Thai **J**ournal of **M**athematics : (2020) 135–144
Special Issue: The 14^{th} IMT-GT ICMSA 2018
http://thaijmath.in.cmu.ac.th
Online ISSN 1686-0209

Hulls of Cyclic Codes over the Ring $\mathbb{F}_2 + v\mathbb{F}_2$

Somphong Jitman[†] **and Ekkasit Sangwisut**[‡,1]

[†]Department of Mathematics, Faculty of Science, Silpakorn University,
Nakhon Pathom 73000, Thailand
e-mail : sjitman@gmail.com
[‡]Department of Mathematics and Statistics, Faculty of Science, Thaksin University,
Phattalung 93210, Thailand
e-mail : ekkasit.sangwisut@gmail.com

Abstract : Hulls of linear codes over finite fields have been introduced and become of interest due to their wide practical applications. Recently, the concept of hulls has been generalized to linear and cyclic codes over the finite chain ring $\mathbb{Z}_4$. In this paper, hulls of cyclic codes over a non-chain ring $\mathbb{F}_2 + v\mathbb{F}_2$ are studied, where $v^2 = v$. The hull dimensions and the average hull dimension $E(n)$ of cyclic codes of length n over $\mathbb{F}_2 + v\mathbb{F}_2$ are determined. Asymptotically, if n is odd, it turns out that $E(n)$ is zero or it grows the same rate as n.

Keywords : average hull dimension; cyclic codes; reciprocal polynomials.
2010 Mathematics Subject Classification : 94B15; 94B05.

1 Introduction

In [1], the hull of a linear code has been first introduced to classify finite projective planes. The hull and the hull dimension of a linear code over finite fields have been of interest and extensively studied due to their wide practical applications (see [2], [3], [4] and references therein). The enumeration of linear codes of length n over a finite field whose hulls have the same dimension has been established in [4]. The average hull dimension of linear codes of length n over a finite field has been given as well. The hulls of cyclic codes over finite fields and the average hull dimension of cyclic codes have been discussed in [3]. In [2], the hull dimensions of cyclic and negacyclic codes and the number of cyclic codes whose hulls share the dimension have been presented. In general, the average hull dimension of constacyclic codes over finite fields have been established in [5, 6, 7].

Codes over rings have become of interest after it has been shown that the Kerdock codes, Preparata codes and Delsarte-Goethals codes can be obtained through the Gray images of linear codes over $\mathbb{Z}_4$ in important works [8, 9]. Recently, the concept of hulls has been generalized to linear and cyclic codes over the finite chain ring $\mathbb{Z}_4$ in [10]. The characterization of the hull of a cyclic code over $\mathbb{Z}_4$ has been

[0]This reasearch was supported by the Thailand Research Fund and the Office of Higher Education Commision of Thailand under Research Grant MRG6080054.

[1]Corresponding author.

established in terms of the generators viewed as ideals in the quotient ring $\mathbb{Z}_4[x]/(x^n-1)$. The average hull dimension of cyclic codes of odd length n over $\mathbb{Z}_4$ has been established.

In this paper, we focus on hulls of cyclic codes over a commutative non-chain ring $\mathcal{R} := \mathbb{F}_2 + v\mathbb{F}_2 = \{0, 1, v, \overline{v} := 1+v\}$, where $v^2 = v$ and the addition and multiplication are given in the Table 1. It is not difficult to see that $\mathcal{R}$ is a commutative ring with identity which is not a field since $v \cdot \overline{v} = 0$. Moreover, $\mathcal{R}$ is not a local ring since the ideals (v) and $(\overline{v})$ are its distinct maximal ideals. Here, we focus on hulls of cyclic codes of length n over $\mathcal{R}$ and determine the average hull dimension of such codes. A general formula for the average hull dimension is established together with its asymptotic behavior.

$+$	0	1	v	$\overline{v}$
0	0	1	v	$\overline{v}$
1	1	0	$\overline{v}$	v
v	v	$\overline{v}$	0	1
$\overline{v}$	$\overline{v}$	v	1	0

$\cdot$	0	1	v	$\overline{v}$
0	0	0	0	0
1	0	1	v	$\overline{v}$
v	0	v	v	0
$\overline{v}$	0	$\overline{v}$	0	$\overline{v}$

Table 1: Multiplication and addition tables for $\mathbb{F}_2 + v\mathbb{F}_2$ respectively.

The paper is organized as follows. Some preliminary results on binary cyclic codes and cyclic codes over $\mathcal{R}$ are discussed in Section 2. The characterization of the hull of cyclic codes of length n over $\mathcal{R}$ is given in Section 3 together with the determination of the dimensions of the hull of cyclic codes of length n over $\mathcal{R}$. In Section 4, the average hull dimension of cyclic codes of length n over $\mathcal{R}$ are studied.

2 PRELIMINARIES

In this section, some preliminary results on binary cyclic codes and cyclic codes over the ring $\mathcal{R} = \mathbb{F}_2 + v\mathbb{F}_2$ are recalled and discussed.

Let R be a finite commutative ring. A *linear code* C of length n over R is defined to be an R-submodule of R^n. The *Euclidean dual* of C is defined to be the set

$$C^{\perp} = \left\{ (x_0, \dots, x_{n-1}) \in R^n \mid \sum_{i=0}^{n-1} x_i c_i = 0 \text{ for all } (c_0, \dots, c_{n-1}) \in C \right\}$$

and the *Euclidean hull* of C is defined as $\mathrm{Hull}(C) = C \cap C^{\perp}$. A linear codes of length n over R is said to be *cyclic* if $(c_{n-1}, c_0, \dots, c_{n-2}) \in C$ for all $(c_0, \dots, c_{n-1}) \in C$. Useful properties of cyclic codes over $\mathbb{F}_2$ and $\mathcal{R}$ are discussed in subsections 2.1 an 2.2, respectively.

