

AIMS Mathematics, 7(6): 9656–9667. DOI: 10.3934/math.2022537 Received: 18 September 2021 Revised: 02 March 2022 Accepted: 03 March 2022 Published: 15 March 2022

http://www.aimspress.com/journal/Math

Research article

Locally recoverable codes in Hermitian function fields with certain types of divisors

Boran Kim*

Department of Mathematics Education, Kyungpook National University, 80 Daehakro, Bukgu, Daegu 41566, Korea

* Correspondence: Email: bkim21@knu.ac.kr.

Abstract: A locally recoverable code with locality **r** can recover the missing coordinate from at most **r** symbols. The locally recoverable codes have attracted a lot of attention because they are more advanced coding techniques that are applied to distributed and cloud storage systems. In this work, we focus on locally recoverable codes in Hermitian function fields over \mathbb{F}_{q^2} , where *q* is a prime power. With a certain type of divisor, we obtain an improved lower bound of the minimum distance for locally recoverable codes in Hermitian function fields. For doing this, we give explicit formulae of the dimension for some divisors of Hermitian function fields. We also present a standard that tells us when a divisor with certain places suggests an improved lower bound.

Keywords: algebraic geometry LRC code; Hermitian function field **Mathematics Subject Classification:** Primary 11T71, Secondary 11G20

1. Introduction

The *locally recoverable codes* (*LRC codes* for short) have been significantly studied because of their techniques which can repair the lost data by a local procedure. Local recovery techniques enable find one value that is erased by accessing the other symbols in the code. Formally, an LRC code $C \subseteq \mathbb{K}^n$ of length **n** with locality **r** can recover the missing coordinate from at most **r** symbols, where \mathbb{K} is a finite field. The LRC codes have attracted a lot of attention because they are more advanced coding techniques that are applied to distributed and cloud storage systems. Most parts of many previous works deal with construction methods [2, 4, 6, 7, 9, 11] and bounds of the minimum distances [1–3, 5, 10, 12] for LRC codes.

In coding theory, many researchers consider various constructions to obtain good codes; a code with a large minimum distance for the given length and dimension. One of them is a Reed-Solomon code, and the code can be viewed as a special code of an algebraic geometry code; Reed-Solomon code is

one of the practical codes in this area. Many works obtain remarkable results from algebraic geometry codes on various algebraic curves. Naturally, LRC codes can be considered on algebraic geometry curves with their constructions and the bound of minimum distances [1, 2, 4, 6, 9]. These codes are called *algebraic geometry locally recoverable codes* (shortly *AG LRC codes*). In the previous results, for constructing AG LRC codes, a divisor consists of a unique place of a certain algebraic function field (such as, [1, 2, 11]). We focus on this point; we deal with a divisor with two places of the Hermitian function field in this work. From this, we get the advantage that is an improvement of the bound for the minimum distance of an AG LRC code in Hermitian function field.

The goal of this work is twofold. First, we present explicit formulae for the dimension of divisors G_1 and G_2 with a certain one place and two places of the Hermitian function field, respectively. Both the dimension and the lower bound b(C(G, h)) of minimum distance for AG LRC codes C(G, h) are related with the dimension dim(G) and degree deg(G) of a divisor G. In detail, with $dim(G_1) = dim(G_2)$, if $deg(G_2) < deg(G_1)$, then $b(C(G_2, h))$ is bigger than $b(C(G_1, h))$. It means that under certain conditions, a divisor G_2 with two places give better result for the bound than the result of a divisor G_1 with one place. Second, we provide a family of AG LRC codes in Hermitian function fields. The code has an improved the lower bound of minimum distance using a divisor with a certain two places. We present an explicit standard that tells us when a divisor with a certain two places suggests an improved lower bound.

Layout of the paper This paper is organized as follows. In Section 2, we introduce the notations and known facts for this work. Section 3 presents the dimensions of certain types of divisors of Hermitian function fields over \mathbb{F}_{q^2} , where q is a prime power. These results are explicit formulae for obtaining the dimensions of the divisors. In Section 4, we obtain a family of algebraic geometry locally recoverable codes in Hermitian function fields with an improved bounds for minimum distances using a certain type of divisor. We suggest the standard when we can get an improved bound for AG LRC codes.

2. Preliminaries

A *linear code* of length **n** over a finite field \mathbb{K} is a subspace of \mathbb{K}^n ; briefly, we call a *code* in this paper. A *codeword* is an element of the code. If a code is a *k*-dimensional subspace of \mathbb{K}^n , then the code is called $[\mathbf{n}, \mathbf{k}]$ code. The next definition is about *locally recoverable code with locality* **r**.

Definition 2.1. Let *C* be an $[\mathbf{n}, \mathbf{k}]$ code over a finite field \mathbb{K} , and $[n] := \{1, ..., n\}$. Given $a \in \mathbb{K}$, let $C(i, a) = \{(c_1, ..., c_n) \in C \mid c_i = a\}$. Then *C* is said to have **locality** \mathbf{r} if for every $i \in [\mathbf{n}]$, there is a set $A_i \subset [\mathbf{n}] \setminus \{i\}$ with $|A_i| \leq \mathbf{r}$ such that

$$C_{A_i}(i,a) \cap C_{A_i}(i,\tilde{a}) = \emptyset$$
 for all $a \neq \tilde{a} \in \mathbb{K}$,

(the notation $C_{A_i}(i, a)$ is the restriction of C(i, a) to the coordinates of A_i). This code is called a **locally** recoverable code (shortly, LRC code) with locality r. We use the notation (n, k, r) to present the parameters of the code.

By using an LRC code *C*, we can find any coordinate of $c \in C$ from at most **r** other coordinates of *c*. In particular, if an *i*-th coordinate c_i of $c = (c_1, ..., c_n) \in C$ is erased, then we can recover the codeword by considering its coordinates in A_i . Here, the set A_i is called a *recovering set* for the coordinate c_i .

