

On covering radius of generalized Zetterberg codes

Maosheng Xiong*, Haode Yan†

*Department of Mathematics, The Hong Kong University of Science and Technology,
Hong Kong, P. R. China.

†School of Science, Harbin Institute of Technology, Shenzhen, 518055, China.

E-mail: mamsxiong@ust.hk, hdyan@swjtu.edu.cn

Abstract

We employ analytic number-theoretic techniques—specifically, character sums and Weil-type estimates—to study the covering radius of the generalized Zetterberg codes $C_s(q_0)$ of length $q_0^s + 1$ and dimension $q_0^s + 1 - 2s$ over the finite field $\mathbb{F}_{q_0}$. Although the even- and odd-field cases require distinct technical treatment, the proofs follow a unified analytic framework that is substantially simpler and more transparent than previous approaches. We prove that $\rho(C_s(q_0)) \leq 3$ for all q_0 and s , and determine its exact value for a wide range of s for each q_0 . When q_0 is even, our results fill the gap left by recent studies focused solely on odd q_0 ; for odd q_0 , the range of s for which $\rho(C_s(q_0))$ is exactly determined is considerably broader than previously known. Combined with the corresponding minimum distance results, we obtain infinitely many quasi-perfect and maximal codes within this family.

Keywords: covering radius, Zetterberg code, quasi-perfect code, maximal code, character sum

Mathematics Subject Classification: 94B05, 11T71

I. INTRODUCTION

A. The covering radius

Let $\mathbb{F}_{q_0}$ denote the finite field of q_0 elements, where q_0 is a prime power. Let n be a positive integer. For two vectors $\mathbf{x} = (x_1, \dots, x_n), \mathbf{y} = (y_1, \dots, y_n) \in \mathbb{F}_{q_0}^n$, their *Hamming distance* is

$$d_H(\mathbf{x}, \mathbf{y}) = \#\{i : x_i \neq y_i\}.$$

Here $\#I$ denotes the cardinality of a finite set I . Any subset $C \subseteq \mathbb{F}_{q_0}^n$ is called a *code* of length n over $\mathbb{F}_{q_0}$. The *covering radius* of C is defined as

$$\rho(C) = \max_{\mathbf{x} \in \mathbb{F}_{q_0}^n} d_H(\mathbf{x}, C), \quad d_H(\mathbf{x}, C) = \min_{\mathbf{c} \in C} d_H(\mathbf{x}, \mathbf{c}).$$

Equivalently, $\rho(C)$ is the smallest integer r such that the Hamming spheres of radius r centered at the codewords cover $\mathbb{F}_{q_0}^n$. This parameter provides a fundamental geometric measure of how densely the codewords of C occupy the ambient space.

The covering radius is a fundamental concept in coding theory and discrete mathematics. It arises naturally in **decoding**, where $\rho(C)$ represents the maximum number of errors a received word may contain before becoming ambiguous under nearest-neighbor decoding; in **data compression** and **quantization**, where it corresponds to the worst-case distortion under nearest-codeword approximation and relates to sphere-covering problems; and in **testing**, **fault detection**, and **memory coding**, where it measures the completeness of test sets and the robustness of storage schemes. Comprehensive treatments of these topics can be found in the standard monographs and surveys [6, 10–12]. In **finite geometry**, the covering radius is closely related to the study of complete caps in projective spaces; see, for instance, [7, 14, 17, 30] for representative research contributions and further developments.

Beyond these applications, the covering radius lies at the core of several notions of optimality in coding theory, giving rise to perfect, quasi-perfect, and maximal codes—classes that represent extremal configurations of the Hamming space. The following discussion recalls these definitions and their relation to $\rho(C)$.

It is well known that

$$\left\lfloor \frac{d(C) - 1}{2} \right\rfloor \leq \rho(C).$$

A code satisfying

$$\rho(C) = \left\lfloor \frac{d(C) - 1}{2} \right\rfloor$$

is called *perfect*; such codes partition the Hamming space into disjoint Hamming spheres and simultaneously achieve optimal error-correction capability and maximum packing efficiency. When

$$\rho(C) = \left\lfloor \frac{d(C) - 1}{2} \right\rfloor + 1, \quad (1)$$

the code is termed *quasi-perfect*, extending the perfect packing by one additional layer.

The parameters of all perfect codes over finite fields were completely determined in the 1970s [50, 51], and the classification of linear perfect codes is now fully known (see [35]). Only a few exceptional families—notably the Hamming and Golay codes—attain this equality. By contrast, the classification of quasi-perfect codes remains substantially more complicated. Consequently, recent research has focused on constructing explicit families of quasi-perfect codes with diverse parameters (see, e.g., [15, 16, 20, 21, 24, 31, 32, 37]); see also [46–48] for several of the latest developments.

A code C is *maximal* if it cannot be strictly contained in a larger code with the same minimum distance. Equivalently [12], a maximal code satisfies

$$\rho(C) \leq d(C) - 1, \quad (2)$$

meaning that every vector of the Hamming space lies within distance $d(C) - 1$ from C . In this sense, the covering radius links two opposite extremal behaviors: perfect codes realize optimal packing, filling the space with disjoint spheres, while maximal codes represent the most dense configurations possible under the given distance constraint. Thus $\rho(C)$ quantifies how closely a code approaches these two geometric extremes within $\mathbb{F}_{q_0}^n$.

Despite extensive study, determining the covering radius of a general linear code remains a challenging problem—it is both **NP-hard** and **co-NP-hard** [41]. Consequently, most work has focused on deriving upper and lower bounds rather than exact values [2, 4, 5, 13, 25, 26, 33, 43, 49, 53]). Exact covering radii are known only for a few highly structured families of codes; see, for example, [15, 16, 20, 21, 31, 32, 34, 37]. For most recent progress, we refer the reader to [23, 27, 29, 48]. The generalized Zetterberg codes introduced below provide another notable instance in which precise analysis is attainable.

B. Generalized Zetterberg Codes

Among the many families of linear codes studied for their distance and covering properties, *Zetterberg codes* occupy a distinctive place. Introduced independently by Zetterberg [58] and Meggitt [42], these cyclic codes combine a high information rate with double-error-correcting capability and admit efficient decoding algorithms [22]. They are quasi-perfect [20], reversible [40, Ch. 7, Sec. 6], and their $\mathbb{Z}_4$ -lifts preserve these algebraic features [1]. Owing to their balance of theoretical elegance and practical efficiency, Zetterberg codes remain an active research topic [18, 36].

Originally defined over $\mathbb{F}_2$, these codes extend naturally to any finite field $\mathbb{F}_{q_0}$, giving rise to the *generalized Zetterberg codes* $C_s(q_0)$. They retain the same cyclic structure while revealing rich number-theoretical connections: for instance, the weight distributions of binary and ternary Zetterberg codes relate to Hecke operators acting on certain spaces of some modular forms [45, 52], and the number of weight-five codewords connects to the Hasse zeta function of certain K3 surfaces [44]. Such links place $C_s(q_0)$ at the intersection of coding theory, number theory, and arithmetic geometry, and they also appear in the study of Niho-type cross-correlation [38, 55–57].

C. Summary of Main Results

Recent research [46, 48] has provided a detailed account of the covering radius of generalized Zetterberg codes $C_s(q_0)$ for odd q_0 . Although these works established impressive results, their proofs rely on lengthy and intricate elementary arguments, and the *even-field case* (q_0 even) has remained largely open.

In this paper we employ analytic number-theoretic techniques—specifically, character sums and Weil-type estimates—to study the covering radius of $C_s(q_0)$ for both even and odd q_0 . This approach greatly advances the understanding of the even-field case and, for the odd-field case, yields new and stronger results than previously obtained. The main results are summarized below:

- (1) We prove that the covering radius of $C_s(q_0)$ satisfies $\rho(C_s(q_0)) \leq 3$ for all q_0 and s ;
- (2) We establish necessary and sufficient conditions under which $\rho(C_s(q_0)) = 3$, and determine its exact value for a wide range of s for each q_0 ; when q_0 is odd, this range extends substantially beyond that of [46, 48];
- (3) By analyzing the parameters of $C_s(q_0)$, we identify infinitely many quasi-perfect and maximal codes arising from this construction.

Although the proofs for even- and odd-field cases require different arguments, the overall analytic framework remains uniform. Compared with [46, 48], our proofs are simpler and more transparent, leading to stronger results for odd q_0 and substantial new progress on the even-field case, though a broad range of s for which $\rho(C_s(q_0))$ is undetermined remains open for future investigation.

This paper is organized as follows. Section II introduces the notation and basic conventions. In Section III we define the generalized Zetterberg code $C_s(q_0)$ and the half-Zetterberg code $\widetilde{C}_s(q_0)$ for odd q_0 , and collect several key lemmas used later in the analysis. Section IV investigates the minimum distance of $C_s(q_0)$ for even q_0 and that of $\widetilde{C}_s(q_0)$ for odd q_0 . In Section V we prove that $\rho(C_s(q_0)) \leq 3$ for all q_0 and s , using character sums and Weil-type estimates; the arguments for even and odd q_0 require separate treatments. A detailed study of $\rho(C_s(q_0))$ for odd q_0 is given in Section VI, followed by the case of even q_0 in Section VII. Section VIII combines our results on the minimum distance and covering radius to identify many families of quasi-perfect and maximal codes derived from $C_s(q_0)$. Finally, in Section IX we conclude the paper and propose an open problem.

II. NOTATION

We use the following notation throughout the paper.

- q_0 denotes a prime power, s a positive integer, $q = q_0^s$;
- $\mathbb{F}_{q_0}, \mathbb{F}_q$ and $\mathbb{F}_{q^2}$ are the finite fields of order q_0, q and q^2 respectively;
- $\mathbb{F}_q^* := \mathbb{F}_q \setminus \{0\}$;
- If q is odd, $\square_q \subseteq \mathbb{F}_q^*$ denotes the set of squares;
- $H \subseteq \mathbb{F}_{q^2}$ is the multiplicative subgroup of order $q+1$, defined by

$$H := \{x \in \mathbb{F}_{q^2} : x^{q+1} = 1\};$$

- For any $x \in \mathbb{F}_{q^2}$, write $\bar{x} := x^q$;
- $C_s(q_0)$ denotes the q_0 -ary generalized Zetterberg code defined in (3);
- For a code C , let $d(C)$ and $\rho(C)$ denote its minimum distance covering radius respectively;
- for a positive integer n , $[n] := \{1, 2, \dots, n\}$;
- $\mathbb{P}^1(\mathbb{F}_q) = \mathbb{F}_q \cup \{\infty\}$.

III. PRELIMINARIES

A. Generalized Zetterberg and half-Zetterberg codes

Let ξ be a generator of H so that

$$H = \{1, \xi, \xi^2, \dots, \xi^q\}.$$

The q_0 -ary *generalized Zetterberg code*, denoted by $C_s(q_0)$, is defined as

$$C_s(q_0) = \left\{ (c_0, c_1, \dots, c_q) \in \mathbb{F}_{q_0}^{q+1} : \sum_{i=0}^q c_i \xi^i = 0 \right\}. \quad (3)$$

Thus $C_s(q_0)$ is a q_0 -ary linear code of length $q+1$.

Let $h_{q_0}(X) \in \mathbb{F}_{q_0}[X]$ be the monic irreducible polynomial of ξ over $\mathbb{F}_{q_0}$. Since $\mathbb{F}_{q^2} = \mathbb{F}_q(\xi)$, we have

$$[\mathbb{F}_q(\xi) : \mathbb{F}_{q_0}] = [\mathbb{F}_q(\xi) : \mathbb{F}_q] \cdot [\mathbb{F}_q : \mathbb{F}_{q_0}] = 2s,$$

so $\deg h_{q_0}(X) = 2s$ and $h_{q_0}(X) \mid (X^{q+1} - 1)$.

Each $\underline{c} = (c_0, \dots, c_q) \in \mathbb{F}_{q_0}^{q+1}$ corresponds to a polynomial $\underline{c}(X) = c_0 + c_1X + \dots + c_qX^q$. This gives an isomorphism from the vector space $\mathbb{F}_{q_0}^{q+1}$ to the quotient ring $\mathbb{F}_{q_0}[X]/(X^{q+1} - 1)$. It is easy to see that

$$\underline{c} \in C_s(q_0) \iff \underline{c}(\xi) = 0 \iff h_{q_0}(X) \mid \underline{c}(X),$$

hence $C_s(q_0)$ can be identified with the cyclic group in $\mathbb{F}_{q_0}[X]/(X^{q+1} - 1)$ generated by $h_{q_0}(X)$. Since $\deg h_{q_0}(X) = 2s$, we have

$$\dim C_s(q_0) = q+1 - 2s,$$

so the code $C_s(q_0)$ has parameters $[q+1, q+1-2s]_{q_0}$.

We will carry out a detailed study of the minimum distance of $C_s(q_0)$ for q_0 even in Section IV. When q_0 is odd, the situation is much easier: since $q+1$ is even, $\pm 1 \in H$, so the minimum distance of $C_s(q_0)$ is always 2. The minimum distance can be improved by dropping half the elements of H . To be more precise, let us define the q_0 -ary *half-Zetterberg code* $\widetilde{C_s}(q_0)$ (when q_0 is odd) as

$$\widetilde{C_s}(q_0) = \left\{ (c_0, c_1, \dots, c_{(q-1)/2}) \in \mathbb{F}_{q_0}^{(q+1)/2} : \sum_{i=0}^{(q-1)/2} c_i \xi^i = 0 \right\}. \quad (4)$$

By the correspondence

$$\underline{c} = (c_0, \dots, c_{(q-1)/2}) \in \mathbb{F}_{q_0}^{(q+1)/2} \mapsto \underline{c}(X) = c_0 + c_1X + \dots + c_{(q-1)/2}X^{(q-1)/2},$$

it is easy to see that

$$\underline{c} \in \widetilde{C_s}(q_0) \iff \underline{c}(\xi) = 0 \iff h_{q_0}(X) \mid \underline{c}(X),$$

hence $\widetilde{C_s}(q_0)$ can be identified with the constacyclic code in $\mathbb{F}_{q_0}[X]/(X^{(q+1)/2} + 1)$ generated by $h_{q_0}(X)$.

Since $\deg h_{q_0}(X) = 2s$, the code $\widetilde{C_s}(q_0)$ has parameters $\left[\frac{q+1}{2}, \frac{q+1}{2} - 2s \right]_{q_0}$ with minimum distance at least 3.

We remark that in [46] the authors defined the so-called “half and twisted Zetterberg codes”, but they are all monomially equivalent to $\widetilde{C_s}(q_0)$. Actually, for any $\underline{\varepsilon} = (\varepsilon_0, \dots, \varepsilon_{(q-1)/2}) \in \{\pm 1\}^{(q+1)/2}$, denote $\xi'_i := \varepsilon_i \xi^i$ for $0 \leq i \leq (q-1)/2$ and define

$$\widetilde{C_s}(q_0)^{\underline{\varepsilon}} := \left\{ (c_0, c_1, \dots, c_{(q-1)/2}) \in \mathbb{F}_{q_0}^{(q+1)/2} : \sum_{i=0}^{(q-1)/2} c_i \xi'_i = 0 \right\}.$$

It is easy to see that $\phi : \widetilde{C_s}(q_0) \rightarrow \widetilde{C_s}(q_0)^{\underline{\varepsilon}}$ given by

$$(c_0, c_1, \dots, c_{(q-1)/2}) \mapsto (\varepsilon_0 c_0, \varepsilon_1 c_1, \dots, \varepsilon_{\frac{q-1}{2}} c_{\frac{q-1}{2}})$$

is an isomorphism, hence the codes $\widetilde{C_s(q_0)}$ and $\widetilde{C_s(q_0)}^\varepsilon$ for any $\varepsilon \in \{\pm 1\}^{\frac{q+1}{2}}$ have the same parameters such as dimension, minimum distance and covering radius. It suffices to consider only the half-Zetterberg code $\widetilde{C_s(q_0)}$ given in (4) when q_0 is odd.

By the code parameters of $C_s(q_0)$ and $\widetilde{C_s(q_0)}$ and the sphere-packing bound (see [35, 40])

$$A_{q_0}(n, d) \leq \frac{q_0^n}{\sum_{i=0}^{\lfloor \frac{d-1}{2} \rfloor} \binom{n}{i} (q_0 - 1)^i},$$

where $A_{q_0}(n, d)$ denotes the largest cardinality of a q_0 -ary code of length n with minimum distance d , we can easily obtain the following:

$$\begin{cases} d(C_s(q_0)) \leq 4 & : q_0 \geq 4 \text{ even;} \\ d(\widetilde{C_s(q_0)}) \leq 4 & : q_0 \geq 5 \text{ odd.} \end{cases} \quad (5)$$

We will determine $d(C_s(q_0))$ for q_0 even and $d(\widetilde{C_s(q_0)})$ for q_0 odd in Section IV.

