




## On the covering radii of a class of binary primitive cyclic codes

Seher Tutdere 

*Department of Mathematics, Faculty of Science and Letters, Balıkesir University, Balıkesir, Turkey*

### Abstract

In 2019, Kavut and Tutdere proved that the covering radii of a class of primitive binary cyclic codes with minimum distance greater than or equal to  $r + 2$  is  $r$ , where  $r$  is an odd integer, under some assumptions. We here show that the covering radii  $R$  of a class of primitive binary cyclic codes with minimum distance strictly greater than  $\ell$  satisfy  $r \leq R \leq \ell$ , where  $\ell, r$  are some integers, with  $\ell$  being odd, depending on the given code. This new class of cyclic codes covers that of Kavut and Tutdere.

**Mathematics Subject Classification (2020).** 94B15, 94B65

**Keywords.** cyclic code, covering radius, finite field, polynomial equations

### 1. Introduction

Let  $\mathbb{F}_q$  be a finite field, with  $q = 2^f$  where  $f \geq 1$  is an integer, and  $C$  be a binary cyclic  $[n, k, d]$  code having length  $n$ , dimension  $k$ , and minimum distance  $d := d(C)$ . The covering radius  $R(C)$  of the code  $C$  is the smallest integer  $r$  such that every  $q$ -ary  $(n - k)$  tuple can be written as a linear combination of at most  $r$  columns of the parity-check matrix of  $C$ . Equivalently, the covering radius of a code is the maximal distance of any vector from the code, i.e.,  $R(C) := \max\{\min\{d(x, c) : x \in \mathbb{F}_q, c \in C\}\}$ , where  $d(., .)$  is the Hamming distance. It has applications in the theory of communications, e.g. data compression, testing, and write-once memories, for instance see [2].

The covering radii of cyclic codes has been studied by many researchers since the paper [5] of Delsarte in 1973, for instance see [2–4, 7, 9, 10]. Let  $\alpha$  be a primitive root of  $\mathbb{F}_{2^f}$  and  $C$  be a primitive binary cyclic code. In [10, Theorem 6], Moreno and Castro proved that if the zeros of  $C$  are  $\alpha, \alpha^{2^i+1}$  with  $(i, f) = 1$ , then  $R(C) = 3$ , where  $d(C) = 5$  [12]. They also showed that if the zeros of  $C$  are  $\alpha, \alpha^{2^i+1}, \alpha^{2^j+1}$  with distinct positive integers  $i, j$  and  $d(C) = 7$ , then  $R(C) = 5$  for  $f > 8$  [10, Theorem 9]. In [9], Kavut and Tutdere gave a generalization of the aforementioned results of Moreno and Castro as follows: if the zeros of  $C$  are  $\alpha, \alpha^{2^{i_1}+1}, \dots, \alpha^{2^{i_t}+1}$ , where  $t = (r - 1)/2$ ,  $r$  is any odd integer such that  $d(C) \geq r + 2$ , then  $R(C) = r$ , under some restrictions on  $f$  and  $r$ . We here show the following: if the zeros of  $C$  are  $\alpha^{d_0}, \alpha^{d_1}, \dots, \alpha^{d_t}$ , where  $d_i$ 's are distinct positive integers, and the sum of 2-weights of  $d_i$ 's, which we call  $\ell$ , is odd such that  $d(C) > \ell$ , then  $r \leq R(C) \leq \ell$ , under some assumptions on  $f$  and  $r$ . We give a proof by generalizing the

methods of [9] and [10]. This new class of cyclic codes covers that of [9], for which  $r = \ell$  holds, and so the exact value of  $R(C)$  is obtained.

The paper is organized as follows: In Section 2, we give some basic background and known results which will be used in the subsequent sections. In Section 3, we give the main results and the last section is devoted to some examples.