We briefly introduce construction for *algebraic geometry locally recoverable codes* over a finite field \mathbb{K} (see [1, 2, 11]). Let *X* and *Y* be smooth projection absolutely irreducible curves over \mathbb{K} . We

denote the rational function field on X (resp. Y) by F(X) (resp. F(Y)). Let $h : X \to Y$ be a rational separable map of curves of degree $\mathbf{r} + 1$. Under those settings, there is a function $x \in F(X)$ such that F(X) = F(Y)(x) because the map h is separable. The function x gives the equation $x^{\mathbf{r}+1} + b_{\mathbf{r}}x^{\mathbf{r}} + \cdots + b_0 = 0$, where $b_i \in F(Y)$. Moreover, x is considered as a map $x : X \to \mathbb{P}^1(\mathbb{K})$, where $\mathbb{P}^1(\mathbb{K})$ is a projective line over \mathbb{K} . We define an algebraic geometry locally recoverable code under the followings:

- $S = \{P_1, \dots, P_s\} \in F(Y)$ is a subset of \mathbb{K} -rational points of Y.
- *G* is a positive divisor such that the support of *G* is different from *S*.
- $A = h^{-1}(S) = \{P_{ij}, 0 \le i \le \mathbf{r}, 1 \le j \le s\} \subseteq F(X)$ (i.e., $h(P_{ij}) = P_j$ for all i, j).
- { $f_i \in F(Y) : 1 \le i \le m$ } is a basis of $\mathcal{L}(G)$.
- *V* is \mathbb{K} -subspace of F(Y) of dimension **r***m* generated by $\{f_i x^i, 0 \le i \le \mathbf{r} 1, 1 \le j \le m\}$
- ev_A is the evaluation map $V \to \mathbb{K}^{(r+1)s}$ such that $f \mapsto (f(P_{ij}), 0 \le i \le \mathbf{r}, 1 \le j \le s)$.

The set of images $(f(P_{ij}), 0 \le i \le \mathbf{r}, 1 \le j \le s)$ is a linear code of length $(\mathbf{r} + 1)s$ over \mathbb{K} which is called an **algebraic geometry locally recoverable code** (shortly, **AG LRC code**), denote by C(G, h). The code coordinates are partitioned into *s* subsets $A_j = \{P_{ij}, 0 \le i \le \mathbf{r}\}$ $(1 \le j \le s)$ of size $\mathbf{r} + 1$ each. If one symbol $f(P_{ij})$ is erased in the codeword, then this can be recoverable through polynomial interpolation using the points of the recovering set A_j . We denote deg(G) is degree of a divisor *G*, and dim(G) is dimension of a divisor *G*.

Lemma 2.2. [2, Theorem 3.1] The subspace $C(G, h) \in \mathbb{K}^{(r+1)s}$ forms an $(\mathbf{n}, \mathbf{k}, \mathbf{r})$ linear LRC code with the parameters

$$\mathbf{n} = (\mathbf{r}+1)s, \mathbf{k} = \mathbf{r}dim(G), d \ge \mathbf{n} - deg(G)(\mathbf{r}+1) - (\mathbf{r}-1)deg(x),$$

where *d* is the minimum distance. Local recovery of an erased symbol $F(P_{ij})$ can be found by polynomial interpolation through the points of the recovery set A_i .

In this paper, we consider the Hermitian curve χ over \mathbb{F}_{q^2} . The *Hermitian function field* $H := \mathbb{F}_{q^2}(x, y)/\mathbb{F}_{q^2}$ with the defining equation

$$\chi : y^q + y = x^{q+1}$$

over \mathbb{F}_{q^2} , where *q* is a prime power. The Hermitian function field has $q^3 + 1$ places of degree 1. Let P_{∞} be the point at infinity (0 : 1 : 0) of χ , and $P_{0,0}$ be the point zero point (0 : 0 : 1) of χ . For any $(\alpha, \beta) \in \mathbb{F}_{q^2}^2$ on χ , there is a unique rational point $P_{\alpha,\beta}$ which is the common zero of $x - \alpha$ and $y - \beta$. The genus of the Hermitian function field *H* is equal to $\frac{q(q-1)}{2}$.

In Hermitian function field over \mathbb{F}_{q^2} , let $h : \chi \to \mathbb{P}^1(\mathbb{F}_{q^2})$ is the natural projection defined by h(x, y) = y; then $deg(h) = q = \mathbf{r} + 1$. Let $G = tP_{\infty}$ be a positive divisor, where $P_{\infty} \in \chi$ is a unique over the point at infinity $\infty \in \mathbb{P}^1(\mathbb{F}_{q^2})$. Take $S = \mathbb{F}_{q^2}$.

Lemma 2.3. [2, Proposition 4.1] There is a family of an AG LRC codes C(G, h) in Hermitian function field over \mathbb{F}_{q^2} with locality $\mathbf{r} = q - 1$ which satisfies

$$\mathbf{n} = q^3$$
, $\mathbf{k} = \mathbf{r}dim(G)$, and $\mathbf{d} \ge b(C(G, h)) = n - deg(G)(\mathbf{r} + 1) - (\mathbf{r} - 1)(\mathbf{r} + 2)$.

The minimum distance **d** *of* C(G, h) *has the lower bound* b(C(G, h))*.*

AIMS Mathematics

3. Dimensions of divisors of Hermitian function fields

In Section 3, we focus on the dimensions of divisors of Hermitian function fields over \mathbb{F}_{q^2} , where q is a prime power. The following lemma is about the dimension dim(G) of a divisor G of Hermitian function field.

Lemma 3.1. [8, Theorem 3.6] Let H be the Hermitian function field over \mathbb{F}_{q^2} , where q is a prime power. Let $G = rP_{\infty} + \sum_{\beta \in K_{\alpha}} k_{\beta}P_{\alpha,\beta}$ be a divisor, where $\alpha \in \mathbb{F}_{q^2}$, $r \in \mathbb{Z}$, and $k_{\beta} \in \mathbb{Z}$ for each $\beta \in K_{\alpha}$. The dimension dim(G) of G is given by

$$dim(G) = \sum_{i=0}^{q} max\left\{ \left\lfloor \frac{r-iq}{q+1} \right\rfloor + \sum_{\beta \in K_{\alpha}} \left\lfloor \frac{k_{\beta}+i}{q+1} \right\rfloor + 1, 0 \right\} \le r + \sum_{\beta \in K_{\alpha}} k_{\beta} + 1.$$
(3.1)

Using Lemma 3.1, we give explicit formulae for dimensions of divisors G_1 and G_2 which consist of one place P_{∞} and two places P_{∞} and $P_{0,0}$ of Hermitian function field H over \mathbb{F}_{q^2} , respectively. For comparing $dim(G_1)$ and $dim(G_2)$, we need to have explicit formulae in Lemmas 3.2 and 3.5. In Section 4, it will be crucial parts for obtaining one of our main results. First, we deal with a divisor which consists of two places P_{∞} and $P_{0,0}$ of H.

