It is obvious that the Gray map ψ is a bijective linear distance preserving map. Thus, $\psi(\mathcal{C})$ has parameters $[4n, k, d_H]$, where $d_L = d_H$ (see [7]).

Let $\mathbf{c}$ and $\mathbf{c}' \in R^n$. The Euclidean inner product of between $\mathbf{c}$ and $\mathbf{c}'$ is defined as

$$\langle \mathbf{c}, \mathbf{c}' \rangle_E = c_0c_0' + c_1c_1' + \cdots + c_{n-1}c_{n-1}'.$$

The Euclidean dual code of $\mathcal{C}$ is given as

$$\mathcal{C}^{\perp} = \{\mathbf{c} \in R^n \mid \langle \mathbf{c}, \mathbf{c}' \rangle_E = 0, \text{ for all } \mathbf{c}' \in \mathcal{C}\}.$$

Let $\zeta_0a_0 + \zeta_1a_1 + \zeta_2a_2 + \zeta_3a_3 \in R$, where $a_i \in \mathbb{F}_q$, $i = 0, 1, 2, 3$ and q is a perfect square. In [15], its conjugate is given as follows:

$$\begin{aligned} \overline{\zeta_0a_0 + \zeta_1a_1 + \zeta_2a_2 + \zeta_3a_3} &= \zeta_0\bar{a_0} + \zeta_1\bar{a_1} + \zeta_2\bar{a_2} \\ &\quad + \zeta_3\bar{a_3} \\ &= \zeta_0a_0^{\sqrt{q}} + \zeta_1a_1^{\sqrt{q}} \\ &\quad + \zeta_2a_2^{\sqrt{q}} + \zeta_3a_3^{\sqrt{q}}. \end{aligned}$$

Recall that the Hermitian inner product of $\mathbf{c}$ and $\mathbf{c}'$ is given by

$$\langle \mathbf{c}, \mathbf{c}' \rangle_H = c_0\bar{c_0'} + c_1\bar{c_1'} + \cdots + c_{n-1}\bar{c_{n-1}'}.$$

The Hermitian dual code of $\mathcal{C}$ is defined as

$$\mathcal{C}^{\perp_H} = \{\mathbf{c} \in R^n \mid \langle \mathbf{c}, \mathbf{c}' \rangle_H = 0, \text{ for all } \mathbf{c}' \in \mathcal{C}\}.$$

It is well-known that if $\mathcal{C} \cap \mathcal{C}^{\perp} = \{0\}$, $\mathcal{C} \cap \mathcal{C}^{\perp_H} = \{0\}$, and $\mathcal{C}^{\perp} \subseteq \mathcal{C}$, then $\mathcal{C}$ is an Euclidean and a Hermitian LCD code, a dual-containing code, respectively. $\mathcal{C}$ is a self-dual code with respect to the Euclidean or Hermitian inner product if and only if $\mathcal{C} = \mathcal{C}^{\perp}$ or $\mathcal{C} = \mathcal{C}^{\perp_H}$, respectively.

In [6], the entropy function is given by

$$h_q(y) = \begin{cases} 0, & \text{if } y = 0, \\ y\log_q(q-1) - y\log_q(y) - \\ (1-y)\log_q(1-y), & 0 < y \le 1 - \frac{1}{q}. \end{cases} \quad (1)$$

In order to construct DC codes, we need to determine when the ring R contains a square root of -1. Similar to the proof of [16, Theorem 6.1], we give the following result.

Theorem 1: The field $\mathbb{F}_q$ and the ring R contain a square root of -1 if and only if $q \equiv 1 \pmod 4$.

Example 1: We determine the solutions of the equation $y^2 + 1 = 0$ in $\mathbb{F}_5$ and $\mathbb{F}_3$. Assume that $q = 5$, we have $5 \equiv 1 \pmod 4$, by Theorem 1, then $\mathbb{F}_5$ contains a square root of -1. They are 2 and 3. Therefore, solutions of the equation $y^2 + 1 = 0$ are 2 and 3. Assume $q = 3$, we have $3 \equiv 3 \pmod 4$, by Theorem 1, then $\mathbb{F}_3$ does not contains a square root of -1. Thus, $y^2 + 1 = 0$ has no solutions. Therefore, solutions of the equation $y^2 + 1 = 0$ over $\mathbb{F}_5$ are 2 and 3; and $y^2 + 1 = 0$ has no solutions over $\mathbb{F}_3$.

Let $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1})$ and $\mathbf{c}' = (c'_0, c'_1, \ldots, c'_{n-1}) \in \mathcal{C}$, where $c_i = \zeta_0 a_i + \zeta_1 b_i + \zeta_2 d_i + \zeta_3 e_i$, $c'_i = \zeta_0 a'_i + \zeta_1 b'_i + \zeta_2 d'_i + \zeta_3 e'_i$, where $a_i, a'_i, b_i, b'_i, d_i, d'_i, e_i, e'_i \in \mathbb{F}_q$, for $0 \le i \le n-1$. If $\mathcal{C}$ is a self-dual code over R, then $\langle \mathbf{c}, \mathbf{c}' \rangle_E = \sum_{i=0}^{n-1} (\zeta_0 a_i + \zeta_1 b_i + \zeta_2 d_i + \zeta_3 e_i)(\zeta_0 a'_i + \zeta_1 b'_i + \zeta_2 d'_i + \zeta_3 e'_i) = 0$. It shows that $\sum_{i=0}^{n-1} a_i a'_i = 0$, $\sum_{i=0}^{n-1} b_i b'_i = 0$, $\sum_{i=0}^{n-1} d_i d'_i = 0$ and $\sum_{i=0}^{n-1} e_i e'_i = 0$. From the definition of the Gray map, the Euclidean inner product between

$$\psi(\zeta_0 a_0 + \zeta_1 b_0 + \zeta_2 d_0 + \zeta_3 e_0, \ldots, \zeta_0 a_{n-1} + \zeta_1 b_{n-1} + \zeta_2 d_{n-1} + \zeta_3 e_{n-1})$$

and

$$\psi(\zeta_0 a'_0 + \zeta_1 b'_0 + \zeta_2 d'_0 + \zeta_3 e'_0, \ldots, \zeta_0 a'_{n-1} + \zeta_1 b'_{n-1} + \zeta_2 d'_{n-1} + \zeta_3 e'_{n-1})$$

equal to zero. It shows that $\psi(\mathbf{c}') \in \psi(\mathcal{C})^\perp$ as $\psi(\mathbf{c}) \in \psi(\mathcal{C})$. Therefore, $\psi(\mathcal{C}^\perp) \subseteq \psi(\mathcal{C})^\perp$. Since ψ is a bijection Gray map, it is simple to verify that $\psi(\mathcal{C}^\perp) = \psi(\mathcal{C})^\perp$. Summarizing our discussions above, the following theorem shows that the Gray map ψ preserves properties of a self-dual code.

Theorem 2: A linear code $\mathcal{C}$ of R is self-dual if and only if $\psi(\mathcal{C})$ is a self-dual code over $\mathbb{F}_q$.

Recall that the multiplicative surjective norm function is given from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q$ as $\text{Norm}(b) = b \cdot b^q \cdots b^{q^{m-1}} = b^{\frac{q^m-1}{q-1}}$, for $b \in \mathbb{F}_{q^m}^*$ and $\text{Norm}(0) = 0$. By [14, Theorem 2.28], Norm is an onto group homomorphism from $\mathbb{F}_{q^m}^*$ to $\mathbb{F}_q^*$. By the fundamental theorem of group homomorphism, we see that

$$\frac{|\mathbb{F}_{q^m}^*|}{|\text{Ker(Norm)}|} = |\mathbb{F}_q^*|,$$

where $\text{Ker(Norm)} = \{b \in \mathbb{F}_{q^m}^* \mid b^{\frac{q^m-1}{q-1}} - 1 = 0\}$. Therefore, $\frac{q^m-1}{|\text{Ker(Norm)}|} = q - 1$. It implies that $|\text{Ker(Norm)}| = \frac{q^m-1}{q-1}$.

Let H be a subgroup of a group G and $a, b \in G$. Then a is congruent to $b \mod H$ if $ab^{-1} \in H$. In notational form, we write $a \equiv b \mod H$.

By Lemma 2.4.3 in [10], this relation is an equivalence relation. Corresponding to the equivalence relation, we get equivalence classes. For any $a \in G$, the equivalence class of a is given by

$$cl(a) = \{x \in G \mid x \equiv a \mod H\}.$$

Let H be a subgroup of group G and let $a \in G$ be any element. Then $Ha = \{ha \mid h \in H\}$ is called a right coset of H in G. Lemma 2.4.4 in [10] states that for any $a \in G$, the set $Ha = \{ha \mid h \in H\}$ is an equivalence class of a with respect to the relation $a \equiv b \mod H$ if and only if $a^{-1}b \in H$. This means that Ha is the equivalence class of a in G/H, the quotient group of G by H. Lemma 2.4.5 in [10] states that any two distinct right cosets of H in G have no element in common, and each has $|H|$ elements. This follows from the fact that the cosets partition G and the equivalence classes partition G modulo H, so the number of cosets and the number of equivalence classes are the same. Since $|G/H| = [G : H]$, the index of H in G, $|Ha| = |H|$ for any $a \in G$. Therefore, $Ha = cl(a)$ and any two distinct right cosets of H in G have no element in common, and each has $|H|$ elements.

Let G be a finite group and H be a subgroup of G. According to Lagrange's Theorem, $|H|$ divides $|G|$. Moreover, the number of distinct right cosets of H in G is $\frac{|G|}{|H|}$. In our case, $H = \text{Ker(Norm)}$ and $G = \mathbb{F}_{q^m}^*$, the number of distinct right cosets of Ker(Norm) in $\mathbb{F}_{q^m}^*$ is $\frac{|\mathbb{F}_{q^m}^*|}{|\text{Ker(Norm)}|} = q - 1$ and each right coset has exactly $\frac{q^m-1}{q-1}$ elements. Therefore, the preimages for each element in $\mathbb{F}_q$ make a right coset in $\mathbb{F}_{q^m}^*$. Each right coset consists of exactly $\frac{q^m-1}{q-1}$ elements in $\mathbb{F}_{q^m}^*$. We can see that Ker(Norm) is also a right coset that has exactly $\frac{q^m-1}{q-1}$ elements. Hence, in particular, the number of different solutions of the equation $b^{\frac{q^m-1}{q-1}} = -1$ is $\frac{q^m-1}{q-1}$. We summarize our discussion above in the following result.

Proposition 1: Let the multiplicative surjective norm function from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q$ be given as $\text{Norm}(b) = b^{\frac{q^m-1}{q-1}}$, for $b \in \mathbb{F}_{q^m}^*$, and $\text{Norm}(0) = 0$. Then each element in $\mathbb{F}_q^*$ has exactly $\frac{q^m-1}{q-1}$ different preimages elements in $\mathbb{F}_{q^m}^*$. In particular, the equation $b^{\frac{q^m-1}{q-1}} = -1$ has precisely $\frac{q^m-1}{q-1}$ different solutions in $\mathbb{F}_{q^m}$.

Example 2: We solve the equation $y^{31} + 1 = 0$ over $\mathbb{F}_{5^3}$. Using $q = 5$ and $m = 3$, the norm function from $\mathbb{F}_{5^3}$ to $\mathbb{F}_5$ is $\text{Norm}(y) = y^{\frac{5^3-1}{5-1}} = y^{31}$, for $y \in \mathbb{F}_{5^3}^*$, we see that $\text{Norm}(y) = y^{31} = -1$. By Proposition 1, the equation $y^{31} + 1 = 0$ has exactly $\frac{5^3-1}{5-1} = 31$ different solutions in $\mathbb{F}_{5^3}$. These different solutions are -1, $-\gamma^4$, $-\gamma^8$, $-\gamma^{12}$, $-\gamma^{16}$, $-\gamma^{20}$, $-\gamma^{24}$, $-\gamma^{28}$, $-\gamma^{32}$, $-\gamma^{36}$, $-\gamma^{40}$, $-\gamma^{44}$, $-\gamma^{48}$, $-\gamma^{52}$, $-\gamma^{56}$, $-\gamma^{60}$, $-\gamma^{64}$, $-\gamma^{68}$, $-\gamma^{72}$, $-\gamma^{76}$, $-\gamma^{80}$, $-\gamma^{84}$, $-\gamma^{88}$, $-\gamma^{92}$, $-\gamma^{96}$, $-\gamma^{100}$, $-\gamma^{104}$, $-\gamma^{108}$, $-\gamma^{112}$, $-\gamma^{116}$, $-\gamma^{120}$. Here we consider a finite field of size 5^3 to be $\frac{\mathbb{F}_5[\gamma]}{\langle \gamma^3 + 3\gamma + 3 \rangle}$.

Let p be an odd prime, m, e be positive integers and q be an odd prime power such that $\gcd(p, q) = 1$. Assume that the order of q modulo p is $f = \frac{p-1}{e}$ and $q^f = 1 + p\lambda$, where p does not divide λ. Let $O_t(q)$ denote the order of q modulo t. Then we have the following proposition.

Proposition 2: [20] $O_{p^m}(q) = fp^{m-1}$ and there are $em+1$ distinct q-cyclotomic cosets modulo p^m for all $m \geq 1$.

Example 3: We find the number of distinct irreducible factors of $y^{27} - 1$ over $\mathbb{F}_5$. In this situation, $n = 27$ and $q = 5$, we can see $\gcd(27, 5) = 1$ then by Euler's theorem [10, page 43], we have $5^{18} \equiv 1 \pmod{27}$ but $5^k \not\equiv 1 \pmod{27}$ for all positive integers $k < 18$), i.e., $O_{27}(5) = 18$, we can write it as $O_{3^3}(5) = 2 * 3^{3-1}$. Using Proposition 2 for $p = 3, m = 3, f = 2$ and $e = \frac{3-1}{2} = 1$, then the number of distinct 5-cyclotomic cosets modulo 27 is $1 * 3 + 1 = 4$. Therefore, the number of monic irreducible factors of $y^{27} - 1$ over $\mathbb{F}_5$ is equal to the number of cyclotomic cosets of 5 modulo 27 (see [17, Corollary 3.4.12]). Hence, the number distinct irreducible factors of $y^{27} - 1$ over $\mathbb{F}_5$ is four. They are $y + 4, y^2 + y + 1, y^6 + y^3 + 1, y^{18} + y^9 + 1$.

