COVERING RADIUS OF GENERALIZED ZETTERBERG TYPE CODES IN ODD CHARACTERISTIC

MINJIA SHI & TOR HELLESETH & FERRUH ÖZBUDAK

Abstract. Let $\mathbb{F}_{q_0}$ be a finite field of odd characteristic. For an integer $s \geq 1$, let $\mathcal{C}_s(q_0)$ be the generalized Zetterberg code of length $q_0^s + 1$ over $\mathbb{F}_{q_0}$. If s is even, then we prove that the covering radius of $\mathcal{C}(s, q_0)$ is 3. Put $q = q_0^s$. If s is odd and $q \not\equiv 7 \mod 8$, then we present an explicit lower bound $N_1(q_0)$ so that if $s \geq N_1(q_0)$, then the covering radius of $\mathcal{C}_s(q_0)$ is 3. We also show that the covering radius of $\mathcal{C}_1(q_0)$ is 2. Moreover we study some cases when s is an odd integer with $3 \leq s \leq N_1(q_0)$ and, rather unexpectedly, we present concrete examples with covering radius 2 in that range. We introduce half generalized Zetterberg codes of length $(q_0^s + 1)/2$ if $q \equiv 1 \mod 4$. Similarly we introduce twisted half generalized Zetterberg codes of length $(q_0^s + 1)/2$ if $q \equiv 3 \mod 4$. We show that the same results hold for the half and twisted half generalized Zetterberg codes.

Keywords: covering radius, Zetterberg codes, algebraic curve, finite field
AMS(2020) Math Sc. Cl. 94B05, 94B65, 11T71, 11T06, 11R58

Minjia Shi is with Key Laboratory of Intelligent Computing Signal Processing, Ministry of Education, School of Mathematical Sciences, Anhui University, Hefei, Anhui, 230601, China, e-mail: smjwcl.good@163.com.

Tor Helleseth is with he Department of Informatics, University of Bergen, 5020 Bergen, Norway, e-mail: tor.helleseth@uib.no.

Ferruh Özbudak is with Department of Mathematics and Institute of Applied Mathematics, Middle East Technical University, Ankara, Turkey; e-mail: ozbudak@metu.edu.tr.

1. Introduction

Covering radius of codes is one of the four fundamental parameters of a code [7]. It has various application including decoding, data compression, testing, write-once memories and combinatorics in general. For further details on the significance and applications of covering radius of codes, we refer, for example, to [2], [4], [5], [6], and the references therein.

Let $\mathbb{F}_{q_0}$ denote a finite field with q_0 elements, where q_0 is a prime power. For an integer $s \geq 1$, let $\mathbb{F}_{q_0^s}^*$ denote the multiplicative group of the field extension $\mathbb{F}_{q_0^s}$, so that $\mathbb{F}_{q_0^s}^* = \mathbb{F}_{q_0^s} \setminus \{0\}$. For a finite set S, let $|S|$ denote its cardinality.

Let n be a positive integer. Let $\mathcal{C}$ be an $\mathbb{F}_{q_0}$-linear code of length n. Let w_H denote the Hamming weight in $\mathbb{F}_{q_0}^n$. If $x \in \mathbb{F}_{q_0}^n$, then the Hamming distance of x to $\mathcal{C}$ is $d(x, C) = \min\{w_H(x - c) : c \in \mathcal{C}\}$. The *covering radius* of $\mathcal{C}$ is the integer given by

$$\max\left\{d(x, C) : x \in \mathbb{F}_{q_0}^n\right\}.$$

The problem of finding the covering radius of a given linear code is very difficult in general. Most of the results in the literature present some bounds on the covering radii rather than giving exact bounds [1], [13], [15], [18], [20]. Exact values of covering radii are known only for a few classes of linear codes [9], [10], [17].

Recently the covering radius of Melas codes are determined [17]. Another interesting class of codes is the class of Zetterberg type codes. They include some quasi-perfect codes [8], [11]. The Zetterberg codes were introduced by L. H. Zetterberg [21]. Let $s \geq 1$ be an integer. Put $q = q_0^s$ and $n = q + 1$. Let H be the subgroup of $\mathbb{F}_{q^2}$ with $|H| = n$. Let $\{h_1, \ldots, h_n\}$ be an enumeration of H. The generalized Zetterberg code $\mathcal{C}_s(q_0)$ of length $n = q_0^s + 1$ over $\mathbb{F}_{q_0}$ is the $\mathbb{F}_{q_0}$-linear code with the parity check matrix

$$P = [h_1 \ h_2 \ \cdots h_n]. \tag{1}$$

Here we use a short notation for the parity check matrix P. In fact we choose an arbitrary $\mathbb{F}_{q_0}$-linear bijective map $\phi : \mathbb{F}_{q^2} \to \mathbb{F}_{q_0}^{2s}$ and we consider each column h_j in P as $\phi(h_j) \in \mathbb{F}_{q_0}^{2s}$. Therefore $\mathcal{C}_s(q_0)$ has dimension $n - 2s$ (see Lemma 6.1 in Appendix).

In this paper we determine the covering radius of Zetterberg type codes. In particular, our contributions in this paper include the following statements in items (i), ..., (vii) below:

We assume that $q_0^s \not\equiv 7 \mod 8$.

(i). For each such q_0 and any integer $s \geq 1$, the covering radius of $\mathcal{C}_s(q_0)$ is either 2 or 3.

(ii). If $s = 1$, then the covering radius of $\mathcal{C}_s(q_0)$ is 2.

(iii). If $s \geq 2$ is an even integer, then the covering radius of $\mathcal{C}_s(q_0)$ is 3. Here the assumption $q_0^s \not\equiv 7 \mod 8$ holds automatically.

(iv). For each such q_0, there exists an odd integer $N_1(q_0) \geq 3$ with the following property: If $s \geq 3$ is an odd integer, then the covering radius of $\mathcal{C}_s(q_0)$ is 3.

(v). For each such q_0, let $I(q_0)$ be the set consisting of odd integers $s \geq 3$ such that the covering radius of $\mathcal{C}_s(q_0)$ is 3. We show that $I(q_0)$ is very different from the case of even s in some cases. For example

$$I(q_0) = \{s\colon\ s \text{ is an odd integer with } s \geq 3\} \text{ if } q_0 \in \{3, 5, 9, 11, 13\}.$$

However we also have that

$$3 \notin I(q_0) \text{ if } q_0 \in \{17, 19, 25\}.$$

(vi). We use some methods from [8] and [11]. We observe that there is a small gap in the proof of the covering radius in the paper of [11], which corresponds to the case that $q_0 = 3$. We indicate that and correct it. For details we refer to Remark 4.2 and Section 5 below.

(vii). We extend the notion generalized Zetterberg code to *half* and *twisted half* generalized Zetterberg codes. If $q_0 = 3$, then half and twisted half generalized Zetterberg codes are quasi-perfect [8] and [11]. We also determine the covering radii of half and twisted half generalized Zetterberg codes.

We use detailed methods from arithmetic of finite fields and algebraic curves over finite fields in our proofs. Our methods are very different from the ones in [17].

It is well known that the covering radius $\rho(s, q_0)$ of the generalized Zetterberg code $\mathcal{C}_s(q_0)$ can also be defined as follows (see, for example, [4, Theorem 2.1.9] and [13, Lemma 1.1]): The covering radius $\rho(s, q_0)$ is the smallest positive integer ρ such that every element of $\mathbb{F}_{q^2}$ is an $\mathbb{F}_{q_0}$-linear combination of at most ρ elements of H.

This paper is organized as follows. We prove the covering radius is at most 3 in Section 2. It is a long and quite technical section. We determine the exact covering radius in most cases in Section 3. This section presents some connections to algebraic curves over finite fields. We use these connections effectively to solve the problem for all sufficiently large values of s. There are rather interesting explicit examples for certain small values of q_0 and s. We extend our results to half and twisted half Zetterberg codes in Section 4. We conclude in Section 5. We also have a short Appendix.

2. The covering radius of the generalized Zetterberg Codes in odd characteristic is at most 3

Let $\mathbb{F}_{q_0}$ be an arbitrary finite field of odd characteristic. Let $s \geq 1$ be an integer. Put $q = q_0^s$. Let H be the subgroup of $\mathbb{F}_{q^2}^*$ with $|H| = q + 1$.

The main result of this section is the following theorem.

Theorem 2.1. *Let $\mathbb{F}_{q_0}$ be a finite field of odd characteristic. Let $s \geq 1$ be an integer. Put $q = q_0^s$ and $n = q + 1$. Assume that $q_0^s \not\equiv 7 \mod 8$. Then the covering radius of the Zetterberg code over $\mathbb{F}_{q_0}$ of length n is at most 3.*

Recall that Theorem 2.1 is equivalent to the following statement (see Section 1 above): For $\alpha \in \mathbb{F}_{q^2}$, there exist $c_1, c_2, c_3 \in \mathbb{F}_{q_0}$ and $h_1, h_2, h_3 \in H$ such that

$$c_1 h_1 + c_2 h_2 + c_3 h_3 = \alpha. \tag{2}$$

Our proof of Theorem 2.1 is quite involved. As a first step we use the following theorem, which extends an important technique from [11]. Namely [11] introduce and use a very useful technique only for $\mathbb{F}_3$ and odd integers $s \geq 1$. We extend their technique from $\mathbb{F}_3$ and odd integers $s \geq 1$ to arbitrary $\mathbb{F}_{q_0}$ of odd characteristic and arbitrary integers $s \geq 1$, provided $q_0^s \not\equiv 7 \mod 8$. We also observe a small gap in their proof and we cover their gap (see Remark 4.2 and Section 5 below).

Theorem 2.2. *Let $\mathbb{F}_{q_0}$ be a finite field of odd characteristic. Let $s \geq 1$ be an integer. Put $q = q_0^s$ and $n = q + 1$. Assume that $q \not\equiv 7 \mod 8$. Let P1, P2, P3 and P4 be the properties defined depending on q_0 and s as follows. Note that P3 and P4 are defined only if $q \equiv 3 \mod 8$.*

- **Property P1:**
  For each $\alpha \in \mathbb{F}_q^*$, there exist $c_1, c_2, c_3 \in \mathbb{F}_{q_0}$ and $h_1, h_2, h_3 \in H$ such that $c_1 h_1 + c_2 h_2 + c_3 h_3 = \alpha$.
- **Property P2:**
  For each $\alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ with $\alpha^q = -\alpha$, there exist $c_1, c_2, c_3 \in \mathbb{F}_{q_0}$ and $h_1, h_2, h_3 \in H$ such that $c_1 h_1 + c_2 h_2 + c_3 h_3 = \alpha$.
- **Property P3:**
  Assume $q \equiv 3 \mod 4$. Let $\theta \in \mathbb{F}_{q^2}$ be a primitive 4-th root of 1. For each $\alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ with $\alpha^q = \theta\alpha$, there exist $c_1, c_2, c_3 \in \mathbb{F}_{q_0}$ and $h_1, h_2, h_3 \in H$ such that $c_1 h_1 + c_2 h_2 + c_3 h_3 = \alpha$.
- **Property P4:**
  We keep the assumption on q and the notation on θ of P3 above. For each $\alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ with $\alpha^q = -\theta\alpha$, there exist $c_1, c_2, c_3 \in \mathbb{F}_{q_0}$ and $h_1, h_2, h_3 \in H$ such that $c_1 h_1 + c_2 h_2 + c_3 h_3 = \alpha$.

Then we have the following:

- **Case** $q \equiv 1 \mod 4$**:**
  The covering radius of $\mathcal{C}_s(q_0)$ *is at most* 3 *if both of the the properties P1 and P2 hold simultaneously.*

- **Case** $q \equiv 3 \mod 8$**:**
  The covering radius of $\mathcal{C}_s(q_0)$ *is at most* 3 *if all of the four properties P1, P2, P3 and P4 hold simultaneously.*

Remark 2.1. *An important strength of Theorem 2.2 is the following: If* $q \equiv 1 \mod 4$*, then using properties P1 and P2 we need to consider only* α *in the set*

$$\left\{\alpha \in \mathbb{F}_{q^2}^* : \alpha^q = \alpha\right\} \bigsqcup \left\{\alpha \in \mathbb{F}_{q^2}^* : \alpha^q = -\alpha\right\}.$$

Here and throughout the paper $\bigsqcup$ *is the disjoint union. Assume* $q \equiv 3 \mod 4$ *and* $\theta \in \mathbb{F}_{q^2}$ *is a primitive 4-th root of 1. Then using properties P1, P2, P3 and P4 we need to consider only* α *in the set*

$$\{\alpha \in \mathbb{F}_{q^2} : \alpha^q = \alpha\} \bigsqcup \left\{\alpha \in \mathbb{F}_{q^2}^* : \alpha^q = -\alpha\right\} \bigsqcup \left\{\alpha \in \mathbb{F}_{q^2}^* : \alpha^q = \theta\alpha\right\}$$
$$\bigsqcup \left\{\alpha \in \mathbb{F}_{q^2}^* : \alpha^q = -\theta\alpha\right\}.$$

Hence, if $q \equiv 1 \mod 4$*, the number of* α *we need to consider is* $2q - 1$*. Similarly if* $q \equiv 3 \mod 4$*, the number of* α *we need to consider is* $4q - 3$*. In particular, if* q *is large, then*

$$max\,\{2q - 1, 4q - 3\} \ll q^2. \tag{3}$$

This shows that Theorem 2.2 is a strong improvement compared to the well known statement in (2). Indeed it follows from (3) that we need to consider extremely small number of α *to complete the proof: around, at most,* $4q$ *versus* q^2*.*

Proof. We need to show that if $\alpha \in \mathbb{F}_{q^2}^*$, then there exist $c_1, c_2, c_3 \in \mathbb{F}_{q_0}$ and $h_1, h_2, h_3 \in H$ such that

$$c_1 h_1 + c_2 h_2 + c_3 h_3 = \alpha. \tag{4}$$

Assume first that $q \equiv 1 \mod 4$. Then

$$\gcd(\tfrac{q+1}{2}, q - 1) = 1.$$

Hence we obtain

$$\gcd(q + 1, 2(q - 1)) = 2. \tag{5}$$

Note that $2(q-1) \mid (q^2-1)$, and let G_2 be the subgroup of $\mathbb{F}_{q^2}^*$ such that $|G_2| = 2(q-1)$. Using (5) we conclude that

$$\text{lcm } (|H|, |G_2|) = \tfrac{2(q-1)(q+1)}{2} = q^2 - 1. \tag{6}$$

Using (6) we conclude that if $\alpha \in \mathbb{F}_{q^2}^*$, then there exist $h \in H$ and $\alpha_1 \in G_2$ such that

$$\alpha = h\alpha_1. \tag{7}$$

Combining (4) and (7) we conclude that we can assume $\alpha_1 \in G_2$ without loss of generality. Note that

$$G_2 = \left\{\alpha \in \mathbb{F}_{q^2}^* : \alpha^q = \alpha\right\} \bigsqcup \left\{\alpha \in \mathbb{F}_{q^2}^* : \alpha^q = -\alpha\right\}.$$

This completes the proof if $q \equiv 1 \mod 4$.

Next we assume that $q \equiv 3 \mod 4$. In this case $4(q-1) \mid (q^2-1)$ and let G_4 be the subgroup of $\mathbb{F}_{q^2}^*$ such that $|G_4| = 4(q-1)$. Note that we have

$$\gcd(\tfrac{q+1}{4}, q-1) = 1 \tag{8}$$

and hence

$$\gcd(q+1, 4(q-1)) = 4. \tag{9}$$

Using (8) and (9) we obtain

$$\text{lcm}\ (|H|, |G_4|) = \tfrac{4(q-1)(q+1)}{4} = q^2 - 1.$$

Therefore if $\alpha \in \mathbb{F}_{q^2}^*$, then there exist $h \in H$ and $\alpha_1 \in G_4$ such that

$$\alpha = h\alpha_1. \tag{10}$$

Let $\theta \in \mathbb{F}_{q^2}$ be a primitive 4-th root of 1. We have

$$\begin{aligned} G_4 = &\left\{\alpha \in \mathbb{F}_{q^2}^* : \alpha^q = \alpha\right\} \bigsqcup \left\{\alpha \in \mathbb{F}_{q^2}^* : \alpha^q = -\alpha\right\} \\ &\bigsqcup \left\{\alpha \in \mathbb{F}_{q^2}^* : \alpha^q = \theta\alpha\right\} \bigsqcup \left\{\alpha \in \mathbb{F}_{q^2}^* : \alpha^q = -\theta\alpha\right\}. \end{aligned}$$

Combining (4) and (10) we conclude that we can assume $\alpha_1 \in G_4$ without loss of generality. This completes the proof of $q \equiv 1 \mod 4$. □

Using Theorem 2.2, the proof of Theorem 2.1 is immediate if

- properties P1 and P2 hold when $q \equiv 1 \mod 4$, and
- properties P1, P2, P3 and P4 hold when $q \equiv 3 \mod 4$.

We prove that Theorem 2.1 in four subsections below. Subsection 1 has its main theorem that we prove Property P1 holds for any $\mathbb{F}_q$ odd characteristic. Similarly we consider properties P2, P3 and P4 in the other subsections. In particular we complete the proof of Theorem 2.1 using Theorem 2.2 and the four theorems in the following four subsections.

2.1. **Property P1.** In this subsection we prove that Property P1 holds, namely we prove Lemma 2.2 and Theorem 2.3 below.

Throughout this subsection let $\mathbb{F}_{q_0}$ be a finite field of odd characteristic. Let $s \geq 1$ be an integer. Put $q = q_0^s$. Let H be the subgroup of $\mathbb{F}_{q^2}^*$ with $|H| = q+1$. Let $w \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ with $w + w^q = 1$. Put $D = (\frac{w-w^q}{2})^2$. We start with a rather simple lemma. Note that $\{w, w^q\}$ is a basis of $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$.

Lemma 2.1. *We have $D = \frac{1}{4} - w^{q+1}$. In particular, $D \in \mathbb{F}_q^*$ and D is not a square in $\mathbb{F}_q$.*

Proof. Note $\frac{w-w^q}{2} = \frac{w+w^q}{2} - w^q$, $\frac{w+w^q}{2} \in \mathbb{F}_q$ and $w^q \notin \mathbb{F}_q$. Hence D is not a square in $\mathbb{F}_q$. Moreover

$$\begin{aligned} D &= (\tfrac{w-w^q}{2})^2 = \tfrac{w^2+w^{2q}-2w^{q+1}}{4} = \tfrac{w^2+2w^{q+1}+w^{2q}-4w^{q+1}}{4} \\ &= \tfrac{1-4w^{q+1}}{4} = \tfrac{1}{4} - w^{q+1}. \end{aligned}$$

This completes the proof. □

The next simple lemma covers a special subcase, which needs a separate proof.