Lemma 3.2. Let q be a prime power. Let u and k be integers such that $u \ge 0$ and $k \ge 1$. Set $r = (q + 1)u + \tau \ge 1$, where $0 \le \tau \le q$. Let $\tilde{\epsilon}_k = k \pmod{q+1}$ and $\epsilon_k = \lfloor \frac{k}{q+1} \rfloor$. Then for fixed r and k, the values $\lfloor \frac{r-iq}{q+1} \rfloor + \lfloor \frac{k+i}{q+1} \rfloor + 1$ can be calculated by the following formulae for all $0 \le i \le q$:

Case 1. Suppose that $\tau = 0$ *.*

(i) If
$$\tilde{\epsilon}_k = 0$$
, then $\lfloor \frac{r-iq}{q+1} \rfloor + \lfloor \frac{k+i}{q+1} \rfloor + 1 = u - i + \epsilon_k + 1$ for $0 \le i \le q$.
(ii) If $\tilde{\epsilon}_k \ge 1$, then

$$\left\lfloor \frac{r-iq}{q+1} \right\rfloor + \left\lfloor \frac{k+i}{q+1} \right\rfloor + 1 = \begin{cases} u-i+\epsilon_k+1 & \text{if } 0 \le i \le q-\tilde{\epsilon}_k, \\ u-i+\epsilon_k+2 & \text{if } q-\tilde{\epsilon}_k+1 \le i \le q. \end{cases}$$

Case 2. Suppose that $\tau \ge 1$ *.*

(*i*) If $\tilde{\epsilon}_k = \tau$, then

$$\left\lfloor \frac{r-iq}{q+1} \right\rfloor + \left\lfloor \frac{k+i}{q+1} \right\rfloor + 1 = \begin{cases} u-i+\epsilon_k+1 & \text{if } 0 \le i \le q-\tilde{\epsilon}_k, \\ u-i+\epsilon_k+3 & \text{if } q-\tilde{\epsilon}_k+1 \le i \le q. \end{cases}$$

(*ii*) If $\tilde{\epsilon}_k \neq \tau$, then

$$\left\lfloor \frac{r-iq}{q+1} \right\rfloor + \left\lfloor \frac{k+i}{q+1} \right\rfloor + 1 = \begin{cases} u-i+\epsilon_k+1 & \text{if } 0 \le i \le q - \max\{\tau, \tilde{\epsilon}_k\}, \\ u-i+\epsilon_k+2 & \text{if } q - \max\{\tau, \tilde{\epsilon}_k\} + 1 \le i \le q - \min\{\tau, \tilde{\epsilon}_k\}, \\ u-i+\epsilon_k+3 & \text{if } q - \min\{\tau, \tilde{\epsilon}_k\} + 1 \le i \le q. \end{cases}$$

Proof. We note that the integer k can be written as $k = \epsilon_k(q+1) + \tilde{\epsilon}_k$.

Case 1 (i). $\tau = 0$: suppose that $\tilde{\epsilon}_k \ge 1$.

AIMS Mathematics

- If $0 \le i \le q \tilde{\epsilon}_k$, then $\left\lfloor \frac{r-iq}{q+1} \right\rfloor = u i$ since $1 \le r iq (u i)(q + 1) = i \le q \tilde{\epsilon}_k$. Moreover, $\left\lfloor \frac{k+i}{q+1} \right\rfloor = \left\lfloor \frac{\epsilon_k(q+1)+\tilde{\epsilon}_k+i}{q+1} \right\rfloor = \epsilon_k$ because $1 < \tilde{\epsilon}_k + i \le q$. Hence we have $\left\lfloor \frac{r-iq}{q+1} \right\rfloor + \left\lfloor \frac{k+i}{q+1} \right\rfloor + 1 = u i + \epsilon_k + 1$.
- If $q \tilde{\epsilon}_k + 1 \le i \le q$, then $\left\lfloor \frac{r-iq}{q+1} \right\rfloor = u i$ and $\left\lfloor \frac{k+i}{q+1} \right\rfloor = \epsilon_k + 1$ since $q + 1 \le \tilde{\epsilon}_k + i \le \tilde{\epsilon}_k + q \le 2q$.

Case 1 (ii). $\tau = 0$: if $\tilde{\epsilon}_k = 1$, then we obtain the result by the similar way as Case 1 (i). Case 2 (i). $\tau \ge 1$: suppose that $\tilde{\epsilon}_k > \tau$.

- If $q \tau + 1 \le i \le q$, then $\left\lfloor \frac{r-iq}{q+1} \right\rfloor = u i + 1$ since $0 \le r iq (u i + 1)(q + 1) = (\tau q 1) + i < q$. Similarly, we have that $\left\lfloor \frac{k+i}{q+1} \right\rfloor = \left\lfloor \frac{\epsilon_k(q+1)+\tilde{\epsilon}_k+i}{q+1} \right\rfloor = \epsilon_k + 1$ as above.

Case 2 (ii). $\tau \ge 1$: $\tilde{\epsilon}_k < \tau$, the result can be proved by the similar way as Case 2 (i).

Case 3. $\tau \ge 1$: For $\tilde{\epsilon}_k = \tau$, we can also have the result; in detail, when $q - \tilde{\epsilon}_k + 1 \le i \le q$, $\left\lfloor \frac{r-iq}{q+1} \right\rfloor = u - i + 1$ and $\left\lfloor \frac{k+i}{q+1} \right\rfloor = \left\lfloor \frac{\epsilon_k(q+1) + \tilde{\epsilon}_k + i}{q+1} \right\rfloor = \epsilon_k + 1$ as above.

By Lemma 3.2, for a divisor $G_2 = rP_{\infty} + kP_{0,0}$ of Hermitian function field H over \mathbb{F}_{q^2} , we obtain the dimension $dim(G_2)$ of G_2 explicitly.

Theorem 3.3. Let $G_2 = rP_{\infty} + kP_{0,0}$ be a divisor of Hermitian function field H over \mathbb{F}_{q^2} , where r and k are integers such that $r \ge 1$ and $k \ge 1$. For fixed r and k, let $\Gamma_{i,r,k} := \lfloor \frac{r-iq}{q+1} \rfloor + \lfloor \frac{k+i}{q+1} \rfloor + 1$ be the value determined by Lemma 3.2 for all $0 \le i \le q$. Then the dimension $\dim(G_2)$ of G_2 is $\sum_{i=0}^{q} \max\{\Gamma_{i,r,k}, 0\}$.