2.1 Binary Cyclic Codes

In this subsection, properties of codes over $R = \mathbb{F}_2$ are recalled. A linear code of length n over $\mathbb{F}_2$ is sometime called a *binary linear code* and it can be viewed as a $\mathbb{F}_2$-vector space of $\mathbb{F}_2^n$. The *dimension* of a binary linear code C is denoted by $\dim(C) = \log_2(|C|)$. Each binary cyclic code C of length n can be identified as an ideal of the principal ideal ring $\mathbb{F}_2[x]/(x^n-1)$ generated by a unique monic divisor $g(x)$ of $x^n - 1$. Such a polynomial is called the *generator polynomial* for C and $\dim(C) = n - \deg g(x)$.

Let $f(x) = 1 + a_1 x + \cdots + a_{k-1}x^{k-1} + x^k \in \mathbb{F}_2[x]$ be a polynomial of degree k whose constant term is 1. The *reciprocal polynomial* of $f(x)$ is defined to be $f^*(x) = x^k f\left(\frac{1}{x}\right)$. It is not difficult to see that $(f^*(x))^* = f(x)$. Then the polynomials over $\mathbb{F}_2[x]$ can be classified into 2 types. If $f(x) = f^*(x)$, then $f(x)$ is called a *self-reciprocal polynomial.* Otherwise, we have $f(x) \neq f^*(x)$ and the polynomials $f(x)$ and $f^*(x)$ are called a *reciprocal polynomial pair.*

For a given binary cyclic code C of length n with the generator polynomial $g(x)$. The Euclidean dual of C denoted by $C^{\perp}$ has the generator polynomial of the form $h^*(x)$ where $h(x) = \frac{x^n-1}{g(x)}$ (see [11, Lemma

2.1]). Note that $h^*(x)$ is a monic divisor of $x^n - 1$ and $\mathrm{lcm}(f(x), h^*(x))$ is the generator polynomial of $\mathrm{Hull}(C)$ (see [2, Theorem 1]).

Let n be a positive integer and write $n = 2^\nu \overline{n}$, where $\overline{n}$ is odd and $\nu \geq 0$ is an integer. For an odd positive integer j, $\mathrm{ord}_j(2)$ is the multiplicative order of 2 modulo j. Let

$$N_2 = \left\{\ell \geq 1 : \ell \mid (2^k + 1) \text{ for some } k \in \mathbb{N}\right\}.$$

By [2, Equation (6)], $x^n - 1$ can be factored into a product of monic irreducible polynomials over $\mathbb{F}_2$ of the form

$$x^n - 1 = \left(x^{\overline{n}} - 1\right)^{2^\nu} = \prod_{j \mid \overline{n}, j \in N_2} \left(\prod_{i=1}^{\gamma(j)} g_{ij}(x)\right)^{2^\nu} \prod_{j \mid \overline{n}, j \notin N_2} \left(\prod_{i=1}^{\beta(j)} f_{ij}(x) f_{ij}^*(x)\right)^{2^\nu}, \tag{2.1}$$

where

$$\gamma(j) = \frac{\phi(j)}{\mathrm{ord}_j(2)}, \quad \beta(j) = \frac{\phi(j)}{2\,\mathrm{ord}_j(2)},$$

$f_{ij}(x)$ and $f_{ij}^*(x)$ form a reciprocal polynomial pair of degree $\mathrm{ord}_j(2)$ and $g_{ij}(x)$ is a self-reciprocal polynomial of degree $\mathrm{ord}_j(2)$. Let $B_{\overline{n}} = \deg \prod_{j \mid \overline{n}, j \in N_2} \left(\prod_{i=1}^{\gamma(j)} g_{ij}(x)\right)$. The number $B_{\overline{n}}$ can be simplified as follows

$$B_{\overline{n}} = \deg \prod_{j \mid \overline{n}, j \in N_2} \left(\prod_{i=1}^{\gamma(j)} g_{ij}(x)\right) = \sum_{j \in \overline{n}, j \in N_2} \frac{\phi(j)}{\mathrm{ord}_j(2)} \cdot \mathrm{ord}_j(2) = \sum_{j \in \overline{n}, j \in N_2} \phi(j).$$

The number $B_{\overline{n}}$ plays a crucial role in the study the average dimension of the hull of cyclic codes over $\mathcal{R}$ in Section 4.

2.2 Cyclic Codes over $\mathbb{F}_2 + v\mathbb{F}_2$

Some results on cyclic codes of length n over $\mathcal{R} = \mathbb{F}_2 + v\mathbb{F}_2$ in [12] are recalled and additional useful properties of linear and cyclic codes over $\mathcal{R}$ are discussed and proved.

