LETTER

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

Ryutaroh MATSUMOTO†, *Student Member and* **Shinji MIURA**††, *Member*

SUMMARY We show how to apply the Feng-Rao decoding algorithm and the Feng-Rao bound for the Ω-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 Ω-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, $P_1, \dots, P_n, Q$ pairwise distinct places of F with degree one, and $D := P_1 + \cdots + P_n$. Goppa [4] introduced the algebraic geometry code

$$C_\Omega(D, mQ) := \{(\mathrm{res}_{P_1}(\omega), \dots, \mathrm{res}_{P_n}(\omega)) \mid \omega \in \Omega(mQ - D)\},$$

which is called the Ω-construction. On the other hand, another kind of algebraic geometry code

$$C_\mathcal{L}(D, mQ) := \{(f(P_1), \dots, f(P_n)) \mid f \in \mathcal{L}(mQ)\},$$

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 $C_\Omega(D, m'Q)$ while their dimensions are the same, where F, D, Q are common to $C_\mathcal{L}(D, mQ)$ and $C_\Omega(D, m'Q)$. Thus it is worth considering $C_\mathcal{L}(D, mQ)$ as well for fixed F, D, Q.

Manuscript received November 26, 1999.
†The author is with the Department of Electrical and Electronic Engineering, Tokyo Institute of Technology, Tokyo, 152-8552 Japan. He is supported by JSPS Research Fellowships for Young Scientists.
††The author is with Sony Corporation Information & Network Technologies Laboratories, Tokyo, 141-0001 Japan.

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 Ω-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 $\{\boldsymbol{u}_1, \dots, \boldsymbol{u}_n\}$, $\{\boldsymbol{v}_1, \dots, \boldsymbol{v}_n\}$ and $\{\boldsymbol{w}_1, \dots, \boldsymbol{w}_n\}$ be bases of K^n. For $i = 1, \dots, n$, let $\mathcal{W}_i$ be the linear space spanned by $\{\boldsymbol{w}_1, \dots, \boldsymbol{w}_i\}$, with $\mathcal{W}_0 = \{0\}$ and $\mathcal{W}_{-1} = \emptyset$. For $\boldsymbol{a}$ and $\boldsymbol{b} \in K^n$, $\boldsymbol{a} * \boldsymbol{b} \in K^n$ denotes the componentwise product of $\boldsymbol{a}$ and $\boldsymbol{b}$.

Definition 2.1: A pair $(\boldsymbol{u}_i, \boldsymbol{v}_j)$ is said to be *well-behaving* if $\boldsymbol{u}_i * \boldsymbol{v}_j \in \mathcal{W}_s \setminus \mathcal{W}_{s-1}$ for some s and $\boldsymbol{u}_u * \boldsymbol{v}_v \in \mathcal{W}_{s-1}$ for all $1 \le u \le i$, $1 \le v \le j$, $(u, v) \ne (i, j)$.

A pair $(\boldsymbol{u}_i, \boldsymbol{v}_j)$ is said to be *weakly well-behaving* if $\boldsymbol{u}_i * \boldsymbol{v}_j \in \mathcal{W}_s \setminus \mathcal{W}_{s-1}$ for some s, $\boldsymbol{u}_u * \boldsymbol{v}_j \in \mathcal{W}_{s-1}$ for all $1 \le u < i$, and $\boldsymbol{u}_i * \boldsymbol{v}_v \in \mathcal{W}_{s-1}$ for all $1 \le v < j$.

Definition 2.2: For $s = 1, \dots, n$, we define ν_s (resp. λ_s) to be $\#\{(\boldsymbol{u}_i, \boldsymbol{v}_j) \mid (\boldsymbol{u}_i, \boldsymbol{v}_j)$ is well-behaving (resp. weakly well-behaving) and $\boldsymbol{u}_i * \boldsymbol{v}_j \in \mathcal{W}_s \setminus \mathcal{W}_{s-1}\}$.

Throughout this paper W denotes a nonempty proper subset of $\{\boldsymbol{w}_1, \dots, \boldsymbol{w}_n\}$. Let $C(W)$ be the dual code of the linear code generated by the elements in W.

We shall consider the minimum distance of $C(W)$ and a decoding algorithm for $C(W)$.

Definition 2.3: We define

$$\delta_{\mathrm{FR}}(W) := \min\{\nu_s \mid \boldsymbol{w}_s \notin W\},$$

$$\delta_{\mathrm{WFR}}(W) := \min\{\lambda_s \mid \boldsymbol{w}_s \notin W\}.$$

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

Proposition 2.4: The minimum distance of $C(W)$ is greater than or equal to δ_{WFR}.