As for the covering radius, it is worth mentioning that (see [46])

$$\rho(C_s(q_0)) = \rho(\widetilde{C_s(q_0)}), \quad q_0 \text{ is odd,}$$

and $\rho(C_s(q_0))$ can be described in a very simple way (see [11, 33] and [46]):

Lemma 1. *The covering radius of $C_s(q_0)$ is the least positive integer ρ such that for any $\alpha \in \mathbb{F}_{q^2}$, there exist $(c_1, \dots, c_\rho) \in \mathbb{F}_{q_0}^\rho$ and $(x_1, \dots, x_\rho) \in H^\rho$ such that*

$$\alpha = c_1 x_1 + \dots + c_\rho x_\rho.$$

B. Character sums over finite fields

Let m, n be positive integers such that $m|n$. The trace and the norm functions from $\mathbb{F}_{q_0^n}$ to $\mathbb{F}_{q_0^m}$ are define as

$$\begin{aligned} \text{Tr}_{\mathbb{F}_{q_0^n}/\mathbb{F}_{q_0^m}}(x) &= x + x^{q_0^m} + \dots + x^{q_0^{m(\frac{n}{m}-1)}}, \\ \text{N}_{\mathbb{F}_{q_0^n}/\mathbb{F}_{q_0^m}}(x) &= x \cdot x^{q_0^m} \dots x^{q_0^{m(\frac{n}{m}-1)}}. \end{aligned}$$

If q is odd, let $\chi(\cdot)$ be the quadratic character of $\mathbb{F}_q$, which is defined as

$$\chi(x) = \begin{cases} 1, & \text{if } x \in \square_q, \\ -1, & \text{if } x \in \mathbb{F}_q^* \setminus \square_q, \\ 0, & \text{if } x = 0. \end{cases}$$

Let $\mathbb{F}_q[X]$ be the polynomial ring over $\mathbb{F}_q$. For $f \in \mathbb{F}_q[X]$, we consider character sums of the form

$$\sum_{x \in \mathbb{F}_q} \chi(f(x)). \quad (6)$$

The case that $\deg(f) = 1$ is trivial. For $\deg(f) = 2$, we have the following result:

Lemma 2. [39, Theorem 5.48] *Let $f(X) = a_2 X^2 + a_1 X + a_0 \in \mathbb{F}_q[X]$ with q odd and $a_2 \neq 0$. Put $d = a_1^2 - 4a_0 a_2$ and let χ be the quadratic character of $\mathbb{F}_q$. Then*

$$\sum_{x \in \mathbb{F}_q} \chi(f(x)) = \begin{cases} -\chi(a_2), & \text{if } d \neq 0, \\ (q-1)\chi(a_2), & \text{if } d = 0. \end{cases}$$

For a polynomial f with degree 3 or higher, computing the character sum (6) is generally challenging. The subsequent lemma provides a standard Weil-type bound which is sufficient for our purpose.

Lemma 3. [54, Corollary 2.3] *Let $f_1(T), \dots, f_n(T)$ be n monic pairwise prime polynomials in $\mathbb{F}_q[T]$ whose largest squarefree divisors have degrees $d_1, \dots, d_n$ respectively. Let $\chi_1, \dots, \chi_n$ be multiplicative non-trivial characters of order $r_1, \dots, r_n$ respectively on the finite field $\mathbb{F}_q$. Assume that for some $1 \leq i \leq n$, the polynomial $f_i(T)$ is not of the form $g(T)^{r_i}$ in $\mathbb{F}_q[T]$. Then, we have the estimate*

$$\left| \sum_{c \in \mathbb{F}_q} \chi_1(f_1(c)) \cdots \chi_n(f_n(c)) \right| \leq \left(\sum_{i=1}^n d_i - 1 \right) \sqrt{q}. \quad (7)$$

Moreover, if $\chi_i^{d_i} = 1$ for all i , then the right hand side of (7) can be improved to

$$1 + \left(\sum_{i=1}^n d_i - 2 \right) \sqrt{q}.$$

As a simple application of Lemma 3, we obtain the following result.

Lemma 4. *Let $q_0 \geq 5$ be an odd prime power. Then there exist $(c_1, c_2) \in \mathbb{F}_{q_0}^{*2}$, such that*

$$\chi((c_1 + c_2 + 1)(c_1 + c_2 - 1)(c_1 - c_2 + 1)(c_1 - c_2 - 1)) = -1,$$

where $\chi(\cdot)$ denotes the quadratic multiplicative character of $\mathbb{F}_{q_0}$.

Proof. For an arbitrary $c_2 \in \mathbb{F}_{q_0}^*$, define the quartic polynomial $f(X) = (X + c_2 + 1)(X + c_2 - 1)(X - c_2 + 1)(X - c_2 - 1) \in \mathbb{F}_{q_0}[X]$. For $i = -1, 0, 1$, let

$$n_i = \left| \{x \in \mathbb{F}_{q_0} \mid \chi(f(x)) = i\} \right|.$$

Clearly, $n_{-1} + n_0 + n_1 = q_0$, and since $f(X)$ has at most four roots in $\mathbb{F}_{q_0}$, we have $0 \leq n_0 \leq 4$. Moreover, because $c_2 \neq 0$, f is not a square of a polynomial over $\mathbb{F}_{q_0}$. By Lemma 3, we obtain

$$\left| \sum_{x \in \mathbb{F}_{q_0}} \chi(f(x)) \right| \leq 3\sqrt{q_0}.$$

Note that

$$\sum_{x \in \mathbb{F}_{q_0}} \chi(f(x)) = n_1 - n_{-1},$$

this implies

$$|n_1 - n_{-1}| \leq 3\sqrt{q_0}.$$

Combining this with $n_1 + n_{-1} = q_0 - n_0 \geq q_0 - 4$, we deduce that

$$n_{-1} \geq \frac{1}{2}(q_0 - 3\sqrt{q_0} - 4).$$

Now for $q_0 \geq 17$, a direct computation shows that $\frac{1}{2}(q_0 - 3\sqrt{q_0} - 4) > 0$, this with $\chi(f(0)) \neq -1$ implies that there must exist some $c_1 \in \mathbb{F}_{q_0}^*$ such that $\chi(f(c_1)) = -1$. For the remaining cases $q_0 \in \{5, 7, 11, 13\}$, the existence of such c_1 and c_2 in $\mathbb{F}_{q_0}^*$ can be verified easily by using MAGMA. This completes the proof of Lemma 4. $\square$

An additive character of $\mathbb{F}_q$ is a function $\psi: \mathbb{F}_q \rightarrow \mathbb{C} \setminus \{0\}$ such that

$$\psi(\beta_1 + \beta_2) = \psi(\beta_1)\psi(\beta_2), \quad \forall \beta_1, \beta_2 \in \mathbb{F}_q.$$

Suppose $\mathbb{F}_q$ is of characteristic p . The canonical additive character is given by

$$\psi(\beta) = \zeta_p^{\text{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\beta)}, \quad \forall \beta \in \mathbb{F}_q,$$

where $\zeta_p := \exp(2\pi\sqrt{-1}/p)$ is the complex primitive p -th root of unity. When $p = 2$, then $\zeta_2 = -1$, this character takes values in $\{\pm 1\}$, a fact frequently used in coding theory. The following Weil-type bound was given in [9].

Lemma 5. [9] Consider the finite field $\mathbb{F}_q$ with characteristic p . Let $f(X) \in \mathbb{F}_q(X)$ be a rational function,

$$f(X) = p(X) + \frac{r(X)}{q(X)}, \quad \deg(r(X)) < \deg(q(X)), \quad M := \deg(p(X)),$$

where $p(X), q(X), r(X) \in \mathbb{F}_q[x]$ are polynomials, and $\gcd(r(X), q(X)) = 1$. Suppose further that $f(X)$ is non-constant, and that $M = 0$ or $p \nmid M$. Write

$$q(X) = \prod_{i=1}^Q q_i(X)^{m_i},$$

where $q_i(X)$ are distinct irreducible polynomials over $\mathbb{F}_q$, and $m_i \geq 1$ for each i . Define

$$L := \sum_{i=1}^Q (m_i + 1) \deg(q_i(X)).$$

Then there exist complex numbers $\omega_j \in \mathbb{C}$, $1 \leq j \leq M + L - 1$, such that

$$\sum_{\beta \in \mathbb{F}_q \setminus S} \psi(f(\beta)) = - \sum_{j=1}^{M+L-1} \omega_j,$$

where S is the set of poles of $f(X)$. Additionally, $|\omega_j| = \sqrt{q}$ for all j , except for a single value, j' , satisfying $|\omega_{j'}| = 1$. Thus,

$$\left| \sum_{\beta \in \mathbb{F}_q \setminus S} \psi(f(\beta)) \right| \leq 1 + (M + L - 2) \sqrt{q}.$$

We will also use the following three criteria for quadratic polynomial over $\mathbb{F}_q$.

Lemma 6. [8, Lemma 3] Let q be odd and $D(X) = \alpha X^2 + \beta X + \alpha^q$ with $\alpha \in \mathbb{F}_{q^2}$ and $\beta \in \mathbb{F}_q$, not both zero. Define $\Delta(D) := \beta^2 - 4\alpha^{q+1}$. Then the following hold:

- 1) $D(X)$ has a multiple root (which must be in H) if and only if $\Delta(D) = 0$;
- 2) $D(X)$ has two distinct roots in H if and only if $\Delta(D)$ is a non-square in $\mathbb{F}_q^*$;
- 3) $D(X)$ has no roots in H if and only if $\Delta(D)$ is a square in $\mathbb{F}_q^*$.

Lemma 7. [3] For a positive integer n , the quadratic equation $x^2 + ax + b = 0$, $a, b \in \mathbb{F}_{2^n}$, $a \neq 0$ has solutions in $\mathbb{F}_{2^n}$ if and only if $\text{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}(b/a^2) = 0$.

Lemma 8. [19, Lemma 2.4] If q is even and $A(X) = \alpha X^2 + \beta X + \alpha^q$ with $\alpha \in \mathbb{F}_{q^2}$ and $\beta \in \mathbb{F}_q^*$, then the following are equivalent:

- (1) $A(X)$ has at least one root in H ;
- (2) $A(X)$ has two distinct roots in H ;
- (3) $\text{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(\alpha^{q+1}/\beta^2) = 1$.

IV. MINIMUM DISTANCE OF $C_s(q_0)$ AND $\widetilde{C_s(q_0)}$

In this section we determine the minimum distance of $C_s(q_0)$ when q_0 is even and the minimum distance of $\widetilde{C_s(q_0)}$ which exists only when q_0 is odd. If q_0 is odd, it is trivial that the minimum distance of $C_s(q_0)$ is 2.

A. Case: q_0 is even

When $q_0 = 2$, it was well-known that (see for example [18])

$$d(C_s(2)) = \begin{cases} 5, & \text{if } s \text{ is even;} \\ 3, & \text{if } s \text{ is odd.} \end{cases}$$

For $q_0 \geq 4$ even, the result on $d(C_s(q_0))$ is elementary but it is not easy for us to find a reference, so we compute the value $d(C_s(q_0))$ below.

Theorem 1. *Let $q_0 \geq 4$ be even. Then*

$$d(C_s(q_0)) = \begin{cases} 4, & \text{if } s \text{ is even;} \\ 3, & \text{if } s \text{ is odd.} \end{cases}$$

Proof. First, recall that $C_s(q_0)$ is a q_0 -ary $[q+1, q+1-2s]$ linear code and $d(C_s(q_0)) \leq 4$ by (5). Next, we establish a lower bound on the minimum distance. It is obvious that there is no codeword of weight 1 in $C_s(q_0)$. If there is a codeword of weight 2 in $C_s(q_0)$, then there are $c_i, c_j \in \mathbb{F}_{q_0}^*$, $0 \leq i < j \leq q$, such that

$$c_i \xi^i + c_j \xi^j = 0.$$

This implies $\xi^{j-i} = \frac{c_i}{c_j} \in \mathbb{F}_{q_0}^* \cap H$. Since $\mathbb{F}_{q_0} \cap H = \{1\}$, we have $\xi^{j-i} = 1$, and consequently $j = i$, which is a contradiction. Hence, $d(C_s(q_0)) \geq 3$ and thus we have $d(C_s(q_0)) \in \{3, 4\}$.

Assume now that s is even. Suppose there exists a codeword of weight 3 in $C_s(q_0)$, then there are $c_i, c_j, c_k \in \mathbb{F}_{q_0}^*$ where $0 \leq i < j < k \leq q$ such that

$$c_i \xi^i + c_j \xi^j + c_k \xi^k = 0. \quad (8)$$

Noting $\xi^q = \xi^{-1}$, taking the q -th power on both sides of Equation (8), we obtain

$$c_i \xi^{-i} + c_j \xi^{-j} + c_k \xi^{-k} = 0. \quad (9)$$

From (8) and (9), we derive

$$c_i^2 = (c_i \xi^i)(c_i \xi^{-i}) = (c_j \xi^j + c_k \xi^k)(c_j \xi^{-j} + c_k \xi^{-k}),$$

so we have

$$\xi^{k-j} + \xi^{j-k} = \frac{c_i^2 + c_j^2 + c_k^2}{c_j c_k}.$$

Let $t = \xi^{k-j}$. The above equation becomes a quadratic equation in the variable t :

$$t^2 + \frac{c_i^2 + c_j^2 + c_k^2}{c_j c_k} t + 1 = 0. \quad (10)$$

There are two subcases. If $c_i^2 + c_j^2 + c_k^2 = 0$, then $t = 1$, which implies $k = j$, a contradiction. If $c_i^2 + c_j^2 + c_k^2 \neq 0$, by Lemma 7, Equation (10) is solvable for $t \in \mathbb{F}_q$ if and only if

$$\text{Tr}_{\mathbb{F}_q/\mathbb{F}_2} \left(\frac{(c_j c_k)^2}{(c_i^2 + c_j^2 + c_k^2)^2} \right) = 0.$$

Since s is even and $\frac{(c_j c_k)^2}{(c_i^2 + c_j^2 + c_k^2)^2} \in \mathbb{F}_{q_0}$, the above condition always holds, so Equation (10) is always solvable for $t \in \mathbb{F}_q$. Thus, $t = \xi^{k-j} \in \mathbb{F}_q \cap H = \{1\}$ and we have $k = j$, which is again a contradiction. Therefore, no codewords of weight 3 exist in $C_s(q_0)$ and thus $d(C_s(q_0)) = 4$ when s is even.

Now we assume that s is odd. Define

$$H_0 = \left\{ x \in \mathbb{F}_{q_0^2} : x^{q_0+1} = 1 \right\}.$$

Since s is odd, $(q_0+1)|(q+1)$, H_0 is a subgroup of H . Let θ be a generator of H_0 and consider distinct elements $\theta^i, \theta^j \in H_{q_0+1} \setminus \{1\}$ with some $1 \leq i < j \leq q_0$. It can be easily checked that

$$\frac{\theta^i(\theta^j+1)^2}{(\theta^i+\theta^j)^2}, \quad \frac{\theta^j(\theta^i+1)^2}{(\theta^i+\theta^j)^2} \in \mathbb{F}_{q_0}^*,$$

and

$$\frac{\theta^i(\theta^j+1)^2}{(\theta^i+\theta^j)^2} \cdot \theta^i + \frac{\theta^j(\theta^i+1)^2}{(\theta^i+\theta^j)^2} \cdot \theta^j + 1 \cdot 1 = 0.$$

Since $1, \theta^i, \theta^j$ are distinct elements of H_0 and $H_0 \subseteq H$, this gives a codeword of weight 3 in $C_s(q_0)$. Hence, $d(C_s(q_0)) = 3$ when s is odd. $\square$

B. Case: q_0 is odd

In the following, we investigate the minimum distance of $\widetilde{C_s(q_0)}$. For $q_0 = 3$, it was known from [20, 28] that $d(\widetilde{C_s(3)}) = 5$ for any $s \geq 2$ (when $s = 1$, the code $\widetilde{C_1(3)}$ is a trivial code of dimension 0, containing only the zero vector). For $q_0 \geq 5$, We have the following theorem.

Theorem 2. *Let $q_0 \geq 5$ be odd. Then*

$$d(\widetilde{C_s(q_0)}) = \begin{cases} 4, & \text{if } s \text{ is even} \\ 3, & \text{if } s \text{ is odd.} \end{cases}$$

Proof. It is clear by construction that $d(\widetilde{C_s(q_0)}) \geq 3$. Now we assume that s is even. We will show that there is no codeword in $\widetilde{C_s(q_0)}$ of weight 3. Otherwise, by the definition of $\widetilde{C_s(q_0)}$, there exist $c_i, c_j, c_k \in \mathbb{F}_{q_0}^*$, such that

$$c_i \xi^i + c_j \xi^j + c_k \xi^k = 0, \tag{11}$$

where $0 \leq i < j < k \leq \frac{q-1}{2}$. Let $c_1 = \frac{c_j}{c_i}$, $c_2 = \frac{c_k}{c_i}$, $j' = j - i$ and $k' = k - i$. We have

$$1 + c_1 \xi^{j'} + c_2 \xi^{k'} = 0.$$

Taking the q -th power of the above equation, we have

$$1 + c_1 \xi^{-j'} + c_2 \xi^{-k'} = 0.$$

Hence,

$$c_2^2 = c_2 \xi^{k'} \cdot c_2 \xi^{-k'} = (-c_1 \xi^{j'} - 1)(-c_1 \xi^{-j'} - 1),$$

i.e.,

$$(\xi^{j'})^2 - \frac{c_2^2 - c_1^2 - 1}{c_1} \xi^{j'} + 1 = 0.$$

Consider the above equation as a quadratic equation in the variable $\xi^{j'}$. Then the discriminant is

$$\Delta = \left(\frac{c_2^2 - c_1^2 - 1}{c_1} \right)^2 - 4,$$

which is an element of $\mathbb{F}_{q_0}$. Since s is even, Δ is 0 or an square element in $\mathbb{F}_q$. Therefore, $\xi^{j'} \in \mathbb{F}_q$. We conclude that $\xi^{j'} = 1$ since $\mathbb{F}_q \cap H_0 = \{1\}$, which contradicts $i < j$. Then $d(C_s(q_0)) \geq 4$ when s is even. The equality holds because of (5).

In the following, we assume that s is odd. We will prove the existence of a weight-3 codeword in $\widetilde{C_s(q_0)}$.

