Parameters and Decoding Performance of Subfield Subcodes of One-Point Elliptic Codes

Jianguo Zhao†, Li Chen‡
† School of System Science and Engineering, Sun Yat-sen University, Guangzhou, China
‡ School of Electronics and Information Technology, Sun Yat-sen University, Guangzhou, China
Email: zhaojg5@mail2.sysu.edu.cn, chenli55@mail.sysu.edu.cn

2022 IEEE/CIC International Conference on Communications in China (ICCC Workshops) | 978-1-6654-5977-8/22/$31.00 ©2022 IEEE | DOI: 10.1109/ICCCWORKSHOPS55477.2022.9896651

***Abstract*—It is known that subfield subcodes of Reed-Solomon (RS) codes include many good codes, such as BCH codes and classical Goppa codes. Extending the subfield subcode discovery from RS codes to the more general algebraic-geometric (AG) codes, this paper investigates the subfield subcodes of one-point elliptic codes, in order to provide an alternative to BCH codes. Lower bounds on the dimension and the minimum distance of these codes are characterized, which behave tight for the medium-to-high rate subfield subcodes of differential elliptic codes. The work will show that subfield subcodes of differential elliptic codes are superior to those of the evaluation ones. Many good codes and even the best known linear codes can be found in the family of these codes. With both the elliptic codes and the RS codes defined over the same field, near maximum likelihood (ML) decoding results show that some binary subfield subcodes of the elliptic codes outperform the similar rate BCH codes.**

***Index Terms*—Algebraic-geometric codes, elliptic codes, subfield subcodes**

I. Introduction

It is known that BCH codes are subfield subcodes of Reed-Solomon (RS) codes [1]. They inherit the algebraic structure of RS codes, yielding a strong error-correction capability and efficient decoding methods. Moreover, subfield subcodes of generalized RS (GRS) codes, namely, alternant codes also include classical Goppa codes and other celebrated codes [2]. It reveals that one can obtain many good codes from RS (or GRS) codes through the subfield subcode approach. Constructed from a straight line, RS codes are a special class of algebraic-geometric (AG) codes. Motivated by the good subfield subcodes of RS codes, it is also important to further investigate subfield subcodes of other AG codes. This will provide more alternatives to BCH codes.

The first systematic study on subfield subcodes of GRS codes was presented by Delsarte [1], which related subfield subcodes to trace codes and introduced a general bound on the parameters, i.e., the dimension and the minimum distance of subfield subcodes. After the introduction of AG codes [3], their subfield subcodes also attracted research interest. More precise estimations for the dimension of these codes than Delsarte's bound were proposed in [4]–[6], which can be included as a special case of Stichtenoth's bound for general subfield subcodes [7]. It was shown in [8] that subfield subcodes of certain AG codes meet the Gilbert-Varshamov bound. Subsequently, many improvements on Grassl's table of the best known linear codes [1] [9] were found in certain variants of subfield subcodes of AG codes, e.g., RS codes [10] [11] and elliptic codes [12]. Recently, subfield subcodes become prominent in the cryptosystems based on codes, for which a fast algorithm to compute the dimension of subfield subcodes of Hermitian codes was designed in [13].

With a genus of one, elliptic codes are almost maximum distance separable (MDS), ensuring the distance property of their subcodes. Meanwhile, defined over the same field, they can possess a larger codeword length than RS codes. Moreover, the efficient algebraic decoding algorithms of elliptic codes, including the unique decoding [14] [15] and the list decoding [16], can be modified to decode their subfield subcodes. Therefore, subfield subcodes of elliptic codes have a potential to replace BCH codes. This paper studies on the subfield subcodes of one-point elliptic codes. For simplicity, we call them elliptic subfield subcodes. Lower bounds on their dimension and minimum distance are characterized. Combining bounds and numerical results, this work shows the difference in parameters between evaluation and differential elliptic subfield subcodes. With both the elliptic codes and the RS codes defined over the same field, the near maximum likelihood (ML) decoding performance of their binary subfield subcodes is given. It demonstrates that some elliptic subfield subcodes can outperform the similar rate BCH codes.

II. Preliminaries

This section will introduce the basic knowledges of AG codes and subfield subcodes, including their construction and parameters.

A. AG Codes

Let $\mathbb{F}_q$ denote a finite field of size q, where $q = p^m$, p is a prime power and m is a positive integer. Let $\mathcal{X}$ denote an irreducible nonsingular algebraic curve over $\mathbb{F}_q$ with degree θ. The genus of $\mathcal{X}$ is [17]

$$g = \frac{(\theta-1)(\theta-2)}{2}. \tag{1}$$

[1]The minimum distance of these code is maximum among all known linear codes.

Points on $\mathcal{X}$ with all their coordinates in $\mathbb{F}_q$ are called rational points. Suppose there are $N(\mathcal{X})$ rational points on $\mathcal{X}$, $N(\mathcal{X})$ satisfies the Serre improvement of the Hasse-Weil bound [18]

$$|N(\mathcal{X}) - (q+1)| \leqslant g\lfloor 2\sqrt{q} \rfloor. \tag{2}$$

Definition I *([19]).* A divisor on a curve $\mathcal{X}$ is defined as a formal sum $D = \sum_{P\in\mathcal{X}} n_P P$, where P is a point on $\mathcal{X}$ and n_P is an integer with $n_P \neq 0$ for only a finite number of P. If $n_P \geqslant 0$ for all P, D is called effective and written as $D \succeq 0$. The divisor has a degree of $\deg(D) = \sum_{P\in\mathcal{X}} n_P \deg(P)$, where $\deg(P)$ is the degree of P over $\mathbb{F}_q$.

Let $\mathbb{F}_q(\mathcal{X})$ denote the function field of $\mathcal{X}$ and $\Omega(\mathcal{X})$ denote the set of rational differentials on $\mathcal{X}$. Given $f \in \mathbb{F}_q(\mathcal{X})$ with $f \neq 0$, the divisor of f is $\mathrm{div}(f) = \sum_{P\in\mathcal{X}} v_P(f)P$, where $v_P(f)$ is the order of f at P. The divisor of $\omega \in \Omega(\mathcal{X})$ can be defined similarly.