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

$$S(\boldsymbol{y}) = \begin{pmatrix} \boldsymbol{u}_1 \\ \vdots \\ \boldsymbol{u}_n \end{pmatrix} \begin{pmatrix} y_1 & & \\ & \ddots & \\ & & y_n \end{pmatrix} \begin{pmatrix} \boldsymbol{v}_1 \\ \vdots \\ \boldsymbol{v}_n \end{pmatrix}^T.$$

Then the Hamming weight of $\boldsymbol{y}$ is equal to $\mathrm{rank}(S(\boldsymbol{y}))$, and the (i,j)-entry of $S(\boldsymbol{y})$ is equal to $\langle \boldsymbol{y}, \boldsymbol{u}_i * \boldsymbol{v}_j \rangle$, where $\langle , \rangle$ denotes the inner product.

Suppose that $\langle \boldsymbol{y}, \boldsymbol{w}_1 \rangle = \cdots = \langle \boldsymbol{y}, \boldsymbol{w}_{s-1} \rangle = 0$ and $\langle \boldsymbol{y}, \boldsymbol{w}_s \rangle \neq 0$ for some positive integer s. If $(\boldsymbol{u}_i, \boldsymbol{v}_j)$ is weakly well-behaving and $\boldsymbol{u}_i * \boldsymbol{v}_j \in \mathcal{W}_s \setminus \mathcal{W}_{s-1}$, then the (i,j)-entry of $S(\boldsymbol{y})$ is nonzero, because $\boldsymbol{u}_i * \boldsymbol{v}_j$ is a linear combination of $\boldsymbol{w}_1, \ldots, \boldsymbol{w}_s$ and the coefficient of $\boldsymbol{w}_s$ is nonzero. The (u,j) and (i,v)-entries are zero for all $1 \leq u < i$, $1 \leq v < j$, because $\boldsymbol{u}_u * \boldsymbol{v}_j$ and $\boldsymbol{u}_i * \boldsymbol{v}_v$ are linear combinations of $\boldsymbol{w}_1, \ldots, \boldsymbol{w}_{s-1}$. The number of weakly well-behaving $(\boldsymbol{u}_i, \boldsymbol{v}_j)$ such that $\boldsymbol{u}_i * \boldsymbol{v}_j \in \mathcal{W}_s \setminus \mathcal{W}_{s-1}$ is λ_s. Thus the Hamming weight of $\boldsymbol{y}$ $(= \mathrm{rank}(S(\boldsymbol{y})))$ is equal to or greater than λ_s.

Suppose further that $\boldsymbol{y}$ is a nonzero codeword in the linear code $C(W)$. Then $\boldsymbol{w}_s \notin W$, which completes the proof. □

Proposition 2.5: We can correct $\lfloor (\delta_{\mathrm{FR}}(W) - 1)/2 \rfloor$ 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:

- ν_s in our paper corresponds to ν_l in [6].
- The syndrome matrix $S(\boldsymbol{y})$ 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

$$W(d) := \{\boldsymbol{w}_s \mid \nu_s \leq d - 1\} \quad (1)$$

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 δ_{WFR} is strictly greater than δ_{FR}. Suppose that K is the finite field with 2 elements, $\{\boldsymbol{u}_1, \boldsymbol{u}_2\} = \{\boldsymbol{v}_1, \boldsymbol{v}_2\} = \{(1,0),(0,1)\}$, $\{\boldsymbol{w}_1, \boldsymbol{w}_2\} = \{(0,1),(1,0)\}$, and $W = \{\boldsymbol{w}_1\}$. Then $\delta_{\mathrm{FR}}(W) = 0$ but $\delta_{\mathrm{WFR}}(W) = 1$. We do not know an algebraic geometry code in which δ_{WFR} gives strictly better estimation than δ_{FR}.

Problem 2.7: It is an open problem to find an efficient decoding algorithm that corrects errors up to δ_{WFR}.