Let A, B be $n \times n$ matrices. Then A is circulant if

$$A = \begin{bmatrix} a_0 & a_1 & \dots & a_{n-1} \\ a_{n-1} & a_0 & \dots & a_{n-2} \\ \vdots & \vdots & \ddots & \vdots \\ a_1 & a_2 & \dots & a_0 \end{bmatrix}.$$

The matrix B is negacirculant if

$$B = \begin{bmatrix} a_0 & a_1 & a_2 & \dots & a_{n-1} \\ -a_{n-1} & a_0 & a_1 & \dots & a_{n-2} \\ -a_{n-2} & -a_{n-1} & a_0 & \dots & a_{n-2} \\ \dots & \dots & \dots & \dots & \dots \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ -a_1 & -a_2 & -a_3 & \dots & a_0 \end{bmatrix}.$$

A linear code $\mathcal{C}$ is said to be DC code if $\mathcal{C}$ has a generator matrix of the form $G = [I_n, A]$. If it has of the form $G = [I_n, B]$, then it is a negacirculant code, where I_n denotes the identity matrix of order n. Moreover, a DC code of length $2n$ is a $\frac{\mathbb{F}_q[y]}{\langle y^n-1\rangle}$-submodule of $\left(\frac{\mathbb{F}_q[y]}{\langle y^n-1\rangle}\right)^2$ and a DN code of length $2n$ is a $\frac{\mathbb{F}_q[y]}{\langle y^n+1\rangle}$-submodule of $\left(\frac{\mathbb{F}_q[y]}{\langle y^n+1\rangle}\right)^2$ (see [13], [15], [16], [21]).

Assume that $n = ml$. Then C is called a (λ, l)-quasi-twisted code of index l if for any $c \in C$, we get $(\lambda c_{m-l}, \lambda c_{m-l+1}, \dots, \lambda c_{m-1}, c_0, \dots, c_{m-l-1}) \in C$. By identifying a polynomial $c(y) = c_0 + c_1 y + \dots + c_{n-1} y^{n-1} \in \frac{\mathbb{F}_q[y]}{\langle y^n-1\rangle}$ by a codeword $(c_0, c_1, \dots, c_{n-1}) \in C$, it is easy to prove that a (λ, l)-quasi-twisted code of length n with index l can be identified with a $\frac{\mathbb{F}_q[y]}{\langle y^n-1\rangle}$-submodule of $\left(\frac{\mathbb{F}_q[y]}{\langle y^n-1\rangle}\right)^l$.

From the definition of the Gray map, we have $\psi : R \longmapsto \mathbb{F}_q^4$ such that

$$\psi(\zeta_0 b_0 + \zeta_1 b_1 + \zeta_2 b_2 + \zeta_3 b_3) = (b_0, b_3, b_2, b_1)A,$$

where $b_0, b_1, b_2, b_3 \in \mathbb{F}_q$ and

$$A = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}.$$

By assumption, $B = \zeta_0 B_0 + \zeta_1 B_1 + \zeta_2 B_2 + \zeta_3 B_3$, where $B_i = [a^i_{jk}]_{n\times n}$, $i = 0, 1, 2, 3; j, k = 1, 2, \dots, n$.

$$\text{If } i = 0, \text{ then } B_0 = [a^0_{jk}] = \begin{bmatrix} a^0_{11} & a^0_{12} & \dots & a^0_{1n} \\ a^0_{21} & a^0_{22} & \dots & a^0_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a^0_{n1} & a^0_{n2} & \dots & a^0_{nn} \end{bmatrix}.$$

$$\text{If } i = 1, \text{ then } B_1 = [a^1_{jk}] = \begin{bmatrix} a^1_{11} & a^1_{12} & \dots & a^1_{1n} \\ a^1_{21} & a^1_{22} & \dots & a^1_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a^1_{n1} & a^1_{n2} & \dots & a^1_{nn} \end{bmatrix},$$

$$\text{If } i = 2, \text{ then } B_2 = [a^2_{jk}] = \begin{bmatrix} a^2_{11} & a^2_{12} & \dots & a^2_{1n} \\ a^2_{21} & a^2_{22} & \dots & a^2_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a^2_{n1} & a^2_{n2} & \dots & a^2_{nn} \end{bmatrix},$$

$$\text{If } i = 3, \text{ then } B_3 = [a^3_{jk}] = \begin{bmatrix} a^3_{11} & a^3_{12} & \dots & a^3_{1n} \\ a^3_{21} & a^3_{22} & \dots & a^3_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a^3_{n1} & a^3_{n2} & \dots & a^3_{nn} \end{bmatrix}.$$

Hence,

$$G = \begin{bmatrix} 1 & 0 & \dots & 0 & \sum_{i=0}^3 \zeta_i a^i_{11} & \sum_{i=0}^3 \zeta_i a^i_{12} & \dots & \sum_{i=0}^3 \zeta_i a^i_{1n} \\ 0 & 1 & \dots & 0 & \sum_{i=0}^3 \zeta_i a^i_{21} & \sum_{i=0}^3 \zeta_i a^i_{22} & \dots & \sum_{i=0}^3 \zeta_i a^i_{2n} \\ \vdots & \vdots & \ddots & & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 & \sum_{i=0}^3 \zeta_i a^i_{n1} & \sum_{i=0}^3 \zeta_i a^i_{n2} & \dots & \sum_{i=0}^3 \zeta_i a^i_{nn} \end{bmatrix}$$

Then we have

$$\begin{bmatrix} \zeta_0 G \\ \zeta_1 G \\ \zeta_2 G \\ \zeta_3 G \end{bmatrix} \longmapsto \begin{bmatrix} \psi(\zeta_0 G) \\ \psi(\zeta_1 G) \\ \psi(\zeta_2 G) \\ \psi(\zeta_3 G) \end{bmatrix},$$

where

$$\zeta_i G = \begin{bmatrix} \zeta_i & 0 & \dots & 0 & \zeta_i a^i_{11} & \zeta_i a^i_{12} & \dots & \zeta_i a^i_{1n} \\ 0 & \zeta_i & \dots & 0 & \zeta_i a^i_{21} & \zeta_i a^i_{22} & \dots & \zeta_i a^i_{2n} \\ \vdots & \vdots & \ddots & & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \zeta_i & \zeta_i a^i_{n1} & \zeta_i a^i_{n2} & \dots & \zeta_i a^i_{nn} \end{bmatrix}$$

for $i, j = 0, 1, \dots, 3$, $i \neq j$, and $\zeta_i^2 = \zeta_i$, $\zeta_i \zeta_j = 0$. By Gray map, we see that

$$\psi(\zeta_i G) = \begin{bmatrix} \psi(\zeta_i) & \psi(0) & \dots & \psi(0) & \psi(\zeta_i a^i_{11}) & \psi(\zeta_i a^i_{12}) & \dots & \psi(\zeta_i a^i_{1n}) \\ \psi(0) & \psi(\zeta_i) & \dots & 0 & \psi(\zeta_i a^i_{21}) & \psi(\zeta_i a^i_{22}) & \dots & \psi(\zeta_i a^i_{2n}) \\ \vdots & \vdots & \ddots & & \vdots & \vdots & \ddots & \vdots \\ \psi(0) & \psi(0) & \dots & \psi(\zeta_i) & \psi(\zeta_i a^i_{n1}) & \psi(\zeta_i a^i_{n2}) & \dots & \psi(\zeta_i a^i_{nn}) \end{bmatrix}$$

Thus,

$$M = \begin{bmatrix} \psi(\zeta_0 G) \\ \psi(\zeta_1 G) \\ \psi(\zeta_2 G) \\ \psi(\zeta_3 G) \end{bmatrix}_{4n \times 8n}.$$

Hence, the generator matrix of $\psi(\mathcal{C})$ can be determined as follows

$$M = \begin{bmatrix} I & I & I & I & B_0 & B_0 & B_0 & B_0 \\ I & -I & -I & I & B_1 & -B_1 & -B_1 & B_1 \\ I & I & -I & -I & B_2 & B_2 & -B_2 & -B_2 \\ I & -I & I & -I & B_3 & -B_3 & B_3 & -B_3 \end{bmatrix}_{4n \times 8n}.$$

By the discussions above, for finding their parameters, we give the following lemma.

Lemma 1: Let I be a $n \times n$ identity matrix and B_i be a $n \times n$ matrix over $\mathbb{F}_q$ such that $B = \zeta_0 B_0 + \zeta_1 B_1 + \zeta_2 B_2 + \zeta_3 B_3$ and B_i are q-ary matrices of order n for $i = 0, 1, 2, 3$. Assume that $G = [I, B]$ is the generator matrix of code $\mathcal{C}$. Then the generator matrix of $\psi(\mathcal{C})$ is as follows

$$M = \begin{bmatrix} I & I & I & I & B_0 & B_0 & B_0 & B_0 \\ I & -I & -I & I & B_1 & -B_1 & -B_1 & B_1 \\ I & I & -I & -I & B_2 & B_2 & -B_2 & -B_2 \\ I & -I & I & -I & B_3 & -B_3 & B_3 & -B_3 \end{bmatrix}.$$

We discuss some examples of DC codes by the map ψ. By Lemma 1, we present some DC codes parameters over $\mathbb{F}_5 + u\mathbb{F}_5 + v\mathbb{F}_5 + uv\mathbb{F}_5$ in Table 1. We use Magma software to compute [4]. The length of codes $\mathcal{C}$ over $\mathbb{F}_5 + u\mathbb{F}_5 + v\mathbb{F}_5 + uv\mathbb{F}_5$ is provided in the first column of Table 1. In the second, third, fourth and fifth columns, we list the generator polynomials $a_1(y)$, $a_2(y)$, $a_3(y)$ and $a_4(y)$, respectively. In the sixth column, corresponding parameters as the Gray images of $\mathcal{C}$ over $\mathbb{F}_5 + u\mathbb{F}_5 + v\mathbb{F}_5 + uv\mathbb{F}_5$ are listed in the Table 1.

The coefficients of $a_1(y)$, $a_2(y)$, $a_3(y)$ and $a_4(y)$ in decreasing order are presented in the second, third, fourth and fifth column of Table 1; for example, we express a polynomial $a_d y^d + a_{d-1} y^{d-1} + \cdots + a_0$ by $a_d a_{d-1} \ldots a_0$.

Example 4: We find the parameters of a Gray image of a DC code over $\mathbb{F}_7 + u\mathbb{F}_7 + v\mathbb{F}_7 + uv\mathbb{F}_7$. Let $B_0 = [1]$, $B_1 = [2]$, $B_2 = [3]$ and $B_3 = [4]$ be 1×1 matrices over $\mathbb{F}_7$ such that $B = \zeta_0 B_0 + \zeta_1 B_1 + \zeta_2 B_2 + \zeta_3 B_3$. Assume that $\mathcal{C}$ has the generator matrix $G = [I, B]$. By Lemma 1, the generator matrix of $\psi(\mathcal{C})$ is as follows

$$M = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & -1 & 1 & 2 & -2 & -2 & 2 \\ 1 & 1 & -1 & -1 & 3 & 3 & -3 & -3 \\ 1 & -1 & 1 & -1 & 4 & -4 & 4 & -4 \end{bmatrix}.$$

We use Magma software to compute [4], we get parameters of the code over $\mathbb{F}_7$ is [8, 4, 4].

Example 5: We find the parameters of a Gray image of a DC code over $\mathbb{F}_{17} + u\mathbb{F}_{17} + v\mathbb{F}_{17} + uv\mathbb{F}_{17}$. Let $B_0 = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$, $B_1 = \begin{bmatrix} 5 & 6 \\ 7 & 8 \end{bmatrix}$, $B_2 = \begin{bmatrix} 9 & 10 \\ 11 & 12 \end{bmatrix}$ and $B_3 = \begin{bmatrix} 13 & 14 \\ 15 & 16 \end{bmatrix}$ be 2×2 matrices over $\mathbb{F}_{17}$ such that $B = \zeta_0 B_0 + \zeta_1 B_1 + \zeta_2 B_2 + \zeta_3 B_3$. Assume that $\mathcal{C}$ has the generator matrix $G = [I, B]$. By Lemma 1 the generator matrix of $\psi(\mathcal{C})$ is as shown in the equation at the bottom of the page.

We use Magma software to compute [4], we get parameters of the code over $\mathbb{F}_{17}$ is [16, 8, 2].

Example 6: We find the parameters of a Gray image of a DC code over $\mathbb{F}_{13} + u\mathbb{F}_{13} + v\mathbb{F}_{13} + uv\mathbb{F}_{13}$. Let $B_0 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, $B_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, $B_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ and $B_3 = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ be 2×2 matrices over $\mathbb{F}_{13}$ such that $B = \zeta_0 B_0 + \zeta_1 B_1 + \zeta_2 B_2 + \zeta_3 B_3$. Let $G = [I, B]$ be the generator matrix of $\mathcal{C}$. By Lemma 1, the generator matrix of $\psi(\mathcal{C})$ is as shown in the equation at the bottom of the next page.

We use Magma software to compute [4], we get parameters of the code over $\mathbb{F}_{13}$ is [16, 8, 3].

