

LOCALLY RECOVERABLE CODES FROM TOWERS OF FUNCTION FIELDS

M. CHARA, F. GALLUCCIO AND E. MARTÍNEZ-MORO

ABSTRACT. In this work we construct sequences of locally recoverable AG codes arising from a tower of function fields and give bound for the parameters of the obtained codes. In a particular case of a tower over \mathbb{F}_{q^2} for any odd q , defined by Garcia and Stichtenoth in [3], we show that the bound is sharp for the first code in the sequence, and we include a detailed analysis for the following codes in the sequence based on the distribution of rational places that split completely in the considered function field extension.

Key words: Function fields, Towers, Codes, LRC, Asymptotic behavior

2020 Mathematical Subject Classification: 94B27, 14H05, 11G20, 11T71

1. INTRODUCTION

Let q be a prime power. A linear code \mathcal{C} of length n over the finite field \mathbb{F}_q with q elements is a linear subspace of \mathbb{F}_q^n . The dimension of the code k is the dimension of \mathcal{C} as a \mathbb{F}_q -vector space and its minimum distance d is the minimum of the number of non-zero entries of a vector in $\mathcal{C} \setminus \{\mathbf{0}\}$. A linear code \mathcal{C} of length n and dimension k is a locally recoverable error-correcting code, (LRC for short) with locality r if it is a code that produces an n -coordinate codeword from k information symbols and, for any coordinate of the codeword, there exist at most r other coordinates that allow to recover the lost coordinate. LRCs were introduced in [4] motivated by the significant use of coding techniques applied to data distribution and cloud storage systems, since local recovery techniques enable us to repair lost encoded data by making use of small amount of data within the received vector instead of all information.

One of the problems of interest in the field is the construction of long non trivial codes, in which the ground field cardinality is not much larger than the code length. It is well known that one way of obtaining long codes is by the use of algebraic curves with many rational points, or equivalently, algebraic function fields with many rational places. In this work we are interested in working with this type of algebraic-geometry codes (AG codes for short), or codes coming from the evaluation of rational points on an algebraic curve over \mathbb{F}_q , (see Section 2 for precise

This work is partially supported by CONICET, ANPCyT PICT, UNL CAI+D 2020. First autor was partially funded by Research in Pairs Fellowship - CIMPA 2021. Second author was partially funded by a doctoral grant of the program Erasmus+ KA 107. Third author was supported in part by Grant PGC2018-096446-B-C21 funded by MCIN/AEI/ 10.13039/501100011033 and by “ERDF A way of making Europe”.

M. Chara: Researcher of CONICET at FIQ, Universidad Nacional del Litoral, Argentina

F. Galluccio: Universidad Nacional del Litoral and CONICET, Argentina

E. Martínez-Moro: Institute of Mathematics, Universidad de Valladolid, Spain.

definitions). In this direction, Barg, Tamo and Vladut [1] constructed algebraic-geometry locally recoverable codes, generalizing previous works of Barg and Tamo [9, 10]. Haymaker, Malmskog and Matthews in [5], used fiber products of maximal curves to construct LRC with availability, giving in this way a generalization of [1] for more than one recovery set.

Since we aim to build sequences of AG codes that are also LR codes, we will work with towers $\mathcal{F} = (F_0, F_1, \dots)$ of function fields over the same finite field \mathbb{F}_q , in the way defined by Garcia and Stichtenoth (see for example [3, 8]). By using these type of asymptotically optimal towers, Tamo, Barg and Frolov in [11] gave a construction of asymptotically good locally recoverable codes over \mathbb{F}_{q^2} with locality $r = q - 1$ whose rate R and relative distance δ satisfy the following equation

$$(1) \quad R \geq \frac{r}{r+1} \left(1 - \delta - \frac{3}{q+1} \right).$$

In our work, we also employ the Garcia-Stichtenoth function field given in [3] to build asymptotically good LRCs. Our method can be viewed as an extension of the construction given in [1]. Furthermore, our construction allows to compute the exact dimension of the code in several steps on the tower, using a different evaluation set but in this case, although we can improve the dimension, we have a cost to pay in the bound for the minimum distance. Nevertheless, we are able to construct a family of LRC over \mathbb{F}_{q^2} with locality $r = q - 1$ whose rate R and relative distance δ satisfy

$$(2) \quad R \geq \frac{r}{r+1} \left(1 - \delta - \frac{2}{q} \right),$$

which improves the asymptotic Gilbert-Varshamov type bound for LRCs with a single recovery given by (1). This bound is a particular case of the bound given by Li, Ma and Xing in [6], in which they use the same tower and the automorphism group of the function fields involved to build asymptotically good LRCs. Nevertheless, note that the main difference with this work is that we are able to compute the exact dimension of the constructed codes.

This work is organized as follows. In Section 2 we give some preliminary definitions and facts on the behavior of towers of function fields. Section 3 is devoted to build locally recoverable codes from a tower of function fields, see Theorem 3.4. Determining the exact minimum distance of linear codes can be a hard problem. In particular, few results are known for the exact minimum distance of LRCs. In [2], this problem is addressed by using the construction given in [5], and analyzing relative parameters. In Section 4, and in particular in Propositions 4.1 and 4.2, we compute the exact minimum distance of the constructed codes in one step extension of the tower, and we show that the method used to compute this distance will not be enough to compute the minimum distance in further steps. Finally, in the last section of this paper, we compute some asymptotic parameters and show the improvements mentioned in Equation (2).

2. PRELIMINARIES

Throughout this work, we will use the terminology of function fields for defining AG-codes (instead of algebraic curves). An algebraic function field F over \mathbb{F}_q is a finite algebraic extension of the rational function field $\mathbb{F}_q(x)$, where x is a

transcendental element over \mathbb{F}_q . For a complete introduction on algebraic function field and their relationship with codes see for example [8].

Let D and $S = P_1 + \cdots + P_n$ be two disjoint divisors of an algebraic function field F over \mathbb{F}_q , where P_1, \dots, P_n are different rational places of F , and consider the Riemann-Roch space associated to D

$$\mathcal{L}(D) = \{f \in F \setminus \{0\} : (f) \geq -D\} \cup \{0\},$$

where (f) denotes the principal divisor of $f \in F$. The algebraic-geometry code defined by F , D and S is

$$C = C_{\mathcal{L}}(S, D) = \{(f(P_1), f(P_2), \dots, f(P_n)) \in \mathbb{F}_q^n : f \in \mathcal{L}(D)\},$$

where $f(P_i)$ stands for the residue class of f modulo P_i , $i = 1, \dots, n$.

Since our aim is to build infinite sequences of AG codes that are also LR codes, we will work with infinite sequences of function fields. For fixing our notation and settings we will use the following definitions.

Definition 1. We will consider sequences $\mathcal{F} = (F_0, F_1, \dots)$, of function fields over the same finite field \mathbb{F}_q such that

1. $F_0 \subsetneq F_1 \subsetneq F_2 \subsetneq \cdots$,
2. the field extension F_{i+1}/F_i is finite and separable for all $i \geq 0$, and
3. \mathbb{F}_q is the full constant field of each F_i for all $i \geq 0$, i.e., the only elements of F_i which are algebraic over \mathbb{F}_q are the elements of \mathbb{F}_q .