By Lemma 4, there exist $c_1, c_2 \in \mathbb{F}_{q_0} \setminus \{0, \pm 1\}$ such that

$$\delta = (c_1 + c_2 + 1)(c_1 + c_2 - 1)(c_1 - c_2 + 1)(c_1 - c_2 - 1)$$

is a nonsquare element in $\mathbb{F}_{q_0}$. Since s is odd, δ is a nonsquare element in $\mathbb{F}_q$ as well. Let $\sqrt{\delta}$ be one of the square roots of δ , which is in $\mathbb{F}_{q^2}$. Define

$$\zeta_1 = \frac{c_2^2 - c_1^2 - 1 + \sqrt{\delta}}{2c_1}, \quad \zeta_2 = \frac{c_1^2 - c_2^2 - 1 - \sqrt{\delta}}{2c_2}.$$

One can verify that ζ_1, ζ_2 are two distinct elements in $H \setminus \{\pm 1\}$ and $\zeta_1 \neq \zeta_2$. Then we can choose suitable $\varepsilon_1, \varepsilon_2 \in \{\pm 1\}$ such that $\varepsilon_1 \zeta_1, \varepsilon_2 \zeta_2 \in H_0 \setminus \{1\}$ and they are distinct. Moreover, by a direct calculation, we have

$$(\varepsilon_1 c_1) \cdot (\varepsilon_1 \zeta_1) + (\varepsilon_2 c_2) \cdot (\varepsilon_2 \zeta_2) + 1 \cdot 1 = 0,$$

where $\varepsilon_1 c_1, \varepsilon_2 c_2 \in \mathbb{F}_{q_0}$, $\varepsilon_1 \zeta_1, \varepsilon_2 \zeta_2 \in H_0 \setminus \{1\}$ and they are distinct. Hence, $\widetilde{C_s(q_0)}$ has a codeword of weight 3. We conclude that $d(C_s(q_0)) = 3$ when s is odd. This completes the proof. $\square$

V. COVERING RADIUS OF $C_s(q_0)$ IS AT MOST 3

Denote by $\rho(C_s(q_0))$ the covering radius of the code $C_s(q_0)$. In this section, we prove that $\rho(C_s(q_0)) \leq 3$ for all q_0 and s . We first prove a technical lemma.

Lemma 9. For any $\alpha \in \mathbb{F}_{q^2}$ and any $(c_1, c_2, c_3) \in \mathbb{F}_{q_0}^3$, denote by N_1 the number of solutions $(x_1, x_2, x_3) \in H^3$ to the equation

$$\alpha = c_1 x_1 + c_2 x_2 + c_3 x_3. \quad (12)$$

Denote by N_2 the number of solutions $(x_1, x_2) \in H^2$ to the equation

$$c_2(\bar{\alpha} - c_1 \bar{x}_1) x_2^2 - ((\alpha - c_1 x_1)(\bar{\alpha} - c_1 \bar{x}_1) + c_2^2 - c_3^2) x_2 + c_2(\alpha - c_1 x_1) = 0. \quad (13)$$

If $c_3 \neq 0$, then $N_1 = N_2$.

Proof. Suppose $(x_1, x_2, x_3) \in H^3$ is a solution to Eq (12), then we have

$$c_3 x_3 = \alpha - c_1 x_1 - c_2 x_2.$$

Since $c_i \in \mathbb{F}_{q_0} \subseteq \mathbb{F}_q$ for each i , we have

$$c_3 \bar{x}_3 = \bar{\alpha} - c_1 \bar{x}_1 - c_2 \bar{x}_2.$$

Here for $x \in \mathbb{F}_{q^2}$ we denote $\bar{x} := x^q$. Since $x_3 \in H$, $\bar{x}_3 x_3 = 1$, so we have

$$c_3^2 = (\alpha - c_1 x_1 - c_2 x_2)(\bar{\alpha} - c_1 \bar{x}_1 - c_2 \bar{x}_2). \quad (14)$$

From this we obtain

$$(\alpha - c_1 x_1)(\bar{\alpha} - c_1 \bar{x}_1) - c_2 x_2(\bar{\alpha} - c_1 \bar{x}_1) - c_2 \bar{x}_2(\alpha - c_1 x_1) + c_2^2 = c_3^2. \quad (15)$$

Multiplying x_2 on both sides of Eq (15) and noting $x_2 \bar{x}_2 = 1$, we obtain Eq (13).

On the other hand, suppose $(x_1, x_2) \in H^2$ is a solution to Eq (13), then (x_1, x_2) also satisfies Eq (15) and hence Eq (14), so $\alpha - c_1x_1 - c_2x_2 \neq 0$ as $c_3 \neq 0$. It is easy to see that by defining

$$x_3 := \frac{\alpha - c_1x_1 - c_2x_2}{c_3},$$

we have $x_3 \in H$ and this triple $(x_1, x_2, x_3) \in H^3$ is a solution to Eq (12). This completes the proof of Lemma 9. $\square$

We now proceed to prove that $\rho(C_s(q_0)) \leq 3$. While the proofs for even and odd q_0 are similar in nature, the technical treatments are different and non-trivial. For the sake of clarity, we write these two cases as two separate theorems. It is worth pointing out that the result for odd q_0 was already obtained (see [46, Theorem II.1] and [48, Corollary 3.14]). Here for odd q_0 , we provide a new proof.

Theorem 3. *Let $q_0 \geq 3$ be odd and $s \geq 1$. Then the covering radius of $C_s(q_0)$ is at most 3.*

Proof. The case that $s = 1$ is trivial as was noted in [46]. From now on let us assume that $s \geq 2$. To prove that $\rho(C_s(q_0)) \leq 3$, by Lemma 1, it suffices to show that for any $\alpha \in \mathbb{F}_{q^2}$, there exist $c_1, c_2, c_3 \in \mathbb{F}_{q_0}$ and $x_1, x_2, x_3 \in H$, such that

$$\alpha = c_1x_1 + c_2x_2 + c_3x_3. \quad (16)$$

If $\alpha \in \mathbb{F}_{q_0} \cdot H = \{cx : c \in \mathbb{F}_{q_0}, x \in H\}$, then taking $c_1 \in \mathbb{F}_{q_0}$ and $x_1 \in H$ such that $\alpha = c_1x_1$ and taking $c_2 = c_3 = 0$, we see that (16) holds for these c_i and x_i . Now suppose $\alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_{q_0} \cdot H$. For any fixed $(c_1, c_2, c_3) \in \mathbb{F}_{q_0}^{*3}$, let us define

$$N(c_1, c_2, c_3) := \#\{(x_1, x_2, x_3) \in H^3 : \alpha = c_1x_1 + c_2x_2 + c_3x_3\}.$$

We will prove that $N(c_1, c_2, c_3) > 0$ for any fixed $(c_1, c_2, c_3) \in \mathbb{F}_{q_0}^{*3}$ and any $\alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_{q_0} \cdot H$. This would imply that $\rho(C_s(q_0)) \leq 3$.

By Lemma 9, $N(c_1, c_2, c_3)$ equals the number of solutions $(x_1, x_2) \in H^2$ to the equation

$$c_2(\bar{\alpha} - c_1\bar{x}_1)x_2^2 - ((\alpha - c_1x_1)(\bar{\alpha} - c_1\bar{x}_1) + c_2^2 - c_3^2)x_2 + c_2(\alpha - c_1x_1) = 0. \quad (17)$$

Since $\alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_{q_0} \cdot H$, $\alpha - c_1x_1 \neq 0$, hence for any fixed $x_1 \in H$, Eq (17) is a quadratic equation in x_2 , whose discriminant is given by

$$\Delta(x_1) = ((\alpha - c_1x_1)(\bar{\alpha} - c_1\bar{x}_1) + c_2^2 - c_3^2)^2 - 4c_2^2(\alpha - c_1x_1)(\bar{\alpha} - c_1\bar{x}_1).$$

It is also easy to check that

$$\Delta(x_1) = ((\alpha - c_1x_1)(\bar{\alpha} - c_1\bar{x}_1) - (c_2 + c_3)^2)((\alpha - c_1x_1)(\bar{\alpha} - c_1\bar{x}_1) - (c_2 - c_3)^2). \quad (18)$$

According to Lemma 6, for any given $x_1 \in H$, the number of roots $x_2 \in H$ satisfying Eq (17) is exactly $1 - \chi(\Delta(x_1))$, where χ denotes the quadratic character of $\mathbb{F}_q$, so we derive that

$$N(c_1, c_2, c_3) = \sum_{x_1 \in H} (1 - \chi(\Delta(x_1))) = q + 1 - \sum_{x_1 \in H} \chi(\Delta(x_1)).$$

Now we fix an element $a \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ and consider the bijection $\phi : \mathbb{P}^1(\mathbb{F}_q) \rightarrow H$ given by $\phi : y \mapsto \frac{y+a}{y+\bar{a}}$. Since $\phi(\infty) = 1 \in H$, we have

$$N(c_1, c_2, c_3) = q + 1 - \chi(\Delta(1)) - \sum_{x \in \mathbb{F}_q} \chi\left(\Delta\left(\frac{x+a}{x+\bar{a}}\right)\right).$$

For the function $\Delta(\frac{x+a}{x+\bar{a}})$, from (18) we can obtain

$$\Delta\left(\frac{x+a}{x+\bar{a}}\right) = \left(\left(\alpha - c_1\frac{x+a}{x+\bar{a}}\right)\left(\bar{\alpha} - c_1\frac{x+\bar{a}}{x+a}\right) - (c_2 + c_3)^2\right) \times$$

$$\begin{aligned}
& \left(\left(\alpha - c_1 \frac{x+a}{x+\bar{a}} \right) \left(\bar{\alpha} - c_1 \frac{x+\bar{a}}{x+a} \right) - (c_2 - c_3)^2 \right) \\
&= \left(\frac{(\alpha - c_1)(\bar{\alpha} - c_1)}{(x+a)(x+\bar{a})} \right)^2 f_1(x) f_2(x),
\end{aligned}$$

where

$$\begin{aligned}
f_1(x) &= \left(x + \frac{\alpha\bar{a} - c_1 a}{\alpha - c_1} \right) \left(x + \frac{\bar{\alpha}a - c_1 \bar{a}}{\bar{\alpha} - c_1} \right) - \frac{(c_2 + c_3)^2}{(\alpha - c_1)(\bar{\alpha} - c_1)}, \\
f_2(x) &= \left(x + \frac{\alpha\bar{a} - c_1 a}{\alpha - c_1} \right) \left(x + \frac{\bar{\alpha}a - c_1 \bar{a}}{\bar{\alpha} - c_1} \right) - \frac{(c_2 - c_3)^2}{(\alpha - c_1)(\bar{\alpha} - c_1)}.
\end{aligned}$$

Since $a \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$, $c_1 \in \mathbb{F}_{q_0}^*$ and $\alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_{q_0} \cdot H$, we have

$$\frac{(\alpha - c_1)(\bar{\alpha} - c_1)}{(x+a)(x+\bar{a})} \in \mathbb{F}_q^*, \quad \forall x \in \mathbb{F}_q,$$

so

$$\chi \left(\Delta \left(\frac{x+a}{x+\bar{a}} \right) \right) = \chi(f_1(x)f_2(x)), \quad \forall x \in \mathbb{F}_q,$$

and thus

$$N(c_1, c_2, c_3) = q + 1 - \chi(\Delta(1)) - \sum_{x \in \mathbb{F}_q} \chi(f_1(x)f_2(x)).$$

As $c_2, c_3 \in \mathbb{F}_{q_0}^*$, $(c_2 + c_3)^2 \neq (c_2 - c_3)^2$, it is easy to see that $\gcd(f_1(X), f_2(X)) = 1$, and the quadratic polynomials $f_1(X)$ and $f_2(X)$ can not be squares of linear polynomials simultaneously, hence by Lemma 3, we have

$$\left| \sum_{x \in \mathbb{F}_q} \chi(f_1(x)f_2(x)) \right| \leq 3\sqrt{q}.$$

This gives

$$N(c_1, c_2, c_3) \geq q - \left| \sum_{x \in \mathbb{F}_q} \chi(f_1(x)f_2(x)) \right| \geq q - 3\sqrt{q} > 0,$$

as long as $q > 9$. Hence we obtain $\rho(C_s(q_0)) \leq 3$ if $q > 9$.

For $q \leq 9$ and odd, since $s \geq 2$, the only possibility is $q_0 = 3, s = 2$ and $q = 9$. It can be easily checked by MAGMA that $\rho(C_2(3)) = 3$. This completes the proof of Theorem 3. $\square$

Theorem 4. *Let $q_0 \geq 2$ be even and $s \geq 1$. Then the covering radius of $C_s(q_0)$ is at most 3.*

Proof. The case $s = 1$ is trivial, because in this case $q = q_0$, by the standard polar representation, every $x \in \mathbb{F}_{q_0}^*$ can be written uniquely as $x = yz$ with $y \in \mathbb{F}_{q_0}^*$ and $z \in H$. Therefore in this case $\rho(C_1(q_0)) = 1$.

If $q_0 = 2$ and $s = 2$, it is easy to check by MAGMA that $\rho(C_s(2)) = 2$. So from now on let us assume either “ $q_0 = 2$ and $s \geq 3$ ” or “ $q_0 \geq 4$ and $s \geq 2$ ”, so we always have $q \geq 8$.

By Lemma 1, to show that $\rho(C_s(q_0)) \leq 3$, it suffices to prove that for every $\alpha \in \mathbb{F}_{q^2}$, there exist $c_1, c_2, c_3 \in \mathbb{F}_{q_0}$ and $x_1, x_2, x_3 \in H$ such that

$$\alpha = c_1 x_1 + c_2 x_2 + c_3 x_3. \tag{19}$$

We may write α as $\alpha = \alpha_0 \alpha_H$ with $\alpha_0 \in \mathbb{F}_q$ and $\alpha_H \in H$. Suppose (19) holds for α . Then

$$\alpha_0 = c_1 \frac{x_1}{\alpha_H} + c_2 \frac{x_2}{\alpha_H} + c_3 \frac{x_3}{\alpha_H},$$

where $\frac{x_i}{\alpha_H} \in H$ for each i since H is the multiplicative subgroup of order $q+1$ in $\mathbb{F}_{q^2}^*$. Therefore, without loss of generality, we may assume $\alpha \in \mathbb{F}_q$. If $\alpha \in \mathbb{F}_{q_0}$, we can set $c_1 = \alpha$, $x_1 = 1$, and $c_2 = c_3 = 0$, so (19) holds trivially. Hence, from now on let us assume that $\alpha \in \mathbb{F}_q \setminus \mathbb{F}_{q_0}$.

For fixed $(c_1, c_2, c_3) \in \mathbb{F}_{q_0}^{*3}$, let us define

$$N(c_1, c_2, c_3) = \# \{ (x_1, x_2, x_3) \in H^3 : \alpha = c_1 x_1 + c_2 x_2 + c_3 x_3 \}.$$

Our goal is to show that $N(c_1, c_2, c_3) > 0$ for any $(c_1, c_2, c_3) \in (\mathbb{F}_{q_0}^*)^3$ and any $\alpha \in \mathbb{F}_q \setminus \mathbb{F}_{q_0}$. This would imply that $\rho(C_s(q_0)) \leq 3$.

By Lemma 9 again, $N(c_1, c_2, c_3)$ equals the number of solutions $(x_1, x_2) \in H^2$ to the equation

$$c_2(\alpha + c_1 \bar{x}_1)x_2^2 + ((\alpha + c_1 x_1)(\alpha + c_1 \bar{x}_1) + c_2^2 + c_3^2)x_2 + c_2(\alpha + c_1 x_1) = 0. \quad (20)$$

For any fixed $x_1 \in H$, to analyze the existence of solutions $x_2 \in H$ of Eq (20), we denote

$$\Delta(x_1) := (\alpha + c_1 x_1)(\alpha + c_1 \bar{x}_1) + c_2^2 + c_3^2.$$

We consider two cases.

Case 1: $\Delta(x_1) = 0$. Then (20) reduces to

$$(\alpha + c_1 \bar{x}_1)c_2 x_2^2 + (\alpha + c_1 x_1)c_2 = 0,$$

that is,

$$x_2^2 = \frac{\alpha + c_1 x_1}{\alpha + c_1 \bar{x}_1}.$$

Since q is even, this gives a unique solution $x_2 \in H$ to Eq (20).