Recall that $\mathcal{R} = \mathbb{F}_2 + v\mathbb{F}_2 = \{0, 1, v, \bar{v} := 1 + v\}$, where $v^2 = v$. For each element in $\mathcal{R}$ can be uniquely written as $a + bv$ for some $a, b \in \mathbb{F}_2$. Then the map $\phi : \mathcal{R} \to \mathbb{F}_2 \times \mathbb{F}_2$ defined by $\phi(a + bv) = (a, a + b)$ is a ring isomorphism form $\mathcal{R}$ to $\mathbb{F}_2 \times \mathbb{F}_2$. The map ϕ can be extended to be a ring isomorphism $\phi : \mathcal{R}^n \to \mathbb{F}_2^n \times \mathbb{F}_2^n$ given as follows

$$\phi(\boldsymbol{r}) = \phi(a_0 + b_0 v, \ldots, a_{n-1} + b_{n-1} v) = (a_0, \ldots, a_{n-1}, a_0 + b_0, \ldots, a_{n-1} + b_{n-1}).$$

Moreover, the map ϕ can be viewed as an $\mathbb{F}_2$-linear isomorphism. Hence, a linear code C of length n over $\mathcal{R}$ can be viewed as a vector space over $\mathbb{F}_2$ and denoted by $\dim_2(C)$ the 2-dimension of C, the dimension of C over $\mathbb{F}_2$. It is not difficult to see that $\dim_2(C) = \log_2(|C|)$.

For each linear code C of length n over $\mathcal{R}$, let

$$\mathrm{R}(C) = \{a \mid a + bv \in C \text{ for some } a \in \mathbb{F}_2^n\} \text{ and } \mathrm{T}(C) = \{a + b \mid a + bv \in C \text{ for some } a \in \mathbb{F}_2^n\}.$$

It is not difficult to see that $\mathrm{R}(C)$ and $\mathrm{T}(C)$ are binary linear codes of length n.

Lemma 2.1. *Let C_1 and C_2 be binary linear codes of length n. Then $(1 + v)C_1 \cap vC_2 = \{0\}$.*

Proof. Let $x \in (1 + v)C_1 \cap vC_2$. Then $(1 + v)c_1 = x = vc_2$ where $c_1 \in C_1$ and $c_2 \in C_2$. It follows that $0 = c_1 + (c_1 + c_2)v$, and hence, $c_1 = 0 = c_2$. Therefore, $x = 0$ and $(1 + v)C_1 \cap vC_2 = \{0\}$ as desired. □

For linear codes C_1 and C_2 of length n over $\mathcal{R}$, the *direct sum* of C_1 and C_2 is defined to be

$$C_1 \oplus C_2 = \{c_1 + c_2 \mid c_1 \in C_1, c_2 \in C_2\}$$

satisfying $C_1 \cap C_2 = \{0\}$. In this case, for every $c \in C_1 \oplus C_2$, there exist unique $c_1 \in C_1$ and $c_2 \in C_2$ such that $c = c_1 + c_2$.

A linear code C of length n over $\mathcal{R}$ can be written as the direct sum of $R(C)$ and $T(C)$ as follows.

Theorem 2.2 ([12, Theorem 3.1 and Corollary 3.3])**.** *Let C be a linear code of length n over $\mathcal{R}$. Then $\phi(C) = \mathrm{R}(C) \times \mathrm{T}(C)$ and $|C| = |\mathrm{R}(C)||\mathrm{T}(C)|$. Moreover, C can be uniquely expressed as $C = (1+v)\,\mathrm{R}(C) \oplus v\,\mathrm{T}(C)$.*

The decomposition of the intersection of any two linear codes of the same length over $\mathcal{R}$ is given in the next theorem.

Theorem 2.3. *Let $C = (1+v)\,\mathrm{R}(C) \oplus v\,\mathrm{T}(C)$ and $D = (1+v)\,\mathrm{R}(D) \oplus v\,\mathrm{T}(D)$ be linear codes of length n over $\mathcal{R}$. Then $C \cap D = (1+v)\,(\mathrm{R}(C) \cap \mathrm{R}(D)) \oplus v\,(\mathrm{T}(C) \cap T(D))$.*

Proof. Let $c = (1+v)c' + vc'' \in C \cap D$. Since $c \in C = (1+v)\,\mathrm{R}(C) \oplus v\,\mathrm{T}(C)$, we have $c' \in \mathrm{R}(C)$ and $c'' \in \mathrm{T}(C)$. Since $c \in D = (1+v)\,\mathrm{R}(D) \oplus v\,\mathrm{T}(D)$, we have $c' \in \mathrm{R}(D)$ and $c'' \in \mathrm{T}(D)$. It follows that $c \in \mathrm{R}(C) \cap \mathrm{R}(D)$ and $c' \in \mathrm{T}(C) \cap T(D)$. Hence, $c \in (1+v)\,(\mathrm{R}(C) \cap \mathrm{R}(D)) \oplus v\,(\mathrm{T}(C) \cap T(D))$. The reverse inclusion is obvious. □

Each cyclic code C of length n over $\mathcal{R}$ can be viewed as an ideal of the quotient ring $\mathcal{R}_n = \mathcal{R}[x]/(x^n-1)$ and the corresponding ideal is generated by

$$((1+v)g_1(x), vg_2(x)),$$

where $g_1(x)$ and $g_2(x)$ are monic divisors of $x^n - 1$ over $\mathbb{F}_2$ [12, Theorem 4.5]. Furthermore, $|C| = 2^{2n - \deg g_1(x) - \deg g_2(x)}$. In this case, the 2-dimension of C is $2n - \deg g_1(x) - \deg g_2(x)$. By [12, Corollary 4.8], the dual $C^{\perp}$ of C is generated by

$$((1+v)h_1^*(x), vh_2^*(x)), \tag{2.2}$$

where $h_1(x) = \frac{x^n-1}{g_1(x)}$ and $h_2(x) = \frac{x^n-1}{g_2(x)}$.