## 2. Preliminaries

Let  $\mathbb{F}_q$  be a finite field, with  $q = 2^f$  where  $f \geq 1$  is an integer. For simplicity, by a code  $C$  we mean a binary primitive cyclic  $[n, k, d]$  code having length  $n := q - 1$ , dimension  $k$ , minimum distance  $d := d(C)$ , and covering radius  $R := R(C)$ . It is well-known that there exists a unique monic polynomial  $g(x) \in \mathbb{F}_2[x]$  such that  $C = \langle g(x) \rangle = \{h(x)g(x) \mid h(x) \in \mathbb{F}_2[x] \text{ with } \deg h(x) < k\}$ . The polynomial  $g(x)$ , which is called the *generator* of  $C$ , has  $\deg g(x) = n - k$  and  $g(x) \mid (x^n - 1)$ . Hence, the roots of  $g(x)$  lie in the field  $\mathbb{F}_{2^f}$ . Let  $\alpha$  be a primitive element of  $\mathbb{F}_{2^f}$ . The set  $D_C := \{i : g(\alpha^i) = 0\}$  is called the *defining set* of  $C$ . For any  $r \geq 0$ , the set  $M_r := \{rq^j \bmod n \mid j = 0, \dots, n_r - 1\}$ , where  $n_r$  is the smallest integer such that  $rq^{n_r} \equiv r \pmod n$ , is called a *cyclotomic coset* of  $r$ . The minimal polynomial of any  $\alpha^r$  is given by  $M_r(x) = \prod_{i \in M_r} (x - \alpha^i)$ . Then the defining set  $D_C$  can be written as a disjoint union of  $w$  cyclotomic cosets, i.e.,  $D_C = M_{r_1} \cup M_{r_2} \cup \dots \cup M_{r_w}$ . Hence,  $g(x) = \prod_{i=1}^w M_{r_i}(x)$ . For each  $i = 1, \dots, w$ , we call  $\alpha^{r_i}$  a *zero* of the code  $C$  and we denote by  $Z(C) := \{\alpha^{r_i} \mid i = 1, \dots, w\}$  the set of all zeros of  $C$ .

Throughout this paper, we consider binary primitive cyclic codes with  $n = 2^f - 1$ , and  $\alpha$  denotes a primitive element of  $\mathbb{F}_{2^f}$ . We begin with the following result of [9].

**Theorem 2.1.** [9, Theorem 2] *Suppose that  $C_1$  is a primitive binary cyclic code such that  $Z(C_1) = \{\alpha, \alpha^{2^{i_1}+1}, \alpha^{2^{i_2}+1}, \dots, \alpha^{2^{i_{t-1}}+1}\}$  for some distinct positive integers  $i_1, i_2, \dots, i_{t-1}$ , with  $t = \frac{r-1}{2}$ , and  $d(C_1) = r$  for some odd integer  $r$ . Let  $C_2$  be a code with  $Z(C_2) = Z(C_1) \cup \{\alpha^{2^{i_t}+1}\}$  where  $0 < i_t \neq i_1, \dots, i_{t-1}$ . If  $d(C_2) \geq r + 2$ , then  $R(C_2) = r$  for  $f > 2(r - s)$ , where  $s$  is the largest integer such that  $2^s \mid (r + 1)$ .*

We here give a generalization of Theorem 2.1. Our method is based on the technique of [9] and [10], which essentially arises from the following fact. Recall that for a binary primitive cyclic code  $C$  of length  $n$ , with the set of zeros  $\{\alpha^{d_0}, \alpha^{d_1}, \dots, \alpha^{d_w}\}$ , has a parity-check matrix

$$H = \begin{bmatrix} 1 & \alpha^{d_0} & \alpha^{2d_0} & \dots & \alpha^{(n-1)d_0} \\ 1 & \alpha^{d_1} & \alpha^{2d_1} & \dots & \alpha^{(n-1)d_1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{d_w} & \alpha^{2d_w} & \dots & \alpha^{(n-1)d_w} \end{bmatrix},$$

where each entry is represented as a column vector in  $\mathbb{F}_2^f$  according to some basis of  $\mathbb{F}_{2^f}$  over  $\mathbb{F}_2$ . Set  $F^{(t)}(x_1, \dots, x_r) := x_1^t + x_2^t + \dots + x_r^t \in \mathbb{F}_{2^f}[x_1, \dots, x_r]$  with  $t \geq 1$ . It is well-known that if the system

$$F^{(d_0)}(x_1, \dots, x_r) = \beta_0, F^{(d_1)}(x_1, \dots, x_r) = \beta_1, \dots, F^{(d_w)}(x_1, \dots, x_r) = \beta_w$$

has a solution  $(x_1, x_2, \dots, x_r) \in \mathbb{F}_{2^f}^r$  for each  $(\beta_0, \beta_1, \dots, \beta_w) \in \mathbb{F}_{2^f}^{(w+1)}$ , then the code  $C$  has covering radius at most  $r$ .