Following the works of Garcia and Stichtenoth (see for example [3], [8]), we will say that the sequence \mathcal{F} is a *tower of function fields over \mathbb{F}_q* , if the genus $g(F_i)$ grows to infinity as $i \rightarrow \infty$.

Definition 2. A sequence (or a tower) $\mathcal{F} = (F_0, F_1, \dots)$ is *recursively defined* if there exist a bivariate polynomial $f \in \mathbb{F}_q[S, T]$ and transcendental elements x_i $i = 1, 2, \dots$, such that for all $i \geq 0$ the following statements hold:

1. $F_0 = \mathbb{F}_q(x_0)$ is the rational function field.
2. $F_{i+1} = F_i(x_{i+1})$ with $f(x_i, x_{i+1}) = 0$.
3. $[F_{i+1} : F_i] = \deg_T f$.

The following definitions are important in the study of the asymptotic behavior of sequences of function fields. As usual, we will denote by $\mathbb{P}(F)$ the set of all places of the function field F/\mathbb{F}_q . Given a finite extension E/F and a place $P \in \mathbb{P}(F)$ there are finitely many places $Q \in \mathbb{P}(E)$ lying above P . We will write $Q|P$ when Q lies over P . If $\mathcal{F} = (F_0, F_1, \dots)$ is a sequence of function fields over \mathbb{F}_q , we say that a place $P \in \mathbb{P}(F_i)$ *splits completely* in \mathcal{F} if P splits completely in each extension F_j/F_i (and in this case we have $[F_j : F_i]$ different places over P). The *splitting locus* of \mathcal{F} over F_0 is defined as

$$\text{Split}(\mathcal{F}/F_0) := \{P \in \mathbb{P}(F_0) : \deg(P) = 1 \text{ and } P \text{ splits completely in } \mathcal{F}\},$$

where $\deg(P)$ is the degree of the place P . A place $P \in \mathbb{P}(F_i)$ is *ramified* in \mathcal{F} if P is ramified in any extension F_j/F_i . The *ramification locus* of \mathcal{F} over F_0 is the set

$$\text{Ram}(\mathcal{F}/F_0) := \{P \in \mathbb{P}(F_0) : P \text{ ramified in some extension } F_n/F_0\}.$$

A place $P \in \mathbb{P}(F_i)$ is *totally ramified* in \mathcal{F} if P is totally ramified in each extension F_j/F_i (in this case we have only one place Q in $\mathbb{P}(F_j)$ over P and the ramification

index $e(Q|P)$ is equal to $[F_j : F_i]$. The *complete ramification locus* of \mathcal{F} over F_0 is defined as

$$\text{CRam}(\mathcal{F}/F_0) := \{P \in \mathbb{P}(F_0) : \deg(P) = 1 \text{ and } P \text{ is totally ramified in } \mathcal{F}\}.$$

Since every place $Q \in \mathbb{P}(F_i)$ lying above a place in $\text{Split}(\mathcal{F}/F_0) \cup \text{CRam}(\mathcal{F}/F_0)$ is a rational place (i.e. of degree one), we have that

$$(3) \quad N(F_i) \geq [F_i : F_0] |\text{Split}(\mathcal{F}/F_0)| + |\text{CRam}(\mathcal{F}/F_0)|,$$

where $N(F_i)$ is the number of rational places of F_i .

Lemma 2.1. *If \mathcal{F} is a sequence such that $\text{Split}(\mathcal{F}/F_0) \neq \emptyset$ then \mathcal{F} is a tower.*

Proof. Since $\text{Split}(\mathcal{F}/F_0) \neq \emptyset$ there is a rational place P in F_0 that splits completely in each extension F_i/F_0 then, by the Hasse-Weil bound, we have that $g(F_i) \rightarrow \infty$ as $i \rightarrow \infty$ so that \mathcal{F} is actually a tower. \square

The *limit* of a tower of function fields \mathcal{F} is given by

$$\lambda(\mathcal{F}) = \frac{N(F)}{g(F)},$$

it always exist and it is a non negative amount, so it is said that the tower is *asymptotically good* if $\lambda(\mathcal{F}) > 0$ and *asymptotically bad* on the other case. Therefore, a tower is asymptotically good if and only if it has non-empty splitting locus and finite ramification locus (see [8, Proposition 7.2.6]).

In this work we will “lift” divisors from one function field F to an extension E by using the conorm map on divisors

$$\text{Con}_{E/F} : \text{Div}(F) \rightarrow \text{Div}(E),$$

that we now recall. If P is a place in F , the conorm divisor of P is the divisor

$$\text{Con}_{E/F}(P) = \sum_{Q|P} e(Q|P) Q$$

in E , where $e(Q|P)$ is the ramification index of the place Q in E over P . Now, the *conorm divisor* of $D = \sum_P n_P P \in \text{Div}(F)$ in E is given by

$$D' := \text{Con}_{E/F}(D) = \sum_P n_P \text{Con}_{E/F}(P).$$

3. SEQUENCES OF LRC

First we will present the construction of a LR code on an extension of function fields. This construction can be found Theorem 3.1 in [1]. We included here for the sake of completeness and adapting it to the function field language.

Theorem 3.1. *Let F a function field over \mathbb{F}_q and let $E = F(x)$ a function field extension of degree m . Let S be a set of places of F that split completely in E/F and such that*

$$\{Q \in \mathbb{P}(E) : Q \cap F \in S\} \cap \{Q \in \mathbb{P}(E) : \nu_Q(x) < 0\} = \emptyset$$

and let $\mathcal{B} = \{Q \in \mathbb{P}(E) : Q \cap F \in S\}$. Then, if $|S| = s > 0$ we have that $|\mathcal{B}| = sm$. Choose a divisor D of F of degree l such that $\text{Supp}(D) \cap S = \emptyset$, and let $\{f_1, \dots, f_\ell\}$ a basis for $\mathcal{L}(D)$, the Riemann-Roch space associated to D . Let $r = m - 1$ and consider the space V generated by

$$\{f_w x^e : w = 1, \dots, \ell; e = 0, \dots, r - 1\}.$$

Since $\text{Supp}(D)$ is disjoint from S , the evaluation map

$$\begin{aligned} ev : V &\longrightarrow \mathbb{F}_q^{(r+1)s} \\ f &\longrightarrow (f(P_{11}), \dots, f(P_{ms})) \end{aligned}$$

is well defined. The image of this mapping is a locally recoverable code \mathcal{C} with locality r , which we denote by $C(S, D)$. The code coordinates are naturally partitioned into s subsets $A_j = \{P_{ij}\}_{i=1, \dots, r+1}$ of size $r+1$ each. Denoting by $g(F)$ the genus of F and $h = [E : \mathbb{F}_q(x)]$, we have that the parameters of the code satisfy

- $n = (r+1)s$,
- $k = rl \geq r(l+1 - g(F))$,
- $d \geq n - l(r+1) - (r-1)h$,

provided that the right-hand side of the inequality for d is a positive integer. Local recovery of an erased symbol $c_{ij} = f(P_{ij})$ can be performed by polynomial interpolation through the positions of the points in the recovery set $A_j \setminus \{P_{ij}\}$.

Remark 3.2. Notice that the previous construction can be performed for any step in a tower of function fields, either consecutive or not.