3. On the Feng-Rao Bound and the Goppa Bound for $C_{\mathcal{L}}(D, mQ)$

Let $\{a_1, \ldots, a_n\} := \{m \mid C_\Omega(D, mQ) \neq C_\Omega(D, (m+1)Q)\}$ such that $a_1 > a_2 > \cdots > a_n$. Choose $\omega_i \in \Omega(a_i Q - D)$ 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 $\{b_1, \ldots, b_n\} := \{m \mid C_{\mathcal{L}}(D, mQ) \neq C_{\mathcal{L}}(D, (m-1)Q)\}$ 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 $\boldsymbol{u}_i = (g_i(P_1), \ldots, g_i(P_n))$ and $\boldsymbol{v}_i = \boldsymbol{w}_i = (\mathrm{res}_{P_1}(\omega_i), \ldots, \mathrm{res}_{P_n}(\omega_i))$ for $i = 1, \ldots, n$, and apply the results in Sect. 2 to this setting. If $\dim C_\Omega(D, mQ) = r$, then $C_\Omega(D, mQ) = \mathcal{W}_r$. Therefore if $W = \{\boldsymbol{w}_1, \ldots, \boldsymbol{w}_r\}$, then $C(W) = C_{\mathcal{L}}(D, mQ)$. It is clear that we can correct errors up to the designed minimum distance $\delta_{\mathrm{FR}}(W)$. Hereafter g denotes the genus of the function field F. By the Goppa bound we know that the minimum distance of $C_{\mathcal{L}}(D, mQ)$ is greater than or equal to $r + 1 - g$. But it is not clear whether $\delta_{\mathrm{FR}}(W) \geq r + 1 - g$. We shall show that $\delta_{\mathrm{FR}}(W) \geq r + 1 - g$, which is an immediate consequence of Proposition 3.2.

Lemma 3.1: If $v_Q(g_i \omega_j) = v_Q(\omega_s)$, then $(\boldsymbol{u}_i, \boldsymbol{v}_j)$ is well-behaving and $\boldsymbol{u}_i * \boldsymbol{v}_j \in \mathcal{W}_s \setminus \mathcal{W}_{s-1}$.

Proof: Let $\omega \in \Omega(v_Q(\omega_s)Q - D)$. By the definition of $\{\boldsymbol{w}_1, \ldots, \boldsymbol{w}_n\}$, we have

$$\begin{cases} (\mathrm{res}_{P_1}(\omega), \ldots, \mathrm{res}_{P_n}(\omega)) \in \mathcal{W}_{s-1} \\ \qquad\qquad \text{if } v_Q(\omega) > v_Q(\omega_s), \\ (\mathrm{res}_{P_1}(\omega), \ldots, \mathrm{res}_{P_n}(\omega)) \in \mathcal{W}_s \setminus \mathcal{W}_{s-1} \\ \qquad\qquad \text{if } v_Q(\omega) = v_Q(\omega_s). \end{cases}$$

Since $g_i \omega_j \in \Omega(v_Q(\omega_s)Q - D)$, $\boldsymbol{u}_i * \boldsymbol{v}_j = (\mathrm{res}_{P_1}(g_i\omega_j), \ldots, \mathrm{res}_{P_n}(g_i\omega_j)) \in \mathcal{W}_s \setminus \mathcal{W}_{s-1}$. For all $1 \leq u \leq i$, $1 \leq v \leq j$ and $(u,v) \neq (i,j)$, we have $g_u \omega_v \in \Omega(v_Q(\omega_s)Q - D)$ and $v_Q(g_u \omega_v) > v_Q(\omega_s)$. Hence $\boldsymbol{u}_u * \boldsymbol{v}_v = (\mathrm{res}_{P_1}(g_u\omega_v), \ldots, \mathrm{res}_{P_n}(g_u\omega_v)) \in \mathcal{W}_{s-1}$. This completes the proof. □

Proposition 3.2: $\nu_s \geq s - g$.

Proof: We shall count the number of pairs (f_i, ω_j) such that $v_Q(f_i \omega_j) = v_Q(\omega_s)$. For fixed ω_j and ω_s, there