Next, we give the following notion which will be used frequently throughout the paper.

**Definition 2.2.** Let  $p$  be a prime number and  $n$  be an integer with  $p$ -*expansion*

$$n = a_0 + a_1p + \dots + a_sp^s, \quad \text{where } 0 \leq a_i < p.$$

The sum  $\sigma_p(n) := \sum_{i=0}^s a_i$  is called the  $p$ -weight of  $n$  and the  $p$ -weight degree of a monomial  $x^d = x_1^{d_1} x_2^{d_2} \dots x_n^{d_n}$  is defined as

$$w_p(x^d) := \sigma_p(d_1) + \dots + \sigma_p(d_n).$$

The  $p$ -weight degree of a polynomial  $F(x_1, x_2, \dots, x_n) = \sum_d a_d x^d$  is

$$w_p(F) := \max_{x^d, a_d \neq 0} w_p(x^d).$$

The following result of Moreno-Moreno [11] on the divisibility of the number of solutions of a system of polynomial equations plays a crucial role in the proof of our main result.

**Theorem 2.3.** [11, Theorem 1] *Let  $F_1, F_2, \dots, F_t$  be polynomials in  $n$  variables with coefficients in  $\mathbb{F}_{p^f}$ ,  $\ell_i := w_p(F_i)$  be the  $p$ -weight degree of  $F_i$ , and*

$$\mu := \left\lceil f \left( \frac{n - \sum_{i=1}^t \ell_i}{\max_i \ell_i} \right) \right\rceil.$$

*Then  $p^\mu$  divides the number of solutions of the system of the polynomial equations  $F_1 = 0, \dots, F_t = 0$ .*

The following very significant result of Gorenstein, Peterson and Zierler [6] will be often used in the subsequent sections.

**Proposition 2.4** (Supercode Lemma). *Let  $C$  and  $C'$  be linear codes such that  $C \subset C'$ . Then  $R(C) \geq d(C')$ .*

### 3. The covering radii of a class of binary primitive cyclic codes

In this section we give our main result, which is a generalization of Theorem 2.1, see Remark 3.2.

**Theorem 3.1.** *Let  $C$  be a primitive binary cyclic code with the zero set  $Z(C) = \{\alpha^{d_0}, \dots, \alpha^{d_t}\}$  for some distinct positive integers  $d_0, d_1, \dots, d_t$ . Suppose that there is a code  $C'$  such that  $C \subset C'$  and  $d(C') = r$  for any integer  $r$ . Assume that the sum  $\ell := \sum_{i=0}^t \sigma_2(d_i)$  is an odd integer. If  $d(C) > \ell$ , then  $r \leq R(C) \leq \ell$  for  $f > (\ell - s) \max_i \sigma_2(d_i)$ , where  $s$  is the largest integer such that  $2^s | (\ell + 1)$ .*

**Proof.** We give a proof by generalizing the method used in the proof of Theorem 2.1 given in [9]. Let  $C$  and  $C'$  be the codes as in the theorem. Since  $C \subset C'$ , by Proposition 2.4,  $R(C) \geq d(C') = r$ . We only need to show that  $R(C) \leq \ell$ . It is enough to show that the following system of polynomial equations has a solution  $(x_1, x_2, \dots, x_\ell) \in \mathbb{F}_{2^f}^\ell$  for each  $\beta = (\beta_0, \beta_1, \beta_2, \dots, \beta_t) \in \mathbb{F}_{2^f}^{t+1}$ :

$$\begin{aligned} x_1^{d_0} + x_2^{d_0} + \dots + x_\ell^{d_0} &= \beta_0, \\ x_1^{d_1} + x_2^{d_1} + \dots + x_\ell^{d_1} &= \beta_1, \\ &\vdots \\ x_1^{d_t} + x_2^{d_t} + \dots + x_\ell^{d_t} &= \beta_t. \end{aligned} \tag{3.1}$$