In particular, we can consider a tower of function fields, and build a LR code, but starting with the rational function field, as the base field in the tower.

Theorem 3.3. Let $\mathcal{F} = \{F_j\}_{j=0}^\infty$ be a sequence of function fields and $\{x_i\}_{i=0}^\infty$ a sequence of transcendental elements over \mathbb{F}_q such that $F_0 = \mathbb{F}_q(x_0)$ is the rational function field and $F_j = F_{j-1}(x_j)$ for every $j > 0$. Denote by $m_j = [F_j : F_{j-1}]$ and consider $E = F_i$, for some index $i \geq 2$. Let S be a set of places of F_0 that split completely in E/F_0 and such that

$$\{Q \in \mathbb{P}(E) : Q \cap F_0 \in S\} \cap \left(\bigcup_{j=1}^i \{Q \in \mathbb{P}(E) : \nu_Q(x_j) < 0\} \right) = \emptyset$$

and let $\mathcal{B} = \{Q \in \mathbb{P}(E) : Q \cap F_0 \in S\}$. Then, if $|S| = s > 0$ we have that $|\mathcal{B}| = sm$ where $m = m_i \dots m_1$. Choose a divisor D of F_0 of degree l such that $\text{Supp}(D) \cap S = \emptyset$, and let D' be the conorm divisor of D in F_{i-1} , i.e., $D' = \text{Con}_{F_{i-1}/F_0}(D)$. Let $\{f_1, \dots, f_w\}$ be a basis for $\mathcal{L}(D')$, the Riemann-Roch space associated to D' . Consider the space V generated by

$$\{f_j x_i^{e_i} : 1 \leq j \leq w \text{ and } 0 \leq e_i \leq m_i - 2\}.$$

Since $\text{Supp}(D)$ is disjoint from S , the evaluation map

$$\begin{aligned} ev : V &\longrightarrow \mathbb{F}_q^{ms} \\ f &\longrightarrow (f(P_{11}), \dots, f(P_{ms})) \end{aligned}$$

is well defined. The image of this mapping is a locally recoverable code with locality $r = m_i - 1$, which we denote by $C_i(S, D)$. The code coordinates are naturally partitioned into $\tilde{m}s$ subsets of size m_i each:

$$\begin{aligned} A_t^j &= \{P_{tu}^j : 1 \leq u \leq m_i\} \\ &= \{Q \in \mathbb{P}(F_i) : Q \cap F_{i-1} = P_{t1}^j \cap F_{i_0-1} = \tilde{P}_t^j\} \end{aligned}$$

where $1 \leq j \leq s$; $1 \leq t \leq \tilde{m}$ and $\tilde{m} = m_{i-1} \dots m_1 = m/m_i$. Denoting by $h = [F_i : \mathbb{F}_q(x_i)]$, we have that the parameters of the code satisfy

- $n = ms = m_i \dots m_1 s$,

- $k = w(m_i - 1) \geq (\deg(D') + 1 - g(F_{i-1}))(m_i - 1) = (\tilde{m}l + 1 - g(F_{i-1}))(m_i - 1)$,
- $d \geq n - lm - (m_i - 2)h$,

provided that the right-hand side of the inequality for d is a positive integer. Local recovery of an erased symbol $f(P_{tu}^j)$ can be performed by polynomial interpolation through the positions of the points in the recovery set $A_t^j \setminus \{P_{tu}^j\}$.

Proof. Straightforward from Theorem 3.1 in the particular case of one step extension in the tower. \square

A modification of the previous result allow us to compute the exact dimension of the code, using a different vector space. Note that in this case, although we can compute the exact dimension, and improve the dimension in some cases, we have to pay a cost in the bound for the minimum distance of the code.

Theorem 3.4. *Let $\mathcal{F} = \{F_j\}_{j=0}^\infty$ be a sequence of function fields and $\{x_i\}_{i=0}^\infty$ a sequence of transcendental elements over \mathbb{F}_q such that $F_0 = \mathbb{F}_q(x_0)$ is the rational function field and $F_j = F_{j-1}(x_j)$ for every $j > 0$. Denote by $m_j = [F_j : F_{j-1}]$ and consider $E = F_i$, for some index $i \geq 2$. Let S be a set of places of F_0 that split completely in E/F_0 and such that*

$$\{Q \in \mathbb{P}(E) : Q \cap F_0 \in S\} \cap \left(\bigcup_{j=1}^i \{Q \in \mathbb{P}(E) : \nu_Q(x_j) < 0\} \right) = \emptyset$$

and let $\mathcal{B} = \{Q \in \mathbb{P}(E) : Q \cap F_0 \in S\}$. Then, if $|S| = s > 0$ we have that $|\mathcal{B}| = sm$ where $m = m_i \dots m_1$. Choose a divisor D of F_0 of degree l such that $\text{Supp}(D) \cap S = \emptyset$, and let $\{f_1, \dots, f_\ell\}$ a basis for $\mathcal{L}(D)$, the Riemann-Roch space associated to D . Consider the space V generated by

$$\{f_w x_1^{e_1} \dots x_i^{e_i} : 1 \leq w \leq \ell; 0 \leq e_i \leq m_i - 2 \text{ and } 0 \leq e_j \leq m_j - 1 \text{ for } j = 1, \dots, i-1\}.$$

Since $\text{Supp}(D)$ is disjoint from S , the evaluation map

$$\begin{aligned} ev : V &\longrightarrow \mathbb{F}_q^{ms} \\ f &\longrightarrow (f(P_{11}), \dots, f(P_{ms})) \end{aligned}$$

is well defined. The image of this mapping is a locally recoverable code \mathcal{C} with locality $m_i - 1$, which we denote by $C_i(S, D)$. The code coordinates are naturally partitioned into $\tilde{m}s$ subsets of size m_i each:

$$\begin{aligned} A_t^j &= \{P_{tu}^j : 1 \leq u \leq m_i\} \\ &= \{Q \in \mathbb{P}(F_i) : Q \cap F_{i-1} = P_{t1}^j \cap F_{i-1} = \tilde{P}_t^j\} \end{aligned}$$

where $1 \leq j \leq s$; $1 \leq t \leq \tilde{m}$ and $\tilde{m} = m_{i-1} \dots m_1 = m/m_i$. Denoting by $h_j = [F_i : \mathbb{F}_q(x_j)]$, we have that the parameters of the code satisfy

- $n = ms = m_i \dots m_1 s$,
- $k = \ell(m_i - 1)m_{i-1} \dots m_1 \geq (l + 1)(m_i - 1)m_{i-1} \dots m_1$,
- $d \geq n - lm - (m_1 - 1)h_1 - \dots - (m_{i-1} - 1)h_{i-1} - (m_i - 2)h_i$.

provided that the right-hand side of the inequality for d is a positive integer. Local recovery of an erased symbol $f(P_{tu}^j)$ can be performed by polynomial interpolation through the positions of the points in the recovery set $A_t^j \setminus \{P_{tu}^j\}$.