Proof. The values $\Gamma_{i,r,k} = \lfloor \frac{r-iq}{q+1} \rfloor + \lfloor \frac{k+i}{q+1} \rfloor + 1$ are determined for all cases by Lemma 3.2. By Lemma 3.1, the dimension $dim(G_2)$ of G_2 is $\sum_{i=0}^{q} \max\{\Gamma_{i,r,k}, 0\}$.

We present the following example.

Example 3.4. Let H be the Hermitian function field over \mathbb{F}_{8^2} (i.e., q = 8). Let $G_2 = rP_{\infty} + kP_{0,0}$ be a divisor of H, where r and k are integers such that $r \ge 1$ and $k \ge 1$. Set $r = u(q+1) + \tau = 9u + \tau$, where $0 \le \tau \le 8$ and $u \ge 0$.

For example, we focus on u = 4 and k = 5; thus $r = 36 + \tau$ with $0 \le \tau \le 8$. The dimension dim (G_2) of $G_2 = (36 + \tau)P_{\infty} + 5P_{0,0}$ ($0 \le \tau \le 8$) can be calculated by Magma program as follows:

$$dim(G_2) = \begin{cases} 17 & for \ 0 \le \tau \le 2, \\ 18 & for \ \tau = 3, \\ 19 & for \ \tau = 4, \\ 20 & for \ \tau = 5, \\ 21 & for \ \tau = 6, \\ 22 & for \ \tau = 7, \\ 23 & for \ \tau = 8. \end{cases}$$
(3.2)

AIMS Mathematics

Now, we check if our results in Theorem 4.1 are true; if our formulae give the same results as (3.2), *then these are correct. In Lemma 3.2, we obtain the values*

$$\Gamma_{i,r,k} = \left\lfloor \frac{r - iq}{q + 1} \right\rfloor + \left\lfloor \frac{k + i}{q + 1} \right\rfloor + 1 = \left\lfloor \frac{36 + \tau - 8i}{9} \right\rfloor + \left\lfloor \frac{k + i}{9} \right\rfloor + 1;$$
(3.3)

here, $\epsilon_k = \lfloor \frac{k}{9} \rfloor = 0$ and $\tilde{\epsilon}_k = k = 5$.

(i) $\tau = 0$: in this case, we get that $[\Gamma_{i,36+\tau,5}]_{i=0}^{8} = [5,4,3,2,2,1,0,-1,-2]$ since

$$\Gamma_{i,36+\tau,5} = \begin{cases} 5-i & \text{for } 0 \le i \le 3, \\ 6-i & \text{for } 4 \le i \le 8, \end{cases}$$

by (3.3) and Case 1 (ii) of Lemma 3.2. Hence, $\sum_{i=0}^{8} \max\{\Gamma_{i,36+\tau,5}, 0\} = 17$ in Theorem 3.3. (ii) $\tau = \tilde{\epsilon}_k = 5$: we have

$$\Gamma_{i,36+\tau,5} = \begin{cases} 5-i & \text{for } 0 \le i \le 3, \\ 7-i & \text{for } 4 \le i \le 8, \end{cases}$$

by (3.3) and Case 2 (i) of Lemma 3.2. Hence, we calculate the values as $[\Gamma_{i,36+\tau,5}]_{i=0}^{8} = [5,4,3,2,3,2,1,0,-1]$ and $\sum_{i=0}^{8} \max\{\Gamma_{i,36+\tau,5},0\} = 20$ in Theorem 3.3.

(iii) $\tau \neq \tilde{\epsilon}_k \geq 1$: this case is matched with Case 2 (ii) of Lemma 3.2. So we obtain

$$\Gamma_{i,36+\tau,5} = \begin{cases} 5-i & \text{for } 0 \le i \le 8 - \max\{\tau, 5\}, \\ 6-i & \text{for } 8 - \max\{\tau, 5\} + 1 \le i \le 8 - \min\{\tau, 5\}, \\ 7-i & \text{for } 8 - \min\{\tau, 5\} + 1 \le i \le 8. \end{cases}$$

By calculation for each cases,

$$\sum_{i=0}^{8} \max\{\Gamma_{i,36+\tau,5}, 0\} = \begin{cases} 17 & \text{for } \tau = 1 \text{ or } \tau = 2\\ 18 & \text{for } \tau = 3,\\ 19 & \text{for } \tau = 4,\\ 21 & \text{for } \tau = 6,\\ 22 & \text{for } \tau = 7,\\ 23 & \text{for } \tau = 8. \end{cases}$$

By (i), (ii) and (iii), we can check the results of Lemma 3.2 and Theorem 3.3 are correct.

From now on, we focus on a divisor $G_1 = (r+k+\ell)P_{\infty}$ which consists of one point P_{∞} of Hermitian function field over \mathbb{F}_{q^2} .

Lemma 3.5. Let q be a prime power. Let u, k and ℓ be integers such that $u \ge 0$, $k \ge 1$ and $\ell \ge 1$. Set $r = (q+1)u + \tau \ge 1$, where $0 \le \tau \le q$. Let $\tilde{\delta}_{k,\ell,\tau} = k + \tau + \ell \pmod{q+1}$ and $\delta_{k,\ell,\tau} = \left\lfloor \frac{k+\tau+\ell}{q+1} \right\rfloor$. Then for fixed r, k and ℓ , the values $\lfloor \frac{r+k+\ell-iq}{q+1} \rfloor$ can be calculated by the following formulae for all $0 \le i \le q$:

(*i*) If
$$\tilde{\delta}_{k,\ell,\tau} = 0$$
, then $\lfloor \frac{r+k+\ell-iq}{q+1} \rfloor + 1 = u - i + \delta_{k,\ell,\tau} + 1$ for $0 \le i \le q$.

AIMS Mathematics

Volume 7, Issue 6, 9656–9667.

