On Deep Holes of Elliptic Curve Codes

Jun Zhang and Daqing Wan

***Abstract*— We give a method to construct deep holes for elliptic curve codes. For long elliptic curve codes, we conjecture that our construction is complete in the sense that it gives all deep holes. Some evidence and heuristics on the completeness are provided by means of connections with problems and results in finite geometry.**

***Index Terms*— Algebraic geometry code, elliptic curve, covering radius, deep hole, finite geometry.**

I. Introduction

THE classification of deep holes in a linear code is a fundamental and difficult problem in coding theory. Deciding if a given received word is a deep hole is already NP-hard, even for short Reed-Solomon codes. For long Reed-Solomon codes, this problem has been studied extensively, and it is better understood if one assumes the MDS conjecture or the rational normal curve conjecture in finite geometry. Algebraically, Reed-Solomon codes are just algebraic geometry codes of genus zero. From this point of view, it is natural to study the deep hole problem for algebraic geometry codes of higher genus g. The difficulty naturally increases as the genus g grows. In fact, the minimum distance is already unknown and NP-hard to determine when genus $g = 1$. In this paper, we give a first study of the deep hole problem for elliptic curve codes, i.e., the genus $g = 1$ case. Our main result is an explicit construction of a class of deep holes for long elliptic curve codes. We conjecture that our construction already gives the complete set of all deep holes for long elliptic curve codes. In the final section, we provide some heuristics and evidence about this completeness conjecture by means of its connection with problems and results in finite geometry.

Let $\mathbb{F}_q^n$ be the n-dimensional vector space over the finite field $\mathbb{F}_q$ of q elements with characteristic p. For any vector (also, called *word*) $x = (x_1, x_2, \cdots, x_n) \in \mathbb{F}_q^n$, the *Hamming weight* $\mathrm{Wt}(x)$ of x is defined to be the number of its non-zero coordinates, i.e., $\mathrm{Wt}(x) = |\{i \,|\, 1 \leqslant i \leqslant n,\ x_i \neq 0\}|$. For integers $1 \leq k \leq n$, a *linear* $[n, k]$ *code* C is a k-dimensional linear subspace of $\mathbb{F}_q^n$. The *minimum distance* $d(C)$ of C is the minimum Hamming weight among all non-zero vectors in C, i.e., $d(C) = \min\{\mathrm{Wt}(c) \,|\, c \in C \setminus \{0\}\}$. A linear $[n, k]$ code $C \subseteq \mathbb{F}_q^n$ is called an $[n, k, d]$ linear code if C has minimum distance d. For error correction purposes, an $[n, k]$ code C is good if its minimum distance d is large. Ideally, for a given $[n, k]$-code C, one would like its minimum distance d to be as large as possible. A well-known trade-off between the parameters of a linear $[n, k, d]$ code is the Singleton bound which states that

$$d \leqslant n - k + 1.$$

An $[n, k, d]$ code is called a *maximum distance separable* (MDS) code if $d = n - k + 1$. The MDS codes of dimension 1 and their duals of dimension $n - 1$ are called trivial MDS codes. The trivial MDS codes can have arbitrary length n. For length $n \leq q$, an important class of non-trivial MDS codes are Reed-Solomon codes with evaluation set D chosen to be any n rational points on the affine line $\mathbb{A}^1(\mathbb{F}_q)$. For $n = q + 1$, one has the projective Reed-Solomon code which is also an MDS code. For length $n \geq q + 2$, one does not expect any non-trivial MDS code to exist for odd q. This is the main part of the long standing MDS conjecture proposed by Segre [29].

Conjecture 1.1 (MDS conjecture): The length n of non-trivial MDS codes over the finite field $\mathbb{F}_q$ cannot exceed $q + 1$ with two exceptions: for $k \in \{3, q - 1\}$ and even q the length can reach $q + 2$.

This conjecture remains open in general, although a lot of progress has been made [2], [3], [4]. In particular, it is known to be true if q is a prime, see [2] for further information. It is also known to be true for elliptic curve codes, see [32].

Let C be an $[n, k, d]$ linear code over $\mathbb{F}_q$. The *error distance* of any word $u \in \mathbb{F}_q^n$ to C is defined to be

$$d(u, C) = \min\{d(u, v) \,|\, v \in C\},$$

where

$$d(u, v) = |\{i \,|\, u_i \neq v_i,\ 1 \leq i \leq n\}|$$

is the Hamming distance between words u and v. Computing the error distance is essentially equivalent to solving the maximal likelihood decoding problem. Although there are decoding algorithms available for important codes such as Reed-Solomon codes and algebraic geometric codes, these algorithms only work if the error distance $d(u, C)$ is small. If the error distance is large, then decoding becomes a problem of major difficulty. The maximum error distance

$$\rho(C) = \max\{d(u,\, C) \,|\, u \in \mathbb{F}_q^n\}$$

is called the *covering radius* of C.

Manuscript received 24 July 2022; revised 16 February 2023; accepted 5 March 2023. Date of publication 15 March 2023; date of current version 16 June 2023. The work of Jun Zhang was supported in part by the National Natural Science Foundation of China under Grant 11971321 and Grant 12222113 and in part by the National Key Research and Development Program of China under Grant 2018YFA0704703. The work of Daqing Wan was supported in part by NSF under Grant CCF-1900929. *(Corresponding author: Jun Zhang.)*

Jun Zhang is with the School of Mathematical Sciences, Capital Normal University, Beijing 100048, China (e-mail: junz@cnu.edu.cn).

Daqing Wan is with the Department of Mathematics, University of California at Irvine, Irvine, CA 92697 USA (e-mail: dwan@math.uci.edu).

Communicated by C. Xing, Associate Editor for Coding and Decoding.

Digital Object Identifier 10.1109/TIT.2023.3257320

The covering radius is perhaps the next most important quantity of a linear code, after the minimal distance. Covering radii of codes was studied extensively [9], [10], [13], [15], [26], [27]. There are very few families of codes with known covering radius, e.g., Reed-Solomon codes, the first order Reed-Muller code $RM(1,m)$ with even m, etc. For the first order Reed-Muller code $RM(1,m)$ with odd m, to determine the covering radius is already very difficult and, in general, wide open [16]. A recent breakthrough is due to Schmidt [28]. Surprisingly, even for the projective Reed-Solomon code (which is an MDS code), the exact covering radius is unknown, see [35] for the discussion. In general, the covering radius of MDS codes is unknown. The covering radius of a class of short MDS elliptic curve codes was studied in [5].

A word is called a *deep hole* of the code C if its distance from C achieves the covering radius of C. Deciding deep holes of a given code is an extreme instance of decoding. It is much harder than the covering radius problem, even for affine RS codes. The deep hole problem for Reed-Solomon codes was studied in [6], [8], [18], [19], [20], [22], [23], [24], [33], [34], [35], and [36]. For Reed-Solomon codes of length n much smaller than q, deciding if a given word is a deep hole is equivalent to a general subset sum problem, which is NP-hard. For Reed-Solomon codes of length n close to q, the deep hole problem can be solved if one assumes the MDS conjecture or the rational normal curve conjecture in finite geometry, see [35]. In summary, the deep hole problem is expected to be well structured for long Reed-Solomon codes, but it has no structure for short Reed-Solomon codes.

In this paper, we will study deep holes of elliptic curve codes. For the definition and basics of elliptic curve codes, please see Section II. Again, we expect that the deep hole problem is well structured for long elliptic curve codes, but no structure for general short elliptic curve codes. For this reason, we will mostly restrict to long elliptic curve codes in this paper.

In practical applications, for codes of length $\leq q+2$, Reed-Solomon codes already achieve the largest minimum distance. For codes of length $n \geq q+3$, there are no non-trivial MDS codes by the MDS conjecture, and the next best thing would be near-MDS codes, i.e., $[n,k,d]$ codes with $d = n-k$. Long elliptic curve codes are known to be near-MDS and have the best parameters according to the Singleton bound. By the Hasse-Weil theorem, the length n of an elliptic curve code C is bounded above by $n \leq q+2\sqrt{q}+1$. This significantly goes beyond the bound $n \leq q+1$ for Reed-Solom codes. For good codes C with length $n > q+2\sqrt{q}+1$, one could use algebraic geometry codes of genus $g > 1$ with many rational points. In this paper, we only consider the case $g = 1$, which is already sufficiently interesting and difficult.

We always assume, throughout the rest of the paper, the finite field $\mathbb{F}_q$ to have odd characteristic, as to avoid technical complications arising when the characteristic is even. In the statement of the following theorem, we focus on the functional elliptic curve $[n,k]$-code $C_{\mathcal{L}}(D,kO)$, see section II for precise definitions. With appropriate changes, the results hold for a general divisor G. Our main result on minimum distance, covering radius, and deep holes of long elliptic curve codes is the following.