Definition II *([19]).* Let D be a divisor on $\mathcal{X}$, two finite dimensional linear spaces over $\mathbb{F}_q$ are defined as

$$\mathcal{L}(D) = \{f \in \mathbb{F}_q(\mathcal{X})\backslash\{0\} \,|\, \mathrm{div}(f) + D \succeq 0\} \cup \{0\}, \tag{3}$$

and

$$\Omega(D) = \{\omega \in \Omega(\mathcal{X})\backslash\{0\} \,|\, \mathrm{div}(\omega) - D \succeq 0\} \cup \{0\}. \tag{4}$$

Armed with the above knowledges, the construction of AG codes can be introduced. Let $P_1, P_2, ..., P_n$ be n distinct rational points on $\mathcal{X}$, $D = \sum_{i=1}^{n} P_i$ be a divisor and $G = \sum_{P\in\mathcal{X}} n_P P$ be another divisor with $n_{P_i} = 0$ for $i = 1, 2, ..., n$.

Definition III *([19]).* An evaluation AG code $\mathbb{C}_{\mathcal{L}}(D, G)$ of length n over $\mathbb{F}_q$ is defined as the image of the linear map

$$\begin{aligned} \Phi : \mathcal{L}(G) &\to \mathbb{F}_q^n \\ f &\mapsto (f(P_1), f(P_2), ..., f(P_n)). \end{aligned} \tag{5}$$

Similarly, a differential AG code $\mathbb{C}_{\Omega}(D, G)$ is defined as the image of the linear map

$$\begin{aligned} \Psi : \Omega(G - D) &\to \mathbb{F}_q^n \\ \omega &\mapsto (\mathrm{Res}_{P_1}(\omega), \mathrm{Res}_{P_2}(\omega), ..., \mathrm{Res}_{P_n}(\omega)), \end{aligned} \tag{6}$$

where $\mathrm{Res}_{P_i}(\omega)$ is the residue of ω at P_i.

Theorem 1 *([18]).* $\mathbb{C}_{\mathcal{L}}(D, G)$ and $\mathbb{C}_{\Omega}(D, G)$ are dual codes.

The above theorem is based on the residue theorem. Let k, d and d^* denote the dimension, the minimum distance and the designed distance of the code $\mathbb{C}_{\mathcal{L}}(D, G)$ (or $\mathbb{C}_{\Omega}(D, G)$), respectively. They are distinguished by the subscript $\mathcal{L}$ (or Ω).

Theorem 2 *([18]).* Assume $2g - 2 < \deg(G) < n$, then

$$\begin{cases} k_{\mathcal{L}} = \dim \mathcal{L}(G) = \deg(G) - g + 1, \\ k_{\Omega} = \dim \Omega(G - D) = n - \deg(G) + g - 1, \end{cases} \tag{7}$$

and

$$\begin{cases} d_{\mathcal{L}} \geqslant d^*_{\mathcal{L}} = n - \deg(G), \\ d_{\Omega} \geqslant d^*_{\Omega} = \deg(G) - 2g + 2. \end{cases} \tag{8}$$

Therefore, the designed distance of an AG code is $d^* = n - k + 1 - g$. The genus g prevents d^* from reaching the Singleton bound.

B. Subfield Subcodes

Given a linear code $\mathbb{C}[n, k, d]_q$ defined over $\mathbb{F}_q$ with parity-check matrix $\mathbf{H} = (h_{ji})_{(n-k)\times n}$, $\mathbb{C}$ is defined by $\mathbf{H}$ as $\mathbb{C} = \{\underline{c} = (c_1, c_2, ..., c_n) \in \mathbb{F}_q^n \,|\, \underline{c} \cdot \mathbf{H}^T = \underline{0}\}$.

Definition IV. The subfield subcode of $\mathbb{C}$ over $\mathbb{F}_p$ is $\mathbb{C} \cap \mathbb{F}_p^n$, denoted by $\mathbb{C}|\mathbb{F}_p$.

Furthermore, $\mathbb{C}|\mathbb{F}_p$ can be equivalently defined as

$$\mathbb{C}|\mathbb{F}_p = \{\tilde{\underline{c}} = (\tilde{c}_1, \tilde{c}_2, ..., \tilde{c}_n) \in \mathbb{F}_p^n \,|\, \tilde{\underline{c}} \cdot \mathbf{H}^T = \underline{0}\}. \tag{9}$$

The code $\mathbb{C}|\mathbb{F}_p$ is a linear code over $\mathbb{F}_p$ with length n the same as $\mathbb{C}$. But it has a dimension $\tilde{k}$ and a minimum distance $\tilde{d}$, which may be different from $\mathbb{C}$.

Suppose $\alpha_1, \alpha_2, ..., \alpha_m$ form a basis of $\mathbb{F}_q$ over $\mathbb{F}_p$. For any $\beta \in \mathbb{F}_q$, there exist $\beta^{(1)}, \beta^{(2)}, ..., \beta^{(m)} \in \mathbb{F}_p$ such that $\beta = \sum_{l=1}^{m} \beta^{(l)} \alpha_l$. Since $h_{ji} \in \mathbb{F}_q$,

$$h_{ji} = \sum_{l=1}^{m} h_{ji}^{(l)} \alpha_l, \tag{10}$$

where $h_{ji}^{(l)} \in \mathbb{F}_p$. Given an arbitrary codeword $\tilde{\underline{c}} \in \mathbb{C}|\mathbb{F}_p$, $\tilde{\underline{c}} \cdot \mathbf{H}^T = \underline{0}$, i.e.

$$\sum_{i=1}^{n} \tilde{c}_i h_{ji} = 0, \quad \text{for } j = 1, 2, ..., n - k. \tag{11}$$