Let $\mathcal{C}(n)$ be the *set of all cyclic codes of length n over $\mathcal{R}$*. The *average 2-dimension of the hull of cyclic codes of length n* over $\mathcal{R}$ is defined to be

$$E(n) = \sum_{C \in \mathcal{C}(n)} \frac{\dim_2 \mathrm{Hull}(C)}{|\mathcal{C}(n)|}.$$

The characterization of $\mathrm{Hull}(C)$ and the average 2-dimension $E(n)$ will be discussed in Sections 3 and 4, respectively.

3 Hulls of Cyclic Codes over $\mathbb{F}_2 + v\mathbb{F}_2$

In this section, algebraic structure of the hull of a cyclic code of length n over $\mathcal{R} = \mathbb{F}_2 + v\mathbb{F}_2$ are focused on. Subsequently, the 2-dimensions of the hulls of cyclic codes of length n over $\mathcal{R}$ are determined.

Theorem 3.1. *Let $C = (1+v)C_1 \oplus vC_2$ be a cyclic code of length n over $\mathcal{R}$ generated by $((1+v)g_1(x), vg_2(x))$, where $g_1(x)$ and $g_2(x)$ are monic divisors of $x^n - 1$ over $\mathbb{F}_2$. Then $\mathrm{Hull}(C)$ is generated by*

$$\left((1+v)\,\mathrm{lcm}(g_1(x), h_1^*(x)), v\,\mathrm{lcm}(g_2(x), h_2^*(x))\right),$$

where $h_1(x) = \frac{x^n-1}{g_1(x)}$ and $h_2(x) = \frac{x^n-1}{g_2(x)}$.

Proof. Note that $g_1(x)$ and $g_2(x)$ are generator polynomials of binary cyclic codes C_1 and C_2, respectively. By Equation (2.2), we have $C^{\perp} = (1+v)C_1^{\perp} \oplus vC_2^{\perp}$ generated by $((1+v)h_1^*(x), vh_2^*(x))$, where $h_1(x) = \frac{x^n-1}{g_1(x)}$ and $h_2(x) = \frac{x^n-1}{g_2(x)}$. Moreover, $h_1^*(x)$ and $h_2^*(x)$ are the generator polynomials of binary cyclic codes

$C_1^\perp$ and $C_2^\perp$, respectively. By [2, Theorem 1], the generator polynomials of $\mathrm{Hull}(C_1)$ and $\mathrm{Hull}(C_2)$ are $\mathrm{lcm}(g_1(x), h_1^*(x))$ and $\mathrm{lcm}(g_2(x), h_2^*(x))$ respectively. Therefore, by Theorem 2.3,

$$\mathrm{Hull}(C) = C \cap C^\perp = ((1+v)\,\mathrm{Hull}(C_1), v\,\mathrm{Hull}(C_2))$$

is generated by

$$((1+v)\,\mathrm{lcm}(g_1(x), h_1^*(x)), v\,\mathrm{lcm}(g_2(x), h_2^*(x)))$$

as desired. □

The 2-dimension of $\mathrm{Hull}(C)$ is given in Theorem 3.3 based on the following lemma.

Lemma 3.2. *Let ν be a nonnegative integer. Let $0 \le a, b, c \le 2^\nu$ be integers. Then the following statements hold.*

1. $0 \le 2^\nu - \max\{a, 2^\nu - a\} \le 2^{\nu-1}$.

2. $0 \le 2^{\nu+1} - \max\{b, 2^\nu - c\} - \max\{c, 2^\nu - b\} \le 2^\nu$.

Proof. To prove Statement 2, we consider the following two cases.

Case I: $0 \le a \le 2^{\nu-1}$. We have $-2^\nu \le -a \le 0$ which implies that $2^{\nu-1} \le 2^\nu - a \le 2^\nu$. Hence, $2^{\nu-1} \le \max\{a, 2^\nu - a\} \le 2^\nu$.

Case II: $2^{\nu-1} < a \le 2^\nu$. We have $-2^\nu \le a < -2^{\nu-1}$ which means $0 \le 2^\nu - a < 2^{\nu-1}$. Consequently, $2^{\nu-1} < \max\{a, 2^\nu - a\} \le 2^\nu$.

All together, we conclude that $0 \le 2^\nu - \max\{a, 2^\nu - a\} \le 2^{\nu-1}$. Hence, Statement 1 is proved.

To prove Statement 2, we consider the following two cases.

Case I: $\max\{b, 2^\nu - c\} = b$. We have $\max\{c, 2^\nu - b\} = c$ which means $2^{\nu+1} - \max\{b, 2^\nu - c\} - \max\{c, 2^\nu - b\} = 2^{\nu+1} - b - c$. Since $2^\nu \le b + c \le 2^{\nu+1}$, we have $0 \le 2^{\nu+1} - b - c \le 2^\nu$.

Case II: $\max\{b, 2^\nu - c\} = 2^\nu - c$. We have $\max\{c, 2^\nu - b\} = 2^\nu - b$ which implies that $\max\{b, 2^\nu - c\} + \max\{c, 2^\nu - b\} = 2^\nu - c + 2^\nu - b = 2^{\nu+1} - c - b$. Thus $0 \le 2^{\nu+1} - \max\{b, 2^\nu - c\} - \max\{c, 2^\nu - b\} = b + c \le 2^\nu$.

