LETTER

On the Feng-Rao Bound for the \( \mathcal{L} \)-construction of Algebraic Geometry Codes

Ryutaroh MATSUMOTO\(^{1}\), Student Member and Shinji MIURA\(^{11}\), Member

SUMMARY We show how to apply the Feng-Rao decoding algorithm and the Feng-Rao bound for the \( \Omega \)-construction of algebraic geometry codes to the \( \mathcal{L} \)-construction. Then we give examples in which the \( \mathcal{L} \)-construction gives better linear codes than the \( \Omega \)-construction in certain range of parameters on the same curve.

key words: algebraic geometry code, minimum distance, decoding, \( \mathcal{L} \)-construction

1. Introduction

Let \( K \) be a finite field, \( F/K \) an algebraic function field of one variable, \( P_1, \ldots, P_n, Q \) pairwise distinct places of \( F \) with degree one, and \( D := P_1 + \cdots + P_n \). Goppa [4] introduced the algebraic geometry code

\[
C_{\Omega}(D, mQ) := \{(\text{res}_{P_1}(\omega), \ldots, \text{res}_{P_n}(\omega)) \mid \omega \in \Omega(mQ - D)\},
\]

which is called the \( \Omega \)-construction. On the other hand, another kind of algebraic geometry code

\[
C_{\mathcal{L}}(D, mQ) := \{(f(P_1), \ldots, f(P_n)) \mid f \in \mathcal{L}(mQ)\},
\]

which is called the \( \mathcal{L} \)-construction, was not explicitly mentioned by Goppa but known to researchers including Goppa and Manin [17, p.386]. \( C_{\mathcal{L}}(D, mQ) \) seems to be first explicitly defined in [8], [15].

Most research articles treat only \( C_{\Omega}(D, mQ) \). A reason for this trend may be due to the lack of efficient decoding algorithms for \( C_{\mathcal{L}}(D, mQ) \), while we know efficient decoding algorithms for \( C_{\Omega}(D, mQ) \) proposed by Feng and Rao [1] and Sakata et al. [12]. In this paper we show how to apply the Feng-Rao algorithm to \( C_{\mathcal{L}}(D, mQ) \). The reader may wonder if there is any advantage considering \( C_{\mathcal{L}}(D, mQ) \) over \( C_{\Omega}(D, mQ) \). We shall give examples in which the error-correcting capability of \( C_{\mathcal{L}}(D, mQ) \) is larger than \( C_{\Omega}(D, mQ) \) while their dimensions are the same, where \( F, D, Q \) are common to \( C_{\mathcal{L}}(D, mQ) \) and \( C_{\Omega}(D, mQ) \). Thus it is worth considering \( C_{\mathcal{L}}(D, mQ) \) as well for fixed \( F, D, Q \).

In Sect. 2, we slightly generalize Miura’s definition [9], [10] of the Feng-Rao bound [1] and the improved algebraic geometry codes [2]. In Sect. 3, we show how to apply the Feng-Rao bound in Sect. 2 to \( C_{\mathcal{L}}(D, mQ) \). In Sect. 4, we give examples in which the \( \mathcal{L} \)-construction gives better linear codes than the \( \Omega \)-construction in certain range of parameters. In Sect. 5, concluding remarks are given.

2. Improved Geometric Goppa Codes and Their Decoding

Notations follow those in Stichtenoth’s textbook [16] unless otherwise specified. Feng and Rao presented an efficient decoding algorithm for one-point algebraic geometry codes \( C_{\Omega}(D, mQ) \) [1], then pointed out that one can increase the dimension of an algebraic geometry code \( C_{\Omega}(D, mQ) \) without decreasing its error-correcting capability by deleting unnecessary rows in the check matrix [2]. The latter construction is called improved geometric Goppa codes. Miura observed that the results of Feng and Rao can be obtained using only linear algebra [9], [10]. In order to apply the Feng-Rao bound and decoding algorithm to \( C_{\mathcal{L}}(D, mQ) \), we slightly generalize Miura’s results in this section. Other reformulation of [1], [2] can be found in [5]–[7], [9]–[11], [13], [14].

Let \( \{u_1, \ldots, u_n\}, \{v_1, \ldots, v_n\} \) and \( \{w_1, \ldots, w_n\} \) be bases of \( K^n \). For \( i = 1, \ldots, n \), let \( W_i \) be the linear space spanned by \( \{w_1, \ldots, w_i\} \), with \( W_0 = \{0\} \) and \( W_{-1} = \emptyset \). For \( a \) and \( b \in K^n \), \( a \ast b \in K^n \) denotes the componentwise product of \( a \) and \( b \).