Example 7: We find the parameters of a Gray image of a DC code over $\mathbb{F}_{19} + u\mathbb{F}_{19} + v\mathbb{F}_{19} + uv\mathbb{F}_{19}$. Let $B_0 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, $B_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, $B_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ and $B_3 = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ be 2×2 matrices over $\mathbb{F}_{19}$ such that $B = \zeta_0 B_0 + \zeta_1 B_1 + \zeta_2 B_2 + \zeta_3 B_3$. Assume that $G = [I, B]$ is the generator matrix of a code $\mathcal{C}$. By Lemma 1, the generator matrix of $\psi(\mathcal{C})$ is the same as the generator matrix of $\psi(\mathcal{C})$ given in Example 6. We use Magma software to compute [4], we get parameters of the code over $\mathbb{F}_{19}$ is [16, 8, 3].

$$M = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 2 & 1 & 2 & 1 & 2 & 1 & 2 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 3 & 4 & 3 & 4 & 3 & 4 & 3 & 4 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & 5 & 6 & -5 & -6 & -5 & -6 & 5 & 6 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & 7 & 8 & -7 & -8 & -7 & -8 & 7 & 8 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & 9 & 10 & 9 & 10 & -9 & 10 & -9 & -10 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & 11 & 12 & 11 & 12 & -11 & -12 & -11 & -12 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & 13 & 14 & -13 & -14 & 13 & 14 & -13 & -14 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & 15 & 16 & -15 & -16 & 15 & 16 & -15 & -16 \end{bmatrix}$$

TABLE 1. Gray images of DC codes over $\mathbb{F}_5 + u\mathbb{F}_5 + v\mathbb{F}_5 + uv\mathbb{F}_5$.

n	$a_1(y)$	$a_2(y)$	$a_3(y)$	$a_4(y)$	Parameter over $\mathbb{F}_5$
1	4	0	2	3	[8 4 4]
2	42	40	42	40	[16 8 4]
2	40	23	24	34	[16 8 5]
2	11	32	40	42	[16 8 4]
3	121	402	131	240	[24 12 7]
4	3242	0334	3242	0334	[32 16 6]
5	02402	03133	24020	31330	[40 20 9]
5	43030	04131	12003	22314	[40 20 10]
6	002402	003133	240200	313300	[48 24 9]
7	2132202	4010044	2132202	4010044	[56 28 8]
8	24002000	31330000	24002000	31330000	[64 32 9]
9	421322021	240100442	421322021	240100442	[72 36 10]

III. SDDC CODES

In this section, we obtain necessary and sufficient conditions for a DC code to be a self-dual code over R. In addition, we give an enumeration of SDDC codes over R.

A. ALGEBRAIC STRUCTURE OF DC CODES

In this subsection, let n be an odd positive integer and q be an odd prime power satisfying $\gcd(n, q) = 1$. The factorization of $t^n - 1$ into irreducible polynomials over R is

$$t^n - 1 = \alpha(t-1)\prod_{i=1}^{s} f_i(t)\prod_{j=1}^{l} k_j(t)k_j^*(t),$$

where

- $\alpha \in R^*$ (R^* is the set of all units of R);
- For each $1 \le i \le s$, $f_i(t)$ is a self reciprocal polynomial of even degree $2e_i$ and
- For each $1 \le j \le l$, $k_j^*(t)$ is a reciprocal polynomial of $k_j(t)$ with degree d_j.

Recall that if $a(t) = a^*(t)$, then $a(t)$ is a self reciprocal polynomial, where $a^*(t) = t^{\deg a}a(t^{-1})$ is the reciprocal polynomial of $a(t)$.

As discussions in [15] and [22], $\frac{R[t]}{\langle t^n-1\rangle} \cong \frac{R[t]}{\langle t-1\rangle} \oplus \left(\oplus_{i=1}^{s}\frac{R[t]}{\langle f_i(t)\rangle}\right) \oplus \left(\oplus_{j=1}^{l}\left(\frac{R[t]}{\langle k_j(t)\rangle} \oplus \frac{R[t]}{\langle k_j^*(t)\rangle}\right)\right) \cong R \oplus \left(\oplus_{i=1}^{s}R_{(2e_i)}\right) \oplus \left(\oplus_{j=1}^{l}(R_{(d_j)} \oplus R_{(d_j)})\right)$, where $R_{(r)} := \mathbb{F}_{q^r} + u\mathbb{F}_{q^r} + v\mathbb{F}_{q^r} + uv\mathbb{F}_{q^r}$ such that $u^2 = u, v^2 = v, uv = vu$. Hence, $\left(\frac{R[t]}{\langle t^n-1\rangle}\right)^2 \cong R^2 \oplus \left(\oplus_{i=1}^{s}\left(R_{(2e_i)}\right)^2\right) \oplus \left(\oplus_{j=1}^{l}\left(R_{(d_j)}\right)^2 \oplus \left(R_{(d_j)}\right)^2\right)$. It implies that the linear code $\mathcal{C}$ over R of length 2 over $\frac{R[t]}{\langle t^n-1\rangle}$ can be expressed as

$$\mathcal{C} \cong \mathcal{C}_0 \oplus \left(\oplus_{i=1}^{s}\mathcal{C}_i\right) \oplus \left(\oplus_{j=1}^{l}(\mathcal{C}_j' \oplus \mathcal{C}_j'')\right), \tag{2}$$

where $\mathcal{C}_0$ is a linear code of length 2 over R, $\mathcal{C}_i$ is a linear code of length 2 over $R_{(2e_i)}$ for each $i = 1, \cdots s$ and $\mathcal{C}_j', \mathcal{C}_j''$ are linear codes of length 2 over $R_{(d_j)}$ for all $1 \le j \le l$. Furthermore, the component codes $\mathcal{C}_0, \mathcal{C}_i$ and $\{\mathcal{C}_j', \mathcal{C}_j''\}$ are called the constituents of $\mathcal{C}$ and their generators are $\beta_0 = (1, c_{e_0})$, $\beta_i = (1, c_{e_i})$, $\beta_j' = (1, c_{d_j}')$ and $\beta_j'' = (1, c_{d_j}'')$, respectively, where $c_{e_0} \in R$, $c_{e_i} \in R_{(2e_i)}$, $c_{d_j}', c_{d_j}'' \in R_{(d_j)}$.

By [16, Theorem 4.2], $\mathcal{C}$ is a SDDC code over R if and only if $\mathcal{C}_0$ is a Euclidean self-dual code, $\mathcal{C}_i$ are Hermitian self-dual codes, for all $1 \le i \le s$, and $\mathcal{C}_j''$ is a Euclidean

$$M = \begin{bmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\
1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & 0 & -1 & 0 & -1 & 0 & 1 & 0 \\
1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & 0 & 1 & 0 & -1 & 0 & -1 & 0 & 1 \\
1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & 0 & 1 & 0 & -1 & 0 & -1 & 0 \\
1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & 0 & 1 & 0 & 1 & 0 & -1 & 0 & -1 \\
1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\
1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & 0 & 1 & 0 & -1 & 0 & 1 & 0 & -1
\end{bmatrix}$$

dual code of $\mathcal{C}'_j$ for all $1 \le j \le l$. Since $\beta_0 = (1, c_{e_0})$, $\beta_i = (1, c_{e_i})$, $\beta'_j = (1, c'_{d_j})$ and $\beta''_j = (1, c''_{d_j})$ are the generators of the codes $\mathcal{C}_0$, $\mathcal{C}_i$, $\mathcal{C}'_j$, and $\mathcal{C}''_j$, $\mathcal{C}$ is a self-dual code if and only if $1 + c^2_{e_0} = 0$, $1 + c^{1+q^{e_i}}_{e_i} = 0$ and $1 + c'_{d_j} c''_{d_j} = 0$. We summarize our discussions above in the following result.

Lemma 2: Let $\mathcal{C} \cong \mathcal{C}_0 \oplus (\oplus_{i=1}^{s} \mathcal{C}_i) \oplus (\oplus_{j=1}^{l} (\mathcal{C}'_j \oplus \mathcal{C}''_j))$ be a DC code over R. We have the generators $\beta_0 = (1, c_{e_0})$, $\beta_i = (1, c_{e_i})$, $\beta'_j = (1, c'_{d_j})$, $\beta''_j = (1, c''_{d_j})$ corresponding to the codes $\mathcal{C}_0$, $\mathcal{C}_i$, $\mathcal{C}'_j$, $\mathcal{C}''_j$ over R, $R_{(2e_i)}$, $R_{(d_j)}$, $R_{(d_j)}$ respectively, for all $1 \le i \le s$, $1 \le j \le l$. Then $\mathcal{C}$ is a self-dual code if and only if the following three equations hold true $1 + c^2_{e_0} = 0$, $1 + c^{1+q^{e_i}}_{e_i} = 0$ and $1 + c'_{d_j} c''_{d_j} = 0$. In particular, the number of SDDC codes over R equals the product of the numbers of solutions of these three equations.

B. ENUMERATION OF DC CODES

By applying Lemma 2, we have the following result.

Theorem 3: Let n be an odd positive integer, q be an odd prime power, and $\gcd(n, q) = 1$. If $t^n - 1$ can be expressed into the irreducible polynomials over R as

$$t^n - 1 = \alpha(t-1) \prod_{i=1}^{s} f_i(t) \prod_{j=1}^{l} k_j(t) k^*_j(t),$$

where $\alpha \in R^*$ and $n = 1 + \sum_{i=1}^{s} 2e_i + 2\sum_{j=1}^{l} d_j$, then the total number of SDDC codes over R is

$$\begin{cases} 2^4 \prod_{i=1}^{s} (q^{e_i} + 1)^4 \prod_{j=1}^{l} (q^{d_j} - 1)^4 \ \text{if } q \equiv 1 \pmod 4 \\ 0 \qquad\qquad\qquad\qquad\qquad\qquad \text{if } q \equiv 3 \pmod 4 \end{cases}$$

Proof: Let $\mathcal{C}$ be a SDDC code over R as specified in Equation (2). We can determine the total number of SDDC codes over R by counting the number of SDDC codes of the constituents $\mathcal{C}_0$, $\mathcal{C}_i$ and $\{\mathcal{C}'_j, \mathcal{C}''_j\}$ of $\mathcal{C}$. By Lemma 2, the number of SDDC codes over R equals to the product of the numbers of solutions of the following three equations

1) $1 + c^2_{e_0} = 0$,
2) $1 + c^{1+q^{e_i}}_{e_i} = 0$, for all $1 \le i \le s$, and
3) $1 + c'_{d_j} c''_{d_j} = 0$ for all $1 \le j \le l$.

We obtain the numbers of solutions of each of the aforementioned three equations separately as follows:

1) For the code $\mathcal{C}_0$ over R, we need to determine the number of solutions of the equation $1 + c^2_{e_0} = 0$. Since $c_{e_0} \in R$, we have $c_{e_0} = a_0\zeta_0 + a_1\zeta_1 + a_2\zeta_2 + a_3\zeta_3$, where $a_j \in \mathbb{F}_q$ and $j = 0, 1, 2, 3$. Substituting the value of c_{e_0} in $1 + c^2_{e_0} = 0$, $1 + (a^2_0\zeta_0 + a^2_1\zeta_1 + a^2_2\zeta_2 + a^2_3\zeta_3) = 0$.

Since $1 = \zeta_0 + \zeta_1 + \zeta_2 + \zeta_3$, we get $a^2_0 = -1$, $a^2_1 = -1$, $a^2_2 = -1$, $a^2_3 = -1$, where $a_j \in \mathbb{F}_q$ and $j = 0, 1, 2, 3$. We have two cases as follows:

Case 1. If $q \equiv 1 \pmod 4$, by Theorem 1, then $\mathbb{F}_q$ contains a square root of -1. Thus, the number of solutions for equation $a^2_j = -1$ is 2 for all $j = 0, 1, 2, 3$. Thus, the total number of solutions such that $1 + c^2_{e_0} = 0$ is 2^4.

Case 2. If $q \equiv 3 \pmod 4$, by Theorem 1, then $\mathbb{F}_q$ does not contains a square root of -1. Thus, $a^2_j = -1$ for all $j = 0, 1, 2, 3$ has no solutions. Hence, the total number of solutions such that $1 + c^2_{e_0} = 0$ is 0.

2) Since $c_{e_i} \in R_{(2e_i)}$,

$$c_{e_i} = b_0\zeta_0 + b_1\zeta_1 + b_2\zeta_2 + b_3\zeta_3,$$

where $b_j \in \mathbb{F}_{q^{2e_i}}$ and $j = 0, 1, 2, 3$. Substituting the value of c_{e_i} in $1 + c^{q^{e_i}+1}_{e_i} = 0$,

$$\begin{aligned} 0 &= 1 + \left(b_0\zeta_0 + b_1\zeta_1 + b_2\zeta_2 + b_3\zeta_3\right)^{q^{e_i}+1} \\ &= 1 + b_0^{q^{e_i}+1}\zeta_0 + b_1^{q^{e_i}+1}\zeta_1 + b_2^{q^{e_i}+1}\zeta_2 + b_3^{q^{e_i}+1}\zeta_3. \end{aligned}$$

It implies that $b_0^{q^{e_i}+1}\zeta_0 + b_1^{q^{e_i}+1}\zeta_1 + b_2^{q^{e_i}+1}\zeta_2 + b_3^{q^{e_i}+1}\zeta_3 = -1 = -\zeta_0 - \zeta_1 - \zeta_2 - \zeta_3$.

Therefore, $b_0^{q^{e_i}+1} = -1$, $b_1^{q^{e_i}+1} = -1, b_2^{q^{e_i}+1} = -1, b_3^{q^{e_i}+1} = -1$ where $b_j \in \mathbb{F}_{q^{2e_i}}$ and $j = 0, 1, 2, 3$.

For $m = 2$, the multiplicative surjective norm function from $\mathbb{F}_{q^{2e_i}}$ to $\mathbb{F}_{q^{e_i}}$ can be calculated as $\mathrm{Norm}(b) = b^{\frac{q^{2e_i}-1}{q^{e_i}-1}} = b^{q^{e_i}+1}$, for $b \in \mathbb{F}^*_{q^{2e_i}}$. We see that $\mathrm{Norm}(b_0) = b_0^{q^{e_i}+1} = -1$, $\mathrm{Norm}(b_1) = b_1^{q^{e_i}+1} = -1$, $\mathrm{Norm}(b_2) = b_2^{q^{e_i}+1} = -1$, $\mathrm{Norm}(b_3) = b_3^{q^{e_i}+1} = -1$. By Proposition 1, each element in $\mathbb{F}^*_{q^{e_i}}$ has a preimage of exactly $\frac{q^{2e_i}-1}{q^{e_i}-1} = q^{e_i} + 1$ elements in $\mathbb{F}^*_{q^{2e_i}}$. Hence, the number of solutions for equation $b_j^{q^{e_i}+1} = -1$ is $q^{e_i} + 1$ for $j = 0, 1, 2, 3$. Thus, for all $i = 2, \ldots s$, the total number of solutions satisfying $1 + c_{e_i} c^{q^{e_i}}_{e_i} = 0$ are $(q^{e_i} + 1)^4$.

3) For $\{\mathcal{C}'_j, \mathcal{C}''_j\}$, where $1 \le j \le l$, we will determine the total number of $\{c'_{d_j}, c''_{d_j}\}$ satisfying $1 + c'_{d_j} c''_{d_j} = 0$. To do that, we consider two cases as follows.