Case 2: $\Delta(x_1) \neq 0$. Then by Lemma 8, for each fixed $x_1 \in H$, Eq (20) has one and hence two distinct solutions $x_2 \in H$ if and only if

$$\text{Tr}_{\mathbb{F}_q/\mathbb{F}_2} \left(\frac{c_2^2(\alpha + c_1 \bar{x}_1)(\alpha + c_1 x_1)}{((\alpha + c_1 x_1)(\alpha + c_1 \bar{x}_1) + c_2^2 + c_3^2)^2} \right) = 1. \quad (21)$$

Note that the left hand side can be rewritten as

$$\begin{aligned} & \text{Tr}_{\mathbb{F}_q/\mathbb{F}_2} \left(\frac{c_2^2((\alpha + c_1 \bar{x}_1)(\alpha + c_1 x_1) + c_2^2 + c_3^2) + c_2^2(c_2^2 + c_3^2)}{((\alpha + c_1 x_1)(\alpha + c_1 \bar{x}_1) + c_2^2 + c_3^2)^2} \right) \\ &= \text{Tr}_{\mathbb{F}_q/\mathbb{F}_2} \left(\frac{c_2^2}{(\alpha + c_1 x_1)(\alpha + c_1 \bar{x}_1) + c_2^2 + c_3^2} \right) + \text{Tr}_{\mathbb{F}_q/\mathbb{F}_2} \left(\frac{c_2^2(c_2^2 + c_3^2)}{((\alpha + c_1 x_1)(\alpha + c_1 \bar{x}_1) + c_2^2 + c_3^2)^2} \right) \\ &= \text{Tr}_{\mathbb{F}_q/\mathbb{F}_2} \left(\frac{c_2^2}{(\alpha + c_1 x_1)(\alpha + c_1 \bar{x}_1) + c_2^2 + c_3^2} \right) + \text{Tr}_{\mathbb{F}_q/\mathbb{F}_2} \left(\frac{c_2(c_2 + c_3)}{(\alpha + c_1 x_1)(\alpha + c_1 \bar{x}_1) + c_2^2 + c_3^2} \right) \\ &= \text{Tr}_{\mathbb{F}_q/\mathbb{F}_2} \left(\frac{c_2 c_3}{(\alpha + c_1 x_1)(\alpha + c_1 \bar{x}_1) + c_2^2 + c_3^2} \right). \end{aligned}$$

So the following condition is equivalent to (21):

$$\text{Tr}_{\mathbb{F}_q/\mathbb{F}_2} \left(\frac{c_2 c_3}{(\alpha + c_1 x_1)(\alpha + c_1 \bar{x}_1) + c_2^2 + c_3^2} \right) = 1.$$

Hence for the given $x_1 \in H$, the number of solutions $x_2 \in H$ to Eq (20) is given by

$$1 - \psi \left(\frac{c_2 c_3}{(\alpha + c_1 x_1)(\alpha + c_1 \bar{x}_1) + c_2^2 + c_3^2} \right),$$

where $\psi : \beta \mapsto (-1)^{\text{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(\beta)}$ is the standard additive character defined on $\mathbb{F}_q$. Summarizing **Cases 1** and **2** above, we conclude that

$$\begin{aligned} N(c_1, c_2, c_3) &= \sum_{\substack{x_1 \in H \\ \Delta(x_1)=0}} 1 + \sum_{\substack{x_1 \in H \\ \Delta(x_1) \neq 0}} \left(1 - \psi \left(\frac{c_2 c_3}{(\alpha + c_1 x_1)(\alpha + c_1 \bar{x}_1) + c_2^2 + c_3^2} \right) \right) \\ &= q + 1 - \sum_{\substack{x_1 \in H \\ \Delta(x_1) \neq 0}} \psi \left(\frac{c_2 c_3}{(\alpha + c_1 x_1)(\alpha + c_1 \bar{x}_1) + c_2^2 + c_3^2} \right). \end{aligned}$$

Let us define

$$T := \sum_{\substack{x_1 \in H \\ \Delta(x_1) \neq 0}} \psi \left(\frac{c_2 c_3}{(\alpha + c_1 x_1)(\alpha + c_1 \bar{x}_1) + c_2^2 + c_3^2} \right).$$

We fix an element $a \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ and consider the bijection $\phi : \mathbb{P}^1(\mathbb{F}_q) \rightarrow H$ given by $\phi : y \mapsto \frac{y+a}{y+\bar{a}}$. Since $\phi(\infty) = 1 \in H$ and

$$\Delta(1) = (\alpha + c_1 + c_2 + c_3)^2 \neq 0,$$

using this bijection ϕ we can rewrite T as

$$T = \psi \left(\frac{c_2 c_3}{(\alpha + c_1 + c_2 + c_3)^2} \right) + \sum_{\substack{y \in \mathbb{F}_q \\ \Delta(\phi(y)) \neq 0}} \psi \left(\frac{c_2 c_3}{(\alpha + c_1 \phi(y))(\alpha + c_1 \phi(y)^{-1}) + c_2^2 + c_3^2} \right).$$

The right hand side can be rewritten as

$$T = \psi \left(\frac{c_2 c_3}{(\alpha + c_1 + c_2 + c_3)^2} \right) + \sum_{y \in \mathbb{F}_q \setminus S} \psi(f(y)),$$

where $f(y)$ is a rational function in $\mathbb{F}_q(y)$ given by

$$f(y) = \frac{c_2 c_3}{(\alpha + c_1 + c_2 + c_3)^2} \left(1 + \frac{A}{y^2 + (a + \bar{a})y + a\bar{a} + A} \right),$$

S is the set of poles of $f(y)$ in $\mathbb{F}_q$ and

$$A = \frac{\alpha c_1 (a + \bar{a})^2}{(\alpha + c_1 + c_2 + c_3)}.$$

Now we apply Lemma 5. From the explicit form of $f(y)$, it is easy to see that $M = 0$ and $L = 4$, so we deduce

$$|T| \leq 1 + (1 + 2\sqrt{q}) = 2(1 + \sqrt{q}).$$

Armed with this estimate, we obtain

$$N(c_1, c_2, c_3) \geq q + 1 - |T| \geq q + 1 - 2(1 + \sqrt{q}) = q - 2\sqrt{q} - 1.$$

Since we have assumed that $q \geq 8$, it is easy to check that $q - 2\sqrt{q} - 1 > 0$, so $N(c_1, c_2, c_3) > 0$ as desired for any $(c_1, c_2, c_3) \in \mathbb{F}_{q_0}^{*3}$ and any $\alpha \in \mathbb{F}_q \setminus \mathbb{F}_{q_0}$. This completes the proof of Theorem 4. $\square$

Since $\rho(C_s(q_0)) > 1$ if $s \geq 2$, we summarize Theorems 3 and 4 in the following corollary.

Corollary 1. *For any q_0 , if $s \geq 2$, then the covering radius of $C_s(q_0)$ satisfies $\rho(C_s(q_0)) \in \{2, 3\}$.*

VI. DETERMINING COVERING RADIUS OF $C_s(q_0)$: q_0 ODD

Let $q_0 \geq 3$ be odd and $s \geq 2$. It is known by Corollary 1 that $\rho(C_s(q_0)) \in \{2, 3\}$. In this section we study explicit conditions to distinguish these two cases. While this case was treated in [46, 48], we will provide new proofs and stronger results.

We know by the proof of Theorem 3 that $\rho(C_s(q_0)) = 2$ if and only if for any $y \in \mathbb{F}_{q^2} \setminus \mathbb{F}_{q_0} \cdot H$, there exist $(c_1, c_2) \in \mathbb{F}_{q_0}^{*2}$ and $(x_1, x_2) \in H^2$ such that

$$y = c_1 x_1 + c_2 x_2. \quad (22)$$

Taking the q -th power on both sides of the above equation, using $\bar{x} = x^q$ for any $x \in \mathbb{F}_{q^2}$ we obtain

$$\bar{y} = c_1 \bar{x}_1 + c_2 \bar{x}_2.$$

Hence, x_1 satisfies the equation

$$(y - c_1 x_1)(\bar{y} - c_1 \bar{x}_1) = c_2^2 x_2 \bar{x}_2 = c_2^2,$$

which simplifies to

$$\bar{y} x_1^2 - \left(\frac{y \bar{y} + c_1^2 - c_2^2}{c_1} \right) x_1 + y = 0. \quad (23)$$

For the given $y \in \mathbb{F}_{q^2} \setminus \mathbb{F}_{q_0} \cdot H$ and $c_1, c_2 \in \mathbb{F}_{q_0}^*$, if the above quadratic equation has a solution $x_1 \in H$, then by taking $x_2 = \frac{y - c_1 x_1}{c_2}$, it is easy to see that $x_2 \in H$ and this pair $(x_1, x_2) \in H^2$ satisfies Eq (22). So to study Eq (22), we just need to study Eq (23).

The discriminant of the quadratic equation (23) is

$$\Delta := \left(\frac{y \bar{y} + c_1^2 - c_2^2}{c_1} \right)^2 - 4y \bar{y},$$

and according to Lemma 6, the number of solutions $x_1 \in H$ to Eq (23) is exactly $1 - \chi(\Delta)$, here χ is the quadratic character of $\mathbb{F}_q$. So $\rho(C_s(q_0)) = 2$ if and only if for any $y \in \mathbb{F}_{q^2} \setminus \mathbb{F}_{q_0} \cdot H$, there exist $(c_1, c_2) \in \mathbb{F}_{q_0}^{*2}$ such that

$$1 - \chi(\Delta) > 0,$$

and thus $\rho(C_s(q_0)) = 3$ if and only if there exists $y \in \mathbb{F}_{q^2} \setminus \mathbb{F}_{q_0} \cdot H$ such that for any $(c_1, c_2) \in \mathbb{F}_{q_0}^{*2}$ we have

$$1 - \chi(\Delta) = 0 \iff \Delta \in \square_q \subseteq \mathbb{F}_q^*.$$

We summarize the above in the following lemma.

Lemma 10. *Let q_0 be odd and $s \geq 2$. Then $\rho(C_s(q_0)) = 3$ if and only if there exists $y \in \mathbb{F}_{q^2} \setminus \mathbb{F}_{q_0} \cdot H$ such that*

$$\left(\frac{y \bar{y} + c_1^2 - c_2^2}{c_1} \right)^2 - 4y \bar{y} \in \square_q, \quad \forall c_1, c_2 \in \mathbb{F}_{q_0}^*. \quad (24)$$

Let us simplify Eq (24) further in Lemma 10. It is easy to see that

$$(y \bar{y} + c_1^2 - c_2^2)^2 - 4c_1^2 y \bar{y} = (y \bar{y} - (c_1 + c_2)^2)(y \bar{y} - (c_1 - c_2)^2).$$

Setting

$$\alpha = c_1 + c_2, \quad \beta = c_1 - c_2,$$

then

$$c_1 = \frac{1}{2}(\alpha + \beta), \quad c_2 = \frac{1}{2}(\alpha - \beta).$$

It is easy to see that

$$c_1, c_2 \in \mathbb{F}_{q_0}^* \iff \alpha \neq \pm\beta \iff \alpha^2 \neq \beta^2, \alpha, \beta \in \mathbb{F}_{q_0}.$$

So Eq (24) is equivalent to

$$(y\bar{y} - \alpha^2)(y\bar{y} - \beta^2) \in \square_q, \quad \forall \alpha, \beta \in \mathbb{F}_{q_0} \text{ with } \alpha^2 \neq \beta^2.$$

Considering the case that $\alpha = 0$, the above can be further simplified as

$$y\bar{y}(y\bar{y} - \beta) \in \square_q, \quad \forall \beta \in \square_{q_0}.$$

Finally, $y \in \mathbb{F}_{q^2} \setminus \mathbb{F}_{q_0} \cdot H$ if and only if $y\bar{y} \in \mathbb{F}_q^* \setminus \square_{q_0}$. Summarizing the above results, we obtain the following simplified characterization.

Theorem 5. *Let q_0 be odd and $s \geq 2$. Then $\rho(C_s(q_0)) = 3$ if and only if there exists $x \in \mathbb{F}_q^* \setminus \square_{q_0}$ such that*

$$x(x - \beta) \in \square_q, \quad \forall \beta \in \square_{q_0}.$$

Otherwise $\rho(C_s(q_0)) = 2$.

As consequences of Theorem 5, we collect below several results about $\rho(C_s(q_0))$ for some special q_0 and s .

Corollary 2. *Let q_0 be odd. If $s \geq 3$ is odd and*

$$s < 1 + \frac{1}{2} \left(\sqrt{q_0} - \frac{1}{\sqrt{q_0}} \right), \quad (25)$$

then $\rho(C_s(q_0)) = 2$.

Proof. Suppose $\rho(C_s(q_0)) = 3$, by Theorem 5, there is an element $x_0 \in \mathbb{F}_q^* \setminus \square_{q_0}$ such that

$$x_0(x_0 - \beta) \in \square_q, \quad \forall \beta \in \square_{q_0}.$$

Let t be the least positive integer such that $x_0 \in \mathbb{F}_{q_0^t}$. Since $q = q_0^s$, obviously $t|s$. For any fixed $\beta \in \square_{q_0}$, since $x_0(x_0 - \beta) \in \square_q$, we have

$$(x_0(x_0 - \beta))^{q_0^i} = x_0^{q_0^i} \left(x_0^{q_0^i} - \beta \right) \in \square_q, \quad \forall 0 \leq i \leq t-1.$$

Multiplying these terms together for $0 \leq i \leq t-1$, also noting that s is odd, we find that

$$\mathbf{N}_{\mathbb{F}_{q_0^t}/\mathbb{F}_{q_0}}(x_0(x_0 - \beta)) = \mathbf{N}_{\mathbb{F}_{q_0^t}/\mathbb{F}_{q_0}}(x_0) \mathbf{N}_{\mathbb{F}_{q_0^t}/\mathbb{F}_{q_0}}(x_0 - \beta) \in \square_q \cap \mathbb{F}_{q_0} = \square_{q_0}, \quad \forall \beta \in \square_{q_0}. \quad (26)$$

Here $\mathbf{N}_{\mathbb{F}_{q_0^t}/\mathbb{F}_{q_0}} : \mathbb{F}_{q_0^t} \rightarrow \mathbb{F}_{q_0}$ is the Norm function given by $\mathbf{N}_{\mathbb{F}_{q_0^t}/\mathbb{F}_{q_0}}(x) = x \cdot x^{q_0} \cdots x^{q_0^{t-1}}$ for any $x \in \mathbb{F}_{q_0^t}$.

Now we evaluate this norm function explicitly. Let $f(X)$ be the monic irreducible polynomial of x_0 over $\mathbb{F}_{q_0}$. Then $f(X) \in \mathbb{F}_{q_0}[X]$, $\deg f = t$ and

$$f(X) = \prod_{i=0}^{t-1} (X - x_0^{q_0^i}),$$

so we find

$$f(0) = (-x_0) \cdot (-x_0^{q_0}) \cdots (-x_0^{q_0^{t-1}}) = (-1)^t \mathbf{N}_{\mathbb{F}_{q_0^t}/\mathbb{F}_{q_0}}(x_0).$$

Since $t|s$ and s is odd, we have

$$\mathbf{N}_{\mathbb{F}_{q_0^t}/\mathbb{F}_{q_0}}(x_0) = -f(0). \quad (27)$$

Next, denote

$$g_\beta(X) := f(X + \beta), \quad \forall \beta \in \square_{q_0}.$$

It is easy to see that $g_\beta(X)$ is the monic irreducible polynomial of $x_0 - \beta$ over $\mathbb{F}_{q_0}$. From Eq (27) we obtain

$$N_{\mathbb{F}_{q_0}/\mathbb{F}_{q_0}}(x_0 - \beta) = -g_\beta(0) = -f(\beta). \quad (28)$$

Plugging (27) and (28) into Eqs (26) we find that

$$f(0)f(\beta) \in \square_{q_0}, \quad \forall \beta \in \square_{q_0}, \quad (29)$$

where $f(X) \in \mathbb{F}_{q_0}[X]$ is the monic irreducible polynomial of x_0 over $\mathbb{F}_{q_0}$.

Let χ denote the quadratic character defined on $\mathbb{F}_{q_0}$. Eqs (29) imply that

$$\chi(f(x^2)) = \chi(f(0)) \in \{\pm 1\}, \quad \forall x \in \mathbb{F}_{q_0}.$$

So we have

$$A := \left| \sum_{x \in \mathbb{F}_{q_0}} \chi(f(x^2)) \right| = q_0. \quad (30)$$

On the other hand, denote $g(X) := f(X^2)$. Let $\lambda \in \mathbb{F}_{q_2}^*$ be such that $\lambda^2 = x_0$, then $(\pm \lambda^{q_0^i})^2 = \lambda^{2q_0^i} = x_0^{q_0^i}$ for any $0 \leq i \leq t-1$, from (27) we can obtain

$$g(X) = \prod_{i=0}^{t-1} (X^2 - x_0^{q_0^i}) = \prod_{i=0}^{t-1} (X - \lambda^{q_0^i}) (X + \lambda^{q_0^i}).$$

It is easy to see that all the roots $\pm \lambda^{q_0^i}, 0 \leq i \leq t-1$ are distinct: suppose $\varepsilon_1 \lambda^{q_0^i} = \varepsilon_2 \lambda^{q_0^j}$ for some $\varepsilon_1, \varepsilon_2 \in \{\pm 1\}$ and $0 \leq i, j \leq t-1$. Taking squares on both sides, we obtain $x_0^{q_0^i} = x_0^{q_0^j}$, thus $i = j$ from which we also obtain $\varepsilon_1 = \varepsilon_2$. So $g(X)$ is not a square of polynomials. By Lemma 3 we obtain

$$A = \left| \sum_{x \in \mathbb{F}_{q_0}} \chi(f(x^2)) \right| = \left| \sum_{x \in \mathbb{F}_{q_0}} \chi(g(x)) \right| \leq 1 + (2t-2)\sqrt{q_0}. \quad (31)$$

Combining (30) and (31), we obtain

$$A = q_0 \leq 1 + (2t-2)\sqrt{q_0} \leq 1 + (2s-2)\sqrt{q_0}.$$

That is,

$$2(s-1) \geq \sqrt{q_0} - \frac{1}{\sqrt{q_0}} \implies s \geq 1 + \frac{1}{2} \left(\sqrt{q_0} - \frac{1}{\sqrt{q_0}} \right).$$

This contradicts the assumption that $s < 1 + \frac{1}{2} \left(\sqrt{q_0} - \frac{1}{\sqrt{q_0}} \right)$. This completes the proof of Corollary 2. $\square$

For the sake of completeness, we also include the following results from [46].

Corollary 3. *Let q_0 be odd and $s \geq 2$.*

- 0). *If $s \geq 2$, then $\rho(C_s(3)) = 3$;*
- 1). *If $s \geq 2$ is even, then $\rho(C_s(q_0)) = 3$;*
- 2). *If s is odd, and there is $s' | s$ such that $\rho(C_{s'}(q_0)) = 3$, then $\rho(C_s(q_0)) = 3$;*

Proof. Items 0) 1) and 2) were all proved in [46]. In particular they correspond to [46, Corollary III.1, Corollary III.3 and Proposition V.1] respectively. We omit the details. $\square$

Finally, similar to [46, Theorem IV.4] and [48, Theorem 4.8], for any $q_0 \geq 3$ odd and s odd, we prove that if s is sufficiently large, then $\rho(C_s(q_0)) = 3$.