**Definition 2.1:** A pair \((u_i, v_j)\) is said to be well-behaving if \( u_i \ast v_j \in W_s \setminus W_{s-1} \) for some \( s \) and \( u_i \ast v_v \in W_v \setminus W_{v-1} \) for all \( 1 \leq u \leq i, 1 \leq v \leq j \), \( (u, v) \neq (i, j) \).

A pair \((u_i, v_j)\) is said to be weakly well-behaving if \( u_i \ast v_j \in W_s \setminus W_{s-1} \) for some \( s \), \( u_i \ast v_v \in W_v \setminus W_{v-1} \) for all \( 1 \leq u < i \), and \( u_i \ast v_v \in W_v \setminus W_{v-1} \) for all \( 1 \leq v < j \).

**Definition 2.2:** For \( s = 1, \ldots, n \), we define \( \nu_s \) (resp. \( \lambda_s \)) to be \#\{(u_i, v_j) \mid (u_i, v_j) \text{ is well-behaving} \} \text{ (resp. weakly well-behaving)} \) and \( u_i \ast v_v \in W_s \setminus W_{s-1} \).
We shall consider the minimum distance of \(C(W)\) and a decoding algorithm for \(C(W)\).

**Definition 2.3:** We define

\[
\delta_{\text{FR}}(W) := \min \{ \nu_s | w_s \notin W \},
\]

\[
\delta_{\text{WFR}}(W) := \min \{ \lambda_s | w_s \notin W \}.
\]

We can easily see that \(\delta_{\text{WFR}} \geq \delta_{\text{FR}}\), because well-behaving implies weakly well-behaving.

**Proposition 2.4:** The minimum distance of \(C(W)\) is greater than or equal to \(\delta_{\text{WFR}}\).

**Proof:** For \(y = (y_1, \ldots, y_n) \in K^n\), we define the syndrome matrix by

\[
S(y) = \begin{pmatrix}
       u_1 & \cdots & u_n \\
       \vdots & \ddots & \vdots \\
       u_n & \cdots & u_1
\end{pmatrix}
\begin{pmatrix}
       y_1 \\
       \vdots \\
       y_n
\end{pmatrix}^T.
\]

Then the Hamming weight of \(y\) is equal to \(\text{rank}(S(y))\), and the \((i, j)\)-entry of \(S(y)\) is equal to \(\langle y, u_i \ast v_j \rangle\), where \(\langle \cdot, \cdot \rangle\) denotes the inner product.

Suppose that \(\langle y, w_1 \rangle = \cdots = \langle y, w_{s-1} \rangle = 0\) and \(\langle y, w_s \rangle \neq 0\) for some positive integer \(s\). If \((u_i, v_j)\) is weakly well-behaving and \(u_i \ast v_j \in W_s \setminus W_{s-1}\), then the \((i, j)\)-entry of \(S(y)\) is nonzero, because \(u_i \ast v_j\) is a linear combination of \(w_1, \ldots, w_s\) and the coefficient of \(w_s\) is nonzero. The \((u, j)\) and \((i, v)\)-entries are zero for all \(1 \leq u < i, 1 \leq v < j\), because \(u_u \ast v_j\) and \(u_i \ast v_v\) are linear combinations of \(w_1, \ldots, w_{s-1}\). The number of weakly well-behaving \((u_i, v_j)\) such that \(u_i \ast v_j \in W_s \setminus W_{s-1}\) is \(\lambda_s\). Thus the Hamming weight of \(y = \text{rank}(S(y))\) is equal to or greater than \(\lambda_s\).

Suppose further that \(y\) is a nonzero codeword in the linear code \(C(W)\). Then \(w_s \notin W\), which completes the proof.

**Proposition 2.5:** We can correct \(|\delta_{\text{FR}}(W) - 1|/2\) or less errors of \(C(W)\) in computational complexity \(O(n^3)\).

**Proof:** The decoding algorithm, the proof of its correctness and the analysis of its computational complexity are almost the same as those given in [6, Section 6.3], with differences:

- \(\nu_s\) in our paper corresponds to \(\nu_1\) in [6].
- The syndrome matrix \(S(y)\) in our paper is smaller than that in [6].

In order to construct a linear code \(C(W)\) with the minimum distance not less than \(d\) with an error-correcting algorithm, \(W\) has to be chosen as

\[
W(d) := \{ w_s | \nu_s \leq d - 1 \}
\]

(1)

to minimize the number of check symbols of \(C(W)\). Feng and Rao pointed out in [2] that unnecessary rows in the check matrix can be deleted without decreasing the error-correcting capability as Eq. (1).