Proof. Since $[E : F_0] = \prod_{j=1}^i [F_j : F_{j-1}] = \prod_{j=1}^i m_j$ we have that $n = |\mathcal{B}| = sm_i \dots m_1$. The dimension of the code is the dimension of the vector space V (since the evaluation map is injective). Note also that the bound of the minimum distance is just the length of a codeword minus the maximum number of zeroes that a function f in V can have. In fact, $f_w x_1^{e_1} \dots x_{i-1}^{e_{i-1}} \in F_{i-1}$, and there is a divisor G of F_{i-1} of degree $(l + (m_1 - 1) + \dots + (m_{i-1} - 1))\tilde{m}$ such that

$$f_w x_1^{e_1} \dots x_{i-1}^{e_{i-1}} \in \mathcal{L}(G)$$

and if $Q \in \text{Supp}(G)$ then $Q|P$ for some $P \in \text{Supp}(D)$ or $Q|Q_j$ where Q_j is the simple pole of x_j in $\mathbb{F}_q(x_j)$, for some $j = 1, \dots, i-1$. Therefore, if we denote by \tilde{G} the conorm divisor of G in F_i , i.e., $\tilde{G} = \text{Con}_{F_i/F_{i-1}}(G)$ and $\tilde{Q}_i = \text{Con}_{F_i/\mathbb{F}_q}(Q_i)$ the conorm divisor of the simple pole Q_i of x_i in $\mathbb{F}_q(x_i)$, we have that

$$f_w x_1^{e_1} \dots x_i^{e_i} \in \mathcal{L}(\tilde{G} + (m_i - 2)\tilde{Q}_i)$$

where

$$\begin{aligned} \deg(\tilde{G}) &= [F_i : F_{i-1}] \deg(G) \\ &= [l + (m_1 - 1) + \dots + (m_{i-1} - 1)]\tilde{m} m_i \\ &= [l + (m_1 - 1) + \dots + (m_{i-1} - 1)]m, \end{aligned}$$

and $\deg(\tilde{Q}_i) = [F_i : \mathbb{F}_q(x_i)] = h$. Finally, since a function $f \in V$ can have at most

$$[l + (m_1 - 1) + \dots + (m_{i-1} - 1)]m + (m_i - 2)h$$

poles (and thus zeros) we have a lower bound for the minimum distance. Now, let us show how the recovery of the coordinate is achieved. Let $f \in V$ and

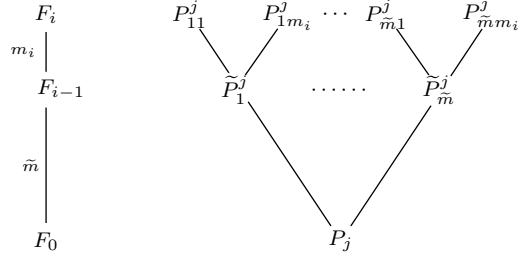
$$\mathbf{c} = (f(P_{11}^1), \dots, f(P_{\tilde{m}m_i_0}^j))$$

be a codeword. Assume, that the coordinate $f(P_{tu}^j)$ is missing, for some fixed t, u and j . Recall that we denote by $P_j = P_{tu}^j \cap F_0$ and $\tilde{P}_t^j = P_{tu}^j \cap F_{i-1}$ (See Figure 1). The recovery set for this coordinate is the evaluation of f in the points of the set $A_t^j \setminus \{P_{tu}^j\}$, in other words, $\{f(P_{tk}^j)\}_{1 \leq k \leq r+1, k \neq u}$. Since $f_w x_1^{e_1} \dots x_{i-1}^{e_{i-1}} \in F_{i-1}$ the evaluation of this in any point of the recovery set is constant and equal to the evaluation in \tilde{P}_t^j . So, $f(P_{tu}^j)$ can be seen as the evaluation in P_{tu}^j of a polynomial in T :

$$\tilde{f}(T) := \sum_{k=0}^{m_i-2} b_k T^k$$

with some appropriate chosen coefficients. And the same is true for all points in the recovery set (since they are all above the same place in F_{i-1}). Therefore, the coefficients b_0, \dots, b_{m_i-1} can be found by polynomial interpolation of the remaining $m_i - 1$ points in the recovery set. \square

Remark 3.5. Notice that the elements in the set S are the places that split completely in all the extensions F_j/F_0 , $j = 1, \dots, i$ but this is not a necessary condition. Actually, the necessary condition is that the places in the set S have above them places of degree one in E , and that we have enough of them to build a recovery set and bound the dimension of V to have an injective application, but they could ramify in some intermediate extension.

FIGURE 1. Diagram of an splitting place P_j of F_0 in F_i

Example 1. For each $q > 2$ let us consider the recursive tower $\mathcal{F} = \{F_j\}_{j=0}^\infty$ over \mathbb{F}_{q^2} defined by Garcia and Stichtenoth in [3], whose defining equation is

$$(4) \quad y^q + y = \frac{x^q}{x^{q-1} + 1}.$$

It is known (see, for instance, [7, Example 5.4.1]) that $N(F_j) \geq q^j(q^2 - q) + 1$ and the genus is given by

$$g(F_j) = \begin{cases} (q^{\frac{j+1}{2}} - 1)^2 & \text{for } j \text{ odd,} \\ (q^{\frac{j}{2}+1} - 1)(q^{\frac{j}{2}} - 1) & \text{for } j \text{ even.} \end{cases}$$

In this case, we have the set

$$S = \{P_\alpha \in \mathbb{P}(F_0) : \alpha \in \mathbb{F}_{q^2} \text{ and } \alpha^q + \alpha \neq 0\},$$

where P_α denotes the only single zero of $x_0 - \alpha$ in the rational function field $F_0 = \mathbb{F}_{q^2}(x_0)$. All the places in S split completely in the tower, so for some $i > 1$ we can consider

$$\mathcal{B}_i = \{Q \in \mathbb{P}(F_i) : Q|P \text{ for some } P \in S\}$$

as the evaluation set. Notice that using the defining equation of the tower, is not hard to verify that the places in \mathcal{B}_i are not poles of x_j , $j = 0, \dots, i$. Moreover, the only pole of x_0 in F_0 , that we denote by P_∞ is totally ramified in the tower, and we can choose $D = lP_\infty$. Since \mathcal{F} is an asymptotically good tower and every step in the tower is of degree q , we have that $m = [F_i : F_0] = q^i = [F_i : \mathbb{F}_q^2(x_i)] = h$. Therefore, considering the set

$$V_i = \langle x_0^{e_0} x_1^{e_1} \cdots x_i^{e_i} : 0 \leq e_0 \leq l; 0 \leq e_i \leq q-2 \text{ and } 0 \leq e_j \leq q-1 \text{ for } j = 1, \dots, i-1 \rangle,$$

we can build a locally recoverable code $C_i(S, D)$ with locality $q - 1$, whose parameters satisfy

$$\begin{aligned} n &= q^i(q^2 - q) \\ k &= (l + 1)(q - 1)q^{i-1} \\ d &\geq (q^2 - 2q + 2 - l - (q - 1)(i - 1))q^i \end{aligned}$$

provided that the right-hand side of the third inequality for d is a positive integer.