Lemma 2.2. *Let $\alpha \in \{0, 1, -1\}$. There exist $c_1, c_2, c_3 \in \mathbb{F}_{q_0}$ and $h_1, h_2, h_3 \in H$ such that $c_1 h_1 + c_2 h_2 + c_3 h_3 = \alpha$.*

Proof. Note that $1 \in H$ and $\{0, 1, -1\} \in \mathbb{F}_{q_0}$. Let $h_1 = 1$ and $h_2, h_3 \in H$ arbitrary chosen elements. We have

$$\begin{aligned} 0 \cdot h_1 + 0 \cdot h_2 + 0 \cdot h_3 &= 0, \\ 1 \cdot h_1 + 0 \cdot h_2 + 0 \cdot h_3 &= 1, \\ -1 \cdot h_1 + 0 \cdot h_2 + 0 \cdot h_3 &= -1. \end{aligned}$$

This completes the proof. □

The main result of this subsection is the following, which we prove at the end of this subsection.

Theorem 2.3. *Let $\alpha \in \mathbb{F}_q \setminus \{0, 1, -1\}$. There exist $h_1, h_2, h_3 \in H$ such that*

$$h_1 + h_2 + h_3 = \alpha.$$

We need some preliminary results before the proof of Theorem 2.3. We use Propositions 2.1, 2.2 and 2.3 below in the proof of Theorem 2.3, which we give at the end of this subsection.

Proposition 2.1. *Let $\alpha \in \mathbb{F}_q \setminus \{0, 1, -1\}$. Then Theorem 2.3 holds if and only if there exist $x_1, x_2, x_3, y_1, y_2, y_3 \in \mathbb{F}_q$ such that*

$$\begin{aligned} x_1 + x_2 + x_3 &= \alpha, \\ y_1 + y_2 + y_3 &= 0, \\ x_1^2 - Dy_1^2 &= 1, \\ x_2^2 - Dy_2^2 &= 1, \quad \textit{and} \\ x_3^2 - Dy_3^2 &= 1. \end{aligned}$$

Proof. Put $x_1, x_2, x_3, y_1, y_2, y_3 \in \mathbb{F}_q$ such that $h_i = x_i w + y_i w^q$ for $1 \leq \mathrm{i} \leq 3$. Note that $\alpha = \alpha w + \alpha w^q$ and hence

$$h_1 + h_2 + h_3 = \alpha \Longleftrightarrow x_1 + x_2 + x_3 = \alpha \text{ and } \mathrm{y}_1 + \mathrm{y}_2 + \mathrm{y}_3 = \alpha. \tag{11}$$

Moreover

$$(h_i)^{q+1} = (x_i w + y_i w^q)^{q+1} = (x_i^2 + y_i^2) w^{q+1} + (w^2 + w^{2q}) x_i y_i = 1 \tag{12}$$

for $1 \leq i \leq 3$. Put

$$\begin{cases} x_{new,i} = \frac{x_i + y_i}{2} \text{ and} \\ y_{new,i} = x_i - y_i \end{cases}$$

for $1 \leq i \leq 3$. This change of variables and (11), (12) imply that Theorem 2.3 holds if and only if

$$\begin{cases} x_{new,1} + x_{new,2} + x_{new,3} = \alpha, \\ y_{new,1} + y_{new,2} + y_{new,3} = 0, \quad \text{and} \\ x_{new,i}^2 - Dy_{new,i}^2 = 1 \end{cases}$$

for $1 \leq i \leq 3$. Indeed, using Lemma 2.1 we obtain

$$\begin{aligned} x_{new,i}^2 - Dy_{new,i}^2 &= \frac{x_i^2 + y_i^2 + 2x_iy_i}{4} - D(x_i^2 + y_i^2 - 2x_iy_i) \\ &= \left(\frac{1}{4} - D\right)(x_i^2 + y_i^2) + \left(\frac{1}{2} + 2D\right)x_iy_i \\ &= w^{q+1}(x_i^2 + y_i^2) + (1 - 2w^{q+1})x_iy_i \\ &= w^{q+1}(x_i^2 + y_i^2) + (w^2 + w^{2q})x_iy_i \\ &= 1. \end{aligned}$$

This completes the proof. ∎

Proposition 2.2. *Let* $\alpha \in \mathbb{F}_q \backslash \{0, 1, -1\}$. *Let* $a(x), b(x), c(x) \in \mathbb{F}_q[x]$ *be the polynomials given by*

$$\begin{aligned} a(x) &= 2\alpha x - \alpha^2 - 1, \\ b(x) &= 2\alpha x^2 + (-3\alpha^2 - 1)x + \alpha^3 + \alpha, \quad \textit{and} \\ c(x) &= (-\alpha^2 - 1)x^2 + (\alpha^3 + \alpha)x - \frac{\alpha^4}{4} - \frac{\alpha^2}{2} + \frac{3}{4}. \end{aligned}$$

Put

$$\Delta(x) = b(x)^2 - 4a(x)c(x) \in \mathbb{F}_q[x]. \tag{13}$$

Assume that there exists $x_1 \in \mathbb{F}_q$ *such that*

(i). $x_1^2 - 1$ is a nonsquare in $\mathbb{F}_q$,
(ii). $a(x_1) \neq 0$, *and*
(iii). $\Delta(x_1)$ is a nonzero square in $\mathbb{F}_q$.

Then Theorem 2.3 holds.

Proof. We use Proposition 2.1. Put $y_3 = -(y_1 + y_2)$ and $x_3 = \alpha - x_1 - x_2$. Then the system in Proposition 2.1 is equivalent to the system

$$\begin{aligned} &x_1^2 - Dy_1^2 = 1, \\ &x_2^2 - Dy_2^2 = 1, \ \textit{and} \\ &(\alpha - x_1 - x_2)^2 - D(y_1 + y_2)^2 = 1. \end{aligned}$$

Here the variables x_1, x_2, y_1, y_2 run through $\mathbb{F}_q$. Using the last equation we obtain

$$\begin{aligned}\alpha^2 + x_1^2 + x_2^2 + 2x_1x_2 - 2\alpha x_1 - 2\alpha x_2 &= Dy_1^2 + Dy_2^2 + 2Dy_1y_2 + 1\\ = (x_1^2 - 1) + (x_2^2 - 1) &+ 2Dy_1y_2 + 1 = x_1^2 + x_2^2 + 2Dy_1y_2 - 1.\end{aligned}$$

Hence

$$Dy_2 = \frac{x_1x_2 - \alpha x_1 - \alpha x_2 + \frac{\alpha^2+1}{2}}{y_1}.$$

Taking square of both sides and using the equations $Dy_1^2 = x_1^2 - 1$ and $Dy_2^2 = x_2^2 - 1$, we obtain

$$x_2^2 - 1 = \frac{(x_1x_2 - \alpha x_1 - \alpha x_2 + \frac{\alpha^2+1}{2})^2}{x_1^2 - 1}.$$

Here we assume that $x_1^2 \neq 1$. The last equation is equivalent to

$$a(x_1)x_2^2 + b(x_1)x_2 + c(x_1) = 0, \tag{14}$$

where $a(x_1), b(x_1), c(x_1) \in \mathbb{F}_q[x_1]$ given in the statement of Proposition 2.2.

Assume further that $a(x_1) \neq 0$. Then there exists $x_2 \in \mathbb{F}_q$ satisfying (14) if $\Delta(x_1)$ is a nonzero square in $\mathbb{F}_q$. Assuming items (ii) and (iii) of the assumptions of the proposition and the condition $x_1^2 \neq 1$, the system in Proposition 2.1 is equivalent to

$$x_1^2 - Dy_1^2 = 1. \tag{15}$$

Here x_1 is chosen and $y_1 \in \mathbb{F}_q$ is a variable.

As D is a nonsquare in $\mathbb{F}_q$, the equation in (15) has a solution $y_1 \in \mathbb{F}_q$ if we also assume that $x_1^2 - 1$ is a nonsquare. Note that the condition $x_1^2 \neq 1$ is automatically satisfied by the assumption item (i). This completes the proof. □

Let $\overline{\mathbb{F}}_q$ be an algebraic closure of $\mathbb{F}_q$.

Proposition 2.3. *Let $\alpha \in \mathbb{F}_q \setminus \{0, 1, -1\}$. Let $\Delta(x) \in \mathbb{F}_q[x]$ be the polynomial defined in (13) in Proposition 2.2. Then there is no polynomial $f(x) \in \overline{\mathbb{F}}_q[x]$ such that*

$$\Delta(x) = (f(x))^2 \in \mathbb{F}_q[x]. \tag{16}$$

Proof. Note that $\Delta(x)$ is a polynomial of degree 4 with leading coefficient $4\alpha^2$. Put

$$\Delta_1(x) = \frac{\Delta(x)}{4\alpha^2} = x^4 + A_3x^3 + A_2x^2 + A_1x + A_0 \in \overline{\mathbb{F}}_q[x]. \tag{17}$$

Assume the contrary that there exists $f(x) \in \overline{\mathbb{F}}_q[x]$ satisfying (16). This implies that there exist $c_0, c_1 \in \overline{\mathbb{F}}_q$ such that

$$\Delta_1(x) = (x^2 + c_1x + c_0)^2. \tag{18}$$

Assume that

$$A_3 \neq 0. \tag{19}$$

Using (18) and comparing the coefficients of both sides we obtain that

$$c_1 = \frac{A_3}{2} \text{ and } c_0 = \frac{A_1}{A_3}.$$

We also obtain that

$$A_2 = c_1^2 + 2c_0 = \left(\frac{A_3}{2}\right)^2 + 2\frac{A_1}{A_3}. \tag{20}$$

Using (17) and having rather tedious but direct computations we obtain that

$$A_3 = \frac{-\alpha^2+1}{\alpha}, \tag{21}$$

and

$$A_2 - \left[\left(\frac{A_3}{2}\right)^2 + 2\frac{A_1}{A_3}\right] = \frac{\alpha^2-1}{\alpha^2}. \tag{22}$$

As $\alpha \notin \{0, 1, -1\}$, using (21) we obtain that the assumption in (19) holds. Moreover combining (20) and (22) we get a contradiction. This completes the proof. □

Now we are ready to prove Theorem 2.3.

Proof of Theorem 2.3. Recall that $a(x) = 2\alpha x - \alpha^2 - 1 \in \mathbb{F}_q[x]$ and $\Delta(x) \in \mathbb{F}_q[x]$ are defined in Proposition 2.2. Let

$$T_1 = \{x_1 \in \mathbb{F}_q : a(x_1) = 0\}, \; T_2 = \left\{x_1 \in \mathbb{F}_q : x_1^2 - 1 = 0\right\}, \; T_3 = \{x_1 \in \mathbb{F}_q : \Delta(x_1) = 0\}.$$

Note that $deg(\Delta(x)) = 4$. Hence $|T_1| = 1$, $|T_2| = 2$, $|T_3| \le 4$. Put $T = T_1 \bigcup T_2 \bigcup T_3$. Let η be the quadratic character on $\mathbb{F}_q$ given by

$$\begin{aligned} \eta : \mathbb{F}_q \;&\rightarrow\; \{0, 1, -1\} \\ x \;&\mapsto\; \begin{cases} 0, & \text{if } x = 0, \\ 1, & \text{if } x \in \mathbb{F}_q^* \text{ is a square}, \\ -1, & \text{if } x \in \mathbb{F}_q^* \text{ is a nonsquare}. \end{cases} \end{aligned}$$

For $1 \le i \le 3$, put

$$E_i = \sum_{x \in T_i} (1 - \eta(x^2-1))(1 + \eta(\Delta(x))). \tag{23}$$

Let

$$E = \sum_{x \in T} (1 - \eta(x^2-1))(1 + \eta(\Delta(x))), \tag{24}$$

$$N_1 = \sum_{x \in \mathbb{F}_q \setminus T} (1 - \eta(x^2-1))(1 + \eta(\Delta(x))), \tag{25}$$

and

$$N=\sum_{x\in\mathbb{F}_q}(1-\eta(x^2-1))(1+\eta(\Delta(x))). \tag{26}$$

It follows from (24), (25) and (20) that

$$N_1 = N - E. \tag{27}$$

Using (23) we obtain that

$$\begin{aligned}|E_1| &\le 2\cdot 2 = 4,\\ |E_2| &= \sum_{x\in T_2}(1+\eta(\Delta(x))) \le 4\\ |E_3| &\le 4\cdot 2 = 8.\end{aligned}$$

These imply that

$$E \le 4+4+8 = 16. \tag{28}$$

Note that using (26) we have

$$N=\sum_{x\in\mathbb{F}_q}1-\sum_{x\in\mathbb{F}_q}\eta(x^2-1)+\sum_{x\in\mathbb{F}_q}\eta(\Delta(x))-\sum_{x\in\mathbb{F}_q}\eta\left((x^2-1)\Delta(x)\right). \tag{29}$$

It is well-known that

$$\sum_{x\in\mathbb{F}_q}\eta(x^2-1)=0. \tag{30}$$

Using Proposition 2.3 and Weil's sum (see, for example, [14, Theorem 5.41]) we have

$$\sum_{x\in\mathbb{F}_q}\eta(\Delta(x)) \le 3q^{1/2} \tag{31}$$

and

$$\sum_{x\in\mathbb{F}_q}\eta\left((x^2-1)\Delta(x)\right) \le 5q^{1/2}. \tag{32}$$

Combining (27), (28), (29), (30), (31) and (32) we conclude that

$$N_1 \ge q - 8q^{1/2} - 16. \tag{33}$$

Note that $q-8q^{1/2}-16>0$ if $q>94$. Using Proposition 2.2, this completes the proof if $q>94$. The set of cardinalities q such that there exists a finite field $\mathbb{F}_q$ of characteristic odd and $q\le 94$ is

$$\begin{aligned}S \;=\; &\{3,5,7,9,11,13,17,19,23,25,27,29,\\ &31,37,41,43,47,49,53,59,61,67,71,73,79,81,83,89\}.\end{aligned}$$

For each $q\in S$, using Magma [3] and a direct search method we show that Theorem 2.3 holds. This completes the proof. $\square$

2.2. **Property P2.** In this subsection we prove that Property P2 holds, namely we prove Theorem 2.4 below.

As in the previous subsection, throughout this subsection let $\mathbb{F}_{q_0}$ be a finite field of odd characteristic. Let $s \geq 1$ be an integer. Put $q = q_0^s$. Let H be the subgroup of $\mathbb{F}_{q^2}$ with $|H| = q+1$. Still as in the previous subsection, let $w \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ with $w + w^q = 1$. Put $D = (\frac{w-w^q}{2})^2$.

First we prove a proposition, which is analogous to Proposition 2.1. Recall that $D \in \mathbb{F}_q^*$ and D is a nonsquare in $\mathbb{F}_q$.

Proposition 2.4. *Let $\alpha \in \mathbb{F}_{q^2}^*$ with $\alpha^q = -\alpha$. Put $\beta = \frac{2\alpha}{2w-1}$. Note that $\beta \in \mathbb{F}_q^*$. There exist $h_1, h_2, h_3 \in H$ such that*

$$h_1 + h_2 + h_3 = \alpha$$

if and only if there exist $x_1, x_2, x_3, y_1, y_2, y_3 \in \mathbb{F}_q$ such that

$$\begin{aligned} x_1 + x_2 + x_3 &= 0, \\ y_1 + y_2 + y_3 &= \beta, \\ x_1^2 - Dy_1^2 &= 1, \\ x_2^2 - Dy_2^2 &= 1, \\ x_3^2 - Dy_3^2 &= 1. \end{aligned}$$

Proof. Put $x_1, x_2, x_3, y_1, y_2, y_3 \in \mathbb{F}_q$ such that

$$h_i = x_i w + y_i w^q$$

for $1 \leq i \leq 3$. Note that

$$\alpha = \frac{\beta}{2} w - \frac{\beta}{2} w^q$$

and hence

$$h_1 + h_2 + h_3 = \alpha \Longleftrightarrow x_1 + x_2 + x_3 = \frac{\beta}{2} \text{ and } y_1 + y_2 + y_3 = -\frac{\beta}{2}. \tag{34}$$

As in the proof of Proposition 2.1, we have

$$1 = (h_i)^{q+1} = (x_i^2 + y_i^2) w^{q+1} + (w^2 + w^{2q}) x_i y_i \text{ for } 1 \leq i \leq 3. \tag{35}$$

Put

$$\begin{cases} x_{new,i} = \frac{x_i + y_i}{2}, \\ y_{new,i} = x_i - y_i, \quad \text{for } 1 \leq i \leq 3. \end{cases}$$

This change of variables and (34), (35) imply that $h_1 + h_2 + h_3 = \alpha$ if and only if

$$x_{new,1} + x_{new,2} + x_{new,3} = 0, \tag{36}$$

$$y_{new,1} + y_{new,2} + y_{new,3} = \beta, \text{ and} \tag{37}$$

$$x_{new,i}^2 - Dy_{new,i}^2 = 1.$$

for $1 \le i \le 3$. Indeed, using Lemma 2.1 as in the proof of Proposition 2.1 we obtain that

$$x_{new,i}^2 - Dy_{new,i}^2 = (x_i^2 + y_i^2)w^{q+1} + (w^2 + w^{2q})x_i y_i = 1$$

for $1 \le i \le 3$. This completes the proof. □

Before presenting the main result of this subsection we need to deal with a special subcase separately in the following lemma.