Theorem 6. *Let $q_0 \geq 3$ be odd and $s \geq 3$ be odd. Denote $m := \frac{q_0-1}{2}$. If*

$$q_0^s - q_0^{s/2} ((m-3)2^{m-1} + 2) > 3 \cdot 2^{m-1} - 1, \quad (32)$$

then $\rho(C_s(q_0)) = 3$.

Proof. If $q_0 = 3$, then $m = 1$, it is easy to check that Eq (32) holds for $s = 3$. Since it was known that $\rho(C_s(3)) = 3$ for any $s \geq 2$, Theorem 6 holds for this case. From now on let us assume that $q_0 \geq 5$.

Denote by N the number of $y \in \mathbb{F}_q^* \setminus \square_{q_0}$ such that

$$y(y - \beta) \in \square_q, \quad \forall \beta \in \square_{q_0}.$$

We shall prove that $N > 0$ if $s \geq 3$ is odd and s satisfies Eq (32). This would imply $\rho(C_s(q_0)) = 3$ thanks to Theorem 5.

Let

$$\square_{q_0} = \{b_1, \dots, b_m\}$$

and $\chi : \mathbb{F}_q^* \rightarrow \{\pm 1\}$ be the quadratic character. We have

$$N = \sum_{y \in \mathbb{F}_q^* \setminus \square_{q_0}} \prod_{i=1}^m \frac{1}{2} \{1 + \chi(y(y - b_i))\} = \frac{1}{2^m} (A - B), \quad (33)$$

where

$$\begin{aligned} A &= \sum_{y \in \mathbb{F}_q^*} \prod_{i=1}^m \{1 + \chi(y(y - b_i))\}, \\ B &= \sum_{y \in \square_{q_0}} \prod_{i=1}^m \{1 + \chi(y(y - b_i))\}. \end{aligned} \quad (34)$$

We deal with B first. Since s is odd and $q = q_0^2$, $\square_{q_0} \subseteq \square_q$, so we have

$$B = \sum_{y \in \square_{q_0}} \prod_{i=1}^m \{1 + \chi(y(y - b_i))\} = \sum_{y \in \square_{q_0}} \prod_{\beta \in \square_{q_0}} \{1 + \chi(y - \beta)\}.$$

We claim that for any fixed $y \in \square_{q_0}$, there is $\beta \in \square_{q_0}$ such that $\chi(y - \beta) = -1$. The proof is simple: first, since s is odd, χ can be considered as the quadratic character defined on $\mathbb{F}_{q_0}$. Now suppose the claim is not true, then $\chi(y - \beta) = 1$ for any $\beta \in \square_{q_0} \setminus \{y\}$, so as $q_0 \geq 5$ we have

$$\sum_{x \in \mathbb{F}_{q_0}} \chi(y - x^2) = 1 + 2 \sum_{\beta \in \square_{q_0} \setminus \{y\}} \chi(y - \beta) = 1 + 2(m-1) = q_0 - 2 \geq 3. \quad (35)$$

On the other hand, by Lemma 2 we have

$$\left| \sum_{x \in \mathbb{F}_{q_0}} \chi(y - x^2) \right| = 1,$$

which clearly contradicts (35). So the claim is proved, and hence $B = 0$.

Now we deal with the quantity A . Expanding the right hand side of Eq (34) and noting that χ is multiplicative, we have

$$A = \sum_{y \in \mathbb{F}_q^*} \left\{ 1 + \sum_{\emptyset \neq I \subseteq [m]} \chi \left(y^{\#I} \prod_{i \in I} (y - b_i) \right) \right\} = q - 1 + A_1, \quad (36)$$

where

$$A_1 = \sum_{\emptyset \neq I \subseteq [m]} \sum_{y \in \mathbb{F}_q^*} \chi(y)^{\#I} \chi \left(\prod_{i \in I} (y - b_i) \right). \quad (37)$$

Denote

$$T = \left| \sum_{y \in \mathbb{F}_q^*} \chi(y)^{\#I} \chi \left(\prod_{i \in I} (y - b_i) \right) \right|.$$

If $\#I$ is odd, then by Lemma 3

$$T = \left| \sum_{y \in \mathbb{F}_q} \chi \left(y \prod_{i \in I} (y - b_i) \right) \right| \leq 1 + (\#I + 1 - 2) \sqrt{q} = 1 + (\#I - 1) \sqrt{q}. \quad (38)$$

If $\#I$ is even, then by Lemma 3 again

$$\begin{aligned} T &= \left| \sum_{y \in \mathbb{F}_q^*} \chi \left(\prod_{i \in I} (y - b_i) \right) \right| \leq 1 + \left| \sum_{y \in \mathbb{F}_q} \chi \left(\prod_{i \in I} (y - b_i) \right) \right| \\ &\leq 1 + 1 + (\#I - 2) \sqrt{q} = 2 + (\#I - 2) \sqrt{q}. \end{aligned} \quad (39)$$

Plugging the estimates (38) and (39) into the right side of (37), we obtain

$$|A_1| \leq \sum_{\substack{\emptyset \neq I \subseteq [m] \\ \#I \text{ odd}}} \{1 + (\#I - 1) \sqrt{q}\} + \sum_{\substack{\emptyset \neq I \subseteq [m] \\ \#I \text{ even}}} \{2 + (\#I - 2) \sqrt{q}\}.$$

From the elementary identities

$$\begin{aligned} \sum_{\substack{\emptyset \neq I \subseteq [m] \\ \#I \text{ odd}}} 1 &= \sum_{i \text{ odd}} \binom{m}{i} = 2^{m-1}, \\ \sum_{\substack{\emptyset \neq I \subseteq [m] \\ \#I \text{ even}}} 1 &= \sum_{0 < i \text{ even}} \binom{m}{i} = 2^{m-1} - 1, \\ \sum_{\emptyset \neq I \subseteq [m]} \#I &= \sum_{i=1}^m \binom{m}{i} i = m \cdot 2^{m-1}, \end{aligned}$$

we can obtain easily that

$$|A_1| \leq (3 \cdot 2^{m-1} - 2) + \sqrt{q}((m-3) \cdot 2^{m-1} + 2).$$

Finally, noting (33), (36) and $B = 0$, we obtain

$$2^m \cdot N = q - 1 + A_1 - B \geq q - 1 - \{(3 \cdot 2^{m-1} - 2) + \sqrt{q}((m-3) \cdot 2^{m-1} + 2)\}.$$

Now it is clear that if s satisfies (32), then $2^m \cdot N > 0$ and hence $N > 0$ as desired. This completes the proof of Theorem 6. $\square$

It is interesting to compare Theorem 6 with [46, Theorem IV.4] and [48, Theorem 4.8] which state that if $q_0 \geq 5$ and $s \geq 3$ are both odd and satisfy

$$q_0^s - q_0^{s/2}((m-2)2^m + 2) > 2^m - 1, \quad (40)$$

then $\rho(C_s((q_0))) = 3$. While the bound on s from (32) looks stronger than that from (40), they are essentially of the same quality, as seen from the following lemma.

Lemma 11. For any odd prime power q_0 , denote by $s_*(q_0) \geq 3$ and $s'_*(q_0) \geq 3$ the least odd number satisfying (32) and (40) respectively. If $q_0 \geq 13$, then

i). $s_*(q_0)$ is an odd number in the range

$$\frac{q_0 \log 2 - 5}{\log q_0} + 2 < s_*(q_0) < \frac{q_0 \log 2 - 5 \log 2}{\log q_0} + 4. \quad (41)$$

ii). $s'_*(q_0) - s_*(q_0) \in \{0, 2\}$.

Proof. i). For a fixed $q_0 \geq 13$, denote by s_1, s_2 the unique positive real numbers such that

$$q_0^{s_1/2} = (m-3)2^{m-1} + 2, \quad q_0^{s_2/2} = (m-3)2^{m-1} + 3. \quad (42)$$

We claim that

$$s_1 < s_*(q_0) < s_2 + 2. \quad (43)$$

The lower bound of $s_*(q_0)$ in (43) is obvious. As for the upper bound, let $s' := \lceil s_2 \rceil \geq s_2$. By (42) and nothing that $m \geq 6$ we have

$$\begin{aligned} q_0^{s'} - q_0^{s_2/2} ((m-3)2^{m-1} + 2) &\geq q_0^{s_2} - q_0^{s_2/2} ((m-3)2^{m-1} + 2) \\ &= q_0^{s_2/2} = (m-3)2^{m-1} + 2 > 3 \cdot 2^{m-1} - 1. \end{aligned}$$

Since $s_*(q_0)$ is the least odd number satisfying Eq (32), we must have $s_*(q_0) \leq \lceil s_2 \rceil + 1 < s_2 + 2$, which is the desired upper bound. So the claim (43) is proved.

Now we estimate s_1 and s_2 . From (42) it is easy to check that

$$s_i = 2 + \frac{q_0 \log 2 - 5 \log 2}{\log q_0} + \frac{2 \log \left(1 - \frac{7}{q_0} + \frac{\delta_i}{q_0 \sqrt{2^{q_0-5}}} \right)}{\log q_0}, \quad \delta_1 = 2, \delta_2 = 3. \quad (44)$$

It is easy to check, with the help of MAGMA or MATHEMATICA that whenever $q_0 \geq 13$ the following hold:

$$\begin{aligned} s_1 - \frac{q_0 \log 2 - 5}{\log q_0} - 2 &= \frac{1}{\log q_0} \left(5 - 5 \log 2 + 2 \log \left(1 - \frac{7}{q_0} + \frac{2}{q_0 \sqrt{2^{q_0-5}}} \right) \right) > 0, \\ s_2 - \frac{q_0 \log 2 - 5 \log 2}{\log q_0} - 2 &= \frac{2}{\log q_0} \log \left(1 - \frac{7}{q_0} + \frac{2}{q_0 \sqrt{2^{q_0-5}}} \right) < 0, \end{aligned}$$

that is,

$$\frac{q_0 \log 2 - 5}{\log q_0} + 2 < s_1 < s_2 < \frac{q_0 \log 2 - 5 \log 2}{\log q_0} + 2, \quad \forall q_0 \geq 13.$$

Plugging this into Eq (43), we obtain (41) as desired.

ii). Denote by s'_1, s'_2 the unique positive real numbers such that

$$q_0^{s'_1/2} = (m-2)2^m + 2, \quad q_0^{s'_2/2} = (m-2)2^m + 3.$$

By using the same argument as in i), we have

$$s'_1 < s'_*(q_0) < s'_2 + 2,$$

and s'_1, s'_2 can be computed as

$$s'_i = 2 + \frac{q_0 \log 2 - 3 \log 2}{\log q_0} + \frac{2 \log \left(1 - \frac{5}{q_0} + \frac{\delta_i}{q_0 \sqrt{2^{q_0-3}}} \right)}{\log q_0}, \quad \delta_1 = 2, \delta_2 = 3. \quad (45)$$

Thus we have

$$0 \leq s'_*(q_0) - s_*(q_0) < s'_2 + 2 - s_1.$$

Using the expressions of s_1 in (44) and of s'_2 in (45), it is easy to check by MAGMA that when $q_0 \geq 13$,

$$s'_2 - s_1 = \frac{2}{\log q_0} \left(\log 2 + \log \frac{1 - \frac{5}{q_0} + \frac{3}{q_0 \sqrt{2^{q_0-3}}}}{1 - \frac{7}{q_0} + \frac{2}{q_0 \sqrt{2^{q_0-5}}}} \right) < 1,$$

so $0 \leq s'_*(q_0) - s_*(q_0) < 3$. Since both $s'_*(q_0)$ and $s_*(q_0)$ are odd, we have $s'_*(q_0) - s_*(q_0) \in \{0, 2\}$ as desired. $\square$

Remark 1. In Table 1 we list the values $s_*(q_0)$ and $s'_*(q_0)$ for all odd prime powers $5 \leq q_0 \leq 59$ which we computed by MAGMA. The data in Table 1 confirms Lemma 11.

TABLE I
COMPARISON OF $s_*(q_0)$ AND $s'_*(q_0)$ WHICH WERE DERIVED FROM (32) AND (40) RESPECTIVELY.

q_0	5	7	9	11	13	17	19	23	25	27	29	31	37	41	43	47	49	53	59
$s_*(q_0)$	3	3	3	3	5	5	5	7	7	7	7	9	9	9	9	11	11	11	13
$s'_*(q_0)$	3	3	5	5	5	7	7	7	7	7	9	9	9	11	11	11	11	11	13

We can summarize Corollaries 2, 3, Theorem 6 and Lemma 11 in the following proposition. For the sake of completeness, we also include the trivial case that $s = 1$. For q_0 odd, let us define $s^*(q_0) \geq 3$ to be the largest odd number s satisfying (25).

Proposition 1. Let q_0 be odd. The covering radius of $C_s(q_0)$ is given by

- i). If $s = 1$, then $\rho(C_s(q_0)) = 2$;
- ii). If $s \geq 2$ is even, then $\rho(C_s(q_0)) = 3$;
- iii). If $s \geq 3$ is odd, and $s \leq s^*(q_0)$, then $\rho(C_s(q_0)) = 2$;
- iv). If $s \geq 3$ is odd, and $s \geq s_*(q_0)$, then $\rho(C_s(q_0)) = 3$;
- v). If $s \geq 3$ is odd, and $s' | s$ with $\rho(C_{s'}(q_0)) = 3$, then $\rho(C_s(q_0)) = 3$.

In Table VI below, we list the values $s^*(q_0)$ and $s_*(q_0)$ for odd prime powers q_0 such that $3 \leq q_0 \leq 59$. We also list the missing odd numbers s in the interval $(s^*(q_0), s_*(q_0))$ that $\rho(C_s(q_0))$ is not yet determined.

The computations performed using MAGMA agree perfectly with Proposition 1. For the missing odd s in $(s^*(q_0), s_*(q_0))$, for example, we have $\rho(C_3(13)) = 3, \rho(C_3(17)) = 2, \rho(C_5(23)) = 3, \rho(C_5(25)) = 3, \rho(C_5(27)) = 3, \rho(C_5(29)) = 3$.

Since $\rho(C_s(q_0)) = \rho(\widetilde{C_s(q_0)})$ when q_0 is odd, the following proposition holds.

Proposition 2. Let q_0 be odd. The covering radius of $\widetilde{C_s(q_0)}$ is given by

- i). If $s = 1$, then $\rho(\widetilde{C_s(q_0)}) = 2$;
- ii). If $s \geq 2$ is even, then $\rho(\widetilde{C_s(q_0)}) = 3$;
- iii). If $s \geq 3$ is odd, and $s \leq s^*(q_0)$, then $\rho(\widetilde{C_s(q_0)}) = 2$;
- iv). If $s \geq 3$ is odd, and $s \geq s_*(q_0)$, then $\rho(\widetilde{C_s(q_0)}) = 3$;
- v). If $s \geq 3$ is odd, and $s' | s$ with $\rho(\widetilde{C_{s'}(q_0)}) = 3$, then $\rho(\widetilde{C_s(q_0)}) = 3$.

TABLE II

FOR EACH q_0 , $s^*(q_0) \geq 3$ IS THE LARGEST ODD NUMBER SATISFYING (25), $s_*(q_0) \geq 3$ IS THE LEAST ODD NUMBER SATISFYING (32).

q_0	s^*	s_*	the set of missing odd numbers in (s^*, s_*)
3		3	$\emptyset$
5		3	$\emptyset$
7		3	$\emptyset$
9		3	$\emptyset$
11		3	$\emptyset$
13		5	$\{3\}$
17		5	$\{3\}$
19	3	5	$\emptyset$
23	3	7	$\{5\}$
25	3	7	$\{5\}$
27	3	7	$\{5\}$
29	3	7	$\{5\}$
31	3	9	$\{5, 7\}$
37	3	9	$\{5, 7\}$
41	3	9	$\{5, 7\}$
43	3	9	$\{5, 7\}$
47	3	11	$\{5, 7, 9\}$
49	3	11	$\{5, 7, 9\}$
53	3	11	$\{5, 7, 9\}$
59	3	13	$\{5, 7, 9, 11\}$

VII. DETERMINING COVERING RADIUS OF $C_s(q_0)$: q_0 EVEN

Let $q_0 \geq 2$ be even and $s \geq 2$. It is known by Corollary 1 that $\rho(C_s(q_0)) \in \{2, 3\}$. In this section we study explicit conditions to distinguish these two cases.

We know by the proof of Theorem 4 that $\rho(C_s(q_0)) = 2$ if and only if for any $\alpha \in \mathbb{F}_q \setminus \mathbb{F}_{q_0}$ (note that the case $\alpha \in \mathbb{F}_{q_0}$ is trivial), there exist $(c_1, c_2) \in \mathbb{F}_{q_0}^{*2}$ and $(x_1, x_2) \in H^2$ such that

$$\alpha = c_1 x_1 + c_2 x_2. \quad (46)$$

Taking the q -th power on both sides of the above equation, we obtain

$$\alpha = c_1 \bar{x}_1 + c_2 \bar{x}_2.$$

Hence, x_1 satisfies the equation

$$(c_1 x_1 + \alpha)(c_1 \bar{x}_1 + \alpha) = c_2^2,$$

which simplifies to

$$x_1^2 + \frac{\alpha^2 + c_1^2 + c_2^2}{\alpha c_1} x_1 + 1 = 0. \quad (47)$$

For the given $\alpha \in \mathbb{F}_q \setminus \mathbb{F}_{q_0}$ and $c_1, c_2 \in \mathbb{F}_{q_0}^*$, if the above quadratic equation has a solution $x_1 \in H$, then by taking $x_2 = \frac{\alpha + c_1 x_1}{c_2}$, it is easy to see that $x_2 \in H$ and this pair $(x_1, x_2) \in H^2$ satisfies Eq (46). So to study Eq (46), we just need to study Eq (47).