Theorem 1.2: Let E be an elliptic curve over $\mathbb{F}_q$ with a rational point O, and $D \subset E(\mathbb{F}_q) \setminus \{O\}$ be a set of rational points with $n = |D|$. For $2 \leq k \leq n-2$, let $C = C_{\mathcal{L}}(D,kO)$ be the functional elliptic curve $[n,k]$-code. Assume $n \geq q+3$ (the code is long). If any one of the following three conditions holds:

(1) $n \geq q+k$, or
(2) q is a prime, or
(3) $k \leq \sqrt{q}$,

then we have the following results:

(i) The minimum distance $d(C) = n-k$.
(ii) The covering radius $\rho(C) = n-k-1$.
(iii) For any $P \in E(\mathbb{F}_q) \setminus D$, any vector

$$v \in C_{\mathcal{L}}(D,kO+P) \setminus C_{\mathcal{L}}(D,kO)$$

is a deep hole of $C_{\mathcal{L}}(D,kO)$.
(iv) If $k < n-2$, then the deep holes constructed in (iii) are all distinct and thus yield $(|E(\mathbb{F}_q)|-n)(q-1)q^k$ deep holes of $C_{\mathcal{L}}(D,kO)$.

Remark 1.3: Since $n \geq q+3$, the minimum distance $d(C) = n-k$ always holds true for elliptic codes. We need one of conditions (1)-(3) to insure that the covering radius can be shown to be $n-k-1$. These conditions can be removed if one assumes the MDS conjecture or if one simply assumes that the covering radius is $n-k-1$. Without one of these conditions, the covering radius is unknown and thus we cannot prove that the words constructed in (iii) are deep holes.

For the boundary case $k = n-2$, under the conditions in the above theorem, the covering radius $\rho(C) = n-k-1 = 1$. So all vectors in $\mathbb{F}_q^n \setminus C$ are deep holes of C. Hence, the code $C = C_{\mathcal{L}}(D,(n-2)O)$ totally has $(q^2-1)q^{n-2}$ deep holes.

A natural question is if the construction in (iii) is complete, i.e., if there are other deep holes except those in (iii). If it is complete, then there will be exactly $(|E(\mathbb{F}_q)|-n)(q-1)q^k$ deep holes and the elliptic deep hole problem would be solved. For short elliptic curve codes, the construction in (iii) would not be complete. However, we have the following completeness conjecture for sufficiently long elliptic curve codes, namely, when D is the full set $E(\mathbb{F}_q) \setminus \{O\}$ and thus $n = |E(\mathbb{F}_q)| - 1 \geq q+3$. This conjecture is the elliptic code analogue of the Cheng-Murray conjecture [8] for deep holes of Reed-Solomon codes.

Conjecture 1.4: Let E be an elliptic curve over $\mathbb{F}_q$ with $|E(\mathbb{F}_q)| \geq q+4$. Take any rational point $O \in E(\mathbb{F}_q)$ and set $D = E(\mathbb{F}_q) \setminus \{O\}$. Let $2 \leq k \leq |E(\mathbb{F}_q)| - 4$. Then, $C_{\mathcal{L}}(D,(k+1)O) \setminus C_{\mathcal{L}}(D,kO)$ is the set of all deep holes of $C_{\mathcal{L}}(D,kO)$.

It is also an interesting problem to generalize the above results to higher genera.

The rest of this paper is organized as follows. In Section II, we review the definition and basics of algebraic geometry (AG) codes. Regarding Reed-Solomon codes as AG codes constructed from the projective line, we give a new viewpoint

on the deep holes of Reed-Solomon codes to unify the two constructions of the previous works. In Section III, we consider elliptic curve codes. We determine the covering radius, present deep holes and compute the syndromes of the deep holes under our assumption. In Section IV, we discuss the completeness of the deep holes found in Section III. Group actions of certain automorphisms of the elliptic curve are used to generate further deep holes if there is a new one of them. Using a connection with finite geometry we can provide a preliminary approach to the above completeness conjecture.

II. Preliminaries

A. Definitions

In this subsection, We recall the definition and some basics of algebraic geometry codes. First fix some notations valid for the whole paper.

- $\mathbb{F}_q$ *is a finite field of size* q *where* q *is an odd prime power.*
- $X/\mathbb{F}_q$ *is a geometrically irreducible smooth projective curve of genus* g *over the finite field* $\mathbb{F}_q$ *with function field* $\mathbb{F}_q(X)$.
- $X(\mathbb{F}_q)$ *is the set of all* $\mathbb{F}_q$*-rational points on* X.
- $D = \{P_1, P_2, \cdots, P_n\}$ *is a proper subset of rational points* $X(\mathbb{F}_q)$.
- *We also write* $D = P_1 + P_2 + \cdots + P_n$.
- G *is a divisor of degree* k $(2g-2 < k < n)$ *with* $\mathrm{Supp}(G) \cap D = \emptyset$.

Let V be a divisor on X. Denote by $\mathcal{L}(V)$ the $\mathbb{F}_q$-vector space of all rational functions $f \in \mathbb{F}_q(X)$ with the principal divisor $\mathrm{div}(f) \geqslant -V$, together with the zero function. It is well-known that $\mathcal{L}(V)$ is a finite dimensional vector space over $\mathbb{F}_q$. And denote by $\Omega(V)$ the $\mathbb{F}_q$-vector space of all Weil differentials ω with divisor $\mathrm{div}(\omega) \geqslant V$, together with the zero differential (cf. [31]).

The residue AG code $C_\Omega(D, G)$ is defined to be the image of the following residue map:

$$\begin{aligned} \mathrm{res} : \Omega(G - D) &\rightarrow \mathbb{F}_q^n \\ \omega &\mapsto (\mathrm{res}_{P_1}(\omega), \mathrm{res}_{P_2}(\omega), \cdots, \mathrm{res}_{P_n}(\omega)). \end{aligned}$$

The code $C_\Omega(D, G)$ has parameters $[n, n-k-1+g, d \geq k-(2g-2)]$. And its dual code, the functional AG code $C_\mathcal{L}(D, G)$ is defined to be the image of the following evaluation map:

$$\mathrm{ev} : \mathcal{L}(G) \rightarrow \mathbb{F}_q^n;\ f \mapsto (f(P_1), f(P_2), \cdots, f(P_n)).$$

As functions in $\mathcal{L}(G)$ have at most $k = \deg G$ different zeros, the minimum distance of $C_\mathcal{L}(D, G)$ is $d \geqslant n-k$. By the Riemann-Roch theorem, the functional AG code $C_\mathcal{L}(D, G)$ has parameters $[n, k-g+1, d \geqslant n-k]$. This together with the Singleton bound gives

$$k - (2g-2) \leq d(C_\Omega(D, G)) \leq k - g + 2$$

and

$$n - k \leq d(C_\mathcal{L}(D, G)) \leq n - k + g.$$

If $X = E$ is an elliptic curve over $\mathbb{F}_q$, i.e., $g = 1$, then $C_\Omega(D, G)$ has parameters $[n, n-k, d \geq k]$, $C_\mathcal{L}(D, G)$ has parameters $[n, k, d \geqslant n-k]$, and we only have the following two choices for their minimum distance:

$$d(C_\Omega(D, G)) \in \{k, k+1\}$$

and

$$d(C_\mathcal{L}(D, G)) \in \{n-k, n-k+1\}.$$

It is easy to see that the two minimum distances take either $\{k, n-k\}$ or $\{k+1, n-k+1\}$. In the first case, both $C_\Omega(D, G)$ and $C_\mathcal{L}(D, G)$ are near-MDS codes. In the second case, both $C_\Omega(D, G)$ and $C_\mathcal{L}(D, G)$ are MDS codes. It was shown that the MDS property is equivalent to certain general subset sum problem having no solution [7]. So to determine the exact minimum distance of a general elliptic curve code is **NP**-hard under **RP**-reduction. However, non-trivial elliptic code of length $n \geq q+3$ are near-MDS by the MDS conjecture, i.e., the minimum distance take the smaller one. This suggests that long elliptic curve codes behave better. By using the Li-Wan sieve method [20], the authors [21] improved the upper bound on the length of MDS elliptic curve codes without assuming the MDS conjecture.

Proposition 2.1 ([21]): Suppose that $n \geq (\frac{2}{3} + \epsilon)q$ and $q > \frac{4}{\epsilon^2}$, where ϵ is positive. There is a positive constant C_ϵ such that if $C_\epsilon \ln q < k < n - C_\epsilon \ln q$, then the $[n, k]$ elliptic curve code $C_\mathcal{L}(D, G)$ has minimum distance $n-k$ and hence is near-MDS.

It is further conjectured in [21] that the above condition $n \geq (\frac{2}{3}+\epsilon)q$ can be improved to $n \geq (\frac{1}{2}+\epsilon)q$. This conjecture has been proved in the case $3 \leq k \leq \frac{q+1-2\sqrt{q}}{10}$ in the recent paper [14].