(*ii*) If $\tilde{\delta}_{k,\ell,\tau} \geq 1$, then

$$\left\lfloor \frac{r+k+\ell-iq}{q+1} \right\rfloor + 1 = \begin{cases} u-i+\delta_{k,\ell,\tau}+1 & \text{if } 0 \le i \le q-\tilde{\delta}_{k,\ell,\tau}, \\ u-i+\delta_{k,\ell,\tau}+2 & \text{if } q-\tilde{\delta}_{k,\ell,\tau}+1 \le i \le q. \end{cases}$$

Proof. First, the value $k + \tau + \ell$ can be written as $k + \tau + \ell = \delta_{k,\ell,\tau}(q+1) + \tilde{\delta}_{k,\ell,\tau}$. Here,

$$r + k + \ell - iq = (u - i)q + u + k + \tau + \ell,$$

= $(u - i)q + u + \delta_{k,\ell,\tau}(q + 1) + \tilde{\delta}_{k,\ell,\tau}$

Then $(r + k + \ell - iq) - (u - i)(q + 1) = \delta_{k,\ell,\tau}(q + 1) + \tilde{\delta}_{k,\ell,\tau} + i$ and

$$\left\lfloor \frac{r+k+\ell-iq}{q+1} \right\rfloor = \left\lfloor \frac{(u-i+\delta_{k,\ell,\tau})(q+1)+\tilde{\delta}_{k,\ell,\tau}+i}{q+1} \right\rfloor$$
(3.4)

by the previous equations.

- (i) If $\tilde{\delta}_{k,\ell,\tau} = 0$, then the value $\lfloor \frac{r+k+\ell-iq}{q+1} \rfloor = u i + \delta_{k,\ell,\tau}$ since $0 \le \tilde{\delta}_{k,\ell,\tau} + i \le q$ by (3.4) and $0 \le i \le q$.
- (ii) Suppose that $\tilde{\delta}_{k,\ell,\tau} \ge 1$. If $0 \le i \le q \tilde{\delta}_{k,\ell,\tau}$, then $\lfloor \frac{r+k+\ell-iq}{q+1} \rfloor = u i + \delta_{k,\ell,\tau}$ for $0 \le i \le q \tilde{\delta}_{k,\ell,\tau}$ by (3.4). For $q \tilde{\delta}_{k,\ell,\tau} + 1 \le i \le q$, we have that $\lfloor \frac{r+k+\ell-iq}{q+1} \rfloor = u i + \delta_{k,\ell,\tau} + 1$ by $q + 1 \le \tilde{\delta}_{k,\ell,\tau} + i \le 2q$ and (3.4).

From (i) and (ii), the results are follow.

Lemma 3.5, for a divisor $G_1 = (r + k + \ell)P_{\infty}$ of Hermitian function field *H* over \mathbb{F}_{q^2} , present the explicit formula for the dimension $dim(G_1)$ of G_1 .

Theorem 3.6. Let $G_1 = (r+k+\ell)P_{\infty}$ be a divisor of Hermitian function field H over \mathbb{F}_{q^2} , where r, k and ℓ are integers such that $r \ge 1$, $k \ge 1$ and $\ell \ge 1$. For fixed r, k and ℓ , let $\tilde{\Gamma}_{i,r,k,\ell} = \left\lfloor \frac{r+k+\ell-iq}{q+1} \right\rfloor + 1$ be the value determined by Lemma 3.5 for all $0 \le i \le q$. Then the dimension $\dim(G_1)$ of G_1 is $\sum_{i=0}^{q} \max\{\tilde{\Gamma}_{i,r,k,\ell}, 0\}$.

Proof. Lemma 3.5 determines the all values $\tilde{\Gamma}_{i,r,k,\ell} = \left\lfloor \frac{r+k+\ell-iq}{q+1} \right\rfloor + 1$. By Lemma 3.1, the dimension $dim(G_1)$ of G_1 is $\sum_{i=0}^{q} \max\{\tilde{\Gamma}_{i,r,k,\ell}, 0\}$.

The following examples say our results (Lemma 3.5 and Theorem 3.6) are true.

Example 3.7. Let *H* be the Hermitian function field over \mathbb{F}_{8^2} (i.e., q = 8). Let $G_1 = (r + k + \ell)P_{\infty}$ be a divisor of *H*, where *r*, *k*, and ℓ are positive integers. Set $r = u(q+1) + \tau = 9u + \tau \ge 1$, where $0 \le \tau \le 8$. For instance, we consider u = 1, $\tau = 0$, k = 1 and $1 \le \ell \le 8$; thus r = 9.

The dimension $\dim(G_1)$ of the divisor $G_1 = (10 + \ell)P_{\infty}$ is calculated by Magma program as

$$dim(G_1) = \begin{cases} 3 & for \ 1 \le \ell \le 5, \\ 4 & for \ \ell = 6, \\ 5 & for \ \ell = 7, \\ 6 & for \ \ell = 8. \end{cases}$$
(3.5)

From now on, we check our results are matched with (3.5); if these are matched, then Lemma 3.5 and Theorem 3.6 are correct. By Lemma 3.5, we calculate the values $\lfloor \frac{r+k+\ell-iq}{q+1} \rfloor + 1 = \lfloor \frac{10+\ell-8i}{9} \rfloor + 1$ as follows: first, $\tilde{\delta}_{k,\tau} = k + \tau + \ell = \ell + 1 \pmod{9}$.

AIMS Mathematics

Volume 7, Issue 6, 9656–9667.

(a) $\ell = 1$: we have $\tilde{\delta}_{k,\tau} = \ell + 1 = 2$ and $\delta_{k,\tau} = 0$. Furthermore, the sequence $[\tilde{\Gamma}_{i,9,1,1}]_{i=0}^{8}$ is obtained

$$[\tilde{\Gamma}_{i,9,1,1}]_{i=0}^8 = [2, 1, 0, -1, -2, -3, -4, -4, -5]$$

since

$$\tilde{\Gamma}_{i,9,1,1} = \begin{cases} 2 - i & \text{for } 0 \le i \le 6, \\ 3 - i & \text{for } 7 \le i \le 8. \end{cases}$$

Hence, by Lemma 3.5, $\sum_{i=0}^{8} \max{\{\tilde{\Gamma}_{i,9,1,1}, 0\}} = 2 + 1 = 3.$