Notice that in the case $i = 1$ the same construction can be done, where

$$V_1 = \langle x_0^{e_0} x_1^{e_1} : 0 \leq e_0 \leq l; 0 \leq e_1 \leq q - 2 \rangle.$$

Remark 3.6. For $1 < i \leq q - 1$ and $1 \leq l \leq (q - 1)(q - i)$, the code $C_i(S, D)$ in the previous example verifies $d > 0$ since

$$d \geq (q^2 - 2q + 2 - l - (q - 1)(i - 1))q^i = ((q - 1)(q - i) - l + 1)q^i > 0$$

Example 1. (cont.) Taking into account the previous remark, if we want to maximize the dimension, we can choose $l = (q-1)(q-i)$ and in this case we obtain codes $C_i(S, D)$ for $i \leq q-1$ with the following relative parameters:

$$R = \frac{k}{n} = \frac{(l+1)}{q^2} \geq \frac{1}{q} \quad \text{and} \quad \delta = \frac{d}{n} \geq \frac{1}{q(q-1)}.$$

4. A PARTICULAR CASE FOR SMALL STEPS

In this section we will work with the tower presented in Example 1, and we will show that the bound presented in Theorem 3.4 is sharp for the first two steps in the tower.

Proposition 4.1. *For $q \geq 5$, the code $C_2(S, D)$ of Example 1 with $D = qP_\infty$, is a locally recoverable code over \mathbb{F}_{q^2} , with locality $r = q-1$, whose parameters are*

$$\begin{aligned} n &= q^2(q^2 - q), \\ k &= (q+1)q(q-1) = q^3 - q, \\ d &= q^2(q^2 - q - q - (q-1) - (q-2)) = q^2(q^2 - 4q + 3). \end{aligned}$$

Proof. The set $S_0 = \{\alpha \in \mathbb{F}_{q^2} : \alpha^q + \alpha \neq 0\}$, can be naturally partitioned into $q-1$ disjoint subsets

$$(5) \quad S_i = \left\{ \alpha \in \mathbb{F}_{q^2} : \frac{\alpha^q}{\alpha^{q-1} + 1} = \frac{\alpha^{q+1}}{\alpha^q + \alpha} =: \beta_i \right\}, \quad \beta_i \in \mathbb{F}_q^*$$

each one of size q . For a rational place $P \in \mathbb{P}(F_j)$, we denote

$$N(P) = N_{\mathbb{F}_{q^2}/\mathbb{F}_q}(x_j(P)) = x_j(P)^{q+1}$$

and

$$Tr(P) = Tr_{\mathbb{F}_{q^2}/\mathbb{F}_q}(x_j(P)) = x_j(P)^q + x_j(P),$$

where x_j is the transcendental element over \mathbb{F}_{q^2} such that $F_j = F_{j-1}(x_j)$, for every step j in the tower. Using the defining equation of the tower, we have that if Q is a place of F_j over a place P of F_{j-1} such that $x_{j-1}(P) \in S_i$, then

$$Tr(Q) = \frac{N(P)}{Tr(P)} = \beta_i.$$

In particular we obtain that, for each place $P \in \mathcal{B} \cap \mathbb{P}(F_{j-1})$ and each S_i , there are at most two places Q_1 and Q_2 of \mathcal{B} such that

$$x_{j-1}(Q_1) = x_{j-1}(Q_2) = x_{j-1}(P) \in S_i,$$

since there are at most two elements in \mathbb{F}_{q^2} with the same norm and trace. Moreover, if σ is the only non trivial automorphism in $\mathbb{F}_{q^2}/\mathbb{F}_q$, we have that

$$x_j(Q_1) = \sigma(x_j(Q_2)),$$

and since q is odd, there is exactly one remaining place $Q|P$ such that

$$x_{j-1}(Q) = x_{j-1}(P) \in S_i, \quad \text{and} \quad \sigma(x_j(Q)) = x_j(Q).$$

In other words, if we consider the $q-1$ disjoint sets

$$(6) \quad B_i = \{\alpha \in \mathbb{F}_{q^2} : Tr(\alpha) = \beta_i\}, \quad \text{for } \beta_i \in \mathbb{F}_q^*,$$

we have that for any indexes $1 \leq i, k \leq q-1$,

$$(7) \quad |S_k \cap B_i| = |\{Q \in \mathbb{P}(F_j) : x_j(Q) \in S_k \text{ and } x_j(Q) \in B_i\}| \leq 2$$

and

$$(8) \quad |\{Q \in \mathbb{P}(F_j) : x_j(Q) \in S_k \text{ and } x_j(Q) \in B_i\}| = 1 \text{ if and only if } x_j(Q) \in \mathbb{F}_q.$$

Now, using the notation in Theorem 3.4, we take $i = 2$ and $l = q$ and we consider $D = lP_\infty$ so that V is generated by

$$\{x_0^{e_0} x_1^{e_1} x_2^{e_2} : 0 \leq e_0 \leq q; 0 \leq e_1 \leq q-1; 0 \leq e_2 \leq q-2\}.$$

From the proof of the theorem we have that any function on V has at most

$$(l+1)q^2 + q^3 + (q-1)q^2 = q^2(3q-3)$$

zeros, and we will now exhibit a function that actually achieves that number of zeros. Consider an element $\beta_1 \in \mathbb{F}_{q^2}^*$ and set

$$h_0 = \prod_{\alpha \in S_1} (x_0 - \alpha),$$

so we have exactly $q^3 = |S_1|[F_2 : F_0]$ places $Q \in \mathcal{B}$ that are zeroes of h_0 . In other words, for any of these places we have that $x_0(Q) \in S_i$ and $x_1(Q) \in B_1$, by the recursive definition of the tower. Now since q is odd, chose β_i such that

$$|S_i \cap B_1| = 1$$

and set

$$h_1 = \prod_{\alpha \in S_i \setminus B_1} (x_1 - \alpha),$$

so we have $(q-1)q^2 = (|S_i| - 1)[F_2 : F_1]|\{Q \in F_1 : x_1(Q) = \alpha\}|$ new places $Q \in \mathcal{B}$ that are zeroes of h_1 .

Since $|B_1| = q$, from (7) and (8), we can write B_1 as a disjoint union of $(q+1)/2$ non empty sets

$$B_1 = \bigcup_{k=1}^{\frac{q+1}{2}} B_1 \cap S_{i_k}$$

and therefore if $Q \in \mathcal{B}$ is such that $x_0(Q) \in S_1$ or $x_1(Q) = S_i$ then $x_2(Q)$ is one of the $q(q+1)/2$ different values in \mathbb{F}_{q^2} . Now, since $q \geq 5$ implies that $q \left(\frac{q+1}{2}\right) < q^2 - q - (q-2)$ we can choose $q-2$ values $\gamma_1, \dots, \gamma_{q-2}$ in S_0 such that $x_2(Q) = \gamma_i$ for $Q \in F_2$ and

$$h_2 = \prod_{i=1}^{q-2} (x_2 - \gamma_i),$$

has $q^2(q-2)$ new different zeros in \mathcal{B} .