Based on (10), each of the above equations can be equivalently written as

$$\sum_{i=1}^{n} \tilde{c}_i (\sum_{l=1}^{m} h_{ji}^{(l)} \alpha_l) = \sum_{l=1}^{m} \alpha_l \sum_{i=1}^{n} \tilde{c}_i h_{ji}^{(l)} = 0. \tag{12}$$

Since $\alpha_1, \alpha_2, ..., \alpha_m$ are a basis of $\mathbb{F}_q$, the equality holds iff $\sum_{i=1}^{n} \tilde{c}_i h_{ji}^{(l)} = 0, \forall l$. Let $\underline{h}_{ji} = (h_{ji}^{(1)}, h_{ji}^{(2)}, ..., h_{ji}^{(m)})$ denote a vector over $\mathbb{F}_p$. An $m(n-k) \times n$ matrix over $\mathbb{F}_p$ can be defined as

$$\tilde{\mathbf{H}} = \begin{bmatrix} \underline{h}_{1,1}^T & \underline{h}_{1,2}^T & \cdots & \underline{h}_{1,n}^T \\ \underline{h}_{2,1}^T & \underline{h}_{2,2}^T & \cdots & \underline{h}_{2,n}^T \\ \vdots & \vdots & \ddots & \vdots \\ \underline{h}_{n-k,1}^T & \underline{h}_{n-k,2}^T & \cdots & \underline{h}_{n-k,n}^T \end{bmatrix}. \tag{13}$$

Hence, (11) can be equivalently transformed to $\tilde{\underline{c}} \cdot \tilde{\mathbf{H}}^T = \underline{0}$. The matrix $\tilde{\mathbf{H}}$ is not necessarily full rank. Performing Gaussian elimination, $\tilde{\mathbf{H}}$ is reduced to $n - \tilde{k}$ rows. Note that $\mathrm{rank}(\tilde{\mathbf{H}}) \leqslant m(n-k)$. The above description also implies a lower bound on the dimension of $\mathbb{C}|\mathbb{F}_p$, as stated below.

Theorem 3 *([1]).* The dimension and the minimum distance of $\mathbb{C}|\mathbb{F}_p$ satisfies

$$\begin{aligned} n - m(n-k) \leqslant \tilde{k} \leqslant k, \\ d \leqslant \tilde{d}. \end{aligned} \tag{14}$$

III. Parameters of Elliptic Subfield Subcodes

In this section, the one-point elliptic codes are first constructed. Subsequently, bounds on the parameters of their subfield subcodes are investigated. Finally, numerical results of the parameters are provided.

A. Elliptic Codes

Let $\mathcal{X}$ be an elliptic curve in the projective space over $\mathbb{F}_q$, which is characterized by the following homogeneous equation [20]

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3, \quad (15)$$

where $a_1, a_2, a_3, a_4, a_6 \in \mathbb{F}_q$. With $z = 1$, $\mathcal{X}$ yields an affine curve, on which the rational points are called affine points and denoted by $P_1, P_2, ..., P_n$. It can be verified that $P_\infty = (0 : 1 : 0)$ is the only point at infinity on $\mathcal{X}$. Based on (1) and (2), the genus of $\mathcal{X}$ is 1, and the number of rational points on $\mathcal{X}$ is bounded by

$$\lfloor 2\sqrt{q} \rfloor - q - 1 \leqslant N(\mathcal{X}) \leqslant \lfloor 2\sqrt{q} \rfloor + q + 1. \quad (16)$$

In fact, the maximal $N(\mathcal{X})$ always meets the above upper bound unless $p \equiv 0 \bmod \lfloor 2\sqrt{q} \rfloor$ and m is odd, in which case the maximal $N(\mathcal{X}) = \lfloor 2\sqrt{q} \rfloor + q$ [18]. This paper focuses on elliptic curves with the maximal $N(\mathcal{X})$, to enable the largest codeword length.

Let divisors $D = \sum_{i=1}^{n} P_i$ and $G = uP_\infty$, for $2g - 2 = 0$ and $0 < u < n$. Based on *Definition* III, the evaluation elliptic code and the differential elliptic code are $\mathbb{C}_{\mathcal{L}}(D, uP_\infty)$ and $\mathbb{C}_{\Omega}(D, uP_\infty)$, respectively. Since the divisor G only contains one point at infinity, these elliptic codes are called one-point elliptic codes. The designed distance of an elliptic code is $d^* = n - k$. Hence, they are almost MDS.

B. Parameterizations

Consider $\mathbb{C}_{\Omega}(D, uP_\infty)$ whose dual code is $\mathbb{C}_{\mathcal{L}}(D, uP_\infty)$. The parity-check matrix $\mathbf{H}_\Omega$ of $\mathbb{C}_\Omega$ will be the generator matrix of $\mathbb{C}_{\mathcal{L}}$. Assume $\phi_1, \phi_2, ..., \phi_u$ form a basis of $\mathcal{L}(uP_\infty)$, $\Phi(\phi_1), \Phi(\phi_2), ..., \Phi(\phi_u)$ constitute the rows of $\mathbf{H}_\Omega$. Based on (11), for each $\tilde{\underline{c}} \in \mathbb{C}_\Omega|\mathbb{F}_p$, the following check equations hold

$$\tilde{\underline{c}}^T \cdot \Phi(\phi_j) = 0, \quad \text{for } j = 1, 2, ..., u. \quad (17)$$

Similarly, the parity-check matrix $\tilde{\mathbf{H}}_\Omega$ over $\mathbb{F}_p$ can be established for $\mathbb{C}_\Omega|\mathbb{F}_p$. As mentioned in Section II.B, it is possible to eliminate some rows of $\tilde{\mathbf{H}}_\Omega$. The following introduces a lemma for the redundant row elimination of $\tilde{\mathbf{H}}_\Omega$.