(b) $2 \le \ell \le 7$: by Lemma 3.5, we get the following results as the same reason:

$$([\tilde{\Gamma}_{i,9,1,\ell}]_{i=0}^{8}, \sum_{i=0}^{8} \max\{\tilde{\Gamma}_{i,9,1,\ell}, 0\}) = \begin{cases} ([2,1,0,-1,-2,-3,-3,-4,-5],3) & for \ \ell = 2, \\ ([2,1,0,-1,-2,-2,-3,-4,-5],3) & for \ \ell = 3, \\ ([2,1,0,-1,-1,-2,-3,-4,-5],3) & for \ \ell = 4, \\ ([2,1,0,0,-1,-2,-3,-4,-5],3) & for \ \ell = 5, \\ ([2,1,1,0,-1,-2,-3,-4,-5],4) & for \ \ell = 6, \\ ([2,2,1,0,-1,-2,-3,-4,-5],5) & for \ \ell = 7. \end{cases}$$

(c) $\ell = 8$: the values $\tilde{\delta}_{k,\tau} = 0$ and $\delta_{k,\tau} = 1$ are obtained. And then $[\tilde{\Gamma}_{i,9,1,\ell}]_{i=0}^{8} = [3, 2, 1, 0, -1, -2, -3, -4, -5]$. That is, $\sum_{i=0}^{8} \max\{\tilde{\Gamma}_{i,9,1,8}, 0\} = 3 + 2 + 1 = 6$.

The results in (a), (b) and (c) are matched with (3.5) by Theorem 3.6, that is, our results of Lemma 3.5 and Theorem 3.6 are correct. \Box

4. LRC codes with two-point divisors

In this section, we consider the lower bounds of minimum distances for AG LRC codes in Hermitian function fields over \mathbb{F}_{q^2} (q: a prime power). We set that $G_1 = (r + k + \ell)P_{\infty}$ is a divisor, and $G_2 = rP_{\infty} + kP_{0,0}$ is a divisor, where r, k, and ℓ are integers such that $r \ge 1$, $k \ge 1$ and $\ell \ge 1$; then $deg(G_1) = r + k + \ell > deg(G_2) = r + k$. We compare the lower bounds of minimum distances of AG LRC codes $C(G_1, h)$ and $C(G_2, h)$; the map h is introduced in Section 2.

As we can see in Lemma 2.2, both the dimension and the lower bound for minimum distance of C(G, h) are related to deg(G) and dim(G). We use a divisor G_2 for obtaining an improved lower bound for minimum distance of AG LRC codes. The key point is that we find the divisors G_2 satisfying both $dim(G_2) = dim(G_1)$ and $deg(G_2) < deg(G_1)$; and then, $b(C(G_2, h))$ is bigger than $b(C(G_1, h))$ with $dim(C(G_1, h)) = dim(C(G_2, h))$.

In Lemma 4.1, we give an exact standard to check when $deg(G_1) > deg(G_2)$ with $dim(G_1) = dim(G_2)$. It means that this lemma tells us when we can get an improved lower bound of minimum distance for AG LRC codes in Hermitian function field over \mathbb{F}_{q^2} (q: a prime power).

Lemma 4.1. Let *H* be the Hermitian function field over \mathbb{F}_{q^2} , where *q* is a prime power. Let $\tilde{\delta}_{k,\ell,\tau} = k + \tau + \ell \pmod{q+1}$, $\tilde{\epsilon}_k = k \pmod{q+1}$, and $\delta_{k,\ell,\tau} = \lfloor \frac{k+\tau+\ell}{q+1} \rfloor$, where *k*, ℓ and τ are non-negative integers ($k \ge 1, \ell \ge 1$ and $0 \le \tau \le q$). Let $G_1 = (r+k+\ell)P_{\infty}$ and $G_2 = rP_{\infty} + kP_{0,0}$ be divisors of *H*,

AIMS Mathematics

where $r = u(q + 1) + \tau \ge 1$ with a non-negative integer u. Suppose that $\tilde{\epsilon}_k + \tau + \ell < q + 1$. Then

$$\delta_{k,\ell,\tau} + \tilde{\delta}_{k,\ell,\tau} \leq q - u - 1$$
 if and only if $deg(G_1) > deg(G_2)$ and $dim(G_1) = dim(G_2)$.

Proof. As in the previous lemmas and theorems of Section 3, we denote the followings: $\tilde{\delta}_{k,\ell,\tau} = k + \tau + \ell \pmod{q+1}$, $\tilde{\delta}_{k,\ell,\tau} = \lfloor \frac{k+\tau+\ell}{q+1} \rfloor$, $\tilde{\epsilon}_k = k \pmod{q+1}$, and $\epsilon_k = \lfloor \frac{k}{q+1} \rfloor$.

First, we check that the condition $\tilde{\epsilon}_k + \tau + \ell < q + 1$ is necessary. If $\tilde{\epsilon}_k + \tau + \ell \ge q + 1$, then we have that for $k + \ell + \tau = (q + 1)\epsilon_k + \tilde{\epsilon}_k + \ell + \tau$,

$$\delta_{k,\ell,\tau} \ge \epsilon_k + 1 \tag{4.1}$$

since $\tilde{\epsilon}_k + \ell + \tau \ge q + 1$ and $\delta_{k,\ell,\tau} = \left\lfloor \frac{k+\tau+\ell}{q+1} \right\rfloor = \left\lfloor \frac{(q+1)\epsilon_k+\tilde{\epsilon}_k+\ell+\tau}{q+1} \right\rfloor \ge \epsilon_k + 1$. In this case, we obtain that $\Gamma_{0,r,k} = u + \epsilon_k + 1$, and $\tilde{\Gamma}_{0,r,k,\ell} = u + \delta_{k,\ell,\tau} + 1 \ge u + \epsilon_k + 2$; the value $\Gamma_{0,r,k}$ is from Lemma 3.2, and $\tilde{\Gamma}_{0,r,k,\ell}$ is given by (4.1) and Lemma 3.5 (for i = 0). It means that $dim(G_1) > dim(G_2)$ by Theorems 3.3 and 3.6. Hence, we should assume that $\tilde{\epsilon}_k + \tau + \ell < q + 1$.

By the following two cases, we prove our results.