Since $\frac{\alpha^2 + c_1^2 + c_2^2}{\alpha c_1} \neq 0$ as $\alpha \in \mathbb{F}_q \setminus \mathbb{F}_{q_0}$ and $c_1, c_2 \in \mathbb{F}_{q_0}^*$, by Lemma 8, Eq (47) has a solution $x_1 \in H$ if and only if

$$\text{Tr}_{\mathbb{F}_q/\mathbb{F}_2} \left(\left(\frac{\alpha c_1}{(\alpha + c_1 + c_2)^2} \right)^2 \right) = \text{Tr}_{\mathbb{F}_q/\mathbb{F}_2} \left(\frac{\alpha c_1}{(\alpha + c_1 + c_2)^2} \right) = 1.$$

Note that

$$\text{Tr}_{\mathbb{F}_q/\mathbb{F}_2} \left(\frac{\alpha c_1}{(\alpha + c_1 + c_2)^2} \right)$$

$$\begin{aligned}
&= \text{Tr}_{\mathbb{F}_q/\mathbb{F}_2} \left(\frac{c_1(\alpha + c_1 + c_2)}{(\alpha + c_1 + c_2)^2} \right) + \text{Tr}_{\mathbb{F}_q/\mathbb{F}_2} \left(\frac{c_1(c_1 + c_2)}{(\alpha + c_1 + c_2)^2} \right) \\
&= \text{Tr}_{\mathbb{F}_q/\mathbb{F}_2} \left(\frac{c_1}{\alpha + c_1 + c_2} \right) + \text{Tr}_{\mathbb{F}_q/\mathbb{F}_2} \left(\frac{c_1^2}{(\alpha + c_1 + c_2)^2} \right) + \text{Tr}_{\mathbb{F}_q/\mathbb{F}_2} \left(\frac{c_1 c_2}{(\alpha + c_1 + c_2)^2} \right) \\
&= \text{Tr}_{\mathbb{F}_q/\mathbb{F}_2} \left(\frac{c_1 c_2}{(\alpha + c_1 + c_2)^2} \right).
\end{aligned}$$

The above derivation shows that the existence of a solution $x_1 \in H$ to Eq (47) is equivalent to the condition:

$$\text{Tr}_{\mathbb{F}_q/\mathbb{F}_2} \left(\frac{c_1 c_2}{(\alpha + c_1 + c_2)^2} \right) = 1.$$

This directly leads to the characterization of conditions under which $\rho(C_s(q_0)) = 2$. Specifically, for $\rho(C_s(q_0)) = 2$, this condition must hold for all $\alpha \in \mathbb{F}_q \setminus \mathbb{F}_{q_0}$, while for $\rho(C_s(q_0)) = 3$, it must fail for at least one such α . We summarize these results in the following lemma.

Lemma 12. *Let q_0 be even and $s \geq 2$. Then $\rho(C_s(q_0)) = 2$ if and only if for every $\alpha \in \mathbb{F}_q \setminus \mathbb{F}_{q_0}$, there exist $c_1, c_2 \in \mathbb{F}_{q_0}^*$ such that*

$$\text{Tr}_{\mathbb{F}_q/\mathbb{F}_2} \left(\frac{c_1 c_2}{(\alpha + c_1 + c_2)^2} \right) = 1.$$

Otherwise $\rho(C_s(q_0)) = 3$ if and only if there exists $\alpha \in \mathbb{F}_q \setminus \mathbb{F}_{q_0}$ such that

$$\text{Tr}_{\mathbb{F}_q/\mathbb{F}_2} \left(\frac{c_1 c_2}{(\alpha + c_1 + c_2)^2} \right) = 0, \quad \forall c_1, c_2 \in \mathbb{F}_{q_0}^*. \quad (48)$$

Let us simplify Eq (48) further in Lemma 12. Suppose Eq (48) holds for any $c_1, c_2 \in \mathbb{F}_{q_0}^*$. Obvious it also holds when $c_1 = 0$ or $c_2 = 0$. Next for $c_1, c_2 \in \mathbb{F}_{q_0}$, define

$$c_1 c_2 = a, \quad c_1 + c_2 = b, \quad (49)$$

where $a, b \in \mathbb{F}_{q_0}$. If $b = 0$, then $c_1 = c_2$, so in this case Eq (48) reduces to $\text{Tr}_{\mathbb{F}_q/\mathbb{F}_2} (c_1/\alpha) = 0$ for any $c_1 \in \mathbb{F}_{q_0}$. Rewriting this as

$$\text{Tr}_{\mathbb{F}_q/\mathbb{F}_2} (c_1/\alpha) = \text{Tr}_{\mathbb{F}_{q_0}/\mathbb{F}_2} \left(c_1 \text{Tr}_{\mathbb{F}_q/\mathbb{F}_{q_0}} (1/\alpha) \right) = 0, \quad \forall c_1 \in \mathbb{F}_{q_0},$$

we easily derive

$$\text{Tr}_{\mathbb{F}_q/\mathbb{F}_{q_0}} (1/\alpha) = 0. \quad (50)$$

If $b \neq 0$, then by Lemma 7, the quadratic equation $x^2 + bx + a = 0$ has two distinct roots $x = c_1, c_2$ in $\mathbb{F}_{q_0}$ satisfying Eq (49) if and only if

$$\text{Tr}_{\mathbb{F}_{q_0}/\mathbb{F}_2} (a/b^2) = 0. \quad (51)$$

Let $a = b^2 t$. Then Eq (51) implies that $\text{Tr}_{\mathbb{F}_{q_0}/\mathbb{F}_2} (t) = 0$, which means $t = \tau^2 + \tau$ for some $\tau \in \mathbb{F}_{q_0}$. Substituting $a = b^2 t = b^2 (\tau^2 + \tau)$ into (48), noting $c_1 c_2 = a, c_1 + c_2 = b$, we obtain

$$\text{Tr}_{\mathbb{F}_q/\mathbb{F}_2} \left(\frac{b^2 (\tau^2 + \tau)}{(\alpha + b)^2} \right) = 0, \quad \forall b \in \mathbb{F}_{q_0}^*, \tau \in \mathbb{F}_{q_0}.$$

This can be written as

$$\text{Tr}_{\mathbb{F}_{q_0}/\mathbb{F}_2} \left(\tau \text{Tr}_{\mathbb{F}_q/\mathbb{F}_{q_0}} \left(\frac{b}{\alpha + b} + \frac{b^2}{(\alpha + b)^2} \right) \right) = 0, \quad \forall b \in \mathbb{F}_{q_0}^*, \tau \in \mathbb{F}_{q_0}.$$

So we have

$$\text{Tr}_{\mathbb{F}_q/\mathbb{F}_{q_0}} \left(\frac{b}{\alpha + b} + \frac{b^2}{(\alpha + b)^2} \right) = 0, \quad \forall b \in \mathbb{F}_{q_0}^*,$$

from which we conclude easily that

$$\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_{q_0}}\left(\frac{b}{\alpha+b}\right) \in \{0, 1\}, \quad \forall b \in \mathbb{F}_{q_0}^*.$$

Combining this and Eq (50), we find that Eq (48) in Lemma 12 is equivalent to

- 1) $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_{q_0}}\left(\frac{1}{\alpha}\right) = 0$, and
- 2) $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_{q_0}}\left(\frac{b}{\alpha+b}\right) \in \{0, 1\}$ for all $b \in \mathbb{F}_{q_0}^*$.

By substitution $\alpha \rightarrow \frac{1}{\alpha}$, we obtain the following simplified characterization.

Theorem 7. *Let $q_0 \geq 2$ be even and $s \geq 2$. Then $\rho(C_s(q_0)) = 3$ if and only if there exists $\alpha \in \mathbb{F}_q \setminus \mathbb{F}_{q_0}$ such that*

- 1) $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_{q_0}}(\alpha) = 0$, and
- 2) $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_{q_0}}\left(\frac{1}{1+b\alpha}\right) \in \{0, 1\}$ for all $b \in \mathbb{F}_{q_0}^*$.

Otherwise $\rho(C_s(q_0)) = 2$.

As simple consequences of Theorem 7, we collect below several results about $\rho(C_s(q_0))$ for some special q_0 and s .

Corollary 4. *Let q_0 be even and $s \geq 2$ be a positive integer. If $s = 2$ or if $s \geq 3$ is odd and $s \leq \frac{q_0}{2}$, then $\rho(C_s(q_0)) = 2$.*

Proof. If $s = 2$ then $q = q_0^2$, for any $\alpha \in \mathbb{F}_q$,

$$\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_{q_0}}(\alpha) = \alpha + \alpha^{q_0} = 0 \implies \alpha \in \mathbb{F}_{q_0}.$$

So there is no $\alpha \in \mathbb{F}_q \setminus \mathbb{F}_{q_0}$ such that $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_{q_0}}(\alpha) = 0$, by Theorem 7, $\rho(C_s(q_0)) = 2$.

Now suppose s is odd and $s \leq q_0/2$. For any $\alpha \in \mathbb{F}_q \setminus \mathbb{F}_{q_0}$, let t be the least positive integer such that $\alpha^{q_0^t} = \alpha$. It is easy to see that $t|s$ and $\alpha, \dots, \alpha^{q_0^{t-1}}$ are distinct elements in $\mathbb{F}_{q_0^t} \subseteq \mathbb{F}_q$. So the rational function $f(x) \in \mathbb{F}_q(x)$ defined by

$$f(x) := \sum_{i=0}^{s-1} \frac{1}{1 + x\alpha^{q_0^i}}$$

satisfies

$$f(x) = \frac{s}{t} \left(\sum_{i=0}^{t-1} \frac{1}{1 + x\alpha^{q_0^i}} \right) = \sum_{i=0}^{t-1} \frac{1}{1 + x\alpha^{q_0^i}}.$$

Let us define

$$g(x) = \sum_{i=0}^{t-1} \frac{1}{1 + x\alpha^{q_0^i}}.$$

Then $g(x)$ is a non-constant rational function defined over $\mathbb{F}_q$. We can write

$$g(x) = \frac{N(x)}{D(x)},$$

where $D(x), N(x) \in \mathbb{F}_q[x]$ are given by

$$D(x) = \prod_{i=0}^{t-1} (1 + x\alpha^{q_0^i}), \quad N(x) = D(x) \left(\sum_{i=0}^{t-1} \frac{1}{1 + x\alpha^{q_0^i}} \right).$$

It is easy to see that $\deg D = t$ and $\deg N \leq t - 1$, and $N \neq 0$.

For any ϵ , denote by N_ϵ the number of solutions $x \in \mathbb{F}_{q_0}$ such that $f(x) = g(x) = \epsilon$, which is equivalent to the equation

$$N(x) + \epsilon D(x) = 0.$$

Since $N(x), D(x) \in \mathbb{F}_q[x]$ are not zero polynomials with $\deg D = t$, $\deg N \leq t - 1$, we have

$$N_0 + N_1 \leq t - 1 + t = 2t - 1 \leq 2s - 1 \leq q_0 - 1,$$

which implies that there is always $b \in \mathbb{F}_{q_0}$ such that

$$\text{Tr}_{\mathbb{F}_q/\mathbb{F}_{q_0}} \left(\frac{1}{1+b\alpha} \right) = \frac{1}{1+b\alpha} + \frac{1}{1+b\alpha^{q_0}} + \cdots + \frac{1}{1+b\alpha^{q_0^{s-1}}} = f(b) \notin \{0, 1\}.$$

Obvioulsy $b \neq 0$. Thus by Theorem 7, $\rho(C_s(q_0)) = 2$. □

Corollary 5. *Let q_0 be even.*

1). *If $s \geq 4$ is even, then $\rho(C_s(q_0)) = 3$.*

2). *If s is odd, and there is $s'|s$ such that $\rho(C_{s'}(q_0)) = 3$, then $\rho(C_s(q_0)) = 3$.*

Proof. 1). Since $s \geq 4$ is even, we have $q = q_0^s = q_1^2$, where $q_1 = q_0^{\frac{s}{2}} > q_0$. Take any $\alpha \in \mathbb{F}_{q_1} \setminus \mathbb{F}_{q_0}$. Then

$$\text{Tr}_{\mathbb{F}_q/\mathbb{F}_{q_0}}(\alpha) = \text{Tr}_{\mathbb{F}_{q_1}/\mathbb{F}_{q_0}}(\alpha \text{Tr}_{\mathbb{F}_q/\mathbb{F}_{q_1}}(1)) = 0,$$

and

$$\text{Tr}_{\mathbb{F}_q/\mathbb{F}_{q_0}} \left(\frac{1}{1+b\alpha} \right) = \text{Tr}_{\mathbb{F}_{q_1}/\mathbb{F}_{q_0}} \left(\frac{1}{1+b\alpha} \text{Tr}_{\mathbb{F}_q/\mathbb{F}_{q_1}}(1) \right) = 0, \quad \forall b \in \mathbb{F}_{q_0}^*.$$

By Theorem 7, $\rho(C_s(q_0)) = 3$.

2). By Theorem 7, since $\rho(C_{s'}(q_0)) = 3$, then there exists $\alpha \in \mathbb{F}_{q_0^{s'}} \setminus \mathbb{F}_{q_0}$, such that $\text{Tr}_{\mathbb{F}_{q_0^{s'}/\mathbb{F}_{q_0}}}(\alpha) = 0$, and $\text{Tr}_{\mathbb{F}_{q_0^{s'}/\mathbb{F}_{q_0}}} \left(\frac{b}{\alpha+b} \right) \in \{0, 1\}$ for all $b \in \mathbb{F}_{q_0}^*$. Since $s'|s$ and s is odd, we have $\mathbb{F}_{q_0^{s'}} \subseteq \mathbb{F}_{q_0^s}$, and $\frac{s}{s'}$ is odd. So

$$\text{Tr}_{\mathbb{F}_{q_0^s}/\mathbb{F}_{q_0}}(\alpha) = \text{Tr}_{\mathbb{F}_{q_0^{s'}/\mathbb{F}_{q_0}}}(\alpha \text{Tr}_{\mathbb{F}_{q_0^s}/\mathbb{F}_{q_0^{s'}}}(1)) = 0$$

and

$$\text{Tr}_{\mathbb{F}_{q_0^s}/\mathbb{F}_{q_0}} \left(\frac{1}{1+b\alpha} \right) = \text{Tr}_{\mathbb{F}_{q_0^{s'}/\mathbb{F}_{q_0}}} \left(\frac{1}{1+b\alpha} \text{Tr}_{\mathbb{F}_{q_0^s}/\mathbb{F}_{q_0^{s'}}}(1) \right) \in \{0, 1\} \quad \forall b \in \mathbb{F}_{q_0}^*.$$

Thus by Theorem 7, we have $\rho(C_s(q_0)) = 3$. □

Finally, for any $q_0 \geq 4$ even and s odd, we prove that if s is sufficiently large, then $\rho(C_s(q_0)) = 3$.

Theorem 8. *Let q_0 be even. If $s \geq 3$ is odd and satisfies*

$$q_0^s - q_0^{s/2} \left(\frac{q_0}{2} \right)^{q_0-1} (2q_0^2 - 7q_0 + 3) > \left(\frac{q_0}{2} \right)^{q_0-1} (4q_0 - 2) - q_0^2, \quad (52)$$

then $\rho(C_s(q_0)) = 3$.

Proof. First, when $q_0 = 2$, it is well-known that $\rho(C_2(2)) = 2$ and $\rho(C_s(2)) = 3$ when $s \geq 3$ (see [20]) and it satisfies Theorem 8, from now on let us assume that $q_0 \geq 4$ is even and $s \geq 3$ is odd.

Since $q = q_0^s$, for simplicity define $\mathbb{F} := \mathbb{F}_q \setminus \mathbb{F}_{q_0}$ and denote by N the number of $y \in \mathbb{F}$ such that $\text{Tr}_{\mathbb{F}_q/\mathbb{F}_{q_0}}(y) = 0$ and $\text{Tr}_{\mathbb{F}_q/\mathbb{F}_{q_0}} \left(\frac{1}{1+by} \right) \in \{0, 1\}$ for all $b \in \mathbb{F}_{q_0}^*$. We shall prove that $N > 0$ if $s \geq 2q_0 + 1$, which implies that $\rho(C_s(q_0)) = 3$ thanks to Theorem 7.