Let $\sigma : \mathbb{F}_q \to \mathbb{F}_q$ denote the Frobenius map given by $\sigma(x) = x^p$, which is an automorphism of $\mathbb{F}_q = \mathbb{F}_{p^m}$. Moreover, σ can be extended to a vector $\underline{b} = (b_1, b_2, ..., b_n) \in \mathbb{F}_q^n$ by $\sigma(\underline{b}) = (\sigma(b_1), \sigma(b_2), ..., \sigma(b_n))$.

Lemma 4 *([4]).* Give any $\underline{b} \in \mathbb{F}_p^n$ and any $f \in \mathcal{L}(uP_\infty)$, $\underline{b}^T \cdot \Phi(f) = 0$ iff $\underline{b}^T \cdot \Phi(\sigma f) = 0$.

Proof: Since σ is an automorphism of $\mathbb{F}_q$, $\sigma(\underline{b}^T \cdot \Phi(f)) = \sigma(\underline{b}^T) \cdot \sigma(\Phi(f))$. In addition, $\sigma(f(P_i)) = \sigma f(P_i)$ for $f \in \mathcal{L}(uP_\infty) \subset \mathbb{F}_q[x, y]$. Hence,

$$\begin{aligned} 0 = \underline{b}^T \cdot \Phi(f) \Rightarrow 0 &= \sigma(\underline{b}^T \cdot \Phi(f)) = \sigma(\underline{b}^T) \cdot \sigma(\Phi(f)), \\ &= \underline{b}^T \cdot \sigma(\Phi(f)) = \underline{b}^T \cdot \Phi(\sigma f). \end{aligned}$$

The necessity can be proven in a similar way. □

Lemma 4 implies if ϕ and $\sigma\phi$ are both in a basis of $\mathcal{L}(uP_\infty)$, one of their check equations can be omitted. Furthermore, the m corresponding rows of $\tilde{\mathbf{H}}_\Omega$ can be eliminated. If there are e distinct pairs of ϕ and $\sigma\phi$ in a basis of $\mathcal{L}(uP_\infty)$, the rank of $\tilde{\mathbf{H}}_\Omega$ will not be greater than $m(u - e)$.

Based on (15), it can be seen that $v_{P_\infty}(x) = -2$, $v_{P_\infty}(y) = -3$ and $v_{P_\infty}(x^\lambda y^\gamma) = -2\lambda - 3\gamma$. Thus $\mathcal{L}(uP_\infty)$ contains a basis as

$$\begin{aligned} \mathcal{B}_{uP_\infty} &= \{\psi_s \,|\, v_{P_\infty}(\psi_s) = -s, s = 0, 2, 3, ..., u\} \\ &= \{\psi_0, \psi_2, \psi_3, ..., \sigma\psi_2, \sigma\psi_3, ..., \psi_u\}. \end{aligned} \quad (18)$$

Since ψ_0 represents a constant function, the m rows of $\tilde{\mathbf{H}}$ generated by ψ_0 are linearly dependent, which can be reduced to one row. For the other $\psi_s \in \mathcal{B}_{uP_\infty}$, if $sp \leqslant u$, there exists a rational function ψ with $v_{P_\infty}(\psi) = -sp$ such that $\psi = \sigma\psi_s$. The function ψ can be another element of $\mathcal{B}_{uP_\infty}$. Therefore, the following theorems hold.

Theorem 5. The dimension of $\mathbb{C}_\Omega(D, uP_\infty)|\mathbb{F}_p$ for $0 < u < n$ is lower bounded by

$$\begin{aligned} \tilde{k}_\Omega &\geqslant n - 1 - m \left\lceil \frac{u}{p} \right\rceil \\ &= n - 1 - m \left\lceil \frac{n - k_\Omega}{p} \right\rceil. \end{aligned} \quad (19)$$

Proof: For every $s = 2, 3, ..., \lfloor u/p \rfloor$, there exists a rational function $\psi_s \in \mathcal{B}_{uP_\infty} \subset \mathcal{L}(uP_\infty)$ with $v_{P_\infty}(\psi_s) = -s$. Since $v_{P_\infty}(\sigma\psi_s) = v_{P_\infty}(\psi_s^p) = pv_{P_\infty}(\psi_s) = -ps$ and $-ps + u \geqslant 0$, $\mathrm{div}(\sigma\psi_s) + uP_\infty \succeq 0$. Therefore, $\sigma\psi_s \in \mathcal{L}(uP_\infty)$ can be selected as another element of $\mathcal{B}_{uP_\infty}$.

Based on *Lemma* 4, the $\lfloor u/p \rfloor - 1$ check equations given by $\sigma\psi_2, \sigma\psi_3, ..., \sigma\psi_{\lfloor u/p \rfloor}$ can be eliminated. Hence, the parity-check matrix $\tilde{\mathbf{H}}_\Omega$ of $\mathbb{C}_\Omega|\mathbb{F}_p$ has $\mathrm{rank}(\tilde{\mathbf{H}}_\Omega) \leqslant m(\lceil u/p \rceil + 1)$. Moreover, there must be a constant function ψ_0 with $v_{P_\infty}(\psi_0) = 0$ in $\mathcal{B}_{uP_\infty}$. This results in $\mathrm{rank}(\tilde{\mathbf{H}}_\Omega)$ being reduced by $m - 1$. Therefore, $\mathrm{rank}(\tilde{\mathbf{H}}_\Omega) \leqslant m\lceil u/p \rceil + 1$ and the lower bound on $\tilde{k}_\Omega$ is given by $\tilde{k}_\Omega = n - \mathrm{rank}(\tilde{\mathbf{H}}_\Omega)$. □

Theorem 6. If $0 < u < n$ and $u \equiv p - 1 \bmod p$,

$$\mathbb{C}_\Omega(D, uP_\infty)|\mathbb{F}_p = \mathbb{C}_\Omega(D, (u + 1)P_\infty)|\mathbb{F}_p. \quad (20)$$

Furthermore, the minimum distance of $\mathbb{C}_\Omega(D, uP_\infty)|\mathbb{F}_p$ is lower bounded by

$$\begin{aligned} \tilde{d}_{\Omega(uP_\infty - D)} &\geqslant u + 1 \\ &= d^*_{\Omega(uP_\infty - D)} + 1. \end{aligned} \quad (21)$$