Hence, we conclude that $0 \le 2^{\nu+1} - \max\{b, 2^\nu - c\} - \max\{c, 2^\nu - b\} \le 2^\nu$. Therefore, Statement 2 is proved. □

Theorem 3.3. *Let n be a positive integer and write $n = 2^\nu \overline{n}$, where $\overline{n}$ is odd and $\nu \ge 0$ is an integer. Then the 2-dimensions of the hull of cyclic codes of length n over $\mathcal{R}$ are of the form*

$$\sum_{j \in \overline{n}, j \in N_2} \mathrm{ord}_j(2) \cdot a_j + \sum_{j \in \overline{n}, j \notin N_2} \mathrm{ord}_j(2) \cdot b_j,$$

where $0 \le a_j \le 2^\nu$ and $0 \le b_j \le 2^{\nu+1}$.

Proof. Let $C = (1+v)C_1 \oplus vC_2$ be a cyclic code of length n over $\mathcal{R}$ generated by $((1+v)g_1(x), vg_2(x))$. Then $C^\perp = (1+v)C_1^\perp \oplus vC_2^\perp$ generated by $((1+v)h_1^*(x), vh_2^*(x))$ by Equation (2.2). Note that $g_1(x), g_2(x), h_1^*(x)$ and $h_2^*(x)$ are monic divisors of $x^n - 1$.

By Equation (2.1), we have

$$
\begin{aligned}
g_1(x) &= \prod_{j|\overline{n}, j\in N_2} \prod_{i=1}^{\gamma(j)} g_{ij}(x)^{a_{ij}} \prod_{j|\overline{n}, j\notin N_2} \prod_{i=1}^{\beta(j)} f_{ij}(x)^{b_{ij}} f_{ij}^*(x)^{c_{ij}},\\
g_2(x) &= \prod_{j|\overline{n}, j\in N_2} \prod_{i=1}^{\gamma(j)} g_{ij}(x)^{u_{ij}} \prod_{j|\overline{n}, j\notin N_2} \prod_{i=1}^{\beta(j)} f_{ij}(x)^{v_{ij}} f_{ij}^*(x)^{w_{ij}},\\
h_1(x) &= \prod_{j|\overline{n}, j\in N_2} \prod_{i=1}^{\gamma(j)} g_{ij}(x)^{2^\nu - a_{ij}} \prod_{j|\overline{n}, j\notin N_2} \prod_{i=1}^{\beta(j)} f_{ij}(x)^{2^\nu - b_{ij}} f_{ij}^*(x)^{2^\nu - c_{ij}},\\
h_2(x) &= \prod_{j|\overline{n}, j\in N_2} \prod_{i=1}^{\gamma(j)} g_{ij}(x)^{2^\nu - u_{ij}} \prod_{j|\overline{n}, j\notin N_2} \prod_{i=1}^{\beta(j)} f_{ij}(x)^{2^\nu - v_{ij}} f_{ij}^*(x)^{2^\nu - w_{ij}},\\
h_1^*(x) &= \prod_{j|\overline{n}, j\in N_2} \prod_{i=1}^{\gamma(j)} g_{ij}(x)^{2^\nu - a_{ij}} \prod_{j|\overline{n}, j\notin N_2} \prod_{i=1}^{\beta(j)} f_{ij}(x)^{2^\nu - c_{ij}} f_{ij}^*(x)^{2^\nu - b_{ij}},\\
h_2^*(x) &= \prod_{j|\overline{n}, j\in N_2} \prod_{i=1}^{\gamma(j)} g_{ij}(x)^{2^\nu - u_{ij}} \prod_{j|\overline{n}, j\notin N_2} \prod_{i=1}^{\beta(j)} f_{ij}(x)^{2^\nu - w_{ij}} f_{ij}^*(x)^{2^\nu - v_{ij}},
\end{aligned}
$$

for some $0 \leq a_{ij}, b_{ij}, c_{ij}, u_{ij}, v_{ij}, w_{ij} \leq 2^\nu$.

Since Hull(C) generated by $((1+v)\operatorname{lcm}(g_1(x), h_1^*(x)), v\operatorname{lcm}(g_2(x), h_2^*(x)))$, we have

$$
\begin{aligned}
\operatorname{lcm}(g_1(x), h_1^*(x)) = &\prod_{j|\overline{n}, j\in N_2} \prod_{i=1}^{\gamma(j)} g_{ij}(x)^{\max\{a_{ij}, 2^\nu - a_{ij}\}}\\
&\prod_{j|\overline{n}, j\notin N_2} \prod_{i=1}^{\beta(j)} f_{ij}(x)^{\max\{b_{ij}, 2^\nu - c_{ij}\}} f_{ij}^*(x)^{\max\{c_{ij}, 2^\nu - b_{ij}\}}, \qquad (3.1)\\
\operatorname{lcm}(g_2(x), h_2^*(x)) = &\prod_{j|\overline{n}, j\in N_2} \prod_{i=1}^{\gamma(j)} g_{ij}(x)^{\max\{u_{ij}, 2^\nu - u_{ij}\}}\\
&\prod_{j|\overline{n}, j\notin N_2} \prod_{i=1}^{\beta(j)} f_{ij}(x)^{\max\{v_{ij}, 2^\nu - w_{ij}\}} f_{ij}^*(x)^{\max\{w_{ij}, 2^\nu - v_{ij}\}}. \qquad (3.2)
\end{aligned}
$$