Lemma 2.3. *Let $\alpha \in \mathbb{F}_{q^2}^*$ with $\alpha^q = -\alpha$. Put $\beta = \frac{2\alpha}{2w-1}$. Assume that*

$$q \equiv 3 \bmod 4 \quad \textit{and} \quad \mathrm{D}\beta^2 + 1 = 0. \tag{38}$$

Then there exist $h_1, h_2, h_3 \in H$ such that

$$h_1 + h_2 + h_3 = \alpha.$$

Proof. As $q \equiv 3 \bmod 4$, -1 is not a square in $\mathbb{F}_q$. Then $\frac{-1}{D}$ is a square in $\mathbb{F}_q$. Indeed, it follows from the assumption (38) that $\beta^2 = \frac{-1}{D}$. Put

$$x_1 = x_2 = x_3 = 0, \; y_1 = \beta, \; y_2 = -\beta, \; y_3 = \beta.$$

Then

$$x_1 + x_2 + x_3 = 0, \, y_1 + y_2 + y_3 = \beta,$$
$$x_1^2 - Dy_1^2 = -D\beta^2 = 1, \; x_2^2 - Dy_2^2 = -D\beta^2 = 1, \; x_3^2 - Dy_3^2 = -D\beta^2 = 1.$$

We complete the proof using Proposition 2.4. □

Now we are ready to present the main result of this subsection in the following theorem.

Theorem 2.4. *Let $\alpha \in \mathbb{F}_{q^2}^*$ with $\alpha^q = -\alpha$. There exist $h_1, h_2, h_3 \in H$ such that*

$$h_1 + h_2 + h_3 = \alpha.$$

We need some further results (as in Subsection 2.1) before the proof of Theorem 2.4. The following is an analog of Proposition 2.2.

Proposition 2.5. *Let $\alpha \in \mathbb{F}_{q^2}^*$ with $\alpha^q = -\alpha$. Put $\beta = \frac{2\alpha}{2w-1}$. Let $a(y), b(y), c(y) \in \mathbb{F}_q[y]$ be the polynomials given by*

$$\begin{aligned} a(y) &= 2D^2\beta y - D^2\beta^2 + D, \\ b(y) &= 2D^2\beta y^2 + (-3D^2\beta^2 + D)y + D^2\beta^3 - D\beta, \quad \text{and} \\ c(y) &= (-D^2\beta^2 + D)y^2 + (D^2\beta^3 - D\beta)y - \frac{D^2\beta^4}{4} + \frac{D\beta^2}{2} + \frac{3}{4}. \end{aligned}$$

Put

$$\Delta(y) = b(y)^2 - 4a(y)c(y) \in \mathbb{F}_q[y].$$

Assume that there exists $y_1 \in \mathbb{F}_q$ such that

(i). $1 + Dy_1^2$ *is a nonzero square in* $\mathbb{F}_q$,

(ii). $a(y_1) \neq 0$, *and*

(iii). $\Delta(y_1)$ *is a nonzero square in* $\mathbb{F}_q$.

Then Theorem 2.4 holds.

Proof. We use Proposition 2.4. Put $x_3 = -(x_1 + x_2)$ and $y_3 = \beta - y_1 - y_2$. Then the system in Proposition 2.4 is equivalent to the system

$$x_1^2 - Dy_1^2 = 1,$$

$$x_2^2 - Dy_2^2 = 1,$$

$$(x_1 + x_2)^2 - D(\beta - y_1 - y_2)^2 = 1.$$

Using the last equation we obtain

$$\begin{aligned} x_1^2 + x_2^2 + 2x_1x_2 &= D(\beta^2 + y_1^2 + y_2^2 + 2y_1y_2 - 2\beta y_1 - 2\beta y_2) + 1 \\ &= (x_1^2 - 1) + (x_2^2 - 1) + 2Dy_1y_2 - 2D\beta y_1 - 2D\beta y_2 + D\beta^2 + 1. \end{aligned}$$

Hence

$$x_2 = \frac{2Dy_1y_2 - 2D\beta y_1 - 2D\beta y_2 + D\beta^2 - 1}{2x_1}.$$

Taking square of both sides and using the equations $x_2^2 = 1 + Dy_2^2$ and $x_1^2 = 1 + Dy_1^2$ we obtain

$$1 + Dy_2^2 = \frac{(Dy_1y_2 - D\beta y_1 - D\beta y_2 + \frac{D\beta^2 - 1}{2})^2}{1 + Dy_1^2}.$$

Hence we assume that $1 + Dy_1^2 \neq 0$. The last equation is equivalent to

$$a(y_1)y_2^2 + b(y_1)y_2 + c(y_1) = 0, \tag{39}$$

where $a(y_1), b(y_1), c(y_1) \in \mathbb{F}_q[y_1]$ are given in the statement of Proposition 2.5.

Assume further that $a(y_1) \neq 0$. Then there exists $y_2 \in \mathbb{F}_q$ satisfying (39) if $\Delta(y_1)$ is a nonzero square in $\mathbb{F}_q$. Assuming items (ii) and (iii) of the assumptions of the proposition and the condition $1 + Dy_1^2 \neq 0$, the system in Proposition 2.5 is equivalent to

$$x_1^2 - Dy_1^2 = 1.$$

Here y_1 is chosen and $x_1 \in \mathbb{F}_q$ is a variable.

If $1 + Dy_1^2$ is a nonzero square as well, the last equation has a solution $x_1 \in \mathbb{F}_q$ and the assumption $1 + Dy_1^2 \neq 0$ holds. This completes the proof. $\square$

Recall that $\overline{\mathbb{F}}_q$ is an algebraic closure of $\mathbb{F}_q$. Next proposition is analogous to Proposition 2.3.

Proposition 2.6. *Let $\alpha \in \mathbb{F}_{q^2}^*$ such that $\alpha^q = -\alpha$. Put $\beta = \frac{2\alpha}{2w-1}$. Assume (38) in Lemma 2.3 does not hold. Let $\Delta(y) \in \mathbb{F}_q[y]$ be the polynomial defined in Proposition 2.5. Then there is no polynomial $f(y) \in \overline{\mathbb{F}}_q[y]$ such that*

$$\Delta(y) = (f(y))^2 \in \mathbb{F}_q[y]. \tag{40}$$

Proof. The proof is analogous to the proof of Proposition 2.3. Here $\Delta(y)$ is a polynomial of degree 4 with leading coefficient $4D^4\beta^2$. Put

$$\Delta_1(y) = \frac{\Delta(y)}{4D^4\beta^2} = y^4 + A_3y^3 + A_2y^2 + A_1y + A_0 \in \mathbb{F}_q[y].$$

Assume that

$$A_3 \neq 0. \tag{41}$$

As in the proof of Proposition 2.3, if there exists $f(y) \in \overline{\mathbb{F}}_q[y]$ satisfying (40), then we have

$$A_2 - \left[\left(\frac{A_3}{2}\right)^2 + 2\frac{A_1}{A_3}\right] = 0. \tag{42}$$

Using rather tedious but direct computations we obtain that

$$A_3 = \frac{-D\beta^2 - 1}{D\beta},$$

and

$$A_2 - \left[\left(\frac{A_3}{2}\right)^2 + 2\frac{A_1}{3}\right] = \frac{-D\beta^2 - 1}{D^2\beta^2}. \tag{43}$$

Assume first that $q \equiv 1 \bmod 4$. Then -1 is a square and hence $D\beta^2 + 1 \neq 0$ as D is a nonsquare in $\mathbb{F}_q$ and $\beta \in \mathbb{F}_q$. Assume next that $q \equiv 3 \bmod 4$. As the condition (38) in Lemma 2.3 does not hold $D\beta^2 + 1 \neq 0$.

These imply that the assumption in (41) holds. Moreover these also imply that we get a contradiction using (42) and (43). This completes the proof. $\square$

Now we are ready to prove Theorem 2.4.

Proof of Theorem 2.4. If $q \equiv 3 \bmod 4$ and $D\beta^2 + 1 = 0$, then the proof follows from Lemma 2.3. Next we assume that if $q \equiv 3 \bmod 4$, then the condition $D\beta^2 + 1 = 0$ does not hold. Recall that $a(y) \in \mathbb{F}_q[y]$ and $\Delta(y) \in \mathbb{F}_q[y]$ are defined in Proposition 2.5. Let

$T_1 = \{y_1 \in \mathbb{F}_q : a(y_1) = 0\}$, $T_2 = \left\{y_1 \in \mathbb{F}_q : 1 + Dy_1^2 = 0\right\}$, $T_3 = \{y_1 \in \mathbb{F}_q : \Delta(y_1) = 0\}$.

Put $T = T_1 \cup T_2 \cup T_3$. Using the notation in the proof of Theorem 2.3, let

$$N_1 = \sum_{y \in \mathbb{F}_q \setminus T} (1 + \eta((1 + Dy^2))(1 + \eta(\Delta(y))).$$

As in the proof of Theorem 2.3 we have

$$N_1 \geq q - 8q^{1/2} - 16.$$

If $q > 94$, then this completes the proof as in the proof of Theorem 2.3, namely using Proposition 2.5 instead of Proposition 2.2. For $2 < q < 94$, we use Magma as in the proof of Theorem 2.3. □

2.3. **Property P3.** In this subsection we prove that Property P3 holds. Namely we prove Theorem 2.5 below.

The assumptions in this subsection are rather different. Let $\mathbb{F}_{q_0}$ be a finite field of odd characteristic. Let $s \geq 1$ be an integer. Put $q = q^s$. Assume that $q \equiv 3 \bmod 4$. Let H be the subgroup of $\mathbb{F}_{q^2}$ with $|H| = q + 1$. Let $\theta \in \mathbb{F}_{q^2}^*$ be a primitive 4-th root of 1. Let $w = \theta - 1$.

We start with a simple lemma.

Lemma 2.4. *Under notation and assumptions as above we have the following:*

(i). $\{w, w^q\}$ *is linearly independent over* $\mathbb{F}_q$.
(ii). $w^{q+1} = 2$.
(iii). $w^{2q} + w^2 = 0$ *and* $w^{2q} - w^2 = 4\theta$.
(iv). $\theta w^q - w = 2(1 - \theta)$ *and* $w^q - \theta w = 0$.

Proof. As $q \equiv 3 \mod 4$, we have that $4 \nmid (q - 1)$ and hence $\theta \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$. Note that $x^2 + 1 \in \mathbb{F}_q[x]$ is the minimal polynomial of θ over $\mathbb{F}_q$. This implies that $x^2 + 1 = (x - \theta)(x - \theta^q)$ and considering the coefficients of the monomial x in both sides we conclude that $\theta^q = -\theta$.

Using the definition of w we obtain that $w^q = \theta^q - 1 = -\theta - 1$. It is clear that $\{\theta - 1, -\theta - 1\}$ is linearly independent over $\mathbb{F}_q$. These arguments complete the proof of item (i).

The proof of item (ii) follows from the observation

$$w^{q+1} = (\theta - 1)(-\theta - 1) = -(\theta^2 - 1) = -(-1 - 1) = 2.$$

Similarly we prove item (iii) using the identities

$$w^2 = (\theta-1)^2 \text{ and } w^{2q} = (-\theta-1)^2 = (\theta+1)^2,$$

which imply

$$w^{2q} + w^2 = 2(\theta^2+1) = 0$$

and

$$w^{2q} - w^2 = 4\theta.$$

Finally we prove item (iv) using

$$\theta w^q - w = \theta(-\theta-1) - (\theta-1) = -\theta^2 - \theta - \theta + 1 = 2(1-\theta)$$

and

$$w^q - \theta w = -(\theta+1) - \theta(\theta-1) = -(\theta+1) - (-1-\theta) = 0.$$

□

Now we are ready to state the main result of this subsection in the next theorem.

Theorem 2.5. *Recall that $q \equiv 3 \mod 4$ and θ is a primitive 4-th root of 1. Let $\alpha \in \mathbb{F}_{q^2}^*$ such that $\alpha^q = \theta\alpha$. There exist $h_1, h_2, h_3 \in H$ such that*

$$h_1 + h_2 + h_3 = \alpha.$$

As in the previous subsections, we need to prove some preliminary results before the proof of Theorem 2.5. The next proposition is an analog of Proposition 2.4.

Proposition 2.7. *Let $\alpha \in \mathbb{F}_{q^2}^*$ with $\alpha^q = \theta\alpha$. Put $\mu = \frac{\alpha(1-\theta)}{2\theta}$. Note that $\mu \in \mathbb{F}_q^*$. Then Theorem 2.5 holds if and only if there exist $x_1, x_2, x_3, y_1, y_2, y_3 \in \mathbb{F}_q$ such that*

$$x_1 + x_2 + x_3 = \mu,$$

$$y_1 + y_2 + y_3 = 0,$$

$$x_1^2 + y_1^2 = \tfrac{1}{2},$$

$$x_2^2 + y_2^2 = \tfrac{1}{2},$$

$$x_3^2 + y_3^2 = \tfrac{1}{2}.$$

Proof. Put $x_1, x_2, x_3, y_1, y_2, y_3 \in \mathbb{F}_q$ such that

$$h_i = x_i w + y_i w^q$$

for $1 \le i \le 3$. Let $\beta_1, \beta_2 \in \mathbb{F}_q$ such that

$$\alpha = \beta_1 w + \beta_2 w^q.$$

Then we have

$$\theta\alpha = \alpha^q = \beta_1 w^q + \beta_2 w.$$

These imply that

$$\beta_1 = \frac{\alpha(\theta w^q - w)}{w^{2q} - w^2} \text{ and } \beta_2 = \frac{\alpha(w^q - \theta w)}{w^{2q} - w^2}.$$

Using Lemma 2.4 items (iii) and (iv), we obtain that

$$\beta_1 = \frac{\alpha(1-\theta)}{2\theta} = \mu \text{ and } \beta_2 = 0.$$

Moreover

$$h_i^{q+1} = (x_i w + y_i w^q)^{q+1} = (x_i^2 + y_i^2) w^{q+1} + x_i y_i (w^2 + w^{2q}) = 1$$

for $1 \le i \le 3$. Using Lemma 2.4 items (ii) and (iii), we obtain that

$$h_i^{q+1} = 1 \Longleftrightarrow 2(x_i^2 + y_i^2) = 1 \text{ for } 1 \le i \le 3.$$

This completes the proof. □

We need to consider a special case separately as in Subsection 2.2. The next lemma is analogous to Lemma 2.3.

Lemma 2.5. *Let $\alpha \in \mathbb{F}_{q^2}^*$ such that $\alpha^q = \theta\alpha$. Put $\mu = \frac{\alpha(1-\theta)}{2\theta}$. Assume that*

$$\mu^2 = \frac{1}{2}. \tag{44}$$

Then there exist $h_1, h_2, h_3 \in H$ such that

$$h_1 + h_2 + h_3 = \alpha.$$

Proof. Note that $\mu \in \mathbb{F}_q$. Put $x_1 = x_2 = \mu$, $x_3 = -\mu$ and $y_1 = y_2 = y_3 = 0$. It is clear that

$$x_1 + x_2 + x_3 = \mu \text{ and } y_1 + y_2 + y_3 = 0.$$

Also

$$x_i^2 + y_i^2 = x_i^2 = \mu^2 = \frac{1}{2} \text{ for } 1 \le i \le 3.$$

Using Proposition 2.7 we complete the proof. □

The next proposition is an analog of Proposition 2.5.

Proposition 2.8. *Let $\alpha \in \mathbb{F}_{q^2}^*$ such that $\alpha^q = \theta\alpha$. Put $\mu = \frac{\alpha(1-\theta)}{2\theta}$. Let $a(x), b(x), c(x) \in \mathbb{F}_q[x]$ be the polynomials given by*

$$a(x) = 2\mu x - \mu^2 - \tfrac{1}{2},$$

$$b(x) = 2\mu x^2 + \left(-3\mu^2 - \tfrac{1}{2}\right) x + \mu^3 + \tfrac{\mu}{2},$$

$$c(x) = \left(-\mu^2 - \tfrac{1}{2}\right) x^2 + \left(\mu^3 + \tfrac{\mu}{2}\right) x - \tfrac{\mu^4}{4} - \tfrac{\mu^2}{2} + \tfrac{3}{16}.$$

Put

$$\Delta(x) = b(x)^2 - 4a(x)c(x).$$

Assume that there exists $x_1 \in \mathbb{F}_q$ such that

(i). *$x_1^2 - \frac{1}{2}$ is a nonsquare in $\mathbb{F}_q$;*
(ii). *$a(x_1) \neq 0$;*
(iii). *$\Delta(x_1)$ is a nonzero square in $\mathbb{F}_q$.*

Then Theorem 2.5 holds.

Proof. The proof is similar to the proof of Proposition 2.2. We use Proposition 2.7. Put $y_3 = -(y_1 + y_2)$ and $x_3 = \mu - x_1 - x_2$. Then the system in Proposition 2.7 is equivalent to the system

$$\begin{aligned} &x_1^2 + y_1^2 = \tfrac{1}{2}, \\ &x_2^2 + y_2^2 = \tfrac{1}{2}, \quad \text{and} \\ &(\mu - x_1 - x_2)^2 + (y_1 + y_2)^2 = \tfrac{1}{2}. \end{aligned} \tag{45}$$

The last equation is equivalent to

$$y_1^2 + y_2^2 + 2y_1y_2 + x_1^2 + x_2^2 + 2x_1x_2 + \mu^2 - 2\mu x_1 - 2\mu x_2 = \frac{1}{2}.$$

As $x_1^2 + y_1^2 = x_2^2 + y_2^2 = \frac{1}{2}$ we get that

$$1 + 4y_1y_2 + 4x_1x_2 + 2\mu^2 - 4\mu x_1 - 4\mu x_2 = 0.$$

Consequently we obtain

$$y_2 = \frac{-x_1x_2 + \mu x_1 + \mu x_2 + \left(\frac{-2\mu^2-1}{4}\right)}{y_1}. \tag{46}$$

Here we assume that $y_1 \neq 0$, or equivalently $x_1^2 - \frac{1}{2}$ is nonzero.

Taking square of both sides (46) and using the first two equations of (45) we obtain that

$$\left(x_1^2 - \frac{1}{2}\right)\left(x_2^2 - \frac{1}{2}\right) = \left(x_1x_2 - \mu x_1 - \mu x_2 + \left(\frac{2\mu^2+1}{4}\right)\right)^2.$$

The last equation is equivalent to

$$a(x_1)x_2^2 + b(x_1)x_2 + c(x_1) = 0, \tag{47}$$

where $a(x_1), b(x_1), c(x_1) \in \mathbb{F}_q[x_1]$ given in the statement of Proposition 2.8.