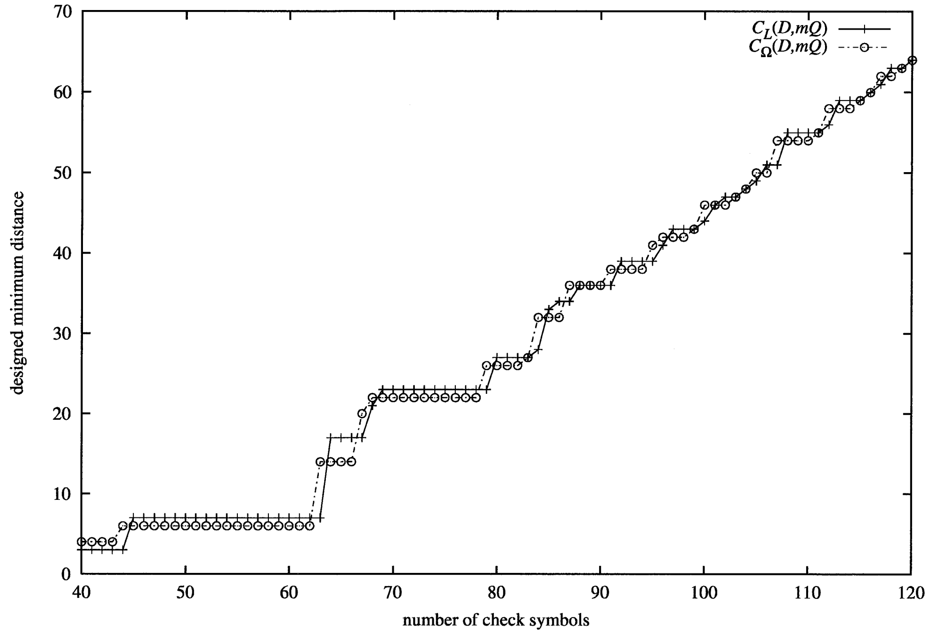

Fig. 1 Performance of $C_{\mathcal{L}}(D, mQ)$ and $C_\Omega(D, mQ)$.

exists f_i such that $v_Q(f_i\omega_j) = v_Q(\omega_s)$ if and only if $v_Q(\omega_s) - v_Q(\omega_j) \in \{v_Q(f_i) \mid i = 1, 2, \ldots\}$. Since the number of nonpositive integers not in $\{v_Q(f_i) \mid i = 1, 2, \ldots\}$ is g, we have $\#\{\omega_j \mid$ there is no f_i such that $v_Q(f_i\omega_j) = v_Q(\omega_s)\} \leq g$. Thus $\#\{(f_i, \omega_j) \mid v_Q(f_i\omega_j) = v_Q(\omega_s)\} \geq s - g$.

Next we shall show that if $v_Q(f_i\omega_j) = v_Q(\omega_s)$ 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 $(\mathrm{res}_{P_1}(\omega_s), \ldots, \mathrm{res}_{P_n}(\omega_s))$ can be written as a linear combination of $(\mathrm{res}_{P_1}(\omega_\ell), \ldots, \mathrm{res}_{P_n}(\omega_\ell))$ for $\ell = 1, \ldots, s-1$ and $(\mathrm{res}_{P_1}(f_u\omega_j), \ldots, \mathrm{res}_{P_n}(f_u\omega_j))$ for $u = 1, \ldots, i-1$. Hence $(\mathrm{res}_{P_1}(\omega_s), \ldots, \mathrm{res}_{P_n}(\omega_s)) \in C_\Omega(D, (v_Q(\omega_s)+1)Q)$, which is a contradiction. □

Remark 3.3: By definition of ω_i, we can take any element in $C_\Omega(D, v_Q(\omega_i)Q) \setminus C_\Omega(D, (v_Q(\omega_i)+1)Q)$ as $(\mathrm{res}_{P_1}(\omega_i), \ldots, \mathrm{res}_{P_n}(\omega_i)) = \boldsymbol{v}_i = \boldsymbol{w}_i$.

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

$$\mathbf{F}_{16}(x_1, x_2, x_3), x_2^4 + x_2 = x_1^5, x_3^4 + x_3 = (x_2/x_1)^5,$$

discovered by Garcia and Stichtenoth [3]. $\mathbf{F}_{16}(x_1, x_2, x_3)$ 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 δ_{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 Ω-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 $C_{\mathcal{L}}(D, mQ) = C_\Omega(D, m'Q)$ for all integer m. In such a case the $\mathcal{L}$-construction does not provide better linear codes than the Ω-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 $C_\Omega(D, mQ)$ to $C_{\mathcal{L}}(D, mQ)$. 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 Ω-construction in certain range of parameters.

It is a further research to find a more efficient decoding algorithm for $C_{\mathcal{L}}(D, mQ)$ than the Feng-Rao algorithm.