Case 1. If $c'_{d_j} \in R^*_{(d_j)}$, then $c''_{d_j} = -\frac{1}{c'_{d_j}}$. As discussed in the preliminary, the ring $R_{(d_j)}$ has $(q^{d_j} - 1)^4$ units. Thus, for each $j = 1, \ldots, l$, the total number of choices for such pair $\{c'_{d_j}, c''_{d_j}\}$ satisfying $1 + c'_{d_j} c''_{d_j} = 0$ is $(q^{d_j} - 1)^4$.

Case 2. Assume that $c'_{d_j} \in R_{(d_j)} \setminus R^*_{(d_j)}$, and $c'_{d_j} = c_0\zeta_0 + c_1\zeta_1 + c_2\zeta_2 + c_2\zeta_2 + c_3\zeta_3$, where $c_i \in \mathbb{F}_{q^{d_j}}$ for $i = 0, 1, 2, 3$. Put $c''_{d_j} = c'_0\zeta_0 + c'_1\zeta_1 + c'_2\zeta_2 + c'_3\zeta_3 \in R_{(d_j)}$; $c'_i \in \mathbb{F}_{q^{d_j}}$, and $i = 0, 1, 2, 3$. Then

$$\begin{aligned} 1 + c'_{d_j} c''_{d_j} &= 1 + \left(c_0\zeta_0 + c_1\zeta_1 + c_2\zeta_2 + c_3\zeta_3\right)\left(c'_0\zeta_0 \right. \\ &\quad \left. + c'_1\zeta_1 + c'_2\zeta_2 + c'_3\zeta_3\right) \\ &= 1 + c_0c'_0\zeta_0 + c_1c'_1\zeta_1 + c_2c'_2\zeta_2 + c_3c'_3\zeta_3 \\ &= (1 + c_0c'_0)\zeta_0 + (1 + c_1c'_1)\zeta_1 + (1 + \\ &\quad c_2c'_2)\zeta_2 + (1 + c_3c'_3)\zeta_3. \end{aligned}$$

From $1 + c'_{d_j} c''_{d_j} = 0$, we have $(1 + c_0 c'_0)\zeta_0 + (1 + c_1 c'_1)\zeta_1 + (1 + c_2 c'_2)\zeta_2 + (1 + c_3 c'_3)\zeta_3 = 0$. It implies that

$$c_0 c'_0 = -1,\ c_1 c'_1 = -1,\ c_2 c'_2 = -1,\ , c_3 c'_3 = -1. \quad (3)$$

We see that c'_{d_j} is a unit of $R_{(d_j)}$ if and only if c_i are nonzero elements of $\mathbb{F}_{q^{d_j}}$ for $i = 0, 1, 2, 3$. Since $c'_{d_j} \in R_{(d_j)} \backslash R^*_{(d_j)}$, $c_i = 0$, for some $i = 0, 1, 2, 3$. This is a contradiction with (3).

Consequently, by combining (1), (2) and (3), the total number of SDDC codes over R is

$$2^4 \prod_{i=1}^{s} (q^{e_i} + 1)^4 \prod_{j=1}^{l} (q^{d_j} - 1)^4.$$

□

Example 8: We consider $R = \mathbb{F}_5 + u\mathbb{F}_5 + v\mathbb{F}_5 + uv\mathbb{F}_5$, and $n = 3$. Then $\gcd(3, 5) = 1$ and the factorization of $t^3 - 1$ into irreducible polynomials over $\mathbb{F}_5$ is

$$t^3 - 1 = (t - 1)(t^2 + t + 1).$$

We see that the self-reciprocal polynomial is t^2+t+1. Hence, $e_1 = 1$ and $d_1 = 0$. Thus, $n = 1+\sum_{i=1}^{1} 2e_i+2\sum_{j=1}^{1} d_j$ $(3 = 1 + (2 \times 1) + 2 \times (0))$. By Theorem 3, the total number of SDDC codes over $\mathbb{F}_5 + u\mathbb{F}_5 + v\mathbb{F}_5 + uv\mathbb{F}_5$ is $2^4 \prod_{i=1}^{1}(5^{e_i} + 1)^4 \prod_{j=1}^{1}(5^{d_j} - 1)^4 = 2^4(5^1 + 1)^4(5^0 - 1)^4 = 0$.

Example 9: We consider $R = \mathbb{F}_5 + u\mathbb{F}_5 + v\mathbb{F}_5 + uv\mathbb{F}_5$ and $n = 39$. Hence, $\gcd(39, 5) = 1$ and the factorization of $t^{39} - 1$ into irreducible polynomials over $\mathbb{F}_5$ is $t^{39} - 1 = (t - 1)(t^2 + t + 1)(t^4 + 3t^3 + 3t + 1)(t^4 + t^3 + 4t^2 + t + 1)(t^4+4t^3+t^2+1)(t^4+2t^3+t^2+2t+1)(t^4+t^2+4t+1)(t^4+2t^3+3t^2+t+1)(t^4+2t^2+2t+1)(t^4+2t^3+2t^2+1)(t^4+t^3+3t^2 + 2t + 1)$. We see that four self-reciprocal polynomials are $t^2+t+1, t^4+t^3+4t^2+t+1, t^4+2t^3+t^2+2t+1$ and $t^4 + 3t^3 + 3t + 1$. Hence, $e_1 = 1$ and $e_2 = e_3 = e_4 = 2$.

The reciprocal polynomials of $t^4 + t^2 + 4t + 1, t^4 + 2t^2 + 2t + 1$ and $t^4 + t^3 + 3t^2 + 2t + 1$ are $t^4 + 4t^3 + t^2 + 1, t^4 + 2t^3 + 2ty^2 + 1$ and $t^4 + 2t^3 + 3t^2 + t + 1$, respectively. Thus, $d_1 = d_2 = d_3 = 4$. Hence,

$$n = 1 + \sum_{i=1}^{4} 2e_i + 2\sum_{j=1}^{3} d_j$$
$$39 = 1 + (2 \times 1 + 2 \times 2 + 2 \times 2 + 2 \times 2) + 2 \times (4 + 4 + 4).$$

By Theorem 3, the total number of SDDC codes over $\mathbb{F}_5 + u\mathbb{F}_5 + v\mathbb{F}_5 + uv\mathbb{F}_5$ is $2^4 \prod_{i=1}^{4}(5^{e_i} + 1)^4 \prod_{j=1}^{3}(5^{d_j} - 1)^4 = 2^4(5^1 + 1)^4(5^2 + 1)^{12}(5^4 - 1)^{12}$.

Example 10: We consider $R = \mathbb{F}_7 + u\mathbb{F}_7 + v\mathbb{F}_7 + uv\mathbb{F}_7$ and $n = 9$. Then $\gcd(9, 7) = 1$ and the factorization of $t^9 - 1$ into irreducible polynomials over $\mathbb{F}_7$ is

$$t^9 - 1 = (t - 1)(t + 3)(t + 5)(t^3 + 3)(t^3 + 5).$$

The reciprocal factors are $(t + 3)^* = 3t + 1 = 3(t + 5)$, $(t+5)^* = 5t+1 = 5(t+3)$, $(t^3+3)^* = 3t^3+1 = 3(t^3+5)$ and $(t^3 + 5)^* = 5t^3 + 1 = 5(t^3 + 3)$. Therefore, there is no self-reciprocal polynomial. Hence, $e_1 = 0$. The reciprocal polynomials of $t + 3$ and $t^3 + 3$ are $3(t + 5)$ and $3(t^3 + 5)$. Thus, $d_1 = 1$ and $d_2 = 3$. Thus,

$$n = 1 + \sum_{i=0}^{0} 2e_i + 2\sum_{j=1}^{2} d_j$$
$$9 = 1 + (2 \times 0) + 2 \times (1 + 3).$$

By Theorem 3, the total number of SDDC codes over $\mathbb{F}_7 + u\mathbb{F}_7 + v\mathbb{F}_7 + uv\mathbb{F}_7$ is 0. Note that if $q \equiv 3 \pmod 4$, then any odd integers n with $\gcd(n, q) = 1$. By Theorem 3, the total number of SDDC codes over R is 0.

Example 11: We consider $R = \mathbb{F}_{13} + u\mathbb{F}_{13} + v\mathbb{F}_{13} + uv\mathbb{F}_{13}$ and $n = 15$. Then $\gcd(15, 13) = 1$ and the factorization of $t^{15} - 1$ into irreducible polynomials over $\mathbb{F}_{13}$ is $t^{15} - 1 = 12(t - 1)(t^4 + t^3 + t^2 + t + 1)(10t + 1)(t + 10)(9t^4 + t^3 + 3t^2 + 9t + 1)(t^4 + 9t^3 + 3t^2 + t + 9)$. It is easy to verify that $t^4 + t^3 + t^2 + t + 1$ is a self-reciprocal polynomial. Thus, $e_1 = 2$. We also see that the reciprocal polynomials of $10t + 1$ and $9t^4+t^3+3t^2+9t+1$ are $t+10$ and $t^4+9t^3+3t^2+t+9$. Hence, $d_1 = 1 = d_2 = 4$. Thus,

$$n = 1 + \sum_{i=1}^{1} 2e_i + 2\sum_{j=1}^{2} d_j$$
$$15 = 1 + (2 \times 2) + 2 \times (1 + 4).$$

By Theorem 3, the total number of SDDC codes over $\mathbb{F}_{13} + u\mathbb{F}_{13} + v\mathbb{F}_{13} + uv\mathbb{F}_{13}$ is $2^4 \prod_{i=1}^{1}(13^{e_i} + 1)^4 \prod_{j=1}^{2}(13^{d_j} - 1)^4 = 2^4(13^1 + 1)^4(13^1 - 1)^4(13^4 - 1)^4$.

Example 12: We consider $R = \mathbb{F}_{25} + u\mathbb{F}_{25} + v\mathbb{F}_{25} + uv\mathbb{F}_{25}$ and $n = 21$. Then $\gcd(21, 25) = 1$ and the factorization of $t^{21} - 1$ into irreducible polynomials over $\mathbb{F}_{25} = \frac{\mathbb{F}_5[w]}{\langle w^2+4w+2\rangle}$ is $t^{21} - 1 = w^4(t - 1)(t^3 + 4w^9t^2 + 4w^9t + 1)(t^3 + 4w^{21}t^2 + 4w^{21}t + 1)(w^{20}t^2 + 1)(t^2 + w^{20})\ (t^3 + 4wt^2 + 4w^{17}t + 1)(t^3 + 4w^5t^2 + 4w^{13}t + 1)(t^3 + 4w^{13}t^2 + 4w^5t + 1)\ (t^3 + 4w^{17}t^2 + 4wt + 1)$. We see that two polynomials $t^3 + 4w^9t^2 + 4w^9t + 1$ and $t^3 + 4w^{21}t^2 + 4w^{21}t + 1$ are self-reciprocal. Thus, $e_1 = e_2 = \frac{3}{2}$. The reciprocal polynomials of $w^{20}t^2 + 1, t^3 + 4wt^2 + 4w^{17}t + 1$ and $t^3 + 4w^5t^2 + 4w^{13}t + 1$ are $t^2 + w^{20}, t^3 + 4w^{17}t^2 + 4wt + 1$ and $t^3 + 4w^{13}t^2 + 4w^5t + 1$, respectively. It implies that $d_1 = d_2 = d_3 = 3$. Thus,

$$n = 1 + \sum_{i=1}^{2} 2e_i + 2\sum_{j=1}^{3} d_j$$
$$21 = 1 + (2 \times \frac{3}{2} + 2 \times \frac{3}{2}) + 2 \times (3 + 3 + 3).$$

By Theorem 3, the total number of SDDC codes over $\mathbb{F}_{25} + u\mathbb{F}_{25} + v\mathbb{F}_{25} + uv\mathbb{F}_{25}$ is $2^4 \prod_{i=1}^{2}(25^{e_i} + 1)^4 \prod_{j=1}^{3}(25^{d_j} - 1)^4 = 2^4(25^{\frac{3}{2}} + 1)^8(25^3 - 1)^{12}$.

IV. DISTANCE BOUNDS FOR SDDC CODES

In this section, we study the distance bound of SDDC codes. Furthermore, we prove that the family of Gray images of SDDC codes is asymptotically good.

Let n be an odd prime and q be a primitive modulo n $(q^{n-1} \equiv 1 \pmod n)$, but $q^k \not\equiv 1 \pmod n$ for all positive

integers $k < n-1$), i.e., $O_n(q) = n-1$. Using Proposition 2 for $p = n, m = 1, f = \frac{p-1}{e} = \frac{n-1}{1}$. Then the number of distinct q-cyclotomic cosets modulo n is $1 * 1 + 1 = 2$.

Recall that n is a positive integer with $\gcd(n, q) = 1$. Then the number of monic irreducible factors of $y^n - 1$ over $\mathbb{F}_q$ equals to the number of cyclotomic cosets of q modulo n (see [17, Corollary 3.4.12]).

By the above discussions, the factorization of $t^n - 1$ into two distinct irreducible polynomials over $\mathbb{F}_q$ is

$$t^n - 1 = (t-1)(1 + t + t^2 + \cdots + t^{n-1}) = (t-1)h(t), \tag{4}$$

where $h(t) = 1 + t + t^2 + \cdots + t^{n-1}$ is an irreducible polynomial over $\mathbb{F}_q$. Now we proceed to show that $h(t)$ is also irreducible over R.