Assume further that $a(x_1) \neq 0$. Then there exists $x_2 \in \mathbb{F}_q$ satisfying (47) if $\Delta(x_1)$ is a nonzero square in $\mathbb{F}_q$. Assuming items (ii) and (iii) of the proposition and the condition $x_1^2 - \frac{1}{2} \neq 0$, the system in Proposition 2.7 is equivalent to

$$x_1^2 + y_1^2 \;= \tfrac{1}{2}. \tag{48}$$

Here $x_1 \in \mathbb{F}_q$ is a chosen element and $y_1 \in \mathbb{F}_q$ is a variable.

As -1 is a nonsquare in $\mathbb{F}_q$, the equation in (48) has a solution if we further assume that $x_1^2 - \frac{1}{2}$ is a nonsquare in $\mathbb{F}_q$. This completes the proof. $\square$

Recall that $\overline{\mathbb{F}}_q$ be an algebraic closure of $\mathbb{F}_q$. The next proposition is analogous to Proposition 2.6.

Proposition 2.9. *Let $\alpha \in \mathbb{F}_{q^2}^*$ such that $\alpha^q = \theta\alpha$. Put $\mu = \frac{\alpha(1-\theta)}{2\theta}$. Let $\Delta(x) \in \mathbb{F}_q[x]$ be the polynomial defined in Proposition 2.8. Assume the condition (44) in Lemma 2.5 does not hold. Then there is no polynomial $f(x) \in \overline{\mathbb{F}}_q[x]$ such that*

$$\Delta(x) = (f(x))^2 \in \mathbb{F}_q[x].$$

Proof. Note that $\Delta(x)$ is a polynomial of degree 4 with leading coefficient $4\mu^2$. Put

$$\Delta_1(x) = \frac{\Delta(x)}{4\mu^2} = x^4 + A_3x^3 + A_2x^2 + A_1x + A_0 \in \mathbb{F}_q[x].$$

As in the proof of Proposition 2.6, it is enough to prove that

$$A_3 \neq 0. \tag{49}$$

and

$$A_2 - \left[\left(\frac{A_3}{2}\right)^2 - 2\frac{A_1}{A_3}\right] \neq 0. \tag{50}$$

Indeed, using rather tedious but direct computations we obtain that

$$A_3 = \frac{-\mu^2 + \frac{1}{2}}{\mu}, \tag{51}$$

and

$$A_2 - \left[\left(\frac{A_3}{2}\right)^2 - 2\frac{A_1}{A_3}\right] = \frac{\frac{\mu^2}{2} - \frac{1}{4}}{\mu^2}. \tag{52}$$

As $\mu^2 \neq \frac{1}{2}$, using (51) and (52) we conclude that the conditions in (49) and (50) hold. This completes the proof. $\square$

Now we are ready to prove Theorem 2.5.

Proof of Theorem 2.5. Put $\mu = \frac{\alpha(1-\theta)}{2\theta}$. If $\mu^2 = \frac{1}{2}$, then we complete the proof using Proposition 2.7 and Lemma 2.5. Assume that $\mu^2 \neq \frac{1}{2}$. Recall that $a(x_1) = 2\mu x - \mu^2 - \frac{1}{2}$. Let

$$T_1 = \{x_1 \in \mathbb{F}_q : a(x_1) = 0\}, \ T_2 = \left\{x_1 \in \mathbb{F}_q : x_1^2 = \frac{1}{2}\right\}, \ T_3 = \{x_1 \in \mathbb{F}_q : \Delta(x_1) = 0\}.$$

Put $T = T_1 \bigcup T_2 \bigcup T_3$. Let

$$N_1 = \sum_{x \in \mathbb{F}_q \setminus T} (1 - \eta(x^2 - \frac{1}{2}))(1 - \eta(\Delta(x))).$$

Using Proposition 2.8, as in the proof of Theorem 2.3, it is enough to show that

$$N_1 > 0. \tag{53}$$

As in the proof of Theorem 2.3, using Proposition 2.9 we obtain that

$$N_1 \geq q - 8^{1/2} - 16. \tag{54}$$

Combining (53) and (54) we complete the proof using the methods in the proof of Theorem 2.3. $\square$

2.4. **Property P4.** In this subsection we prove that Property P4 holds for suitable parameters. Namely we prove Theorem 2.6 below. We keep the assumptions and notation of Subsection 2.3. In particular $q \equiv 3 \bmod 4$, $\theta \in \mathbb{F}_{q^2}^*$ is a primitive 4-th root of 1 and $w = \theta - 1$.

The main result in this subsection is the following theorem.

Theorem 2.6. *Let $\alpha \in \mathbb{F}_{q^2}^*$ with $\alpha^q = -\theta\alpha$. Then there exist $h_1, h_2, h_3 \in H$ such that*

$$h_1 + h_2 + h_3 = \alpha.$$

First we prove a proposition that we use in the proof of Theorem 2.6, which is given at the end of this subsection.

Proposition 2.10. *Let $\alpha \in \mathbb{F}_{q^2}^*$ with $\alpha^q = -\theta\alpha$. Put $\mu = \frac{-\alpha(1+\theta)}{2\theta}$. Note that $\mu \in \mathbb{F}_q^*$. Then Theorem 2.6 holds if and only if there exist $x_1, x_2, x_3, y_1, y_2, y_3$ such that*

$$x_1 + x_2 + x_3 = 0,$$

$$y_1 + y_2 + y_3 = \mu,$$

$$x_1^2 + y_1^2 = \tfrac{1}{2},$$

$$x_2^2 + y_2^2 = \tfrac{1}{2},$$

$$x_3^2 + y_3^2 = \tfrac{1}{2}.$$

Proof. The proof is similar to the proof of Proposition 2.7. Put $x_1, x_2, x_3, y_1, y_2, y_3 \in \mathbb{F}_q$ such that

$$h_i = x_i w + y_i w^q$$

for $1 \leq i \leq 3$. Let $\beta_1, \beta_2 \in \mathbb{F}_q$ such that

$$\alpha = \beta_1 w + \beta_2 w^q. \tag{55}$$

Then we have

$$\alpha\theta = -\alpha^q = -\beta_1 w^q - \beta_2 w. \tag{56}$$

Using Lemma 2.4, items (iii) and (iv), we obtain that

$$w + \theta w^q = \theta\left(w^q - \theta w\right) = 0, \tag{57}$$

and

$$\frac{(w^q + \theta w)}{w^{2q} - w^2} = \frac{\theta^q - 1 + \theta^2 - \theta}{4\theta} = \frac{-\left(1+\theta\right)}{2\theta}. \tag{58}$$

Combining (55), (56), (57) and (58) implies that

$$\beta_1 = 0 \text{ and } \beta_2 = \frac{-\alpha(1+\theta)}{2\theta}.$$

As in the proof of Proposition 2.7 we have

$$h_i^{q+1} = 1 \Longleftrightarrow 2(x_i^2 + y_i^2) = 1 \text{ for } 1 \leq i \leq 3.$$

This completes the proof. ☐

Now we are ready to prove Theorem 2.6. We remark that we use a new trick which reduces the proof of Theorem 2.6 to some proofs of Subsection 2.3.

Proof of Theorem 2.6. Note that μ in Proposition 2.7 runs through

$$S_3 = \left\{ \frac{\alpha(1-\theta)}{2\theta} : \alpha \in \mathbb{F}_{q^2}^* \text{ with } \alpha^{\mathrm{q}} = \theta\alpha \right\}.$$

We obtain that $S_3 = \mathbb{F}_q^*$. Indeed

$$\begin{aligned} \psi_3 : \left\{\alpha \in \mathbb{F}_{q^2}^* : \alpha^q = \theta\alpha\right\} &\longrightarrow S_3 \\ \alpha &\longmapsto \frac{\alpha(1-\theta)}{2\theta} \end{aligned}$$

is a well-defined map as $\frac{\alpha(1-\theta)}{2\theta} \in \mathbb{F}_q$ when $\alpha \in \mathbb{F}_{q^2}^*$ with $\alpha^q = \theta\alpha$. Moreover ψ_3 is one-to-one.

As the set $\left\{\alpha \in \mathbb{F}_{q^2}^* : \alpha^q = \theta\alpha\right\}$ has cardinality $q-1$, we conclude that $S_3 = \mathbb{F}_q^*$.

Similarly let

$$S_4 = \left\{ \frac{-\alpha(1+\theta)}{2\theta} : \alpha \in \mathbb{F}_{q^2}^* \text{ with } \alpha^{\mathrm{q}} = -\theta\alpha \right\}$$

be the set that μ runs through in Proposition 2.10. Using the same method above we obtain that $S_4 = \mathbb{F}_q^*$.

Moreover it follows from the symmetry and direct observation that, by the change of variables

$$(x_1, x_2, x_3, y_1, y_2, y_3) \longmapsto (y_1, y_2, y_3, x_1, x_2, x_3),$$

the system of equations in Proposition 2.7 change to the system of equations in Proposition 2.10. Hence Theorem 2.6 holds as Theorem 2.5 and Proposition 2.7 hold. This completes the proof. □

3. Exact computation of the covering radius of the generalized Zetterberg Codes in odd characteristic

In this section we determine the exact covering radius of generalized Zetterberg codes. We note that the same results hold for half and twisted half Zetterberg codes (see Definitions 4.1 and 4.2 below). This follows immediately using Theorems 4.3 and 4.4 below. Therefore we do not state the corresponding results for half and twisted half Zetterberg codes separately.

Let $\mathbb{F}_{q_0}$ be a finite field of odd characteristic. For an integer $s \geq 1$, let $q = q_0^s$. Let $\mathcal{C}_s(q_0)$ be the generalized Zetterberg code of length $q+1$ over $\mathbb{F}_{q_0}$. Recall that $H \subseteq \mathbb{F}_{q^2}^*$ is the subgroup with $|H| = q+1$. Put $m = \frac{q_0-1}{2}$. Let $H_m \subseteq \mathbb{F}_{q^2}^*$ be the subgroup with $|H_m| = m(q+1)$.

We start with a simple but useful lemma.

Lemma 3.1. *The covering radius of $\mathcal{C}_s(q_0)$ is at least 2. The covering radius of $\mathcal{C}_s(q_0)$ is at least 3 if and only if there exists $\alpha \in \mathbb{F}_{q^2}$ such that the equation*

$$h_1 + h_2 = \alpha$$

is not solvable with $h_1, h_2 \in H_m$.

Proof. Note that $\gcd(|H|, q_0 - 1) = 2$. Hence the smallest subgroup of $\mathbb{F}_{q^2}^*$ containing both $|H|$ and $\mathbb{F}_{q_0}^*$ is $|H_m|$ as $|H_m| = \text{lcm}\ (|H|, q_0 - 1)$.

Note that $|H_m| = \frac{q_0-1}{2}(q+1) < q^2 - 1$. This implies the existence of $\alpha \in \mathbb{F}_{q^2} \setminus H_m$. Let $\alpha \in \mathbb{F}_{q^2} \setminus H_m$. We claim that it is impossible to choose $c \in \mathbb{F}_{q_0}$ and $h \in H$ such that

$$ch = \alpha.$$

Indeed otherwise $c \neq 0$ and $ch \in H_m$. This is a contradiction as $\alpha \notin H_m$. These arguments imply that the covering radius of $\mathcal{C}_s(q_0)$ is at least 2.

Using Theorem 2.2 we obtain that the covering radius of $\mathcal{C}_s(q_0)$ is either 2 or 3. Let $\alpha \in \mathbb{F}_{q^2}$. Assume that there exist $h_1, h_2 \in H_m$ such that $h_1 = h_2 = \alpha$. As $H_m = \mathbb{F}_{q^0}^* \cdot H$, there exist $c_1, c_2 \in \mathbb{F}_{q_0}^*$ and $\hat{h}_1, \hat{h}_2 \in H$ such that $c_1\hat{h}_1 + c_2\hat{h}_2 = \alpha$. Hence the covering radius of $\mathcal{C}_s(q_0)$ is 2. The converse statement holds similarly. This completes the proof. □

The next theorem uses methods of [11] again.

Theorem 3.1. *Let $\mathbb{F}_{q_0}$ be a finite field of odd characteristic. For an integer $s \geq 1$, let $q = q_0^s$. Assume that $q \not\equiv 7 \mod 8$. Let $\mathcal{C}_s(q_0)$ be the generalized Zetterberg code* *of length $q+1$ over $\mathbb{F}_{q_0}$. Recall that $m = \frac{q_0-1}{2}$ and $H_m \subseteq \mathbb{F}_{q^2}^*$ is the subgroup with $|H_m| = m(q+1)$.*

Let NP1, NP2, NP3 and NP4 be the properties defined depending on q_0 and s as follows. Note that NP3 and NP4 are defined only if $q \equiv 3 \mod 8$.

- **Property NP1:**
  There exists $\alpha \in \mathbb{F}_q^*$ such that the equation
  $$h_1 + h_2 = \alpha$$
  has no solution with $h_1, h_2 \in H_m$.
- **Property NP2:**
  There exists $\alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ such that the equation
  $$h_1 + h_2 = \alpha$$
  has no solution with $h_1, h_2 \in H_m$.
- **Property NP3:** *Assume that $q \equiv 3 \mod 8$. Let $\theta \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ be a primitive 4-th root of 1. There exists $\alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ with $\alpha^q = \theta\alpha$ such that the equation*
  $$h_1 + h_2 = \alpha$$
  has no solution with $h_1, h_2 \in H_m$.
- **Property NP4:** *Assume that $q \equiv 3 \mod 8$. Let $\theta \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ be a primitive 4-th root of 1. There exists $\alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ with $\alpha^q = -\theta\alpha$ such that the equation*
  $$h_1 + h_2 = \alpha$$
  has no solution with $h_1, h_2 \in H_m$.

Then we have the following:

- **Case $q \equiv 1 \mod 4$:**
  The covering radius of $\mathcal{C}_s(q_0)$ is 3 if and only if at least one of the two properties NP1 and NP2 holds. Otherwise the covering radius of $\mathcal{C}_s(q_0)$ is 2.
- **Case $q \equiv 3 \mod 8$:**
  The covering radius of $\mathcal{C}_s(q_0)$ is 3 if and only if at least one of the four properties NP1, NP2, NP3 and NP4 holds. Otherwise the covering radius of $\mathcal{C}_s(q_0)$ is 2.

Proof. We use some methods similar to the ones in the proof of Theorem 2.2. Assume first that $q \equiv 1 \mod 4$. Then $\gcd\left(\frac{q+1}{2}, q-1\right) = 1$. This implies that

$$\gcd\left(m(q+1), 2(q-1)\right) = 2gcd\left(m\frac{q+1}{2}, q-1\right) = 2m.$$

Therefore we obtain

$$\text{lcm }\left(m(q+1), 2(q-1)\right) = \frac{m(q+1)2(q-1)}{2m} = q^2 - 1.$$

Let G_2 be the subgroup of $\mathbb{F}_{q^2}^*$ with $|G_2| = 2(q-1)$. The arguments above imply that

$$\mathbb{F}_{q^2}^* = G_2 \cdot H_m,$$

which means that the smallest subgroup of $\mathbb{F}_{q^2}^*$ containing both G_2 and H_m is itself. Note that

$$G_2 = \left\{\alpha \in \mathbb{F}_{q^2}^* : \alpha^q = \alpha\right\} \sqcup \left\{\alpha \in \mathbb{F}_{q^2}^* : \alpha^q = -\alpha\right\}. \tag{59}$$

The disjoint subsets in (59) correspond to properties NP1 and NP2. Using also Lemma 3.1 we complete the proof if $q \equiv 1 \mod 4$.

Next we assume that $q \equiv 3 \mod 8$. Then $\gcd\left(\frac{q+1}{4}, q-1\right) = 1$. This implies that

$$\gcd\left(m(q+1), 4(q-1)\right) = 4gcd\left(m\frac{q+1}{4}, q-1\right) = 4m.$$

Therefore we obtain

$$\text{lcm }\left(m(q+1), 4(q-1)\right) = \frac{m(q+1)4(q-1)}{4m} = q^2 - 1.$$

Let G_4 be the subgroup of $\mathbb{F}_{q^2}^*$ with $|G_4| = 4(q-1)$. The arguments above imply that

$$\mathbb{F}_{q^2}^* = G_4 \cdot H_m.$$

Let $\theta \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ be a primitive 4-th root of 1. Note that

$$\begin{aligned} G_4 \;=\; & \left\{\alpha \in \mathbb{F}_{q^2}^* : \alpha^q = \alpha\right\} \sqcup \left\{\alpha \in \mathbb{F}_{q^2}^* : \alpha^q = -\alpha\right\} \\ & \sqcup \left\{\alpha \in \mathbb{F}_{q^2}^* : \alpha^q = \theta\alpha\right\} \sqcup \left\{\alpha \in \mathbb{F}_{q^2}^* : \alpha^q = -\theta\alpha\right\}. \end{aligned} \tag{60}$$

The disjoint subsets in (60) correspond to properties NP1, NP2, NP3 and NP4. Using also Lemma 3.1 we complete the proof. □

Remark 3.1. *In Theorem 3.2 below we show that the properties NP3 and NP4 are equivalent using rather detailed arithmetical methods. Therefore Theorem 3.2 below has only three properties instead of four.*

We also use the following simple result in some proofs below.

Lemma 3.2. *Let $\mathbb{F}_q$ be a finite field of odd characteristic. Assume that $q \equiv 3 \mod 8$. Then 2 is not a square in $\mathbb{F}_q$.*

Proof. Let p be the characteristic of $\mathbb{F}_q$ and put $q = p^t$, where t is a positive integer. We observe that $p \equiv 3 \mod 8$ and t is odd. Indeed if $p \equiv 1, 5$, or 7, then $p^t \not\equiv 3 \mod 8$ for any positive integer. Moreover if $p \equiv 3 \mod 8$ and $p^t \equiv 3 \mod 8$, then t is odd.

Using [12, Proposition 5.1.3] we obtain that 2 is not a square in $\mathbb{F}_p$. As t is odd we conclude that 2 is not a square in $\mathbb{F}_q$. □

Next we obtain an equivalent formulation of Theorem 3.1, which gives a connection to algebraic curves over finite fields. We also use this connection later.