By Equations (3.1) and (3.2), it can be concluded that

$$
\begin{aligned}
\dim_2(\text{Hull}(C)) =& 2n - \deg\operatorname{lcm}(g_1(x), h_1^*(x)) - \deg\operatorname{lcm}(g_2(x), h_2^*(x))\\
=& (n - \deg\operatorname{lcm}(g_1(x), h_1^*(x))) + (n - \deg\operatorname{lcm}(g_2(x), h_2^*(x)))\\
=& \left(\sum_{j\in\overline{n}, j\in N_2} \operatorname{ord}_j(2) \sum_{i=1}^{\gamma(j)} 2^\nu + \sum_{j\in\overline{n}, j\notin N_2} \operatorname{ord}_j(2) \sum_{i=1}^{\beta(j)} 2^{\nu+1} \right) -\\
& \left(\sum_{j\in\overline{n}, j\in N_2} \operatorname{ord}_j(2) \sum_{i=1}^{\gamma(j)} \max\{a_{ij}, 2^\nu - a_{ij}\} + \right.\\
& \left. \sum_{j\in\overline{n}, j\notin N_2} \operatorname{ord}_j(2) \sum_{i=1}^{\beta(j)} (\max\{b_{ij}, 2^\nu - c_{ij}\} + \max\{c_{ij}, 2^\nu - b_{ij}\}) \right) +
\end{aligned}
$$

$$\begin{aligned}
&\left(\sum_{j\in\overline{n},j\in N_2}\mathrm{ord}_j(2)\sum_{i=1}^{\gamma(j)}2^{\nu}+\sum_{j\in\overline{n},j\notin N_2}\mathrm{ord}_j(2)\sum_{i=1}^{\beta(j)}2^{\nu+1}\right)-\left(\sum_{j\in\overline{n},j\in N_2}\mathrm{ord}_j(2)\sum_{i=1}^{\gamma(j)}\max\{u_{ij},2^{\nu}-u_{ij}\}\right.\\
&\left.+\sum_{j\in\overline{n},j\notin N_2}\mathrm{ord}_j(2)\sum_{i=1}^{\beta(j)}(\max\{v_{ij},2^{\nu}-w_{ij}\}+\max\{w_{ij},2^{\nu}-v_{ij}\})\right)\\
=&\left(\sum_{j\in\overline{n},j\in N_2}\mathrm{ord}_j(2)\sum_{i=1}^{\gamma(j)}(2^{\nu}-\max\{a_{ij},2^{\nu}-a_{ij}\})+\right.\\
&\left.\sum_{j\in\overline{n},j\notin N_2}\mathrm{ord}_j(2)\sum_{i=1}^{\beta(j)}\left(2^{\nu+1}-(\max\{b_{ij},2^{\nu}-c_{ij}\}+\max\{c_{ij},2^{\nu}-b_{ij}\})\right)\right)+\\
&\left(\sum_{j\in\overline{n},j\in N_2}\mathrm{ord}_j(2)\sum_{i=1}^{\gamma(j)}(2^{\nu}-\max\{u_{ij},2^{\nu}-u_{ij}\})+\right.\\
&\left.\sum_{j\in\overline{n},j\notin N_2}\mathrm{ord}_j(2)\sum_{i=1}^{\beta(j)}\left(2^{\nu+1}-(\max\{v_{ij},2^{\nu}-w_{ij}\}+\max\{w_{ij},2^{\nu}-v_{ij}\})\right)\right)\\
=&\sum_{j\in\overline{n},j\in N_2}\mathrm{ord}_j(2)\sum_{i=1}^{\gamma(j)}\left(2^{\nu+1}-\max\{a_{ij},2^{\nu}-a_{ij}\}-\max\{u_{ij},2^{\nu}-u_{ij}\}\right)+\\
&\sum_{j\in\overline{n},j\notin N_2}\mathrm{ord}_j(2)\sum_{i=1}^{\beta(j)}\left(2^{\nu+2}-(\max\{b_{ij},2^{\nu}-c_{ij}\}+\max\{c_{ij},2^{\nu}-b_{ij}\})-\right.\\
&\left.(\max\{v_{ij},2^{\nu}-w_{ij}\}+\max\{w_{ij},2^{\nu}-v_{ij}\})\right) \qquad (3.3)\\
=&\sum_{j\in\overline{n},j\in N_2}\mathrm{ord}_j(2)\cdot a_j+\sum_{j\in\overline{n},j\notin N_2}\mathrm{ord}_j(2)\cdot b_j \qquad \text{by Lemma 3.2}
\end{aligned}$$

where $0 \leq a_j \leq 2^{\nu}$ and $0 \leq b_j \leq 2^{\nu+1}$. □

Example 3.4. *Let $n = 14$. Then $\overline{n} = 7$ and $\nu = 1$. The divisors of 7 are 1 and 7. Note that $1 \in N_2$ and $7 \notin N_2$. Since $\mathrm{ord}_1(2) = 1$ and $\mathrm{ord}_7(2) = 3$, by Theorem 3.3, the 2-dimensions of the hulls of cyclic codes of length 14 over $\mathcal{R}$ are of the form*

$$a_1 + 3 \cdot b_7,$$

where $0 \leq a_1 \leq 2$ and $0 \leq b_7 \leq 4$, which are $0, 1, 2, \ldots, 13$ and 14.

4 The Average 2-Dimension $E(n)$ and Bounds on $E(n)$

In this section, an explicit expression for the average 2-dimension $E(n)$ of the hull of cyclic codes over $\mathcal{R}$ is given in terms of $B_{\overline{n}}$ and the length of codes. Subsequently, some bounds on $E(n)$ are given together with the asymptotic behavior of $E(n)$.