Let $\zeta_0 = (1 - u - v + uv)$, $\zeta_1 = (uv)$, $\zeta_2 = (u - uv)$ and $\zeta_3 = (v - uv)$. We have $\zeta_0 + \zeta_1 + \zeta_2 + \zeta_3 = 1$, $\zeta_i^2 = \zeta_i$ and $\zeta_i\zeta_j = 0$ where $i, j = 0, 1, 2, 3$ and $i \neq j$. Then $\{\zeta_0, \zeta_1, \zeta_2, \zeta_3\}$ forms a nonzero pairwise orthogonal idempotent set of R. By the CRT, $R \cong \zeta_0\mathbb{F}_q \oplus \zeta_1\mathbb{F}_q \oplus \zeta_2\mathbb{F}_q \oplus \zeta_3\mathbb{F}_q$. Assume that $h(t)$ is reducible over R, i.e., $h(t)$ can be presented as a product $h(t) = h_1(t)h_2(t)$, with $h_1(t) = \zeta_0 f_0(t) + \zeta_1 f_1(t) + \zeta_2 f_2(t) + \zeta_3 f_3(t)$ and $h_2(t) = \zeta_0 f_0'(t) + \zeta_1 f_1'(t) + \zeta_2 f_2'(t) + \zeta_3 f_3'(t)$ from $R[t]$ are non-unit, $f_i(t), f_i'(t) \in \mathbb{F}_q[t]$ for $i = 0, 1, 2, 3$. We have

$$\begin{aligned} h(t) &= \zeta_0 f_0(t) f_0'(t) + \zeta_1 f_1(t) f_1'(t) + \zeta_2 f_2(t) f_2'(t) + \\ &\quad \zeta_3 f_3(t) f_3'(t) \\ &= (1 - u - v + uv) f_0(t) f_0'(t) + (uv) f_1(t) f_1'(t) + \\ &\quad (u - uv) f_2(t) f_2'(t) + (v - uv) f_3(t) f_3'(t) \\ &= f_0(t) f_0'(t) + u(f_1(t) f_1'(t) - f_0(t) f_0'(t)) + \\ &\quad v(f_3(t) f_3'(t) - f_0(t) f_0'(t)) + uv(f_0(x) f_0'(t) + \\ &\quad f_1(t) f_1'(t) - f_2(t) f_2'(t) - f_3(t) f_3'(t)). \end{aligned} \tag{5}$$

Comparing $h(t)$ from (4) and (5), $f_0(t)f_0'(t) = f_1(t)f_1'(t) = f_2(t)f_2'(t) = f_3(t)f_3'(t)$. By using $\zeta_0 + \zeta_1 + \zeta_2 + \zeta_3 = 1$, $h(t) = h_1(t)h_2(t) = f_0(t)f_0'(t)$, where $f_0(t), f_0'(t) \in \mathbb{F}_q[t]$. This contradicts the fact that $h(t)$ is irreducible over $\mathbb{F}_q$. Therefore, $h(t)$ is also irreducible over R.

Let n be an odd prime and q be a primitive root modulo n. By the above discussions, the factorization $t^n - 1$ into distinct irreducible polynomial over R is

$$t^n - 1 = (t-1)(1 + t + t^2 + \cdots + t^{n-1}) = (t-1)h(t), \tag{6}$$

where $h(t) = 1 + t + t^2 + \cdots + t^{n-1}$ is an irreducible polynomial over R. Using the discussions in [15] and [22], and by the CRT, we obtain

$$\frac{R[t]}{\langle t^n - 1\rangle} \cong \frac{R[t]}{\langle t-1\rangle} \oplus \frac{R[t]}{\langle h(t)\rangle} \cong R \oplus R_{(n-1)},$$

where $R_{(n-1)} = \mathbb{F}_{q^{n-1}} + u\mathbb{F}_{q^{n-1}} + v\mathbb{F}_{q^{n-1}} + uv\mathbb{F}_{q^{n-1}}$ such that $u^2 = u$, $v^2 = v$, $uv = vu$.

The cyclic code $\mathcal{C} = \langle t^{n-1} + t^{n-2} + \cdots + 1\rangle$ is just the code consisting of multiple of all-one vector. Then $0 \neq c \in \mathcal{C}$ is a constant vector. Let $0 \neq z = (e, g) \in R^{2n}$ be an element such that e is not a constant. By the CRT, $z = (e, g) \cong (e_1, g_1) \oplus (e_2, g_2)$. Assume that $z \in \mathcal{C}_a$. Then $g = ea$, $g_1 = e_1a_1$ and $g_2 = e_2a_2$, where $e_1, g_1, a_1 \in R$ and $e_2, g_2, a_2 \in R_{(n-1)}$. We consider $a_1 = r_0\zeta_0 + r_1\zeta_1 + r_2\zeta_2 + r_3\zeta_3$, for $r_i \in \mathbb{F}_q$, and $a_2 = r_0'\zeta_0 + r_1'\zeta_1 + r_2'\zeta_2 + r_3'\zeta_3$, for $r_i' \in \mathbb{F}_{q^{n-1}}$, $i = 0, 1, 2, 3$.

For the first constituent of the code $\mathcal{C}_a$, by Theorem 3, $\mathcal{C}_0$ has at most 2^4 choices.

For the second constituent of $\mathcal{C}_a$, we need to determine the choices for a_2 through e_2. Recall that $g_2 = e_2a_2$ and $a_2 = r_0'\zeta_0 + r_1'\zeta_1 + r_2'\zeta_2 + r_3'\zeta_3$, where $e_2, g_2, a_2 \in R_{(n-1)}$ and $r_i' \in \mathbb{F}_{q^{n-1}}$, for $i = 0, 1, 2, 3$. If $e_2 \in R^*$, then $a_2 = \frac{g_2}{e_2}$ has unique choice for a_2. If $e_2 = 0$, then e is a constant vector. Thus, choices for e are not possible. If $e_2 \neq 0$ and $e_2 \in \langle\zeta_0\rangle$, then for some $t_0 \in \mathbb{F}_{q^{n-1}}^*$ and $t_0' \in \mathbb{F}_{q^{n-1}}$, $e_2 = \zeta_0 t_0$ and $g_2 = \zeta_0 t_0'$. Then $g_2 = e_2a_2 = \zeta_0 t_0 a_2 = \zeta_0 t_0 r_0'$. Hence, $\zeta_0 t_0' = \zeta_0 t_0 r_0'$. It shows that $r_0' = \frac{y_0'}{t_0}$. Since $\mathcal{C}_a$ is self-dual, $1 + a_2\bar{a}_2 = 1 + a_2 a_2^{q^{\frac{n-1}{2}}} = 0$. Substituting a_2 in the above equation, and following a similar proof process as Theorem 3, $r_0' r_0'^{q^{\frac{n-1}{2}}} = -1$, $r_1' r_1'^{q^{\frac{n-1}{2}}} = -1$, $r_2' r_2'^{q^{\frac{n-1}{2}}} = -1$, , $r_3' r_3'^{q^{\frac{n-1}{2}}} = -1$. Hence, $\mathrm{Norm}(r_0') = -1$, $\mathrm{Norm}(r_1') = -1$, $\mathrm{Norm}(r_2') = -1$, $\mathrm{Norm}(r_3') = -1$. Thus, there are $(1 + q^{\frac{n-1}{2}})^3$ choices for a_2.

Similarly, if $0 \neq e_2 \in C$, where C is generated by ℓ idempotent elements, then a_2 has $(1 + q^{\frac{n-1}{2}})^{4-\ell}$ choices for each $\ell = 1, 2, 3, 4$. It is easy to verify that the a_2 has at most $(1 + q^{\frac{n-1}{2}})^3$ choices. Finally, combining both constituent's number of choices, for $z \in \mathcal{C}_a$, a has at most $2^4(1 + q^{\frac{n-1}{2}})^3$ choices. We have the following proposition.

Proposition 3: Let $0 \neq z = (e, g) \in R^{2n}$, where e is not a constant. Then there are at most $2^4(1+q^{\frac{n-1}{2}})^3$ self-dual codes $\mathcal{C}_a = (1, a)$ satisfying $z \in \mathcal{C}_a$ and $a \in R_{(n-1)}$.

Example 13: We verify that there are no more than $2^4(6)^3$ self-dual codes $\mathcal{C}_a = (1, a)$ satisfying $z \in \mathcal{C}_a$, where $z = (e, g) \in R^6$ be a nonzero element, e is not a constant and $a \in R_{(2)}$. In this situation, $n = 3$ and $q = 5$, we can see $\gcd(3, 5) = 1$. By Proposition 3, there are at most $2^4(6)^3$ SDDC codes, and by Example 8, the total number of SDDC codes over $\mathbb{F}_5 + u\mathbb{F}_5 + v\mathbb{F}_5 + uv\mathbb{F}_5$ is $2^4(6)^3$.

Example 14: We find the value of q and n such that $(k + 1)^4(k + 5)^3$ are at most SDDC codes, where $0 < k \in \mathbb{Z}$. If $(k + 1)^4(k + 5)^3$ are most SDDC codes, by Proposition 3, then it should at least equal to $2^4(1 + q^{\frac{n-1}{2}})^3$, where n is an odd prime and q is a primitive modulo n with $\gcd(n, q) = 1$. Therefore, $(k + 1)^4(k + 5)^3 = 2^4(1 + q^{\frac{n-1}{2}})^3$. We can write it as $(k + 1)^4(1 + (k + 4)^1)^3 = 2^4(1 + q^{\frac{n-1}{2}})^3$. Thus, $k + 1 = 2$, $k + 4 = q$ and $1 = \frac{n-1}{2}$. Hence, we get $k = 1$, $q = 5$ and $n = 3$.

The conjecture proposed by Artin regarding primitive roots states that there exist an infinite number of prime numbers n satisfying q is a primitive root modulo n and q is neither

a perfect square nor -1. Assuming the validity of Artin's conjecture on primitive roots, we can deduce that there is an endless series of prime numbers n satisfying q is a primitive root modulo n for a fixed value that is not a square. By factoring $y^n - 1$ into a product of two irreducible factors, we are able to generate an infinite family of DC codes over R.

It is well-known from [12, Lemma 2.10.3] that the $h_q(x)$ quantity (1) is crucial for estimating the volume of high-dimensional Hamming balls over $\mathbb{F}_q$. If n goes to infinity and $0 < x < 1$, the volume of the Hamming ball with radius xn is asymptotically equivalent to $q^{nh_q(x)}$. Denote the size of the families of codes as D_n. By Theorem 3, D_n is asymptotically equivalent to $2^4q^{2(n-1)}$ for SDDC codes when n is tending to infinity. Let $\gamma \in R^{2n}$ such that $w_H(\psi(\gamma)) \leq d_n$ (*). Denote $\beta(d_n)$ contains all γ satisfying (*). Assume that $D_n > \alpha_n\beta(d_n)$, where $\alpha_n = 2^4q^{3(\frac{n-1}{2})}$ and d_n is the largest value satisfying $D_n > \alpha_n\beta(d_n)$. Hence, there exists a family of codes $\mathcal{C}_i$ where $\mathcal{C}_i$ are codes of length $2n$ over R such that $w_H(\psi(\mathcal{C}_i)) \leq d_n$. Let δ be the relative distance of the family of codes $\mathcal{C}_i$ above. Let $d_n \sim 8n\delta_0$, for some δ_0. By [12, Lemma 2.10.3], $\beta(d_n)$ is approximately equal to $q^{8nh_q(\delta_0)}$. By using an entropy estimate $h_q(\delta_0) = \frac{1}{16}$ for SDDC codes, $D_n \sim \alpha_n\beta(d_n)$ holds for n large enough. By definition of δ, $\delta \geq \delta_0$ which is equal to $h_q^{-1}(\frac{1}{16})$ for self-dual codes. Hence, if $h_q(\delta) \geq \frac{1}{16}$ for SDDC codes, $D_n > \alpha_n\beta(d_n)$ holds when n is large enough. Finally, we see that $\rho\delta > 0$, and hence, both of the aforementioned families of codes are asymptotically good.

For a family of asymptotically good SDDC codes, we need to find a sequence of SDDC codes in the family of SDDC codes such that ρ and δ are finite. According to this Artin's conjecture on primitive roots, there are an infinite number of prime numbers n satisfying q is a primitive root modulo n for a fixed value that is not a square. As discussed in [5], we factor $t^n - 1$ into a product of two irreducible factors. As a result, over R, we have an infinite family of DC codes. Since the parameters for DC codes are [2n, n] [12], their rates are $\frac{1}{2}$. Moreover, by above discussion, relative distance of the family of SDDC codes is $0 < h_q^{-1}(\frac{1}{16}) \leq 1 - \frac{1}{q}$. Hence we see that ρ and δ are finite. So we have $\rho\delta > 0$.

We summarize our discussions above in the following theorem.

Theorem 4: Let n be an odd prime and q be a primitive root modulo n, where $n > q$. The family of Gray images of SDDC codes over R of length $2n$ with relative distance δ and rate $\frac{1}{2}$ satisfies $h_q(\delta) \geq \frac{1}{16}$. Then the families of SDDC codes under the Gray map are asymptotically good.

Example 15: We will calculate the entropy value $h_5(\delta_0)$ for a set of SDDC codes with a length $2n$ over $\mathbb{F}_5 + u\mathbb{F}_5 + v\mathbb{F}_5 + uv\mathbb{F}_5$ where the code has a rate of $\frac{1}{2}$. This calculation is performed for a given $\delta > 0$,, which represents the relative Hamming distance between Gray images of the codes over $\mathbb{F}_5$ with $\delta \geq \delta_0$. Then the family of codes is asymptotically good.

Let $q = 5$. By using Artin's conjecture on primitive roots, if 5 is not a square, then there are infinitely many prime n satisfying 5 is a primitive root modulo n. In this case, $x^n - 1$ has two irreducible factors. Thus, an infinite family of DC codes over $\mathbb{F}_5 + u\mathbb{F}_5 + v\mathbb{F}_5 + uv\mathbb{F}_5$ is determined.

To find $h_5(\delta_0)$, suppose that

$$D_n > \alpha_n\beta(d_n), \tag{7}$$

where $D_n, \alpha_n, d_n, \beta(d_n)$ are defined in summarize our discussion of Theorem 4. We see that $D_n \sim 2^45^{2(n-1)}$, $\alpha_n = 2^45^{3(\frac{n-1}{2})}$, $d_n \sim 8n\delta_0$ and $\beta(d_n) \sim 5^{8nh_5(\delta_0)}$. Thus, to enforce the inequality (7) for large n,

$$\begin{aligned} D_n &\sim \alpha_n\beta(d_n) \\ 2^45^{2(n-1)} &\sim 2^45^{3(\frac{n-1}{2})}5^{8nh_5(\delta_0)} \\ 8nh_5(\delta_0) &\sim \frac{n-1}{2} \\ h_5(\delta_0) &\sim \frac{n-1}{16n} \sim \frac{1}{16}. \end{aligned}$$

Hence, by Theorem 4, the family of Gray images of SDDC codes over $\mathbb{F}_5 + u\mathbb{F}_5 + v\mathbb{F}_5 + uv\mathbb{F}_5$ of length $2n$, of relative distance δ and rate $\frac{1}{2}$ such that $h_5(\delta) \geq \frac{1}{16}$ is asymptotically good.