Theorem 3.2. *Let $\mathbb{F}_{q_0}$ be a finite field of odd characteristic. For an integer $s \geq 1$, let $q = q_0^s$. Assume that $q \not\equiv 7 \mod 8$. Let $\mathcal{C}_s(q_0)$ be the generalized Zetterberg code of length $q+1$ over $\mathbb{F}_{q_0}$. Put $m = \frac{q_0-1}{2}$. Note that the number of nonzero squares in $\mathbb{F}_{q_0}$ is m. Let $\{\alpha_1, \ldots, \alpha_m\}$ be an enumerated set consisting of the nonzero square elements in $\mathbb{F}_{q_0}$.*

Let $w \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ with $w + w^q = 1$. Put $D = \frac{1}{4} - w^{q+1}$. Recall that $D \in \mathbb{F}_q^*$ and D is not a square in $\mathbb{F}_q$ (see Lemma 2.1 above).

Let PP1, PP2 and PP3 be the properties defined depending on q_0 and s as follows.

- **Property PP1:**

  For $1 \leq i \leq m$, let $f_i(x) \in \mathbb{F}_q[x]$ be the polynomial given by

$$f_i(x) = x^2 - \alpha_i.$$

  There exists $a \in \mathbb{F}_q^*$ such that $f_i(a)$ is a nonzero square in $\mathbb{F}_q$ for each $1 \leq i \leq m$.

- **Property PP2:**

  For $1 \leq i \leq m$, let $f_i(x) \in \mathbb{F}_q[x]$ be the polynomial given by

$$f_i(x) = x^2 + \frac{\alpha_i}{D}.$$

  There exists $a \in \mathbb{F}_q^*$ such that $f_i(a)$ is a nonzero square in $\mathbb{F}_q$ for each $1 \leq i \leq m$.

- **Property PP3:** *For $1 \leq i \leq m$, let $f_i(x) \in \mathbb{F}_q[x]$ be the polynomial given by*

$$f_i(x) = x^2 - 2\alpha_i.$$

  There exists $a \in \mathbb{F}_q^*$ such that $f_i(a)$ is a nonzero square in $\mathbb{F}_q$ for each $1 \leq i \leq m$.

Then we have the following:

- **Case $q \equiv 1 \mod 4$:**

  The covering radius of $\mathcal{C}_s(q_0)$ is 3 if and only if at least one of the two properties PP1 and PP2 holds. Otherwise the covering radius of $\mathcal{C}_s(q_0)$ is 2.

- **Case $q \equiv 3 \mod 8$:**

  The covering radius of $\mathcal{C}_s(q_0)$ is 3 if and only if at least one of the three properties PP1, PP2 and PP3 holds. Otherwise the covering radius of $\mathcal{C}_s(q_0)$ is 2.

Proof. Let a be a generator of $\mathbb{F}_{q_0}^*$. Note that

$$h \in H_m \iff h^{q+1} = a^{2i} \text{ for some } 0 \le i \le m-1. \tag{61}$$

We first show that Property NP1 is equivalent to Property PP1.

Let $\alpha \in \mathbb{F}_q^*$. Using the methods of Theorem 2.3 and (61) we obtain that there exist $h_1, h_2 \in H_m$ such that

$$h_1 + h_2 = \alpha$$

if and only if there exist $x_1, x_2, y_1, y_2 \in \mathbb{F}_q$ and integers $0 \le i, j \le m-1$ such that

$$\begin{cases} x_1 + x_2 &=& \alpha, \\ y_1 + y_2 &=& 0, \\ x_1^2 - Dy_1^2 &=& a^{2i}, \text{ and} \\ x_2^2 - Dy_2^2 &=& a^{2j}. \end{cases} \tag{62}$$

We continue to use some methods from the proof of Theorem 2.3. Putting $x = x_2$, $y = y_2$, $x_1 = x - \alpha$ and $y_1 = -y_2$, the system in (62) becomes equivalent to the system

$$\begin{cases} \alpha^2 + a^{2j} - a^{2i} &=& 2x\alpha, \text{ and} \\ x^2 - a^{2j} &=& Dy^2. \end{cases} \tag{63}$$

Note that $\alpha \neq 0$ and using (63) we obtain

$$x = \frac{\alpha^2 - a^{2i} + a^{2j}}{2\alpha}.$$

Therefore (63) is equivalent to

$$\left(\frac{\alpha^2 - a^{2i} + a^{2j}}{2\alpha}\right)^2 - a^{2j} = Dy^2. \tag{64}$$

Recall that $D \in \mathbb{F}_q^*$ is a nonsquare. Note that Property NP1 does not hold if $\alpha \in \mathbb{F}_{q_0}$. Moreover $y = 0$ in (64) implies that $y_1 = y_2 = 0$ and $x_1, x_2 \in \mathbb{F}_{q_0}$ for the system in (62). Hence $y = 0$ in (64) also implies that $\alpha \in \mathbb{F}_{q_0}$. Therefore we assume that $y \neq 0$ in (64) without loss of generality.

These arguments imply that Property NP1 holds if and only if

$$\left(\frac{\alpha^2 - a^{2i} + a^{2j}}{2\alpha}\right)^2 - a^{2j} \text{ is a square in } \mathbb{F}_q^* \tag{65}$$

for each $0 \le i, j \le m-1$.

The condition in (65) is equivalent to the condition that

$$\left(\alpha^2 - a^{2i} + a^{2j}\right)^2 - 4\alpha^2 a^{2j} \text{ is a square in } \mathbb{F}_q^* \tag{66}$$

for each $0 \le i, j \le m-1$.

Note that the left hand side of (66) is

$$\left(\alpha - a^i + a^j\right)\left(\alpha - a^i - a^j\right)\left(\alpha + a^i + a^j\right)\left(\alpha + a^i - a^j\right). \tag{67}$$

If $0 \le i = j \le m-1$, then using (67) the condition in (66) becomes

$$\left(\alpha - 2a^i\right)\left(\alpha + 2a^i\right) \text{ is a square in } \mathbb{F}_q^* \tag{68}$$

for each $0 \le i \le m-1$. Note that $\{4a^{2i} : 0 \le i \le m-1\}$ is the set of nonzero square elements in $\mathbb{F}_{q_0}$. Hence Property NP1 implies Property PP1. For the converse we also consider the remaining case that $0 \le i, j \le m-1$ with $i \ne j$ in (66). In this remaining case, using (67) the condition in (66) becomes

$$(\alpha - u)(\alpha + u)(\alpha - v)(\alpha + v) \text{ is a square in } \mathbb{F}_q^*, \tag{69}$$

where $u = a^i - a^j \in \mathbb{F}_{q_0}^*$ and $v = a^i + a^j \in \mathbb{F}_{q_0}^*$. Note that if $(u^2 - \alpha_i)$ is a nonzero square for each $1 \le i \le m$, then the condition in (69) is automatically satisfied for this remaining case. These arguments show that Property NP1 is equivalent to Property PP1.

Next we show that Property NP2 is equivalent to Property PP2. Let $\alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ with $\alpha^q = -\alpha$. Put $\beta = \frac{2\alpha}{2w-1}$. Note that $\beta \in \mathbb{F}_q^*$. Using the methods of the proof of Theorem 2.4 and (61) we obtain that that there exist $h_1, h_2 \in H_m$ such that

$$h_1 + h_2 = \alpha$$

if and only if there exist $x_1, x_2, y_1, y_2 \in \mathbb{F}_q$ and integers $0 \le i, j \le m-1$ such that

$$\left\{\begin{array}{rcl} x_1 + x_2 &=& 0, \\ y_1 + y_2 &=& \beta, \\ x_1^2 - Dy_1^2 &=& a^{2i}, \text{ and} \\ x_2^2 - Dy_2^2 &=& a^{2j}. \end{array}\right. \tag{70}$$

We continue to use some methods from the proof of Theorem 2.4. Putting $x = x_2$, $y = y_2$, $x_1 = -x$ and $y_1 = \beta - y$, the system in (70) becomes equivalent to the system

$$\left\{\begin{array}{rcl} -D\beta^2 + 2D\beta y + a^{2j} &=& a^{2i}, \text{ and} \\ x^2 - Dy^2 &=& a^{2j}. \end{array}\right. \tag{71}$$

If $q \equiv 1 \mod 4$, then we can assume that $x \ne 0$ in (71) without loss of generality. Indeed, otherwise $-Dy^2$ becomes a nonzero square in $\mathbb{F}_q$, which is a contradiction as -1 is a square and D is a nonsquare in $\mathbb{F}_q$.

If $q \equiv 3 \mod 4$, then we can also assume that $x \ne 0$ in (71) without loss of generality. This observation needs a detailed explanation. Assume the contrary and let $D_1 \in \mathbb{F}_q^*$ with $D_1^2 = -D$. Then $x_1 = x_2 = 0$ and $y_1, y_2 \in \frac{1}{D_1}\mathbb{F}_{q_0}^*$ in (70). Consequently if $q \equiv 3 \mod 4$ and $x = 0$, then $\beta \in \frac{1}{D_1}\mathbb{F}_{q_0}^*$. If $s = 1$, neither NP2 nor PP2 holds. If $s \ge 2$ and

$\beta \in \frac{1}{D_1}\mathbb{F}_{q_0}^*$, then neither NP2 nor PP2 holds. Hence we can also assume that $x \neq 0$ in (71) without loss of generality.

These arguments show that we can assume that $x \neq 0$ in (71) without loss of generality. As $\beta \neq 0$, using (71) we obtain

$$y = \frac{\beta^2 + \frac{a^{2i}}{D} - \frac{a^{2j}}{D}}{2\beta}.$$

Therefore (71) is equivalent to

$$\left(\frac{\beta^2 + \frac{a^{2i}}{D} - \frac{a^{2j}}{D}}{2\beta}\right)^2 + \frac{a^{2j}}{D} = \frac{x^2}{D}. \tag{72}$$

Recall that $x, D \in \mathbb{F}_q^*$ and D is a nonsquare. These arguments imply that Property NP1 holds if and only if

$$\left(\frac{\beta^2 + \frac{a^{2i}}{D} - \frac{a^{2j}}{D}}{2\beta}\right)^2 + \frac{a^{2j}}{D} \text{ is a square in } \mathbb{F}_q^* \tag{73}$$

for each $0 \leq i, j \leq m-1$.

The condition in (73) is equivalent to the condition that

$$\left(\beta^2 + \frac{a^{2i}}{D} - \frac{a^{2j}}{D}\right)^2 + 4\beta^2\frac{a^{2j}}{D} \text{ is a square in } \mathbb{F}_q^* \tag{74}$$

for each $0 \leq i, j \leq m-1$.

Recall that $\theta \in \mathbb{F}_{q^2}^*$ is a primitive 4-th root of 1. Put $D_2 \in \mathbb{F}_{q^2}^*$ such that $D_2^2 = D$. Note that the left hand side of (74) is

$$\begin{array}{l} \left(\beta - \theta\frac{a^i}{D_2} + \theta\frac{a^j}{D_2}\right)\left(\beta - \theta\frac{a^i}{D_2} - \theta\frac{a^j}{D_2}\right) \\ \left(\beta + \theta\frac{a^i}{D_2} + \theta\frac{a^j}{D_2}\right)\left(\beta + \theta\frac{a^i}{D_2} - \theta\frac{a^j}{D_2}\right). \end{array} \tag{75}$$

If $0 \leq i = j \leq m-1$, then using (75) the condition in (74) becomes

$$\left(\beta - 2\theta\frac{a^i}{D_2}\right)\left(\beta + 2\theta\frac{a^i}{D_2}\right) \text{ is a square in } \mathbb{F}_q^* \tag{76}$$

for each $0 \leq i \leq m-1$. Note that $\left\{\frac{4\theta^2 a^{2i}}{D_2^2} : 0 \leq i \leq m-1\right\} = \left\{\frac{-1}{D}\alpha_i : 1 \leq i \leq m\right\}$. Hence Property NP2 implies Property PP2. For the converse we also consider the remaining case that $0 \leq i, j \leq m-1$ with $i \neq j$ in (74). In this remaining case, using (75) the condition in (74) becomes

$$(\beta - u)(\beta + u)(\beta - v)(\beta + v) \text{ is a square in } \mathbb{F}_q^*, \tag{77}$$

where $u = \frac{\theta}{D_2}(a^i - a^j)$ and $v = \frac{\theta}{D_2}(a^i + a^j)$. Note that if $u^2, v^2 \in \left\{\frac{-1}{D}\alpha_i : 1 \leq i \leq m\right\}$. Therefore if PP2 holds, then the condition in (77) is automatically satisfied for this remaining case. These arguments show that Property NP2 is equivalent to Property PP2.

Assume that $q \equiv 3 \mod 8$. Next we show that Property NP3 is equivalent to Property PP3. Recall that $\theta \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ is a primitive 4-th root of 1. Let $\alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ with $\alpha^q = \theta\alpha$. Let $w = \theta - 1$ and $\mu = \frac{\alpha(1-\theta)}{2\theta}$. Note that $\mu \in \mathbb{F}_q^*$. Using the methods of the proof of Theorem 2.5 and (61) we obtain that there exist $h_1, h_2 \in H_m$ such that

$$h_1 + h_2 = \alpha$$

if and only if there exist $x_1, x_2, y_1, y_2 \in \mathbb{F}_q$ and integers $0 \leq i, j \leq m-1$ such that

$$\left\{ \begin{array}{rcl} x_1 + x_2 & = & \mu, \\ y_1 + y_2 & = & 0, \\ x_1^2 + y_1^2 & = & \frac{a^{2i}}{2}, \text{ and} \\ x_2^2 + y_2^2 & = & \frac{a^{2j}}{2}. \end{array} \right. \tag{78}$$

We continue to use some methods from the proof of Theorem 2.5. Putting $x = x_2$, $y = y_2$, $x_1 = \mu - x$ and $y_1 = -y$, the system in (78) becomes equivalent to the system

$$\left\{ \begin{array}{rcl} \mu^2 - 2\mu x + \frac{a^{2j}}{2} & = & \frac{a^{2i}}{2}, \text{ and} \\ x^2 + y^2 & = & \frac{a^{2j}}{2}. \end{array} \right. \tag{79}$$

Let $\gamma \in \mathbb{F}_{q^2}$ such that $\gamma^2 = 2$. Using Lemma 3.2 we obtain that $\gamma \notin \mathbb{F}_q$.

We assume that y in (79) is not zero without loss of generality. Indeed, otherwise using (71) we obtain that $y_1 = 0$ and hence $x_1^2 = \frac{a^{2i}}{2}2$. This is a contradiction as 2 is not a square in $\mathbb{F}_q$ by Lemma 3.2.

As $\mu \neq 0$, using (79) we obtain

$$x = \frac{\mu^2 + \frac{a^{2j}}{2} - \frac{a^{2i}}{2}}{2\mu}.$$

Therefore (79) is equivalent to

$$\left(\frac{\mu^2 + \frac{a^{2j}}{2} - \frac{a^{2i}}{2}}{2\mu} \right)^2 - \frac{a^{2j}}{2} = -y^2. \tag{80}$$

Recall $y \neq 0$ and -1 is a nonsquare in $\mathbb{F}_q$. These arguments imply that Property NP3 holds if and only if

$$\left(\frac{\mu^2 + \frac{a^{2j}}{2} - \frac{a^{2i}}{2}}{2\mu} \right)^2 - \frac{a^{2i}}{2} \text{ is a square in } \mathbb{F}_q^* \tag{81}$$

for each $0 \leq i, j \leq m-1$.

The condition in (81) is equivalent to the condition that

$$\left(\mu^2 + \frac{a^{2j}}{2} - \frac{a^{2i}}{2} \right)^2 - 4\mu^2 \frac{a^{2j}}{2} \text{ is a square in } \mathbb{F}_q^* \tag{82}$$

for each $0 \leq i, j \leq m-1$.

Recall that $\gamma^2 = 2$. Note that the left hand side of (82) is

$$\begin{array}{c}\left(\mu - \frac{a^j}{\gamma} + \frac{a^i}{\gamma}\right)\left(\mu - \frac{a^j}{\gamma} - \frac{a^i}{\gamma}\right) \\ \left(\mu + \frac{a^j}{\gamma} + \frac{a^i}{\gamma}\right)\left(\mu + \frac{a^j}{\gamma} - \frac{a^i}{\gamma}\right).\end{array} \tag{83}$$

If $0 \le i = j \le m-1$, then using (83) the condition in (82) becomes

$$\left(\mu - 2\frac{a^i}{\gamma}\right)\left(\mu + 2\frac{a^i}{\gamma}\right) \text{ is a square in } \mathbb{F}_q^* \tag{84}$$

for each $0 \le i \le m-1$. Note that $\left\{\frac{4a^{2i}}{\gamma^2} : 0 \le i \le m-1\right\} = \{2\alpha_i : 1 \le i \le m\}$. Hence Property NP3 implies Property PP3. For the converse we also consider the remaining case that $0 \le i, j \le m-1$ with $i \ne j$ in (82). In this remaining case, using (83) the condition in (82) becomes

$$(\mu - u)(\mu + u)(\mu - v)(\mu + v) \text{ is a square in } \mathbb{F}_q^*, \tag{85}$$

where $u = \frac{1}{\gamma}(a^j - a^i)$ and $v = \frac{1}{\gamma}(a^j + a^i)$. Note that if $u^2, v^2 \in \{2\alpha_i : 1 \le i \le m\}$. Therefore if PP2 holds, then the condition in (85) is automatically satisfied for this remaining case. These arguments show that Property NP3 is equivalent to Property PP3.

We still assume that $q \equiv 3 \mod 8$. Finally we show that Property NP4 is equivalent to Property PP3. Recall that $\theta \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ is a primitive 4-th root of 1. Let $\alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ with $\alpha^q = -\theta\alpha$. Let $w = \theta - 1$ and $\mu = -\frac{\alpha(1-\theta)}{2\theta}$. Note that $\mu \in \mathbb{F}_q^*$. Using the methods of the proof of Theorem 2.6 and (61) we obtain that that there exist $h_1, h_2 \in H_m$ such that

$$h_1 + h_2 = \alpha$$

if and only if there exist $x_1, x_2, y_1, y_2 \in \mathbb{F}_q$ and integers $0 \le i, j \le m-1$ such that

$$\left\{\begin{array}{rcl} x_1 + x_2 & = & 0, \\ y_1 + y_2 & = & \mu, \\ x_1^2 + y_1^2 & = & \frac{a^{2i}}{2}, \text{ and} \\ x_2^2 + y_2^2 & = & \frac{a^{2j}}{2}. \end{array}\right. \tag{86}$$

Comparing the systems in (78) and (86) we conclude that Property NP4 is equivalent to Property PP3. This completes the proof. $\square$

As a direct consequence of Theorem 3.2, we obtain the covering radius of $\mathcal{C}_s(q_0)$ if $q_0 = 3$ or $s = 1$.