Therefore, $f = h_0 h_1 h_2 \in V$ has exactly $q^3 + (q-1)q^2 + (q-2)q^2 = q^2(3q-3)$ zeroes, attaining the bound provided by Theorem 3.4. \square

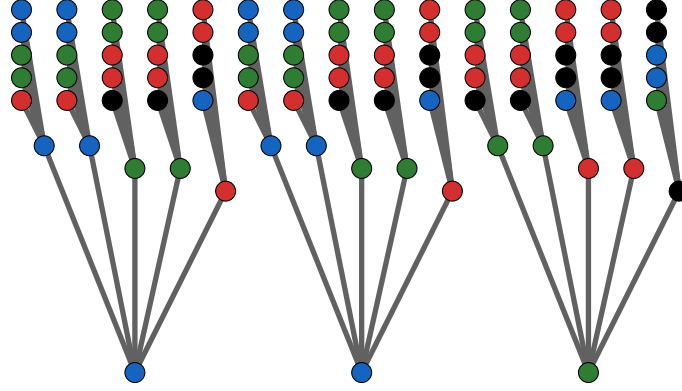


FIGURE 2. Diagram of three splitting places P_j of F_0 in F_2/F_0 , for $q = 5$. Each colour, in each function field, represent a set S_i , for $1 \leq i \leq 4 = q - 1$

Proposition 4.2. *For each odd $q \geq 5$, the code $C_2(S, D)$ in Example 1 with $D = \frac{q(q-1)}{2}P_\infty$, is a locally recoverable code over \mathbb{F}_{q^2} , with locality $r = q - 1$, whose parameters are*

$$\begin{aligned} n &= q^2(q^2 - q), \\ k &= q(q - 1) \left(q \left(\frac{q-1}{2} - 1 \right) + 1 \right), \\ d &= \frac{1}{2}q^2 (q^2 - 3q + 6). \end{aligned}$$

Proof. We follow the same notation as in the previous proposition and we only consider two steps in the tower. Chose one subset, let us say S_1 , which we know it has q elements. So,

$$|\{P \in \mathbb{P}(F_1) : x_1(P) \in S_1\}| = q^2$$

since for each value $x_1(P) \in S_1$ we have q different places $P_\alpha \in \mathbb{P}(F_0)$ under P . Since these places in F_1 come “in pairs” (with the only exceptions of places P with $x_1(P) \in \mathbb{F}_q$) and there are exactly q places $P_\alpha \in \mathbb{P}(F_0)$ with only one place $P|P_\alpha$ and $x_1(P) \in S_1$, we have that there are exactly $\frac{q^2-q}{2} = q\frac{q-1}{2}$ places $P_\alpha \in \mathbb{P}(F_0)$ with two distinct places $P|P_\alpha, \sigma(P)|P_\alpha$ and $x_1(P) \in S_1$. Now we choose the remaining $q^2 - q - q\frac{q-1}{2} - q = q\frac{q-1}{2} - q$ places $P_\alpha \in S \subset \mathbb{P}(F_0)$ such that for all $P \in \mathbb{P}(F_1)$ with $P|P_\alpha$ we have that $x_1(P) \notin S_1$. Set then

$$\mathbb{H}_0 = \{P_\alpha \in S : x_1(P) \notin S_1 \text{ for all } P|P_\alpha\},$$

of cardinality $q \left(\frac{q-1}{2} - 1 \right)$, and put $H_0 = \{x_0(P) : P \in \mathbb{H}_0\}$.

Now, defining

$$h_0 = \prod_{s \in H_0} (x_0 - s) \in V$$

we have that h_0 has $q^3 \left(\frac{q-1}{2} - 1 \right) = \frac{q^4 - 3q^3}{2}$ different zeros in \mathcal{B} .

Now, among all the $q^2(q^2 - q)$ places Q in $\mathcal{B} \subset \mathbb{P}(F_2)$, such that $Q \cap F_0 \in S \setminus \mathbb{H}_0$, the value $x_1(Q)$ can attain $q^2 - q$ possible values, q of those are in S_1 . Since

$$|\{x_1(Q) : Q \in \mathcal{B} \text{ and } Q \cap F_0 \in \mathbb{H}_0\}| = q \left(\frac{q-1}{2} - 1 \right)$$

(recall that the places are naturally partitioned into subsets of size q and inside each subset these places decompose in the same way) and $q \geq 5$, then we have

$$(q^2 - q) - q - q \left(\frac{q-1}{2} - 1 \right) \geq q,$$

so we can build a non empty set $H_1 \subset \mathbb{F}_{q^2}$ of cardinality $q - 1$ such that

$$H_1 \subset \{x_1(Q) : Q \in F_1, Q \cap F_0 \notin H_0 \text{ and } x_1(Q) \notin S_1\}$$

and this allow us to form a function

$$h_1 = \prod_{s \in H_1} (x_1 - s) \in V$$

of degree $q - 1$ with $q^2(q - 1)$ zeroes in \mathcal{B} .

Finally, since no point Q that is a zero of h_0 or h_1 verifies $x_1(Q) \in S_1$ by construction of H_0 and H_1 , we can consider some subset $H_2 \subset \{x_2(Q) : x_1(Q) \in S_1\} = B_1 \subset \mathbb{F}_{q^2}$ of size $q - 2$ and set

$$h_2 = \prod_{s \in H_2} (x_2 - s)$$

of degree $q - 2$ with $q^2(q - 2)$ distinct zeroes in \mathcal{B} .

Since the subsets $\{Q \in \mathcal{B} : x_0(Q) \in H_0\}, \{Q \in \mathcal{B} : x_1(Q) \in H_1\}, \{Q \in \mathcal{B} : x_2(Q) \in H_2\}$ are pairwise disjoint by construction of H_0, H_1, H_2 , we obtain that $f = h_0 h_1 h_2 \in V$ has exactly $\frac{q^4 - 3q^3}{2} + (q - 1)q^2 + q^2(q - 2) = \frac{1}{2}q^2 (q^2 + q - 6)$ zeroes, and thus the minimum distance is exactly

$$\begin{aligned} q^2(q^2 - q) - \frac{1}{2}q^2 (q^2 + q - 6) &= \frac{1}{2}q^2 (q^2 - 3q + 6) \\ &= q^2 \left(q^2 - 2q + 2 - q \left(\frac{q-1}{2} - 1 \right) - (q - 1) \right) \end{aligned}$$

attaining the bound provided by the theorem and the example. \square

The above results show that, in the considered tower, the lower bound for the minimum distance was attained for a small step in the tower, that is, considering the extension F_2 of F_0 over \mathbb{F}_{q^2} . Next, we show that in further steps (i.e., considering extensions F_j/F_i for $j \geq i + 3$) there are common zeroes of x_j and x_i , so the bound will never be attained for this tower.

In the following lemma, we use the same notation as in the previous propositions.

Lemma 4.3. *Consider the field extensions F_j/F_0 over \mathbb{F}_{q^2} of the Garcia-Stichtenoth tower of Example 1. Set $\mathcal{B} \subset \mathbb{P}(F_j)$ the evaluation set with $q^j(q^2 - q)$ places and $S = \{Q \cap F_0, Q \in \mathcal{B}\} \subset \mathbb{P}(F_0)$. For $S_0 = \bigcup_{j=1}^{q-1} S_j \subset \mathbb{F}_{q^2}$, we have*

- (1) *For $0 \leq i \leq j$ and $\alpha \in \mathbb{F}_{q^2} \setminus S_0$, the function $x_i - \alpha$ have no zeroes in \mathcal{B} . For $\alpha \in S_0$, the function $x_i - \alpha$ have exactly q^i zeroes in \mathcal{B} .*
- (2) *For $1 \leq i \leq j$ and $\alpha \in S_0$, if $Q \in \mathbb{P}(F_i)$ is a zero of $x_i - \alpha$, then $P = Q \cap F_{i-1}$ verifies $x_{i-1}(P) \in S_k$, where $\alpha \in B_k$,*

- (3) Conversely, for $1 \leq i \leq j$ and $\alpha \in S_0$, if $P \in \mathbb{P}(F_{i-1})$, verifies $x_{i-1}(P) \in S_k$, where $\alpha \in B_k$, then exists exactly one place $Q \in \mathbb{P}(F_i)$ with $Q|P$ that is a zero of $x_i - \alpha$.