Example 16: For a given $\delta > 0$, considering a family of SDDC codes of length $2n$ over $\mathbb{F}_{17} + u\mathbb{F}_{17} + v\mathbb{F}_{17} + uv\mathbb{F}_{17}$. We denote the entropy value of this family as $h_{17}(\delta_0)$, where δ_0 represents a relative Hamming distance of Gray images of these codes over $\mathbb{F}_{17}$, with $\delta \geq \delta_0$. Furthermore, we demonstrate that this family of codes exhibits asymptotically good properties. Assuming $q = 17$, Artin's conjecture on primitive roots states that if 17 is not a square, there exist infinitely many prime values of n for which 17 is a primitive root modulo n. In such cases, the polynomial x^n-1 can be factored into two irreducible factors. Thus, we obtain an infinite family of DC codes.

To find $h_{17}(\delta_0)$, we assume that

$$D_n > \alpha_n\beta(d_n), \tag{8}$$

where $D_n, \alpha_n, d_n, \beta(d_n)$ are defined in summarize our discussion of Theorem 4. We have $D_n \sim 2^417^{2(n-1)}$, $\alpha_n = 2^417^{3(\frac{n-1}{2})}$, $d_n \sim 8n\delta_0$ and $\beta(d_n) \sim 17^{8nh_{17}(\delta_0)}$. Therefore, for large n, to enforce the inequality (8), we get

$$\begin{aligned} D_n &\sim \alpha_n\beta(d_n) \\ 2^417^{2(n-1)} &\sim 2^417^{3(\frac{n-1}{2})}17^{8nh_{17}(\delta_0)} \\ 8nh_{17}(\delta_0) &\sim \frac{n-1}{2} \\ h_{17}(\delta_0) &\sim \frac{n-1}{16n} \sim \frac{1}{16}. \end{aligned}$$

Hence, by Theorem 4, the family of Gray images of SDDC codes over $\mathbb{F}_{17} + u\mathbb{F}_{17} + v\mathbb{F}_{17} + uv\mathbb{F}_{17}$ of length $2n$, of relative distance δ and rate $\frac{1}{2}$, satisfies $h_{17}(\delta) \geq \frac{1}{16}$ is asymptotically good.

Example 17: Consider the binary repetition code $C = \{(0,0\ldots0),(1,1\ldots1)\}$. It is easy to see that $[n,k,d] = [n,1,n]$. When $n \to \infty$, we have

1) rate $\rho = \lim_{n\to\infty} \sup \frac{k}{n} = \lim_{n\to\infty} \sup \frac{1}{n} = 0$
2) relative distance $\delta = \lim_{n\to\infty} \inf \frac{d}{n} = \lim_{n\to\infty} \inf \frac{n}{n} = 1$.

This code has the largest possible relative distance. It has excellent error-correcting potential. However, this is achieved at the cost of very low efficiency, as reflected in the low information rate.

Example 18: In this example, we aim to compute the entropy value $h_{25}(\delta 0)$ for a set of SDDC codes with a length of $2n$ over the field $\mathbb{F}_{25}+u\mathbb{F}_{25}+v\mathbb{F}_{25}+uv\mathbb{F}_{25}$. These codes have a rate of $\frac{1}{2}$, given a parameter $\delta > 0$, which represents the relative Hamming distance of Gray images for this code family over $\mathbb{F}_{25}$, with $\delta \geq \delta_0$. Additionally, we will demonstrate that this code family is asymptotically good. Let's assume that $q = 25$. According to Artin's conjecture on primitive roots, if 25 is not a square, then there exist infinitely many prime numbers n for which 25 is a primitive root modulo n. In such cases, the polynomial $x^n - 1$ can be factored into two irreducible factors. Consequently, we obtain an infinite family of DC codes over the field $\mathbb{F}_{25}+u\mathbb{F}_{25}+v\mathbb{F}_{25}+uv\mathbb{F}_{25}$.

To find $h_{25}(\delta_0)$, we assume that

$$D_n > \alpha_n \beta(d_n), \tag{9}$$

where $D_n, \alpha_n, d_n, \beta(d_n)$ are defined in summarize our discussion of Theorem 4. We have $D_n \sim 2^4 25^{2(n-1)}$, $\alpha_n = 2^4 25^{3(\frac{n-1}{2})}$, $d_n \sim 8n\delta_0$ and $\beta(d_n) \sim 17^{8nh_{25}(\delta_0)}$. Thus, to enforce the inequality (9) for large n, we get

$$\begin{aligned} D_n &\sim \alpha_n \beta(d_n) \\ 2^4 25^{2(n-1)} &\sim 2^4 25^{3(\frac{n-1}{2})} 25^{8nh_{25}(\delta_0)} \\ 8nh_{25}(\delta_0) &\sim \frac{n-1}{2} \\ h_{25}(\delta_0) &\sim \frac{n-1}{16n} \sim \frac{1}{16}. \end{aligned}$$

Hence, by Theorem 4, the family of Gray images of SDDC codes over $\mathbb{F}_{25}+u\mathbb{F}_{25}+v\mathbb{F}_{25}+uv\mathbb{F}_{25}$ of length $2n$, of relative distance δ and rate $\frac{1}{2}$, satisfies $h_{25}(\delta) \geq \frac{1}{16}$. This demonstrates that it is asymptotically good.

Example 19: Consider the q-ary code $C = \mathbb{F}_q^n$. It is easy to see that $[n,k,d] = [n,n,1]$. Hence,

1) rate $\rho = \lim_{n\to\infty} \sup \frac{k}{n} = \lim_{n\to\infty} \sup \frac{n}{n} = 1$
2) relative distance $\delta = \lim_{n\to\infty} \inf \frac{d}{n} = \lim_{n\to\infty} \inf \frac{1}{n} = 0$

This code achieves the highest achievable information rate, but it has a minimal relative distance of 0. The minimum distance of a code is closely associated with its ability to correct errors, so a low relative minimum distance indicates a comparatively limited error-correcting capability.

V. SELF-DUAL AND LCD DN CODES

In this section, we present the essential criteria for a DN code to be both self-dual and an LCD code over R. Moreover, we provide an enumeration of SDDN codes and LCD DN codes over R.

A. ALGEBRAIC STRUCTURE OF DN CODES

In this subsection, we discuss SDDN codes and LCD DN codes structures over R. Let n be an even positive integer and q a prime power such that $\gcd(n,q) = 1$. The factorization of $t^n + 1$ into distinct irreducible polynomials over R is

$$t^n + 1 = \alpha \prod_{i=1}^{s} f_i(t) \prod_{j=1}^{l} k_j(t) k_j^*(t),$$

where

- $\alpha \in R^*$,
- $f_i(t)$ is a self reciprocal polynomial of even degree $2e_i$ for all $1 \leq i \leq s$; and
- $k_j^*(t)$, is the reciprocal polynomial of $k_j(t)$ with degree d_j for each $1 \leq j \leq l$.

Using the CRT, we obtain

$$\begin{aligned} \frac{R[t]}{\langle t^n+1\rangle} &\cong \left(\oplus_{i=1}^{s} \frac{R[t]}{\langle f_i(t)\rangle}\right) \oplus \\ &\left(\oplus_{j=1}^{l} \left(\frac{R[t]}{\langle k_j(t)\rangle} \oplus \frac{R[t]}{\langle k_j^*(t)\rangle}\right)\right) \\ &\cong \left(\oplus_{i=1}^{s} R_{(2e_i)}\right) \oplus \left(\oplus_{j=1}^{l} \left(R_{(d_j)} \oplus R_{(d_j)}\right)\right), \end{aligned}$$

where $R_{(r)} := \mathbb{F}_{q^r} + u\mathbb{F}_{q^r} + v\mathbb{F}_{q^r} + uv\mathbb{F}_{q^r}$ such that $u^2 = u$, $v^2 = v$, $uv = vu$. Extending the above decomposition, we see that $\left(\frac{R[t]}{\langle y^n-1\rangle}\right)^2 \cong \left(\oplus_{i=1}^{s} \left(R_{(2e_i)}\right)^2\right) \oplus \left(\oplus_{j=1}^{l} \left(\left(R_{(d_j)}\right)^2 \oplus \left(R_{(d_j)}\right)^2\right)\right)$. Hence, a linear code $\mathcal{C}$ over R of length 2 can be expressed as follows

$$\mathcal{C} \cong \left(\oplus_{i=1}^{s} \mathcal{C}_i\right) \oplus \left(\oplus_{j=1}^{l} (\mathcal{C}_j' \oplus \mathcal{C}_j'')\right), \tag{10}$$

where $\mathcal{C}_i$ is a linear code of length 2 over $R_{(2e_i)}$, $\mathcal{C}_j'$ is a linear code of length 2 over $R_{(d_j)}$ and $\mathcal{C}_j''$ is a linear code of length 2 over $R_{(d_j)}$, for all $1 \leq i \leq s$ and $1 \leq j \leq l$. Moreover, the component codes $\mathcal{C}_i$ and $\{\mathcal{C}_j', \mathcal{C}_j''\}$ are called the constituents of $\mathcal{C}$.

Let $\mathcal{C} \cong \left(\oplus_{i=1}^{s} \mathcal{C}_i\right) \oplus \left(\oplus_{j=1}^{l} (\mathcal{C}_j' \oplus \mathcal{C}_j'')\right)$ be a DN code over R. By applying Lemma 2, $\mathcal{C}$ is a self-dual code if and only if $1 + c_{e_i}^{1+q^{e_i}} = 0$ and $1 + c_{d_j}' c_{d_j}'' = 0$ for all $1 \leq i \leq s$ and $1 \leq j \leq l$. By [8, Theorem 3.1], $\mathcal{C}$ is an LCD code if and only if $\mathcal{C}_i$ are LCD codes with respect to the Hermitian inner product over $R_{(2e_i)}$ for all $1 \leq i \leq s$, and $\mathcal{C}_j'' \cap (\mathcal{C}_j')^{\perp} = \{0\}$ and $\mathcal{C}_j' \cap (\mathcal{C}_j'')^{\perp} = \{0\}$, for all $1 \leq j \leq l$. Then using the given generators, the above LCD condition implies that $\mathcal{C}$ is an LCD code if and only if $1 + c_{e_i}^{1+q^{e_i}} \in R_{(2e_i)}^*$ and $1 + c_{d_j}' c_{d_j}'' \in R_{(d_j)}^*$, where $1 \leq i \leq s$ and $1 \leq j \leq l$. Summarizing our discussions, we provide necessary and sufficient conditions for a DN code to be a self-dual code or an LCD code over R by the following lemma.

Lemma 3: Let $\mathcal{C} \cong (\oplus_{i=1}^{s}\mathcal{C}_i) \oplus (\oplus_{j=1}^{l}(\mathcal{C}'_j \oplus \mathcal{C}''_j))$ be a DN code over R. $\beta_i = (1, c_{e_i})$, $\beta'_j = (1, c'_{d_j})$, $\beta''_j = (1, c''_{d_j})$ are generators of the codes $\mathcal{C}_i$, $\mathcal{C}'_j$, $\mathcal{C}''_j$ over $R_{(2e_i)}$, $R_{(d_j)}$, $R_{(d_j)}$, respectively; for all $1 \le i \le s$ and $1 \le j \le l$. Then

1.) $\mathcal{C}$ is a self-dual code if and only if the following two equations hold true $1 + c_{e_i}^{1+q^{e_i}} = 0$ and $1 + c'_{d_j}c''_{d_j} = 0$. In particular, the number of SDDN codes over R equals to the product of the numbers of solutions of these two equations.
2.) $\mathcal{C}$ is an LCD code if and only if $1 + c_{e_i}^{1+q^{e_i}} \in R^*_{(2e_i)}$ and $1 + c'_{d_j}c''_{d_j} \in R^*_{(d_j)}$ for all $1 \le i \le s$ and $1 \le j \le l$.

B. ENUMERATION OF DN CODES

Let $\mathcal{C}$ be a SDDN code over R as defined in Equation (10). In order to find the total number of SDDN codes over R, we need to compute the number of SDDN codes of the constituents $\mathcal{C}_i$ and $\{\mathcal{C}'_j, \mathcal{C}''_j\}$ of $\mathcal{C}$. By Lemma 3, the number of SDDN codes over R equals to the product of the numbers of solutions of the following two equations

1.) $1 + c_{e_i}^{1+q^{e_i}} = 0$, for all $1 \le i \le s$; and
2.) $1 + c'_{d_j}c''_{d_j} = 0$, for all $1 \le j \le l$.

The numbers of solutions to each of the aforementioned two equations are obtained independently as follows:

1.) For $\mathcal{C}_i$, where $1 \le i \le s$, we need to determine the total number of SDDN codes with respect to the Hermitian inner product. Thus, by Lemma 3, we need to determine the number of solutions of the equation $1 + c_{e_i}c_{e_i}^{q^{e_i}} = 0$. Using same argument as in the proof of Theorem 3, we get that the total number of solutions of the above equation is $(q^{e_i} + 1)^4$, for each $1 \le i \le s$.

2.) For $\{\mathcal{C}'_j, \mathcal{C}''_j\}$, where $1 \le j \le l$, we need to compute the dual pair solution $\{c'_{d_j}, c''_{d_j}\}$ with respect to the Euclidean inner product of codes. Since Lemma 3, we need to find the total number of solutions of the equation $1 + c'_{d_j}c''_{d_j} = 0$. Using same argument as in the proof of Theorem 3 again, we obtain that the total number of solutions of the above equation is $(q^{d_j} - 1)^4$ for each $1 \le j \le l$.

Multiplying the total number of solutions of the above two equations, the total number of SDDN codes over R is

$$\prod_{i=1}^{s}(q^{e_i} + 1)^4 \prod_{j=1}^{l}(q^{d_j} - 1)^4.$$

Summarizing our discusions and the first part of Lemma 3, we have the following theorem.

Theorem 5: Let n be an even integer, and q be a prime power satisfying $\gcd(n, q) = 1$. The factorization of $y^n + 1$ over R is

$$y^n + 1 = \alpha \prod_{i=1}^{s} f_i(y) \prod_{j=1}^{l} k_j(y)k_j^*(y),$$

where $\alpha \in R^*$ and $n = \sum_{i=1}^{s} 2e_i + 2\sum_{j=1}^{l} d_j$. Then the total number of SDDN codes over R is

$$\prod_{i=1}^{s}(q^{e_i} + 1)^4 \prod_{j=1}^{l}(q^{d_j} - 1)^4.$$

Using the second part of Lemma 3, the total number of LCD DN codes over R can be determined.