Proof: If $u \equiv p - 1 \bmod p$, $u = p\lfloor u/p \rfloor + p - 1$ and $u+1 = p(\lfloor u/p \rfloor + 1)$. Since $u > 0$, $\lfloor u/p \rfloor + 1 \leqslant u$. There exists a rational function $\psi_{\lfloor u/p \rfloor + 1} \in \mathcal{B}_{uP_\infty}$ with $v_{P_\infty}(\psi_{\lfloor u/p \rfloor + 1}) = -(\lfloor u/p \rfloor + 1)$. Let $\psi = \sigma\psi_{\lfloor u/p \rfloor + 1}$, $v_{P_\infty}(\psi) = -p(\lfloor u/p \rfloor + 1) = -(u + 1)$. Therefore, ψ can be added into $\mathcal{B}_{uP_\infty}$ to form a basis $\mathcal{B}_{(u+1)P_\infty}$ for $\mathcal{L}((u + 1)P_\infty)$.

Based on *Lemma* 4, the check equation given by ψ can be eliminated. Hence, $\tilde{\mathbf{H}}_{\Omega(uP_\infty - D)} = \tilde{\mathbf{H}}_{\Omega((u+1)P_\infty - D)}$ and $\mathbb{C}_\Omega(D, uP_\infty)|\mathbb{F}_p = \mathbb{C}_\Omega(D, (u + 1)P_\infty)|\mathbb{F}_p$. □

Theorems 5 and 6 yield the same results as [4] [7]. Focusing on the case of one-point differential elliptic subfield subcodes,

their proofs have been simplified. The following example illustrate how the theorems can be applied.

Example 1. Given an elliptic curve $\mathcal{X} : y^2 + y = x^3 + x^2$ defined over $\mathbb{F}_{16}$, $N(\mathcal{X}) = 25$. Choose all the affine points to constitute a divisor D. $\mathbb{C}_\Omega(D, uP_\infty)$ has a length $n = 24$. Consider its subfield subcodes over $\mathbb{F}_2$:

1) $u = 4$, $k_\Omega = 20$ and $d_\Omega = 4$. Based on (14), $\tilde{k}_\Omega \geqslant 24-4\times 4 = 8$ and $\tilde{d}_\Omega \geqslant 4$. However, Based on (19) and (21), $\tilde{k}_\Omega \geqslant 24-1-4\times 2 = 15$ and $\tilde{d}_\Omega \geqslant 4$. The true values of $\tilde{k}_\Omega$ and $\tilde{d}_\Omega$ are 15 and 4.

2) $u = 5$, $k_\Omega = 19$ and $d_\Omega = 5$. Based on (14), $\tilde{k}_\Omega \geqslant 24-4\times 5 = 4$ and $\tilde{d}_\Omega \geqslant 5$; However, Based on (19) and (21), $\tilde{k}_\Omega \geqslant 24-1-4\times 3 = 11$ and $\tilde{d}_\Omega \geqslant 5+1 = 6$. The true values of $\tilde{k}_\Omega$ and $\tilde{d}_\Omega$ are 11 and 6.

It can be seen that both (19) and (21) provide a tighter estimation for the dimension and the minimum distance of the differential elliptic subfield subcode $\mathbb{C}_\Omega|\mathbb{F}_p$ than (14). However, it remains difficult to obtain an improved bound like (19) and (21) for the evaluation elliptic subfield subcode $\mathbb{C}_\mathcal{L}|\mathbb{F}_p$. In fact, the dual code of an evaluation AG code, i.e., a differential AG code can also be represented as an evaluation AG code by [17]

$$\mathbb{C}_\Omega(D, G) = \mathbb{C}_\mathcal{L}(D, \mathrm{div}(\eta) + D - G), \tag{22}$$

where η is a rational differential in $\Omega(\mathcal{X})$ with a simple pole and residue 1 at the points $P_1, P_2, ..., P_n$. Nevertheless, a one-point differential elliptic code cannot always be represented as a one-point evaluation elliptic code, making it difficult to be analysed. In most cases, the parameters of the evaluation elliptic subfield subcodes are worse than their differential counterparts. The following table provides some cases of binary elliptic subfield subcodes to demonstrate this fact.

TABLE I
PARAMETERS OF $\mathbb{C}_\mathcal{L}(D, uP_\infty)|\mathbb{F}_2$ AND $\mathbb{C}_\Omega(D, uP_\infty)|\mathbb{F}_2$

$\mathbb{C}_\mathcal{L}$ $[n, k_\mathcal{L}, d^*_\mathcal{L}]_q$	$\mathbb{C}_\mathcal{L}\|\mathbb{F}_2$ $[n, \tilde{k}_\mathcal{L}, \tilde{d}_\mathcal{L}]_2$	$\mathbb{C}_\Omega$ $[n, k_\Omega, d^*_\Omega]_q$	$\mathbb{C}_\Omega\|\mathbb{F}_2$ $[n, \tilde{k}_\Omega, \tilde{d}_\Omega]_2$
$[24, 16, 8]_{16}$	$[24, 5, 8]_2$	$[24, 16, 8]_{16}$	$[24, 9, 8]_2$
$[43, 39, 4]_{32}$	$[43, 23, 6]_2$	$[43, 37, 6]_{32}$	$[43, 27, 6]_2$
$[43, 35, 8]_{32}$	$[43, 10, 8]_2$	$[43, 35, 8]_{32}$	$[43, 22, 8]_2$
$[80, 75, 5]_{64}$	$[80, 57, 6]_2$	$[80, 74, 6]_{64}$	$[80, 61, 6]_2$
$[80, 69, 11]_{64}$	$[80, 31, 12]_2$	$[80, 68, 12]_{64}$	$[80, 43, 12]_2$
$[80, 67, 13]_{64}$	$[80, 22, 16]_2$	$[80, 64, 16]_{64}$	$[80, 34, 16]_2$

Table I shows that with the same length and minimum distance, the dimension of $\mathbb{C}_\Omega|\mathbb{F}_2$ is often greater than that of $\mathbb{C}_\mathcal{L}|\mathbb{F}_2$, especially when the code rate decreases.