Now we compute the quantity N . Set $\mathbb{F}_{q_0}^* = \{b_1, b_2, \dots, b_r\}$ where $r = q_0 - 1$. For any $\vec{e} = (e_1, \dots, e_r) \in \{0, 1\}^r$, denote by $N_{\vec{e}}$ the number of $y \in \mathbb{F}$ such that

$$\text{Tr}_{\mathbb{F}_q/\mathbb{F}_{q_0}}(y) = 0 \text{ and } \text{Tr}_{\mathbb{F}_q/\mathbb{F}_{q_0}} \left(\frac{1}{1+b_i y} \right) = e_i, \quad \forall 1 \leq i \leq r.$$

By the orthogonal relations of character sums over $\mathbb{F}_q$, we have

$$N_{\vec{e}} = \sum_{y \in \mathbb{F}} \left(\frac{1}{q_0} \sum_{a \in \mathbb{F}_{q_0}} (-1)^{\text{Tr}_{\mathbb{F}_{q_0}/\mathbb{F}_2}(a \text{Tr}_{\mathbb{F}_q/\mathbb{F}_{q_0}}(y))} \right) \prod_{i=1}^r \frac{1}{q_0} \sum_{a_i \in \mathbb{F}_{q_0}} (-1)^{\text{Tr}_{\mathbb{F}_{q_0}/\mathbb{F}_2}(a_i (\text{Tr}_{\mathbb{F}_q/\mathbb{F}_{q_0}}(\frac{1}{1+b_i y}) + e_i))}.$$

Using the standard additive character ψ on $\mathbb{F}_q$ given by $\psi(x) = (-1)^{\text{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(x)}$, we can write

$$N_{\vec{e}} = \frac{1}{q_0^{r+1}} \sum_{y \in \mathbb{F}} \left(1 + \sum_{a \in \mathbb{F}_{q_0}^*} \psi(ay) \right) \prod_{i=1}^r \left\{ 1 + \sum_{a_i \in \mathbb{F}_{q_0}^*} \psi \left(a_i \left(\frac{1}{1+b_i y} + e_i \right) \right) \right\}.$$

The product on the right can be expanded as

$$1 + \sum_{\emptyset \neq I \subseteq [r]} \sum_{\substack{a_i \in \mathbb{F}_{q_0}^* \\ \forall i \in I}} \psi \left(\sum_{i \in I} a_i \left(\frac{1}{1+b_i y} + e_i \right) \right) = 1 + \sum_{\emptyset \neq I \subseteq [r]} \sum_{\substack{a_i \in \mathbb{F}_{q_0}^* \\ \forall i \in I}} \psi \left(\sum_{i \in I} a_i e_i \right) \psi \left(\sum_{i \in I} \frac{a_i}{1+b_i y} \right).$$

So we have

$$\begin{aligned} N &= \sum_{\vec{e} \in \{0,1\}^r} N_{\vec{e}} \\ &= \frac{1}{q_0^{r+1}} \sum_{y \in \mathbb{F}} \left(1 + \sum_{a \in \mathbb{F}_{q_0}^*} \psi(ay) \right) \sum_{\vec{e} \in \{0,1\}^r} \left(1 + \sum_{\emptyset \neq I \subseteq [r]} \sum_{\substack{a_i \in \mathbb{F}_{q_0}^* \\ \forall i \in I}} \psi \left(\sum_{i \in I} a_i e_i \right) \psi \left(\sum_{i \in I} \frac{a_i}{1+b_i y} \right) \right). \end{aligned}$$

The sum over $\vec{e} \in \{0,1\}^r$ on the right is

$$\begin{aligned} &2^r + \sum_{\emptyset \neq I \subseteq [r]} 2^{r-\#I} \sum_{\substack{a_i \in \mathbb{F}_{q_0}^* \\ \forall i \in I}} \sum_{\substack{e_i \in \{0,1\} \\ \forall i \in I}} \psi \left(\sum_{i \in I} a_i e_i \right) \psi \left(\sum_{i \in I} \frac{a_i}{1+b_i y} \right) \\ &= 2^r + \sum_{\emptyset \neq I \subseteq [r]} 2^{r-\#I} \sum_{\substack{a_i \in \mathbb{F}_{q_0}^* \\ \forall i \in I}} \left\{ \prod_{i \in I} (1 + \psi(a_i)) \right\} \psi \left(\sum_{i \in I} \frac{a_i}{1+b_i y} \right). \end{aligned}$$

Denote

$$\mathbb{H}_0 := \left\{ a \in \mathbb{F}_{q_0}^* : \text{Tr}_{\mathbb{F}_{q_0}/\mathbb{F}_2}(a) = 0 \right\}.$$

It is easy to see that $\#\mathbb{H}_0 = q_0/2 - 1$ and

$$\prod_{i \in I} (1 + \psi(a_i)) = \begin{cases} 2^{\#I} & \text{if } a_i \in \mathbb{H}_0 \ \forall i, \\ 0 & \text{otherwise.} \end{cases}$$

So we have

$$\begin{aligned} N &= \frac{2^r}{q_0^{r+1}} \sum_{y \in \mathbb{F}} \left(1 + \sum_{a \in \mathbb{F}_{q_0}^*} \psi(ay) \right) \left(1 + \sum_{\emptyset \neq I \subseteq [r]} \sum_{\substack{a_i \in \mathbb{H}_0 \\ \forall i \in I}} \psi \left(\sum_{i \in I} \frac{a_i}{1+b_i y} \right) \right) \\ &= \frac{2^r}{q_0^{r+1}} (I_0 + I_1 + I_2 + I_3) \end{aligned} \tag{53}$$

where

$$I_0 = \sum_{y \in \mathbb{F}} 1 = q - q_0, \tag{54}$$

$$\begin{aligned}
I_1 &= \sum_{a \in \mathbb{F}_{q_0}^*} \sum_{y \in \mathbb{F}} \psi(ay), \\
I_2 &= \sum_{\emptyset \neq I \subseteq [r]} \sum_{\substack{a_i \in \mathbb{H}_0 \\ \forall i \in I}} \sum_{y \in \mathbb{F}} \psi \left(\sum_{i \in I} \frac{a_i}{1 + b_i y} \right), \\
I_3 &= \sum_{a \in \mathbb{F}_{q_0}^*} \sum_{\emptyset \neq I \subseteq [r]} \sum_{\substack{a_i \in \mathbb{H}_0 \\ \forall i \in I}} \sum_{y \in \mathbb{F}} \psi \left(ay + \sum_{i \in I} \frac{a_i}{1 + b_i y} \right).
\end{aligned}$$

Since s is odd, it is easy to see that

$$I_1 = \sum_{a \in \mathbb{F}_{q_0}^*} \left(\sum_{y \in \mathbb{F}_q} \psi(ay) - \sum_{y \in \mathbb{F}_{q_0}} \psi(ay) \right) = 0. \quad (55)$$

We can use Lemma 5 to give an estimate of I_2 and I_3 respectively. In particular, for I_2 , for each $\emptyset \neq I \subseteq [r]$ and fixed $a_i \in \mathbb{H}_0$ where $i \in I$, for the rational function

$$f(y) = \sum_{i \in I} \frac{a_i}{1 + b_i y} \in \mathbb{F}_q(y),$$

this corresponds to $M = 0$, $L = 2\#I$ in Lemma 5, and consequently

$$\left| \sum_{y \in \mathbb{F}_q \setminus \{b_i^{-1} : i \in I\}} \psi \left(\sum_{i \in I} \frac{a_i}{1 + b_i y} \right) \right| \leq 1 + (2\#I - 2) \sqrt{q}.$$

Hence we have

$$\begin{aligned}
\left| \sum_{y \in \mathbb{F}} \psi \left(\sum_{i \in I} \frac{a_i}{1 + b_i y} \right) \right| &\leq q_0 - \#I + \left| \sum_{y \in \mathbb{F}_q \setminus \{b_i^{-1} : i \in I\}} \psi \left(\sum_{i \in I} \frac{a_i}{1 + b_i y} \right) \right| \\
&\leq q_0 - \#I + 1 + 2(\#I - 1) \sqrt{q}.
\end{aligned}$$

Therefore

$$\begin{aligned}
|I_2| &\leq \sum_{\emptyset \neq I \subseteq [r]} \sum_{\substack{a_i \in \mathbb{H}_0 \\ \forall i \in I}} \left| \sum_{y \in \mathbb{F}} \psi \left(\sum_{i \in I} \frac{a_i}{1 + b_i y} \right) \right| \\
&\leq \sum_{\emptyset \neq I \subseteq [r]} \sum_{\substack{a_i \in \mathbb{H}_0 \\ \forall i \in I}} \left(2(\#I - 1) \sqrt{q} + q_0 - \#I + 1 \right) \\
&= \sum_{i=1}^r \binom{r}{i} \left(\frac{q_0}{2} - 1 \right)^i \left(2(i - 1) \sqrt{q} + q_0 - i + 1 \right). \quad (56)
\end{aligned}$$

As for I_3 , for each $\emptyset \neq I \subseteq [r]$, fixed $a \in \mathbb{F}_{q_0}^*$ and fixed $a_i \in \mathbb{H}_0$ where $i \in I$, for the rational function

$$g(y) = ay + \sum_{i \in I} \frac{a_i}{1 + b_i y} \in \mathbb{F}_q(y),$$

this corresponds to $M = 1$, $L = 2\#I$ in Lemma 5, and consequently

$$\left| \sum_{y \in \mathbb{F}_q \setminus \{b_i^{-1} : i \in I\}} \psi \left(ay + \sum_{i \in I} \frac{a_i}{1 + b_i y} \right) \right| \leq 1 + (2\#I - 1) \sqrt{q}.$$

Hence we have

$$\begin{aligned} \left| \sum_{y \in \mathbb{F}} \psi \left(ay + \sum_{i \in I} \frac{a_i}{1 + b_i y} \right) \right| &\leq q_0 - \#I + \left| \sum_{y \in \mathbb{F}_q \setminus \{b_i^{-1} : i \in I\}} \psi \left(ay + \sum_{i \in I} \frac{a_i}{1 + b_i y} \right) \right| \\ &\leq q_0 - \#I + 1 + (2\#I - 1)\sqrt{q}. \end{aligned}$$

Therefore

$$\begin{aligned} |I_3| &\leq \sum_{a \in \mathbb{F}_{q_0}^*} \sum_{\emptyset \neq I \subseteq [r]} \sum_{\substack{a_i \in \mathbb{H}_0 \\ \forall i \in I}} \left| \sum_{y \in \mathbb{F}} \psi \left(ay + \sum_{i \in I} \frac{a_i}{1 + b_i y} \right) \right| \\ &\leq (q_0 - 1) \sum_{\emptyset \neq I \subseteq [r]} \sum_{\substack{a_i \in \mathbb{H}_0 \\ \forall i \in I}} \left((2\#I - 1)\sqrt{q} + q_0 - \#I + 1 \right) \\ &= (q_0 - 1) \sum_{i=1}^r \binom{r}{i} \left(\frac{q_0}{2} - 1 \right)^i \left((2i - 1)\sqrt{q} + q_0 - i + 1 \right). \end{aligned} \quad (57)$$

By (56) and (57) and a routine computation we have

$$\begin{aligned} |I_2| + |I_3| &\leq \sum_{i=1}^r \binom{r}{i} \left(\frac{q_0}{2} - 1 \right)^i \left(2(i - 1)\sqrt{q} + q_0 - i + 1 + (q_0 - 1) \{ (2i - 1)\sqrt{q} + q_0 - i + 1 \} \right) \\ &= A_1 \sqrt{q} + A_2, \end{aligned} \quad (58)$$

where

$$\begin{aligned} A_1 &= \left(\frac{q_0}{2} \right)^{q_0-1} (2q_0^2 - 7q_0 + 3), \\ A_2 &= \left(\frac{q_0}{2} \right)^{q_0-1} (4q_0 - 2) - q_0^2 - q_0. \end{aligned}$$

Combining (53)–(55) and (58), we obtain

$$\begin{aligned} \frac{q_0^{r+1}}{2^r} N &= I_0 + I_1 + I_2 + I_3 \geq q - q_0 - |I_2| - |I_3| \\ &\geq q - q_0 - A_1 \sqrt{q} - A_2 > 0, \end{aligned}$$

which is exactly Eq (52). This completes the proof of Theorem 8. $\square$

For q_0 even, denote by $s_*(q_0) \geq 3$ the least odd number satisfying (52). We have the following result.

Lemma 13. *Let q_0 be even. Then*

- i). $s_*(2) = 3$ and $s_*(4) = 7$;
- ii). *If $q_0 \geq 8$, then $s_*(q_0)$ is an odd number in the range*

$$2q_0 + 2 - \frac{2(q_0 - 1) \log 2}{\log q_0} < s_*(q_0) < 2q_0 + 4 - \frac{2(q_0 - 2) \log 2}{\log q_0}.$$

Proof. i) can be verified by MAGMA easily. The proof of ii) is elementary and very similar to that of (41) in Lemma 11. To be more precise, for fixed q_0 , denote by s_1, s_2 the unique positive real numbers such that

$$q_0^{s_i/2} = \left(\frac{q_0}{2} \right)^{q_0-1} (2q_0^2 - 7q_0 + 3) + \delta_i, \quad \delta_1 = 0, \delta_2 = 1.$$

Very similar to the proof of (41), if $q_0 \geq 8$ we can obtain $s_1 < s_*(q_0) < s_2 + 2$ and

$$s_1 > 2q_0 + 2 - \frac{2(q_0 - 1) \log 2}{\log q_0}, \quad s_2 < 2q_0 + 2 - \frac{2(q_0 - 2) \log 2}{\log q_0}.$$

This completes the proof of Lemma 13. $\square$

Let us also define $s^*(q_0) \geq 3$ to be the largest odd number satisfying $s^*(q_0) \leq q_0/2$. Obviously $s^*(q_0) = q_0/2 - 1$ when $q_0 \geq 8$. We can summarize Corollaries 4, 5, and Theorem 8 in the following proposition. For the sake of completeness, we also include the trivial case that $s = 1$.

Proposition 3. *Let q_0 be even. The covering radius of $C_s(q_0)$ is given by*

- i). *If $s = 1$, then $\rho(C_s(q_0)) = 1$;*
- ii). *If $s = 2$, then $\rho(C_s(q_0)) = 2$;*
- iii). *If $s \geq 4$ is even, then $\rho(C_s(q_0)) = 3$;*
- iv). *If $s \geq 3$ is odd, and $s \leq s^*(q_0)$, then $\rho(C_s(q_0)) = 2$;*
- v). *If $s \geq 3$ is odd, and $s \geq s_*(q_0)$, then $\rho(C_s(q_0)) = 3$;*
- vi). *If $s \geq 3$ is odd, and $s' | s$ with $\rho(C_{s'}(q_0)) = 3$, then $\rho(C_s(q_0)) = 3$.*

In Table VII below, we list the values $s^*(q_0)$ and $s_*(q_0)$ for $q_0 = 2^t$ where $1 \leq t \leq 7$. We also list the missing odd numbers s in the interval $(s^*(q_0), s_*(q_0))$ where the value $\rho(C_s(q_0))$ is not yet determined.

TABLE III

FOR EACH $q_0 = 2^t$, $s^*(q_0) \geq 3$ IS THE LARGEST ODD NUMBER s SUCH THAT $s \leq q_0/2$, $s_*(q_0) \geq 3$ IS THE LEAST ODD NUMBER s SATISFYING (52).

$q_0 = 2^t$	s^*	s_*	the set of missing odd numbers in (s^*, s_*)
2		3	$\emptyset$
4		7	$\{3, 5\}$
8	3	15	$\{5, 7, 9, 11, 13\}$
16	7	27	odd numbers from 9 to 25
32	15	55	odd numbers from 17 to 53
64	31	111	odd numbers from 33 to 109
128	63	223	odd numbers from 65 to 221

The computations performed using MAGMA agree perfectly with Proposition 3. For the missing odd s in $(s^*(q_0), s_*(q_0))$, for example, for $q_0 = 4$, we have $\rho(C_3(4)) = 2$ and $\rho(C_5(4)) = 3$; and for $q_0 = 8$, $\rho(C_5(8)) = \rho(C_7(8)) = 2$.

VIII. DISCUSSION: QUASI-PERFECT AND MAXIMAL CODES

Recall that quasi-perfect and maximal codes are characterized by the minimum distance and the covering radius of the codes as were seen in Eqs (1) and (2). Given the detailed descriptions of the minimum distance and the covering radius in Theorems 1-2 and Propositions 2-3, we can identify quasi-perfect and maximal codes from $C_s(q_0)$ for even q_0 and from $\widetilde{C}_s(q_0)$ for odd q_0 .

For the sake of completeness, we also include the cases $s = 1$ and $q_0 = 2, 3$, which are either trivial or well-known.

A. $C_s(q_0)$ for even q_0

Case $s = 1$: for q_0 even, $C_1(q_0)$ is a linear code with parameters $[q_0 + 1, q_0 - 1, 3]_{q_0}$, $\rho(C_1(q_0)) = 1$, so $C_1(q_0)$ is both perfect and maximal. Actually $C_1(q_0)$ is equivalent to the Hamming code $\mathcal{H}_{q_0, 2}$ (see [35]) which is consistent with the classification of perfect codes.

Now we consider the case that $s \geq 2$.

Case $q_0 = 2$: If $s = 2$: $C_2(2)$ is a linear code with parameters $[5, 1, 5]_{q_0}$ with covering radius $\rho(C_1(q_0)) = 2$, so $C_2(2)$ is both perfect and maximal. The parameters of $C_2(2)$ are also consistent with the classification of perfect codes.

If $s \geq 4$ even, $C_s(2)$ is a linear code with parameters $[2^s + 1, 2^s + 1 - 2s, 5]_{q_0}$ with covering radius $\rho(C_s(q_0)) = 3$, so $C_s(2)$ is both quasi-perfect and maximal. This result is well-known.

Case $q_0 \geq 4$ is even: $C_s(q_0)$ is a linear code with parameters $[2^s + 1, 2^s + 1 - 2s]_{q_0}$. The minimum distance satisfies $d(C_s(q_0)) \in \{3, 4\}$ and the covering radius satisfies $\rho(C_s(q_0)) \in \{2, 3\}$, so if $\rho(C_s(q_0)) = 2$, then $C_s(q_0)$ is quasi-perfect. In particular,

- (1) $s = 2$: $d(C_s(q_0)) = 4, \rho(C_s(q_0)) = 2$, so $C_2(q_0)$ is both quasi-perfect and maximal;
- (2) $s \geq 4$ even: $d(C_s(q_0)) = 4, \rho(C_s(q_0)) = 3$, so $C_2(q_0)$ is maximal;
- (3) $s \geq 3$ odd and $s \leq \frac{q_0}{2}$: $d(C_s(q_0)) = 3, \rho(C_s(q_0)) = 2$, so $C_s(q_0)$ is both quasi-perfect and maximal.