Theorem 6: The total number of LCD DN codes over R is

$$\prod_{i=1}^{s}(q^{2e_i} - q^{e_i} - 1)^4 \prod_{j=1}^{l}(q^{2d_j} - q^{d_j} + 1)^4.$$

Proof: Let $\mathcal{C}$ be an LCD DC code over R as defined in Equation (2). In order to find the total number of LCD DN circulant codes over R, we need to count the number of LCD DN circulant codes of the constituents $\mathcal{C}_i$ and $\{\mathcal{C}'_j, \mathcal{C}''_j\}$ of $\mathcal{C}$. From Lemma 2, the total number of LCD DN circulant codes over R is equal to the product of the total number of solutions of the following equations

1.) $1 + c_{e_i}^{1+q^{e_i}} \in R^*_{(2e_i)}$, for each $1 \le i \le s$; and
2.) $1 + c'_{d_j}c''_{d_j} \in R^*_{(d_j)}$ for each $1 \le j \le l$.

1.) For $\mathcal{C}_i$ with $1 \le i \le s$, we find the total number of LCD DN circulant codes with respect to the Hermitian inner product. By Lemma 2, we need to compute the total number of solutions of the equation

$$1 + c_{e_i}^{1+q^{e_i}} \in R^*_{(2e_i)}.$$

We consider the following possible cases.

i.) If $c_{e_i} = 0$, then $1 + c_{e_i}^{1+q^{e_i}} = 1 \in R^*_{(2e_i)}$. Therefore, we have only 1 choice for such c_{e_i}.

ii.) If $c_{e_i} \neq 0$ and $c_{e_i} \in \langle\zeta_0\rangle$, then

$$c_{e_i} = b_0\zeta_0, \text{ for some } b_0 \in \mathbb{F}^*_{q^{2e_i}}.$$

Hence, $1 + c_{e_i}^{1+q^{e_i}} = 1 + \zeta_0 b_0^{1+q^{e_i}} \in R^*_{(2e_i)}$ if and only if $b_0^{1+q^{e_i}} \neq -1$. From Proposition 1, we have $q^{e_i} + 1$ options for $b_0^{1+q^{e_i}} = -1$. Thus, we have $(q^{2e_i} - 1) - (q^{e_i} + 1) = q^{2e_i} - q^{e_i} - 2$ choices for c_{e_i} satisfying $1 + c_{e_i}^{1+q^{e_i}} \in R^*_{(2e_i)}$. Similarly, if $c_{e_i} \neq 0$ and $c_{e_i} \in \langle\zeta_p\rangle$, then we have $(q^{2e_i} - q^{e_i} - 2)$ choices for $p = 1, 2, 3$. The total number of ideals generated by one element out of four elements is $\binom{4}{1}$. Hence total number of choices in this case is $\binom{4}{1}(q^{2e_i} - q^{e_i} - 2)$.

If $c_{e_i} \neq 0$ and $c_{e_i} \in \langle\zeta_0, \zeta_1\rangle$, then $c_{e_i} = b_0\zeta_0 + b_1\zeta_1$, for some $b_0, b_1 \in \mathbb{F}^*_{q^{2e_i}}$. Hence,

$$1 + c_{e_i}^{1+q^{e_i}} = 1 + \zeta_0 b_0^{1+q^{e_i}} + \zeta_1 b_1^{1+q^{e_i}} \in R^*_{(2e_i)}$$

if and only if $b_0^{1+q^{e_i}} \neq -1$, $b_1^{1+q^{e_i}} \neq -1$. As discussed above, we have $(q^{2e_i} - q^{e_i} - 2)^2$ choices for the above type of c_{e_i}. Similarly, if $c_{e_i} \neq 0$ and $c_{e_i} \in \langle\zeta_p, \zeta'_{p'}\rangle$, for $p, p' = 1, 2, 3$ and $p \neq p'$, then we have $(q^{2e_i} - q^{e_i} - 2)^2$ choices for each case. It is easy to verify that the total number of ideals generated by two elements out of 4 elements is $\binom{4}{2}$. Hence, the total number of choices is $\binom{4}{2}(q^{2e_i} - q^{e_i} - 2)^2$.

Similarly, $c_{e_i} \neq 0$ in the ideal generated by $\ell = 3, 4$ elements, then the total number of choices for these cases is

$$\binom{4}{\ell}(q^{2e_i} - q^{e_i} - 2)^{\ell}, \text{ for } \ell = 3, 4.$$

Thus, the total number of choices for c_{e_i} satisfying $1 + c_{e_i}^{1+q^{e_i}} \in R^*_{(2e_i)}$ is $1 + \binom{4}{1}(q^{2e_i} - q^{e_i} - 2)^1 + \binom{4}{2}(q^{2e_i} - q^{e_i} - 2)^2 + \cdots + \binom{4}{4}(q^{2e_i} - q^{e_i} - 2)^4 = (q^{2e_i} - q^{e_i} - 1)^4$.

2.) Now for $\{\mathcal{C}'_j, \mathcal{C}''_j\}$, where $1 \leq j \leq l$, we need to find $\{c'_{d_j}, c''_{d_j}\}$ satisfying $1 + c'_{d_j}c''_{d_j} \in R^*_{(d_j)}$.

Case 2. If $c'_{d_j} \in R_{(d_j)}$, then $c'_{d_j} = t_0\zeta_0 + t_1\zeta_1 + t_2\zeta_2 + t_2\zeta_2 + c_3\zeta_3$, for some $t_i \in \mathbb{F}_{q^{d_j}}$ and $i = 0, 1, 2, 3$. Put $c''_{d_j} = t'_0\zeta_0 + t'_1\zeta_1 + t'_2\zeta_2 + t'_3\zeta_3 \in R_{(d_j)}$; $t'_i \in \mathbb{F}_{q^{d_j}}$, and $i = 0, 1, 2, 3$. We have

$$\begin{aligned} 1 + c'_{d_j}c''_{d_j} &= 1 + \Big(t_0\zeta_0 + t_1\zeta_1 + t_2\zeta_2 + t_3\zeta_3\Big)\Big(t'_0\zeta_0 + \\ &\quad t'_1\zeta_1 + t'_2\zeta_2 + t'_3\zeta_3\Big) \\ &= 1 + t_0t'_0\zeta_0 + t_1t'_1\zeta_1 + t_2t'_2\zeta_2 + t_3t'_3\zeta_3 \\ &= (1 + t_0t'_0)\zeta_0 + (1 + t_1t'_1)\zeta_1 + (1 + t_2t'_2)\zeta_2 \\ &\quad + (1 + t_3t'_3)\zeta_3. \end{aligned}$$

From $1+c'_{d_j}c''_{d_j} \in R^*_{(d_j)}$, we have $(1+t_0t'_0)\zeta_0+(1+t_1t'_1)\zeta_1+(1+t_2t'_2)\zeta_2+(1+t_3t'_3)\zeta_3 \in R^*_{(d_j)}$ if and only if $1 + t_it'_i \neq 0$ for all $i = 0, 1, 2, 3$. For each t_i, we have the following possibilities:

If $t_i = 0$, then $1 + t_it'_i = 1 \neq 0$, for each $t'_i \in \mathbb{F}_{q^{d_j}}$. Thus, there are q^{d_j} choices for t'_i.

If $t_i \in \mathbb{F}^*_{q^{d_j}}$, then $1 + t_it'_i \neq 0$. It implies that $t'_i \neq -\frac{1}{t_i}$ and we have $q^{d_j} - 1$ choices for t'_i corresponding to the given t_i. Also, for t_i, we have $q^{d_j} - 1$ choices. Therefore, we have $(q^{d_j} - 1)^2$ choices for the pair $\{t_i, t'_i\}$ such that $1 + t_it'_i \neq 0$. Combining the two possibilities mentioned above. For each $j = 1, \ldots, l$, the total number of choices for such pair $\{c'_{d_j}, c''_{d_j}\}$ satisfying $1 + c'_{d_j}c''_{d_j} \in R^*_{(d_j)}$ is $(q^{d_j} + (q^{d_j} - 1)^2)^4 = (q^{2d_j} - q^{d_j} + 1)^4$.

By multiplying the total number of solutions of these two equations, the total number of LCD DN codes over R is

$$\prod_{i=1}^{s}(q^{2e_i} - q^{e_i} - 1)^4 \prod_{j=1}^{l}(q^{2d_j} - q^{d_j} + 1)^4,$$

completing our proof. □

Example 20: We consider $R = \mathbb{F}_5 + u\mathbb{F}_5 + v\mathbb{F}_5 + uv\mathbb{F}_5$, and $n = 4$. Then $\gcd(4, 5) = 1$ and the factorization of $y^4 + 1$ into irreducible polynomials over $\mathbb{F}_5$ is

$$y^4 + 1 = \quad (y^2 + 2)(y^2 + 3) = 3(y^2 + 2)(2y^2 + 1).$$

From the above factors, the reciprocal polynomial of $y^2 + 2$ is $2y^2 + 1$. Following the earlier notations, $e_1 = 0$. and $d_1 = 2$. Thus, we have

$$n = \quad \sum_{i=1}^{1} 2e_i + 2\sum_{j=1}^{1} d_j \quad (4 = (2 \times 0) + 2 \times (2)).$$

By using Theorem 5, the total number of SDDN codes over $\mathbb{F}_5 + u\mathbb{F}_5 + v\mathbb{F}_5 + uv\mathbb{F}_5$ is $\prod_{i=1}^{1}(5^{e_i} + 1)^4 \prod_{j=1}^{1}(5^{d_j} - 1)^4 = (5^0 + 1)^4(5^2 - 1)^4 = 2^4 24^4$. By applying Theorem 6, the total number of LCD DN codes over $\mathbb{F}_5 + u\mathbb{F}_5 + v\mathbb{F}_5 + uv\mathbb{F}_5$ is $\prod_{i=1}^{1}(5^{2e_i} - 5^{e_i} - 1)^4 \prod_{j=1}^{1}(5^{2d_j} - 5^{d_j} + 1)^4 = (5^{2\times 0} - 5^0 - 1)^4(5^{2\times 2} - 5^2 + 1)^4 = (601)^4$.

Example 21: We consider $R = \mathbb{F}_{25} + u\mathbb{F}_{25} + v\mathbb{F}_{25} + uv\mathbb{F}_{25}$, and $n = 4$. Then $\gcd(4, 25) = 1$ and the factorization of $y^4 + 1$ into irreducible polynomials over $\mathbb{F}_{25} = \frac{\mathbb{F}_5[w]}{\langle w^2+4w+2\rangle}$ is $y^4 + 1 = (y + w^3)(y + w^{21})(y + w^9)(y + w^{15}) = w^{12}(w^{21}y + 1)(y + w^{21})(w^{15}y + 1)(y + w^{15})$. From the above factors, the reciprocal polynomials of $w^{21}y + 1$ and $w^{15}y + 1$ are $y + w^{21}$ and $y + w^{15}$, respectively. Following the earlier notations, $e_1 = 0$. and $d_1 = d_2 = 1$. Thus, we have $n = \sum_{i=1}^{1} 2e_i + 2\sum_{j=1}^{2} d_j \quad (4 = (2 \times 0) + 2 \times (1) + 2 \times (1))$. By using Theorem 5, the total number of SDDN codes over $\mathbb{F}_{25} + u\mathbb{F}_{25} + v\mathbb{F}_{25} + uv\mathbb{F}_{25}$ is $\prod_{i=1}^{1}(25^{e_i} + 1)^4 \prod_{j=1}^{2}(25^{d_j} - 1)^4 = (25^0 + 1)^4(25^1 - 1)^8 = 2^4 24^8$. By applying Theorem 6, the total number of LCD DN codes over $\mathbb{F}_{25} + u\mathbb{F}_{25} + v\mathbb{F}_{25} + uv\mathbb{F}_{25}$ is $\prod_{i=1}^{1}(25^{2e_i} - 25^{e_i} - 1)^4 \prod_{j=1}^{2}(25^{2d_j} - 25^{d_j} + 1)^4 = (25^{2\times 0} - 25^0 - 1)^4(25^{2\times 1} - 25^1 + 1)^8 = (601)^8$.

Example 22: We consider $R = \mathbb{F}_9 + u\mathbb{F}_9 + v\mathbb{F}_9 + uv\mathbb{F}_9$, and $n = 4$. Then $\gcd(4, 9) = 1$ and the factorization of $y^4 + 1$ into irreducible polynomials over $\mathbb{F}_9 = \frac{\mathbb{F}_3[w]}{\langle w^2+2w+2\rangle}$ is $y^4 + 1 = (y + w)(y + w^7)(y + w^3)(y + w^5) = w^4(w^7y + 1)(y + w^7)(w^5y + 1)(y + w^5)$. From the above factors, the reciprocal polynomials of $w^7y + 1$ and $w^5y + 1$ are $y + w^7$ and $y + w^5$ respectively. Following the earlier notations, we get that $e_1 = 0$. and $d_1 = d_2 = 1$. Thus, $n = \sum_{i=1}^{1} 2e_i + 2\sum_{j=1}^{2} d_j \quad (4 = (2 \times 0) + 2 \times (1) + 2 \times (1))$. By applying Theorem 5, the total number of SDDN codes over $\mathbb{F}_{25} + u\mathbb{F}_{25} + v\mathbb{F}_{25} + uv\mathbb{F}_{25}$ is $\prod_{i=1}^{1}(25^{e_i} + 1)^4 \prod_{j=1}^{2}(25^{d_j} - 1)^4 = (25^0 + 1)^4(25^1 - 1)^8 = 2^4 24^8$. By using Theorem 6, the total number of LCD DN codes over $\mathbb{F}_{25} + u\mathbb{F}_{25} + v\mathbb{F}_{25} + uv\mathbb{F}_{25}$ is $\prod_{i=1}^{1}(25^{2e_i} - 25^{e_i} - 1)^4 \prod_{j=1}^{2}(25^{2d_j} - 25^{d_j} + 1)^4 = (25^{2\times 0} - 25^0 - 1)^4(25^{2\times 1} - 25^1 + 1)^8 = (601)^8$.