C. Numerical Results

With the above parameterization of differential elliptic subfield subcodes, we now provide more numerical results. Tables II-V list the true dimension $\tilde{k}_\Omega$ and minimum distance $\tilde{d}_\Omega$ of binary subfield subcodes of the differential elliptic codes defined over $\mathbb{F}_{16}$, $\mathbb{F}_{32}$, $\mathbb{F}_{64}$ and $\mathbb{F}_{128}$, respectively. The elliptic codes are constructed with the maximum number of rational points and the divisor D consists of all affine points. Hence, they have a length $n = 24$, 43, 80 and 149, respectively. The Tables also show the dimension k_Ω and the designed distance d^*_Ω of the elliptic codes and the lower bound (19) on $\tilde{k}_\Omega$. Besides, the minimum distance d_B of the best known linear codes [9] that have the same length and dimension as the elliptic subfield subcodes is given together.

TABLE II
PARAMETERS OF $\mathbb{C}_\Omega(D, uP_\infty)|\mathbb{F}_2$ FOR $q = 16$ AND $n = 24$

$\mathbb{C}_\Omega[k_\Omega, d^*_\Omega]$	$\tilde{k}_\Omega \geqslant$	$\mathbb{C}_\Omega\|\mathbb{F}_2[\tilde{k}_\Omega, \tilde{d}_\Omega]$	d_B
$[22, 2]$	19	$[19, 2]$	3
$[20, 4]$	15	$[15, \mathbf{4}]$	4
$[18, 6]$	11	$[11, 6]$	8
$[16, 8]$	7	$[9, \mathbf{8}]$	8
$[14, 10]$	3	$[6, \mathbf{10}]$	10
$[12, 12]$	0	$[4, \mathbf{12}]$	12
$[8, 16]$	0	$[2, \mathbf{16}]$	16

TABLE III
PARAMETERS OF $\mathbb{C}_\Omega(D, uP_\infty)|\mathbb{F}_2$ FOR $q = 32$ AND $n = 43$

$\mathbb{C}_\Omega[k_\Omega, d^*_\Omega]$	$\tilde{k}_\Omega \geqslant$	$\mathbb{C}_\Omega\|\mathbb{F}_2[\tilde{k}_\Omega, \tilde{d}_\Omega]$	d_B
$[41, 2]$	37	$[37, 2]$	3
$[39, 4]$	32	$[32, 4]$	5
$[37, 6]$	27	$[27, 6]$	7
$[35, 8]$	22	$[22, 8]$	9
$[33, 10]$	17	$[17, 10]$	12
$[31, 12]$	12	$[12, 12]$	16
$[29, 14]$	7	$[7, 14]$	20
$[23, 20]$	0	$[2, 26]$	28

TABLE IV
PARAMETERS OF $\mathbb{C}_\Omega(D, uP_\infty)|\mathbb{F}_2$ FOR $q = 64$ AND $n = 80$

$\mathbb{C}_\Omega[k_\Omega, d^*_\Omega]$	$\tilde{k}_\Omega \geqslant$	$\mathbb{C}_\Omega\|\mathbb{F}_2[\tilde{k}_\Omega, \tilde{d}_\Omega]$	d_B
$[78, 2]$	73	$[73, 2]$	3
$[76, 4]$	67	$[67, 4]$	5
$[74, 6]$	61	$[61, 6]$	7
$[72, 8]$	55	$[55, \mathbf{8}]$	8
$[70, 10]$	49	$[49, \mathbf{10}]$	10
$[68, 12]$	43	$[43, \mathbf{12}]$	12
$[66, 14]$	37	$[37, 14]$	16
$[64, 16]$	31	$[34, 16]$	18
$[62, 18]$	25	$[28, 18]$	20
$[60, 20]$	19	$[22, 20]$	24
$[56, 24]$	7	$[16, 24]$	30
$[54, 26]$	1	$[10, 26]$	35
$[52, 28]$	0	$[9, 30]$	36
$[48, 32]$	0	$[7, 32]$	38
$[36, 44]$	0	$[3, 44]$	45
$[32, 48]$	0	$[2, 48]$	53

The numerical results of Tables II-V can be summarized as the following.

Remark 1. For $\mathbb{C}_\Omega|\mathbb{F}_2$ with a medium-to-high rate, (19) provides a precise estimation for $\tilde{k}_\Omega$. However, (19) tends to be loose for codes with a rate below half.

Remark 2. For $\mathbb{C}_\Omega|\mathbb{F}_2$ with a medium-to-high rate, $\tilde{d}$ is within a difference of 2 from d_B, which indicates the elliptic subfield subcodes have a good distance property. However, $\tilde{d}_\Omega$ may depart from d_B when the code rate is low. In the Tables, there are some $\tilde{d}_\Omega$'s (marked in bold) that meet the corresponding d_B's. Therefore, the family of elliptic subfield

TABLE V
PARAMETERS OF $\mathbb{C}_\Omega(D, uP_\infty)|\mathbb{F}_2$ FOR $q = 128$ AND $n = 149$