Lemma 4.1. *Let ν be a nonnegative integer and let $0 \leq a, b, c \leq 2^{\nu}$ be integers. Then*

1. *$E\left(\max\{a, 2^{\nu} - a\}\right) = \frac{3\cdot 2^{\nu}+1}{4} - \frac{\delta_{2^{\nu}}}{4(2^{\nu}+1)}$ and*

2. *$E\left(\max\{b, 2^{\nu} - c\}\right) = \frac{2^{\nu}(4\cdot 2^{\nu}+5)}{6(2^{\nu}+1)}$,*

where $\delta_{2^{\nu}} = 1$ if $\nu > 0$, and $\delta_{2^{\nu}} = 0$ if $\nu = 0$.

Proof. The statements can be obtained using arguments similar to those in the proof of [3, Theorem 23]. □

The formula for the average 2-dimension of the hull of cyclic codes of length n over $\mathcal{R}$ is given as follows.

Theorem 4.2. *Let n be a positive integer and write $n = 2^\nu \overline{n}$, where $\overline{n}$ is odd and $\nu \geq 0$ is an integer. The average 2-dimension of the hull of cyclic codes of length n over $\mathcal{R}$ is*

$$E(n) = n\left(\frac{2^{\nu+1}+1}{3(2^\nu+1)}\right) - B_{\overline{n}}\left(\frac{2^{2\nu}+2^{\nu+1}+3-3\delta_{2^\nu}}{12(2^\nu+1)}\right).$$

Proof. Let C be a cyclic code of length n over $\mathcal{R}$. Then, by Theorem 3.1, $\mathrm{Hull}(C)$ is generated by

$$\left((1+v)\operatorname{lcm}(g_1(x),h_1^*(x)), v\operatorname{lcm}(g_2(x),h_2^*(x))\right).$$

Then

$$\begin{aligned}\dim_2 \mathrm{Hull}(C) =& 2n - \deg\operatorname{lcm}(g_1(x),h_1^*(x)) - \deg\operatorname{lcm}(g_2(x),h_2^*(x)\\ =& \left(n - \deg\operatorname{lcm}(g_1(x),h_1^*(x))\right) + \left(n - \deg\operatorname{lcm}(g_2(x),h_2^*(x)\right)\end{aligned}$$

Let Y be the random variable of the 2-dimension $\dim_2(C)$, where C is chosen randomly form $\mathcal{C}(n)$ with uniform probability. The average 2-dimension $E(n)$ can be determined in terms of the expectation $E(Y)$ as follows

$$\begin{aligned}E(n) =& E(Y)\\ =& E\left(n - \deg\operatorname{lcm}(g_1(x),h_1^*(x))\right) + E\left(n - \deg\operatorname{lcm}(g_2(x),h_2^*(x)\right)\\ =& n - E\left(\sum_{j\in\overline{n}, j\in N_2} \operatorname{ord}_j(2)\sum_{i=1}^{\gamma(j)} \max\{a_{ij}, 2^\nu - a_{ij}\}\right.\\ &\left. + \sum_{j\in\overline{n}, j\notin N_2} \operatorname{ord}_j(2)\sum_{i=1}^{\beta(j)} \left(\max\{b_{ij}, 2^\nu - c_{ij}\} + \max\{c_{ij}, 2^\nu - b_{ij}\}\right)\right) +\\ & n - E\left(\sum_{j\in\overline{n}, j\in N_2} \operatorname{ord}_j(2)\sum_{i=1}^{\gamma(j)} \max\{u_{ij}, 2^\nu - u_{ij}\}\right.\\ &\left. + \sum_{j\in\overline{n}, j\notin N_2} \operatorname{ord}_j(2)\sum_{i=1}^{\beta(j)} \left(\max\{v_{ij}, 2^\nu - w_{ij}\} + \max\{w_{ij}, 2^\nu - v_{ij}\}\right)\right)\\ =& n - \sum_{j\in\overline{n}, j\in N_2} \operatorname{ord}_j(2)\cdot\gamma(j)\cdot E(\max\{a_{ij}, 2^\nu - a_{ij}\})\\ & - \sum_{j\in\overline{n}, j\notin N_2} \operatorname{ord}_j(2)\cdot\beta(j)\cdot E\left(\max\{b_{ij}, 2^\nu - c_{ij}\} + \max\{c_{ij}, 2^\nu - b_{ij}\}\right) +\\ & n - \sum_{j\in\overline{n}, j\in N_2} \operatorname{ord}_j(2)\cdot\gamma(j)\cdot E(\max\{u_{ij}, 2^\nu - u_{ij}\})\\ & - \sum_{j\in\overline{n}, j\notin N_2} \operatorname{ord}_j(2)\cdot\beta(j)\cdot E\left(\max\{v_{ij}, 2^\nu - w_{ij}\} + \max\{w_{ij}, 2^\nu - v_{ij}\}\right)\end{aligned}$$