Proof. The proof of the first part follows from the definition of S_0 and the fact that each place $P \in \mathbb{P}(F_{i-1}) \cap \mathcal{B}$ has exactly q places of F_i above it. The second and third part are straightforward from the definitions (see equations (5) and (6)) of the sets S_i and B_i , for $1 \leq i \leq j$ and the recursive defining equation of the tower. \square

Since there are exactly q^j places $Q \in \mathbb{P}(F_j)$ laying above a place in $S = \mathcal{B} \cap \mathbb{P}(F_0)$, and exactly $q^{j-1}(q^2 - q) = q^j(q - 1)$ places in $\mathbb{P}(F_{j-1})$, we obtain a one-to-one bijection between zeroes Q of $x_j - \alpha$ and places $P \in \mathbb{P}(F_{j-1})$ with $x_{j-1}(P) \in S_k$, where $\alpha \in B_k$.

Definition 3. We say $Q \in \mathbb{P}(F_j)$ it is colored k if $x_j(Q) \in S_k$ for some $1 \leq k \leq q-1$, where Q lays under some place in \mathcal{B} .

Let $i \geq 0$, and $j \geq i + 3$. There are exactly $\frac{q+1}{2}$ different colours appearing over some place $P \in \mathbb{P}(F_i)$. On the other hand, when considering places F_j , each colour appears above exactly $\frac{q+1}{2}$ different colours; that is, for fixed S_l there are exactly $\frac{q+1}{2}$ indexes $\{l_1, \dots, l_{\frac{q+1}{2}}\}$ such that for $Q \in \mathbb{P}(F_j)$ with $x_j(Q) \in S_l$ it is $x_{j-1}(Q \cap F_{j-1}) \in S_k$ for some $k \in \{l_1, \dots, l_{\frac{q+1}{2}}\}$.

Recall that two places of the same colour, when decompose, they decompose each in q places of the same $\frac{q+1}{2}$ colours, independently of the function field they belong.

Corollary 4.4. For $j \geq i + 3$ and any $\alpha, \beta \in S_0$, the functions $x_i - \alpha$ and $x_j - \beta$ have at least one common zero $Q \in \mathcal{B}$.

Proof. Let $Q_0 \in \mathcal{B}$ be a zero of $x_j - \beta$ and $P \in \mathbb{P}(F_i)$ be a zero of $x_i - \alpha$. Without loss of generality, we can assume P is of colour *blue* and $Q_0 \cap F_{i+2}$ is *black*. By the pigeonhole principle, among the $\frac{q+1}{2}$ colours above P and among the $\frac{q+1}{2}$ colours below any black place, there is at least one colour in common, let us say *green*. Then, there is a place $P_0 \in \mathbb{P}(F_{i+1})$ such that $P_0|P$ and P_0 is green, therefore there is also a place $P_1 \in \mathbb{P}(F_{i+2})$ such that $P_1|P_0$ and P_1 is black. Finally, since P_1 is black, there is also a place $Q \in \mathbb{P}(F_j)$ such that $Q|P_1$ and $x_j(Q) = x_j(Q_0) = \beta$. Since $Q|P$ we also have $x_i(Q) = x_i(P) = \alpha$. Thus, $Q \in \mathcal{B}$ and it is a common zero of $x_i - \alpha$ and $x_j - \beta$. \square

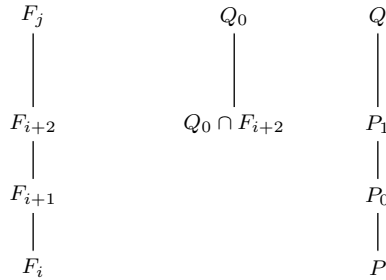


FIGURE 3. Diagram of extension and places of Corollary 4.4

The previous corollary, make us conjecture the following:

Conjecture 4.5. *Any function $f \in V$ will have fewer than*

$$lq^k + (k-1)(q-1)q^{k-1} + (q-2)q^{k-1}$$

zeroes in \mathcal{B} , and therefore the lower bound for the distance in Theorem 3.4 will not be attained for $i \geq 3$.

5. RELATIVE PARAMETERS AND ASYMPTOTICS

In this last section, we will analyze the relative parameters R and δ of the codes $C_i(S, D)$ built in the previous sections, using the tower described in Example 1.

Proposition 5.1. *For each odd $q \geq 5$ and any $2 \leq i \leq q-1$, $1 \leq l \leq (q-1)(q-i)$, the relative parameters R and δ of $C_i(S, D)$ with $D = lP_\infty$ verify:*

$$R + \frac{q-1}{q}\delta > \frac{r}{r+1} \left(\frac{q-i}{q} \right),$$

where $r = q-1$ is the locality of C_i .

Proof. Since $\delta \geq \frac{((q-1)(q-i)-l+1)q^i}{q^i(q^2-q)} = \frac{q}{q-1} \frac{(q-1)(q-i)-l+1}{q^2}$ we have

$$R + \frac{q-1}{q}\delta \geq \frac{(q-1)(q-i)+2}{q^2} > \frac{(q-1)(q-i)}{q^2} = \frac{r}{r+1} \left(\frac{q-i}{q} \right).$$

□

In the case $i = 2$, we have the following result, similar to the bound shown in [6].

We now compare the relative parameters of the codes $C_2(S, D)$ with $D = (q \frac{q-1}{2}) P_\infty$ shown in Proposition 4.2. Recall that

$$R = \frac{k}{n} = \frac{(l+1)}{q^2} \quad \text{and} \quad \delta = \frac{d}{n} \geq \frac{(q-1)(q-2)-l+1}{q^2-q}.$$

Proposition 5.2. *For each odd $q \geq 5$ and any $1 \leq l \leq (q-1)(q-2)$, the relative parameters R and δ of $C_2(S, D)$ with $D = lP_\infty$ verify:*

$$R + \frac{q-1}{q}\delta > \frac{r}{r+1} \left(\frac{q-2}{q} \right),$$

or equivalently,

$$(9) \quad R > \frac{r}{r+1} \left(1 - \delta - \frac{2}{q} \right),$$

where $r = q-1$ is the locality of C_2 .