$\mathbb{C}_\Omega[k_\Omega, d^*_\Omega]$	$\tilde{k}_\Omega \geqslant$	$\mathbb{C}_\Omega\|\mathbb{F}_2[\tilde{k}_\Omega, \tilde{d}_\Omega]$	d_{B}
$[147, 2]$	141	$[141, 2]$	3
$[145, 4]$	134	$[134, 4]$	5
$[143, 6]$	127	$[127, 6]$	7
$[141, 8]$	120	$[120, \mathbf{8}]$	8
$[139, 10]$	113	$[113, \mathbf{10}]$	10
$[137, 12]$	106	$[106, \mathbf{12}]$	12
$[135, 14]$	99	$[99, \mathbf{14}]$	14
$[133, 16]$	92	$[92, \mathbf{16}]$	16
$[131, 18]$	85	$[85, \mathbf{18}]$	18
$[129, 20]$	78	$[78, 20^*]$	22
$[127, 22]$	71	$[71, 22^*]$	24
$[125, 24]$	64	$[64, 24^*]$	26
$[123, 26]$	57	$[57, 26^*]$	32
$[121, 28]$	50	$[50, 28^*]$	34
$[119, 30]$	43	$[43, 30^*]$	36
$[113, 36]$	22	$[36, 36^*]$	44
$[111, 38]$	15	$[29, 38]$	50
$[107, 42]$	1	$[22, 44]$	56
$[105, 44]$	0	$[15, 46]$	64
$[103, 46]$	0	$[11, 46]$	68
$[95, 54]$	0	$[4, 62]$	79

Superscript * means the true $\tilde{d}$ may be greater.

subcodes contains a certain number of the best known linear codes.

IV. DECODING PERFORMANCE

In the previous discussions, it can be seen that differential elliptic subfield subcodes have good parameters at medium-to-high code rates. This section will show the near ML decoding performance of some good binary elliptic subfield subcodes. The ordered statistics decoding (OSD) algorithm [21] is used to achieve the near ML performance for these codes.

Assume a codeword $\underline{\tilde{c}} \in \mathbb{C}_\Omega|\mathbb{F}_2[n, \tilde{k}_\Omega, \tilde{d}_\Omega]$ is transmitted using binary phase shift keying (BPSK) modulation and a vector $\underline{\tilde{y}} \in \mathbb{R}^n$ is received. Let $\underline{\tilde{r}} \in \mathbb{F}_2^n$ denote the hard-decision vector of $\underline{\tilde{y}}$. The OSD of order τ, denoted as OSD-τ, consists of three steps:

1) Calculate the reliability of each symbol in $\underline{\tilde{y}}$. Based on the reliabilities, identify the $\tilde{k}_\Omega$ most reliable independent positions (MRIPs) in $\underline{\tilde{y}}$.

2) Perform Gaussian elimination to obtain a systematic generator matrix $\tilde{\mathbf{G}}_\Omega$ of $\mathbb{C}_\Omega|\mathbb{F}_2$ with weight-1 columns located at the MRIPs.

3) Flip at most τ bits in the MRIPs of $\underline{\tilde{r}}$ to yield a series of information vectors. Encode them to generate the codeword candidates using $\tilde{\mathbf{G}}_\Omega$. Select the most likely candidate w.r.t. $\underline{\tilde{y}}$ as the decoding output.

Figs. 1 and 2 show the OSD performance of the subfield subcodes of differential elliptic codes defined over $\mathbb{F}_{32}$ and $\mathbb{F}_{64}$, respectively. Performance of extended primitive BCH (eBCH) codes [1] with similar rates is also given in the figure as a benchmark. Note the eBCH codes come from the RS codes defined over the same finite field as the elliptic codes. The decoding frame error rate (FER) are obtained over the additive white Gaussian noise (AWGN) channel using BPSK modulation.

[1]Subfield subcodes of one-point RS codes are eBCH codes.

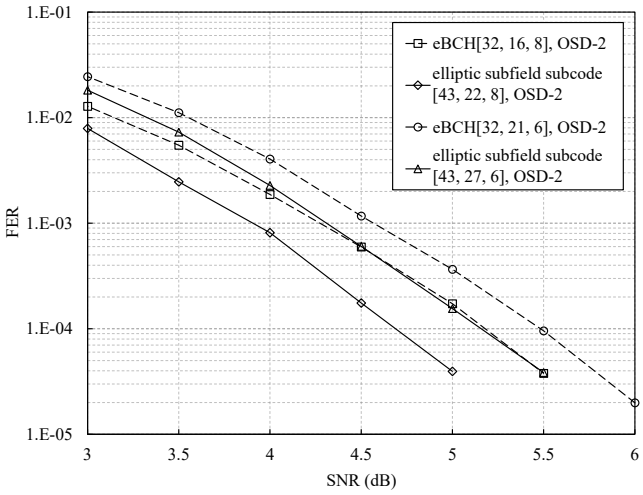

Fig. 1. OSD performance of elliptic subfield subcodes for $q = 32$.

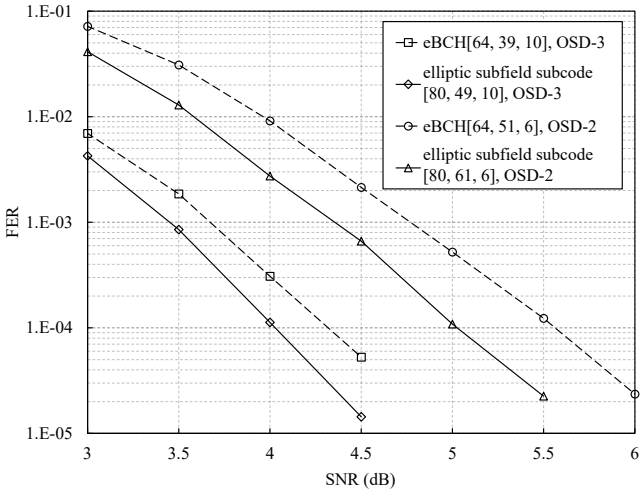

Fig. 2. OSD performance of elliptic subfield subcodes for $q = 64$.