Corollary 3.1. *For an integer $s \ge 1$, let $\mathcal{C}_s(q_0)$ be the generalized Zetterberg code of length $3^s + 1$ over $\mathbb{F}_3$. Then the covering radius of $\mathcal{C}_s(q_0)$ is 3 if $s \ge 2$. Moreover the covering radius of $\mathcal{C}_s(q_0)$ is 2 if $s = 1$.*

Proof. We use the notation of Theorem 3.2. We have $q_0 = 3$, $m = 1$ and $\alpha_1 = 1$.

Assume that $s = 1$ and hence $q = q_0$. It is clear that Property PP1 does not hold as $a^2 - 1 = 0$ for all $a \in \mathbb{F}_q^*$. Note that 2 is the only nonzero nonsquare element in $\mathbb{F}_q$. Then Property PP2 does not hold as $a^2 + \frac{1}{D} = a^2 + 2 = 0$ for all $a \in \mathbb{F}_q^*$, where $D = 2$. Finally we observe that $a^2 - 2 = -1$, which is not a square in $\mathbb{F}_q$, for all $a \in \mathbb{F}_q^*$. This implies that Property PP3 does not hold as well. Hence the covering radius of $\mathcal{C}_s(q_0)$ is 2 if $s = 1$.

Assume that $s \geq 2$ and hence $q = q_0^s \geq 9$. Consider the map

$$\begin{array}{rcl} \psi : \mathbb{F}_q \setminus \{-1, 0, 1\} & \rightarrow & \mathbb{F}_q \setminus \{-1, 0, 1\} \\ x & \mapsto & 1 + \frac{2}{x-1}. \end{array}$$

Note that ψ is one-to-one and onto. Note that the number of nonzero square in $\mathbb{F}_q$ is at least $\frac{q-1}{2} - 2 > 0$. Therefore we choose $y \in \mathbb{F}_q \setminus \{-1, 0, 1\}$ which is a square in $\mathbb{F}_q$. Let $x \in \mathbb{F}_q \setminus \{-1, 0, 1\}$ such that $\psi(x) = y$. We observe that $x^2 - 1$ is a nonzero square in $\mathbb{F}_q$ as $y = \psi(x) = \frac{x^2-1}{(x-1)^2}$ is a nonzero square. These arguments show that Property PP1 holds for any $s \geq 2$. This completes the proof. $\square$

Corollary 3.2. *Let $\mathbb{F}_{q_0}$ be a finite field with odd characteristic. Assume that* $q_0 \not\equiv 7 \mod 8$. *Let $\mathcal{C}_s(q_0)$ be the generalized Zetterberg code of length $q_0 + 1$ over $\mathbb{F}_{q_0}$. Then the covering radius of $\mathcal{C}_s(q_0)$ is 2.*

Proof. Note that $q = q_0$ as $s = 1$.

We first show that Property PP1 does not hold. Assume the contrary and let $a \in \mathbb{F}_{q_0}^*$ such that

$$a^2 - \alpha_i \text{ is a nonzero square in } \mathbb{F}_{q_0} \tag{87}$$

for each $1 \leq i \leq m$. Note that if $1 \leq i < j \leq m$, then

$$a^2 - \alpha_i \neq a^2 - \alpha_j. \tag{88}$$

Moreover there are exactly m nonzero square elements in $\mathbb{F}_{q_0}$ and a^2 is one of them. Therefore using (87) and (88) we obtain the existence of $1 \leq i_0 \leq m$ such that

$$a^2 - \alpha_{i_0} = a^2,$$

which is a contradiction as $\alpha_i \neq 0$ for $1 \leq i \leq m$. Hence Property PP1 does not hold.

Recall that, when $s = 1$, D is a fixed nonzero nonsquare element of $\mathbb{F}_{q_0}$. Next we show that Property PP2 does not hold using a similar method. Assume the contrary and let $a \in \mathbb{F}_{q_0}^*$ such that

$$a^2 + \frac{\alpha_i}{D} \text{ is a nonzero square in } \mathbb{F}_{q_0} \tag{89}$$

for each $1 \leq i \leq m$. Note that if $1 \leq i < j \leq m$, then

$$a^2 + \frac{\alpha_i}{D} \neq a^2 + \frac{\alpha_j}{D}. \tag{90}$$

Moreover there are exactly m nonzero square elements in $\mathbb{F}_{q_0}$ and a^2 is one of them. Therefore using (89) and (90) we obtain the existence of $1 \leq i_0 \leq m$ such that

$$a^2 + \frac{\alpha_{i_0}}{D} = a^2,$$

which is a contradiction as $\alpha_i \neq 0$ for $1 \leq i \leq m$. Hence Property PP2 does not hold.

Assume that $q \equiv 3 \mod 8$. Finally we show that Property PP3 does not hold again using a similar method. Assume the contrary and let $a \in \mathbb{F}_{q_0}^*$ such that

$$a^2 - 2\alpha_i \text{ is a nonzero square in } \mathbb{F}_{q_0} \tag{91}$$

for each $1 \leq i \leq m$. Note that if $1 \leq i < j \leq m$, then

$$a^2 - 2\alpha_i \neq a^2 - 2\alpha. \tag{92}$$

Moreover there are exactly m nonzero square elements in $\mathbb{F}_{q_0}$ and a^2 is one of them. Therefore using (91) and (92) we obtain the existence of $1 \leq i_0 \leq m$ such that

$$a^2 - 2\alpha_{i_0} = a^2,$$

which is a contradiction as $\alpha_i \neq 0$ for $1 \leq i \leq m$. Hence Property PP3 does not hold. Using Theorem 3.2 we complete the proof. □

The next corollary shows that the covering radius is always 3 if $s \geq 2$ is an **even** integer, independent of q_0.

Corollary 3.3. *Let $\mathbb{F}_{q_0}$ be a finite field of odd characteristic. Let $s \geq 2$ be an* **even** *integer. Let $\mathcal{C}_s(q_0)_s$ be the generalized Zetterberg code of length $q_0^s + 1$ over $\mathbb{F}_{q_0}$. Then the covering radius of $\mathcal{C}_s(q_0)_s$ is 3.*

Proof. We show that Property PP1 holds, which is enough by Theorem 3.2. Let β be a nonzero and nonsquare element of $\mathbb{F}_{q_0}$. We keep the notation of Theorem 3.2. In particular $m = \frac{q_0-1}{2}$ and $\{\alpha_1, \ldots, \alpha_m\}$ is an enumerated set consisting of the nonzero square elements of $\mathbb{F}_{q_0}$. Then $\beta \notin \{\alpha_1, \ldots, \alpha_m\}$ and $(\beta - \alpha_i) \in \mathbb{F}_{q_0}^*$ for each $1 \leq i \leq m$. Note that there exists $a \in \mathbb{F}_{q_0^2} \setminus \mathbb{F}_{q_0}$ such that $a^2 = \beta$. Hence we have that

$$a^2 - \alpha_i \text{ is a nonzero square in } \mathbb{F}_{q_0^2} \text{ for each } 1 \leq i \leq m. \tag{93}$$

Indeed $a^2 - \alpha_i = \beta - \alpha_i \in \mathbb{F}_{q_0}^*$ and hence has a square root in $\mathbb{F}_{q_0^2}$ for each $1 \leq i \leq m$. Using (93) we show that Property PP1 holds, which completes the proof. □

It is rather surprising that there exists a finite field $\mathbb{F}_{q_0}$ of odd characteristic and odd integer $s \geq 3$ such that $q_0 \not\equiv 7 \mod 8$ and the covering radius of the generalized Zetterberg code of length $q_0^s + 1$ over $\mathbb{F}_{q_0}$ is 2, not 3 as in the case of even integers $s \geq 2$ as proved in Corollary 3.3. We refer to Examples 3.6, 3.7 and Example 3.8 for some concrete examples.

From now on till the end of this section we consider the remaining cases so that $\mathbb{F}_{q_0}$ is a finite field with $q_0 > 3$, $q_0 \not\equiv 7 \mod 8$, and $s \geq 3$ is an odd integer, if not explicitly stated otherwise.

First we have a simple lemma that we use in some proofs below.

Lemma 3.3. *Let $\mathbb{F}_{q_0}$ be a finite field of odd characteristic. Assume that $q_0 > 3$. If $x \in \mathbb{F}_{q_0}^*$, then there exists $y \in \mathbb{F}_{q_0} \setminus \{0, x, -x\}$ such that $(x^2 - y^2)$ is a nonzero nonsquare element in $\mathbb{F}_{q_0}$.*

Proof. Let $x \in \mathbb{F}_{q_0}^*$. We define the map $\psi_x : \mathbb{F}_{q_0} \setminus \{0, x, -x\} \to \mathbb{F}_{q_0} \setminus \{0, 1, -1\}$ given by

$$\psi_x(y) = 1 + \frac{2y}{x - y}.$$

It is not difficult to observe that ψ_x is one-to-one and onto.

Note that 1 is a square in $\mathbb{F}_{q_0}$. Hence there exists at least

$$\frac{q_0 - 1}{2} - 1 = \frac{q_0 - 3}{2}$$

distinct nonsquare elements of $\mathbb{F}_{q_0}$ in the image set $\mathbb{F}_{q_0} \setminus \{0, -1, 1\}$ of ψ_x. As $q_0 > 3$, we conclude that there exists $\beta \in \mathbb{F}_{q_0} \setminus \{0, 1, -1\}$ such that β is a nonsquare in $\mathbb{F}_{q_0}$. Let $y \in \mathbb{F}_{q_0} \setminus \{0, x, -x\}$ such that $\psi_x(y) = \beta$. We obtain that

$$1 + \frac{2y}{x - y} \tag{94}$$

is a nonsquare in $\mathbb{F}_q$ and $y \notin \{0, x, -x\}$. We observe that $(x^2 - y^2)$ is a nonsquare in $\mathbb{F}_{q_0}$ if and only if

$$\frac{x^2 - y^2}{(x - y)^2} = \frac{x + y}{x - y} = 1 + \frac{2y}{x - y} \tag{95}$$

is a nonsquare in $\mathbb{F}_{q_0}$. Combining (94) and (95) we complete the proof. □

The following three theorems are related to the properties PP1, PP2 and PP3 in Theorem 3.2 above. We refer to [16] and [19] for notation and further background on algebraic curves over finite fields.

The following theorem is related to Property PP1 of Theorem 3.2 (see the last item in the following theorem).

Theorem 3.3. *Let $\mathbb{F}_{q_0}$ be a finite field of odd characteristic. Assume that $q_0 > 3$. Let $m = \frac{q_0 - 1}{2}$ and $\{\alpha_1, \ldots, \alpha_m\}$ be an enumerated set consisting of the nonzero squares in $\mathbb{F}_{q_0}$. Let $s \geq 3$ be an odd integer and put $q = q_0^s$.*

Let χ_1 be the fibre product of the projective lines over $\mathbb{F}_q$ given by

$$\chi_1 : \begin{cases} y_1^2 &= x^2 - \alpha_1, \\ y_2^2 &= x^2 - \alpha_2, \\ &\vdots \\ y_m^2 &= x^2 - \alpha_m. \end{cases}$$

Let P_∞ be the pole of x in $\mathbb{F}_q(x)$. For $\alpha \in \mathbb{F}_q$, let P_α be the zero of $(x-\alpha)$ in $\mathbb{F}_q(x)$. We have the following:

(i). *The genus g of χ_1 is*

$$g = 1 + 2^{m-1}(m-2).$$

(ii). *There are exactly 2^m $\mathbb{F}_q$-rational points of χ_1 over P_∞.*

(iii). *If $q \equiv 1 \mod 4$, then there are exactly 2^m $\mathbb{F}_q$-rational points of χ_1 over P_0.*
If $q \equiv 3 \mod 4$, then there is no $\mathbb{F}_q$-rational point of χ_1 over P_0.

(iv). *If $\alpha \in \mathbb{F}_q^*$, then there are exactly 2^m $\mathbb{F}_q$-rational points of χ_1 over P_α if and only if*

$$f_i(\alpha) \text{ is a nonzero square in } \mathbb{F}_q \tag{96}$$

for each $1 \le i \le m$, where $f_i(x) = x^2 - \alpha_i \in \mathbb{F}_q[x]$.
If (96) does not hold, then there is no $\mathbb{F}_q$-rational point of χ_1 over P_α.

Proof. For $1 \le i \le m$, let $\mathbb{F}_q(x_0)(y_i)$ be the algebraic extension of $\mathbb{F}_q(x)$ such that $y^2 = x^2 - \alpha_i$. Note that the polynomial

$$T^2 - (x^2 - \alpha_i) \in \mathbb{F}_{q_0}(x)[T]$$

is absolutely irreducible for $1 \le i \le m$. Let K be an algebraic closure of $\mathbb{F}_q$. For $1 \le i \le m$, let $S_i \subseteq K$ be the roots of the equation

$$x^2 - \alpha_i.$$

We observe that $S_i \cap S_j = \emptyset$ if $1 \le i < j \le m$, and $|S_i| = 2$ for each $1 \le i \le m$. Put $S = \sum_{i=1}^m S_i$.

Let $E = \mathbb{F}_q(x)(y_1, y_2, \ldots, y_m)$ and $\overline{E} = K(x)(y_1, y_2, \ldots, y_m)$. The arguments above imply that $[E : \mathbb{F}_q(x)] = 2^m$ and $\overline{E} : K(x)] = 2^m$. Note that E is the algebraic function field of the curve χ_1 and $\overline{E}$ is the algebraic closure of the constant field extension of χ_1 by the extension $K/\mathbb{F}_q$. Hence the genus of E and the genus of $\overline{E}$ are the same.

Let Q_∞ be the pole of x in $K(x)$. For $\beta \in K$, let Q_β be the zero of $(x-\beta)$ in $K(x)$. Note that Q_∞ is unramified in the extension $\overline{E}/K(x)$. Moreover if $\beta \in K \setminus S$, then Q_β is also unramified in the extension $\overline{E}/K(x)$.

It remains to consider Q_β with $\beta \in S$. Using Abhyankar's Lemma (see, for example, [19, Theorem 3.9.1]), for the ramification index $e(Q_\beta)$ of Q_β in the extension $\overline{E}/K(x)$ we obtain that

$$e(Q_\beta) = 2. \tag{97}$$

Then using Hurwitz genus formula (see, for example, [19, Theorem 3.4.13]) for the extension $\overline{E}/K(x)$ we obtain that

$$2g - 2 = 2^m(0-2) + 2^{m-1}|S|(2-1) = -2^{m+1} + 2^m m = (m-2)2^m.$$

This completes a proof of item (i).

Note that P_∞ splits completely in the extension $\mathbb{F}_q(x)(y_i)/\mathbb{F}_q(x)$ for each $1 \le i \le m$. This implies a proof of item (ii).

Assume that $q \equiv 1 \mod 4$. Note that the evaluation of the polynomial $x^2 - \alpha_i$ at the place P_0 is $-\alpha_i$ for $1 \le i \le m$. As -1 and α_i are square elements in $\mathbb{F}_q$, we have that $-\alpha_i$ is a square in $\mathbb{F}_q$ for each $1 \le i \le m$. This implies a proof of item (iii) for the case $q \equiv 1 \mod 4$.

Assume that $q \equiv 3 \mod 4$. Hence -1 is not a square in $\mathbb{F}_q$. Then, for example, $-\alpha_1$ is not a square in $\mathbb{F}_q$. This implies a proof of item (iii) for the case $q \equiv 3 \mod 4$.

Let $\alpha \in \mathbb{F}_{q_0}^*$. Assume first that $f_i(\alpha) \neq 0$ for each $1 \le i \le m$. Then using the methods of [16] we obtain that there exists either no or exactly 2^m many $\mathbb{F}_q$-rational points of χ_1 over P_α. Moreover these methods also imply that there exists an $\mathbb{F}_q$-rational point of χ_1 over P_α if and only if (96) holds.

Finally we assume that $\alpha \in \mathbb{F}_{q_0}^*$ and there exists $1 \le i_0 \le m$ such that $f_{i_0}(\alpha) = 0$. Note that α_{i_0} is a square element in $\mathbb{F}_{q_0}^*$ and hence we have that $\alpha \in \mathbb{F}_{q_0}$ and $\alpha^2 = \alpha_{i_0}$. Using Lemma 3.3 we obtain that there exists $1 \le i \le m$ such that $i \neq i_0$ and $(\alpha^2 - \alpha_i)$ is a nonzero nonsquare in $\mathbb{F}_{q_0}$. As s is odd we also obtain that for that $1 \le i \le m$ with $i \neq i_0$, $(\alpha^2 - \alpha_i)$ is nonzero nonsquare in $\mathbb{F}_q$ as well. These arguments imply that there is no $\mathbb{F}_q$-rational point of χ_1 over P_α. This completes the proof of item (iv). $\square$

The following theorem is related to Property PP2 of Theorem 3.2 (see the last item in the following theorem).

Theorem 3.4. *We keep the notation and assumptions of Theorem 3.3. In particular* $q_0 > 3$, $s \ge 3$ *is an odd integer and* $q = q_0^s$. *Let* $D \in \mathbb{F}_q^*$ *be a nonzero nonsquare in* $\mathbb{F}_q$.

Let χ_2 *be the fibre product of the projective lines over* $\mathbb{F}_q$ *given by*

$$\chi_2 : \begin{cases} y_1^2 &= x^2 + \frac{\alpha_1}{D}, \\ y_2^2 &= x^2 + \frac{\alpha_2}{D}, \\ &\vdots \\ y_m^2 &= x^2 + \frac{\alpha_m}{D}. \end{cases}$$

Let P_∞ be the pole of x in $\mathbb{F}_q(x)$. For $\alpha \in \mathbb{F}_q$, let P_α be the zero of $(x-\alpha)$ in $\mathbb{F}_q(x)$. We have the following:

(i). *The genus g of χ_2 is*

$$g = 1 + 2^{m-1}(m-2).$$

(ii). *There are exactly 2^m $\mathbb{F}_q$-rational points of χ_2 over P_∞.*

(iii). *There is no $\mathbb{F}_q$-rational point of χ_2 over P_0.*

(iv). *If $\alpha \in \mathbb{F}_q^*$, then there are exactly 2^m $\mathbb{F}_q$-rational points of χ_2 over P_α if and only if*

$$f_i(\alpha) \text{ is a nonzero square in } \mathbb{F}_q \tag{98}$$

for each $1 \le i \le m$, where $f_i(x) = x^2 + \frac{\alpha_i}{D} \in \mathbb{F}_q[x]$.