(i) Suppose that $\tilde{\epsilon}_k = 0$. We have that $\tilde{\delta}_{k,\ell,\tau} = k + \tau + \ell \pmod{q+1} = \tau + \ell$; this is because $k + \ell + \tau = (q+1)\epsilon_k + \tilde{\epsilon}_k + \ell + \tau$ and $\tilde{\epsilon}_k + \ell + \tau = \ell + \tau < q + 1$. It follows that

$$\delta_{k,\ell,\tau} = \epsilon_k = \left\lfloor \frac{k}{q+1} \right\rfloor. \tag{4.2}$$

Then we have

$$\Gamma_{i,r,k} = u - i + \epsilon_k + 1 \text{ for all } 0 \le i \le q, \tag{4.3}$$

and

$$\tilde{\Gamma}_{i,r,k,\ell} = \begin{cases} u - i + \epsilon_k + 1 & \text{for } 0 \le i \le q - \tilde{\delta}_{k,\ell,\tau}, \\ u - i + \epsilon_k + 2 & \text{for } q - \tilde{\delta}_{k,\ell,\tau} + 1 \le i \le q, \end{cases}$$
(4.4)

by (4.2), Lemmas 3.2 and 3.5.

We claim that $dim(G_1) = dim(G_2)$ if and only if $u - i + \epsilon_k + 2 \le 0$ for $i = q - \tilde{\delta}_{k,\ell,\tau} + 1$. Suppose that $dim(G_1) = dim(G_2)$. In (4.4), $u - i + \epsilon_k + 2 \le 0$ for $i = q - \tilde{\delta}_{k,\ell,\tau} + 1$ since $\epsilon_k = \delta_{k,\ell,\tau}$. That is, $\delta_{k,\ell,\tau} + \tilde{\delta}_{k,\ell,\tau} \le q - u - 1$; if not, clearly we have $dim(G_1) > dim(G_2)$.

Conversely, if $\delta_{k,\ell,\tau} + \hat{\delta}_{k,\ell,\tau} \le q - u - 1$, then we say that $u - i + \epsilon_k + 2 \le 0$ for $q - \hat{\delta}_{k,\ell,\tau} + 1 = i$. This implies $u - i + \epsilon_k + 1 \le 0$ for $q - \tilde{\delta}_{k,\ell,\tau} + 1 \le i \le q$. Hence

$$dim(G_1) = \sum_{i=0}^{q-\tilde{\delta}_{k,\ell,\tau}} \max\{\tilde{\Gamma}_{i,r,k,\ell}, 0\} = \sum_{i=0}^{q-\tilde{\delta}_{k,\ell,\tau}} \max\{\Gamma_{i,r,k}, 0\} = dim(G_2)$$
(4.5)

since $\tilde{\Gamma}_{i,r,k,\ell} = \Gamma_{i,r,k} = u - i + \epsilon_k + 1$ for $0 \le i \le q - \tilde{\delta}_{k,\ell,\tau}$ by (4.3) and (4.4). Thus we obtain the result.

(ii) Suppose that $1 \leq \tilde{\epsilon}_k \leq q$. The similar arguments show that $\tilde{\delta}_{k,\ell,\tau} = k + \ell + \tau \pmod{q+1} = \tilde{\epsilon}_k + \ell + \tau$. Hence $\delta_{k,\ell,\tau} = \epsilon_k$ is also followed. As (i), the results are obtained.

AIMS Mathematics

In Lemma 2.3, a divisor with one place P_{∞} is considered to construct AG LRC code. In our work, we use a divisor $G_2 = rP_{\infty} + kP_{0,0}$ with two places P_{∞} and $P_{0,0}$, where r and k are integers such that $r \ge 1$ and $k \ge 1$; by Lemma 2.2, we can constructing AG LRC codes with a divisor G_2 . And we set a divisor $G_1 = (r + k + \ell)P_{\infty}$ with a place P_{∞} . An AG LRC code $C(G_2, h)$ in Hermitian function field over \mathbb{F}_{q^2} has the length $\mathbf{n} = q^2(q - 1)$ since we should take $S = \mathbb{F}_{q^2} \setminus \{0\}$ (See Section 2). We compare the lower bounds of minimum distances for AG LRC codes $C(G_1, h)$ and $C(G_2, h)$; under certain conditions, we say that the lower bound of minimum distance for $C(G_2, h)$ is better than the bound for $C(G_1, h)$.

Theorem 4.2. Let *H* be the Hermitian function field over \mathbb{F}_{q^2} . Let b(C(G,h)) be the lower bound of minimum distance for an AG LRC code C(G,h). Set $G_1 = (r + k + \ell)P_{\infty}$ and $G_2 = rP_{\infty} + kP_{0,0}$ are divisors of *H* satisfying $deg(G_1) > deg(G_2)$ and $dim(G_1) = dim(G_2)$ (the divisors G_1 and G_2 can be determined by Lemma 4.1). There is a family of AG LRC codes $C(G_2,h)$ in *H* over \mathbb{F}_{q^2} which satisfy

 $dim(C(G_2, h)) = dim(C(G_1, h))$ and $b(C(G_2, h)) > b(C(G_1, h))$,

that is, the bound $b(C(G_2, h))$ of minimum distance for $C(G_2, h)$ is better than the bound $b(C(G_1, h))$ of minimum distance for $C(G_1, h)$.

Proof. By Lemma 2.2, both the dimension and the lower bound of minimum distance for an AG LRC code on Hermitian curve can be obtained. First, dimensions of codes $C(G_1, h)$ and $C(G_2, h)$ are the same; the dimension of the codes are $\mathbf{r}dim(G_1)$ and $\mathbf{r}dim(G_2)$, respectively. That is, we have $dim(C(G_1, h)) = dim(C(G_2, h))$.

Furthermore, the lower bound of minimum distance for an AG LRC code C(G, h) is improving when deg(G) is getting smaller by Lemma 2.2. In our settings, $deg(G_1) = r + k + \ell$ and $deg(G_2) = r + k$ with $\ell \ge 1$, that is, $deg(G_1) > deg(G_2)$. So we get that $b(C(G_2, h)) > b(C(G_1, h))$. We proved the results.

The following examples stand for Lemma 4.1 and Theorem 4.2.

Example 4.3. The dimensions of divisors $G_1 = (r + k + \ell)P_{\infty}$ and $G_2 = rP_{\infty} + kP_{0,0}$ are double checked by Magma software; the results are matched with ours.