**Example 2.6:** We can construct an example in which \(\delta_{\text{WFR}}\) is strictly greater than \(\delta_{\text{FR}}\). Suppose that \(K\) is the finite field with 2 elements, \((u_1, u_2) = \{v_1, v_2\} = \{(0, 0), (0, 1)\}\), \((w_1, w_2) = \{(0, 1), (0, 0)\}\), and \(W = \{w_1\}\). Then \(\delta_{\text{FR}}(W) = 0\) but \(\delta_{\text{WFR}}(W) = 1\). We do not know an algebraic geometry code in which \(\delta_{\text{WFR}}\) gives strictly better estimation than \(\delta_{\text{FR}}\).

**Problem 2.7:** It is an open problem to find an efficient decoding algorithm that corrects errors up to \(\delta_{\text{WFR}}\).

3. On the Feng-Rao Bound and the Goppa Bound for \(C_\Omega(D, mQ)\)

Let \(\{a_1, \ldots, a_n\} := \{m | C_\Omega(D, mQ) \neq C_\Omega(D, (m + 1)Q)\}\) such that \(a_1 > a_2 > \cdots > a_n\). Choose \(\omega_i \in \Omega(a_iQ - D)\) such that \(v_Q(\omega_i) = a_i\) for \(i = 1, \ldots, n\).

\(\mathcal{L}(\infty Q)\) denotes \(\mathcal{L}(Q) \cup \mathcal{L}(2Q) \cup \cdots\). Choose a \(K\)-basis \(\{f_1, f_2, \ldots\}\) of \(\mathcal{L}(\infty Q)\) such that \(v_Q(f_i) > v_Q(f_{i+1})\) for all positive integer \(i\). Let \(\{b_1, \ldots, b_n\} := \{m | C_\Omega(D, mQ) \neq C_\Omega(D, (m - 1)Q)\}\) such that \(b_1 < b_2 < \cdots < b_n\). Choose \(g_i\) among \(\{f_1, f_2, \ldots\}\) such that \(v_Q(g_i) = -b_i\) for \(i = 1, \ldots, n\).

Hereafter we set \(u_i = (g_i(P_1), \ldots, g_i(P_n))\) and \(v_i = v_i = (\text{res}_{P_1}(\omega_i), \ldots, \text{res}_{P_n}(\omega_i))\) for \(i = 1, \ldots, n\), and apply the results in Sect. 2 to this setting. If \(\dim C_\Omega(D, mQ) = r\), then \(C_\Omega(D, mQ) = W_r\). Therefore if \(W = \{u_1, \ldots, u_n\}\), then \(C(W) = C_\Omega(D, mQ)\). It is clear that we can correct errors up to the designed minimum distance \(\delta_{\text{FR}}(W)\). Hereafter \(g\) denotes the genus of the function field \(F\). By the Goppa bound we know that the minimum distance of \(C_\Omega(D, mQ)\) is greater than or equal to \(r + 1 - g\). But it is not clear whether \(\delta_{\text{FR}}(W) \geq r + 1 - g\). We shall show that \(\delta_{\text{FR}}(W) \geq r + 1 - g\), which is an immediate consequence of Proposition 3.2.

**Lemma 3.1:** If \(v_Q(g_i\omega_j) = v_Q(\omega_j)\), then \((u_i, v_j)\) is well-behaving and \(u_i \ast v_j \in W_s \setminus W_{s-1}\).

**Proof:** Let \(\omega \in \Omega(v_Q(\omega_j)Q - D)\). By the definition of \(\{w_1, \ldots, w_n\}\), we have

\[
\begin{cases}
\text{res}_{P_1}(\omega), \ldots, \text{res}_{P_n}(\omega) \in W_{s-1} & \text{if } v_Q(\omega) > v_Q(\omega_j), \\
\text{res}_{P_1}(\omega), \ldots, \text{res}_{P_n}(\omega) \in W_s \setminus W_{s-1} & \text{if } v_Q(\omega) = v_Q(\omega_j).
\end{cases}
\]

Since \(g_i\omega_j \in \Omega(v_Q(\omega_j)Q - D)\), \(u_i \ast v_j = (\text{res}_{P_1}(g_i\omega_j), \ldots, \text{res}_{P_n}(g_i\omega_j)) \in W_s \setminus W_{s-1}\). For all \(1 \leq u \leq i, 1 \leq v \leq j\) and \((u, v) \neq (i, j)\), we have \(g_i\omega_j \in \Omega(v_Q(\omega_j)Q - D)\) and \(v_Q(g_i\omega_j) > v_Q(\omega_j)\). Hence \(u_i \ast v_v = (\text{res}_{P_1}(g_i\omega_v), \ldots, \text{res}_{P_n}(g_i\omega_v)) \in W_{s-1}\). This completes the proof.