We add a new variable  $x_{\ell+1}$  as follows:

$$\begin{aligned} x_1^{d_0} + x_2^{d_0} + \dots + x_\ell^{d_0} &= \beta_0(x_{\ell+1})^{d_0}, \\ x_1^{d_1} + x_2^{d_1} + \dots + x_\ell^{d_1} &= \beta_1(x_{\ell+1})^{d_1}, \\ &\vdots \\ x_1^{d_t} + x_2^{d_t} + \dots + x_\ell^{d_t} &= \beta_t(x_{\ell+1})^{d_t}. \end{aligned} \tag{3.2}$$

By applying Theorem 2.3 with  $n = \ell + 1$ , we obtain that the number of solutions of the system (3.2) is divisible by  $2^{\lceil \frac{f}{m} \rceil}$  with  $m := \max_i \sigma_2(d_i)$ . To show that the system (3.1) has a solution, it is enough to prove that the system (3.2) has a solution with  $x_{\ell+1} \neq 0$ . Suppose that the system (3.2) has no solutions for  $x_{\ell+1} \neq 0$ . Then the system (3.2) reduces to the following form:

$$\begin{aligned} x_1^{d_0} + x_2^{d_0} + \dots + x_\ell^{d_0} &= 0, \\ x_1^{d_1} + x_2^{d_1} + \dots + x_\ell^{d_1} &= 0, \\ &\vdots \\ x_1^{d_t} + x_2^{d_t} + \dots + x_\ell^{d_t} &= 0. \end{aligned} \tag{3.3}$$

Let  $S_\ell$  be the set of solutions of the equation (3.3) and  $s_\ell := |S_\ell|$ . A solution  $(x_1, x_2, \dots, x_\ell)$  of (3.3) is nontrivial if all the  $x_i$ 's are distinct. Because of the assumption that  $d(C) > \ell$ , any  $\ell$  columns of the parity-check matrix  $H$  of  $C$  must be linearly independent. Hence, the system (3.3) cannot have a nontrivial solution. Thus, it is enough to count only trivial solutions, as in the proof of [9, Theorem 2]. We here give the sketch of the computation accordingly as follows. Since by assumption  $d(C) > \ell$ , for any solution  $(x_1, x_2, \dots, x_\ell)$  of (3.3), we have that

$$x_{j_1} = 0, \quad x_{j_2} = x_{j_3}, \quad \dots, \quad x_{j_{\ell-1}} = x_{j_\ell}, \tag{3.4}$$

where  $j_1, j_2, \dots, j_\ell \in \{1, 2, \dots, \ell\}$ . We need to find the number of solutions of (3.4). Let  $A_i := \{(x_1, x_2, \dots, x_\ell) \in S_\ell : x_i = 0\}$  for  $1 \leq i \leq \ell$ . It is clear that  $S_\ell = \bigcup_{i=1}^{\ell} A_i$ . Thus, to compute  $s_\ell := |S_\ell|$ , we will find  $|A_i|$  for each  $1 \leq i \leq \ell$ , and then  $|A_{t_1} \cap A_{t_2} \dots \cap A_{t_j}|$  for all  $2 \leq j \leq \ell$  and  $1 \leq t_1 < t_2 < \dots < t_j \leq \ell$ . For simplicity, we first set  $q := 2^f$ . One obtains recursively the following for each  $j = 1, 2, \dots, \ell$ :

$$\bigcap_{i=1}^j A_i = \begin{cases} qs_{\ell-j-1} & \text{if } j \text{ is odd} \\ s_{\ell-j} & \text{otherwise.} \end{cases} \tag{3.5}$$

Then by using the principle of inclusion-exclusion, the following recursive equation is obtained:

$$\begin{aligned} s_\ell = |S_\ell| &= \ell qs_{\ell-2} - \binom{\ell}{2} s_{\ell-2} + \binom{\ell}{3} qs_{\ell-4} - \binom{\ell}{4} s_{\ell-4} + \dots \\ &+ \binom{\ell}{\ell-2} qs_1 - \binom{\ell}{\ell-1} s_1 + \binom{\ell}{\ell} \\ &= q \left[ \ell s_{\ell-2} + \binom{\ell}{3} s_{\ell-3} + \dots + \binom{\ell}{\ell-2} s_1 \right] \\ &- \left[ \binom{\ell}{2} s_{\ell-2} + \binom{\ell}{4} s_{\ell-4} + \dots + \binom{\ell}{\ell-1} s_1 \right] + 1 \end{aligned} \tag{3.6}$$