(i) Let H be the Hermitian function field over \mathbb{F}_{7^2} , that is, q = 7. Set $\ell = 1$; then $deg(G_1) = deg((r+k+\ell)P_{\infty})$ is equal to $deg(G_2) + 1 = deg(rP_{\infty} + kP_{0,0}) + 1$. In the followings, we will check

$$\tilde{\epsilon}_k + \tau + \ell < q + 1 \text{ and } \delta_{k,\ell,\tau} + \tilde{\delta}_{k,\ell,\tau} \le q - u - 1.$$

$$(4.6)$$

For instance, we consider r = 9 and k = 8. Thus,

$$deg(G_1) = 18 > deg(G_2) = 17.$$

We obtain u = 1 and $\tau = 1$ since $r = u(q + 1) + \tau$ in our settings in Lemma 4.1. Then we have $\tilde{\epsilon}_k = 0$, $\tilde{\delta}_{k,\ell,\tau} = k + \tau + \ell \pmod{8} = 2$, and $\delta_{k,\ell,\tau} = \lfloor \frac{10}{8} \rfloor = 1$. Thus, (4.6) is satisfied. By Lemma 4.1,

$$dim(G_1) = dim(G_2) = 6$$

the second equality is from Lemma 3.5 (ii) and Theorem 3.6.

AIMS Mathematics

(ii) Let H be the Hermitian function field over \mathbb{F}_{13^2} (i.e., q = 13). Set $\ell = 8$, r = 29 and K = 14; it means that

$$deg(G_1) = 69 > deg(G_2) = 61.$$

Then $\tau = 1$, u = 2, $\tilde{\epsilon}_k = 0$ and $\tilde{\delta}_{k,\ell,\tau} = 9$ and $\delta_{k,\ell,\tau} = 1$. Clearly, the above values satisfy (4.6). Similarly, by Lemma 3.5 and Theorem 3.6, we have

$$dim(G_1) = dim(G_2) = 10.$$

As a result, in both (i) and (ii),

 $dim(C(G_1, h)) = dim(C(G_2, h))$ and $b(C(G_2, h)) > b(C(G_1, h))$

by Lemma 2.2; that is, the lower bound $b(C(G_2, h))$ of minimum distance for $C(G_2, h)$ is better than the lower bound $b(C(G_1, h))$ of minimum distance for $C(G_1, h)$.

Remark 4.4. We can find many cases that satisfy conditions of Lemma 4.1. We calculate the number of divisors which are convincing cases for our results.

For examples, for $2 \le q \le 15$ and $1 \le u, \tau, k \le 50$ (q: a prime power), we get that

the number of divisors
$$G_2 = \begin{cases} 1391 & \text{for } \ell = 1, \\ 1024 & \text{for } \ell = 2, \\ 717 & \text{for } \ell = 3, \\ 474 & \text{for } \ell = 4, \\ 293 & \text{for } \ell = 5, \end{cases}$$

where the divisor G_2 satisfies the conditions of Lemma 4.1. Hence, using these divisors G_2 , we can improve the lower bound of minimum distance for AG LRC codes on Hermitian curve over \mathbb{F}_{q^2} . And so on, we can find more cases on the other ranges for q, u, τ , k and ℓ .

5. Conclusions

We study locally recoverable codes in Hermitian function fields over \mathbb{F}_{q^2} (*q*: a prime power). We give explicit formulae of the dimension for some divisors of Hermitian function fields. From this, we obtain an improved lower bound of the minimum distance for locally recoverable codes in Hermitian function fields with a certain type of divisor. These results can be extended to various algebraic function fields in future research.

Acknowledgments

We would like to thank the reviewers for their helpful comments for improving the clarity of this paper. Boran Kim is supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (NRF-2021R1C1C2012517).

Conflict of interest

The authors declare no conflict of interest.

References

- 1. E. Ballico, C. Marcolla, Higher hamming weights for locally recoverable codes on algebraic curves, *Finite Fields Th. App.*, **40** (2016), 61–72. https://doi.org/10.1016/j.ffa.2016.03.004
- 2. A. Barg, I. Tamo, S. Vlăduţ, Locally recoverable codes on algebraic curves, *IEEE T. Inform. Theory*, **63** (2017), 4928–4939. https://doi.org/10.1109/TIT.2017.2700859
- 3. P. Gopalan, C. Huang, H. Simitci, S. Yekhanin, On the locality of codeword symbols, *IEEE T. Inform. theory*, **58** (2012), 6925–6934. https://doi.org/10.1109/TIT.2012.2208937
- 4. L. Jin, H. Kan, Y. Zhang, Constructions of locally repairable codes with multiple recovering sets via rational function fields. *IEEE T. Inform. Theory*, **66** (2019), 202–209. https://doi.org/10.1109/TIT.2019.2946627
- 5. S. Kruglik, K. Nazirkhanova, A. Frolov, New bounds and generalizations of locally recoverable codes with availability, *IEEE T. Inform. Theory*, **65** (2019), 4156–4166. https://doi.org/10.1109/TIT.2019.2897705.
- X. Li, L. Ma, C. Xing, Optimal locally repairable codes via elliptic curves, *IEEE T. Inform. Theory*, 65 (2018), 108–117. https://doi.org/10.1109/TIT.2018.2844216
- 7. Y. Luo, C. Xing, C. Yuan, Optimal locally repairable codes of distance 3 and 4 via cyclic codes, *IEEE T. Inform. Theory*, **65** (2018), 1048–1053. https://doi.org/10.1109/TIT.2018.2854717
- H. Maharaj, G. L. Matthews, G. Pirsic, Riemann-roch spaces of the hermitian function field with applications to algebraic geometry codes and low-discrepancy sequences, *J. Pure Appl. Algebra*, 195 (2005), 261–280. https://doi.org/10.1016/j.jpaa.2004.06.010
- 9. C. Munuera, W. Tenório, F. Torres, Locally recoverable codes from algebraic curves with separated variables, *Adv. Math. Commun.*, **14** (2020), 265. https://doi.org/10.1587/bplus.14.265
- 10. I. Tamo, A. Barg, Bounds on locally recoverable codes with multiple recovering sets, In: 2014 *IEEE International Symposium on Information Theory*, 2014, 691–695.
- 11. I. Tamo, A. Barg, A family of optimal locally recoverable codes, *IEEE T. Inform. Theory*, **60** (2014), 4661–4676. https://doi.org/10.1109/TIT.2014.2321280
- 12. A. Wang, Z. Zhang, Repair locality with multiple erasure tolerance, *IEEE T. Inform. Theory*, **60** (2014), 6979–6987. https://doi.org/10.1109/TIT.2014.2351404



© 2022 the Author(s), licensee AIMS Press. This is an open access article distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0)