We summarize the above result below (for simplicity, we focus on the case $q_0 \geq 4$ is even):

Theorem 9. *Let $q_0 \geq 4$ be even.*

- (0) *If $s = 1$, then $C_s(q_0)$ is both perfect and maximal;*
- (1) *If $s = 2$ or if s is odd and $3 \leq s \leq q_0/2$, then $C_s(q_0)$ is both quasi-perfect and maximal;*
- (2) *If $s \geq 4$ is even, then $C_s(q_0)$ is maximal.*

The above results are summarized in the following table.

TABLE IV
PARAMETERS OF $C_s(q_0)$ IN EVEN CHARACTERISTIC

q_0 even	s	$d(C_s(q_0))$	$\rho(C_s(q_0))$	perfect/quasi-perfect	maximal
any q_0 even	1	3	1	perfect	✓
$q_0 = 2$	2	5	2	perfect	✓
$q_0 = 2$	$s \geq 4$ and even	5	3	quasi-perfect	✓
$q_0 \geq 4$	2	4	2	quasi-perfect	✓
$q_0 \geq 4$	$3 \leq s \leq \frac{q_0}{2}, s$ odd	3	2	quasi-perfect	✓
$q_0 \geq 4$	$s \geq 4$ and even	4	3	-	✓

B. $\widetilde{C_s(q_0)}$ for odd q_0

Case $q_0 = 3$: If $s = 1$, $\widetilde{C_s(q_0)}$ is trivial with parameters $[2, 0]$; if $s \geq 2$, $\widetilde{C_s(3)}$ is a linear code with parameters $\left[\frac{3^s+1}{2}, \frac{3^s+1}{2} - 2s, 5\right]_3$, with covering radius $\rho(\widetilde{C_s(3)}) = 3$, so $\widetilde{C_s(3)}$ is both quasi-perfect and maximal for any $s \geq 2$. This result is well-known.

Now we assume that $q_0 \geq 5$.

Case $s = 1$: $\widetilde{C_1(q_0)}$ is a linear code with parameters $\left[\frac{q_0+1}{2}, \frac{q_0-3}{2}, 3\right]_{q_0}$, which is an MDS code. Moreover, $\rho(\widetilde{C_1(q_0)}) = 2$, so $\widetilde{C_1(q_0)}$ is both quasi-perfect and maximal.

Case $s \geq 2$ even: $\widetilde{C_s(q_0)}$ is a linear code with parameters $\left[\frac{q_0^s+1}{2}, \frac{q_0^s+1}{2} - 2s, 4\right]_{q_0}$ with covering radius $\rho(\widetilde{C_s(q_0)}) = 3$, so $\widetilde{C_s(q_0)}$ is maximal.

Case $s \geq 3$ odd: $\widetilde{C_s(q_0)}$ is a linear code with parameters $\left[\frac{q_0^s+1}{2}, \frac{q_0^s+1}{2} - 2s, 3\right]_{q_0}$. The covering radius satisfies $\rho(\widetilde{C_s(q_0)}) \in \{2, 3\}$, so if $\rho(\widetilde{C_s(q_0)}) = 2$, then $\widetilde{C_s(q_0)}$ is quasi-perfect. In particular, when s is odd and $3 \leq s \leq s^*(q_0)$, then $d(C_s(q_0)) = 3, \rho(C_s(q_0)) = 2$, so $C_s(q_0)$ is both quasi-perfect and maximal.

Theorem 10. *Let $q_0 \geq 5$ be odd.*

- (0) *If $s = 1$, then $\widetilde{C_s(q_0)}$ is both quasi-perfect and maximal;*
- (1) *If s is odd and $3 \leq s \leq s^*(q_0)$, then $\widetilde{C_s(q_0)}$ is both quasi-perfect and maximal;*
- (2) *If $s \geq 2$ is even, then $\widetilde{C_s(q_0)}$ is maximal.*

The above results are summarized in the following table.

TABLE V
PARAMETERS OF $C_s(q_0)$ IN ODD CHARACTERISTIC

q_0 odd	s	$d(\widetilde{C_s(q_0)})$	$\rho(\widetilde{C_s(q_0)})$	perfect/quasi-perfect	maximal
$q_0 = 3$	$s \geq 2$	5	3	quasi-perfect	✓
$q_0 \geq 5$	1	3	2	quasi-perfect	✓
$q_0 \geq 5$	$s \geq 2$ even	4	3	-	✓
$q_0 \geq 5$	$3 \leq s \leq s^*(q_0)$, s odd	3	2	quasi-perfect	✓

IX. CONCLUDING REMARKS

In this paper, we employed Weil-type estimates of character sums over finite fields to study the covering radius of generalized Zetterberg codes $C_s(q_0)$ for both even and odd q_0 , and for each q_0 , we determined the covering radius explicitly for a wide range of s . The study revealed many classes of quasi-perfect and maximal codes from $C_s(q_0)$. This complemented and strengthened previous works on odd characteristic. Here we raise one question which we might return in the future:

Let q_0 be either even or odd and $s \geq 2$. It was proved in Corollary 1 that $\rho(C_s(q_0)) \in \{2, 3\}$. Moreover, by Propositions 2-3 we have

- (i) if $s \geq 3$ is odd and $s \leq s^*(q_0)$, then $\rho(C_s(q_0)) = 2$;
- (ii) if $s \geq 3$ is odd and $s \geq s_*(q_0)$, then $\rho(C_s(q_0)) = 3$.

Here for odd and even q_0 , the odd numbers $s^*(q_0)$ and $s_*(q_0)$ are defined explicitly at the end of Sections VI and VII respectively.

Open question: Can one determine additional values of $\rho(C_s(q_0))$ for odd s in the range $(s^*(q_0), s_*(q_0))$? Affirmative results would likely uncover new families of quasi-perfect and maximal codes arising from the generalized Zetterberg codes $C_s(q_0)$.

REFERENCES

- [1] A. Alahmadi, H. Alhazmi, T. Hellesest, R. Hijazi, N. Muthana, and P. Solé, “On the lifted Zetterberg code,” *Des. Codes Cryptogr.*, vol. 80, no. 3, pp. 561–576, 2016.
- [2] A. Ashikhmin and A. Barg, “Bounds on the covering radius of linear codes,” *Des. Codes Cryptogr.*, vol. 27, no. 3, pp. 261–269, 2002.
- [3] E. R. Berlekamp, H. Rumsey, and G. Solomon, “On the solution of algebraic equations over finite fields,” *Information and Control*, vol. 10, pp. 553–564, 1967.
- [4] S. Bezzateev and N. Shekhunova, “Lower bound of covering radius of binary irreducible Goppa codes,” *Des. Codes Cryptogr.*, vol. 82, no. 1-2, pp. 69–76, 2017.
- [5] 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*, vol. 64, no. 11, pp. 7171–7177, 2018.
- [6] R. A. Brualdi, S. Litsyn, and V. S. Pless, “Covering radius,” in *Handbook of Coding Theory, Vol. I, II*. North-Holland, Amsterdam, 1998, pp. 755–826.
- [7] A. A. Bruen and D. L. Wehlau, “Long binary linear codes and large caps in projective space,” *Des. Codes Cryptogr.*, vol. 17, no. 1-3, pp. 37–60, 1999.
- [8] C. H. Chan and M. Xiong, “Classification of a class of planar quadrinomials,” 2025.
- [9] T. Cochrane and C. Pinner, “Using Stepanov’s method for exponential sums involving rational functions,” *J. Number Theory*, vol. 116, no. 2, pp. 270–292, 2006.
- [10] G. D. Cohen, S. N. Litsyn, A. C. Lobstein, and H. F. Mattson, Jr., “Covering radius 1985–1994,” *Appl. Algebra Engrg. Comm. Comput.*, vol. 8, no. 3, pp. 173–239, 1997.
- [11] G. Cohen, I. Honkala, S. Litsyn, and A. Lobstein, *Covering Codes*, ser. North-Holland Mathematical Library. North-Holland Publishing Co., Amsterdam, 1997.
- [12] G. D. Cohen, M. G. Karpovsky, H. F. Mattson, Jr., and J. R. Schatz, “Covering radius—survey and recent results,” *IEEE Trans. Inform. Theory*, vol. 31, no. 3, pp. 328–343, 1985.

- [13] S. D. Cohen, “The length of primitive BCH codes with minimal covering radius,” *Des. Codes Cryptogr.*, vol. 10, no. 1, pp. 5–16, 1997.
- [14] A. Cossidente, B. Csajbók, G. Marino, and F. Pavese, “Small complete caps in $PG(4n+1, q)$,” *Bull. Lond. Math. Soc.*, vol. 55, no. 1, pp. 522–535, 2023.
- [15] D. Danev and S. Dodunekov, “A family of ternary quasi-perfect BCH codes,” *Des. Codes Cryptogr.*, vol. 49, no. 1-3, pp. 265–271, 2008.
- [16] D. Danev, S. Dodunekov, and D. Radkova, “A family of constacyclic ternary quasi-perfect codes with covering radius 3,” *Des. Codes Cryptogr.*, vol. 59, no. 1-3, pp. 111–118, 2011.
- [17] A. A. Davydov, S. Marcugini, and F. Pambianco, “New results on binary codes obtained by doubling construction,” *Cybern. Inf. Technol.*, vol. 18, no. 5, pp. 63–76, 2018.
- [18] C. Ding, T. Hellese, H. Niederreiter, and C. Xing, “The minimum distance of the duals of binary irreducible cyclic codes,” *IEEE Trans. Inform. Theory*, vol. 48, no. 10, pp. 2679–2689, 2002.
- [19] Z. Ding and M. E. Zieve, “Determination of a class of permutation quadrinomials,” *Proc. Lond. Math. Soc. (3)*, vol. 127, no. 2, pp. 221–260, 2023.
- [20] S. M. Dodunekov, “The optimal double-error correcting codes of Zetterberg and Dumer-Zinovev are quasiperfect,” *C. R. Acad. Bulgare Sci.*, vol. 38, no. 9, pp. 1121–1123, 1985.
- [21] —, “Some quasiperfect double error correcting codes,” *Problems Control Inform. Theory/Problemy Upravlén. Teor. Inform.*, vol. 15, no. 5, pp. 367–375, 1986.
- [22] S. Dodunekov and J. Nilsson, “Algebraic decoding of the Zetterberg codes,” *IEEE Trans. Inform. Theory*, vol. 38, no. 5, pp. 1570–1573, 1992.
- [23] R. Dougherty, R. D. Mauldin, and M. Tiefenbruck, “The covering radius of the Reed-Muller code $RM(m-4, m)$ in $RM(m-3, m)$,” *IEEE Trans. Inform. Theory*, vol. 68, no. 1, pp. 560–571, 2022.
- [24] T. Etzion and B. Mounits, “Quasi-perfect codes with small distance,” *IEEE Trans. Inform. Theory*, vol. 51, no. 11, pp. 3938–3946, 2005.
- [25] R. Franken, *The covering radius of long primitive ternary BCH codes*. ProQuest LLC, Ann Arbor, MI, 2005, thesis (Ph.D.)—University of Glasgow (United Kingdom).
- [26] R. Franken and S. D. Cohen, “The covering radius of some primitive ternary BCH codes,” in *Finite fields and applications*, ser. Lecture Notes in Comput. Sci. Springer, Berlin, 2004, vol. 2948, pp. 166–180.
- [27] J. Gao, H. Kan, Y. Li, and Q. Wang, “The covering radius of the third-order Reed-Muller code $RM(3, 7)$ is 20,” *IEEE Trans. Inform. Theory*, vol. 69, no. 6, pp. 3663–3673, 2023.
- [28] I. B. Gashkov and V. M. Sidel’nikov, “Linear ternary quasi-perfect codes that correct double errors,” *Probl. Peredachi Inf.*, vol. 22, no. 4, pp. 43–48, 1986.
- [29] V. Gillot and P. Langevin, “Covering radius of $RM(4, 8)$,” *Adv. Math. Commun.*, vol. 18, no. 2, pp. 383–393, 2024.
- [30] M. Giulietti, “The geometry of covering codes: small complete caps and saturating sets in Galois spaces,” in *Surveys in combinatorics 2013*, ser. London Math. Soc. Lecture Note Ser. Cambridge Univ. Press, Cambridge, 2013, vol. 409, pp. 51–90.
- [31] D. Gorenstein, W. W. Peterson, and N. Zierler, “Two-error correcting Bose-Chaudhuri codes are quasi-perfect,” *Information and Control*, vol. 3, pp. 291–294, 1960.
- [32] T. Hellese, “All binary 3-error-correcting BCH codes of length $2^m - 1$ have covering radius 5,” *IEEE Trans. Inform. Theory*, vol. IT-24, no. 2, pp. 257–258, 1978.
- [33] —, “On the covering radius of cyclic linear codes and arithmetic codes,” *Discrete Appl. Math.*, vol. 11, no. 2, pp. 157–173, 1985.
- [34] X.-D. Hou, “Covering radius of the Reed-Muller code $R(1, 7)$ —a simpler proof,” *J. Combin. Theory Ser. A*, vol. 74, no. 2, pp. 337–341, 1996.
- [35] W. C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes*. Cambridge University Press, Cambridge, 2003.
- [36] M.-H. Jing, Y. Chang, C.-D. Lee, J.-H. Chen, and Z.-H. Chen, “A result on Zetterberg codes,” *IEEE Commun. Letters*, vol. 14, no. 7, pp. 662–663, 2010.

- [37] C. Li and T. Helleseeth, "Quasi-perfect linear codes from planar and APN functions," *Cryptogr. Commun.*, vol. 8, no. 2, pp. 215–227, 2016.
- [38] S. Li, M. Xiong, and H. Yan, "On a question of cyclic codes with generalized niho-type nonzroes," *IEEE Trans. Inform. Theory*, to appear.
- [39] R. Lidl and H. Niederreiter, *Finite Fields*, 2nd ed., ser. Encyclopedia of Mathematics and Its Applications. Cambridge University Press, Cambridge, 1997.
- [40] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes. I*, ser. North-Holland Mathematical Library, Vol. 16. North-Holland Publishing Co., Amsterdam-New York-Oxford, 1977.
- [41] A. McLoughlin, "The complexity of computing the covering radius of a code," *IEEE Trans. Inform. Theory*, vol. 30, no. 6, pp. 800–804, 1984.
- [42] J. Meggitt, "Error correcting codes and their implementation for data transmission systems," *IRE Trans.*, vol. 7, no. 4, pp. 234–244, 1961.
- [43] O. Moreno and F. N. Castro, "Divisibility properties for covering radius of certain cyclic codes," *IEEE Trans. Inform. Theory*, vol. 49, no. 12, pp. 3299–3303, 2003.
- [44] C. Peters, J. Top, and M. van der Vlugt, "The Hasse zeta function of a K3 surface related to the number of words of weight 5 in the Melas codes," *J. Reine Angew. Math.*, vol. 432, pp. 151–176, 1992.
- [45] R. Schoof and M. van der Vlugt, "Hecke operators and the weight distributions of certain codes," *J. Combin. Theory Ser. A*, vol. 57, no. 2, pp. 163–186, 1991.
- [46] M. Shi, T. Helleseeth, and F. Özbudak, "Covering radius of generalized Zetterberg type codes over finite fields of odd characteristic," *IEEE Trans. Inform. Theory*, vol. 69, no. 11, pp. 7025–7048, 2023.
- [47] M. Shi, T. Helleseeth, F. Özbudak, and P. Solé, "Covering radius of Melas codes," *IEEE Trans. Inform. Theory*, vol. 68, no. 7, pp. 4354–4364, 2022.
- [48] M. Shi, S. Li, T. Helleseeth, and F. Özbudak, "Determining the covering radius of all generalized Zetterberg codes in odd characteristic," *IEEE Trans. Inform. Theory*, vol. 71, no. 5, pp. 3602–3613, 2025.
- [49] N. J. A. Sloane, "A new approach to the covering radius of codes," *J. Combin. Theory Ser. A*, vol. 42, no. 1, pp. 61–86, 1986.
- [50] A. Tietäväinen, "On the nonexistence of perfect codes over finite fields," *SIAM J. Appl. Math.*, vol. 24, pp. 88–96, 1973.
- [51] A. Tietäväinen, "A short proof for the nonexistence of unknown perfect codes over $\text{GF}(q)$, $q > 2$," *Ann. Acad. Sci. Fenn. Ser. A. I.*, no. 580, p. 6, 1974.
- [52] G. van der Geer and M. van der Vlugt, "Artin-Schreier curves and codes," *J. Algebra*, vol. 139, no. 1, pp. 256–272, 1991.
- [53] S. G. Vlèduts and A. N. Skorobogatov, "On the covering radius of long BCH codes," *Problems Inform. Transmission*, vol. 25, no. 1, pp. 38–45, 1989.
- [54] D. Wan, "Generators and irreducible polynomials over finite fields," *Math. Comp.*, vol. 66, no. 219, pp. 1195–1212, 1997.
- [55] Y. Xia, N. Li, X. Zeng, and T. Helleseeth, "An open problem on the distribution of a Niho-type cross-correlation function," *IEEE Trans. Inform. Theory*, vol. 62, no. 12, pp. 7546–7554, 2016.
- [56] —, "On the correlation distribution for a Niho decimation," *IEEE Trans. Inform. Theory*, vol. 63, no. 11, pp. 7206–7218, 2017.
- [57] M. Xiong and H. Yan, "On correlation distribution of Niho-type decimation $d = 3(p^m - 1) + 1$," *IEEE Trans. Inform. Theory*, vol. 70, no. 11, pp. 8289–8302, 2024.
- [58] L.-H. Zetterberg, "Cyclic codes from irreducible polynomials for correction of multiple errors," *IRE Trans. Information Theory*, vol. IT-8, pp. 13–20, 1962.