B. A New Viewpoint on the Deep Holes of Reed-Solomon Codes

In this subsection, we give a new viewpoint on the deep holes of Reed-Solomon codes regarded as algebraic geometry codes of genus zero. The advantage of this new viewpoint is that the two classes of deep holes of generalized Reed-Solomon codes are essentially the same. This method extends immediately to elliptic curve codes and even more general AG codes.

Let $\mathbb{F}_q(x)$ be the rational function field. Let O be the infinite point with uniformizer $\frac{1}{x}$ and P_a be the finite point with uniformizer $x - a$ for any $a \in \mathbb{F}_q$. For any subset $D = \{a_1, a_2, \cdots, a_n\} \subset \mathbb{F}_q$, denote the corresponding set of finite points also by $D = \{P_{a_1}, P_{a_2}, \cdots, P_{a_n}\}$. For any integer $1 \leq k \leq n$, the Reed-Solomon (RS) code $RS(D, k)$ is defined to be $C_\mathcal{L}(D, (k-1)O)$. The dual code of RS code $RS(D, k)$ is the residue AG code $C_\Omega(D, (k-1)O)$. Both of these codes are MDS codes and their covering radii are easy to determine.

For RS codes with odd q and $k \geq \lfloor \frac{q-1}{2} \rfloor$, it was proved in [18] that there are only two classes of deep holes. The first class of deep holes of RS code $RS(D, k)$ was given in [8] which corresponds to polynomials of degree k. In fact, these deep holes are vectors in $C_\mathcal{L}(D, kO) \setminus C_\mathcal{L}(D, (k-1)O)$. The second class of deep holes of RS code $RS(D, k)$ was given first in [33] for $D = \mathbb{F}_q^*$ and later in [34] for general $D \subsetneq \mathbb{F}_q$

which corresponds to the rational functions $\{\frac{b}{x-a} \mid a \in \mathbb{F}_q \setminus D, b \in \mathbb{F}_q^*\}$. In fact, these deep holes are exactly the vectors in

$$\bigcup_{a \in \mathbb{F}_q \setminus D} C_{\mathcal{L}}(D, (k-1)O + P_a) \setminus C_{\mathcal{L}}(D, (k-1)O).$$

In the language of AG codes, the two classes of known deep holes can be unified as follows: for any $P \in \mathbb{P}^1(\mathbb{F}_q) \setminus D$, the vectors in $C_{\mathcal{L}}(D, (k-1)O + P) \setminus C_{\mathcal{L}}(D, (k-1)O)$ are deep holes of the Reed-Solomon code $RS(D, k)$. In the case D is the full set $\mathbb{F}_q$, the only possibility for P is O. In this case, the above construction of deep holes is conjectured to be complete in [8], which has been proved to be true if q is a prime [36] or if $k > (q-1)/2$ [18], using results from finite geometry.

III. Covering Radius and Deep Holes

Before we move on to address the deep hole problem for elliptic curve codes, we need to first understand the covering radius for elliptic curve codes. But this is already a difficult problem as seen below.

A. Covering Radius of Elliptic Curve Codes

In this subsection, we study the covering radius of elliptic curve codes. Just like the minimal distance, in general, there are only two possible choices for the covering radius of elliptic curve codes.

The following lemma is essentially derived from [17]. To be self-contained, we give a proof here.

Lemma 3.1: Let $\mathbb{F}_q$ be a finite field with q elements. Let E be an elliptic curve over $\mathbb{F}_q$ with a rational point O, and $D \subset E(\mathbb{F}_q) \setminus \{O\}$ be a set of rational points with $n = |D|$. For $2 \le k \le n-2$, let $C = C_\Omega(D, kO)$ or $C = C_{\mathcal{L}}(D, kO)$. Then the covering radius of C equals either $n - \dim(C) - 1$ or $n - \dim(C)$.

Proof: Denote $k^\perp = n - \dim(C)$. Let $H \in \mathbb{F}_q^{k^\perp \times n}$ be any parity-check matrix for the linear code C. Then the covering radius ρ of C is the smallest positive integer ρ such that any vector $w \in \mathbb{F}_q^{k^\perp}$ can be written as a linear combination of some ρ columns of H. As H is of full rank, we have

$$\rho \le k^\perp.$$

We have seen that from the section Preliminaries:

$$k^\perp - 1 \le d(C_\Omega(D, (k-1)O)) \le k^\perp,$$
$$k^\perp - 1 \le d(C_{\mathcal{L}}(D, (k+1)O)) \le k^\perp,$$

and

$$k^\perp \le d(C) \le k^\perp + 1.$$

Now, by considering any vector

$$v \in \begin{cases} C_\Omega(D, (k-1)O) \setminus C_\Omega(D, kO), & \text{if } C = C_\Omega(D, kO); \\ C_{\mathcal{L}}(D, (k+1)O) \setminus C_{\mathcal{L}}(D, kO), & \text{if } C = C_{\mathcal{L}}(D, kO), \end{cases}$$

we deduce that

$$\begin{aligned} \rho &\ge d(v, C) \\ &\ge \begin{cases} \min(d(C), d(C_\Omega(D, (k-1)O))) & \text{if } C = C_\Omega(D, kO) \\ \min(d(C), d(C_{\mathcal{L}}(D, (k+1)O))) & \text{if } C = C_{\mathcal{L}}(D, kO) \end{cases} \\ &\ge k^\perp - 1. \end{aligned}$$

So $\rho \in \{k^\perp, k^\perp - 1\} = \{n - \dim(C) - 1, n - \dim(C)\}$. □

Remark 3.2: For short elliptic curve codes, to determine the minimum distance is already **NP**-hard [7] under **RP**-reduction. To determine the covering radius is even harder, which not only depends on the MDS property but also on certain extendability of MDS or near-MDS codes. For instance, if C is MDS, then $k^\perp = d(C) - 1$. The covering radius of C can still take any one of the two choices $\{n - \dim(C) - 1, n - \dim(C)\}$. For the covering radius of C to be $n - \dim(C)$, it is equivalent to that there is a vector $v \in \mathbb{F}_q^n \setminus C$ such that $C \oplus \mathbb{F}_q v$ is MDS. Even for $v \in C_{\mathcal{L}}(D, kO + P) \setminus C_{\mathcal{L}}(D, kO)$, the problem is already hard which is equivalent to certain subset sum problem.

However, for long elliptic curve codes of length $n \ge q + 3$, the problem becomes easier, at least under the MDS conjecture. In any case, long AG codes are preferred in applications.

Recall that an $[n, k, d]$ linear code is called *n-optimal* if there does not exist $[n', k, d]$ linear code with $n' < n$.

Theorem 3.3: Let $\mathbb{F}_q$ be a finite field with q elements. Let E be an elliptic curve over $\mathbb{F}_q$ which has at least $q + 4$ rational points. Let $O \in E(\mathbb{F}_q)$ be a rational point on E and $D \subset E(\mathbb{F}_q) \setminus \{O\}$ be a set of rational points with $n = |D| \ge q + 3$. For $2 \le k \le n - 2$, let $C = C_\Omega(D, kO)$ or $C = C_{\mathcal{L}}(D, kO)$. The minimum distance of C is given by $d(C) = n - \dim(C)$. If we further assume that the MDS conjecture holds for all $[n-1, \dim(C)]$-codes over $\mathbb{F}_q$, then the covering radius of C is given by $\rho(C) = d(C) - 1 = n - \dim(C) - 1$.

Proof: The MDS conjecture is known to be true for the elliptic code C, see [32]. Since $n \ge q + 3$, this implies that the code C is not MDS, and hence must be near-MDS with parameters $[n, \dim(C), d(C) = n - \dim(C)]$. In particular, the minimum distance is $d(C) = n - \dim(C)$. Now $n - 1 \ge q + 2$ and q is odd. By the MDS conjecture for $[n-1, \dim(C)]$-codes, we deduce that there is no MDS code with parameters $[n - 1, \dim(C), d(C) = n - \dim(C)]$. So the code C is n-optimal. By [17, Corollary 8.1], we have the following bound on the covering radius

$$\rho(C) \le d(C) - \lceil \frac{d(C)}{q^{\dim(C)}} \rceil.$$

Since $d(C) = n - \dim(C) > 0$, it follows that

$$\rho(C) \le d(C) - 1.$$

On the other hand, by Lemma 3.1, we have

$$\rho(C) \in \{d(C) - 1, d(C)\}.$$

We conclude that $\rho(C) = d(C) - 1$. □

Now, any non-trivial MDS code C of dimension $k \ge 3$ over the finite field $\mathbb{F}_q$ has length $n \le q + k - 2$ by [25, Chapter 11, Theorem 11]. The MDS conjecture holds for prime fields [2], and also for general q with $k \le \sqrt{q}$ [4], [29]. This means that under one of the conditions (1)-(3) in Theorem 1.2, the MDS conjecture holds for all $[n, k]$-codes and $[n-1, k]$-codes over $\mathbb{F}_q$. As a consequence, we obtain the conclusions (i) and (ii) of Theorem 1.2 from Theorem 3.3.