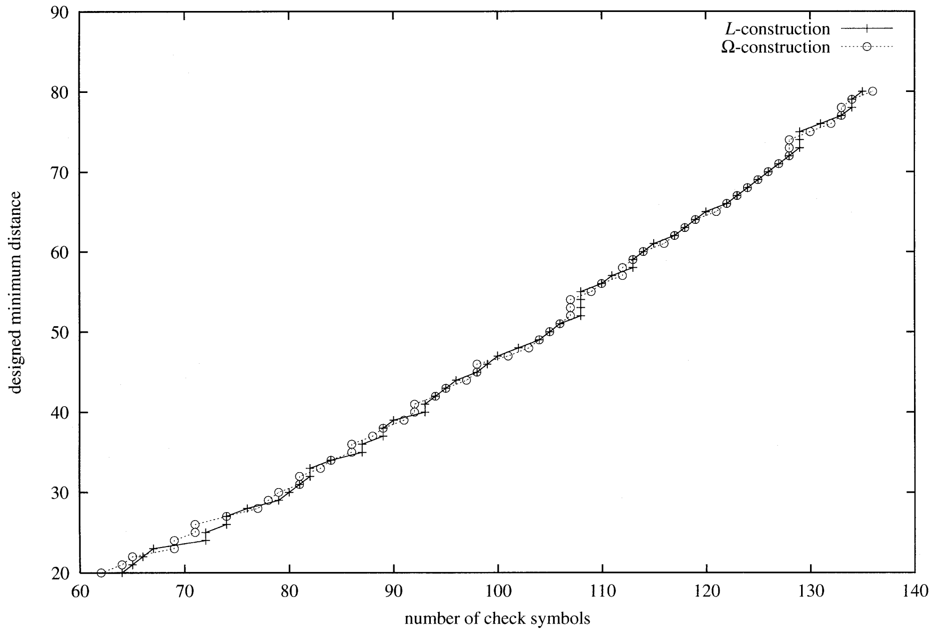

Fig. 2 Performance of improved geometric Goppa codes.

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

[1] G.L. Feng and T.R.N. Rao, "Decoding algebraic geometric codes up to the designed minimum distance," IEEE Trans. Inform. Theory, vol.39, no.1, pp.36–47, 1993.
[2] G.L. Feng and T.R.N. Rao, "Improved geometric Goppa codes part I, basic theory," IEEE Trans. Inf. Theory, vol.41, no.6, pp.1678–1693, 1995.
[3] A. Garcia and H. Stichtenoth, "A tower of Artin-Schreier extensions of function fields, attaining the Drinfeld-Vladut bound," Invent. Math., vol.121, pp.211–222, 1995.
[4] V.D. Goppa, "Codes on algebraic curves," Soviet Math. Dokl., vol.24, no.1, pp.170–172, 1981.
[5] T. Høholdt, J.H. van Lint, and R. Pellikaan, "Order functions and evaluation codes," Proc. AAECC-12, Lecture Notes in Computer Science, vol.1255, pp.138–150, Springer-Verlag, 1997.
[6] T.Høholdt, J.H. van Lint, and R. Pellikaan, "Algebraic geometry codes," in Handbook of Coding Theory, eds. V. Pless and W.C. Huffman, pp.871–961, Elsevier, 1998.
[7] C. Kirfel and R. Pellikaan, "The minimum distance of codes in an array coming from telescopic semigroups," IEEE Trans. Inf. Theory, vol.41, no.6, pp.1720–1732, 1995.
[8] J.H. van Lint and T.A. Springer, "Generalized Reed-Solomon codes from algebraic geometry," IEEE Trans. Inf. Theory, vol.IT-33, no.3, pp.305–309, 1987.
[9] S. Miura, Ph.D. thesis, Univ. Tokyo, May 1997.
[10] S. Miura, "Linear codes on affine algebraic varieties," IEICE Trans., vol.J81-A, no.10, pp.1386–1397, Oct. 1998.
[11] R. Pellikaan, "The shift bound for cyclic, Reed-Muller and geometric Goppa codes," in Arithmetic, Geometry and Coding Theory, eds. R. Pelikkan, M. Perret, and S.G. Vlăduţ, Walter de Gruyter, pp.155–174, 1996.
[12] S. Sakata, D.A. Leonard, H. Elbrønd Jensen, and T. Høholdt, "Fast erasure-and-error decoding of algebraic geometry codes up to the Feng-Rao bound," IEEE Trans. Inf. Theory, vol.44, no.4, pp.1558–1564, 1998.
[13] B.-Z. Shen and K.K. Tzeng, "A code decomposition approach for decoding cyclic and algebraic-geometric codes," IEEE Trans. Inf. Theory, vol.41, no.6, pp.1969–1987, 1995.
[14] B.-Z. Shen and K.K. Tzeng, "Generation of matrices for determining minimum distance and decoding of algebraic-geometric codes," IEEE Trans. Inf. Theory, vol.41, no.6, pp.1703–1708, 1995.
[15] H. Stichtenoth, "Self-dual Goppa codes," J. Pure Appl. Algebra, vol.55, pp.199–211, 1988.
[16] H. Stichtenoth, Algebraic function fields and codes, Springer-Verlag, 1993.
[17] M.A. Tsfasman and S.G. Vlăduţ, Algebraic-geometric codes, Kluwer Academic Publishers, 1991.
[18] D. Umehara and T. Uyematsu, "One-point algebraic geometric codes from Artin-Schreier extensions of Hermitian function fields," IEICE Trans. Fundamentals, vol.E81-A, no.10, pp.2025–2031, Oct. 1998.