If (98) does not hold, then there is no $\mathbb{F}_q$-rational point of χ_2 over P_α.

Proof. The arguments in the proofs of items (i) and (ii) of Theorem 3.3 imply similar proofs for the items (i) and (ii) of the current theorem.

Let $1 \le i \le m$. Note that the evaluation of the polynomial $x^2 + \frac{\alpha_i}{D}$ at the place P_0 is $\frac{\alpha_i}{D}$. As α_i is a square in $\mathbb{F}_{q_0}^*$, it is also a square in $\mathbb{F}_q^*$. Moreover D is a nonsquare in $\mathbb{F}_q^*$ and hence $\frac{\alpha_i}{D}$ cannot be a square in $\mathbb{F}_q^*$. These arguments complete the proof of item (iii).

In the rest of this proof we consider item (iv). Let $\alpha \in \mathbb{F}_q^*$. Assume first that $f_i(\alpha) \neq 0$ for each $1 \le i \le m$. Under this assumption, the corresponding arguments in the proof of item (iv) of Theorem 3.3 imply a similar proof for the item (iv) of the current theorem.

Assume secondly that $q \equiv 1 \mod 4$. We claim that there is no $1 \le i \le m$ such that $f_i(\alpha) = 0$. Indeed otherwise $\alpha^2 = -\frac{\alpha_i}{D}$ for some $1 \le i \le m$. In particular $-\frac{\alpha_i}{D}$ is a square in $\mathbb{F}_q^*$, which is a contradiction as (-1) and α_i are squares and D is a nonsquare.

Assume finally that $q \equiv 3 \mod 4$ and there exists $1 \le i_0 \le m$ such that $f_{i_0}(\alpha) = 0$. Note that $\frac{-1}{D}$ is a square in $\mathbb{F}_q^*$ and let $D_1 \in \mathbb{F}_q^*$ such that $D_1^2 = \frac{-1}{D}$. As $f_{i_0}(\alpha) = 0$ we obtain that $\alpha = D_1^2 \alpha_{i_0}^2$. Using Lemma 3.3 we obtain that there exists $1 \le i \le m$ such that $i \neq i_0$ and $(\alpha_{i_0} - \alpha_i)$ is a nonsquare in $\mathbb{F}_{q_0}^*$. As s is odd, we also obtain that there exists $1 \le i \le m$ such that $i \neq i_0$ and $(\alpha_{i_0} - \alpha_i)$ is a nonsquare in $\mathbb{F}_q^*$. Note that $f_i(\alpha) = D_1^2 (\alpha_{i_0} - \alpha_i)$. These arguments imply that there is no $\mathbb{F}_q$-rational point of χ_2 over P_α. This completes the proof of item (iv). □

The following theorem is related to Property PP3 of Theorem 3.2 (see the last item in the following theorem).

Theorem 3.5. *We keep the notation and assumptions of Theorem 3.3. In particular $q_0 > 3$, $s \ge 3$ is an odd integer and $q = q_0^s$. Furthermore we assume that $q \equiv 3 \mod 8$.*

Let χ_3 be the fibre product of the projective lines over $\mathbb{F}_q$ given by

$$\chi_3 : \begin{cases} y_1^2 &= x^2 - 2\alpha_1, \\ y_2^2 &= x^2 - 2\alpha_2, \\ &\vdots \\ y_m^2 &= x^2 - 2\alpha_m. \end{cases}$$

Let P_∞ be the pole of x in $\mathbb{F}_q(x)$. For $\alpha \in \mathbb{F}_q$, let P_α be the zero of $(x-\alpha)$ in $\mathbb{F}_q(x)$. We have the following:

(i). *The genus g of χ_3 is*

$$g = 1 + 2^{m-1}(m-2).$$

(ii). *There are exactly 2^m $\mathbb{F}_q$-rational points of χ_3 over P_∞.*

(iii). *There are exactly 2^m $\mathbb{F}_q$-rational points of χ_3 over P_0.*

(iv). *If $\alpha \in \mathbb{F}_q^*$, then there are exactly 2^m $\mathbb{F}_q$-rational points of χ_3 over P_α if and only if*

$$f_i(\alpha) \text{ is a nonzero square in } \mathbb{F}_q \tag{99}$$

for each $1 \le i \le m$, where $f_i(x) = x^2 - 2\alpha_i \in \mathbb{F}_q[x]$.

If (99) does not hold, then there is no $\mathbb{F}_q$-rational point of χ_3 over P_α.

Proof. The arguments in the proofs of items (i) and (ii) of Theorem 3.3 imply similar proofs for the items (i) and (ii) of the current theorem.

Let $1 \le i \le m$. Note that the evaluation of the polynomial $x^2 - 2\alpha_i$ at the place P_0 is $-2\alpha_i$ for $1 \le i \le m$. As $q \equiv 3 \mod 8$, we observe that -1 is a nonsquare in $\mathbb{F}_q^*$. Using Lemma 3.2 we obtain that 2 is a nonsquare in $\mathbb{F}_q^*$. Hence we have that -2 is a square in $\mathbb{F}_q^*$. This implies that $-2\alpha_i$ is also a square in $\mathbb{F}_q^*$. These arguments complete the proof of item (iii).

In the rest of this proof we consider item (iv). Let $\alpha \in \mathbb{F}_q^*$. Assume first that $f_i(\alpha) \neq 0$ for each $1 \le i \le m$. Under this assumption, the corresponding arguments in the proof of item (iv) of Theorem 3.3 imply a similar proof for the item (iv) of the current theorem.

We claim that there is no $1 \le i \le m$ such that $f_i(\alpha) = 0$. Indeed, otherwise there exists $1 \le i \le m$ such that $\alpha^2 = 2\alpha_i$. As 2 is not a square in $\mathbb{F}_q^*$ and α_i is a square in $\mathbb{F}_q^*$, we get a contradiction. This completes the proof. □

Combining Theorems 3.2, 3.3, 3.4, 3.5 and using Hasse-Weil inequality (see, for example, [19, Theorem 5.2.1]) we prove that the covering radius of generalized Zetterberg code $\mathcal{C}_s(q_0)$ over $\mathbb{F}_{q_0}$ of length $q_0^s + 1$ is 3 if $s \ge 3$ is a sufficiently large odd integer. We also give an explicit lower bound in the following theorem for the sufficiency statement.

Theorem 3.6. *Let $\mathbb{F}_{q_0}$ be a finite field of odd characteristic. Assume that $q_0 > 3$ and $q_0 \not\equiv 7 \mod 8$. Put $m = \frac{q_0-1}{2}$.*

Let s_1^* be the smallest odd integer with $s_1^* \geq 3$ such that

$$q_0^{s_1^*} + 1 - 2\left(1 + 2^{m-1}(m-2)\right) q_0^{s_1^*/2} > 2^m.$$

If s is an odd integer with $s \geq s_1^*$, then the generalized Zetterberg code $\mathcal{C}_s(q_0)$ over $\mathbb{F}_{q_0}$ of length $q_0^s + 1$ has covering radius 3.

Proof. Let $\{\alpha_1, \ldots \alpha_m\}$ be an enumerated set of nonzero squares on $\mathbb{F}_{q_0}$. Assume that $q_0 \not\equiv 7 \mod 8$. Let $s \geq 3$ be an odd integer with $s \geq s_1^*$. Put $q = q_0^s$. Note that $q \not\equiv 7 \mod 8$.

Let $w \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ with $w + w^q = 1$. Put $D = \frac{1}{4} - w^{q+1}$. Note that $D \in \mathbb{F}_q^*$ is a nonsquare. Let N denote the number of $a \in \mathbb{F}_q^*$ such that

$$a^2 + \frac{\alpha_i}{D} \text{ is a nonzero square in } \mathbb{F}_q \text{ for each } 1 \leq i \leq m.$$

Let χ_2 be the algebraic curve in Theorem 3.4. Let $N(\chi_2)$ denote the number of $\mathbb{F}_q$-rational points of χ_2. Using Theorem 3.4 we obtain that

$$N(\chi_2) = 2^m + 0 + 0 + 2^m N.$$

This implies that if

$$N(\chi_2) > 2^m, \tag{100}$$

we have that $N > 0$. Using also Theorem 3.2 we conclude that if (100) holds, then Property PP2 holds and hence the covering radius of $\mathcal{C}_s(q_0)$ is 3.

Using Theorem 3.4, item (i) and Hasse-Weil inequality we obtain that

$$N(\chi_2) \geq q_0^s + 1 - 2gq_0^{s/2} = q_0^s + 1 - 2\left(1 + 2^{m-1}(m-2)\right) q^{s_0/2}. \tag{101}$$

Combining (100) and (101) we conclude that the covering radius of $\mathcal{C}_s(q_0)$ is 3 if

$$q_0^s + 1 - 2\left(1 + 2^{m-1}(m-2)\right) q^{s_0/2} > 2^m. \tag{102}$$

Note that (102) holds if $s \geq s_1^*$. This completes the proof. $\square$

Theorem 3.6 implies the following definitions naturally.

Definition 3.7. Let $\mathbb{F}_{q_0}$ be a finite field of odd characteristic. Assume that $q_0 > 3$ and $q_0 \not\equiv 7 \mod 8$. Let $N_1(q_0)$ be the smallest odd integer with $s_1 \geq 3$ such that if s is an odd integer satisfying $s \geq s_1$, then the generalized Zetterberg code over $\mathbb{F}_{q_0}$ of length $q_0^s + 1$ has covering radius 3.

Let $\mathbb{F}_{q_0}$ be a finite field of odd characteristic with $q_0 > 3$. Assume that $q_0 \not\equiv 7 \mod 8$. Let $s_1^* \geq 3$ be the odd integer defined in Theorem 3.6. Using Theorem 3.6 and Definition 3.7 we immediately obtain that

$$N_1(q_0) \leq s_1^*. \tag{103}$$

Using Theorem 3.6 and (103), we obtain the following numerical values on certain upper bounds on $N_1(q_0)$ easily for small q_0:

$$\begin{aligned} q_0 = 5: &\quad N_1(5) \leq 3; \\ q_0 = 9: &\quad N_1(9) \leq 5; \\ q_0 = 11: &\quad N_1(11) \leq 5; \\ q_0 = 13: &\quad N_1(13) \leq 5; \\ q_0 = 17: &\quad N_1(17) \leq 7; \\ q_0 = 19: &\quad N_1(19) \leq 7; \\ q_0 = 25: &\quad N_1(25) \leq 7. \end{aligned} \tag{104}$$

Note that (104) implies that $N_1(5) = 3$.

The following definition is a refinement of Definition 3.7.

Definition 3.8. Let $\mathbb{F}_{q_0}$ be a finite field of odd characteristic. Assume that $q_0 \not\equiv 7 \mod 8$. For an odd integer $s \geq 3$, let $\mathcal{C}_s(q_0)$ be the generalized Zetterberg code of length $q_0^s + 1$ over $\mathbb{F}_{q_0}$.

Let $I(q_0)$ be the set of odd integers given by

$$I(q_0) = \{s \geq 3 : s \text{ is odd and } \mathcal{C}_s(q_0) \text{ has covering radius } 3\}.$$

It follows immediately from Definitions 3.7 and 3.8 that we have the following:

$$\{s : s \geq N_1(q_0) \text{ and } s \text{ is odd}\} \subseteq I(q_0).$$

The following proposition is also useful in determining $I(q_0)$.

Proposition 3.1. *Let $\mathbb{F}_{q_0}$ be a finite field of odd characteristic with $q_0 > 3$. Assume that $q_0 \not\equiv 7 \mod 8$. If $s \in I(q_0)$ and $t \geq 1$ is an odd integer, then $st \in I(q_0)$.*

Proof. Let $s \geq 3$ and $t \geq 1$ be odd integers. Put $q_1 = q_0^s$ and $q_2 = q_0^{st}$. Note that $q_1 \not\equiv 7 \mod 8$, $q_2 \not\equiv 7 \mod 8$ and $\mathbb{F}_{q_2}$ is a finite extension of $\mathbb{F}_{q_1}$.

Assume further that $q_1 \not\equiv 3 \mod 8$. As $s \in I(q_0)$, using Theorem 3.2, at least one of the properties PP1 and PP2 holds. Assume that Property PP1 holds and let $a \in \mathbb{F}_{q_1}^*$ satisfying Property PP1. As $a \in \mathbb{F}_{q_2}^*$ as well, applying Theorem 3.2 for q_2 using a we obtain that Property PP1 holds and hence $st \in I(q_0)$. The same argument holds if Property PP2 holds. This completes the proof under the assumption that $q_1 \not\equiv 3 \mod 8$.

Next we assume that $q_1 \equiv 3 \mod 8$. As $s \in I(q_0)$, using Theorem 3.2, at least one of the properties PP1, PP2 and PP3 holds. If Property PP1 or Property PP2 holds, then the same argument in the proceeding paragraph implies that $st \in I(q_0)$. Assume that Property PP3 holds. Note that as t is odd, then $q_2 \equiv 3 \mod 8$ as well. Hence if $a \in \mathbb{F}_{q_1}^*$ satisfies Property PP3 for $\mathbb{F}_{q_1}$, it also satisfies Property PP3 for $\mathbb{F}_{q_2}$ as $\mathbb{F}_{q_1} \subseteq \mathbb{F}_{q_2}$. This completes the proof. $\square$

In the following examples we exactly determine $I(q_0)$ for any finite field $\mathbb{F}_{q_0}$ of odd characteristic with $q_0 \leq 25$ and $q_0 \not\equiv 7 \mod 8$, except the case of $\mathbb{F}_{25}$ that we determine $I(25)$ only upto two candidates.

Example 3.1. *Let $q_0 = 3$. Using Corollary 3.1 we obtain that*

$$I(3) = \{s : s \geq 3 \text{ is an odd integer}\}.$$

Example 3.2. *Let $q_0 = 5$. Using (104) we obtain that*

$$I(5) = \{s : s \geq 3 \text{ is an odd integer}\}.$$

In the following three examples we also use Theorem 3.2.

Example 3.3. *Let $q_0 = 9$. Using (104) we obtain that*

$$I(9) \supseteq \{s : s \geq 5 \text{ is an odd integer}\}.$$

It remains to consider whether $3 \in I(9)$ or not. Using Theorem 3.2 and Magma, we conclude that $3 \in I(9)$. These imply that

$$I(9) = \{s : s \geq 3 \text{ is an odd integer}\}.$$

Example 3.4. *Let $q_0 = 11$. Using (104) we obtain that*

$$I(11) \supseteq \{s : s \geq 5 \text{ is an odd integer}\}.$$

It remains to consider whether $3 \in I(11)$ or not. Using Theorem 3.2 and Magma, we conclude that $3 \in I(11)$. These imply that

$$I(11) = \{s : s \geq 3 \text{ is an odd integer}\}.$$

Example 3.5. *Let $q_0 = 13$. Using (104) we obtain that*

$$I(13) \supseteq \{s : s \geq 5 \text{ is an odd integer}\}.$$

It remains to consider whether $3 \in I(13)$ or not. Using Theorem 3.2 and Magma, we conclude that $3 \in I(13)$. These imply that

$$I(13) = \{s : s \geq 3 \text{ is an odd integer}\}.$$

The next example gives the smallest value of q_0 such that there exists a finite field $\mathbb{F}_{q_0}$ of odd characteristic with $q_0 \not\equiv 7 \mod 8$ such that $I(q_0) \neq \{s :$ $s \geq 3$ is an odd integer$\}$.

Example 3.6. *Let $q_0 = 17$. Using (104) we obtain that*

$$I(17) \supseteq \{s : s \geq 7 \text{ is an odd integer}\}.$$

It remains to consider $\{3, 5\} \cap I(17)$. Using Theorem 3.2 and Magma, it is interesting that we obtain $5 \in I(17)$ and $3 \notin I(17)$. These imply that

$$I(17) = \{s : s \geq 5 \text{ is an odd integer}\}.$$

The next example gives the second smallest value of q_0 such that there exists a finite field $\mathbb{F}_{q_0}$ of odd characteristic with $q_0 \not\equiv 7 \mod 8$ such that $I(q_0) \neq \{s : s \geq 3$ is an odd integer$\}$.

Example 3.7. *Let $q_0 = 19$. Using (104) we obtain that*

$$I(19) \supseteq \{s : s \geq 7 \text{ is an odd integer}\}.$$

It remains to consider whether $\{3,5\} \cap I(19)$. Using Theorem 3.2 and Magma, it is interesting that we obtain $5 \in I(19)$ and $3 \notin I(19)$. We note that the computation for $5 \in I(19)$ takes too long. These imply that

$$I(19) = \{s : s \geq 5 \text{ is an odd integer}\}.$$

The next example gives the third smallest value of q_0 such that there exists a finite field $\mathbb{F}_{q_0}$ of odd characteristic with $q_0 \not\equiv 7 \mod 8$ such that $I(q_0) \neq \{s : s \geq 3$ is an odd integer$\}$.

Example 3.8. *Let $q_0 = 25$. Using (104) we obtain that*

$$I(25) \supseteq \{s : s \geq 7 \text{ is an odd integer}\}.$$

It remains to consider $\{3,5\} \cap I(19)$. Using Theorem 3.2 and Magma, it is interesting that we obtain $3 \notin I(25)$. We note that the computation for $5 \in I(19)$ takes too long and we had to stop waiting after some time so that we do not know if $5 \in I(25)$ or not. These imply that $I(25)$ is either

$$\{s : s \geq 5 \text{ is an odd integer}\},$$

or

$$\{s : s \geq 7 \text{ is an odd integer}\}.$$

4. Covering Radius of Half and twisted Half Generalized Zettenberg Codes in Odd Characteristic

In this section we introduce half and twisted half generalized Zettenberg codes in odd characteristic. We also show that their covering radii are the same as the covering radius of the (full) generalized Zettenberg code, that we consider in Sections 2 and 3. Namely we prove Theorems 4.3 and 4.4 below. We also explain a small issue in [11] in Remark 4.2 below.