B. Deep Holes of Elliptic Curve Codes and Their Syndromes

In this subsection, we first prove Theorem 1.2(iii)-(iv). In order to study further geometry of deep holes, we will

later focus on residue elliptic curve codes since they have an explicit parity-check matrix of the form (1). The residue and functional algebraic geometry codes can be represented by each other (cf. [31, Proposition 2.2.10]). Thus, in principal, it is sufficient to consider the residue elliptic curve codes.

Lemma 3.4: For any rational point $P \in E(\mathbb{F}_q) \setminus D$ and any $f \in \mathcal{L}(kO+P) \setminus \mathcal{L}(kO)$, we have

1. If $P \neq O$, then P is a simple pole of f.
2. If $P = O$, then O is a pole of f of order $k+1$.

Proof of Theorem 1.2(iii)-(iv). For any rational point $P \in E(\mathbb{F}_q) \setminus D$ and any vector $v \in C_{\mathcal{L}}(D, kO+P) \setminus C$, we have

$$\begin{aligned} n-k-1 &= \rho(C) \geq d(v, C) \\ &\geq \min(d(C), d(C_{\mathcal{L}}(D, kO+P))) \geq n-(k+1). \end{aligned}$$

So $d(v, C) = n-k-1$. That is, the vector v is a deep hole. This proves Theorem 1.2(iii).

Next, we prove Theorem 1.2(iv). For any two distinct rational points $P, Q \in E(\mathbb{F}_q) \setminus D$, since functions in $\mathcal{L}(kO+P+Q)$ have at most $k+2 < n$ zeros, the evaluation map $\mathrm{ev} : \mathcal{L}(kO+P+Q) \to \mathbb{F}_q^n$ is injective. The codes $C_{\mathcal{L}}(D, kO+P)$ and $C_{\mathcal{L}}(D, kO+Q)$ are two sub-codes of the code $C_{\mathcal{L}}(D, kO+P+Q)$. Now, if there exsit $f \in \mathcal{L}(kO+P) \setminus \mathcal{L}(kO)$ and $g \in \mathcal{L}(kO+Q) \setminus \mathcal{L}(kO)$ such that $\mathrm{ev}(f) = \mathrm{ev}(g)$, then $f-g$ regarded as a function in $\mathcal{L}(kO+P+Q)$ satisfies

$$\mathrm{ev}(f-g) = 0.$$

Since the evaluation map $\mathrm{ev} : \mathcal{L}(kO+P+Q) \to \mathbb{F}_q^n$ is injective, we have $f-g=0$, i.e., $f=g$ in $\mathcal{L}(kO+P+Q)$. This is impossible according to Lemma 3.4 by comparing the orders of poles P and Q. So the sets $C_{\mathcal{L}}(D, kO+P) \setminus C$ and $C_{\mathcal{L}}(D, kO+Q) \setminus C$ are disjoint for any distinct rational points $P, Q \in E(\mathbb{F}_q) \setminus D$.

For any rational point $P \in E(\mathbb{F}_q) \setminus D$, we have

$$|C_{\mathcal{L}}(D, kO+P) \setminus C| = q^{k+1} - q^k = (q-1)q^k.$$

According to the above disjointness, there are totally

$$|E(\mathbb{F}_q) \setminus D|(q-1)q^k = (|E(\mathbb{F}_q)| - n)(q-1)q^k$$

deep holes provided by the theorem. □

Remark 3.5: For the case $k = n-2$, let $P, Q \in E(\mathbb{F}_q) \setminus D$ be two distinct rational points. Then the spaces $C_{\mathcal{L}}(D, kO+P) = C_{\mathcal{L}}(D, kO+Q)$ if and only if the divisor $D-kO-P-Q$ is principal.

In the rest of this subsection, we focus on the residue elliptic codes. We will compute the syndromes of deep holes. On the one hand, it will help us to separate the deep holes and then to count them. On the other hand, this computation will help us to connect the deep hole problem and the corresponding finite geometry problem which will be discussed later for the completeness of the found deep holes.

Because we only consider elliptic curves over finite fields of odd characteristic, we may assume the elliptic curve is given by the non-singular Weierstrass equation $y^2 = x^3 + \epsilon x^2 + \lambda x + \mu$ ($\epsilon, \lambda, \mu \in \mathbb{F}_q$) together with the infinity point O. Let

$$D = \{P_i = (\alpha_i, \beta_i) \mid i = 1, 2, \cdots, n\} \subset E(\mathbb{F}_q) \setminus \{O\}\}$$

be a set of rational points on E of size $n = |D|$. Let $C = C_{\Omega}(D, kO)$ be the residue elliptic curve code. Then the dual code of C is $C^{\perp} = C_{\mathcal{L}}(D, kO)$.

The following lemma plays an important role in the explicit computation procedure. The lemma should be well-known in the literature. But we have not found any reference for it. To be self-contained, we give a proof here.

Lemma 3.6: Notations as above. We have

1) For any integer $k \geq 1$, the Riemann-Roch space $\mathcal{L}(kO)$ has a basis

$$\{x^i y^j \mid i \in \mathbb{Z}_{\geq 0},\ j \in \{0,1\},\ 2i+3j \leq k\}.$$

2) For any integer $k \geq 2$ and for any $P = (\alpha, \beta) \in E(\mathbb{F}_q) \setminus \{O\}$, the Riemann-Roch space $\mathcal{L}(kO-P)$ has a basis

$$\begin{aligned} \{x-\alpha, &(x-\alpha)x, \cdots, (x-\alpha)x^{\lfloor \frac{k}{2} \rfloor - 1}, \\ &y-\beta, x(y-\beta), \cdots, x^{\lfloor \frac{k-3}{2} \rfloor}(y-\beta)\}. \end{aligned}$$

Proof: 1. Since we have the valuations $v_O(x) = -2$ and $v_O(y) = -3$, we have $v_O(x^i y^j) = -2i-3j$. So for any non-negative integers i, j satisfying $2i+3j \leq k$, the divisor $\mathrm{div}(x^i y^j) + kO$ is effective, i.e.,

$$\mathrm{div}(x^i y^j) + kO \geq 0.$$

That is, $x^i y^j \in \mathcal{L}(kO)$. By restricting to $j \in \{0,1\}$, it is easy to see that functions $\{x^i y^j \mid i \in \mathbb{Z}_{\geq 0},\ j \in \{0,1\},\ 2i+3j \leq k\}$ are linearly independent over $\mathbb{F}_q$. By direct computing, there are

$$\left(\lfloor \frac{k}{2} \rfloor + 1\right) + \left(\lfloor \frac{k-3}{2} \rfloor + 1\right) = k$$

elements in the set $\{x^i y^j \mid i \in \mathbb{Z}_{\geq 0},\ j \in \{0,1\},\ 2i+3j \leq k\}$. On the other hand, by the Riemann-Roch theorem, the dimension of the Riemann-Roch space $\mathcal{L}(kO)$ is k. So functions in $\{x^i y^j \mid i \in \mathbb{Z}_{\geq 0},\ j \in \{0,1\},\ 2i+3j \leq k\}$ form a basis for the Riemann-Roch space $\mathcal{L}(kO)$.

2. First, functions in $\{x-\alpha, (x-\alpha)x, \cdots, (x-\alpha)x^{\lfloor \frac{k}{2} \rfloor - 1}, y-\beta, x(y-\beta), \cdots, x^{\lfloor \frac{k-3}{2} \rfloor}(y-\beta)\}$ are $\mathbb{F}_q$-linear combinations of functions in $\{x^i y^j \mid i \in \mathbb{Z}_{\geq 0},\ j \in \{0,1\},\ 2i+3j \leq k\}$. It is easy to write down the transform matrix which implies that functions in $\{x-\alpha, (x-\alpha)x, \cdots, (x-\alpha)x^{\lfloor \frac{k}{2} \rfloor - 1}, y-\beta, x(y-\beta), \cdots, x^{\lfloor \frac{k-3}{2} \rfloor}(y-\beta)\}$ are $\mathbb{F}_q$-linearly independent. Secondly, functions in $\{x-\alpha, (x-\alpha)x, \cdots, (x-\alpha)x^{\lfloor \frac{k}{2} \rfloor - 1}, y-\beta, x(y-\beta), \cdots, x^{\lfloor \frac{k-3}{2} \rfloor}(y-\beta)\}$ have a common zero P. So

$$\begin{aligned} \{x-\alpha, &(x-\alpha)x, \cdots, (x-\alpha)x^{\lfloor \frac{k}{2} \rfloor - 1}, \\ &y-\beta, x(y-\beta), \cdots, x^{\lfloor \frac{k-3}{2} \rfloor}(y-\beta)\} \subset \mathcal{L}(kO-P). \end{aligned}$$