We want to check whether  $2^{\lceil \frac{f}{m} \rceil}$ , where  $m = \max_i \sigma_2(d_i)$ , divides  $s_\ell$  or not. To do this, we only need to find the constant term in the  $q$ -extension of  $s_\ell$ , say  $c_\ell$ , i.e., the term which is not a multiple of  $q$ . It follows from (3.6) that

$$c_\ell = 1 - \binom{\ell}{2} c_{\ell-2} - \binom{\ell}{4} c_{\ell-4} - \dots - \binom{\ell}{\ell-1} c_1 \quad \text{with } c_1 = 1. \tag{3.7}$$

By using generating functions, solving the recurrence relation (3.7) for all odd  $\ell \geq 1$  gives that

$$c_\ell = \frac{2^{\ell+1}(2^{\ell+1} - 1)B_{\ell+1}}{\ell + 1}, \quad (3.8)$$

where  $B_{\ell+1}$  is the  $(\ell+1)$ th Bernoulli number (of first kind). It is a well known fact that any Bernoulli number is of the form  $\frac{\mp 1}{2 \cdot D}$  for some odd integer  $D$  (for instance, see [8, Example 5.3]). Next, by applying Theorem 2.3 with  $n = \ell + 1$ , we obtain that for all  $f > (\ell - s)m$ , with  $m = \max_i \sigma_2(d_i)$ , where  $s$  is the largest integer such that  $2^s | (\ell + 1)$ , we have that  $2^{\lceil \frac{f}{m} \rceil}$  does not divide  $c_\ell$ , which is a contradiction. This implies that Eq. (3.2) has at least one solution for  $x_{\ell+1} \neq 0$ , and so Eq. (3.1) has a solution. Consequently,  $R(C) \leq \ell$  holds.  $\square$

**Remark 3.2.** Theorem 2.1 is a special case of Theorem 3.1 with  $C_1 = C'$ ,  $C_2 = C$ ,  $\max_i \sigma_2(d_i) = 2$ , where  $d_0 = 1, d_1 = 2^{i_1} + 1, \dots, d_t = 2^{i_t} + 1$  and  $t = \frac{r-1}{2}$ , and so  $\ell = 2t + 1 = r$ . Thus,  $R(C) = r$  holds. Note that the minimum distances of a code with the zero set as in Theorem 2.1 is an odd integer, see [9, Remark 1] or [12, Lemma 6].

**Remark 3.3.** We note that the codes in Theorem 3.1 are *maximal* codes (which have no proper supercode with the same length and minimum distance) determined by the condition  $R(C) \leq d(C) - 1$  [3].

**Remark 3.4.** In Theorem 3.1, when  $\ell$  is even, the computation done in the proof of that theorem does not give rise to a contradiction obtained in the last paragraph of the proof. That means; in the even case we could not obtain any result by using this method. Therefore, we consider only the case where  $\ell$  is odd.

## 4. Examples

In this section, we discuss some examples. In Tables 1 and 2,  $d$  and  $R$  denote the minimum distance and the covering radius of a given binary primitive cyclic code  $C$ , respectively. For simplicity, we represent the zero set  $Z(C) = \{\alpha^{d_0}, \alpha^{d_1}, \dots, \alpha^{d_t}\}$  of  $C$  by the set  $\{d_0, d_1, \dots, d_t\}$ , and call it *the representative of the zero set*. In Examples 4.1 and 4.2 we write it as  $Z(C) : \{d_0, d_1, \dots, d_t\}$ . In the tables, we give the exact values of the minimum distance and covering radius of the codes with the given zero sets for  $\mathbb{F}_{2^4}$  and  $\mathbb{F}_{2^5}$ , respectively. The results are obtained by a computer computation. Since for large values of  $f$ , it is not feasible to perform computer computations, we here consider only the values of  $f = 4$  and  $f = 5$ . One can observe from the tables that there are some codes satisfying the conditions of Theorem 3.1 (except the bound of  $f$  which is in general larger than four), as given in the following examples.