$$
\begin{aligned}
&= \left(n - \sum_{j\in\overline{n}, j\in N_2} \phi(j)\cdot E(\max\{a_{ij}, 2^{\nu} - a_{ij}\}) \right. \\
&\qquad \left. - \sum_{j\in\overline{n}, j\notin N_2} \phi(j)\cdot \frac{1}{2} \cdot E\left(\max\{b_{ij}, 2^{\nu} - c_{ij}\} + \max\{c_{ij}, 2^{\nu} - b_{ij}\}\right) \right) + \\
&\quad \left(n - \sum_{j\in\overline{n}, j\in N_2} \phi(j)\cdot E(\max\{u_{ij}, 2^{\nu} - u_{ij}\}) \right. \\
&\qquad \left. - \sum_{j\in\overline{n}, j\notin N_2} \phi(j)\cdot \frac{1}{2} \cdot E\left(\max\{v_{ij}, 2^{\nu} - w_{ij}\} + \max\{w_{ij}, 2^{\nu} - v_{ij}\}\right) \right) \\
&= (n - B_{\overline{n}} \cdot E(\max\{a_{ij}, 2^{\nu} - a_{ij}\}) - (\overline{n} - B_{\overline{n}}) \cdot E(\max\{b_{ij}, 2^{\nu} - c_{ij}\})) + \\
&\quad (n - B_{\overline{n}} \cdot E(\max\{u_{ij}, 2^{\nu} - u_{ij}\}) - (\overline{n} - B_{\overline{n}}) \cdot E(\max\{v_{ij}, 2^{\nu} - w_{ij}\})) \\
&=2\left(n - B_{\overline{n}} \cdot E\left(\max\{a_{ij}, 2^{\nu} - a_{ij}\}\right) - (\overline{n} - B_{\overline{n}}) \cdot E\left(\max\{b_{ij}, 2^{\nu} - c_{ij}\}\right)\right) \\
&=2\left(n - B_{\overline{n}}\left(\frac{3\cdot 2^{\nu} + 1}{4} - \frac{\delta_{2^{\nu}}}{4(2^{\nu}+1)}\right) - (\overline{n} - B_{\overline{n}})\left(\frac{2^{\nu}\left(4\cdot 2^{\nu} + 5\right)}{6\left(2^{\nu}+1\right)}\right)\right) \text{by Lemma 4.1} \\
&=2\left(n\left(\frac{1}{3} - \frac{1}{6(2^{\nu}+1)}\right) - B_{\overline{n}}\left(\frac{2^{\nu}+1}{12} + \frac{2 - 3\delta_{2^{\nu}}}{12(2^{\nu}+1)}\right)\right) \\
&=n\left(\frac{2}{3} - \frac{1}{3(2^{\nu}+1)}\right) - B_{\overline{n}}\left(\frac{2^{\nu}+1}{6} + \frac{2 - 3\delta_{2^{\nu}}}{6(2^{\nu}+1)}\right)
\end{aligned}
$$

as required. □

The next corollary follows immediately from Theorem 4.2.

Corollary 4.3. *Let $n = \overline{n}2^{\nu}$, where $\bar{n}$ is odd and $\nu \geq 0$. Then the following statements hold.*

1. $E(n) < \frac{2n}{3}$.
2. $E(\overline{n}) = \frac{\overline{n} - B_{\overline{n}}}{2}$.
3. $E(\overline{n}) < \frac{\overline{n}}{2}$.

In the case where n is odd, we have the following upper and lower bounds.

Theorem 4.1. *Let n be an odd integer. Then the following statements hold.*

1. $E(n) = 0$ *if and only if* $n \in N_2$.
2. $\frac{n}{6} \leq E(n) \leq \frac{2n}{3}$ *for all* $n \notin N_2$.

Proof. Let $E_2(n)$ denote the average hull dimension of cyclic codes of length n over $\mathbb{F}_2$. By [3, Corollary 11] and Theorem 4.2, we have $E(n) = 2E_2(n)$. The results can be derived analogous to [3, Theorem 25]. □

From Theorem 4.1, we can conclude that the average 2-dimension of the hull of cyclic codes of odd length n over $\mathcal{R}$ is zero or grows the same rate as n.

Acknowledgments : This research was supported by the Thailand Research Fund and the Office of Higher Education Commission of Thailand under Research Grant MRG6080054.

References

[1] E. F. Assmus, J. D. Key, Affine and projective planes, *Discrete Math.*, **83** (1990) 161–187.

[2] E. Sangwisut, S. Jitman, S. Ling, P. Udomkavanich, Hulls of cyclic and negacyclic codes over finite fields, *Finite Fields Appl.*, **33** (2015) 232–257.

[3] G. Skersys, The average dimension of the hull of cyclic codes, *Discrete Appl. Math.*, **128** (2003) 275–292.

[4] N. Sendrier, On the dimension of the hull, *SIAM J. Appl. Math.*, **10** (1997) 282–293.

[5] S. Jitman, E. Sangwisut, The average dimension of the Hermitian hull of cyclic codes over finite fields of square order, *AIP Proceeding of the International Conference on Mathematics, Engineering and Industrial Applications (IC0MEIA2016)*, **1775** (2016) 030026-1 – 030026-8.

[6] S. Jitman, E. Sangwisut, The average dimension of the Hermitian hull of constacyclic codes over finite fields, Adv. Math. Commun. **12** (2018) 451–463.

[7] S. Jitman, E. Sangwisut, The average hull dimension of negacyclic codes over finite fields, Mathematical and Computational Applications 23, Article ID 41 (2018).

[8] A. R. Calderbank, A. R. Hammons, Jr., P. V. Kumar, N. J. A. Sloane and P. Sole, A linear construction for certain Kerdock and Preparata codes, Bull. AMS **23** (1993) 218–222.

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

[10] S. Jitman, E. Sangwisut, P. Udomkavanich, Hulls of Cyclic Codes over $\mathbb{Z}_4$, preprint (2018), available at https://arxiv.org/abs/1806.07590.

[11] Y. Yang, W Cai On self-dual constacyclic codes over finite fields. *Des. Codes Cryptogr.* **74** (2015) 355–64.

[12] S. Zhu, Y. Wang, M. Shi, Cyclic codes over $\mathbb{F}_2 + v\mathbb{F}_2$, *IEEE Trans. Inform. Theory*, **56** (2010) 1680 – 1684.

(Received 21 November 2018)
(Accepted 27 June 2019)