Finally, by the Riemann-Roch theorem, the dimension of the Riemann-Roch space $\mathcal{L}(kO-P)$ is $k-1$. So functions in $\{x-\alpha, (x-\alpha)x, \cdots, (x-\alpha)x^{\lfloor \frac{k}{2} \rfloor - 1}, y-\beta, x(y-\beta), \cdots, x^{\lfloor \frac{k-3}{2} \rfloor}(y-\beta)\}$ form a basis for the Riemann-Roch space $\mathcal{L}(kO-P)$. □

By the above lemma, the Riemann-Roch space $\mathcal{L}(kO)$ has a basis

$$\{x^i y^j \mid i \in \mathbb{Z}_{\geq 0},\, j \in \{0,1\},\, 2i+3j \leq k\}.$$

So we can choose a parity-check matrix of C as follows:

$$H(k) = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{\lfloor \frac{k}{2} \rfloor} & \alpha_2^{\lfloor \frac{k}{2} \rfloor} & \cdots & \alpha_n^{\lfloor \frac{k}{2} \rfloor} \\ \beta_1 & \beta_2 & \cdots & \beta_n \\ \alpha_1\beta_1 & \alpha_2\beta_2 & \cdots & \alpha_n\beta_n \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{\lfloor \frac{k-3}{2} \rfloor}\beta_1 & \alpha_2^{\lfloor \frac{k-3}{2} \rfloor}\beta_2 & \cdots & \alpha_n^{\lfloor \frac{k-3}{2} \rfloor}\beta_n \end{pmatrix}. \quad (1)$$

Theorem 3.7: Notations as above. Suppose the $[n, n-k]$-code $C = C_\Omega(D, kO)$ has covering radius $\rho(C) = n - \dim(C) - 1 = k - 1$. Let $P = (\alpha, \beta) \in E(\mathbb{F}_q) \setminus D$ be any rational point on the elliptic curve E. Then we have

1) Any vector $v \in C_\Omega(D, kO - P) \setminus C$ is a deep hole of C.
2) If $P = O$, then the syndrome of v is

$$H(k)v^T = \begin{cases} (0, \cdots, 0, \sum_{i=1}^{n} \alpha_i^{\frac{k}{2}} v_i, 0, \cdots, 0)^T, & \\ & \text{if } k \text{ is even;} \\ (0, \cdots, 0, \sum_{i=1}^{n} \alpha_i^{\frac{k-3}{2}} \beta_i v_i)^T, & \\ & \text{if } k \text{ is odd.} \end{cases}$$

3) If $P \neq O$, then the syndrome of v is

$$H(k)v^T = b(1, \alpha, \cdots, \alpha^{\lfloor \frac{k}{2} \rfloor}, \beta, \beta\alpha, \cdots, \beta\alpha^{\lfloor \frac{k-3}{2} \rfloor})^T,$$

where $b = \sum_{i=1}^{n} v_i \neq 0$.

Proof: Since $d(C) \geq n - \dim(C) = n - (n-k) = k$, the first statement follows from

$$\begin{aligned} k - 1 &= \rho(C) \geq d(v, C) \\ &\geq \min(d(C), d(C_\Omega(D, kO - P))) \geq k - 1. \end{aligned}$$

Next, we compute the syndrome $H(k)v^T$ by separating two cases: $P = O$ and $P \in E(\mathbb{F}_q) \setminus (D \cup \{O\})$.

For the case $P = O$, any vector $v \in C_\Omega(D, (k-1)O) \setminus C_\Omega(D, kO))$ can be annihilated by vectors in $C_\mathcal{L}(D, (k-1)O)$ but not by vectors in $C_\mathcal{L}(D, kO) \setminus C_\mathcal{L}(D, (k-1)O)$. So $H(k-1)v^T = 0$. Hence, the syndrome equals

$$H(k)v^T = \begin{cases} (0, \cdots, 0, \sum_{i=1}^{n} \alpha_i^{\frac{k}{2}} v_i, 0, \cdots, 0)^T, & \text{if } k \text{ is even;} \\ (0, \cdots, 0, \sum_{i=1}^{n} \alpha_i^{\frac{k-3}{2}} \beta_i v_i)^T, & \text{if } k \text{ is odd.} \end{cases}$$

For the case $P = (\alpha, \beta) \in E(\mathbb{F}_q) \setminus (D \cup \{O\})$, similarly, any vector $v \in C_\Omega(D, kO - P) \setminus C_\Omega(D, kO)$ is annihilated by vectors in $C_\mathcal{L}(D, kO - P)$ but not by vectors in $C_\mathcal{L}(D, kO) \setminus C_\mathcal{L}(D, kO - P)$. By Lemma 3.6, the Riemann-Roch space $\mathcal{L}(kO - P)$ has a basis

$$\begin{aligned} \{x - \alpha, &(x-\alpha)x, \cdots, (x-\alpha)x^{\lfloor \frac{k}{2} \rfloor - 1}, \\ &y - \beta, x(y-\beta), \cdots, x^{\lfloor \frac{k-3}{2} \rfloor}(y-\beta)\}. \end{aligned}$$

So we have

$$\begin{pmatrix} \alpha_1 - \alpha & \cdots & \alpha_n - \alpha \\ (\alpha_1 - \alpha)\alpha_1 & \cdots & (\alpha_n - \alpha)\alpha_n \\ \vdots & \ddots & \vdots \\ (\alpha_1 - \alpha)\alpha_1^{\lfloor \frac{k}{2} \rfloor - 1} & \cdots & (\alpha_n - \alpha)\alpha_n^{\lfloor \frac{k}{2} \rfloor - 1} \\ \beta_1 - \beta & \cdots & \beta_n - \beta \\ \alpha_1(\beta_1 - \beta) & \cdots & \alpha_n(\beta_n - \beta) \\ \alpha_1^2(\beta_1 - \beta) & \cdots & \alpha_n^2(\beta_n - \beta) \\ \vdots & \ddots & \vdots \\ \alpha_1^{\lfloor \frac{k-3}{2} \rfloor}(\beta_1 - \beta) & \cdots & \alpha_n^{\lfloor \frac{k-3}{2} \rfloor}(\beta_n - \beta) \end{pmatrix} v^T = 0.$$

Let $b = \sum_{i=1}^{n} v_i$. Since the vector v can not be annihilated by vectors in $C_\mathcal{L}(D, kO) \setminus C_\mathcal{L}(D, kO - P)$, we have $b \neq 0$. So we have

$$\begin{pmatrix} 1 & \cdots & 1 \\ \alpha_1 - \alpha & \cdots & \alpha_n - \alpha \\ (\alpha_1 - \alpha)\alpha_1 & \cdots & (\alpha_n - \alpha)\alpha_n \\ \vdots & \ddots & \vdots \\ (\alpha_1 - \alpha)\alpha_1^{\lfloor \frac{k}{2} \rfloor - 1} & \cdots & (\alpha_n - \alpha)\alpha_n^{\lfloor \frac{k}{2} \rfloor - 1} \\ \beta_1 - \beta & \cdots & \beta_n - \beta \\ \alpha_1(\beta_1 - \beta) & \cdots & \alpha_n(\beta_n - \beta) \\ \alpha_1^2(\beta_1 - \beta) & \cdots & \alpha_n^2(\beta_n - \beta) \\ \vdots & \ddots & \vdots \\ \alpha_1^{\lfloor \frac{k-3}{2} \rfloor}(\beta_1 - \beta) & \cdots & \alpha_n^{\lfloor \frac{k-3}{2} \rfloor}(\beta_n - \beta) \end{pmatrix} v^T = \begin{pmatrix} b \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