**Proposition 3.2:** \(\nu_s \geq s - g\).

**Proof:** We shall count the number of pairs \((f_i, \omega_j)\) such that \(v_Q(f_i\omega_j) = v_Q(\omega_s)\). For fixed \(\omega_j\) and \(\omega_s\), there
exists \( f_i \) such that \( v_Q(f_i \omega_j) = v_Q(\omega_i) \) if and only if \( v_Q(\omega_i) - v_Q(\omega_j) \in \{v_Q(f_i) \mid i = 1, 2, \ldots \} \). Since the number of nonpositive integers not in \( \{v_Q(f_i) \mid i = 1, 2, \ldots \} \) is \( g \), we have \( \#\{\omega_j \mid \text{there is no } f_i \text{ such that } v_Q(f_i \omega_j) = v_Q(\omega_i) \} \leq g \). Thus \( \#\{(f_i, \omega_j) \mid v_Q(f_i \omega_j) = v_Q(\omega_i) \} \geq s - g \).

Next we shall show that if \( v_Q(f_i \omega_j) = v_Q(\omega_i) \) then there exists an index \( i' \) such that \( f_i = g_{i'} \), which completes the proof by the previous lemma. Suppose that there is no \( i' \) such that \( f_i = g_{i'} \). Then \( (f_i(P_1), \ldots, f_i(P_n)) \) can be written as a linear combination of \( (f_u(P_1), \ldots, f_u(P_n)) \) for \( u = 1, \ldots, i - 1 \), which implies \( (\text{res}_{P_1}(\omega_1), \ldots, \text{res}_{P_n}(\omega_1)) \) can be written as a linear combination of \( (\text{res}_{P_1}(\omega_i), \ldots, \text{res}_{P_n}(\omega_i)) \) for \( i = 1, \ldots, s - 1 \) and \( (\text{res}_{P_1}(f_u \omega_1), \ldots, \text{res}_{P_n}(f_u \omega_1)) \) for \( u = 1, \ldots, i - 1 \). Hence \( (\text{res}_{P_1}(\omega_1), \ldots, \text{res}_{P_n}(\omega_1)) \in \mathbb{C}_1(D, (v_Q(\omega_1) + 1)Q) \), which is a contradiction. \( \square \)

**Remark 3.3:** By definition of \( \omega_i \), we can take any element in \( C_{11}(D, v_Q(\omega_1)Q) \setminus C_{12}(D, (v_Q(\omega_1) + 1)Q) \) as \( (\text{res}_{P_1}(\omega_1), \ldots, \text{res}_{P_n}(\omega_1)) = v_i = \omega_i \).

4. **Examples in which the \( \mathcal{L} \)-construction Gives Better Linear Codes in Certain Range of Parameters**

In this section we consider algebraic geometry codes on the algebraic function field defined by

\[
F_{16}(x_1, x_2, x_3), x_1^4 + x_2 = x_1^5, x_2^5 + x_3 = (x_2/x_1)^5,
\]

discovered by Garcia and Stichtenoth [3]. \( F_{16}(x_1, x_2, x_3) \) is of genus 57 and has 248 places of degree one. \( x_1 \) has a unique pole \( Q \) of degree one. Let \( D \) be the sum of all places of degree one except \( Q \). Let \( g_1, \ldots, g_{247}, \omega_1, \ldots, \omega_{247} \) be as in Sect. 3. \( g_1, \ldots, g_{247} \) are calculated in [18]. The number of check symbols and the designed minimum distance \( \delta_{FR} \) is compared in Fig. 1.

It is desirable to delete unnecessary rows in the check matrix as in Eq. (1). Performance of improved geometric Goppa codes of the \( \mathcal{L} \)-construction and the \( \Omega \)-construction is compared in Fig. 2.

**Remark 4.1:** For certain choices of a function field \( F \) (e.g. Hermitian function fields), a divisor \( D \), and a place \( Q \), there always exists an integer \( m' \) such that \( C_{11}(D, mQ) = C_{12}(D, m'Q) \) for all integer \( m \). In such a case the \( \mathcal{L} \)-construction does not provide better linear codes than the \( \Omega \)-construction. But such a condition does not usually hold.

**Remark 4.2:** AG codes plotted in Fig. 1 and Fig. 2 are not better than BCH codes of the same length.

5. **Conclusion**

We showed how to apply the Feng-Rao decoding algorithm and the Feng-Rao bound for \( C_{11}(D, mQ) \) to \( C_{12}(D, mQ) \). Then we showed that we can correct errors beyond the Goppa bound. Finally we presented examples in which the \( \mathcal{L} \)-construction gives better linear codes than the \( \Omega \)-construction in certain range of parameters.

It is a further research to find a more efficient decoding algorithm for \( C_{11}(D, mQ) \) than the Feng-Rao algorithm.
Fig. 2 Performance of improved geometric Goppa codes.

Acknowledgement

We thank Mr. Shinbashi at Sony Corporation Information & Network Technologies Laboratories for drawing our attention to this problem, and Prof. Sakaniwa for reading and criticizing the preliminary manuscript.

References