Let $\mathbb{F}_{q_0}$ be an arbitrary finite field of odd characteristic. Let $s \geq 1$ be an integer. Put $q = q_0^s$.

Definition 4.1. Under notation as above, assume that $q \equiv 1 \mod 4$. Let H be the subgroup of $\mathbb{F}_{q^2}^*$ with $|H| = q+1$. Let H_2 be the subgroup of $\mathbb{F}_{q^2}^*$ with $|H_2| = \frac{q+1}{2}$. Note that $-1 \in H \setminus H_2$ and

$$H = H_2 \sqcup -H_2.$$

Here $-H_2 = \{-x : x \in H_2\}$. Let $h_2 \in H_2$ be a generator of H_2. Put $n = \frac{q+1}{2}$. We define the *half generalized Zettenberg code* $\mathcal{C}_s^{(2)}(q_0)$ *of length* n *over* $\mathbb{F}_{q_0}$ as the linear code over $\mathbb{F}_{q_0}$ with the parity check matrix

$$\begin{bmatrix} 1 & h_2 & h_2^2 & \cdots & h_2^{n-1} \end{bmatrix}.$$

Namely $\mathcal{C}_s^{(2)}(q_0)$ consists of $[a_0, a_1, \ldots, a_{n-1}] \in \mathbb{F}_{q_0}^n$ such that

$$\begin{bmatrix} 1 & h_2 & h_2^2 & \cdots & h_2^{n-1} \end{bmatrix} \cdot \begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{bmatrix} = 0.$$

Definition 4.2. Under notation as above, assume that $q \equiv 3 \mod 4$. Let H be the subgroup of $\mathbb{F}_{q^2}^*$ with $|H| = q+1$. Let H_4 be the subgroup of $\mathbb{F}_{q^2}^*$ with $|H_4| = \frac{q+1}{4}$. Let $\theta \in \mathbb{F}_{q^2}$ be a primitive 4-th root of 1. Note that

$$H = (H_4 \sqcup \theta H_4) \sqcup -(H_4 \sqcup \theta H_4)$$

and $\theta \notin \mathbb{F}_{q_0}$. Here $-(H_4 \sqcup \theta H_4) = \{-x : x \in (H_4 \sqcup \theta H_4)\}$. Let $h_4 \in H_4$ be a generator of H_4. Put $n = \frac{q+1}{2}$. Note that $H_4 \sqcup \theta H_4$ is a subset of H with $|H_4 \sqcup \theta H_4| = n$ and $H_4 \sqcup \theta H_4$ is not the subgroup of H with n elements, for example $-1 \notin (H_4 \sqcup \theta H_4)$. We define the *twisted half generalized Zettenberg code* $\mathcal{C}_s^{(2,\mathrm{t})}(q_0)$ *of length* n *over* $\mathbb{F}_{q_0}$ as the linear code over $\mathbb{F}_{q_0}$ with the parity check matrix

$$\begin{bmatrix} 1 & h_4 & h_4^2 & \cdots & h_4^{n/2-1}\theta & \theta h_4 & \theta h_4^2 & \cdots & \theta h_4^{n/2-1} \end{bmatrix}.$$

Namely $\mathcal{C}_s^{(2,\mathrm{t})}(q_0)$ consists of $[a_0, a_1, \ldots, a_{n-1}] \in \mathbb{F}_{q_0}^n$ such that

$$\begin{bmatrix} 1 & h_4 & h_4^2 & \cdots & h_4^{n/2-1}\theta & \theta h_4 & \theta h_4^2 & \cdots & \theta h_4^{n/2-1} \end{bmatrix} \cdot \begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{bmatrix} = 0.$$

In particular we define

- an half generalized Zettenberg code if $q \equiv 1 \mod 4$, and
- a twisted half generalized Zettenberg code if $q \equiv 3 \mod 4$.

Remark 4.1. *If $q_0 = 3$ and $s \geq 2$ is an even integer, then the half Zettenberg code over $\mathbb{F}_3$ of Definition 4.1 corresponds to one of the two classes of ternary quasi-perfect codes considered in* [8].

If $q_0 = 3$ and $s \geq 3$ is odd integer, then the twisted half Zettenberg code over $\mathbb{F}_3$ of Definition 4.2 corresponds to the remaining class of the two classes of ternary quasi-perfect codes considered in [11].

We are ready to state the first theorem of this section. The following two theorems have simple proofs. Nevertheless we think that the results are interesting and useful. Therefore we prefer to state these results as theorems.

Theorem 4.3. *Let $\mathbb{F}_{q_0}$ be an arbitrary finite field of odd characteristic. Let $s \geq 1$ be an integer. Put $q = q_0^s$. Assume that $q \equiv 1 \mod 4$. Let $\mathcal{C}_s(q_0)$ be the generalized Zettenberg code of length $q+1$ over $\mathbb{F}_{q_0}$. Let $\mathcal{C}_s^{(2)}(q_0)$ be the half generalized Zettenberg code of length $\frac{q+1}{2}$ over $\mathbb{F}_{q_0}$ defined in Definition 4.1. Then the covering radius of $\mathcal{C}_s(q_0)$ is equal to the covering radius of $\mathcal{C}_s^{(2)}(q_0)$.*

Proof. It follows from the definition that the covering radius of $\mathcal{C}_s(q_0)$ is smaller or equal to the covering radius of $\mathcal{C}_s^{(2)}(q_0)$. Indeed, let $\alpha \in \mathbb{F}_{q^2}$ be given. Let $I_2^{(\alpha)} \subseteq H_2$ be a subset and $\psi^{(\alpha)} : I_2 \to \mathbb{F}_{q_0}^*$ be a mapping such that

$$\sum_{a \in I_2^{(\alpha)}} \psi^{(\alpha)}(a)a = \alpha.$$

Here we use the equivalent characterization for the definition of covering radius of linear codes (see (2) for an analogous characterization). As

$$H = H_2 \sqcup -H_2, \tag{105}$$

it is clear that $I_2^{(\alpha)} \subseteq H$ as well. Moreover these arguments hold for any $\alpha \in \mathbb{F}_{q^2}$. Hence we conclude that the covering radius of $\mathcal{C}_s(q_0)$ is smaller or equal to the covering radius of $\mathcal{C}_s^{(2)}(q_0)$.

Conversely, let $\alpha \in \mathbb{F}_{q^2}$ be given. Let $I^{(\alpha)} \subseteq H$ be a subset and $\psi^{(\alpha)} : I \to \mathbb{F}_{q_0}^*$ be a mapping such that

$$\sum_{a \in I^{(\alpha)}} \psi^{(\alpha)}(a)a = \alpha. \tag{106}$$

Here we use the equivalent characterization for the covering radius of $\mathcal{C}_s(q_0)$, that we use for $\mathcal{C}_s^{(2)}(q_0)$ above. Moreover, as we consider the covering radius, we assume that $|I^{(\alpha)}|$ is minimal among all such subsets. Let $I_1^{(\alpha)} = I^{(\alpha)} \cap H_2$ and $I_2^{(\alpha)} = I^{(\alpha)} \cap (-H_2)$. Using (105) and the minimality of $|I^{(\alpha)}|$, we obtain that

$$I_1^{(\alpha)} \cap -I_2^{(\alpha)} = \emptyset. \tag{107}$$

Let $J^{(\alpha)} \subseteq H_2$ be the subset defined as $J^{(\alpha)} = I_1^{(\alpha)} \cup -I_2^{(\alpha)}$. Note that

$$|J^{(\alpha)}| = |I^{(\alpha)}|. \tag{108}$$

Let $\varphi^{(\alpha)} : J^{(\alpha)} \to \mathbb{F}_{q_0}^*$ be the map defined as

$$\varphi^{(\alpha)}(x) = \begin{cases} \psi^{(\alpha)}(x) & \text{if } x \in I_1^{(\alpha)}, \\ -\psi^{(\alpha)}(-x) & \text{if } -x \in I_2^{(\alpha)}. \end{cases} \tag{109}$$

Combining (106), (107), (108) and (109) we obtain that

$$\sum_{a \in J^{(\alpha)}} \varphi^{(\alpha)}(a)a = \alpha. \tag{110}$$

Moreover these arguments hold for any $\alpha \in \mathbb{F}_{q^2}$. Hence we conclude that the covering radius of $\mathcal{C}_s^{(2)}(q_0)$ is smaller or equal to the covering radius of $\mathcal{C}_s(q_0)$. This completes the proof. □

The next theorem is an analog of Theorem 4.3 for twisted half generalized Zettenberg codes.

Theorem 4.4. *Let $\mathbb{F}_{q_0}$ be an arbitrary finite field of odd characteristic. Let $s \geq 1$ be an integer. Put $q = q_0^s$. Assume that $q \equiv 3 \mod 4$. Let $\mathcal{C}_s(q_0)$ be the generalized Zettenberg code of length $q+1$ over $\mathbb{F}_{q_0}$. Let $\mathcal{C}_s^{(2,\mathrm{t})}(q_0)$ be the twisted half generalized Zettenberg code of length $\frac{q+1}{2}$ over $\mathbb{F}_{q_0}$ defined in Definition 4.2. Then the covering radius of $\mathcal{C}_s(q_0)$ is equal to the covering radius of $\mathcal{C}_s^{(2,\mathrm{t})}(q_0)$.*

Proof. We use similar methods as in the proof of Theorem 4.3. Note that the main technique in the proof of Theorem 4.3 uses the fact that

$$H = H_2 \sqcup -H_2. \tag{111}$$

In this proof we have

$$H = (H_4 \sqcup \theta H_4) \sqcup -(H_4 \sqcup \theta H_4) \tag{112}$$

instead of (111). Hence using the same methods and applying them to (112) instead of (111). □

Remark 4.2. *If $q_0 = 3$ and $s \geq 3$ is an odd integer then for $q = q_0^s$ we have that $q \equiv 3 \mod 4$. Using Theorems 4.4 and 2.2, we obtain that it is necessary to show that Properties P3 and P4 in Theorem 2.2 hold, together with Properties P1 and P2. Recall that this case corresponds to one of the ternary quasi-perfect code classes considered in* [11] *(see also Remark 4.1 above). In the proof for the covering radius in this case in* [11]*, the proofs of the facts that Properties P1 and P2 hold exist, however the proof of the facts that Properties P3 and P4 hold is missing. In this paper we fix this issue by extending the methods of* [11]*. Note that we also extend these results to arbitrary odd characteristic $\mathbb{F}_{q_0}$ from $\mathbb{F}_3$, provided that $q_0^s \not\equiv 7 \mod 8$.*

5. Conclusion

Throughout this paper we restrict ourselves of $\mathbb{F}_{q_0}$ of odd characteristic. Our methods do not directly generalize to even characteristic. We plan to consider the covering radius of Zetterberg type codes in even characteristic in a future work.

We have treated each finite field $\mathbb{F}_{q_0}$ of odd characteristic if $q_0 \not\equiv 7 \mod 8$. Our methods would be extended rather naturally to cover each finite field $\mathbb{F}_{q_0}$ of odd characteristic if $q_0 \not\equiv 15 \mod 16$. However it would be interesting to develop a new method which covers each finite field $\mathbb{F}_{q_0}$ of odd characteristic without any restriction of the form $q_0 \not\equiv (2^t - 1) \mod 2^t$, where $t \geq 4$ is an integer.

It would be interesting to extend the explicit examples of Section 3 for larger values of q_0 and give an explanation for the unexpected behaviour of the sets $I(q_0)$ for small odd values of s for some q_0.

Acknowledgement

This research is supported by the National Natural Science Foundation of China (Grants no. 12071001).

6. Appendix

In this appendix we give a proof of the following lemma, which is used in Section 1.

Lemma 6.1. *Let $\mathbb{F}_{q_0}$ be a finite field and $s \geq 1$ be an integer. Let $\mathcal{C}_s(q_0)$ be the generalized Zetterberg code of length $q_0^s + 1$ over $\mathbb{F}_{q_0}$. Then the dimension of $\mathcal{C}_s(q_0)$ is $q_0^s + 1 - 2s$.*

Proof. Let $H \subseteq \mathbb{F}_{q_0^{2s}}^*$ be the subgroup with $|H| = q_0^s + 1$. Let P be the parity check matrix given in (1). It is enough to prove that the column rank of P is $2s$. Hence we need to show that $\mathrm{Span}_{\mathbb{F}_{q_0}}\{h : h \in H\} = \mathbb{F}_{q_0^{2s}}$. Let $W = \mathrm{Span}_{\mathbb{F}_{q_0}}\{h : h \in H\}$ and $t = \dim_{\mathbb{F}_{q_0}} W$. As $H \subseteq W$, it is clear that $t \geq s + 1$. Assume the contrary that $t < 2s$. Put $u = t - s$. These arguments and the assumption imply that

$$1 \leq u \leq s - 1. \tag{113}$$

Let

$$A(T) = \prod_{w \in W} (T - w).$$

It is well known that $A(T)$ is a monic additive polynomial of degree p^{s+u} with coefficients from $\mathbb{F}_{q_0}$. Hence we obtain $A_0, A_1, \ldots, A_{s+u-1} \in \mathbb{F}_{q_0}$ such that

$$h^{p^{s+u}} + A_{s+u-1} h^{p^{s+u-1}} + \cdots + A_1 h^p + A_0 h = 0$$

for each $h \in H$. As $h^{p^s} = 1/h$ for each $h \in H$, we also get that

$$\left(\frac{1}{h}\right)^{p^u} + A_{s+t-1}\left(\frac{1}{h}\right)^{p^{u-1}} + \cdots + A_s\frac{1}{h}$$

$$+A_{s-1}h^{p^{s-1}} + \cdots + A_1h^p + A_0h = 0.$$

This is equivalent to

$$A_{s-1}h^{p^{s-1}+p^u} + A_{s-2}h^{p^{s-2}+p^u} + \cdots + A_1h^{p+p^u} + A_0h^{1+p^u}$$

$$+1 + A_{s+u-1}h^{p^u-p^{u-1}} + \cdots + A_sh^{p^u-1} = 0.$$

In particular there exists a nonzero polynomial $B(T) \in \mathbb{F}_{q_0}[T]$ such that

$$\deg B \le p^{s-1} + p^u \text{ and } B(h) = 0 \text{ for each } h \in H. \tag{114}$$

Using (113) and (114) we obtain a contradiction as

$$\deg B \le p^{s-1} + p^u \le p^{s-1} + p^{s-1} < p^s + 1 = |H|.$$

This completes the proof. □

References

[1] A. Ashikhmin and A. Barg, *Bounds on the covering radius of linear codes*, Des. Codes Cryptogr., vol. 27, no. 3, pp. 261-269, 2002.

[2] R. A. Brualdi, S. Litsyn, and V. S. Pless, *Covering radius*, in Handbook of Coding Theory. Amsterdam, The Netherlands: North-Holland, 1998, pp. 755826.

[3] W. Bosma, J. Cannon, and C. Playoust: The Magma algebra system. I. The user language, J. Symbolic Comput. **24** (1997), 235–265.

[4] G. Cohen, I. Honkala, S. Litsyn, and A. Lobstein, *Covering codes*, in North-Holland Mathematical Library, vol. 54. Amsterdam, The Netherlands: North-Holland Publishing Co., 1997.

[5] G. Cohen, M. Karpovsky, H. Mattson, and J. Schatz, *Covering radius- Survey and recent results*, IEEE Trans. Inf. Theory, vol. IT-31, no. 3, pp. 328-343, May 1985. in North-Holland Mathematical Library, vol. 54. Amsterdam, The Netherlands: North-Holland Publishing Co., 1997.

[6] G. D. Cohen, S. N. Litsyn, A. C. Lobstein, and H. F. Mattson, Jr., *Covering radius 19851994*, Applicable Algebra Eng., Commun. Comput., vol. 8, no. 3, pp. 173239, Feb. 1997.

[7] P. Delsarte, *Four fundamental parameters of a code and their combinatorial significance*, Inf. Control, vol. 23, no. 5, pp. 407438, Dec. 1973.

[8] S.M. Dodunekov, *The optimal double error correcting codes of Zetterberg and Dumer-Zinoviev are quasiperfect*, Bull. Bulgarian Acad. Sc, 38 (1985) 1121–1123.

[9] R. Dougherty and H. Janwa, *Covering radius computations for binary cyclic codes*, Math. Comp., vol. 57, no. 195, pp. 415434, 1991.

[10] D. Downie and N. Sloane, *The covering radius of cyclic codes of length up to 31*, IEEE Trans. Inf. Theory, vol. IT-31, no. 3, pp. 446447, May 1985.

[11] I. Gashkov and V. Sidel'nikov, *Linear ternary quasiperfect codes that correct double errors*, Problemy Peredachi Inf., vol. 22, no. 4, pp. 4348, 1986.

[12] K. Ireland and M. Rosen, *A classical introduction to modern number theory*, Second Edition. Springer-Verlag, New York, 1990.

[13] T. Helleseth, *On the covering radius of cyclic linear codes and arithmetic codes*, Discrete Appl. Math., vol. 11, no. 2, pp. 157173, Jun. 1985.

[14] R. Lidl, H. Niederreiter, *Finite fields*. Cambridge University Press, (2003).

[15] O. Moreno and F. N. Castro, *Divisibility properties for covering radius of certain cyclic codes*, IEEE Trans. Inf. Theory, vol. 49, no. 12, pp. 32993303, Dec. 2003.

[16] F. Özbudak and H. Stichtenoth, *Curves with many points and configurations of hyperplanes over finite fields*, Finite Fields Appl., 5 (1999), 436449.

[17] M. Shi, T. Helleseth, F. Özbudak and P. Solé, *Covering radius of Melas codes*, IEEE Trans. Inf. Theory, vol. 68, no. 7, pp. 4354–4364, 2022.

[18] P. Solé, *Packing radius, covering radius, and dual distance*, IEEE Trans. Inf. Theory, vol. 41, no. 1, pp. 268272, Jan. 1995.

[19] H. Stichtenoth, *Algebraic Function Fields and Codes*, vol. 254. New York, NY, USA: Springer, 2009.

[20] A. Tietaivainen, *On the covering radius of long binary BCH codes*, Discrete Appl. Math., vol. 16, no. 1, pp. 7577, Jan. 1987.

[21] L.H. Zetterberg, *Cyclic codes from irreducible polynomials for correction of multiple errors* , IRE Trans. Inf. Theory, vol. 8, no. 1, pp. 13–20, 1962.