By adding the second row by α-times of the first row, then adding the third row by α-times of the new second row, and so on, we obtain

$$\begin{pmatrix} 1 & \cdots & 1 \\ \alpha_1 & \cdots & \alpha_n \\ \vdots & \ddots & \vdots \\ \alpha_1^{\lfloor \frac{k}{2} \rfloor} & \cdots & \alpha_n^{\lfloor \frac{k}{2} \rfloor} \\ \beta_1 - \beta & \cdots & \beta_n - \beta \\ \alpha_1(\beta_1 - \beta) & \cdots & \alpha_n(\beta_n - \beta) \\ \alpha_1^2(\beta_1 - \beta) & \cdots & \alpha_n^2(\beta_n - \beta) \\ \vdots & \ddots & \vdots \\ \alpha_1^{\lfloor \frac{k-3}{2} \rfloor}(\beta_1 - \beta) & \cdots & \alpha_n^{\lfloor \frac{k-3}{2} \rfloor}(\beta_n - \beta) \end{pmatrix} v^T = \begin{pmatrix} b \\ b\alpha \\ \vdots \\ b\alpha^{\lfloor \frac{k}{2} \rfloor} \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Now, by adding β times of the first $\lfloor \frac{k-3}{2} \rfloor + 1$ rows to the lower part in the above equation, we have

$$\begin{pmatrix} 1 & \cdots & 1 \\ \alpha_1 & \cdots & \alpha_n \\ \vdots & \ddots & \vdots \\ \alpha_1^{\lfloor \frac{k}{2} \rfloor} & \cdots & \alpha_n^{\lfloor \frac{k}{2} \rfloor} \\ \beta_1 & \cdots & \beta_n \\ \alpha_1\beta_1 & \cdots & \alpha_n\beta_n \\ \vdots & \ddots & \vdots \\ \alpha_1^{\lfloor \frac{k-3}{2} \rfloor}\beta_1 & \cdots & \alpha_n^{\lfloor \frac{k-3}{2} \rfloor}\beta_n \end{pmatrix} v^T = \begin{pmatrix} b \\ b\alpha \\ \vdots \\ b\alpha^{\lfloor \frac{k}{2} \rfloor} \\ b\beta \\ b\beta\alpha \\ \vdots \\ b\beta\alpha^{\lfloor \frac{k-3}{2} \rfloor} \end{pmatrix}.$$

That is,

$$H(k)v^T = b(1, \alpha, \cdots, \alpha^{\lfloor \frac{k}{2} \rfloor}, \beta, \beta\alpha, \cdots, \beta\alpha^{\lfloor \frac{k-3}{2} \rfloor})^T.$$

□

In the above theorem, one checks that

$$|C_\Omega(D, kO - P) \setminus C| = q^{n-k+1} - q^{n-k} = (q-1)q^{n-k}.$$

If $k \geq 3$, the syndrome formula implies that the union

$$\bigcup_{P \in E(\mathbb{F}_q) \setminus D} C_\Omega(D, kO - P) \setminus C$$

is a disjoint union. This disjoint union gives $(|E(\mathbb{F}_q)| - n)(q-1)q^{n-k}$ deep holes of C. This proves the analogue of Theorem 1.2 for the residue elliptic code $C_\Omega(D, kO)$.

Remark 3.8: It is natural to ask if the deep holes given in the above theorem form all the deep holes. The answer is expected to be yes for long elliptic curve codes, but it is going to be difficult to prove. In next section, we use finite geometry to discuss the completeness of deep holes in the above theorem and use the automorphism technique to obtain more ones if there is any new deep hole.

IV. On the Completeness of Deep Holes

A. Automorphisms of Elliptic Curves and Deep Holes of Elliptic Curve Codes

In this subsection, we use a Hamming distance-preserving subgroup of automorphism group of the linear code C to construct more deep holes if there is any new deep hole. This idea was used in [35].

Let $\mathrm{Aut}(E/\mathbb{F}_q)$ be the $\mathbb{F}_q$-automorphism group of E as an elliptic curve and let $\mathrm{Aut}_{D,G}(E/\mathbb{F}_q)$ be its subgroup fixing D and G, respectively. That is,

$$\mathrm{Aut}_{D,G}(E/\mathbb{F}_q) = \{\sigma \in \mathrm{Aut}(E/\mathbb{F}_q) \,|\, \sigma(D) = D,\, \sigma(G) = G\}.$$

For any linear code C, denote by $\mathrm{PAut}(C)$ the permutation automorphism group of C whose elements are not only permutations of coordinates but also automorphisms of C.

Lemma 4.1: Let $C = C_\Omega(D, G)$ or $C = C_\mathcal{L}(D, G)$ be the algebraic geometry code constructed from the elliptic curve E. There is a homomorphism $\rho : \mathrm{Aut}_{D,G}(E/\mathbb{F}_q) \to \mathrm{PAut}(C)$.

Proof: The statement holds for general algebraic geometry codes [31, Proposition VII.3.3]. In order to describe the detail of the homomorphism which we need to use to obtain new deep holes, we give the construction of the homomorphism, i.e., the proof of the lemma.

We only prove the statement for $C = C_\mathcal{L}(D, G)$. The proof for the case $C = C_\Omega(D, G)$ is the same. Let $\mathrm{Aut}_{D,G}(\mathbb{F}_q(E)/\mathbb{F}_q)$ be the $\mathbb{F}_q$-automorphism group of the elliptic function field $\mathbb{F}_q(E)$ whose elements fix D and G. There is a homomorphism

$$\rho_1 : \mathrm{Aut}_{D,G}(E/\mathbb{F}_q) \to \mathrm{Aut}_{D,G}(\mathbb{F}_q(E)/\mathbb{F}_q)$$

defined by as follows: for any $T \in \mathrm{Aut}_{D,G}(E/\mathbb{F}_q)$, and $f \in \mathbb{F}_q(E)$, $\rho_1(T)(f) = T^*(f)$ is the pull-back of f which is defined by $T^*(f)(P) = f(T^{-1}(P))$ for any $P \in E(\mathbb{F}_q)$.

Next, we show that for any $T \in \mathrm{Aut}_{D,G}(E/\mathbb{F}_q)$, it holds $\rho_1(T) \in \mathrm{Aut}(\mathcal{L}(G))$. For any $f \in \mathcal{L}(G)$, we have $\mathrm{div}(f) + G \geq 0$. So $T^{-1}(\mathrm{div}(f)) + T^{-1}(G) \geq 0$. Since $T^{-1}(G) = G$ and $T^{-1}(\mathrm{div}(f)) = \mathrm{div}(T^*(f))$, we have $\mathrm{div}(T^*(f)) + G \geq 0$. That is, $T^*(f) \in \mathcal{L}(G)$.

Since the map ev is an isomorphism from $\mathcal{L}(G)$ to C, we define $\rho = \mathrm{ev} \circ \rho_1 \circ \mathrm{ev}^{-1} : C \to C$. It is obvious that ρ is an automorphism of C. To finish the proof, we need to show that for any $T \in \mathrm{Aut}_{D,G}(E/\mathbb{F}_q)$, $\rho(T)$ is a permutation of coordinates. Indeed, for any $f \in \mathcal{L}(G)$, we have

$$\begin{aligned}
&\rho(T)(f(P_1), f(P_2), \cdots, f(P_n)) \\
=&\mathrm{ev} \circ \rho_1(T) \circ \mathrm{ev}^{-1}(f(P_1), f(P_2), \cdots, f(P_n)) \\
=&\mathrm{ev}(\rho_1(T)(f)) \\
=&\mathrm{ev}(T^*(f)) \\
=&(T^*(f)(P_1), T^*(f)(P_2), \cdots, T^*(f)(P_n)) \\
=&(f(T^{-1}(P_1)), f(T^{-1}(P_2)), \cdots, f(T^{-1}(P_n))).
\end{aligned}$$

□

Note that for any $T \in \mathrm{Aut}_{D,G}(E/\mathbb{F}_q)$, as a permutation of coordinates, the map $\rho(T)$ can be extended to the whole space $\mathbb{F}_q^n$ which is still denoted by $\rho(T)$.

Proposition 4.2: Let $C = C_\Omega(D, G)$ or $C = C_\mathcal{L}(D, G)$ be the algebraic geometry code constructed from the elliptic curve E. If the word v is a deep hole of C, then so is the word $\rho(T)(v)$ for any $T \in \mathrm{Aut}_{D,G}(E/\mathbb{F}_q)$.

Proof: We have seen that the map $\rho(T) : \mathbb{F}_q^n \to \mathbb{F}_q^n$ preserves the Hamming distance and is an automorphism of C if restricted to the linear subspace C. So

$$d(\rho(T)(v), C) = d(v, \rho(T)^{-1}C) = d(v, C).$$

Hence, the word $\rho(T)(v)$ is a deep hole of C. □

Remark 4.3: Since $T(P) \in E(\mathbb{F}_q) \setminus D$ for any $T \in \mathrm{Aut}_{D,G}(E/\mathbb{F}_q)$ and $P \in E(\mathbb{F}_q) \setminus D$, the deep holes found in Theorem 3.7 are invariant under the action in Proposition 4.2.

If any new deep hole except those in Theorem 3.7 was found, then its orbit under the action of $\rho(\mathrm{Aut}_{D,G}(E/\mathbb{F}_q))$ would provide new ones. So it is interesting to find new deep hole not of the form in Theorem 3.7. We will see this is already very hard for small $n - k$ in the next subsection.

B. Deep Holes of Elliptic Curve Codes and Finite Geometry

In this subsection, we discuss the geometry of deep holes of elliptic curve codes.

Definition 4.4: An n-track in $PG(k-1, \mathbb{F}_q)$, the projective $k-1$-dimensional space over the finite field $\mathbb{F}_q$, is a set $\mathcal{T}$ of n points which satisfies the following two conditions:

(i) Any $k-1$ points in $\mathcal{T}$ are linearly independent as vectors in $\mathbb{F}_q^k$;
(ii) There exists a hyperplane passing through some k points in $\mathcal{T}$.