**Example 4.1.** Suppose that  $\alpha$  is a primitive element of  $\mathbb{F}_{2^4}$  and  $C, C'$ , and  $\ell$  are as in Theorem 3.1. We can deduce from Table 1 that in the following situations, the conditions  $d(C) > \ell, r \leq R(C) \leq \ell$ , with  $\ell$  being odd, of Theorem 3.1 are satisfied:

- (1)  $Z(C) : \{1, 3\}$  and  $Z(C') : \{1\}$ . We have that  $d(C) = 5$  and  $\ell = d(C') = R(C) = 3$ .
- (2)  $Z(C) : \{1, 3, 5\}$  and  $Z(C') : \{1, 3\}$ . We have that  $d(C) = 7$  and  $\ell = d(C') = R(C) = 5$ .

**Example 4.2.** Suppose that  $\alpha$  is a primitive element of  $\mathbb{F}_{2^5}$  and  $C, C', \ell$  are as in Theorem 3.1. It can be seen from Table 2 that in the following situations, the conditions  $d(C) > \ell, r \leq R(C) \leq \ell$ , with  $\ell$  being odd, of Theorem 3.1 are satisfied:

- (1)  $Z(C) : \{1, d\}$ , where  $d = 3$  or  $5$ , and  $Z(C') : \{1\}$ . Then  $d(C) = 5$  and  $\ell = d(C') = R(C) = 3$ .
- (2)  $Z(C) : \{1, 3, 5\}$  and  $Z(C') = \{1, 3\}$ . Then  $d(C) = 7$  and  $\ell = d(C') = R(C) = 5$ .
- (3)  $Z(C) : \{1, 3, 5, 15\}$  and  $Z(C') = \{1, 5, 15\}$ . Then  $d(C) = 11, \ell = 9, d(C') = 6$ , and  $R(C) = 7$ .

- (4)  $Z(C) : \{1, 3, 5, 7, 11\}$  and  $Z(C') = \{1, 3, 5, 7\}$ . Then  $d(C) = 15$  and  $\ell = d(C') = R(C) = 11$ .
- (5)  $Z(C) : \{1, 5, 7, 11, 15\}$  and  $Z(C') : \{1, 5, 7, 11\}$ . Then  $d(C) = 15$ ,  $\ell = 13$ , and  $d(C') = R(C) = 11$ .
- (6)  $Z(C) : \{1, 3, 5, 7, 11, 15\}$  and  $Z(C') : \{1, 5, 7, 11, 15\}$ . Then  $d(C) = 31$  and  $\ell = d(C') = R(C) = 15$ .

**Table 1.** Representatives of the zero sets,  $d$  and  $R$  for  $\mathbb{F}_{2^4}$ .

Representative of the zero set	$d$	$R$
$\{1\}$ or $\{7\}$	3	1
$\{3\}$	2	2
$\{5\}$	2	1
$\{1, 3\}$ or $\{3, 7\}$	5	3
$\{1, 5\}$ or $\{1, 7\}$	3	3
$\{3, 5\}$	4	3
$\{5, 7\}$	3	3
$\{1, 3, 5\}$ or $\{3, 5, 7\}$	7	5
$\{1, 3, 7\}$	5	6
$\{1, 5, 7\}$	3	5
$\{1, 3, 5, 7\}$	15	7