Proof. Since $\delta = \frac{(q-1)(q-2)-l+1}{q^2-q} = \frac{q}{q-1} \frac{(q-1)(q-2)-l+1}{q^2}$ we have

$$R + \frac{q-1}{q}\delta = \frac{(q-1)(q-2)+2}{q^2} > \frac{(q-1)(q-2)}{q^2} = \frac{q-1}{q} \left(1 - \frac{2}{q} \right).$$

□

Proposition 5.3. *For each odd $q \geq 5$ and $l = q \left(\frac{q-1}{2} - 1 \right)$, the relative parameters R and δ of $C_2(S, D)$ with $D = lP_\infty$ verify:*

$$(10) \quad R = \frac{(l+1)}{q^2} > \frac{1}{2} \left(\frac{q-2}{q} \right)^2 \quad \text{and} \quad \delta = \frac{(q-1)(q-2) - l + 1}{q^2 - q} > \frac{1}{2} \left(\frac{q-3}{q-1} \right).$$

Proof. By Proposition 4.2 we have $n = q^2(q^2 - q)$, $k = (l+1)(q-1)q$ and $d = \frac{1}{2}q^2(q^2 - 3q + 6)$ so

$$\begin{aligned} R &= \frac{l+1}{q^2} \\ &= \frac{q \left(\frac{q-1}{2} - 1 \right) + 1}{q^2} \\ &= \frac{1}{2} \frac{q(q-1-2) + 2}{q^2} \\ &= \frac{1}{2} \frac{(q-1)(q-2)}{q^2} > \frac{1}{2} \left(\frac{q-2}{q} \right)^2. \end{aligned}$$

On the other hand,

$$\delta = \frac{1}{2} \frac{q^2 - 3q + 6}{q^2 - q} > \frac{1}{2} \frac{q-3}{q-1}.$$

□

For $q \geq 5$ and $1 \leq l \leq (q-1)(q-2)$, Proposition 5.2 ensures that the relative parameters of $C_2(S, D)$ are all above the line $R = \frac{q}{q+1} \left(1 - \delta - \frac{2}{q} \right)$ improving slightly a result in [1], while Proposition 5.3 shows the existence of a code whose relative parameters lie exactly on that line. In Figures 4 and 5 below, we can see those cases for $q = 7$ and $q = 17$.

Remark 5.4. *For $C_3(S, D)$ and $1 \leq l \leq (q-1)(q-3)$ we can not guarantee by Proposition 5.1 that its relative parameters (R, δ) lie above that line $R = \frac{q}{q+1} \left(1 - \delta - \frac{3}{q+1} \right)$. However, taking Corollary 4.4 in consideration, one could expect that the lower bound of δ may be improved from some step and on, obtaining in this way a stronger lower bound for δ .*

Remark 5.5. *For q sufficiently large, and for certain $2 \leq i \leq q-1$, and $1 \leq l \leq (q-1)(q-i)$, we have from Proposition 5.1, that the lower bound for the relative parameters (R, δ) of $C_i(S, D)$ with $D = lP_\infty$, improves a bound analogous to the GV bound, derived in [11]. This is, for suitable i and l , we have that (R, δ) lies above the curve*

$$(11) \quad R = \frac{r}{r+1} - \min_{0 < s \leq 1} \left\{ \frac{1}{r+1} \log_q b_2(s) - \delta \log_q(s) \right\}$$

where $b_2(s) = \frac{1}{q} \left((1 + (q-1)s)^{r+1} + (q-1)(1-s)^{r+1} \right)$.

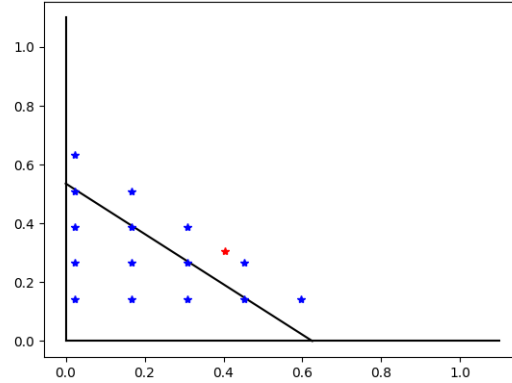


FIGURE 4. Inequality (1) for $r + 1 = q = 7$ is shown as a black line. For $2 \leq i \leq 6$, lower bounds of the relative parameters of $C_i(S, D)$ are shown as blue points. The parameters of $C_2(S, D)$ shown in (10) appeared as a red point.

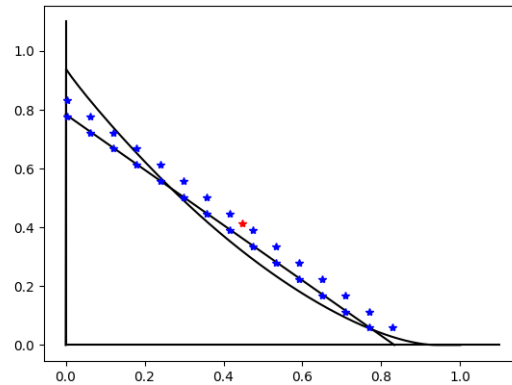


FIGURE 5. Inequalities (1) and (11) for $r + 1 = q = 17$ are shown as black curves. For $2 \leq i \leq 3$, lower bounds of the relative parameters of $C_i(S, D)$ are shown as blue points. The parameters of $C_2(S, D)$ shown in (10) appeared as a red point.

REFERENCES

- [1] Alexander Barg, Itzhak Tamo, and Serge Vlăduț. Locally recoverable codes on algebraic curves. *IEEE Transactions on Information Theory*, 63(8):4928–4939, 2017.
- [2] María Chara, Sam Kottler, Beth Malmskog, Bianca Thompson, and Mckenzie West. Minimum distance and parameter ranges of locally recoverable codes with availability from fiber products of curves. [*arXiv:2204.03755*], 2022.
- [3] Arnaldo Garcia and Henning Stichtenoth. On the galois closure of towers. *Recent trends in coding theory and its applications*, 41:83–92, 2007.

- [4] P. Gopalan, C. Huang, H. Simitci, and S. Yekhanin. On the locality of codeword symbols. *IEEE Trans. Inf. Theory*, 58(11):6925–6934, 2012.
- [5] Kathryn Haymaker, Beth Malmskog, and Gretchen L Matthews. Locally recoverable codes with availability $t \geq 2$ from fiber products of curves. *Advances in Mathematics of Communications*, 12(2):317, 2018.
- [6] Xudong Li, Liming Ma, and Chaoping Xing. Construction of asymptotically good locally repairable codes via automorphism groups of function fields. *IEEE Trans. Inform. Theory*, 65(11):7087–7094, 2019.
- [7] Harald Niederreiter and Chaoping Xing. *Rational points on curves over finite fields: Theory and Applications*, volume 285. London Mathematical Society Lecture Note Series, 285. Cambridge University Press, Cambridge, 2001.
- [8] Henning Stichtenoth. *Algebraic function fields and codes*, volume 254. Springer Science & Business Media, 2009.
- [9] Itzhak Tamo and Alexander Barg. Bounds on locally recoverable codes with multiple recovering sets. *2014 IEEE International Symposium on Information Theory*, pages 691–695, 2014.
- [10] Itzhak Tamo and Alexander Barg. A family of optimal locally recoverable codes. *IEEE Transactions on Information Theory*, 60(8):4661–4676, 2014.
- [11] Itzhak Tamo, Alexander Barg, and Alexey Frolov. Bounds on the parameters of locally recoverable codes. *IEEE Transactions on Information Theory*, 62(6):3070–3083, 2016.

Email address: M. Chara: `mchara@santafe-conicet.gov.ar`

Email address: F. Galluccio: `frangallu996@gmail.com`

Email address: E. Martinez-Moro: `edgar.martinez@uva.es`