Definition 4.5: An $(n; k)$-set $\mathcal{A}$ in $PG(k-1, \mathbb{F}_q)$ is an n-track with an extra condition: any $k+1$ points of $\mathcal{A}$ can linearly generate $PG(k-1, \mathbb{F}_q)$.

The following proposition give the structure of long tracks.

Proposition 4.6: [11, Theorem 3.4] If $n > q + k$, then any n-track in $PG(k-1, \mathbb{F}_q)$ is an $(n; k)$-set.

Definition 4.7: An $(n;k)$-set $\mathcal{A}$ in $PG(k-1,\mathbb{F}_q)$ is called complete if there is no $(n+1;k)$-set in $PG(k-1,\mathbb{F}_q)$ containing $\mathcal{A}$ as a subset.

Definition 4.8: An $(n;k)$-set $\mathcal{A}$ in $PG(k-1,\mathbb{F}_q)$ is called extendable if there is some $n+1$-track in $PG(k-1,\mathbb{F}_q)$ containing $\mathcal{A}$ as a subset. Otherwise, we call it non-extendable.

Note that when $n > q+k$, all n-tracks in $PG(k-1,\mathbb{F}_q)$ are $(n;k)$-set. So in this case, "complete" and "non-extendable" are the same thing.

An important class of long $(n;k)$-sets is constructed from elliptic curves, i.e., columns of $H(k)$. We can rearrange the rows of $H(k)$ such that $2i+3j$ of the corresponding row defined by x^iy^j is in the increasing order. Define the map

$$\phi_k : E(\mathbb{F}_q)\setminus\{O\} \to PG(k-1,\mathbb{F}_q)$$
$$(x,y) \mapsto \begin{cases} (1,x,y,x^2,xy,x^3,\cdots,x^{\frac{k}{2}-2}y,x^{\frac{k}{2}})^T \\ \qquad\qquad \text{if } k \text{ is even;} \\ (1,x,y,x^2,xy,x^3,\cdots,x^{\frac{k-1}{2}},x^{\frac{k-3}{2}}y)^T \\ \qquad\qquad \text{if } k \text{ is odd,} \end{cases}$$

and $\phi_k(O) = (0,0,\cdots,0,1)^T \in PG(k-1,\mathbb{F}_q)$. If $n = |D| \geq q+1$, then the code $C_\Omega(D\cup\{P\},kO)$ has minimum distance k for any rational point $P \in E(\mathbb{F}_q)\setminus D$ by MDS conjecture (for a proof of MDS conjecture for elliptic curve codes, we refer to [32]). Note that the matrix $[\phi_k(P_1),\cdots,\phi_k(P_n),\phi_k(P)]$ is a parity-check matrix of the code $C_\Omega(D\cup\{P\},kO)$, so the vectors $\phi_k(P_1),\phi_k(P_2),\cdots,\phi_k(P_n)$ and $\phi_k(P)$ form an $(n+1;k)$-set for any rational point $P \in E(\mathbb{F}_q)\setminus D$.

Proposition 4.9: Suppose the residue elliptic curve code $C = C_\Omega(D,kO)$ has covering radius $\rho = k-1$. Let $H = (h_1,h_2,\cdots,h_n) \in \mathbb{F}_q^{k\times n}$ be a parity-check matrix of C. The vector v is a deep hole of C if and only if vectors $h_1,h_2,\cdots,h_n$ and Hv^T form an $n+1$-track in $PG(k-1,\mathbb{F}_q)$.

Proof: First, since the code $C = C_\Omega(D,kO)$ has minimum distance $\geq k$, any $k-1$ columns of the parity-check matrix H are linearly independent.

Secondly, since C has covering radius $\rho = k-1$, we have that the vector v is a deep hole of C if and only the syndrome Hv^T can not be written as any linear combination of any $\leq k-2$ columns of H.

So if the vector v is a deep hole of C, then

(i) any $k-1$ vectors from $\{h_1,h_2,\cdots,h_n,Hv^T\}$ are linearly independent;

(ii) there exists a hyperplane passing through Hv^T and some $k-1$ vectors from $\{h_1,h_2,\cdots,h_n\}$, since $d(v,C) = k-1$.

Hence $\{h_1,h_2,\cdots,h_n,Hv^T\}$ forms an $n+1$-track in $PG(k-1,\mathbb{F}_q)$.

Conversely, if $\{h_1,h_2,\cdots,h_n,Hv^T\}$ is an $n+1$-track in $PG(k-1,\mathbb{F}_q)$, then any $k-1$ vectors from $\{h_1,h_2,\cdots,h_n,Hv^T\}$ are linearly independent. So the syndrome Hv^T can not be written as any linear combination of any $\leq k-2$ columns of H. Hence the vector v is a deep hole of C. □

The above proposition characterizes the geometry of deep holes of the residue elliptic curve code $C = C_\Omega(D,kO)$, equivalently the extendability of the $(n;k)$-set $\{\phi_k(P_1),\phi_k(P_2),\cdots,\phi_k(P_n)\}$. We have seen that for large $n \geq q+1$ and for any rational point $P \in E(\mathbb{F}_q)\setminus D$ the vectors $\phi_k(P_1),\phi_k(P_2),\cdots,\phi_k(P_n)$ and $\phi_k(P)$ form an $(n+1;k)$-set. As a consequence, we can re-obtain the deep holes of $C = C_\Omega(D,kO)$ in Theorem 3.7.

Here raises the interesting problem: Is the $(|E(\mathbb{F}_q)|;k)$-set $\varepsilon = \{\phi_k(P) \mid P \in E(\mathbb{F}_q)\}$ extendable? If not, does there exist an integer $\mathcal{N}_0$ such that any track intersecting with ε at $\mathcal{N}_0$ or more points must be a part of ε?

Remark 4.10: The authors [1], [12] studied the extendibility of the $(|E(\mathbb{F}_q)|;k)$-set $\varepsilon = \{\phi_k(P) \mid P \in E(\mathbb{F}_q)\}$. The problem for small k is already very difficult, e.g. see [12] for $k=5$. Let $q \geq 121$ be an odd prime power. Let E be an elliptic curve over the finite field $\mathbb{F}_q$ with non-zero j-invariant. Then for $k = 3,4,6$ the $(|E(\mathbb{F}_q)|;k)$-set $(\phi_k(P))_{P\in E(\mathbb{F}_q)}$ is non-extendable. It is conjectured in [1] that for $k=9$ the $(|E(\mathbb{F}_q)|;9)$-set $(\phi_9(P))_{P\in E(\mathbb{F}_q)}$ is complete.

Corollary 4.11: Suppose the $(|E(\mathbb{F}_q)|;k)$-set $\varepsilon = \{\phi_k(P) \mid P \in E(\mathbb{F}_q)\}$ is non-extendable and $\mathcal{N}_0$ is the smallest integer such that any track intersecting with ε at $\mathcal{N}_0$ or more points must be a part of ε. Let $D \subset E(\mathbb{F}_q)\setminus\{O\}$ with cardinality $n = |D| \geq \mathcal{N}_0$. If the residue elliptic curve code $C = C_\Omega(D,kO)$ is near-MDS and has covering radius $\rho = k-1$, then the following words

$$\bigcup_{P\in E(\mathbb{F}_q)\setminus D} C_\Omega(D,kO-P)\setminus C$$

form all the deep holes of C.

Proof: First, for any point $P \in E(\mathbb{F}_q)\setminus D$ and any vector $v \in C_\Omega(D,kO-P)\setminus C$, we have

$$k-1 = \rho \geq d(v,C) \geq \min(d(C),d(C_\Omega(D,kO-P))) \geq k-1.$$

So $d(v,C) = k-1$. That is, the word v is a deep hole of C.

Next, we show the completeness. The code C has a parity-check matrix $H = [\phi_k(P)]_{P\in D}$. Let v be a deep hole of C. By Proposition 4.9, $\phi_k(P), P \in D$ and Hv^T form an $n+1$-track in $PG(k-1,\mathbb{F}_q)$. Since the $n+1$-track $\{\phi_k(P) \mid P \in D\} \cup \{Hv^T\}$ intersects with ε at $n \geq \mathcal{N}_0$ points, by the assumption of the corollary, the syndrome Hv^T has to be of the form $\phi_k(Q)$ for some $Q \in E(\mathbb{F}_q)\setminus D$. From the proof of Theorem 3.7, $\phi_k(Q)$ is the syndrome of some word $w \in C_\Omega(D,kO-Q)\setminus C$. That is,

$$Hv^T = \phi_k(Q) = Hw^T$$

for some $w \in C_\Omega(D,kO-Q)\setminus C$. So we have $v \equiv w \bmod C$. That is, $v \in w+C$ for some $w \in C_\Omega(D,kO-Q)\setminus C$. The completeness is proved. □

If such an $\mathcal{N}_0 \leq |E(\mathbb{F}_q)|-1$ in the above corollary exists, then Conjecture 1.4 holds for $C = C_\Omega(D,kO)$ where $k \in \{n-3,n-4,n-6\}$. As an extension of [30, Theorem 1] from the genus $g=0$ to the genus $g=1$, it is interesting to study the non-extendability of $\{\phi_k(P) \mid P \in E(\mathbb{F}_q)\}$ and the existence of $\mathcal{N}_0$ in Corollary 4.11.