**Table 2.** Representatives of the zero sets,  $d$  and  $R$  for  $\mathbb{F}_{2^5}$ .

Representative of the zero set	$d$	$R$
$\{1\}, \{3\}, \{5\}, \{7\}, \{11\},$ or $\{15\}$	3	1
$\{d_1, d_2\}$ for $d_1, d_2 \in \{1, 3, 5, 7, 11, 15\}$	5	3
$\{1, 3, 5\}, \{1, 3, 11\}, \{1, 5, 7\}, \{1, 7, 11\},$ $\{3, 5, 15\}, \{3, 11, 15\}, \{5, 7, 15\}$ or $\{7, 11, 15\}$	7	5
$\{1, 3, 15\}, \{1, 5, 11\}, \{1, 7, 15\}, \{3, 5, 7\},$ $\{3, 7, 11\}, \{5, 11, 15\},$	5	5
$\{1, 3, 7\}, \{1, 5, 15\}, \{1, 11, 15\}, \{3, 5, 11\},$ $\{3, 7, 15\}, \{5, 7, 11\}$	6	5
$\{1, 3, 5, 7\}, \{1, 3, 5, 11\}, \{1, 3, 5, 15\},$ $\{1, 3, 7, 11\}, \{1, 3, 11, 15\}, \{1, 5, 7, 11\},$ $\{1, 5, 7, 15\}, \{1, 7, 11, 15\}, \{3, 5, 7, 15\}, \{3, 5, 11, 15\},$ $\{3, 7, 11, 15\}, \{5, 7, 11, 15\},$	11	7
$\{1, 3, 7, 15\}, \{1, 5, 11, 15\}, \{3, 5, 7, 11\}$	10	8
$\{1, 3, 5, 7, 11\}, \{1, 3, 5, 7, 15\},$ $\{1, 3, 5, 11, 15\}, \{1, 3, 7, 11, 15\}, \{1, 5, 7, 11, 15\}, \{3, 5, 7, 11, 15\}$	15	11
$\{1, 3, 5, 7, 11, 15\}$	31	15

## 5. Conclusion

In this study, we show that the covering radii  $R$  of a class of primitive binary cyclic codes with minimum distance strictly greater than an odd integer  $\ell$  satisfy  $r \leq R \leq \ell$ , where  $\ell, r$  are some integers determined by the given code. This new class of cyclic codes covers that of Kavut and Tutdere [9], where the equality holds, i.e., the exact value of  $R$  is obtained. We use a generalization of the methods of [9] and [10]. Moreover, we give some examples

in the cases of  $\mathbb{F}_{2^4}$  and  $\mathbb{F}_{2^5}$ . We note that finding good bounds (possibly the exact value) of the covering radii of irreducible Goppa codes is a hard task [1]. Performing a study on the method that we used here to obtain bounds on the covering radii of irreducible Goppa codes could be a future work.

### References

- [1] S.V. Bezzateev and N.A. Shekhunova, *Lower Bounds on the Covering Radius of the Non-Binary and Binary Irreducible Goppa Codes*, IEEE Trans. Inform. Theory **64** (11), 7171–7177, 2018.
- [2] G.D. Cohen, I. Honkala, S. Litsyn and A. Lobstein, *Covering Codes*, Elsevier, 1997.
- [3] G.D. Cohen, M.G. Karpovsky, H.F. Jr. Mattson and J.R. Schatz, *Covering radius-survey and recent results*, IEEE Trans. Inform. Theory **31** (3), 328–343, 1985.
- [4] G.D. Cohen, S.N. Litsyn, A.C. Lobstein and H.F. Jr. Mattson, *Covering radius 1985–1994*, Appl. Algebra Engrg. Comm. Comput. **8** (3), 173–239, 1997.
- [5] P. Delsarte, *Four fundamental parameters of a code and their combinatorial significance*, Inf. Control **23**, 407–438, 1973.
- [6] D. Gorenstein, W.W. Peterson and N. Zierler, *Two-error correcting Bose-Chaudhuri codes are quasi-perfect*, Inf. Control **3** (3), 291–294, 1960.
- [7] T. Helleseth, *On the covering radius of cyclic linear codes and arithmetic codes*, Discrete Appl. Math. **11.2**, 157–173, 1985.
- [8] F.T. Howard, *The power of 2 dividing the coefficients of certain power series*, Fibonacci Quart. **39** (4), 358–363, 2001.
- [9] S. Kavut and S. Tutdere, *The covering radii of a class of binary cyclic codes and some BCH codes*, Des. Codes Cryptogr. **87**, 317–325, 2019.
- [10] O. Moreno and N.F. Castro, *Divisibility properties for covering radius of certain cyclic codes*, IEEE Trans. Inform. Theory **49** (12), 3299–3303, 2003.
- [11] O. Moreno and C.J. Moreno, *Improvement of Chevalley-Waring and the Ax-Katz Theorems*, Amer. J. Math. **117** (1), 241–244, 1995.
- [12] J.H. Van Lint and R. Wilson, *On the minimum distance of cyclic codes*, IEEE Trans. Inform. Theory **32** (1), 23–40, 1986.