For the eBCH codes and the elliptic subfield subcodes shown in Fig. 1, an OSD of order $\tau = 2$ is sufficient to yield near ML decoding performance for these codes. The elliptic subfield subcodes $\mathbb{C}_\Omega|\mathbb{F}_2[43, 22, 8]$ and $\mathbb{C}_\Omega|\mathbb{F}_2[43, 27, 6]$ outperform eBCH$[32, 16, 8]$ and eBCH$[32, 21, 6]$ with coding gains of 0.5 dB and 0.3 dB at FER = 10^{-4}, respectively. A similar result can be observed in Fig. 2, where $\mathbb{C}_\Omega|\mathbb{F}_2[80, 49, 10]$ achieves a coding gain of 0.3 dB over eBCH$[64, 39, 10]$ with $\tau = 3$, and $\mathbb{C}_\Omega|\mathbb{F}_2[80, 61, 6]$ achieves a coding gain of 0.6 dB over eBCH$[64, 51, 6]$ with $\tau = 2$. As shown in Tables III and IV, $\mathbb{C}_\Omega|\mathbb{F}_2[43, 22, 8]$, $\mathbb{C}_\Omega|\mathbb{F}_2[43, 27, 6]$ and $\mathbb{C}_\Omega|\mathbb{F}_2[80, 61, 6]$ have a minimum distance close to the best known result d_{B}, while $\mathbb{C}_\Omega|\mathbb{F}_2[80, 49, 10]$ has a minimum distance that meets d_{B}. Hence, their competent decoding performance partially attributes to their good distance property. On the other hand, they possess a larger codeword length than the eBCH codes, which also gives them a greater error-correction capability.

V. Conclusion

This paper has analysed the parameters and the decoding performance of one-point elliptic subfield subcodes. A tight lower bound on the dimension of medium-to-high rate differential elliptic subfield subcodes has been characterized. The bounds and the numerical results have shown that differential elliptic subfield subcodes are superior to their evaluation counterparts. Many good codes and even the best known linear codes are contained in the family of these codes. The OSD results have demonstrated that some binary elliptic subfield subcodes can outperform the similar rate BCH codes. Therefore, elliptic subfield subcodes have a potential to replace BCH codes in practical applications. The future work should focus on designing efficient decoding methods for elliptic subfield subcodes based on their algebraic structure.

Acknowledgement

This work is sponsored by the National Natural Science Foundation of China (NSFC) with project ID 62071498.

References

[1] P. Delsarte, "On subfield subcodes of modified Reed-Solomon codes (Corresp.)," *IEEE Trans. Inform. Theory*, vol. 21, no. 5, pp. 575–576, Sep. 1975.

[2] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error Correcting Codes*. Elsevier, 1977, vol. 16.

[3] V. D. Goppa, "Codes on algebraic curves," *Soviet Math. Doklady*, vol. 24, pp. 170–172, 1981.

[4] M. Wirtz, "On the parameters of Goppa codes," *IEEE Trans. Inform. Theory*, vol. 34, no. 5, pp. 1341–1343, Sep. 1988.

[5] G. L. Katsman and M. A. Tsfasman, "A remark on algebraic geometric codes," *Contemp. Math.*, 1989.

[6] A. N. Skorobogatov, "The parameters of subcodes of algebraic-geometric codes over prime subfields," *Discrete Appl. Math.*, vol. 33, no. 1-3, pp. 205–214, 1991.

[7] H. Stichtenoth, "On the dimension of subfield subcodes," *IEEE Trans. Inform. Theory*, vol. 36, no. 1, pp. 90–93, Jan. 1990.

[8] C. Voss and H. Stichtenoth, "Asymptotically good families of subfield subcodes of geometric Goppa codes," *Geom. Dedicata*, vol. 33, no. 1, Jan. 1990.

[9] M. Grassl, "Bounds on the minimum distance of linear codes and quantum codes," Online available at http://www.codetables.de, 2007.

[10] J. Bierbrauer and Y. Edel, "New code parameters from Reed-Solomon subfield codes," *IEEE Trans. Inform. Theory*, vol. 43, no. 3, pp. 953–968, May 1997.

[11] F. Hernando, K. Marshall, and M. E. O'Sullivan, "The dimension of subcode-subfields of shortened generalized Reed–Solomon codes," *Des. Codes Cryptogr.*, vol. 69, no. 1, pp. 131–142, Oct. 2013.

[12] C. Xing and S. Ling, "A class of linear codes with good parameters from algebraic curves," *IEEE Trans. Inform. Theory*, vol. 46, no. 4, pp. 1527–1532, Jul. 2000.

[13] F. Piñero and H. Janwa, "On the subfield subcodes of Hermitian codes," *Des. Codes Cryptogr.*, vol. 70, no. 1-2, pp. 157–173, Jan. 2014.

[14] G. Feng and T. R. Rao, "Decoding algebraic-geometric codes up to the designed minimum distance," *IEEE Trans. Inform. Theory*, vol. 39, no. 1, pp. 37–45, 1993.

[15] S. Sakata, J. Justesen, Y. Madelung *et al.*, "Fast decoding of algebraic-geometric codes up to the designed minimum distance," *IEEE Trans. Inform. Theory*, vol. 41, no. 6, pp. 1672–1677, 1995.

[16] Y. Wan, L. Chen, and F. Zhang, "Guruswami-Sudan decoding of elliptic codes through module basis reduction," *IEEE Trans. Inform. Theory*, vol. 67, no. 11, pp. 7197–7209, 2021.

[17] H. Stichtenoth, *Algebraic Function Fields and Codes*, 2nd ed., ser. Graduate Texts in Mathematics. Berlin: Springer, 2009, no. 254.

[18] I. Blake, C. Heegard, T. Høholdt, and V. Wei, "Algebraic-geometry codes," *IEEE Trans. Inform. Theory*, vol. 44, no. 6, pp. 2596–2618, Oct. 1998.

[19] T. Høholdt, J. van Lint, and R. Pellikaan, *Algebraic Geometry Codes, Handbook of Coding Theory*, V. Pless, W. Huffman, and R. Brualdi, Eds. Elsevier, 1998, vol. 16.

[20] Y. Driencourt and J. F. Michon, "Elliptic codes over fields of characteristics 2," *Journal of Pure and Applied Algebra*, vol. 45, no. 1, pp. 15–39, 1987.

[21] M. Fossorier and S. Lin, "Soft-decision decoding of linear block codes based on ordered statistics," *IEEE Trans. Inform. Theory*, vol. 41, no. 5, pp. 1379–1396, Sep. 1995.