V. Conclusion

In this paper, we studied deep holes of elliptic curve codes. If the covering radius ρ is equal to $k-1$, which typically holds

for long residue elliptic $[n, n-k]$-codes, then classes of deep holes and their syndromes are determined. The completeness of the deep holes found was discussed in connection with extendability of $(n;k)$-sets in finite geometry. If the deep holes found are not complete, then permutation automorphisms can be applied to obtain more deep holes.

ACKNOWLEDGMENT

The authors would like to thank the anonymous reviewers and Associate Editor, Prof. Chaoping Xing, for their valuable suggestions and comments that helped to greatly improve the article.

REFERENCES

[1] A. Aguglia, L. Giuzzi, and A. Sonnino, "Near-MDS codes from elliptic curves," *Des., Codes Cryptogr.*, vol. 89, no. 5, pp. 965–972, May 2021.
[2] S. Ball, "On sets of vectors of a finite vector space in which every subset of basis size is a basis," *J. Eur. Math. Soc.*, vol. 3, nos. 1–2, pp. 733–748, 2012.
[3] S. Ball and J. De Beule, "On sets of vectors of a finite vector space in which every subset of basis size is a basis II," *Des., Codes Cryptograph.*, vol. 65, nos. 1–2, pp. 5–14, 2012.
[4] S. Ball and M. Lavrauw, "Arcs in finite projective spaces," *EMS Surv. Math. Sci.*, vol. 6, no. 1, pp. 133–172, 2019.
[5] D. Bartoli, M. Giulietti, and I. Platoni, "On the covering radius of MDS codes," *IEEE Trans. Inf. Theory*, vol. 61, no. 2, pp. 801–811, Feb. 2015.
[6] M. Privitelli, G. Matera, and A. Cafure, "Singularities of symmetric hypersurfaces and Reed–Solomon codes," *Adv. Math. Commun.*, vol. 6, no. 1, pp. 69–94, Jan. 2012.
[7] Q. Cheng, "Hard problems of algebraic geometry codes," *IEEE Trans. Inf. Theory*, vol. 54, no. 1, pp. 402–406, Jan. 2008.
[8] Q. Cheng and E. Murray, "On deciding deep holes of Reed–Solomon codes," in *Theory and Applications of Models of Computation* (Lecture Notes in Computer Science), vol. 4484, 2007, pp. 296–305.
[9] 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.
[10] G. Cohen, A. Lobstein, and N. Sloane, "Further results on the covering radius of codes," *IEEE Trans. Inf. Theory*, vol. IT-32, no. 5, pp. 680–694, Sep. 1986.
[11] S. Dodunekov and I. Landjev, "On near-MDS codes," *J. Geometry*, vol. 54, nos. 1–2, pp. 30–43, 1994.
[12] M. Giulietti, "On the extendibility of near-MDS elliptic codes," *Applicable Algebra Eng., Commun. Comput.*, vol. 15, no. 1, pp. 1–11, Jun. 2004.
[13] R. Graham and N. Sloane, "On the covering radius of codes," *IEEE Trans. Inf. Theory*, vol. IT-31, no. 3, pp. 385–401, Jun. 1985.
[14] D. Han and Y. Ren, "A tight upper bound for the maximal length of MDS elliptic codes," *IEEE Trans. Inf. Theory*, vol. 69, no. 2, pp. 819–822, Feb. 2023.
[15] T. Helleseth, T. Klove, and J. Mykkeltveit, "On the covering radius of binary codes (Corresp.)," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 5, pp. 627–628, Sep. 1978.
[16] X. D. Hou, "Some results on the covering radii of Reed–Múller codes," *IEEE Trans. Inf. Theory*, vol. 39, no. 2, pp. 366–378, Mar. 1993.
[17] H. Janwa, "Some optimal codes from algebraic geometry and their covering radii," *Eur. J. Combinatorics*, vol. 11, no. 3, pp. 249–266, May 1990.
[18] K. Kaipa, "Deep holes and MDS extensions of Reed–Solomon codes," *IEEE Trans. Inf. Theory*, vol. 63, no. 8, pp. 4940–4948, Aug. 2017.
[19] M. Keti and D. Wan, "Deep holes in Reed–Solomon codes based on Dickson polynomials," *Finite Fields Their Appl.*, vol. 40, pp. 110–125, Jul. 2016.
[20] J. Li and D. Wan, "On the subset sum problem over finite fields," *Finite Fields Appl.*, vol. 14, no. 4, pp. 911–929, 2008.
[21] J. Li, D. Wan, and J. Zhang, "On the minimum distance of elliptic curve codes," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jun. 2015, pp. 2391–2395.
[22] Y. Li and D. Wan, "On error distance of Reed–Solomon codes," *Sci. China*, vol. 51, no. 11, pp. 1982–1988, 2008.
[23] Y. Li and G. Zhu, "On the error distance of extended Reed–Solomon codes," *Adv. Math. Commun.*, vol. 10, no. 2, pp. 413–427, Apr. 2016.
[24] Q. Liao, "On Reed–Solomon codes," *Chin. Ann. Math.*, vol. 1, pp. 89–98, Jan. 2011.
[25] F. MacWilliams and N. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam, The Netherlands: North-Holland, 2006.
[26] A. McLoughlin, "The complexity of computing the covering radius of a code," *IEEE Trans. Inf. Theory*, vol. IT-30, no. 6, pp. 800–804, Nov. 1984.
[27] P. R. J. Östergård, "New constructions for q-ary covering codes," *Ars Combinatoria-Waterloo Winnipeg*, vol. 52, pp. 51–63, Jan. 1999.
[28] K.-U. Schmidt, "Asymptotically optimal Boolean functions," *J. Combinat. Theory A*, vol. 164, pp. 50–59, May 2019.
[29] B. Segre, "Curve razionali normali ek-archi negli spazi finiti," *Annali Matematica Pura Applicata*, vol. 39, no. 1, pp. 357–379, 1955.
[30] G. Seroussi and R. M. Roth, "On MDS extensions of generalized Reed–Solomon codes," *IEEE Trans. Inf. Theory*, vol. IT-32, no. 3, pp. 349–354, May 1986.
[31] H. Stichtenoth, *Algebraic Function Fields and Codes* (Graduate Texts in Mathematics), vol. 254, 2nd ed. Berlin: Springer-Verlag, 2009.
[32] J. L. Walker, *A New Approach to the Main Conjecture on Algebraic-Geometric MDS Codes*. Boston, MA, USA: Springer, 1996, pp. 111–116.
[33] R. Wu and S. Hong, "On deep holes of standard Reed–Solomon codes," *Sci. China Math.*, vol. 55, no. 12, pp. 2447–2455, Dec. 2012.
[34] J. Zhang, F.-W. Fu, and Q.-Y. Liao, "New deep holes of generalized Reed–Solomon codes," 2012, *arXiv:1205.6593*.
[35] J. Zhang, D. Wan, and K. Kaipa, "Deep holes of projective Reed–Solomon codes," *IEEE Trans. Inf. Theory*, vol. 66, no. 4, pp. 2392–2401, Apr. 2020.
[36] J. Zhuang, Q. Cheng, and J. Li, "On determining deep holes of generalized Reed–Solomon codes," *IEEE Trans. Inf. Theory*, vol. 62, no. 1, pp. 199–207, Jan. 2016.

Jun Zhang received the B.S. degree in mathematics and the Ph.D. degree from Nankai University, Tianjin, China, in 2008 and 2014, respectively. Since August 2014, he has been with the School of Mathematical Sciences, Capital Normal University, Beijing, China, where he is currently an Associate Professor. He visited the Department of Mathematics, University of California at Irvine, USA, from September 2012 to September 2013. He visited the School of Computer Science, University of Oklahoma, USA, from January 2017 to December 2017. His research interests include number theory, coding theory, and cryptography.

Daqing Wan received the B.S. degree from the Chengdu Institute of Geology in 1982, the M.S. degree from Sichuan University in 1986, and the Ph.D. degree from the University of Washington, Seattle, in 1991. In 1997, he joined the University of California at Irvine, where he is currently a Professor of mathematics. His research interests include number theory, coding theory, algorithms, and complexity.