Example 23: We consider $R = \mathbb{F}_7 + u\mathbb{F}_7 + v\mathbb{F}_7 + uv\mathbb{F}_7$, and $n = 6$. Then $\gcd(6, 7) = 1$ and the factorization of $y^6 + 1$ into irreducible polynomials over $\mathbb{F}_7$ is $y^6 + 1 = (y^2 + 1)(y^2 + 2)(y^2 + 4) = 2(y^2 + 1)(4y^2 + 1)(y^2 + 4)$. From the above factors, the reciprocal polynomial of $y^2 + 2$ is $2y^2 + 1$. Hence, $e_1 = 1$ and $d_1 = 2$. Thus,

$$n = \quad \sum_{i=1}^{1} 2e_i + 2\sum_{j=1}^{1} d_j \quad (6 = (2 \times 1) + 2 \times (2)).$$

From Theorem 5, the total number of SDDN codes over $\mathbb{F}_7 + u\mathbb{F}_7 + v\mathbb{F}_7 + uv\mathbb{F}_7$ is

$$\begin{aligned} \prod_{i=1}^{1}(7^{e_i} + 1)^4 \prod_{j=1}^{1}(7^{d_j} - 1)^4 &= (7^0 + 1)^4(7^2 - 1)^4 \\ &= 2^4 48^4. \end{aligned}$$

By using Theorem 6, the total number of LCD DN codes over $\mathbb{F}_7+u\mathbb{F}_7+v\mathbb{F}_7+uv\mathbb{F}_7$ is $\prod_{i=1}^{1}(7^{2e_i}-7^{e_i}-1)^4\prod_{j=1}^{1}(7^{2d_j}-7^{d_j}+1)^4=(7^{2\times1}-7^1-1)^4(7^{2\times2}-7^2+1)^4=41^4 2352^4$.

Example 24: We consider $R=\mathbb{F}_{25}+u\mathbb{F}_{25}+v\mathbb{F}_{25}+uv\mathbb{F}_{25}$, and $n=8$. Then $\gcd(8,25)=1$ and the factorization of y^8+1 into irreducible polynomials over $\mathbb{F}_{25}=\frac{\mathbb{F}_5[w]}{\langle w^2+4w+2\rangle}$ is

$$y^8+1=\quad (y^2+w^3)(y^2+w^{21})(y^2+w^9)(y^2+w^{15}).$$

From the above factors, the reciprocal polynomials of y^2+w^3 and y^2+w^9 are $y+w^{21}$ and $y+w^{15}$, respectively. Therefore, $e_1=0$. and $d_1=d_2=2$. Thus, we have $n=\sum_{i=1}^{1}2e_i+2\sum_{j=1}^{2}d_j$ $(8=(2\times0)+2\times(2)+2\times(2))$. By using Theorem 5, the total number of SDDN codes over $\mathbb{F}_{25}+u\mathbb{F}_{25}+v\mathbb{F}_{25}+uv\mathbb{F}_{25}$ is $\prod_{i=1}^{1}(25^{e_i}+1)^4\prod_{j=1}^{2}(25^{d_j}-1)^4=(25^0+1)^4(25^2-1)^8=2^4624^8$. By applying Theorem 6, the total number of LCD DN codes over $\mathbb{F}_{25}+u\mathbb{F}_{25}+v\mathbb{F}_{25}+uv\mathbb{F}_{25}$ is $\prod_{i=1}^{1}(25^{2e_i}-25^{e_i}-1)^4\prod_{j=1}^{2}(25^{2d_j}-25^{d_j}+1)^4=(25^{2\times0}-25^0-1)^4(25^{2\times2}-25^2+1)^8=(390001)^8$.

VI. CONCLUSION

In this paper, we studied the algebraic structure of double circulant codes and DN codes over a finite ring $\mathbb{F}_q+u\mathbb{F}_q+v\mathbb{F}_q+uv\mathbb{F}_q$, where q is an odd prime power. We provided some examples of Gray images of double circulant codes by Lemma 1. We obtained the necessary and sufficient conditions for a double circulant code to be a self-dual code over R in Lemma 2. We enumerated the number of SDDC codes in Theorem 3 by using the factorization of y^n-1 into irreducible polynomials over R. Assume that n is an odd prime and q is a primitive root modulo n with the factorization of y^n-1 into distinct irreducible polynomials over R. Then we obtained a distance bound for SDDC codes over R (Proposition 3). On the assumption that the Artin's conjecture on primitive roots holds true, there are an infinite number of prime numbers n such that q is a primitive root modulo n for a fixed value that is not a square, we gave the factorization of y^n-1 into a product of two irreducible factors. As a result, over R, we have an infinite family of double circulant codes. In addition, we used a Gray map and proved that the families of SDDC codes under this Gray map are asymptotically good (Theorem 4). A necessary and sufficient condition for a DN code to be a self-dual code or an LCD code over R is provided by Lemma 3. Furthermore, we assumed n to be a even positive integer and the factorization of y^n+1 into distinct irreducible polynomials with $\gcd(n,q)=1$, then we determined the number of self-dual and LCD DN codes computed in Theorems 5 and 6, respectively.

Let A and B be two circulants (resp. negacirculant) matrices and I_n be an identity matrix of order n. We take

$$S=\begin{bmatrix} I_n & 0 & A & B \\ 0 & I_n & -B^T & A^T \end{bmatrix}.$$

A linear code C is a four circulant code (resp. four negacirculant) if C is generated by S. In addition, a four circulant code of length $4n$ is a $\frac{\mathbb{F}_q[x]}{\langle x^n-1\rangle}$-submodule of $\left(\frac{\mathbb{F}_q[x]}{\langle x^n-1\rangle}\right)^4$ and a four negacirculant code of length $4n$ is a $\frac{\mathbb{F}_q[x]}{\langle x^n+1\rangle}$-submodule of $\left(\frac{\mathbb{F}_q[x]}{\langle x^n+1\rangle}\right)^4$ (see [9]). In the future, it would be interesting to study the self-dual four circulant codes, LCD four circulant and four negacirculant codes over a finite ring $R=\frac{\mathbb{F}_q[u,v]}{\langle u^2-u,v^2-v,uv-vu\rangle}$.

REFERENCES

[1] A. Alahmandi, C. Güneri, B. Özdemir, H. Shoaib, and P. Solé, "On SDDN codes," *Discrete Appl. Math.*, vol. 222, pp. 205–212, Jan. 2017.

[2] A. Alahmadi, F. Özdemir, and P. Solé, "On SDDC codes," *Des. Codes, Cryptogr.*, vol. 86, pp. 1257–1265, Jul. 2017.

[3] E. F. Assmus, H. F. Mattson, and R. Turyn, "Cyclic codes," AF Cambridge Res. Labs, Bedford, U.K., Tech. Rep. AFCRL-66-348, 1966, pp. 66–348.

[4] W. Bosma, J. Cannon, C. Fieker, and A. Steel, Eds., *Handbook of Magma Functions*, 2nd ed. Sydney, NSW, Australia: Univ. of Sydney, School of Mathematics and Statistics, 2013, p. 5488.

[5] C. L. Chen, W. W. Peterson, and E. J. Weldon, "Some results on quasi-cyclic codes," *Inf. Control*, vol. 15, no. 5, pp. 407–423, Nov. 1969.

[6] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. New York, NY, USA: Wiley, 1991.

[7] H. Q. Dinh, T. Bag, S. Pathak, A. K. Upadhyay, and W. Chinnakum, "Quantum codes obtained from constacyclic codes over a family of finite ring $\mathbb{F}_p[u_1,u_2,\ldots,u_s]$," *IEEE Access*, vol. 8, pp. 194082–194091, 2020.

[8] C. Güneri, B. Özkaya, and P. Solé, "Quasi-cyclic complementary dual codes," *Finite Fields Their Appl.*, vol. 42, pp. 67–80, Nov. 2016.

[9] M. Harada, W. Holzmann, H. Kharaghani, and M. Khorvash, "Extremal ternary self-dual codes constructed from negacirculant matrices," *Graphs Combinatorics*, vol. 23, no. 4, pp. 401–417, Aug. 2007.

[10] I. N. Herstein, *Topics in Algebra*. Hoboken, NJ, USA: Wiley, 1975.

[11] D. Huang, M. Shi, and P. Solé, "Double circulant self-dual and LCD codes over $\mathbb{Z}_{p^2}$," *Int. J. Found. Comput.*, vol. 30, no. 3, pp. 407–416, 2019.

[12] W. C. Huffman and V. Pless, *Fundamentals of Error Correcting Codes*. Cambridge, U.K.: Cambridge Univ. Press, 2003.

[13] T. Kasami, "A Gilbert–Varshamov bound for quasi-cycle codes of rate $\frac{1}{2}$ (corresp.)," *IEEE Trans. Inf. Theory*, vol. IT-20, no. 5, p. 679, Sep. 1974.

[14] R. Lidl and H. Niederreiter, *Introduction to Finite Fields and Their Applications*, 2nd ed. Cambridge, U.K.: Cambridge Univ. Press, 1986.

[15] S. Ling and P. Solé, "On the algebraic structure of quasi-cyclic codes. I. Finite fields," *IEEE Trans. Inf. Theory*, vol. 47, no. 7, pp. 2751–2760, Nov. 2001.

[16] S. Ling and P. Solé, "On the algebraic structure of quasi-cyclic codes II: Chain rings," *Des. Codes, Cryptogr.*, vol. 30, pp. 113–130, Aug. 2003.

[17] S. Ling and C. Xing, *Coding Theory: A First Course*. Cambridge, U.K.: Cambridge Univ. Press, 2004.

[18] C. Martinez-Perez and W. Willems, "Is the class of cyclic codes asymptotically good?" *IEEE Trans. Inf. Theory*, vol. 52, no. 2, pp. 696–700, Feb. 2006.

[19] P. Moree, "Artin's primitive root conjecture—A survey," *Integers*, vol. 10, pp. 1305–1416, Jul. 2012.

[20] A. Sharma, G. K. Bakshi, V. C. Dumir, and M. Raka, "Cyclotomic numbers and primitive idempotents in the ring $G\mathbb{F}_q[x]/\langle x^{p^m}-1\rangle$," *Finite Fields Their Appl.*, vol. 10, no. 4, pp. 653–673, Oct. 2004.

[21] M. Shi, D. Huang, L. Sok, and P. Solé, "Double circulant LCD codes over $\mathbb{Z}_4$," *Finite Fields Appl.*, vol. 58, pp. 133–144, Jul. 2019.

[22] M. Shi, H. Zhu, L. Qian, and S. Sok, and P. Solé, "On self-dual and LCD double circulant and DN codes over $\mathbb{F}_q+u\mathbb{F}_q$," *Crypogr. Commun.*, vol. 12, pp. 53–70, Mar. 2020.

[23] T. Yao, S. Zhu, and X. Kai, "On self-dual and LCD double circulant codes over a non-chain ring," *Chin. J. Electron.*, vol. 28, no. 5, pp. 1018–1024, Sep. 2019.

[24] S. Yadav, H. Islam, O. Prakash, and P. Solé, "Self-dual and LCD double circulant and DN codes over $\mathbb{F}_q+u\mathbb{F}_q+v\mathbb{F}_q$," *J. Appl. Math. Comput.*, vol. 67, pp. 689–705, Jan. 2021.

HAI Q. DINH received the B.Sc., M.Sc., and Ph.D. degrees in mathematics from Ohio University, Athens, OH, USA, in 1998, 2000, and 2003, respectively. He was a Visiting Professor with North Dakota State University, Fargo, ND, USA, for one year. Since 2004, he has been a tenure Professor in mathematics with Kent State University, Kent, OH, USA, where he is currently a Professor in applied mathematics with the Department of Mathematical Sciences. Since 2004, he has published more than 75 papers at high-level SCI(E) research journals, such as *Journal of Algebra*, *Journal of Pure and Applied Algebra*, IEEE TRANSACTIONS ON INFORMATION THEORY, IEEE COMMUNICATION LETTERS, *Finite Fields and Their Applications*, *Applicable Algebra in Engineering Communication and Computing*, and *Discrete Applied Mathematics*. His research interests include algebra and coding theory. He was a recipient of the International Association of Geomagnetism and Aeronomy Young Scientist Award for Excellence, in 2008, and the IEEE Electromagnetic Compatibility Society Best Symposium Paper Award, in 2011. He has been a well-known invited/keynote speaker at numerous international conferences and mathematics colloquium. Other than universities in the U.S., he also gave many honorary tutorial lectures at international universities in China, Indonesia, Kuwait, Mexico, Singapore, Thailand, and Vietnam.

BHANU PRATAP YADAV received the B.Sc. and M.Sc. degrees from Banaras Hindu University, Varanasi, India, and the Ph.D. degree from the Department of Mathematics, IIT Patna, India. He is currently a Postdoctoral Researcher with the Department of Communications and Networking, Aalto University, Finland. His main research interests include algebraic coding theory and codes over rings.

BAC T. NGUYEN received the B.Sc. degree in mathematics from Thai Nguyen University, Vietnam, in 2008, the M.Sc. degree in mathematics from the Institute of Mathematics, Hanoi, Vietnam, in 2010, and the Ph.D. degree from Mahidol University, Bangkok, Thailand, in 2015. He has published 15 papers in high-ranked peer-reviewed journals, such as IEEE TRANSACTIONS ON INFORMATION THEORY, IEEE COMMUNICATION LETTERS, *Discrete Applied Mathematics*, and *Finite Fields and Their Applications*. His research interests include algebraic coding theory and algebra.

ASHISH KUMAR UPADHYAY received the B.Sc. and M.Sc. degrees in mathematics from the University of Allahabad, India, and the Ph.D. degree from the Indian Institute of Science, in 2005. He is currently a Professor with the Department of Mathematics, Banaras Hindu University, Varanasi, India. His research interests include algebraic coding theory and algebraic topology.

WORAPHON YAMAKA received the bachelor's, master's, and Ph.D. degrees in economics from Chiang Mai University, Chiang Mai, Thailand, in 2011, 2014, and 2017, respectively. Since 2018, he has been a Lecturer with the Faculty of Economics, Chiang Mai University. He is currently the Vice Director of the Centre of Excellence in Econometrics, Chiang Mai University. Since 2015, he has published more than 90 papers which indexed in the SCOPUS. His research interests include economics and econometrics.